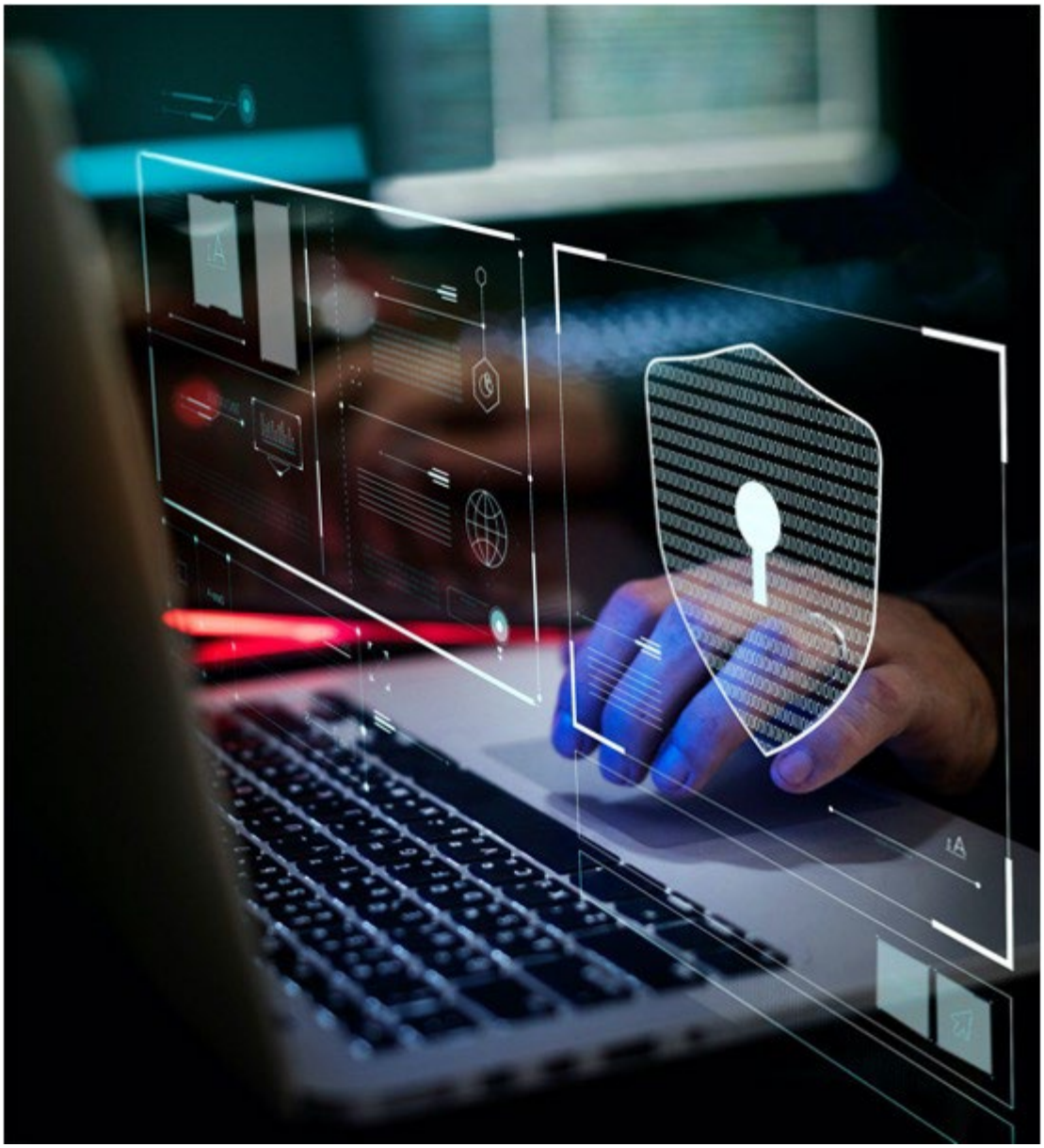


Sicurezza di nuova generazione Xerox: Collaborazione con Trellix[1]

White Paper

[1]Trellix, azienda precedentemente nota come McAfee Enterprise

xerox™

Lo scenario

Le stampanti multifunzione del giorno d'oggi sono sistemi integrati complessi. Contengono, tra le altre cose, sistemi operativi completi, server Web integrati, supporto per molteplici stack di protocolli, interfacce hardware e software esterne e interfacce API (Application Programming Interface) per interagire con i sistemi aziendali. Proprio perché così ricchi di funzionalità e straordinariamente potenti, se non adeguatamente protetti questi dispositivi multifunzione rappresentano potenzialmente un serio rischio per la vostra rete e i vostri sistemi aziendali.

