Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

ISTITUTO COMPRENSIVO 5 - -NOCERA INFERIORE
Prot. 0004556 del 04/09/2023
III-4 (Entrata)

PROGETTO TECNICO

PROGETTO "INNOVAzioni 4.0" nell'ambito del piano Next Generation EU - PNRR – Missione 4: Istruzione e ricerca – Componente 1 – Investimento 3.2: Scuola 4.0 – Azione 1 – Next generation classroom – Ambienti di apprendimento innovativi.

Committente: V ISTITUTO COMPRENSIVO di NOCERA INFERIORE (SA)

C.F. 94076690653

Sede legale: Via Marconi - 84014– Nocera Inferiore (SA)

TITOLO DEL PROGETTO: "INNOVAzioni 4.0"
CUP: E34D22005320006

Codice Progetto: M4C1I3.2-2022-961-P-18553

Il presente progetto descrive gli aspetti tecnici relativi alla fornitura di prodotti e servizi per la realizzazione di ambienti didattici innovativi nell'ambito del potenziamento dell'offerta dei servizi di istruzione: dagli asili nido alle Università Investimento 3.2: Scuola 4.1 Azione 1 - Next generation classroom.

Il sottoscritto Per. Ind. Sandro Falivene, in qualità di Progettista del progetto in epigrafe, con la presente, sottopone all'attenzione di codesto spett.le Istituto, relazione Tecnica e capitolato degli ambienti oggetto di intervento, relativamente al progetto indicato in oggetto. Si precisa che sono state esperite tutte le operazioni necessarie in risposta alle richieste pervenute, con effettuazione di sopralluoghi e rilievo dati degli apparati ed infrastruttura esistente, di tutti i plessi dell'Istituto interessati dalla realizzazione del progetto in conformità del **target minimo richiesto pari a 15**.

Pertanto, quanto di seguito descritto, è stato redatto, in conformità alle richieste dell'Istituto e sulla base delle esigenze emerse e delle verifiche effettuate durante il sopralluogo tecnico ed in considerazione della proposta progettuale inoltrata.

La presente relazione è articolata nelle seguenti sezioni e sottosezioni:

1. PREMESSA
2. DESCRIZIONE DEL PROGETTO
3. ANALISI PRELIMINARE E RICOGNIZIONE DEGLI SPAZI E DELLE DOTAZIONI ESISTENTI
4. CAPITOLATO E SPECIFICHE TECNICHE

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

1 – PREMESSA

L'Istituto ha aderito al progetto PNRR – Missione 4: Istruzione e ricerca – Componente 1 – Investimento 3.2: Scuola 4.0 – Azione 1 – Next generation classroom – Ambienti di apprendimento innovativi che ha l'obiettivo di trasformare almeno 100.000 aule delle scuole primarie, secondarie di primo grado e secondarie di secondo grado, in ambienti innovativi di apprendimento. Ciascuna istituzione scolastica ha la possibilità di trasformare la metà delle attuali classi/aule grazie ai finanziamenti del PNRR. L'istituzione scolastica potrà curare la trasformazione di tali aule sulla base del proprio curricolo, secondo una comune matrice metodologica che segue principi e orientamenti omogenei a livello nazionale, in coerenza con gli obiettivi e i modelli promossi dalle istituzioni e dalla ricerca europea e internazionale.

2 - DESCRIZIONE DEL PROGETTO

Il Quinto Istituto Comprensivo, ubicato a Nocera Inferiore, ha cinque sedi dislocate nelle zone limitrofe dell'agro-nocerino-sarnese. Quattro plessi, sede di Scuola Primaria e Scuola Secondaria di I grado, sono dotati di ampi locali, che permettono di coniugare lo spazio fisico, l' ambiente comunicativo ed educativo, dove si costruiscono le relazioni, e l' ambiente virtuale, diventando così una grande risorsa educativa. Sulla base di quanto indicato nel Piano "Scuola 4.0", l'Istituzione scolastica ha stabilito di adottare in questi plessi il modello ibrido che prevede il potenziamento e/o l'integrazione dei dispositivi tecnologici nelle "aule fisse" e la realizzazione di nuovi ambienti di apprendimento che sono ideati con particolare attenzione a tutte le componenti, al fine di sviluppare una riorganizzazione didattico-metodologica implementando paradigmi didattici che hanno bisogno di strumenti tecnologici e software didattici di supporto. L'intento è di promuovere l'inclusione, la sostenibilità e la cittadinanza attiva , oltre a processi di rinnovamento della pratica pedagogico-didattica. Saranno realizzati in modalità ibrida quindici ambienti innovativi, spazi di apprendimento con infrastrutture tecnologiche nuove o implementate, flessibili, con arredi modulari specifici restituendo ad ogni asse disciplinare una dimensione laboratoriale e sviluppando autonomia e responsabilizzazione nei vari gruppi di lavoro per consentire attività di gruppo, ricerca, cooperative learning, lettura/recitazione, recupero degli apprendimenti, didattica a classi parallele, studio collettivo. Alcune aule saranno riconfigurate per consentire alla scuola di sperimentare la Didattica per Ambienti di Apprendimento (DADA), dedicate a più aree tematiche, all' Arte e Tecnologia, alle Scienze Geografiche e Naturali, alla Musica ed alle arti espressive, alla lettura ed ascolto, drammatizzazione e recitazione; qualche aula sarà allestita in modo da essere polifunzionale: gli alunni potranno sperimentare nuove modalità di scuola, in cui parola, suono, gesto, immagine, tecnologia si fondono., In perfetto unisono con i principi della Gestalt Esperienziale, delle ricerche nell' ambito delle neuroscienze e della psicologia relazionale; si creeranno, pertanto, per gli studenti nuove opportunità formative ed inclusive e nuove strategie organizzative; alcuni Docenti avranno un loro ambiente di apprendimento e si innoveranno l' educazione linguistico-storico-letteraria, l' ambito scientifico e artistico e, con l' aumento del senso di responsabilità ed autonomia, gli studenti sperimenteranno anche nuove opportunità di educazione alla cittadinanza attiva : "creatività", "comunicazione", "collaborazione", "inclusione" racchiudono perfettamente il senso del Progetto "INNOVAzioni 4.0" promosso dall'istituzione scolastica

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

3 - ANALISI PRELIMINARE E RICOGNIZIONE DEGLI SPAZI E DELLE DOTAZIONI ESISTENTI

L'Istituzione scolastica ha partecipato ai precedenti finanziamenti PON FESR come Smart Class, Digital Board e Reti cablate ed alle misure del PNSD inerenti alla Didattica Digitale Integrata e alla Didattica a Distanza e STEM. Grazie a questi finanziamenti i quattro plessi della Scuola Primaria e della Scuola Secondaria sono stati dotati di un' infrastruttura di rete capace di coprire gli spazi didattici e di consentire la connessione alla rete da parte del personale scolastico, delle studentesse e degli studenti, nonchè di strumentazioni digitali nuove: alcuni monitor di ultima generazione sono stati carrellati e resi trasportabili dovunque per ciascun plesso e 18 aule dotate di monitor touch di nuovissima generazione e dei nuovissimi notebook a completamento; un laboratorio con dotazioni STEM e set di coding e robotica educativa. Le aule rimanenti sono dotate di LIM, ancora funzionanti e di laptop più lenti, ma regolarmente operanti con il potenziamento della rete operato attraverso il cablaggio. Nuovi arredi, sostanzialmente banchi monoposto e relative sedute sono stati acquisiti per l¿emergenza, a supporto di un gran numero di aule. Si elencano le strumentazioni elettroniche acquisite con le varie misure: PNSD STEM n. 13 Robot - n. 13 KIT per ROBOT - n. 3 stampanti 3 D - n. 7 bobine per stampa 3 D - n. 10 Robotica Ability Krypton -n. 1 kit fotosintesi - n. 1 laboratorio analisi portatile PNSD STEM art. 120 (lett. A D.L. 18/2020) - n. 20 Notebook - n. 8 Tablet PNSD STEM art. 120 (lett.. B D.L. 18/2020) - n. 2 Notebook - Access point PNSD # 28 n. 1 Notebook - n. 2 tablet PNSD DDI Mezzogiorno n. 4 Monitor - n. 2 carrelli portamonitor - PON FESR SMART CLASS n. 18 Notebook - n. 21 Tablet PON FESR DIGITAL BOARD n. 18 Monitor - n. 1 stampante - n. 4 tavolette grafiche - L'esigenza prioritaria dell'Istituto è sicuramente migliorare ulteriormente le dotazioni tecnologiche degli gli ambienti didattici per poter attuare una reale didattica di tipo collaborativo ed incidere significativamente sulla motivazione all'apprendimento, sullo stile di apprendimento, sull'inclusione e sul successo formativo delle nuove generazioni.

4 - CAPITOLATO E SPECIFICHE TECNICHE

Il presente Capitolato Speciale definisce e disciplina la fornitura e le specifiche tecniche, funzionali e prestazionali per la realizzazione del progetto che presenta il seguente piano finanziario:

PIANO FINANZIARIO PROGETTO

Importo massimo a base d'asta euro 86.772,25 (oltre IVA) pari a 105.862,14 (IVATO)

Di seguito per ogni aula sono rappresentate le caratteristiche tecnico funzionali dei beni.

Per ogni Aula vi è il dettaglio dei beni che saranno oggetto della fornitura.

Di seguito se non diversamente specificato gli ambienti saranno utilizzati come aule fisse.

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

CAPITOLATO TECNICO DI DETTAGLIO

Di seguito per ogni plesso e per ogni aula sono rappresentate le caratteristiche tecnico funzionali dei beni.

