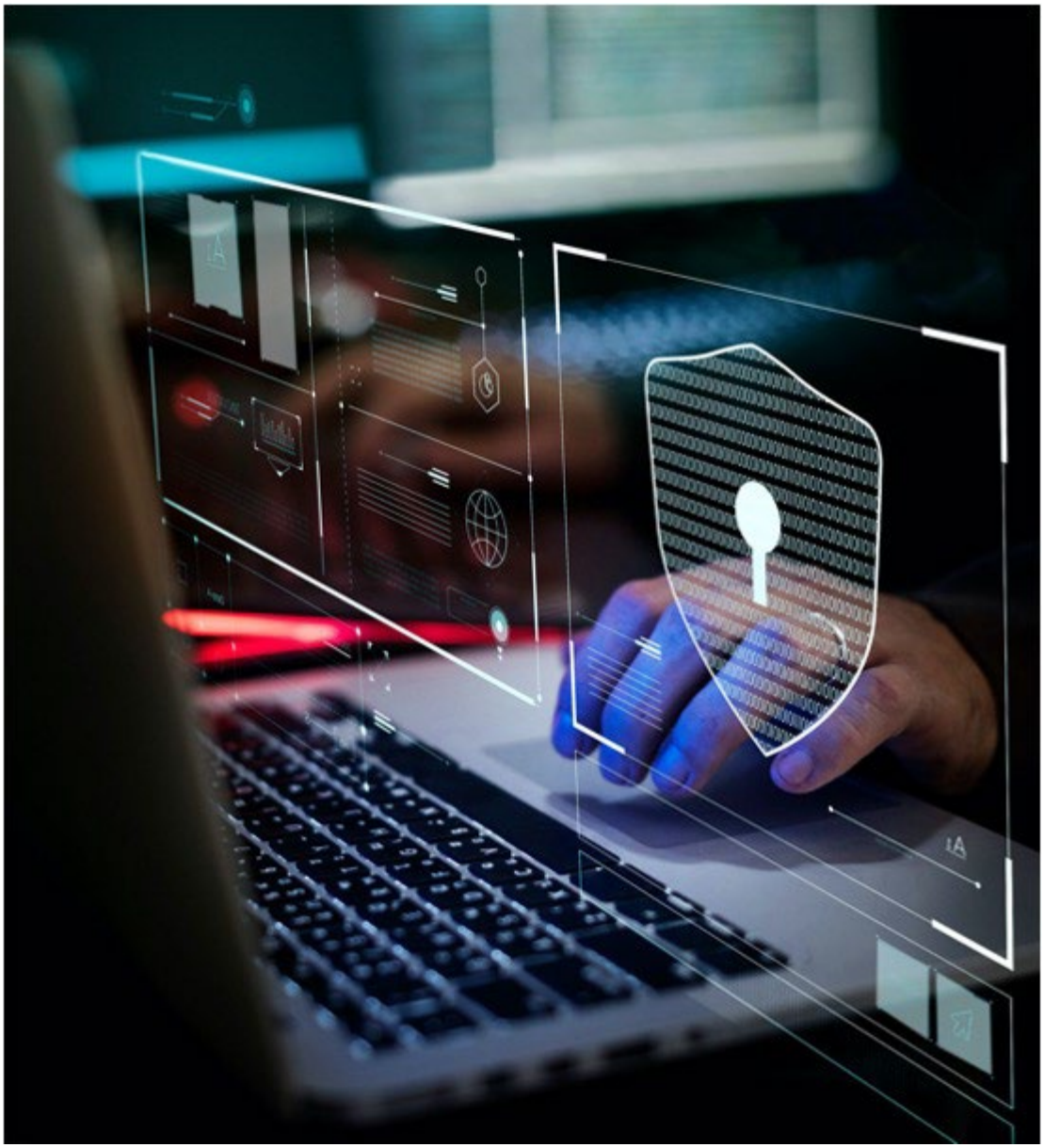


Sicherheit der nächsten Generation von Xerox: Partnerschaft mit Trellix[1]

Whitepaper

[1]Trellix, ehemals McAfee Enterprise Business

xerox™

Hintergrund

Die heutigen Multifunktionsdrucker sind komplexe, integrierte Systeme. Sie enthalten unter anderem vollwertige Betriebssysteme und integrierte Webserver, Support für mehrere Protokoll-Stacks, externe Hardware- und Softwareschnittstellen sowie Anwendungsprogrammierschnittstellen (Application Programming Interfaces, APIs) für die Interaktion mit Unternehmenssystemen. Aufgrund des großen Funktions- und Leistungsumfangs dieser Multifunktionsdrucker stellen sie möglicherweise ein ernsthaftes Risiko für Ihre Netzwerk- und Unternehmenssysteme dar, wenn sie nicht angemessen geschützt sind.