I vendor di stampanti multifunzione hanno significativamente intensificato i loro sforzi ingegneristici volti a rafforzare i controlli di sicurezza in questi dispositivi, introducendo miglioramenti alla protezione quali:

- Crittografia del disco e sovrascrittura del disco per proteggere i dati degli utenti finali
- Abilitazione di protocolli crittografati quali TLS (Transport Layer Security), IPsec (Internet Protocol Security) e SNMPv3 (Simple Network Management Protocol Versione 3) per proteggere i dati trasmessi al/dal dispositivo
- Autenticazione utente per la gran parte delle attività
- Controllo dell'accesso tramite l'aggiunta di firewall e ruoli basati su gruppi Active Directory (AD)
- Registri di controllo per la tracciabilità
- Programmi di valutazione della sicurezza quali la certificazione Common Criteria

Le stampanti multifunzione sono sistemi integrati o sistemi aperti? Tali dispositivi necessitano di un ulteriore livello di sicurezza? Se sì, qual è la soluzione giusta per proteggere server, desktop e reti da minacce odierne e future? Questa è una domanda alla quale gli esperti nel campo della sicurezza cercano incessantemente di trovare risposta.

Sappiamo che le tradizionali tecnologie di sicurezza, come gli antivirus, hanno un'efficacia limitata contro l'odierna generazione di minacce quali gli attacchi mirati e persistenti (APT) e le botnet.

La realtà è che, nonostante le ulteriori funzioni di sicurezza aggiunte dai vendor di stampanti multifunzione, gli incidenti di sicurezza continuano a susseguirsi. Il comun denominatore di tutti questi incidenti è che i clienti li scoprono solo a violazione avvenuta. A quel punto, il vendor e il cliente si affannano a mitigare i danni, trovare un rimedio, e implementare una soluzione. È l'equivalente del valutare i danni e installare un sistema di sicurezza dopo che la banca è stata assalita e svaligiata.

[1]Trellix, azienda precedentemente nota come McAfee Enterprise

DISPOSITIVI INTEGRATI

Un sistema integrato è un sistema informatico progettato per specifiche funzioni fisse. I sistemi integrati abbracciano tutti gli aspetti della vita moderna: sportelli bancomat, dispositivi medici, stampanti, sistemi POS, chioschi, ecc.

Tuttavia, le stampanti multifunzione del giorno d'oggi svolgono più di una singola funzione: sono un ibrido tra una macchina monofunzione e un server di rete IT. Entrambi sono dotati di dischi rigidi, sistemi operativi, server Web, molteplici connessioni di ingresso e di uscita e interfacce, ed elaborano svariati tipi diversi di informazioni. Tali dispositivi necessitano di un ulteriore livello di sicurezza? Qual è la soluzione giusta in grado di proteggere server, desktop e reti dalle minacce di oggi e di domani? Questa è una domanda alla quale gli esperti nel campo della sicurezza cercano incessantemente di trovare risposta.

Sappiamo che le tradizionali tecnologie di sicurezza, come i software antivirus, non sono in grado di combattere l'odierna generazione di minacce quali gli attacchi mirati e persistenti (ATP) e le botnet, ed è ormai opinione largamente diffusa che la tecnologia Whitelisting/Allowlisting possa essere la risposta giusta per combattere tali minacce.

Iniziamo dunque esaminando cosa sono le whitelist/allowlist e le blacklist/blocklist.

BLACKLIST/BLOCKLIST

Per combattere l'accesso non autorizzato, l'uso improprio di informazioni e i malware, gli amministratori della sicurezza IT si affidano solitamente a strumenti quali software antivirus, anti-malware e monitoraggio dell'accesso alla rete e dei contenuti. La maggior parte degli strumenti può essere suddivisa in due modelli: le blacklist/blocklist e le whitelist/allowlist.

Un antivirus si basa su funzioni di hash per bloccare malware conosciuto. Una volta isolata una particolare variante di un virus, il suo hash viene aggiunto alla blacklist/blocklist, che assume la forma dei file .dat che devono essere scaricati quotidianamente. Il problema è che in media occorrono quattro giorni per isolare il virus e pubblicare un aggiornamento ai file .dat. In questo lasso tempo, i computer che si basano esclusivamente sugli antivirus sono vulnerabili.