AMBIENTE ARTE E TECNOLOGIA: A1 Plesso di Via Cafiero – A2 Plesso Villanova – A3 Plesso Marconi
Fornitura e Installazione di n.51 Notebook di primaria marca internazionale avente le seguenti caratteristiche tecniche : • Processore tipo intel I5-1235U o superiore • Ram 8 Gb DDR4 • Hard Disk 512 Gb SSD PCI EXPRESS o superior • Scheda Grafica Intel Iris Xe Graphics • Display 15,6” FHD • Web Cam e Microfono • Connettività Bluetooth – Wifi 802.11a/b/g/n/ac- Lan RJ45 • Sistema Operativo Windows 11 Pro • Servizio di installazione e configurazione on site Software Didattico incluso avente le seguenti caratteristiche : Avviare • accendere o spegnere e accedere o disconnettersi da tutti i computer della classe dal PC dell'insegnante. • NOVITÀ – Gli insegnanti possono scegliere tre modalità utente (Facile, Intermedio e Avanzato) per rendere le funzionalità accessibili in base al loro livello di sicurezza edtech. • Nascondi gli schermi di tutti gli studenti per attirare l'attenzione e bloccare anche mouse e tastiere. • Ricollegarsi automaticamente ai PC degli studenti se vengono riavviati. • Usa il layout degli studenti sugli schermi degli insegnanti per adattarli al layout della classe fisica. • Utilizza i profili dei singoli insegnanti per fornire le funzionalità richieste da ciascun insegnante. • Utilizzare l'opzione "Richiedi assistenza" con un clic dalla barra degli strumenti dell'insegnante se è necessario il supporto tecnico. • Reimpostazione delle password di sistema per gli studenti senza supporto IT. • Gli insegnanti possono utilizzare Commenti di studenti per valutare come si sentono, la loro fiducia in un argomento e se hanno bisogno di ulteriore supporto. • Gamma flessibile di metodi di connessione ai dispositivi degli studenti, inclusa l'integrazione SIS tramite ClassLink OneRoster e Google Classroom. Gestione della stampante e dei dispositivi • Impedire agli studenti di stampare in classe. • Limita l'utilizzo della stampante per numero di pagine. • Richiedi l'autorizzazione del docente prima della stampa. • Impedire l'utilizzo di singole stampanti. • Visualizza un indicatore di stampa in tempo reale che identifica lo studente che sta attualmente stampando. • Mostra il numero di lavori di stampa in pausa che richiedono l'attenzione dell'insegnante. • Impedire che i dati vengano copiati su o da periferiche di archiviazione USB e CDR / DVD. • Disattiva la webcam sui dispositivi della classe.

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

Registro degli studenti
• Richiedi informazioni standard e personalizzate da ogni studente all'inizio della lezione.
• Stampa il registro degli studenti, incluso un totale di eventuali ricompense o lavori di stampa completati durante la lezione.
• Utilizzare icone personalizzate per ciascun gruppo di studenti.

Distribuisci e raccogli file
• Distribuisci file e cartelle dal PC del tutor a più dispositivi studente.
• Trasferisci file da e verso PC selezionati o multipli in un'unica azione.
• Invio e raccolta automatica dei file, con l'inclusione dei dettagli di ogni Studente.
• Il feedback in tempo reale mostra all'insegnante quali file degli studenti sono pronti per la raccolta e quali studenti devono ricordare.
Barra d'informazioni per gli Studenti
• Visualizza obiettivi della lezione e risultati di apprendimento.
• Fornisce informazioni sulle lezioni in tempo reale, ad esempio il titolo della lezione; tempo rimanente; tutti i premi che sono stati dati dall'insegnante.
• Richiedi assistenza dall'insegnante tramite il pulsante di aiuto.
• Accedi al loro diario digitale.
• Accedi alla cartella delle risorse personali dello studente.
• Verifica quali restrizioni sono attualmente presenti, ad esempio Internet, applicazioni, stampa, chiavette USB.
Strumenti dei tecnici
• Il softwareviene inoltre fornito con una Console dei tecnici per aiutare il team IT della scuola a supportare gli utenti e gestire i dispositivi in tutta la scuola. I tecnici IT possono eseguire il potente 1: 1 PC Remote Control su qualsiasi computer selezionato, acquisire schermate, annotare lo schermo e fornire assistenza tecnica diretta a qualsiasi insegnante di classe. E per un controllo completo, possono anche applicare le impostazioni a livello di scuola come Internet e le restrizioni delle applicazioni che sono "sempre attive".
istruzione in Tempo Reale (Modalità Mostra)
• Mostra il desktop del Tutor a tutti o studenti selezionati.
• Mostrare lo schermo di uno studente (modalità Mostra).
• Limitare l'accesso a Internet ai siti approvati solo durante lo spettacolo.
• Mostra un'applicazione specifica agli studenti selezionati.
• Annotate lo schermo di una Presentazione o durante il Controllo Remoto con una serie di strumenti che facilitano la presentazione (come frecce, forme, evidenziatori e testo).
• Mostrate un "Replay file" (precedentemente registrato) agli studenti selezionati.
• Mostrate un file video agli studenti selezionati.
• Lasciate una registrazione della vostra presentazione sui computer degli studenti, per la revisione in un secondo momento.
• Usate la modalità Audio per parlare agli studenti durante una presentazione.
• Inviate le vostre presentazioni ottimizzate per le reti wireless.
Lavagna virtuale
Una lavagna a tutto schermo, integrata direttamente nella Console Tutor, che contiene una gamma completa distrumenti di disegno per migliorare la collaborazione con l'aula.

Leader di gruppo
Ad uno Studente possono essere assegnati certi diritti di tutor in modo che possa agire da leader di gruppo fino alla revocadi tali privilegi. Adesso include un layout visivo dei leader di gruppo e dei relativi membri del gruppo.
Chat
Apri una discussione in chat a cui puoi partecipare tutti gli studenti o solo quelli selezionati, registrati i loro commenti e condivideteli con gli altri membri della classe (adesso disponibile con emoticon!).
Supporto audio

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

Trasmettete la voce dell'insegnante durante una presentazione. Il supporto audio è incluso in ogni sessione di Presentazione dello schermo e di Controllo Remoto.
Barra degli strumenti dell'insegnante
Quando l'applicazione dell'insegnante è ridotta a icona, Il software dovrà fornire una comoda barra degli strumenti per accedere rapidamente alle sue funzioni chiave. Questa barra degli strumenti è ottimizzata per l'impiego con le lavagne interattive.

Software di sicurezza avente le seguenti caratteristiche

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma. Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito.
Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti. Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura. Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset , che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows.
L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti.

Sicurezza con i sistemi Windows Anti-malware avanzato
Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore.
• DeepGuard
Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale.
• Patch management
Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc.
• Protezione web
Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing.
• Exchange, SharePoint, Citrix, Linux
Componenti di sicurezza dedicate disponibili per piattaforme differenti.

Fornitura e Installazione di n.03 Carrello di ricarica avente le seguenti caratteristiche :
Il carrello dovrà essere composto da 2 ripiani con 32 postazioni per dispositivi fino a 15,6" (tablet e notebook), ventole raffreddamento, Sistema di apertura e chiusura Digital Lock , Smart Charging System, input Volt 100-250V, max power 110V/230V max 16A, adattatore AC, garanzia 24 mesi on center

Fornitura e installazione di n.03 Access Point Professionale avente le seguenti caratteristiche minime:
• Access Point Wi-Fi 6 (802.11ax) - Velocità Wi-Fi fino a 3550 Mbps (1148 Mbps in2.4 GHz + 2402 Mbps in 5 GHz).
• Scenari ad alta densità - Il nuovo standard Wi-Fi 6 introduce le tecnologie 8x8 MU-MIMO (uplink e downlink) e OFDMA che aumentano notevolmente la capacità della rete, fino a 4 volte maggiore rispetto al precedente standard, consentendo di gestire più dispositivi simultaneamente.
• Connettività 2.5 GE PoE+ - Connettività cablata dalle alte velocità e alimentazione Power over Ethernet (802.3at).

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

• Piena compatibilità con il sistema di gestione già presente a scuola • Saranno a carico della ditta le operazioni di installazione a soffitto/parete secondo le indicazioni del progettista . • Saranno a carico della ditta le operazioni di configurazione di tipo sistemistica secondo le necessità della nostra amministrazione
Fornitura e Installazione di n.51 Cuffia e Microfono Professionale avente le seguenti caratteristiche minime: CARATTERISTICHE FISICHE • Tipologia Cuffie con filo • Fattore di forma Sovraurali (On-Ear Headphones) • Microfono incorporato Sì CARATTERISTICHE TECNICHE • Sensibilità 120 dB • Impedenza 38 Ohm • Risposta in frequenza 20 - 20.000 • Ascolto musica Sì • Controllo remoto Controllo chiamate • Noise canceling si CONNETTIVITÀ • Alimentazione USB • Tipo di porta USB-A
Installazione e configurazione di n.01 Education Security Gateway: - Firewall di rete - Gateway VPN - Controllo della rete automatizzato - Ottimizzazione della banda tramite QoS dinamico - Navigazione sicura con inibizione dei tracciatori - Rilevamento attacchi interni/esterni - IPS ed IDS inclusi - Possibilità di collegare le IOC dell'AGID Servizi inclusi per 12 Mesi - DNS per dispositivi esterni alla rete incluso* - Relay di posta con certificati PGP* - DLP per Google Drive* - Monitoraggio h24 degli utenti e dei dati* - Monitoraggio e manutenzione delle piattaforme Didattiche*

Aula a rotazione (Biblioteca) (1 Plesso S.Mauro 1 Cafiero 1 Centrale)
Plesso Cafiero
Fornitura e installazione di n.01 Monitor Interattivi a supporto della didattica aventi le seguenti caratteristiche tecniche minime: • Area Attiva 65” • Tecnologia Pannello Ips • Risoluzione 4K UHD (3840x2160 @ 60 Hz)4K