Anbieter von Multifunktionsdruckern haben ihre technischen Anstrengungen zur Verschärfung der Sicherheitskontrollen bei diesen Geräten durch die Einführung besserer Schutzmaßnahmen und -vorkehrungen erheblich verstärkt, z. B. durch:

- Festplattenverschlüsselung und Festplattenüberschreibung zum Schutz von Endbenutzerdaten
- Aktivierung verschlüsselter Protokolle wie Transport Layer Security (TLS), Internet Protocol Security (IPsec) und Simple Network Management Protocol Version 3 (SNMPv3) zum Schutz der an das und von dem Gerät übermittelten Daten
- Benutzerauthentifizierung für die meisten Aufgaben
- Zugriffskontrolle durch Hinzufügen von Firewalls und Rollen auf Basis von Active Directory (AD)-Gruppen
- Überwachungsprotokolle zur Gewährleistung der Rückverfolgbarkeit
- Programme zur Sicherheitsbeurteilung wie Zertifizierung nach den Common Criteria

Sind die Multifunktionsdrucker integrierte oder offene Systeme? Brauchen diese Geräte eine zusätzliche Sicherheitsebene? Falls ja, was ist die richtige Lösung zum Schutz von Servern, Desktops und Netzwerken vor aktuellen und zukünftigen Bedrohungen? Diese Frage versuchen Experten in Sicherheits-Communities ständig zu beantworten.

Wir wissen, dass traditionelle Sicherheitstechnologien, etwa die Antivirus-Technologie, gegen die Vielzahl von Bedrohungen von heute wie Advanced Persistent Threats (APT) und Botnets nur begrenzt wirksam sind.

Die Realität ist doch, dass es trotz des zusätzlichen Schutzes durch die Anbieter von Multifunktionsdruckern weiterhin Sicherheitsvorfälle gibt. Und all diesen Sicherheitsvorfällen ist gemeinsam, dass Kunden sie erst erkennen, wenn die Sicherheitsverletzung stattgefunden hat. Anbieter und Kunde versuchen dann, den Schaden zu begrenzen, die Schwachstelle kurzfristig zu schließen und eine Lösung bereitzustellen. Diese Vorgehensweise könnte man mit der Bewertung des Sachschadens und der Durchführung der Reparaturarbeiten nach der Sprengung eines Geldautomaten und dem Raub des darin befindlichen Bargelds vergleichen.

[1]Trellix, ehemals McAfee Enterprise Business

INTEGRIERTE GERÄTE

Ein integriertes System ist ein speziell für feste Funktionen konzipiertes Computersystem. Integrierte Systeme decken alle Aspekte des modernen Lebens ab – Geldautomaten, medizinische Geräte, Drucker, Kassenterminals, Kioske usw.

Moderne Multifunktionsgeräte haben jedoch nicht mehr nur eine einzige, feste Funktion. Sie sind hybride Systeme, die zwischen einem Gerät mit fester Funktion und einem Server in einem IT-Netzwerk angesiedelt sind. Beide verfügen über Festplatten, Betriebssysteme, Webserver, mehrere Eingangs- und Ausgangsverbindungen sowie Schnittstellen und verarbeiten verschiedene Arten von Informationen. Brauchen diese Geräte eine zusätzliche Sicherheitsebene? Was ist die richtige Lösung, die Server, Desktops und Netzwerke vor aktuellen und zukünftigen Bedrohungen schützen kann? Diese Frage versuchen Experten in Sicherheits-Communities ständig zu beantworten.

Wir wissen, dass traditionelle Sicherheitstechnologien wie Antivirus-Software nicht in der Lage sind, die heutigen Bedrohungen wie Advanced Persistent Threats (APT) und Botnets zu bekämpfen. Experten sind weitgehend der Meinung, dass die Whitelisting-/Allowlisting-Technologie die Antwort auf diese Bedrohungen sein könnte.

Schauen wir uns daher zunächst an, was genau Whitelists/Allowlists sowie Blacklists/Blocklists sind.

BLACKLISTS/BLOCKLISTS

Im Kampf gegen unberechtigten Zugriff, Missbrauch von Informationen und Malware setzen IT-Sicherheitsadministratoren in der Regel auf Tools wie Antivirus- und Anti-Malware-Software sowie die Überwachung des Netzwerkzugriffs und Content Monitoring. Die meisten Tools können einem dieser beiden Modelle zugeordnet werden: Blacklists/Blocklists und Whitelists/Allowlists.

Eine Antivirus-Software arbeitet mit den Hash-Werten bekannter Malware. Sobald eine bestimmte Variante eines Virus isoliert ist, wird ihr Hash-Wert zur Blacklist/Blocklist hinzugefügt. Diese Listen liegen als .dat-Dateien vor, die täglich heruntergeladen werden müssen. Das Problem dabei ist, dass die Anbieter von Antivirus-Software durchschnittlich vier Tage brauchen, um das Virus zu isolieren und ein Update für die .dat-Dateien zu veröffentlichen. In dieser Zeit ist jeder Computer, dessen einziger Schutz eine Antivirus-Software ist, ungeschützt und gefährdet.