Il difetto maggiore di questo approccio è che è sempre un passo indietro rispetto alla minaccia. Cosa ancora più importante, gli strumenti basati sul blacklisting/blocklisting sono completamente inefficaci contro un evento come un attacco zero-day.

Attacchi zero-day

Un attacco zero-day sfrutta le vulnerabilità al momento irrisolvibili dei dispositivi. Di norma, quando un produttore di software scopre un bug o un problema con un prodotto dopo il rilascio, sviluppa e offre una patch per risolvere il problema. Un attacco zero-day approfitta di quel problema prima che venga creata la patch. Individuando queste vulnerabilità prima che vengano scoperte dagli sviluppatori software, un programmatore malintenzionato può creare un virus o un worm in grado di approfittarne e danneggiare un sistema in svariati modi.

[1]Trellix, azienda precedentemente nota come McAfee Enterprise

WHITELISTING/ALLOWLISTING

L'approccio whitelisting/allowlisting è fondamentalmente basato sull'identificazione dei file per un ambiente IT e sul consentire l'accesso al sistema soltanto a tali file. In pratica, viene accettato solo ciò che si conosce e si sa essere "pulito", e si blocca tutto ciò che non si conosce. La politica predefinita consiste nel negare l'esecuzione di un programma software a meno che non sia stato esplicitamente aggiunto alla whitelist/allowlist. Molti degli strumenti di monitoraggio impiegati oggigiorno rientrano nel sistema whitelisting/allowlisting in quanto "consentono" solo a utenti designati, a specifici indirizzi IP o a tipi predefiniti di servizi di entrare o di essere eseguiti nel sistema. Con tale sistema, potete essere certi che un esercito di botnet non potrà reclutare i vostri dispositivi multifunzione per lanciare attacchi!

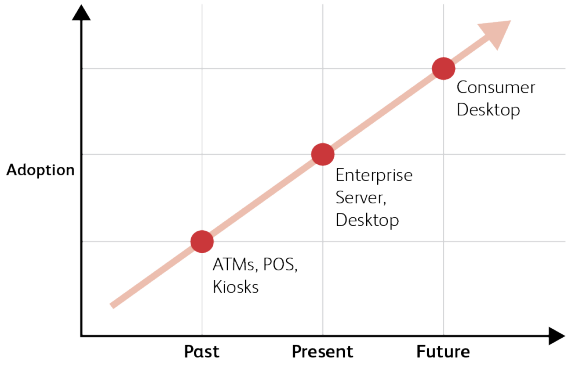
Si sa che le botnet sono composte da migliaia di computer infettati. Una botnet è un insieme di computer infettati da malware che assoggetta il computer al comando e controllo centralizzato di un botmaster. Ogni computer infetto è chiamato uno zombie. Il malware delle botnet risiede nel computer infetto, spesso all'insaputa del proprietario del computer e senza interferire nelle sue operazioni. Il botmaster vende i servizi della botnet a un cliente allo scopo di inviare via e-mail messaggi pubblicitari indesiderati o di provocare un attacco DDOS (Distributed Denial of Service). In un attacco DDOS, tutti gli zombie tentano di accedere simultaneamente a un particolare sito Web, sovraccaricandolo di traffico e causandone il collasso. Pensate ad esempio al movimento "Anonymous" che attacca il sito Web di un governo o una piattaforma digitale non di loro gradimento. Il software Trellix[1] Embedded Control nei dispositivi Xerox® impedisce al malware di penetrare nel dispositivo, proteggendo in tal modo il dispositivo dall'essere catturato nella botnet.

Considerate la differenza tra la tecnologia whitelisting/allowlisting su un computer desktop rispetto a un sistema integrato. Su un computer generico, l'utente può caricare qualsiasi software desideri, cosa che può essere totalmente legittima. Il software whitelisting/allowlisting del desktop deve quindi chiedere all'utente se il nuovo software deve essere accettato. Per contro, in un sistema integrato lo sviluppatore software sa esattamente cosa consentire che venga eseguito su quel sistema, e può bloccare tutto il resto.

Utilizzando una whitelist/allowlist, definiamo cosa deve e non deve accadere. Il caos inizia quando è possibile che accada qualcosa che non dovrebbe accadere, come ad esempio un'applicazione Adobe® Flash® Player che accede a un sistema core. Con la tecnologia whitelisting/allowlisting, è possibile impedire a un'applicazione altrimenti autorizzata di accedere ai file core ai quali non deve avere diritto di accedere.