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

• Contrasto 1200:1
• Color Depth 10bit, 1.07Bilion colors
• Surface Treatment(Haze) Anti Glare, 7H(Mohs)
• Tempo di risposta 8ms (G to G)
• 20 Tocchi simultanei in ambiente Windows
• Casse integrate minimo 10W
• Connettività Hdmi – Usb – Wifi-Lan
• Sistema operativo Integrato Android 8.0
• Cavo Usb 5 Mt
• Cavo Hdmi 3 Mt
• Staffa di supporto omologata inclusa
• Garanzia 36 Mesi Casamadre
• Certificazione Radio Equipment Directive 2014/53/EU
• Certificazione Ecodesign Directive 2009/125/EC - NA - Regulation (EU) 2019/2021
• Certificazione RoHS Directive 2011/65/EU (as amended by EU 2015/863)
• FCC (Regulatory) Class "A"
• Ce (Regulatory)

Saranno a carico della ditta i seguenti servizi:
• Consegna e installazione on site
• Montaggio a parete mediante staffa di supporto omologata
• Eventuale elettrificazione mediante estensione dell'impianto elettrico se necessaria
• Smontaggio (se richiesto) delle vecchie apparecchiature quali Lim e Videoproiettori presenti in classe.
• Corso di formazione al corretto utilizzo delle apparecchiature al personale preposto di almeno 4 ore

Fornitura e Installazione di n.01 Personal Computer a supporto del Monitor Interattivo tipo Ops avente le seguenti caratteristiche tecniche minime:
• Processore Intel Core I5 di 10 Th Generazione o superiore
• Ram 8 Gb DDR4
• Hard Disk tipo SSD da 256 Gb
• Connettività Ethernet 1000 Mbps -Wireless
• Sistema Operativo Windows 10 o superiore
• Piena compatibilità con il monitor interattivo presente nel disciplinare / Piena compatibilità con il monitor interattivo presente in classe
• Installazione on site , installazione degli applicativi indicati dalla scuola
Software di sicurezza avente le seguenti caratteristiche

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma.
Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito.
Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti. Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura. Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset , che contiene regole avanzate che

combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows.
L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti.

Sicurezza con i sistemi Windows Anti-malware avanzato
Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore.
• DeepGuard
Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale.
• Patch management
Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc.
• Protezione web
Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing.
• Exchange, SharePoint, Citrix, Linux
Componenti di sicurezza dedicate disponibili per piattaforme differenti.

Fornitura e installazione di n.01 Access Point Professionale avente le seguenti caratteristiche minime:
• Access Point Wi-Fi 6 (802.11ax) - Velocità Wi-Fi fino a 3550 Mbps (1148 Mbps in2.4 GHz + 2402 Mbps in 5 GHz).
• Scenari ad alta densità - Il nuovo standard Wi-Fi 6 introduce le tecnologie 8x8 MU-MIMO (uplink e downlink) e OFDMA che aumentano notevolmente la capacità della rete, fino a 4 volte maggiore rispetto al precedente standard, consentendo di gestire più dispositivi simultaneamente.
• Connettività 2.5 GE PoE+ - Connettività cablata dalle alte velocità e alimentazione Power over Ethernet (802.3at).
• Piena compatibilità con il sistema di gestione già presente a scuola
• Saranno a carico della ditta le operazioni di installazione a soffitto/parete secondo le indicazioni del progettista .
• Saranno a carico della ditta le operazioni di configurazione di tipo sistemistica secondo le necessità della nostra amministrazione

Plesso Centrale

Fornitura e Installazione di n.01 Personal Computer a supporto del Monitor Interattivo tipo Ops avente le seguenti caratteristiche tecniche minime:
• Processore Intel Core I5 di 10 Th Generazione o superiore
• Ram 8 Gb DDR4
• Hard Disk tipo SSD da 256 Gb
• Connettività Ethernet 1000 Mbps -Wireless
• Sistema Operativo Windows 10 o superiore
• Piena compatibilità con il monitor interattivo presente nel disciplinare / Piena compatibilità con il monitor interattivo presente in classe
• Installazione on site , installazione degli applicativi indicati dalla scuola
Software di sicurezza avente le seguenti caratteristiche

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le

patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma.
Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito.

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti.
Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura.
Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset , che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows.
L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti.

Sicurezza con i sistemi Windows Anti-malware avanzato
Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore.
• DeepGuard
Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale.
• Patch management
Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc.
• Protezione web
Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing.
• Exchange, SharePoint, Citrix, Linux
Componenti di sicurezza dedicate disponibili per piattaforme differenti.

Fornitura e installazione di n.01 Access Point Professionale avente le seguenti caratteristiche minime:
• Access Point Wi-Fi 6 (802.11ax) - Velocità Wi-Fi fino a 3550 Mbps (1148 Mbps in2.4 GHz + 2402 Mbps in 5 GHz).
• Scenari ad alta densità - Il nuovo standard Wi-Fi 6 introduce le tecnologie 8x8 MU-MIMO (uplink e downlink) e OFDMA che aumentano notevolmente la capacità della rete, fino a 4 volte maggiore rispetto al precedente standard, consentendo di gestire più dispositivi simultaneamente.
• Connettività 2.5 GE PoE+ - Connettività cablata dalle alte velocità e alimentazione Power over Ethernet (802.3at).
• Piena compatibilità con il sistema di gestione già presente a scuola
• Saranno a carico della ditta le operazioni di installazione a soffitto/parete secondo le indicazioni del progettista .
• Saranno a carico della ditta le operazioni di configurazione di tipo sistemistica secondo le necessità della nostra amministrazione

Plesso S.Mauro

Fornitura e Installazione di n.01 Personal Computer a supporto del Monitor Interattivo tipo Ops avente le seguenti caratteristiche tecniche minime:
• Processore Intel Core I5 di 10 Th Generazione o superiore
• Ram 8 Gb DDR4
• Hard Disk tipo SSD da 256 Gb
• Connettività Ethernet 1000 Mbps -Wireless
• Sistema Operativo Windows 10 o superiore
• Piena compatibilità con il monitor interattivo presente nel disciplinare / Piena compatibilità con il monitor interattivo presente in classe
• Installazione on site , installazione degli applicativi indicati dalla scuola
Software di sicurezza avente le seguenti caratteristiche

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli

aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma. Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing

apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito.
Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti.
Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura.
Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

Impostare un accesso read-only a USB/CD/altri drive Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici Firewall firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset , che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows. L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti. Sicurezza con i sistemi Windows Anti-malware avanzato Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore. • DeepGuard Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale. • Patch management Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc. • Protezione web Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing. • Exchange, SharePoint, Citrix, Linux Componenti di sicurezza dedicate disponibili per piattaforme differenti.
Fornitura e installazione di n.01 Access Point Professionale avente le seguenti caratteristiche minime: • Access Point Wi-Fi 6 (802.11ax) - Velocità Wi-Fi fino a 3550 Mbps (1148 Mbps in2.4 GHz + 2402 Mbps in 5 GHz). • Scenari ad alta densità - Il nuovo standard Wi-Fi 6 introduce le tecnologie 8x8 MU-MIMO (uplink e downlink) e OFDMA che aumentano notevolmente la capacità della rete, fino a 4 volte maggiore rispetto al precedente standard, consentendo di gestire più dispositivi simultaneamente. • Connettività 2.5 GE PoE+ - Connettività cablata dalle alte velocità e alimentazione Power over Ethernet (802.3at). • Piena compatibilità con il sistema di gestione già presente a scuola • Saranno a carico della ditta le operazioni di installazione a soffitto/parete secondo le indicazioni del progettista . • Saranno a carico della ditta le operazioni di configurazione di tipo sistemistica secondo le necessità della nostra amministrazione

ARREDO
Plesso Cafiero

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

Fornitura e Montaggio di n.06 Libreria Curva Modulare su ruote avente le seguenti caratteristiche :
• realizzata in particelle di legno Sp18mm e Sp 25mm in classe E1 bassa emissione di formaldeide, secondo norme uni EN classe di reazione al fuoco2 .
• Vano interno suddiviso in 2 vani verticali con 2 mensole registrabili sp. mm. 25 per ogni vano, corredata di 2 maniglie di traino e 5 ruote industriali h. 16,5 di cui n°2 dotate di freno.
• Dim L152 x P42,5 x h.95,5 + ruote, H. totale 112.
• Struttura Colore: argento T004 , Bianco T005
• Pannello frontale microforato in laminato
• Installazione e Montaggio on site secondo le esigenze dell'amministrazione

Fornitura e installazione di n.04 Pouf Semicurvo avente le seguenti caratteristiche :
• interno in polistirene rigido dens.10 rivestito con spugna sp 1,4cm., base in legno con piedini neri .
• Rivestimento in finta pelle ignifuca colore a scelta

Fornitura di n.04 Seduta Pouff quadrato, rivestimento in ecopelle colori a scelta: Rosso, Blu, Verde e Giallo Dim. cm.40X40X46H

Plesso Centrale

Fornitura e Montaggio di n.03 Libreria Curva Modulare su ruote avente le seguenti caratteristiche :
• realizzata in particelle di legno Sp18mm e Sp 25mm in classe E1 bassa emissione di formaldeide, secondo norme uni EN classe di reazione al fuoco2 .
• Vano interno suddiviso in 2 vani verticali con 2 mensole registrabili sp. mm. 25 per ogni vano, corredata di 2 maniglie di traino e 5 ruote industriali h. 16,5 di cui n°2 dotate di freno.
• Dim L152 x P42,5 x h.95,5 + ruote, H. totale 112.
• Struttura Colore: argento T004 , Bianco T005
• Pannello frontale microforato in laminato
• Installazione e Montaggio on site secondo le esigenze dell'amministrazione

