



Istituto Comprensivo Statale PICENTIA



Sede Legale via Liguria – 84098 - Pontecagnano Faiano (Sa) – C.M. SAIC8BK008 – C.F. 95156810657 – C.U. UF30A5

Tel/fax 089.383344 - 089.3854657 - e-mail: saic8bk008@istruzione.it - saic8bk008@pec.istruzione.it – sito web: www.icpicentia.edu.it

ISTITUTO COMPRENSIVO - "PICENTIA"-PONTECAGNANO
Prot. 0002921 del 31/08/2023
VI (Uscita)

All'Albo Pretorio
Area PNRR
Al DSGA
Agli atti

OGGETTO: Lettera di Trasmissione PROGETTO e avvio procedure di affidamento PNRR – Missione 4: Istruzione e ricerca – Componente 1 – Investimento 3.2: Scuola 4.0 – Azione 1 – Next generation classroom – Ambienti di apprendimento innovativi, Codice Progetto M4C1I3.2-2022-961-P-20829

CUP: G64D23000920006

LA DIRIGENTE

VISTO Il Decreto prot. n. 1422 del 03/04/2022 con il quale la Dirigente si è autonominato Responsabile Unico del procedimento (RUP);

VISTA la delibera n. 2 del Consiglio di Istituto n. 9 dell'8 maggio 2023 di autorizzazione alla sottoscritta a ricoprire l'incarico di Responsabile di progetto nell'ambito del finanziamento PNRR di cui all'oggetto;

VISTA la nomina della Dirigente quale responsabile del progetto prot. n. 2002 del 16/05/2023);

PRESO ATTO delle indicazioni del Gruppo di supporto al DS, in merito al progetto e che lo stesso risulta coerente con i target assegnati all'istituto dal PNRR;

CONSIDERATI i tempi di attuazione dell'intervento in oggetto come da cronoprogramma compilato all'interno della Piattaforma FUTURA;

in qualità di Progettista del progetto **M4C1I3.2-2022-961-P-20829**

TRASMETTE

L'allegato Capitolato tecnico (Allegato 1) agli atti del PNRR e al DSGA e alle figure di supporto, per gli adempimenti di competenza e

DISPONE

l'avvio della fase di affidamento delle prestazioni e degli acquisti previsti per la realizzazione del progetto.

F.to Il Dirigente Scolastico
Dott.ssa Ginevra de Majo
(Documento firmato digitalmente)

CAPITOLATO TECNICO

LINEA GUIDA - CAPITOLATO

Fornitura e installazione di n.21 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.15 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.

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 software viene 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.
- Inviare 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 di strumenti 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 revocati 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

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. 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 movimenti 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 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.

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 movimenti 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 Carrello Mobile di ricarica e conservazione per notebook e tablet avente le seguenti caratteristiche tecniche :

- Anta anteriore apribile a 270°
- porte con chiusura a chiave
- impugnature ergonomiche
- Gruppo di ventilazione forzata dell'aria incluso
- divisori in ABS con passacavi
- Materiale impugnature ABS/Metallo bianco

- 36 alloggiamenti suddivisi in 3 livelli da 12 dispositivi
- ruote con freno per agevolare lo spostamento
- Power Management System incluso per la gestione temporizzata di 3 cicli diversi di ricarica
- Corso di formazione al corretto utilizzo del prodotto

SCUOLA PRIMARIA RODARI

Fornitura e installazione di n.05 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.23 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.

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.

Distribuisce e raccoglie file

- Distribuisce file e cartelle dal PC del tutor a più dispositivi studente.
- Trasferisce 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 software viene 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.
- Inviare 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 di strumenti 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 revoca di 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

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.