Der größte Nachteil ist jedoch, dass neue Bedrohungen dieser Methode immer einen Schritt voraus sind. Vor allem jedoch sind Tools, die auf Blacklisting/Blocklisting basieren, bei Ereignissen wie Zero-Day-Angriffen völlig ineffektiv.

Zero-Day-Angriffe

Ein Zero-Day-Angriff nutzt Schwachstellen bei Geräten, die aktuell nicht geschlossen werden können. Derzeit ist es meistens so: Wenn ein Softwareunternehmen nach der Veröffentlichung einer Software einen Fehler oder ein Problem entdeckt, entwickelt es einen Patch zur Behebung des Problems und stellt diesen der Nutzer-Community bereit. Ein Zero-Day-Angriff nutzt das Problem aus, noch bevor ein Patch erstellt wird. Durch das Aufdecken dieser Schwachstellen, bevor die Software-Entwickler sie finden, kann ein Programmierer ein Virus oder einen Wurm erzeugen, der die Schwachstellen ausnutzt und ein System auf unterschiedliche Weise schädigt.

[1]Trellix, ehemals McAfee Enterprise Business

WHITELISTING/ALLOWLISTING

Der Whitelisting-/Allowlisting-Ansatz basiert im Wesentlichen auf der Identifizierung von Dateien für eine IT-Umgebung, wobei dann nur diese Dateien auf dem System ausgeführt werden können. Es wird im Wesentlichen nur das erlaubt, was erwiesenermaßen unbedenklich ist; alles andere, was unbekannt ist, wird unterbunden. Grundsätzlich gilt: Wenn ein Softwareprogramm nicht explizit zur Whitelist/Allowlist hinzugefügt wurde, wird die Ausführung verweigert. Viele der heute genutzten Überwachungstools fallen unter Whitelisting/Allowlisting, da sie „nur bestimmten Benutzern, bestimmten IP-Adressen oder vordefinierten Dienstarten erlauben", das System zu durchlaufen oder dort ausgeführt zu werden. So können Sie sicher sein, dass eine Botnet-Armee Ihre Multifunktionsdrucker nicht für die Durchführung von Angriffen rekrutieren kann!

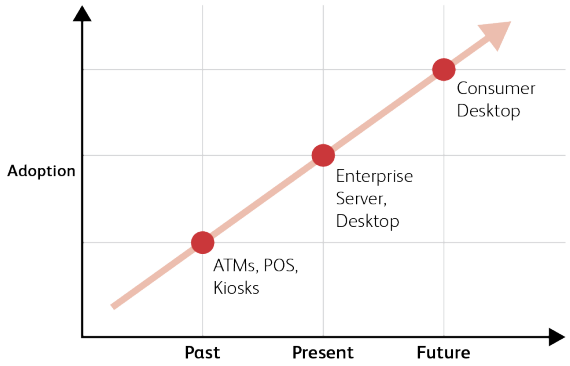
Botnets umfassen bekanntermaßen Tausende von infizierten Computern. Ein Botnet ist ein Netzwerk von durch Malware infizierten Computern, wobei die einzelnen Computer dem zentralen Befehl und der Kontrolle eines Botmasters unterliegen, d. h. quasi versklavt sind. Jeder infizierte Computer wird Zombie oder Zombie-Computer genannt. Die Botnet-Malware befindet sich auf dem infizierten Computer, oft ohne dass der Besitzer des Computers davon weiß oder die Malware den Betrieb des Computers beeinträchtigt. Der Botmaster verkauft die Dienste des Botnets an einen Kunden, damit dieser per E-Mail Spam-Werbung verbreiten oder einen DDOS-Angriff (Distributed Denial of Service) veranlassen kann. Beim einem DDOS-Angriff versuchen alle Zombies, gleichzeitig auf eine bestimmte Website zuzugreifen, sie mit Datenverkehr zu überlasten und so einen kompletten Ausfall herbeizuführen. Denken Sie beispielsweise an Angriffe von „Anonymous" auf eine Regierungs-Website oder Medien-Website, die ihnen nicht gefällt. Die Software Trellix[1] Embedded Control in Xerox®-Geräten würde verhindern, dass die infizierende Malware überhaupt einen Brückenkopf auf dem Gerät bildet, und schützt so das Gerät vor der Aufnahme in das Botnet.

Das Whitelisting/Allowlisting funktioniert auf einem Desktop-Computer ganz anders als bei einem integrierten System. Auf einen Universalcomputer kann der Benutzer – möglicherweise völlig legitim – jede beliebige Software laden. Die Whitelisting-/Allowlisting-Desktop-Software muss den Benutzer dann fragen, ob die neue Software zugelassen werden soll. Im Gegensatz dazu weiß der Softwareentwickler bei einem integrierten System genau, was auf dem betreffenden System ausgeführt werden darf, und kann alles andere blockieren.