Fornitura e installazione di n.02 Pouf Semicurvo avente le seguenti caratteristiche :
• interno in polistirene rigido dens.10 rivestito con spugna sp 1,4cm., base in legno con piedini neri .
• Rivestimento in finta pelle ignifuca colore a scelta

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

Plesso S.Mauro
Fornitura e Montaggio di n.03 Libreria Curva Modulare su ruote avente le seguenti caratteristiche : • realizzata in particelle di legno Sp18mm e Sp 25mm in classe E1 bassa emissione di formaldeide, secondo norme uni EN classe di reazione al fuoco2 . • Vano interno suddiviso in 2 vani verticali con 2 mensole registrabili sp. mm. 25 per ogni vano, corredata di 2 maniglie di traino e 5 ruote industriali h. 16,5 di cui n°2 dotate di freno. • Dim L152 x P42,5 x h.95,5 + ruote, H. totale 112. • Struttura Colore: argento T004 , Bianco T005 • Pannello frontale microforato in laminato • Installazione e Montaggio on site secondo le esigenze dell'amministrazione
Fornitura e installazione di n.02 Pouf Semicurvo avente le seguenti caratteristiche : • interno in polistirene rigido dens.10 rivestito con spugna sp 1,4cm., base in legno con piedini neri . • Rivestimento in finta pelle ignifuca colore a scelta

Piccoli Adattamenti Edilizi
Installazione e posa in opera di n.01 Punto rete lan RJ45 comprensivo di cavi , canaline , accessori e quanto altro necessario al corretto funzionamento dello stesso .Il cavo per la distribuzione deve essere di tipo non schermato U/UTP Cat. 6 CAT.6 CCA AWG23 -LSZA - Cca s1a, d1,a1
Installazione e posa in opera di n.01 punto elettrico con bivalente e shuko con montante al quadro elettrico principale nell'apposito differenziale magnetotermico. Gli impianti saranno realizzati secondo quanto disposto dal d.m. 37/2008

AULA A ROTAZIONE MUSICALE (1 S.MAURO 1 CAFIERO 1)
Fornitura e installazione di n.02 Monitor Interattivi a supporto della didattica aventi le seguenti caratteristiche tecniche minime: • Area Attiva 65" • Tecnologia Pannello Ips • Risoluzione 4K UHD (3840x2160 @ 60 Hz)4K • Contrasto 1200:1 • Color Depth 10bit, 1.07Bilion colors • Surface Treatment(Haze) Anti Glare, 7H(Mohs) • Tempo di risposta 8ms (G to G) • 20 Tocchi simultanei in ambiente Windows • Casse integrate minimo 10W • Connettività Hdmi – Usb – Wifi-Lan • Sistema operativo Integrato Android 8.0 • Cavo Usb 5 Mt • Cavo Hdmi 3 Mt

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

• Staffa di supporto omologata inclusa
• Garanzia 36 Mesi Casamadre
• Certificazione Radio Equipment Directive 2014/53/EU
• Certificazione Ecodesign Directive 2009/125/EC - NA - Regulation (EU) 2019/2021
• Certificazione RoHS Directive 2011/65/EU (as amended by EU 2015/863)
• FCC (Regulatory) Class "A"
• Ce (Regulatory)

Saranno a carico della ditta i seguenti servizi:
• Consegna e installazione on site
• Montaggio a parete mediante staffa di supporto omologata
• Eventuale elettrificazione mediante estensione dell'impianto elettrico se necessaria
• Smontaggio (se richiesto) delle vecchie apparecchiature quali Lim e Videoproiettori presenti in classe.
• Corso di formazione al corretto utilizzo delle apparecchiature al personale preposto di almeno 4 ore

Fornitura e Installazione di n.02 Personal Computer a supporto del Monitor Interattivo tipo Ops avente le seguenti caratteristiche tecniche minime:

• Processore Intel Core I5 di 10 Th Generazione o superiore
• Ram 8 Gb DDR4
• Hard Disk tipo SSD da 256 Gb
• Connettività Ethernet 1000 Mbps -Wireless
• Sistema Operativo Windows 10 o superiore
• Piena compatibilità con il monitor interattivo presente nel disciplinare / Piena compatibilità con il monitor interattivo presente in classe
• Installazione on site , installazione degli applicativi indicati dalla scuola
Software di sicurezza avente le seguenti caratteristiche

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.

Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma. Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito.
Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro

il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti.
Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura.
Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset , che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows.
L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti.

Sicurezza con i sistemi Windows Anti-malware avanzato
Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore.
• DeepGuard

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale.
• Patch management
Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc.
• Protezione web
Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing.
• Exchange, SharePoint, Citrix, Linux
Componenti di sicurezza dedicate disponibili per piattaforme differenti.

Fornitura e Installazione di n.02 All in One avente le seguenti caratteristiche tecniche minime:
• Processore Cpu tipo intel core i7-1260P
• Ram 16 Gb DDR4
• Hard Disk 512 Gb PCIe SSD
• Display 27” Led Fhd (1920x1080)
• Connettività Wireless WIFI 6E – Rj45 lan
• Mouse e Tastiera Wifi
• Uscita Hdmi Out
• Sistema Operativo Windows 11 Pro
• Installazione e configurazione secondo le esigenze del progettista
• Corso di formazione al corretto utilizzo del prodotto

Software di sicurezza avente le seguenti caratteristiche

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine

Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma. Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito.
Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti.
Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura.
Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset , che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows.
L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti.

Sicurezza con i sistemi Windows Anti-malware avanzato
Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore.
• DeepGuard
Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale.
• Patch management
Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc.
• Protezione web
Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing.
• Exchange, SharePoint, Citrix, Linux
Componenti di sicurezza dedicate disponibili per piattaforme differenti.

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

Fornitura e Installazione di n.02 INTERFACCIA AUDIO USB avente le seguenti caratteristiche tecniche minime:

- Compatibilità multipiattaforma Windows, macOS e iOS per una flessibilità superiore
- Preamplificatori microfonici D-PRE di Classe A con alimentazione phantom +48V
- Gli ingressi a doppia combinazione supportano strumenti e connessioni microfoniche
- Il connettore da USB 3.0 a USB-C può connettersi alla maggior parte dei dispositivi moderni
- Il monitoraggio senza latenza ha controlli di bilanciamento del mix
- L'I/O MIDI consente di sincronizzarsi con l'hardware esterno
- Controllo separato del livello delle cuffie
- Fonte di alimentazione selezionabile: USB 3.0 o 9V CC
- Dimensioni: 159 x 37 x 149mm

Saranno a carico della ditta le operazioni di installazione e configurazione on site

Fornitura e Installazione di n.02 Software per produzione musicale Tipo Cubase Elements 12 Ita avente le seguenti caratteristiche tecniche minime:

- Perfetto per tecnici audio professionisti, cantautori, compositori e direttori d'orchestra
- Il motore audio in virgola mobile a 64 bit di nuova generazione ti offre molta potenza
- La registrazione MIDI retrospettiva tiene traccia dell'input MIDI, anche quando non stai registrando
- La modalità di avvio sicuro ti consente di avviare Cubase senza che siano stati caricati plug-in di terze parti
- I canali del mixer colorati velocizzano il tuo flusso di lavoro
- Strumenti compositivi intelligenti come Chord Track, Chord Pad e Chord Assistant
- L'equalizzazione con confronto spettrale semplifica l'identificazione e l'eliminazione delle collisioni di frequenza
- Consente una facile importazione di audio e dati da altri progetti salvati
- MixConsole cattura l'essenza di una console analogica di fascia alta
- Sampler Track e Caleidoscope per costruire loop e frasi
- Set completo di 3 strumenti eccezionali con oltre 1000 suoni
- Controlli MIDI estesi, personalizzazione flusso di lavoro e dei tasti di comando, automazione dei volumi dei sample e conversione audio / MIDI
- Ora ottimizzato per i processori in silicio Apple tramite Rosetta 2

Saranno a carico della ditta le operazioni di installazione on site sul personal computer indicato dall'amministrazione

Fornitura e installazione di n.02 Cuffia Professionale avente le seguenti caratteristiche :

- Principio acustico: Dinamico, aperto
- Risposta in frequenza: 6Hz - 38 kHz (-10dB)
- Impedenza: 120 Ohm
- Livello di pressione sonora (SPL): 110dB (1 kHz / 1V RMS)
- THD, Distorsione Armonica Totale: < 0,05% (1 kHz / 90dB SPL)
- Accoppiamento auricolare: Circumaurale
- Temperatura di stoccaggio: -55°C / +70°C
- Temperatura di esercizio: -15°C / +55°C
- Umidità relativa di esercizio: ≤ 90%
- Materiale dei cuscinetti auricolari: Velluto
- Connettore: Jack 3,5mm con adattatore da 6,3mm
- Peso: 240g
- Consegna e installazione on site, fornitura di eventuali cavi di collegamento necessari

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

Fornitura e installazione di n.02 MICROFONO A CONDENSATORE CARDIOIDE A DIAFRAMMA LARGO avente le seguenti caratteristiche tecniche:

- Microfono a condensatore cardioide a diaframma largo
- Capsula a condensatore HF6 da 1" spruzzata d'oro
- Risposta in frequenza regolare, alta sensibilità e gestione SPL elevata
- Rumore eccezionalmente basso (4dBA): il microfono a condensatore da studio più silenzioso al mondo
- Uscita Dual Connect in attesa di brevetto con connettività XLR e USB
- Prima uscita digitale float a 32 bit al mondo
- Conversione da analogico a digitale ad altissima risoluzione (fino a 192kHz)
- DSP integrato per elaborazione audio APHEX avanzata
- Supporto antiurto e filtro pop da studio, cavi XLR e USB inclusi
- Disponibile in silver con un robusto corpo in alluminio e finiture di alta qualità
- Progettato e realizzato negli impianti di produzione di precisione RØDE a Sydney, in Australia
- Finitura: Silver
- Dimensioni: 52 x 52 x 189mm
- Peso: 308g
- Installazione on site
- Fornitura di eventuali cavi di collegamento necessari