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 movimenti 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 Carrello Mobile di ricarica e conservazione per notebook e tablet avente le seguenti caratteristiche tecniche :

- Anta anteriore apribile a 270°
- porte con chiusura a chiave
- impugnature ergonomiche
- Gruppo di ventilazione forzata dell'aria incluso
- divisori in ABS con passacavi
- Materiale impugnature ABS/Metallo bianco
- 36 alloggiamenti suddivisi in 3 livelli da 12 dispositivi
- ruote con freno per agevolare lo spostamento
- Power Management System incluso per la gestione temporizzata di 3 cicli diversi di ricarica
- Corso di formazione al corretto utilizzo del prodotto

HOME STUDIO RECORDING

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.

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 movimenti 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 Monitor Lcd avente le seguenti caratteristiche tecniche minime:

- Display 23,8" Ips
- Risoluzione 1920x1080 (Full HD)
- Luminosità 300 cd/m2
- Refresh rate 100 Mhz
- Connettività Display Port – 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

Fornitura e Installazione di n.01 INTERFACCIA AUDIO USB avente le seguenti caratteristiche tecniche minime:

- Compatibilità multipiattaforma Windows, macOS e iOS per una flessibilità superiore
- Preamplificatori microfonic 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.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

Fornitura e Installazione di n.01 Kit composto da mouse e tastiera avente le seguenti caratteristiche tecniche minime:

CARATTERISTICHE MOUSE

- Interfaccia mouse Wireless
- Tipo di mouse Mouse Laser
- Numero di tasti totali 2
- Sensore di movimento Laser
- Rotella di scorrimento 1
- Tipo di connessione Wireless

CARATTERISTICHE TASTIERA

- Interfaccia tastiera Wireless
- Keyboard Layout Versione Italiana
- Colore tastiera Nero
- Tipo di connessione Wireless

DIMENSIONI E PESO TASTIERA

- Altezza 17,5 cm
- Larghezza 46,5 cm
- Peso 510 gr

LABORATORIO DI INFORMATICA SECONDARIA

Fornitura e Installazione di n.22 All in One avente le seguenti caratteristiche tecniche minime:

- Processore Intel i5-12400T
 - Ram 8 Gb DDR4
 - Hard Disk 500 Gb SSD
 - Display 21,5 " Touch Screen
 - Connettività Wifi
 - Mouse e Tastiera Wifi
 - 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.

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 movimenti 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. 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 movimenti 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.

INNOLAB SECONDARIA

Fornitura e Installazione di n.02 Workstation di primaria marca internazionale avente le seguenti caratteristiche tecniche minime :

- Processore I9-13900HX
- Ram 16 Gb
- SSD PCI EXPRESS 1000 GB
- Display 16" WQXGA Ips
- GeForce RTX 4060 8 Gb -GDDR6
- Connettività Wifi 6-Bluetooth 5.0
- Sistema Operativo Windows 11 Home
- Servizio di consegna e Installazione on site
- Breve 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.

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 movimenti 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 Visore avente le seguenti caratteristiche tecniche minime:

- Tecnologia 6DoF, il visore effettua il tracking dei movimenti di testa e corpo per poi tradurli in VR con precisione realistica
- Controller Touch ergonomici con appoggio per il pollice
- Cinturino Morbido con regolazione
- Display LCD a commutazione rapida Risoluzione di 1832x1920 per occhio ,Supporto per frequenza di aggiornamento a 60, 72 e 90 Hz
- Audio posizionale 3D integrato direttamente nel visore
- SPAZIO DI ARCHIVIAZIONE 128 GB
- Cavo ottico attivo USB completo. USB 3.2 Gen 1 Type-C della lunghezza di 5 mt
- Configurazione e installazione on site secondo le indicazioni del progettista
- Assistenza nella creazione degli account necessari per il collegamento del visore
- Corso di formazione della durata di 4 ore al corretto utilizzo del prodotto
- Schermo: 1.832 x .1920 pixel per occhio, Fast-switch LCD, 72 Hz
- Processore: Qualcomm Snapdragon XR2
- RAM: 6 GB
- Audio: 3D positional speaker, jack 3,5 mm
- Servizio di Installazione e configurazione on site secondo le indicazioni del progettista
- Assistenza alla creazione degli account necessari per il corretto utilizzo del prodotto
- Corso di formazione della durata di 4 ore al corretto utilizzo del Visore.