Adozione della tecnologia whitelisting/allowlisting

È ormai ampiamente noto che la tecnologia whitelisting/allowlisting è uno strumento efficace per contrastare gli attacchi zero-day.



IN CHE MODO PUÒ AIUTARVI XEROX?

Qual è dunque il passo successivo nell'evoluzione della sicurezza al fine di mitigare il rischio di attacchi alla vostra rete tramite le stampanti multifunzione? Xerox è da sempre un'azienda leader per quanto riguarda la sicurezza delle proprie stampanti e stampanti multifunzione.

In linea con la nostra costante attenzione al tema della sicurezza, Xerox ha siglato una partnership con Trellix[1] al fine di stare sempre un passo avanti rispetto alle sempre più numerose minacce ai sistemi integrati. Insieme, abbiamo realizzato le capacità di auto-monitoraggio e auto-protezione di cui ogni singola unità ha bisogno per proteggersi da attacchi fraudolenti. Inoltre, l'agente Trellix[1] in esecuzione nel dispositivo è in grado di comunicare direttamente con la console di gestione della sicurezza centrale – Trellix[1] ePolicy Orchestrator – per consentire la gestione di stampanti e multifunzione nello stesso modo in cui i clienti gestiscono i propri dispositivi desktop.

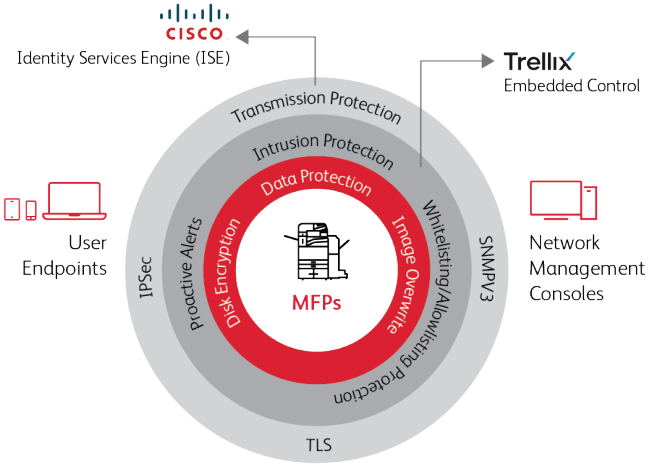
Gli eventi di sicurezza Trellix[1] generati sulle stampanti multifunzione predisposte vengono comunicati alla console Trellix[1] ePolicy Orchestrator configurata. Ciò aiuta a semplificare il monitoraggio di tutte queste stampanti multifunzione da Trellix[1] ePolicy Orchestrator.

Esaminiamo cosa sta facendo Trellix[1] per garantire la migliore sicurezza possibile per le stampanti multifunzione Xerox®.

[1]Trellix, azienda precedentemente nota come McAfee Enterprise

TECNOLOGIA TRELLIX[1] EMBEDDED CONTROL

Con la tecnologia Trellix[1] Embedded Control sui dispositivi Xerox®, i clienti di ogni entità – dalle piccole e medie imprese (PMI) con risorse IT limitate, fino alle grandi aziende – possono avere la tranquillità di sapere che le loro stampanti multifunzione sono totalmente sicure, di serie.



Trellix[1] Embedded Control utilizza la tecnologia whitelisting/allowlisting per proteggere i vostri dispositivi Xerox® dagli attacchi. Tale tecnologia protegge i sistemi chiave e impedisce eventi di modifica non autorizzati, consentendo l'esecuzione solo dei programmi contenuti nella whitelist/allowlist creata da Xerox. Altri programmi, quali i formati file .exe, .dll e script, sono considerati non autorizzati. I tentativi di scrivere in un file di sola lettura o di leggere da una directory o file di sola scrittura vengono impediti, quindi viene creato un evento che viene poi registrato nel registro di controllo del dispositivo. Se SIEM è configurato (in modo nativo su AltaLink® serie 8100 o tramite Xerox® Device Manager per VersaLink®), tutti gli eventi del registro di controllo vengono inoltrati esternamente a un server SIEM per la registrazione e l'analisi. Inoltre, se sul dispositivo Xerox® sono configurati gli avvisi e-mail, viene inviata un'e-mail all'indirizzo designato con i dettagli dell'evento.