Fornitura e Installazione di n.02 MICROFONO DINAMICO CARDIOIDE PER VOCE avente le seguenti caratteristiche tecniche minime:

- Tipo: Dinamico (Moving Coil)
- Risposta in frequenza: 50Hz - 15kHz
- Diagramma Polare: Cardioide
- Sensibilità (@ 1KHz Tensione a Circuito Aperto): -54,5dBV/Pa (1.85 mV) 1 Pa = 94 dB SPL
- Impedenza: 150 Ohm (nominale), 300 Ohm (effettiva)
- Connettore: XLR M 3-pin
- Peso: 0,298 kg
- Cavi di collegamento necessari al corretto funzionamento dell'impianto

Asta Microfonica avente le seguenti caratteristiche :

- Diametro base: 680mm
- Altezza minima: 900mm
- Altezza max: 1500mm
- Lunghezza giraffa: 750mm
- Finitura: Nero opaco
- Peso: 2,2kg

AULA STEM SEDE CENTRALE

Fornitura e installazione di n.01 Monitor Interattivi a supporto della didattica aventi le seguenti caratteristiche tecniche minime:

- Area Attiva 65"
- Tecnologia Pannello Ips
- Risoluzione 4K UHD (3840x2160 @ 60 Hz)4K
- Contrasto 1200:1

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

• Color Depth 10bit, 1.07Bilion colors
• Surface Treatment(Haze) Anti Glare, 7H(Mohs)
• Tempo di risposta 8ms (G to G)
• 20 Tocchi simultanei in ambiente Windows
• Casse integrate minimo 10W
• Connettività Hdmi – Usb – Wifi-Lan
• Sistema operativo Integrato Android 8.0
• Cavo Usb 5 Mt
• Cavo Hdmi 3 Mt
• Staffa di supporto omologata inclusa
• Garanzia 36 Mesi Casamadre
• Certificazione Radio Equipment Directive 2014/53/EU
• Certificazione Ecodesign Directive 2009/125/EC - NA - Regulation (EU) 2019/2021
• Certificazione RoHS Directive 2011/65/EU (as amended by EU 2015/863)
• FCC (Regulatory) Class "A"
• Ce (Regulatory)

Saranno a carico della ditta i seguenti servizi:
• Consegna e installazione on site
• Montaggio a parete mediante staffa di supporto omologata
• Eventuale elettrificazione mediante estensione dell'impianto elettrico se necessaria
• Smontaggio (se richiesto) delle vecchie apparecchiature quali Lim e Videoproiettori presenti in classe.
• Corso di formazione al corretto utilizzo delle apparecchiature al personale preposto di almeno 4 ore

Fornitura e Installazione di n.01 Personal Computer a supporto del Monitor Interattivo tipo Ops avente le seguenti caratteristiche tecniche minime:
• Processore Intel Core I5 di 10 Th Generazione o superiore
• Ram 8 Gb DDR4
• Hard Disk tipo SSD da 256 Gb
• Connettività Ethernet 1000 Mbps -Wireless
• Sistema Operativo Windows 10 o superiore
• Piena compatibilità con il monitor interattivo presente nel disciplinare / Piena compatibilità con il monitor interattivo presente in classe
• Installazione on site , installazione degli applicativi indicati dalla scuola
Software di sicurezza avente le seguenti caratteristiche

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma. Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito.
Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti.
Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura.
Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset , che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

di Windows.
L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti.

Sicurezza con i sistemi Windows Anti-malware avanzato
Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore.
• DeepGuard
Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale.
• Patch management
Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc.
• Protezione web
Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing.
• Exchange, SharePoint, Citrix, Linux
Componenti di sicurezza dedicate disponibili per piattaforme differenti.

Fornitura e installazione di n.01 Access Point Professionale avente le seguenti caratteristiche minime:
• Access Point Wi-Fi 6 (802.11ax) - Velocità Wi-Fi fino a 3550 Mbps (1148 Mbps in2.4 GHz + 2402 Mbps in 5 GHz).
• Scenari ad alta densità - Il nuovo standard Wi-Fi 6 introduce le tecnologie 8x8 MU-MIMO (uplink e downlink) e OFDMA che aumentano notevolmente la capacità della rete, fino a 4 volte maggiore rispetto al precedente standard, consentendo di gestire più dispositivi simultaneamente.
• Connettività 2.5 GE PoE+ - Connettività cablata dalle alte velocità e alimentazione Power over Ethernet (802.3at).
• Piena compatibilità con il sistema di gestione già presente a scuola
• Saranno a carico della ditta le operazioni di installazione a soffitto/parete secondo le indicazioni del progettista .
• Saranno a carico della ditta le operazioni di configurazione di tipo sistemistica secondo le necessità della nostra amministrazione

Piccoli Adattamenti edilizi

Installazione e posa in opera di n.01 punto elettrico con bivalente e shuko con montante al quadro elettrico principale nell'apposito differenziale magnetotermico. Gli impianti saranno realizzati secondo quanto disposto dal d.m. 37/2008

Installazione e posa in opera di n.01 Punto rete lan RJ45 comprensivo di cavi , canaline , accessori e quanto altro necessario al corretto funzionamento dello stesso .Il cavo per la distribuzione deve essere di tipo non schermato U/UTP Cat. 6 CAT.6 CCA AWG23 -LSZA - Cca s1a, d1,a1

AULA LINGUA (1 PLESSO MARCONI 1 PLESSO CAFIERO)

SEDE CENTRALE

Fornitura e Installazione di n.01 Personal Computer a supporto del Monitor Interattivo tipo Ops avente le seguenti caratteristiche tecniche minime:

• Processore Intel Core I5 di 10 Th Generazione o superiore
• Ram 8 Gb DDR4

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

• Hard Disk tipo SSD da 256 Gb
• Connettività Ethernet 1000 Mbps -Wireless
• Sistema Operativo Windows 10 o superiore
• Piena compatibilità con il monitor interattivo presente nel disciplinare / Piena compatibilità con il monitor interattivo presente in classe
• Installazione on site , installazione degli applicativi indicati dalla scuola
Software di sicurezza avente le seguenti caratteristiche

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma. Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito.
Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti

che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti. Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura. Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset , che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows.
L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti.

Sicurezza con i sistemi Windows Anti-malware avanzato
Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore.
• DeepGuard
Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale.
• Patch management
Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc.
• Protezione web
Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing.
• Exchange, SharePoint, Citrix, Linux
Componenti di sicurezza dedicate disponibili per piattaforme differenti.

SEDE CAFIERO

Fornitura e installazione di n.01 Monitor Interattivi a supporto della didattica aventi le seguenti caratteristiche tecniche minime:
• Area Attiva 65”
• Tecnologia Pannello Ips
• Risoluzione 4K UHD (3840x2160 @ 60 Hz)4K
• Contrasto 1200:1
• Color Depth 10bit, 1.07Bilion colors
• Surface Treatment(Haze) Anti Glare, 7H(Mohs)

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

• Tempo di risposta 8ms (G to G)
• 20 Tocchi simultanei in ambiente Windows
• Casse integrate minimo 10W
• Connettività Hdmi – Usb – Wifi-Lan
• Sistema operativo Integrato Android 8.0
• Cavo Usb 5 Mt
• Cavo Hdmi 3 Mt
• Staffa di supporto omologata inclusa
• Garanzia 36 Mesi Casamadre
• Certificazione Radio Equipment Directive 2014/53/EU
• Certificazione Ecodesign Directive 2009/125/EC - NA - Regulation (EU) 2019/2021
• Certificazione RoHS Directive 2011/65/EU (as amended by EU 2015/863)
• FCC (Regulatory) Class "A"
• Ce (Regulatory)

Saranno a carico della ditta i seguenti servizi:
• Consegna e installazione on site
• Montaggio a parete mediante staffa di supporto omologata
• Eventuale elettrificazione mediante estensione dell'impianto elettrico se necessaria
• Smontaggio (se richiesto) delle vecchie apparecchiature quali Lim e Videoproiettori presenti in classe.
• Corso di formazione al corretto utilizzo delle apparecchiature al personale preposto di almeno 4 ore

Fornitura e Installazione di n.01 Personal Computer a supporto del Monitor Interattivo tipo Ops avente le seguenti caratteristiche tecniche minime:
• Processore Intel Core I5 di 10 Th Generazione o superiore
• Ram 8 Gb DDR4
• Hard Disk tipo SSD da 256 Gb
• Connettività Ethernet 1000 Mbps -Wireless
• Sistema Operativo Windows 10 o superiore
• Piena compatibilità con il monitor interattivo presente nel disciplinare / Piena compatibilità con il monitor interattivo presente in classe
• Installazione on site , installazione degli applicativi indicati dalla scuola
Software di sicurezza avente le seguenti caratteristiche

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma.
Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito.
Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti

in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti.
Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura.
Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset , che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows.
L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre,