AULA ATTIVA DIGITAL HUMANITIES

Fornitura e Installazione di n.20 Notebook di primaria marca internazionale avente le seguenti caratteristiche tecniche :

- Processore tipo intel I3-1215U o superiore
- Ram 8 Gb DDR4
- Hard Disk 256 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 tastiera.
- 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.

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.

Distribuisce e raccoglie file

- Distribuisce 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 software viene 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.
- Inviare 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 di strumenti 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

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.

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 movimenti 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 Carrello Mobile di ricarica e conservazione per notebook e tablet avente le seguenti caratteristiche tecniche :

- Anta anteriore apribile a 270°
- porte con chiusura a chiave
- impugnature ergonomiche
- Gruppo di ventilazione forzata dell'aria incluso
- divisori in ABS con passacavi
- Materiale impugnature ABS/Metallo bianco

- 36 alloggiamenti suddivisi in 3 livelli da 12 dispositivi
- ruote con freno per agevolare lo spostamento
- Power Management System incluso per la gestione temporizzata di 3 cicli diversi di ricarica
- Corso di formazione al corretto utilizzo del prodotto

Fornitura e Installazione di n.04 Notebook di primaria marca internazionale avente le seguenti caratteristiche tecniche :

- Processore tipo intel Celeron N4500 o superiore
- Ram 4 Gb DDR4
- Hard Disk Tipo e-MMC 128 Gb
- Scheda Grafica UHD Graphics
- Display 11,6" Lcd Touch Screen (Tipo Convertibile)
- Web Cam e Microfono
- Connettività Bluetooth – Wifi 802.11 AX- 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.

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 software viene 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.
- Inviare 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 di strumenti 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 revoca di 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

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.

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 movimenti 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 Sistema Audio 2.0 Portatile avente le seguenti caratteristiche :

Performance

Controllo del volume Manopola

Telecomando Sì

Tipo telecomando Wireless

Controllo livello dei bassi Sì

Interruttore integrato Sì

Regolazione treble Sì

Prestazione

Plug & Play Sì

Colore del prodotto Nero

Utilizzo raccomandato Universale

Materiale della scocca MDF

Acuto regolabile Sì

Certificazione CE, ROHS

Karaoke Sì

Dettagli tecnici

Durata della garanzia 2 anno/i

Connettività

Connettore 3.5 mm Sì

Bluetooth Sì

Collegamento del dispositivo USB Sì

Connettore USB USB di tipo B

AC (power) in Sì

Tecnologia di connessione Con cavo e senza cavo

Ingresso di linea Sì

Lettore di schede integrato Sì

Portata Bluetooth 10 m

Dimensioni e peso

Profondità 200 mm

Altezza 200 mm

Larghezza 200 mm

Gestione energetica
Consumi (modalità stand-by) 1 W
Tipologia alimentazione AC
Tensione di ingresso AC 220 V
Altoparlanti
Tipo di speaker 2-vie
Sistema audio 2.0 canali
Woofers Sì
Tweeters Sì
Dimensioni Tweeter 1.5 "
Numero di driver tweeter 2
Posizionamento diffusori Tavolo/Libreria
Numero di driver 4
Numero di driver woofer 2
Dimensioni woofer 4 "
Amplificatore
Amplificatore Da Incasso
Classe dell'amplificatore D
Sostenibilità
Conformità alla sostenibilità Sì
Certificati di sicurezza
Conformità ai rifiuti di apparecchiature elettriche ed elettroniche (WEEE) Sì

Fornitura e Installazione di n.24 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 sì

CONNETTIVITÀ

- Alimentazione USB
- Tipo di porta USB-A

Fornitura e Installazione di n.01 Scanner portatile avente le seguenti caratteristiche :

GESTIONE MEDIA

- ADF compreso sì
- PDF Sì
- Formati carta gestiti Up to A4 max
- Tipi di supporti Up to A4 max