Il concetto di whitelisting/allowlisting è semplice: Xerox predefinisce un elenco di applicazioni affidabili, e possono essere eseguite solo quelle applicazioni. È la soluzione ideale per i dispositivi integrati a funzione fissa. La stessa tecnologia viene implementata negli sportelli bancomat.

Funzioni tipiche quali stampa, copia, scansione e fax fanno parte della whitelist/allowlist di un'applicazione ritenuta affidabile. Inoltre, le attività amministrative, quali aggiornamenti firmware, aggiornamenti software, caricamento di moduli e font, modifiche agli attributi di configurazione e diagnostica dei tecnici Xerox, sono tutte operazioni ritenute affidabili.

L'intento del software Trellix[1] è sventare gli attacchi che tentano di danneggiare il software presente del dispositivo o di installare malware non autorizzato. Nel linguaggio della sicurezza, questi attacchi sono noti come "iniezione di codice" o "esecuzione di codice da remoto". Diversamente da altri software che eseguono scansioni periodiche per verificare l'integrità del set di file del sistema operativo, ogni tentativo di lettura, scrittura ed esecuzione viene controllato in tempo reale. Inoltre, il software Trellix[1] Embedded Control gira "sotto" il sistema operativo, di modo che qualsiasi cosa, ad esempio un rootkit, che tenti di lanciare un virus a quel livello, viene rilevata.

Vantaggi che potete attendervi per quanto riguarda la difesa dalle minacce:

- Eliminazione delle patch di emergenza
- Riduzione del numero e della frequenza dei cicli di patch
- Riduzione del rischio di sicurezza derivante da attacchi polimorfici zero-day tramite malware quali worm, virus, Trojan e iniezioni di codice quali buffer overflow, heap overflow e stack overflow
- Sicurezza dell'integrità dei file autorizzati, e garanzia che il sistema è in uno stato noto e verificato
- Riduzione del costo delle operazioni di ripristino correlate a tempi di fermo macchina non programmati
- Aumento della disponibilità del sistema

Trellix[1] Embedded Control rileva i tentativi di modifica in tempo reale. Ad esempio i tentativi di modificare lo stato del sistema, tra cui codice, configurazione e registro di sistema. Tutti gli eventi di modifica vengono registrati e inviati al programma di controllo del sistema.

TRELLIX[1] ENHANCED SECURITY

Trellix[1] Enhanced Security, presente di serie sulle stampanti multifunzione più recenti, è installato e abilitato per impostazione predefinita. Impedisce attacchi generici, come ad esempio la lettura/scrittura non autorizzata di directory e file protetti, ed aggiunge sicurezza alle directory protette designate. Preserva l'integrità della stampante multifunzione consentendo l'esecuzione solo di codice autorizzato e delle modifiche consentite. Con le funzioni di sicurezza base implementate, in presenza di tentativi di modificare le applicazioni di sistema che utilizzano il dispositivo, l'amministratore riceve un avviso e-mail. Inoltre, tali tentativi vengono registrati nei registri di controllo e, a seconda dell'impostazione del cliente, possono quindi essere comunicati tramite il software Xerox® CentreWare® Web o Xerox® Device Manager e, se presente nell'ambiente, tramite Trellix[1] ePolicy Orchestrator® (ePO). Se SIEM è configurato (in modo nativo su AltaLink serie 8100 o tramite Xerox Device Manager per VersaLink), tutti gli eventi del registro di controllo vengono inoltrati esternamente a un server SIEM per la registrazione e l'analisi.

Gli aggiornamenti whitelist/allowlist vengono forniti da Xerox, ma vengono creati solo quando il software integrato viene aggiornato. Alcune funzioni del software sono ritenute intrinsecamente affidabili, ad esempio il processo di aggiornamento software. Viene applicata una firma digitale al software Xerox® per garantirne l'integrità e l'autenticità. Se la firma è valida, il nuovo software viene installato con una nuova whitelist/allowlist.

Indipendentemente dal vostro fornitore di soluzioni di sicurezza, potrete comunque beneficiare delle funzioni di sicurezza integrate di Xerox e Trellix[1] senza necessità di software aggiuntivo. La funzione whitelisting/allowlisting è indipendente da qualsiasi software esterno ed è progettata per funzionare senza compromettere le prestazioni del sistema.