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti. Sicurezza con i sistemi Windows Anti-malware avanzato Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore. • DeepGuard Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale. • Patch management Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc. • Protezione web Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing. • Exchange, SharePoint, Citrix, Linux Componenti di sicurezza dedicate disponibili per piattaforme differenti.
Fornitura e installazione di n.01 Switch avente le seguenti caratteristiche minime: • Tipologia Managed L2+ -Rack Mountable • Numero di porte 24 Gigabit Lan 4 slot SFP • Capacità di Swtiching 56 Gbps • Piena compatibilità con il sistema di gestione già presente a scuola • Saranno a carico della ditta le operazioni di montaggio nell'apposito armadio rack e di configurazione secondo le esigenza della nostra amministrazione
Fornitura e installazione di n.01 Access Point Professionale avente le seguenti caratteristiche minime: • Access Point Wi-Fi 6 (802.11ax) - Velocità Wi-Fi fino a 3550 Mbps (1148 Mbps in2.4 GHz + 2402 Mbps in 5 GHz). • Scenari ad alta densità - Il nuovo standard Wi-Fi 6 introduce le tecnologie 8x8 MU-MIMO (uplink e downlink) e OFDMA che aumentano notevolmente la capacità della rete, fino a 4 volte maggiore rispetto al precedente standard, consentendo di gestire più dispositivi simultaneamente. • Connettività 2.5 GE PoE+ - Connettività cablata dalle alte velocità e alimentazione Power over Ethernet (802.3at). • Piena compatibilità con il sistema di gestione già presente a scuola • Saranno a carico della ditta le operazioni di installazione a soffitto/parete secondo le indicazioni del progettista . • Saranno a carico della ditta le operazioni di configurazione di tipo sistemistica secondo le necessità della nostra amministrazione

Piccoli Adattamenti Edilizi
Installazione e posa in opera di n.01 Punto rete lan RJ45 comprensivo di cavi , canaline , accessori e quanto altro necessario al corretto funzionamento dello stesso .Il cavo per la distribuzione deve essere di tipo non schermato U/UTP Cat. 6 CAT.6 CCA AWG23 -LSZA - Cca s1a, d1,a1

AULA SCIENZE (1 SEDE CENTRALE 1 VILLANOVA)
Sede Villanova

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

Fornitura e installazione di n.01 Monitor Interattivi a supporto della didattica aventi le seguenti caratteristiche tecniche minime:

- Area Attiva 65”
- Tecnologia Pannello Ips
- Risoluzione 4K UHD (3840x2160 @ 60 Hz)4K
- Contrasto 1200:1
- Color Depth 10bit, 1.07Bilion colors
- Surface Treatment(Haze) Anti Glare, 7H(Mohs)
- Tempo di risposta 8ms (G to G)
- 20 Tocchi simultanei in ambiente Windows
- Casse integrate minimo 10W
- Connettività Hdmi – Usb – Wifi-Lan
- Sistema operativo Integrato Android 8.0
- Cavo Usb 5 Mt
- Cavo Hdmi 3 Mt
- Staffa di supporto omologata inclusa
- Garanzia 36 Mesi Casamadre
- Certificazione Radio Equipment Directive 2014/53/EU
- Certificazione Ecodesign Directive 2009/125/EC - NA - Regulation (EU) 2019/2021
- Certificazione RoHS Directive 2011/65/EU (as amended by EU 2015/863)
- FCC (Regulatory) Class “A”
- Ce (Regulatory)

Saranno a carico della ditta i seguenti servizi:

- Consegna e installazione on site
- Montaggio a parete mediante staffa di supporto omologata
- Eventuale elettrificazione mediante estensione dell’impianto elettrico se necessaria
- Smontaggio (se richiesto) delle vecchie apparecchiature quali Lim e Videoproiettori presenti in classe.
- Corso di formazione al corretto utilizzo delle apparecchiature al personale preposto di almeno 4 ore

Fornitura e Installazione di n.01 Personal Computer a supporto del Monitor Interattivo tipo Ops avente le seguenti caratteristiche tecniche minime:

- Processore Intel Core I5 di 10 Th Generazione o superiore
- Ram 8 Gb DDR4
- Hard Disk tipo SSD da 256 Gb
- Connettività Ethernet 1000 Mbps -Wireless
- Sistema Operativo Windows 10 o superiore
- Piena compatibilità con il monitor interattivo presente nel disciplinare / Piena compatibilità con il monitor interattivo presente in classe
- Installazione on site , installazione degli applicativi indicati dalla scuola

Software di sicurezza avente le seguenti caratteristiche

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità

basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma. Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati,

quali indirizzi IP, parole chiave dell'URL e comportamento del sito.
Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti. Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura.
Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset , che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows.
L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti.

Sicurezza con i sistemi Windows Anti-malware avanzato
Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore.
• DeepGuard
Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale.
• Patch management
Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc.
• Protezione web
Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing.
• Exchange, SharePoint, Citrix, Linux
Componenti di sicurezza dedicate disponibili per piattaforme differenti.

Sede Centrale

Fornitura e installazione di n.01 Monitor Interattivi a supporto della didattica aventi le seguenti caratteristiche tecniche minime:
• Area Attiva 65”
• Tecnologia Pannello Ips
• Risoluzione 4K UHD (3840x2160 @ 60 Hz)4K
• Contrasto 1200:1
• Color Depth 10bit, 1.07Bilion colors
• Surface Treatment(Haze) Anti Glare, 7H(Mohs)
• Tempo di risposta 8ms (G to G)
• 20 Tocchi simultanei in ambiente Windows
• Casse integrate minimo 10W
• Connettività Hdmi – Usb – Wifi-Lan
• Sistema operativo Integrato Android 8.0
• Cavo Usb 5 Mt
• Cavo Hdmi 3 Mt
• Staffa di supporto omologata inclusa
• Garanzia 36 Mesi Casamadre
• Certificazione Radio Equipment Directive 2014/53/EU
• Certificazione Ecodesign Directive 2009/125/EC - NA - Regulation (EU) 2019/2021
• Certificazione RoHS Directive 2011/65/EU (as amended by EU 2015/863)
• FCC (Regulatory) Class “A”
• Ce (Regulatory)

Saranno a carico della ditta i seguenti servizi:
• Consegna e installazione on site
• Montaggio a parete mediante staffa di supporto omologata
• Eventuale elettrificazione mediante estensione dell’impianto elettrico se necessaria
• Smontaggio (se richiesto) delle vecchie apparecchiature quali Lim e Videoproiettori presenti in classe.
• Corso di formazione al corretto utilizzo delle apparecchiature al personale preposto di almeno 4 ore

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

Fornitura e Installazione di n.01 Personal Computer a supporto del Monitor Interattivo tipo Ops avente le seguenti caratteristiche tecniche minime:

• Processore Intel Core I5 di 10 Th Generazione o superiore
• Ram 8 Gb DDR4
• Hard Disk tipo SSD da 256 Gb
• Connettività Ethernet 1000 Mbps -Wireless
• Sistema Operativo Windows 10 o superiore
• Piena compatibilità con il monitor interattivo presente nel disciplinare / Piena compatibilità con il monitor interattivo presente in classe
• Installazione on site , installazione degli applicativi indicati dalla scuola

Software di sicurezza avente le seguenti caratteristiche

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti

dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma.
Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito.
Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali

per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti. Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura. Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset , che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows.
L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti.

Sicurezza con i sistemi Windows Anti-malware avanzato
Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore.
• DeepGuard
Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale.
• Patch management
Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc.
• Protezione web
Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing.
• Exchange, SharePoint, Citrix, Linux
Componenti di sicurezza dedicate disponibili per piattaforme differenti.

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

AULA CINEMATOGRAFICA

Fornitura e Installazione di n.01 Workstation per la grafica avente le seguenti caratteristiche tecniche minime:

- Processore Intel Core I7-13700F
- Ram 16 Gb DDR4
- Hard Disk 512 GB M2 Pcie
- Scheda Video RTX 3060 VENTUS 2X 8 GB
- Sistema Operativo Windows 11 Professional
- Mouse e Tastiera Usb
- Installazione e configurazione secondo le indicazioni del Progettista
- Corso di formazione al corretto utilizzo del prodotto

Software di sicurezza avente le seguenti caratteristiche

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.

Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma. Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito.
Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti.
Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura.
Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset , che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows.
L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti.

Sicurezza con i sistemi Windows Anti-malware avanzato
Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore.
• DeepGuard
Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale.
• Patch management
Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc.
• Protezione web
Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing.
• Exchange, SharePoint, Citrix, Linux
Componenti di sicurezza dedicate disponibili per piattaforme differenti.

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

Fornitura e Installazione di n.01 Monitor Lcd avente le seguenti caratteristiche tecniche minime:

- Display 27” Ips
- Risoluzione 1920x1080 (Full HD)
- Luminosità 250 cd/m2
- Refresh rate 60 Mhz
- Connettività Hdmi -Vga
- Multimediale 2x2W
- Less Blue Light (Low Blue)
- Installazione e configurazione secondo le indicazioni del progettista
- Cavi di collegamento inclusi
- Corso di formazione al corretto funzionamento dei prodotti

PLESSO S.MARCO AULA POLIFUNZIONALE

Fornitura e installazione di n.01 Monitor Interattivi a supporto della didattica aventi le seguenti caratteristiche tecniche minime:

- Area Attiva 65”
- Tecnologia Pannello Ips
- Risoluzione 4K UHD (3840x2160 @ 60 Hz)4K
- Contrasto 1200:1
- Color Depth 10bit, 1.07Bilion colors
- Surface Treatment(Haze) Anti Glare, 7H(Mohs)
- Tempo di risposta 8ms (G to G)
- 20 Tocchi simultanei in ambiente Windows
- Casse integrate minimo 10W
- Connettività Hdmi – Usb – Wifi-Lan
- Sistema operativo Integrato Android 8.0
- Cavo Usb 5 Mt
- Cavo Hdmi 3 Mt
- Staffa di supporto omologata inclusa
- Garanzia 36 Mesi Casamadre
- Certificazione Radio Equipment Directive 2014/53/EU
- Certificazione Ecodesign Directive 2009/125/EC - NA - Regulation (EU) 2019/2021
- Certificazione RoHS Directive 2011/65/EU (as amended by EU 2015/863)
- FCC (Regulatory) Class “A”
- Ce (Regulatory)

Saranno a carico della ditta i seguenti servizi:

- Consegna e installazione on site
- Montaggio a parete mediante staffa di supporto omologata
- Eventuale elettrificazione mediante estensione dell’impianto elettrico se necessaria
- Smontaggio (se richiesto) delle vecchie apparecchiature quali Lim e Videoproiettori presenti in classe.
- Corso di formazione al corretto utilizzo delle apparecchiature al personale preposto di almeno 4 ore

Fornitura e Installazione di n.01 Carrello Mobile per Monitor Interattivo avente le seguenti caratteristiche tecniche minime :

- Adatto per Monitor fino a 90”
- Portata massima 80 Kg

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

• Regolazione dell'altezza manuale (Posizione schermo su tre altezze: 1450mm 1530mm 1610mm)
• Ruote piroettanti con freno
• Sarà a carico della ditta il servizio di installazione del Monitor Interattivo indicato dalla nostra amministrazione sullo stesso .

