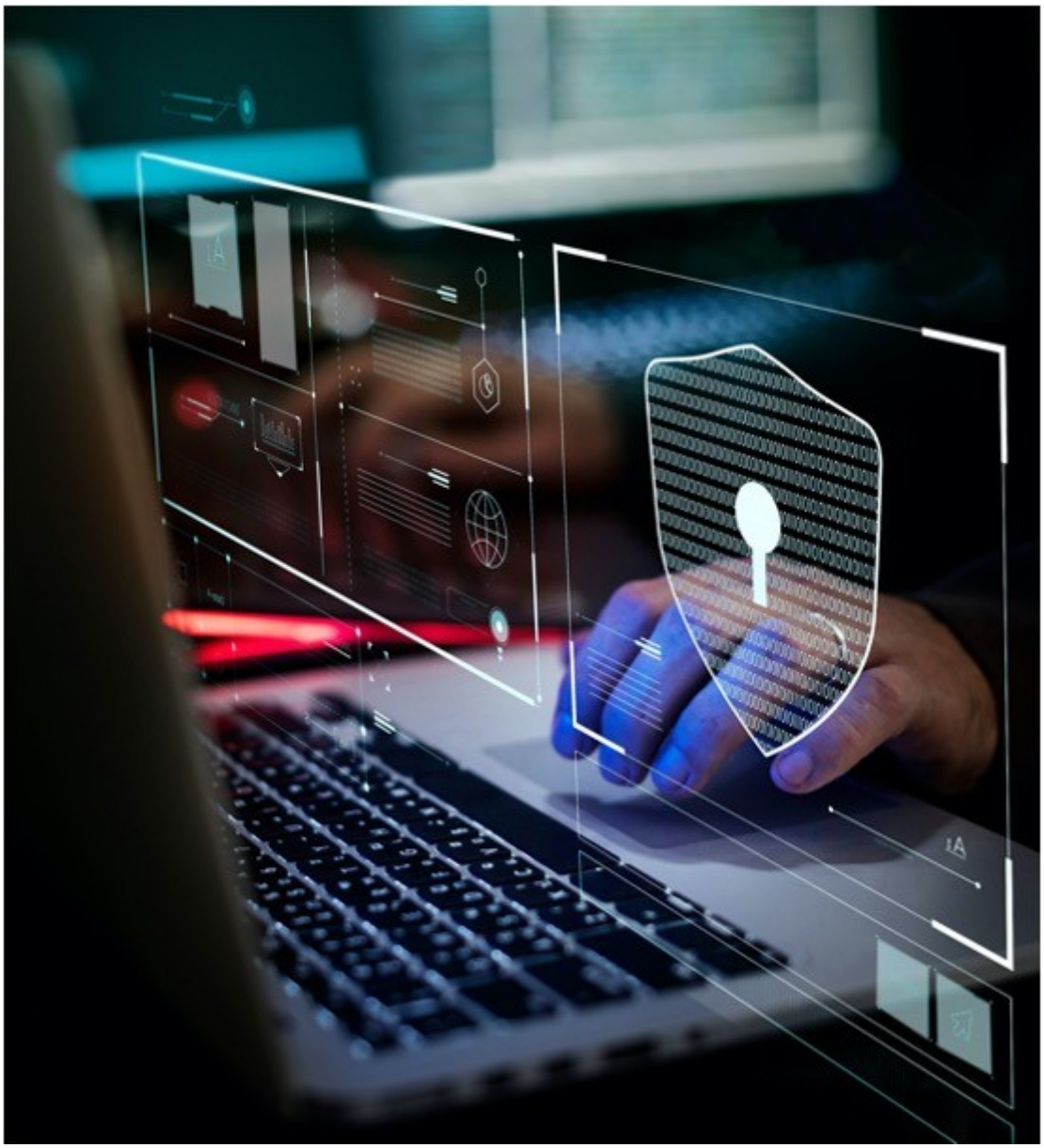


Xerox Sicherheit der nächsten Generation: Partnerschaft mit Trellix1

Weißbuch

[1]Trellix, früher bekannt als McAfee Enterprise Business

Hintergrund

Die heutigen Multifunktionsdrucker (MFP) sind komplexe eingebettete Systeme. Sie enthalten unter anderem vollwertige Betriebssysteme, eingebettete Webserver, Unterstützung für mehrere Protokollstapel, externe Hardware- und Softwareschnittstellen sowie Anwendungsprogrammierschnittstellen (APIs) zur Interaktion mit Unternehmenssystemen. Aufgrund der umfangreichen Funktionen und der Leistungsfähigkeit dieser MFP-Geräte stellen sie potenziell ein ernsthaftes Risiko für Ihr Netzwerk und Ihre Unternehmenssysteme dar, wenn sie nicht angemessen geschützt sind.