SISTEMA SCANSIONE

- Formato massimo scansione A4
 - Modalità di scansione Rotativa
 - Elemento di scansione CIS
 - Profondità colore 24 bit
 - Funziona senza PC Sì
 - Profondità colore esterna 24 bit
 - Funzioni pulsanti pannello di controllo Slide on document to scan Black and white /colorPDF/JPEG
- 300/600/900 dpi selectione
- Tipo sorgente luminosa / lampada Non presente
 - Profondità di grigio 24 bit
 - Profondità di grigio esterna 24 bit

- Jpeg Sì
- Altri formati scansione PDF e Multi-pagePDF
- Dimensione massima di scansione Orizz. 21 cm
- Dimensione massima di scansione Vert 29,7 cm

CONNETTIVITÀ

- Nr. porte usb 2.0 1

PERFORMANCE SCANSIONE

- Risoluzione Ottica Orizzontale 600 dpi
- Velocità scansione b&n 3 sec
- Velocità scansione colori 4 sec
- Ciclo operativo/duty cycle 100 pages/day
- Risoluzione Ottica Verticale 1.200 dpi
- Risoluzione Interpolata Orizzontale 600 dpi
- Velocità scansione anteprima 9 sec
- Risoluzione interpolata verticale 1.200 dpi
- velocità scansione OCR 3 sec
- Scansione foto Sì

REQUISITI E CONSUMO ENERGETICO

- Potenza assorbita in esercizio 2,9 W
- Tensione di alimentazione 5

PANNELLO LCD

- Caratteristiche pannello di controllo 1,5" a colori con indicatore dello stato di acquisizione/anteprima

INCLUSO NELLA CONFEZIONE

- Cavo Usb Sì
- Software incluso Readiris Pro 15 (OCR software) ScannerIRIScan™ Book 5 - Software Readiris™ Pro & IRISCompressor™ Pro per PC e Macscaricabili sul sito www.irislink.com/start - Una scheda SD -Custodia.

CERTIFICAZIONI

- Certificazione IEC 60950-1 Sì
- Certificazione CE Sì
- Altre certificazioni FCC ROHS WEEE

Fornitura e Installazione di n.01 Monitor Interattivo 86" avente le seguenti caratteristiche tecniche minime:

- Tocchi supportati Fino a 40 tocchi simultanei
- Vetro Temperato caldo, sp 4mm, anti glare
- Modalità di scrittura Dita,penna o strumento non trasparente
- Durezza del vetro 7 Mohs
- Precisione di puntamento $\leq 1\text{mm}$
- Profondità del tocco $3 \pm 0.5\text{mm}$
- Caratteristiche display IPS Direct LED
- Rapporto di visualizzazione 16:9
- Risoluzione 4K UHD 3840 x 2160pixels, Freq 60 HZ
- Sistema Operativo Android 11
- o Cpu Quad core ARM Cortex-A55
- o Ram 4 GB DDR4
- o Rom 32 Gb
- o Connettività Bluetooth 5.0 – Wireless Built-in 802.11 a/b/g/n/ac/ax
- Wifi 6 2.4/5GHz, 2x2

- Casse 2x20W
- Porte Frontali Hdmi 2.0 – Usb 3.0 – Usb-c

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 Document Camera avente le seguenti caratteristiche :

Immagini nitide e fluide

Fotocamera con risoluzione Full HD 1080p e frequenza di aggiornamento dello schermo di 30 fps

Immagini estremamente ricche di dettagli

Zoom digitale 8x, messa a fuoco automatica e fermo immagine

Collegamento semplice

Connessione tramite cavo USB 2-in-1, senza necessità di un alimentatore separato

Flessibilità per immagini 2D e oggetti 3D

Altezza regolabile, testina ruotabile di 90° e attacco per microscopio

Leggero e portatile

Soluzione portatile con peso inferiore a 1 kg, facilmente trasportabile nella pratica borsa morbida inclusa