[1]Trellix, azienda precedentemente nota come McAfee Enterprise

Trellix[1] Enhanced Security è progettata per eliminare i problemi relativi all'aumento dei rischi per la sicurezza associati all'adozione di sistemi operativi commerciali nei sistemi integrati. Grazie alle sue dimensioni ridotte e al basso costo di gestione, è una soluzione indipendente dall'applicazione che garantisce tutta la sicurezza che vi occorre, con zero manutenzione.

Vi starete chiedendo come viene installato nuovo software sulla macchina, dal momento che la tecnologia whitelist/allowlist consente solo software di cui è a conoscenza. Tutto il software autorizzato è firmato digitalmente da Xerox. La procedura di installazione del software controlla la firma digitale prima di procedere con un'installazione e, se la firma è valida, informa Trellix[1] Enhanced Security che il nuovo software può essere installato in tutta sicurezza. Poiché Xerox definisce il set di software consentiti durante lo sviluppo, ciascun set di software presenta la propria whitelist/allowlist. Una volta installato il software, Trellix[1] Enhanced Security utilizza la nuova whitelist/allowlist per stabilire cosa è consentito.

Segnalazione di avvisi di minaccia

Gli avvisi di minaccia possono essere comunicati in diversi modi, a seconda della vostra specifica configurazione:

- **Registro di controllo** – Generato dall'interfaccia utente sulla multifunzione, abilitato per impostazione predefinita
- Se SIEM è configurato (in modo nativo su AltaLink® serie 8100 o tramite Xerox® Device Manager per VersaLink®), tutti gli eventi del registro di controllo vengono inoltrati esternamente a un server SIEM per la registrazione e l'analisi
- **Avviso e-mail dal dispositivo** – Configurato tramite l'interfaccia utente di Xerox® CentreWare® Internet Services
- **Avvisi e-mail e report tramite il software Xerox® CentreWare Web e Xerox® Device Manager** – Configurati tramite l'interfaccia utente del software Xerox® CentreWare® Web e di Xerox® Device Manager
- **Avvisi e-mail e report tramite Trellix[1] ePolicy Orchestrator** – Configurati tramite il software di gestione della sicurezza Trellix[1] ePolicy Orchestrator disponibile tramite Trellix[1]
- Gli eventi di sicurezza Trellix[1] generati su tutte le stampanti multifunzione predisposte vengono comunicati alla console Trellix[1] ePolicy Orchestrator configurata. Ciò aiuta a semplificare il monitoraggio di tutte queste stampanti multifunzione da Trellix[1] ePolicy Orchestrator

TRELLIX[1] INTEGRITY CONTROL

Trellix[1] Integrity Control è un software opzionale acquistabile separatamente che coniuga le funzioni di sicurezza di Embedded Control standard e la capacità di monitorare e impedire attacchi mirati e l'esecuzione non autorizzata di file da qualsiasi ubicazione con modalità non attendibili. Impedisce inoltre la scrittura su file eseguibili protetti che non fanno parte del software dei dispositivi Xerox® standard. Rappresenta il massimo livello di sicurezza, la migliore protezione che possiate ottenere per i vostri dispositivi multifunzione Xerox®.

Trellix[1] Integrity Control aggiunge un livello di sicurezza impedendo l'esecuzione di nuovi file da qualsiasi ubicazione non sia considerata un'origine affidabile. Impedisce inoltre la scrittura su file eseguibili protetti, bloccando in questo modo la sovrascrittura fraudolenta di eseguibili forniti da Xerox. Blocca qualsiasi codice non autorizzato o modifica al sistema da parte di malware, worm, Trojan, attacchi zero-day e finanche attacchi mirati. È consentita l'esecuzione solo di software approvato, sventando in tal modo un attacco per il quale non esiste ancora una contromisura.

Xerox e Trellix[1] offrono la tecnologia whitelisting/allowlisting, la quale assicura che solo codice eseguibile affidabile possa essere eseguito su sistemi protetti. Garantisce che sui vostri dispositivi vengano eseguiti solo i servizi che desiderate fornire, impedendo al contempo a un utente non autorizzato di installare codice dannoso. Questa stessa tecnologia viene utilizzata per proteggere server, sportelli bancomat, terminali POS e sistemi quali stampanti e dispositivi mobili.