Mithilfe einer Whitelist/Allowlist legen wir fest, was geschehen darf und was nicht. Zum Chaos kommt es, wenn etwas, das nicht geschehen sollte, möglich ist, z. B. dass eine Adobe® Flash® Player-Anwendung auf ein Kernsystem zugreift. Mit der Whitelisting-/Allowlisting-Technologie lässt sich verhindern, dass eine ansonsten autorisierte Anwendung auf Kerndateien zugreifen kann, für die sie nicht zugriffsberechtigt sein sollte.

Akzeptanz der Whitelisting-/Allowlisting-Methode

Es besteht ein allgemeiner Konsens darüber, dass die Whitelisting-/Allowlisting-Technologie eine effektive Möglichkeit ist, Zero-Day-Bedrohungen abzuwehren.



WIE KANN XEROX SIE UNTERSTÜTZEN?

Was ist also der nächste Schritt bei der Realisierung einer Sicherheitslösung zur Abwehr von Angriffen auf Ihr Netzwerk über Multifunktionsdrucker? Xerox war schon immer tonangebend, wenn es darum ging, Drucker und Multifunktionsdrucker mit Sicherheitsfunktionen auszustatten.

Angesichts des Nachdrucks, mit dem Xerox sich dem Thema Sicherheit widmet, ist es nur konsequent, dass wir mit Trellix[1] partnerschaftlich zusammenarbeiten, um den zunehmenden Bedrohungen durch integrierte Systeme immer einen Schritt voraus zu sein. Gemeinsam haben wir die Selbstüberwachung und den Selbstschutz integriert, den jede einzelne Einheit zum Schutz vor böswilligen Angriffen braucht. Darüber hinaus kann der Trellix[1]-Agent, der im Gerät ausgeführt wird, direkt mit der zentralen Sicherheitsmanagement-Konsole – Trellix[1] ePolicy Orchestrator – kommunizieren, um die Verwaltung von Druckern und Multifunktionsdruckern auf die gleiche Weise zu ermöglichen, wie Kunden ihre Desktops verwalten.

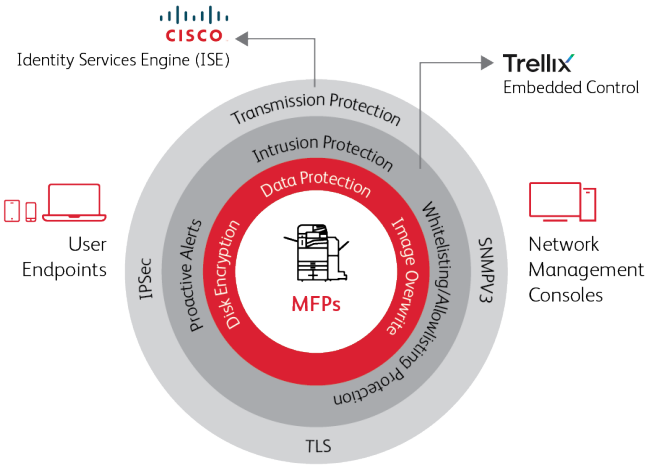
Die auf jedem bereitgestellten Multifunktionsdrucker generierten Trellix[1]-Sicherheitsereignisse werden an den konfigurierten Trellix[1] ePolicy Orchestrator übermittelt. Das erleichtert die Überwachung aller bereitgestellten Multifunktionsdrucker durch Trellix[1] ePolicy Orchestrator.

Im Folgenden erfahren wir, womit Trellix[1] die bestmögliche Sicherheit für Xerox®-Multifunktionsdrucker gewährleistet.

[1]Trellix, ehemals McAfee Enterprise Business

TRELLIX[1] EMBEDDED CONTROL-TECHNOLOGIE

Dank der Trellix[1] Embedded Control-Technologie auf Xerox®-Geräten können Kunden jeder Größe – von kleinen bis mittleren Unternehmen (KMU) mit begrenzten IT-Ressourcen bis hin zu globalen Unternehmen – sich darauf verlassen, dass ihre Multifunktionsdrucker sofort nach dem Auspacken sicher sind.



Trellix[1] Embedded Control nutzt die Whitelisting-/Allowlisting-Technologie, um Ihre Xerox®-Geräte vor Angriffen zu schützen. Kritische Systeme werden gesperrt und unbefugte Änderungen verhindert. Nur Programme auf der von Xerox erstellten Whitelist/Allowlist können ausgeführt werden. Die Ausführung anderer Programme, etwa von .exe- und .dll. Dateien sowie Skripten, ist nicht zulässig. Versuche, in eine schreibgeschützte Datei zu schreiben oder Inhalte aus lesegeschützten Dateien oder Verzeichnissen zu lesen, werden verhindert. Zudem wird ein Ereignis generiert und in das Überwachungsprotokoll des Geräts aufgenommen. Ist SIEM konfiguriert (nativ auf Geräten der AltaLink® 8100 Serie oder über Xerox® Device Manager bei VersaLink®-Geräten), werden alle im Überwachungsprotokoll festgehaltenen Ereignisse zur Off-Box-Protokollierung und -Analyse an einen SIEM-Server weitergeleitet. Sind auf dem Xerox®-Gerät außerdem E-Mail-Benachrichtigungen konfiguriert, wird eine E-Mail mit den Einzelheiten des Ereignisses an die angegebene Adresse gesendet.