Fornitura e Installazione di n.01 Personal Computer a supporto del Monitor Interattivo tipo Ops avente le seguenti caratteristiche tecniche minime:
• Processore Intel Core I5 di 10 Th Generazione o superiore
• Ram 8 Gb DDR4
• Hard Disk tipo SSD da 256 Gb
• Connettività Ethernet 1000 Mbps -Wireless
• Sistema Operativo Windows 10 o superiore
• Piena compatibilità con il monitor interattivo presente nel disciplinare / Piena compatibilità con il monitor interattivo presente in classe
• Installazione on site , installazione degli applicativi indicati dalla scuola
Software di sicurezza avente le seguenti caratteristiche

Gestione automatica delle patch

Software Updater è la funzione automatica di gestione delle patch completamente integrata nei client. Non è necessario installare agenti, server di gestione o console separate.

Software Updater è un componente fondamentale della sicurezza. È il primo livello di protezione contro contenuti nocivi che possono raggiungere gli endpoint e previene l'80% degli attacchi semplicemente installando gli aggiornamenti di sicurezza del software non appena sono disponibili.

Software Updater esegue scansioni per rilevare gli aggiornamenti mancanti, crea un rapporto sulla vulnerabilità basato sulle patch mancanti, quindi scarica e implementa gli aggiornamenti, automaticamente o manualmente. Le patch di sicurezza includono aggiornamenti Microsoft e di oltre 2500 applicazioni di terze parti, come Flash, Java, OpenOffice e altre ancora che generalmente vengono usate come vettori per gli attacchi per via della loro diffusione.

Analisi euristica e del comportamento

DeepGuard unisce alcune delle tecnologie più avanzate per la sicurezza. È il livello finale e più importante di difesa contro le nuove minacce, anche quelle che attaccano vulnerabilità precedentemente sconosciute.
DeepGuard osserva il comportamento dell'applicazione e in modo proattivo intercetta immediatamente qualsiasi azione potenzialmente nociva prima che causi danni. Spostando l'attenzione dalle caratteristiche di firma agli schemi di comportamento nocivi, DeepGuard può identificare e bloccare il malware ancor prima che un campione venga acquisito ed esaminato.
Al primo avvio di un programma sconosciuto o sospetto, DeepGuard ritarda temporaneamente la sua esecuzione per eseguire un controllo della reputazione del file e del suo tasso di diffusione, lo esegue in un ambiente sandbox e infine lo elabora per produrre un'analisi comportamentale e intercettazione degli exploit.

Intelligence in tempo reale sulle minacce

Sistema Security Cloud ,sistema di analisi delle minacce basato sul cloud. Usa, tra gli altri, Big Data e Machine Learning per aggiornare continuamente la nostra base di conoscenza delle minacce digitali. Security Cloud è sempre in contatto con i sistemi client, identificando le nuove minacce non appena emergono e fornendo protezione nell'arco di pochi minuti.
Un servizio di analisi delle minacce basato sul cloud presenta molti vantaggi rispetto agli approcci tradizionali. L'intelligence per le minacce è il risultato della raccolta di centinaia di migliaia di nodi client, realizzando

un'immagine in tempo reale della situazione globale delle minacce. Nell'arco di pochi minuti, usiamo queste informazioni per proteggere i nostri clienti.
Ad esempio, se l'analisi euristica e del comportamento di DeepGuard identifica un attacco zero-day, l'informazione viene condivisa con tutti i dispositivi protetti tramite Security Cloud, rendendo l'attacco inoffensivo pochi minuti dopo la sua individuazione.

Protezione contro i malware

Il componente per la sicurezza dei computer utilizza una piattaforma di protezione a più motori per individuare e bloccare il malware. Fornisce una protezione superiore rispetto alle tradizionali tecnologie basate sulla firma.
Individua una gamma più ampia di funzioni, schemi e trend nocivi, consentendo un rilevamento più affidabile e accurato, anche per varianti precedentemente sconosciute di malware
Sfruttando controlli in tempo reale con Security Cloud, è in grado di individuare più rapidamente minacce nuove ed emergenti oltre ad assicurare un'impronta ridotta
L'emulazione consente il rilevamento di malware che utilizza tecniche di offuscamento e fornisce un ulteriore livello di sicurezza prima dell'esecuzione di un file

Blocco dell'accesso a siti dannosi

Browsing Protection è un livello di sicurezza fondamentale che impedisce in modo proattivo agli utenti di visitare siti dannosi. Ciò è particolarmente efficace in quanto questo genere di intervento riduce l'esposizione generale a contenuti dannosi e quindi ad attacchi.
Browsing Protection impedisce, ad esempio, agli utenti finali di essere indotti ad accedere a siti di phishing apparentemente normali, a siti dannosi attraverso link e-mail e di venire infettati tramite pubblicità di terze parti su siti normalmente innocui.
Questa funzione controlla la reputazione più recente dei siti web e dei file dal Security Cloud, basandosi su vari dati, quali indirizzi IP, parole chiave dell'URL e comportamento del sito.
Browsing Protection è indipendente dal browser in quanto funziona a livello di rete. Ciò assicura una protezione anche nel caso in cui l'utente non utilizzi i browser raccomandati dall'azienda.

Blocco dei contenuti web dannosi

Web Traffic Protection impedisce che contenuti attivi come Java e Flash, ampiamente usati per gli attacchi online, vengano utilizzati per exploit. Questi componenti vengono bloccati automaticamente su siti sconosciuti e sospetti in base ai dati della reputazione. Gli amministratori possono consentire eccezioni aggiungendo voci a un elenco di siti fidati, per esempio contrassegnando in questo modo i siti dell'intranet dell'azienda, per i quali la soluzione non ha informazioni relative alla reputazione.
Web Traffic Protection analizza il traffico Web HTTP in tempo reale, con più motori di analisi anti-malware complementari e controlli della reputazione. In questo modo malware ed exploit vengono individuati e bloccati durante il traffico Web, prima che i dati vengano scritti sul disco fisso. Si tratta di una protezione aggiuntiva contro il malware più avanzato, come la tipologia che agisce su aree della memoria.

Web Content Control

Web Content Control consente di limitare l'utilizzo improduttivo e inappropriato di Internet. Limita la navigazione Web dei dipendenti, negando l'accesso a destinazioni non collegate all'ambito lavorativo come social media e siti per adulti al fine di sfruttare al meglio il tempo ed evitare siti dannosi.
Web Content Control riduce perdite di produttività, consumo della larghezza di banda e rischi legali causati dall'accesso non autorizzato da parte dei dipendenti a materiale web inappropriato o di svago. Riduce inoltre le possibilità che i dipendenti siano esposti a contenuti nocivi.
Gli amministratori IT possono creare eccezioni locali che ignorano le categorie imposte. Ad esempio, anche in caso di blocco dell'accesso ai social network, si può aggiungere come eccezione Linkedin.com all'elenco di siti fidati.

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

Alto livello di sicurezza per siti web fondamentali

Connection Control è un livello di sicurezza che aumenta ampiamente la protezione per attività web fondamentali per l'azienda, ad esempio l'utilizzo di intranet o servizi sensibili basati sul cloud come CRM.
Non appena un dipendente accede a un sito web che richiede una protezione aggiuntiva, Connection Control aumenta automaticamente il livello di sicurezza per la sessione. In questo lasso di tempo, Connection Control chiude le connessioni di rete a tutti i siti sconosciuti dall'endpoint. Gli utenti possono continuare a utilizzare i siti che sono stati verificati come sicuri dal sistema antivirus in modo da non ridurre la produttività dei dipendenti.
Tramite il blocco delle connessioni non sicure, trojan bancari e altri malware non sono in grado di inviare a criminali informazioni aziendali riservate come le credenziali utente e le informazioni basate sul cloud. La sicurezza torna a livello normale quando termina il processo specifico del browser o l'utente conclude la sessione.