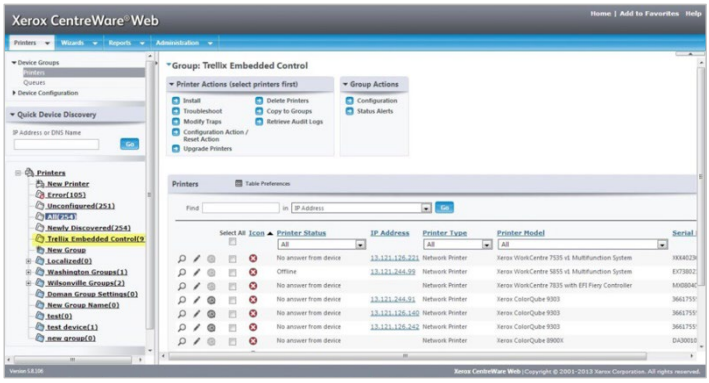
Come detto in precedenza, Trellix[1] Enhanced Security viene offerta come funzione standard, completamente installata e abilitata, su modelli selezionati. Per la funzione opzionale Trellix[1] Integrity Control, non è richiesta alcuna procedura di installazione per i clienti e l'attivazione è basata su un processo con chiave di licenza.

GESTIONE DEI DISPOSITIVI DOTATI DI TRELLIX[1] EMBEDDED CONTROL

Sono disponibili diverse opzioni per gestire i dispositivi dotati di Trellix[1] Embedded Control:

Software Xerox® CentreWare® Web e Xerox® Device Manager

Il software Xerox® CentreWare® Web è un innovativo strumento software basato su browser che installa, configura, gestisce, controlla e invia report sulle stampanti e i dispositivi multifunzione in rete di qualunque marca presenti nella vostra azienda. Xerox® Device Manager è un singolo strumento che consente di installare code di stampa e di configurare, gestire, monitorare e creare report su dispositivi collegati sia in rete che localmente – indipendentemente dal fornitore – a livello di tutta l'azienda. Le funzioni includono individuazione, configurazione e gestione dei dispositivi, monitoraggio e visualizzazione dei lavori, monitoraggio proattivo, diagnostica remota, risoluzione dei problemi e creazione di report.



Trellix[1] ePolicy Orchestrator®

Questo software consente agli amministratori IT di unificare la gestione della sicurezza su endpoint, reti, dati e soluzioni di conformità di Trellix[1] e soluzioni di terze parti.

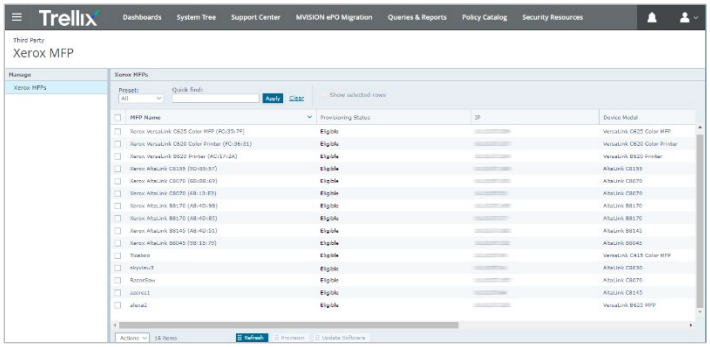
Trellix[1] ePolicy Orchestrator (ePO) è un software di gestione della sicurezza acquistabile che rende più semplice la gestione dei rischi e della conformità per aziende di ogni dimensione. Presenta agli utenti dei dashboard con interfaccia drag-and-drop che forniscono informazioni sulla sicurezza su tutti gli endpoint (dati, dispositivi mobili e reti) per ottenere insight immediati e tempi di risposta più rapidi. Trellix[1] ePO ottimizza le infrastrutture IT esistenti collegando la gestione delle soluzioni di sicurezza Trellix[1] e di terze parti al Protocollo LDAP (Lightweight Directory Access Protocol), alle operazioni IT e agli strumenti di gestione della configurazione.

[1]Trellix, azienda precedentemente nota come McAfee Enterprise

Con visibilità end-to-end e potenti strumenti di automazione che riducono significativamente i tempi di risposta agli eventi imprevisti, il software Trellix[1] ePO migliora la protezione dei dispositivi integrati e riduce i costi e la complessità della gestione dei rischi e della sicurezza.

Il software Trellix[1] ePO fornisce funzionalità di reporting complete per l'esecuzione di query preconfigurate e query personalizzate su informazioni riguardo ai prodotti gestiti sulla vostra rete o alle azioni degli utenti sul vostro server ePO.

I risultati dei report possono essere visualizzati in diversi formati, quali tabelle o grafici a torta, ed esportati per creare report PDF.