Das Konzept von Whitelisting/Allowlisting ist ganz einfach – Xerox erstellt eine vordefinierte, abgeschlossene Liste vertrauenswürdiger Anwendungen und nur diese Anwendungen können ausgeführt werden. Diese Lösung ist ideal für integrierte Geräte mit fester Funktion. Die gleiche Technologie wird auch bei Geldautomaten eingesetzt.

Typische Funktionen wie Drucken, Kopieren, Scannen und Faxen sind Teil einer Whitelist/Allowlist mit vertrauenswürdigen Anwendungen. Verwaltungsaufgaben wie Firmware-Updates, Software-Upgrades, das Laden von Formularen und Schriftarten, Änderungen von Konfigurationsattributen und Diagnosen durch Xerox-Techniker gelten ebenfalls als vertrauenswürdige Vorgänge.

Die Trellix[1]-Software soll Angriffe verhindern, mit denen versucht wird, die vorhandene Software des Geräts zu beschädigen oder nicht autorisierte Malware zu installieren. In der Sicherheitssprache werden diese Angriffe als „Code-Injektion" oder „Remote-Code-Ausführung" bezeichnet. Im Gegensatz zu anderer Software, die regelmäßig Scanvorgänge durchführt, um die Integrität der Betriebssystemdateien zu überprüfen, wird jeder Lese-, Schreib- und Ausführungsversuch in Echtzeit überprüft. Außerdem läuft die Trellix[1] Embedded Control-Software „unterhalb" des Betriebssystems, sodass alles, z. B. ein Root-Kit, das versucht, auf dieser Ebene eine Infektion auszulösen, erkannt wird.

Diese Technologie bietet bei der Bedrohungsabwehr folgende Vorteile:

- Kein Notfall-Patching mehr
- Weniger und seltenere Patching-Zyklen
- Geringeres Sicherheitsrisiko durch Zero-Day- und polymorphe Angriffe über Malware wie Würmer, Viren, Trojaner und Code-Injektionen, z. B. Pufferüberlauf, Heap-Überlauf und Stapelüberlauf
- Vertrauen in die Integrität autorisierter Dateien, die gewährleisten, dass sich das System in einem bekannten und verifizierten Zustand befindet
- Senkung der durch ungeplante Ausfallzeiten für Wiederherstellungen verursachten Betriebskosten
- Erhöhung der Systemverfügbarkeit

Trellix[1] Embedded Control erkennt Änderungsversuche in Echtzeit. Dazu gehören Versuche, den Systemstatus einschließlich Code, Konfiguration und Registrierung zu ändern. Alle Änderungsereignisse werden bei ihrem Auftreten protokolliert und an den System-Controller gesendet.

TRELLIX[1] ENHANCED SECURITY

Trellix[1] Enhanced Security – Standard bei neueren Multifunktionsdruckern – ist standardmäßig installiert und aktiviert. Diese Software verhindert allgemeine Angriffe wie unbefugten Lese-/Schreibzugriff auf geschützte Dateien und Verzeichnisse und ergänzt bestimmte geschützte Verzeichnisse. Das gewährleistet die Integrität des Multifunktionsdruckers, da nur autorisierter Code ausgeführt sowie autorisierte Änderungen vorgenommen werden können. Wurden die Grundeinstellungen vorgenommen, wird der Administrator per E-Mail benachrichtigt, wenn versucht wird, die Systemanwendungen, die das Gerät steuern, zu ändern. Darüber hinaus werden diese Versuche in den Überwachungsprotokollen aufgezeichnet und können je nach Einrichtung des Kunden über die Xerox® CentreWare® Web Software oder den Xerox® Device Manager und, sofern in der Umgebung vorhanden, Trellix[1] ePolicy Orchestrator® (ePO) gemeldet werden. Wenn SIEM konfiguriert ist (nativ auf Geräten der AltaLink 8100 Serie oder über Xerox Device Manager bei VersaLink-Geräten), werden alle im Überwachungsprotokoll festgehaltenen Ereignisse zur Off-Box-Protokollierung und -Analyse an einen SIEM-Server weitergeleitet.

Updates der Whitelist/Allowlist werden von Xerox bereitgestellt – jedoch nur dann, wenn die integrierte Software aktualisiert wird. Bestimmte Funktionen der Software sind von vornherein vertrauenswürdig, so auch der Prozess der Softwareaktualisierung. Die Xerox®-Software wird digital signiert, um ihre Integrität und Authentizität zu garantieren. Ist die Signatur gültig, wird die neue Software mit einer neuen Whitelist/Allowlist installiert.

Unabhängig von Ihrem Sicherheitsanbieter profitieren Sie trotzdem von den integrierten Sicherheitsfunktionen von Xerox und Trellix[1], ohne dass zusätzliche Software erforderlich ist. Die Whitelisting-/Allowlisting-Funktion ist unabhängig von externer Software und so konzipiert, dass sie ohne Herabsetzung der Systemleistung ausgeführt wird.