Accesso solo per hardware autorizzato

Device Control impedisce che le minacce penetrino nel sistema attraverso dispositivi hardware quali chiavette USB, drive CD-ROM e webcam. Impedisce anche la perdita di dati, consentendo ad esempio un accesso in sola lettura.
Se un dispositivo proibito viene connesso, Device Control lo spegne per evitare ogni possibile accesso. E' possibile impedire l'accesso ai dispositivi impostando regole predefinite, e definire regole per consentire dispositivi specifici, mentre tutti gli altri dispositivi della stessa categoria vengono bloccati. Ad esempio è possibile:
Disabilitare l'esecuzione di programmi da USB/CD/altri drive: disabilita auto run, esecuzione accidentale o lancio di moduli da supporti rimovibili
Bloccare completamente alcune tipologie di device
Impostare un accesso read-only a USB/CD/altri drive
Bloccare alcune tipologie di device con l'eccezione di dispositivi specifici

Firewall

firewall che usa il rule engine Windows di default per eseguire regole firewall. Questo incrementa in modo sensibile la compatibilità con altre applicazioni e appliance. Il sofisticato ruleset , che contiene regole avanzate che combattono rischi quali la propagazione del ransomware e i movimemti laterali, sono aggiunte sul ruleset standard di Windows.
L'amministratore può estendere i set di regole per affrontare minacce specifiche per l'azienda e il contesto. Inoltre, regole di auto-selezione consentono agli amministratori di definire profili sulla base delle necessità di sicurezza di reti differenti.

Sicurezza con i sistemi Windows Anti-malware avanzato
Funzionalità di multi-engine detection, che offrono una sicurezza decisamente superiore.
• DeepGuard
Protezione proattiva da malware zero-day ed exploit grazie ad analisi euristica e comportamentale.
• Patch management
Esegue patch su oltre 2.500 software per server e di terze parti, come Apache, BizTalk, SQL, Flash, ecc.
• Protezione web
Blocca contenuti web pericolosi e impedisce l'accesso a siti malevoli e di phishing.
• Exchange, SharePoint, Citrix, Linux
Componenti di sicurezza dedicate disponibili per piattaforme differenti.

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

Servizi aggiuntivi a corredo della fornitura:

- Garanzia su tutte le apparecchiature fornite on site della durata di 24 mesi. Sarà a carico della ditta aggiudicatrice a seguito segnalazione da parte della scuola attraverso i canali stabiliti (Numero Telefonico –Mail – Portale) la rilevazione del malfunzionamento degli appartati e l'eventuale apertura di una pratica di garanzia con il brand di riferimento.
- Gli oneri per la sicurezza aziendale saranno a completo carico della ditta vincitrice , gli stessi dovranno comprendere tutti quelli previsti dal D.Lgs. n.81/2008 e s.m. e i. e, in particolare, quelli contenuti negli artt. 96 e 97 e nell'allegato XIII del citato D.Lgs. n.81/2008 e s.m. e i..
- Tutte le attrezzature e gli arredi dovranno essere in regola con la normativa sulla sicurezza sui luoghi di lavoro (T.U81/2008)
- Saranno a carico della ditta le spese di imballo spedizione, trasporto scarico e installazione del materiale nei locali dell'istituto.
- La ditta dovrà assumersi in proprio ogni responsabilità impegnandosi a tenere indenne l'istituzione scolastica anche in sede giudiziale per infortuni o danni subito a persone, cose, locali o impianti della scuola connessi comunque all'esecuzione della fornitura e installazione oggetto del presente bando.
- L'offerta tecnica pena esclusione dovrà indicare marca e modello di ogni singolo prodotto o software fornito, gli stessi dovranno essere facilmente ricercabili su internet mediante il codice del produttore che pena esclusione dovrà essere chiaramente indicato. Le soluzioni hardware e software proposte dovranno essere presenti nei listini ufficiali della casa madre al momento dell'offerta.
- Tutte le apparecchiature proposte rientranti nella categoria NACE 26.20.00 Fabbricazione di computer e unità periferiche e specificatamente :
    - fabbricazione di computer da scrivania
    - fabbricazione di terminali dedicati per computer
    - fabbricazione di server
    - fabbricazione di scanner, inclusi quelli per codici a barre
    - fabbricazione di lettori di smart card
    - fabbricazione di caschi per la realtà virtuale
    - fabbricazione di proiettori per computer (videoproiettori)
    - fabbricazione di terminali: terminali vocali (Atm), terminali Pos, non azionati meccanicamente, terminali per emettere biglietti, prenotazioni eccetera
    - fabbricazione di attrezzature da ufficio multifunzione che svolgono due o più delle seguenti funzioni: stampa,scansione, copia, fax
    - fabbricazione di distributori automatici di banconote

dovranno rispettare il principio di non arrecare danno significativo agli obiettivi ambientali ai sensi dell'articolo 17 del regolamento (UE)2020/852 (DNSH). Le apparecchiature saranno ritenute conformi mediante analisi da parte della nostra amministrazione dell'Allegato 3 Dnsh (Checklist 3_AEE.v.1)

- Tutti i Servizi Cloud proposti rientranti nelle categorie NACE 631000 – NACE 631100 dovranno rispettare il principio di non arrecare danno significativo agli obiettivi ambientali ai sensi dell'articolo 17 del regolamento (UE)2020/852 (DNSH). I servizi saranno ritenuti conformi mediante analisi da parte della nostra amministrazione dell'Allegato 6 Dnsh (Checklist 6_Servizi informatici di hosting e cloud.v.1)

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

Art. 2 Servizi da fornire

Servizi e lavori minimi richiesti pena esclusione:

1) Montaggio di tutti i beni forniti secondo le esigenze della scuola
2) L'assistenza tecnica in garanzia sui beni forniti presso l'Istituto (On Site) da erogarsi nei normali orari di ufficio, che dovrà essere erogata, a partire dalla data del collaudo effettuato con esito positivo, per un periodo minimo di 24 mesi, con intervento entro almeno due giorni lavorativi.
3) Il ritiro e lo smaltimento degli imballaggi.

Art. 3 Indicazioni per l'offerta

INDICARE MARCA e MODELLO dei prodotti offerti ed allegare documentazione tecnica.
Si precisa che non sono accettati prodotti di importazione che non siano a diffusione internazionale e che non abbiano una garanzia internazionale del produttore, ciò a tutela della stazione appaltante che deve avere garantita la riparazione del prodotto anche in caso di fallimento del fornitore o del distributore nazionale. Si accettano beni prodotti e garantiti direttamente da produttore nazionale solo se aventi le certificazioni previste nel disciplinare; in tal caso inoltre la garanzia del produttore deve prevedere la sostituzione del bene con intervento on-site, ossia presso la stazione appaltante.
Sarà ovviamente sempre e comunque l'operatore economico a rispondere nei riguardi dell'istituzione scolastica nel periodo di garanzia.
Ai fini dell'ammissibilità della spesa, le attrezzature acquistate dovranno rispettare il principio di non arrecare danno significativo agli obiettivi ambientali ai sensi dell'articolo 17 del regolamento (UE) 2020/852 (DNSH). A tal fine è possibile verificare il rispetto di tale principio, applicando i requisiti previsti dal Documento di Lavoro dei Servizi della Commissione "Criteri in materia di appalti pubblici verdi dell'UE per i computer, i monitor, i tablet e gli smart-
phone", SWD(2021) 57 final del 5.3.2021, nel caso di acquisto di attrezzature rientranti in tali tipologie saranno ritenute conformi se in possesso delle sottoelencate etichette ambientali :

- Etichetta ambientale di tipo I, secondo la UNI EN ISO 14024, ad esempio TCO Certified, EPEAT 2018, Blue Angel, TÜV Green Product Mark o di etichetta equivalente)
- In caso di assenza di un etichetta ambientale di tipo I : Etichetta EPA ENERGY STAR on in alternativa dichiarazione del produttore che attesti che il consumo tipico di energia elettrica (Etec), calcolato per ogni dispositivo offerto, non superi il TEC massimo necessario (Etec-max) in linea con quanto descritto nell'Allegato III dei criteri GPP UE

Per condizioni aggiuntive consultare la Scheda 3 - Acquisto, Leasing e Noleggio di computer e apparecchiature elettriche ed elettroniche (Guida Operativa Edizione aggiornata allegata alla circolare RGS n. 33 del 13 ottobre 2022)

Le attrezzature acquistate dovranno rispettare i CRITERI AMBIENTALI MINIMI PER LA FORNITURA DI ARREDI PER INTERNI come da DECRETO del 23 giugno 2022 del MINISTERO DELLA TRANSIZIONE ECOLOGICA (Criteri ambientali minimi per l'affidamento del servizio di fornitura, noleggio ed estensione della vita utile di arredi per interni) ed in particolare i criteri obbligatori in base a quanto previsto dall'art 57 del decreto legislativo 31 marzo 2023 n. 36.

L'operatore economico presenterà le informazioni richieste secondo quanto indicato in appendice "A" del medesimo decreto.

Per.to Ind. Sandro Falivene
Via Carmine Maiorini 1 – 84096, Montecorvino Rovella (SA)
Partita IVA: 04574170652
sandrofalivene@pec.it

Art. 4 Schede tecniche

Vanno necessariamente allegate le schede tecniche del materiale, pena esclusione, fornite dal produttore e non da un rivenditore, e devono essere presenti le specifiche richieste, e/o equivalenti e/o superiori.

Art. 5 Fornitura unitaria ed omnicomprensiva

I beni dovranno essere completamente installati e configurati, comprese le funzionalità di ottimizzazione, secondo la formula "chiavi in mano". Nessun altro onere potrà essere chiesto all'Istituto e l'operatore economico presentando l'offerta accetta tutti gli oneri anche imprevisti ed occulti. E' interesse dell'operatore economico, a sua scelta, effettuare sopralluogo, e comunque non potrà essere addebitato nulla alla stazione appaltante per imprevisti derivanti dalla mancata conoscenza dei luoghi. Non sono ammesse varianti in corso d'opera se non concordate con la stazione appaltante.

In fase di esecuzione la ditta dovrà interfacciarsi con il progettista per eventuali variazioni.

Tanto dovevo per l'incarico ricevuto.

Resto a disposizione dell'Amministrazione per qualsiasi aggiornamento o chiarimento

Montecorvino Rovella, 03/09/2023

Il Progettista

Per. Ind. Sandro Falivene