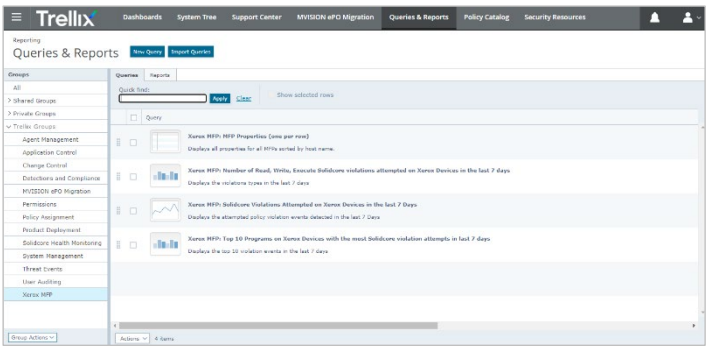


TRELLIX[1] EPOLICY ORCHESTRATOR® ED ESTENSIONE EPO PER STAMPANTE MULTIFUNZIONE XEROX®[2]

Trellix[1] ePO è venduto direttamente da Trellix[1] e non fa parte dei controlli integrati nell'installazione. Tuttavia, se siete già cliente Trellix[1] potreste già star utilizzando Trellix[1] ePO. In tal caso, potete approfittare dell'Estensione ePO per stampante multifunzione Xerox®, che consente di visualizzare i dispositivi Xerox® idonei e le disposizioni per ricevere eventi di sicurezza. Visualizzate fino a 60 attributi per una migliore gestione e informazioni più dettagliate sulle configurazioni di sicurezza.

Inoltre, l'Estensione ePO per stampante multifunzione Xerox® fornisce:

- Una risposta automatizzata per consentire agli amministratori di ricevere notifiche e-mail automatiche
- Una vista di circa 60 attributi di configurazione della sicurezza e delle loro impostazioni correnti
- La possibilità di vedere se il firmware del dispositivo è aggiornato
- La possibilità di caricare firmware del dispositivo in ePO e, successivamente, di aggiornare uno o più dispositivi Xerox®
- Vista in tempo reale di quali porte di ascolto sono attive sul dispositivo Xerox®
- Vista delle porte di ascolto non consentite
- Vista di un evento di sicurezza dei dispositivi Xerox® nel dashboard fornito
- Utilizzo di query e report forniti da Xerox
- Personalizzazione di query o report per eseguire rapidamente controlli sulla conformità della sicurezza sull'intera gamma di servizi



[1]Trellix, azienda precedentemente nota come McAfee Enterprise

[2]Dispositivi Xerox® AltaLink®, Xerox® WorkCentre® iSeries e Xerox® serie EC7800/8000

DISPOSITIVI SUPPORTATI

Trellix[1] Embedded Control Control è disponibile per dispositivi Xerox® AltaLink®, Xerox® VersaLink® serie 7100, WorkCentre® iSeries e serie EC7800 e 8000. Ulteriori prodotti verranno aggiunti in futuro.

RISORSE AGGIUNTIVE

- Xerox e Trellix[1] – Sicurezza dei dati
  https://www.xerox.it/it-it/connectkey/approfondimenti/sicurezza-trellix
- Xerox e Trellix[1] – Domande frequenti
  https://www.xerox.it/ufficio/latest/SECFS-14I.pdf
- Xerox, Trellix[1] e Cisco®: unione di forze per una risposta in tempo reale alle minacce informatiche
  https://www.xerox.it/it-it/connectkey/approfondimenti/sicurezza-della-stampante-di-rete
- Trellix[1] Embedded Control – Scheda tecnica
  https://www.trellix.com/en-us/assets/data-sheets/trellix-embedded-control-datasheet.pdf
- Sicurezza Zero Trust
  https://www.xerox.it/it-it/su-di-noi/soluzioni-di-sicurezza/sicurezza-zero-trust
- Soluzioni per la sicurezza Xerox
  https://www.xerox.it/it-it/su-di-noi/soluzioni-di-sicurezza

[1]Trellix, azienda precedentemente nota come McAfee Enterprise

AUTORI

- Zia Masoom, Worldwide Product Marketing Manager, Xerox
- Doug Tallinger, Worldwide Platform Planning Manager, Xerox

Per ulteriori informazioni sui prodotti Xerox® con Trellix[1] Embedded Control, contattare un rappresentante Xerox o visitare **www.xerox.it/it-it/connectkey/approfondimenti/sicurezza-trellix**.