[1]Trellix, ehemals McAfee Enterprise Business

Trellix[1] Enhanced Security wurde mit dem Ziel entwickelt, die Probleme zu lösen, die durch mit dem Einsatz kommerzieller Betriebssysteme in integrierten Systemen einhergehende erhöhte Sicherheitsrisiken verursacht werden. Diese kompakte und kostengünstige anwendungsunabhängige Lösung bietet die wartungsfreie Sicherheit, die Sie brauchen.

Sie fragen sich vielleicht, wie neue Software auf dem Gerät installiert wird, da die Whitelist/Allowlist nur bekannte Software zulässt. Alle autorisierten Softwareprogramme werden durch Xerox digital signiert. Während der Softwareinstallation wird die digitale Signatur geprüft, bevor der Installationsprozess fortgesetzt wird. Ist die Signatur gültig, wird Trellix[1] Enhanced Security dahin gehend informiert, dass die neue Software sicher installiert werden kann. Da Xerox während der Entwicklung das Paket der zulässigen Software definiert, wird jedes Softwarepaket mit der zugehörigen Whitelist/Allowlist bereitgestellt. Nach der Softwareinstallation ermittelt Trellix[1] Enhanced Security anhand der neuen Whitelist/Allowlist, was zulässig ist.

Meldung von Bedrohungswarnungen

Bedrohungswarnungen können je nach Konfiguration auf verschiedene Arten kommuniziert werden:

- **Überwachungsprotokoll** – auf der Bedienungsoberfläche des Multifunktionsdruckers generiert, standardmäßig aktiviert
- Ist SIEM konfiguriert (nativ auf Geräten der AltaLink® 8100 Serie oder über Xerox® Device Manager bei VersaLink®-Geräten), werden alle im Überwachungsprotokoll festgehaltenen Ereignisse zur Off-Box-Protokollierung und -Analyse an einen SIEM-Server weitergeleitet
- **E-Mail-Warnung vom Gerät** – konfiguriert über die Bedienungsoberfläche von Xerox® CentreWare® Internet Services
- **E-Mail-Warnungen und -Berichte über Xerox® CentreWare Web Software und Xerox® Device Manager** – konfiguriert über die Bedienungsoberflächen der Xerox® CentreWare® Web Software und des Xerox® Device Manager
- **E-Mail-Warnungen und -Berichte über Trellix[1] ePolicy Orchestrator** – konfiguriert über die Sicherheitsmanagement-Software Trellix[1] ePolicy Orchestrator von Trellix[1]
- Die auf jedem bereitgestellten Multifunktionsdrucker generierten Trellix[1]-Sicherheitsereignisse werden an den konfigurierten Trellix[1] ePolicy Orchestrator übermittelt. Das erleichtert die Überwachung aller bereitgestellten Multifunktionsdrucker durch Trellix[1] ePolicy Orchestrator.

TRELLIX[1] INTEGRITY CONTROL

Trellix[1] Integrity Control ist eine optional käufliche Software, die die standardmäßigen Funktionen von Enhanced Security mit der Fähigkeit verbindet, potenzielle Gefahrenquellen zu erkennen und zu blockieren. Dazu gehören zielgerichtete Angriffe sowie Dateien, die von beliebigen Standorten aus ohne Genehmigung mithilfe nicht vertrauenswürdiger Methoden ausgeführt werden. Verhindert wird auch die Erstellung geschützter ausführbarer Dateien, die nicht zur standardmäßigen Xerox®-Gerätesoftware gehören. Das ist das höchste Sicherheitsniveau und der maximale Schutz, den Sie für Ihren Multifunktionsdrucker von Xerox® erhalten können.

Trellix[1] Integrity Control bietet eine zusätzliche Sicherheitsebene, denn die Software verhindert die Ausführung neuer Dateien aus jeder nicht vertrauenswürdigen Quelle. Auch das Speichern geschützter ausführbarer Dateien wird verhindert. So werden Programmdateien von Xerox vor böswilliger Überschreibung bewahrt. Nicht autorisierter Code oder unbefugte Änderungen durch Malware, Würmer, Trojaner, Zero-Day-Angriffe und sogar gezielte Angriffe werden gestoppt. Um Angriffe abzuwehren, für die es noch keine Gegenmaßnahme gibt, darf nur zugelassene Software ausgeführt werden.

Xerox und Trellix[1] bieten Whitelisting-/Allowlisting-Technologie, die sicherstellt, dass auf geschützten Systemen nur unbedenklicher, ausführbarer Code ausgeführt werden kann. Diese Technologie gewährleistet, dass Ihre Geräte nur die Dienste ausführen, die Sie bereitstellen möchten, und verhindert gleichzeitig, dass ein Angreifer bösartigen Code installiert. Die gleiche Technologie wird zum Schutz von Servern, Geldautomaten, Kassenterminals und integrierten Geräten wie Drucker und Mobilgeräte eingesetzt.

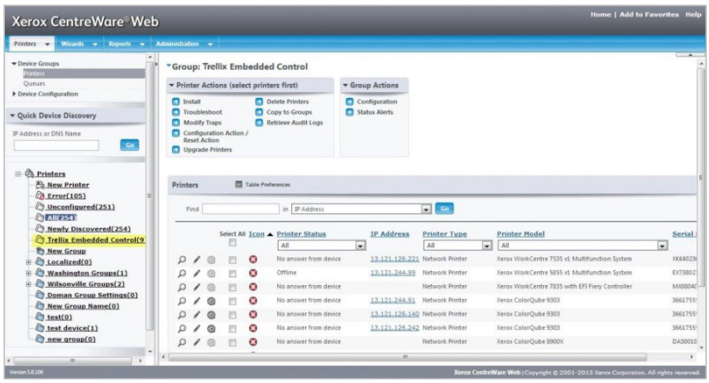
Wie bereits erwähnt, wird Trellix[1] Enhanced Security bei bestimmten Modellen als vollständig installierte und aktivierte Standardfunktion angeboten. Beim optionalen Tool Trellix[1] Integrity Control brauchen die Kunden kein Installationsverfahren durchzuführen und die Aktivierung basiert auf einem Lizenzierungsschlüsselverfahren.

VERWALTEN VON TRELLIX[1] EMBEDDED CONTROL-GERÄTEN

Für die Verwaltung von Trellix[1] Embedded Control-Geräten gibt es mehrere Optionen:

Xerox® CentreWare® Web Software und Xerox® Device Manager

Xerox® CentreWare® Web Software ist ein innovatives, browser-basiertes Software-Tool, das unabhängig vom Hersteller die Installation, Konfiguration, Verwaltung und Überwachung vernetzter Drucker und Multifunktionsgeräte sowie die Erstellung entsprechender Berichte im Unternehmen übernimmt. Mit Xerox® Device Manager lassen sich sowohl Druckwarteschlangen im gesamten Unternehmen installieren als auch vernetzte oder lokal verbundene Geräte beliebiger Hersteller konfigurieren, verwalten, überwachen und Berichte dazu erstellen. Unterstützt werden Funktionen wie Geräteerkennung, Konfiguration und Verwaltung, Auftragsverfolgung und -visualisierung, proaktive Überwachung, Diagnose und Fehlerbehebung aus der Ferne sowie die Erstellung von Berichten.



Trellix[1] ePolicy Orchestrator®

Mit dieser Software können IT-Administratoren das Sicherheitsmanagement für Endgeräte, Netzwerke, Daten und Compliance-Lösungen von Trellix[1] und Drittanbieterlösungen vereinheitlichen.

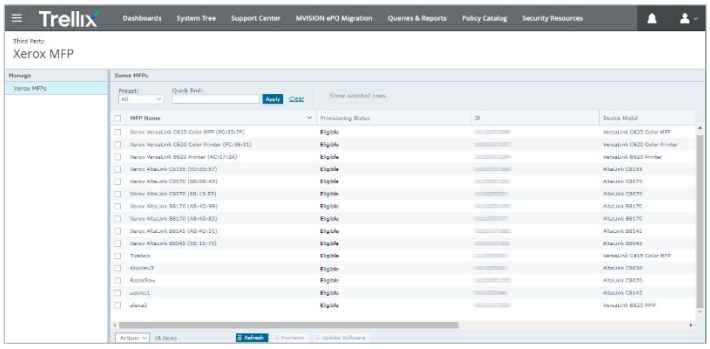
Trellix[1] ePolicy Orchestrator (ePO) ist ein käuflich erwerbbares Sicherheitsmanagement-Tool, das das Risiko- und Compliance-Management für Unternehmen jeder Größe vereinfacht. Über Drag-and-drop-Dashboards werden den Benutzern Sicherheitsinformationen für Endgeräte, Daten, Mobilgeräte und Netzwerke bereitgestellt, um sofortige Erkenntnisse zu erhalten und die Reaktionszeiten zu verkürzen. Trellix[1] ePO nutzt vorhandene IT-Infrastrukturen, indem das Management der Sicherheitslösungen von Trellix[1] und Drittanbietern mit dem LDAP-Protokoll (Lightweight Directory Access Protocol) (LDAP), IT-Prozessen und Konfigurationsmanagement-Tools verbunden wird.

[1]Trellix, ehemals McAfee Enterprise Business

Mit durchgängiger Transparenz und leistungsstarken Automatisierungen, die die Antwortzeiten bei Vorfällen erheblich reduzieren, verbessert die Trellix[1] ePO-Software den Schutz für integrierte Geräte und senkt die Kosten und Komplexität des Risiko- und Sicherheitsmanagements.

Die Trellix[1] ePO-Software bietet umfassende Berichtfunktionen für vorkonfigurierte und kundenspezifische Abfragen von Informationen zu verwalteten Produkten in Ihrem Netzwerk oder Benutzeraktionen auf Ihrem ePO-Server.

Berichtergebnisse können in verschiedenen Formaten, z. B. in Tabellen oder Tortendiagrammen angezeigt und zur Erstellung von PDF-Berichten exportiert werden.

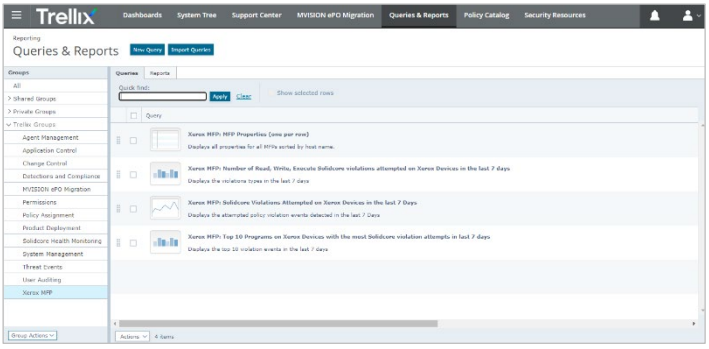


TRELLIX[1] EPOLICY ORCHESTRATOR® UND XEROX® EPO-ERWEITERUNG FÜR MULTIFUNKTIONSDRUCKER[2]

Trellix[1] ePO wird direkt von Trellix[1] verkauft und ist nicht Teil der Installation von Embedded Control. Wenn Sie bereits Trellix[1]-Kunde sind, nutzen Sie Trellix[1] ePO vielleicht schon. Dann können Sie von der ePO-Erweiterung für Xerox®-Multifunktionsdrucker profitieren, die berechtigte Xerox®-Geräte und die Voraussetzungen für den Empfang von Benachrichtigungen zu Sicherheitsereignissen angibt. Bis zu 60 Attribute für besseres Management und detailliertere Informationen zu Sicherheitskonfigurationen können angezeigt werden.

Darüber hinaus bietet die ePO-Erweiterung für den Xerox®-Multifunktionsdrucker Folgendes:

- Eine automatisierte Reaktion, damit Administratoren automatische E-Mail-Benachrichtigungen erhalten
- Eine Anzeige von etwa 60 Attributen zur Sicherheitskonfiguration und deren aktuellen Einstellungen
- Eine Funktion zum Anzeigen, ob die Firmware des Geräts aktuell ist
- Die Möglichkeit, Geräte-Firmware in ePO hochzuladen und anschließend ein oder mehr Xerox®-Geräte zu aktualisieren
- Eine Funktion zur Echtzeit-Anzeige der jeweils auf dem Xerox®-Gerät aktiven Listening-Ports
- Die Anzeige unzulässiger Listening-Ports
- Die Anzeige eines die Sicherheit von Xerox®-Geräten betreffenden Ereignisses auf dem bereitgestellten Dashboard
- Die Nutzung durch Xerox bereitgestellter Abfragen und Berichte
- Die Anpassung von Abfragen oder Berichten zur schnellen Durchführung von Überprüfungen der Sicherheitskonformität bei all Ihren Diensten



[1]Trellix, ehemals McAfee Enterprise Business
[2]Xerox® AltaLink®-Geräte, Geräte der Xerox® WorkCentre® iSeries und Xerox® EC7800/8000 Serie

UNTERSTÜTZTE GERÄTE

Trellix[1] Embedded Control ist verfügbar für Xerox® AltaLink®-Geräte, Geräte der Xerox® VersaLink® 7100 Serie, der WorkCentre® iSeries sowie der EC7800 und 8000 Serie. In Zukunft werden weitere Produkte hinzukommen.

WEITERE RESSOURCEN

- Xerox- und Trellix[1]-Lösungen für Datensicherheit
  https://www.xerox.de/de-de/connectkey/einblicke/trellix-sicherheit
- Häufig gestellte Fragen zur Partnerschaft von Xerox und Trellix[1]
  https://www.xerox.de/office-produkte/latest/SECFS-14G.pdf
- Xerox, Trellix[1] und Cisco®: Bündelung der Kräfte zur Verbesserung der Cybersicherheit in Echtzeit
  https://www.xerox.de/de-de/connectkey/einblicke/netzwerkdrucker-sicherheit
- Datenblatt zu Trellix[1] Embedded Control
  https://www.trellix.com/en-us/assets/data-sheets/trellix-embedded-control-datasheet.pdf
- „Null Vertrauen"-Sicherheit
  https://www.xerox.de/de-de/uber-uns/sicherheitslosungen/zero-trust-sicherheits
- Sicherheitslösungen von Xerox
  https://www.xerox.de/de-de/uber-uns/sicherheitslosungen

[1]Trellix, ehemals McAfee Enterprise Business

AUTOREN

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

Wenn Sie weitere Informationen zu Xerox®-Produkten mit Trellix[1] Embedded Control wünschen, wenden Sie sich bitte an einen Xerox-Partner oder besuchen Sie **www.xerox.de/de-de/connectkey/einblicke/trellix-sicherheit.**