Die MFP-Hersteller haben ihre technischen Bemühungen zur Verschärfung der Sicherheitskontrollen in diesen Geräten erheblich verstärkt, indem sie u. a. verbesserte Schutzmaßnahmen eingeführt haben:

- Festplattenverschlüsselung und Festplattenüberschreibung zum Schutz von Endbenutzerdaten
- Ermöglichung von verschlüsselten Protokollen wie Transport Layer Security (TLS), Internet Protocol Security (IPsec) und Simple Network Management Protocol Version 3 (SNMPv3) zum Schutz der Daten, die zum und vom Gerät übertragen werden
- Benutzerauthentifizierung für die meisten Aufgaben
- Zugriffskontrolle durch Hinzufügen von Firewalls und Rollen auf der Grundlage von Active Directory (AD)-Gruppen
- Audit-Protokolle für die Rückverfolgbarkeit
- Sicherheitsbewertungsprogramme wie die Common Criteria-Zertifizierung

Handelt es sich bei den MFPs um eingebettete Systeme oder um offene Systeme? Brauchen diese Geräte eine zusätzliche Sicherheitsebene? Wenn ja, was ist die richtige Lösung für den Schutz von Servern, Desktops und Netzwerken vor aktuellen und zukünftigen Bedrohungen? Diese Frage versuchen die Sicherheitsexperten ständig zu beantworten.

Wir wissen, dass herkömmliche Sicherheitstechnologien, wie z. B. Antivirenprogramme, gegen die heutige Art von Bedrohungen wie Advanced Persistent Threats (APTs) und Botnets nur begrenzt wirksam sind.

Die Realität sieht so aus, dass es trotz des zusätzlichen Schutzes, den die MFP-Anbieter bieten, immer wieder zu Sicherheitsvorfällen kommt. Das gemeinsame Merkmal dieser Sicherheitsvorfälle ist, dass die Kunden erst davon erfahren, nachdem der Verstoß passiert ist. Der Anbieter und der Kunde bemühen sich dann, den Schaden zu begrenzen, eine Lösung zu finden und zu implementieren. Das ist so, als würde man nach einem Einbruch in einen Banktresor und dem Diebstahl des Geldes die Trümmer begutachten und die Reparatur durchführen.

[1]Trellix, früher bekannt als McAfee Enterprise Business

EMBEDDED GERÄTE

Ein eingebettetes System ist ein Computersystem, das für feste Funktionen ausgelegt ist. Eingebettete Systeme finden sich in allen Bereichen des modernen Lebens - Geldautomaten, medizinische Geräte, Drucker, Verkaufsstellen, Kioske usw.

Die heutigen MFPs erfüllen jedoch mehr als nur eine einzige feste Funktion, sie sind eine Mischung aus einer festen Funktion und einem vernetzten IT-Server. Beide verfügen über Festplatten, Betriebssysteme, Webserver, mehrere Ein- und Ausgabeanschlüsse und Schnittstellen und verarbeiten mehrere verschiedene Arten von Informationen. Brauchen diese Geräte eine zusätzliche Sicherheitsebene? Welches ist die richtige Lösung, um Server, Desktops und Netzwerke vor aktuellen und zukünftigen Bedrohungen zu schützen? Diese Frage versuchen die Sicherheitsexperten ständig zu beantworten.

Wir wissen, dass herkömmliche Sicherheitstechnologien wie Antivirensoftware nicht in der Lage sind, die heutige Art von Bedrohungen wie Advanced Persistent Threats (APTs) und Botnets zu bekämpfen, und es setzt sich die Erkenntnis durch, dass die Whitelisting/Allowlisting-Technologie die Antwort auf diese Bedrohungen sein könnte.
diese Bedrohungen.

Beginnen wir also damit, was Whitelists/Allowlists und Blacklists/Blocklists sind.

SCHWARZE LISTEN/BLO CKLISTEN

Zur Bekämpfung von unbefugtem Zugriff, Informationsmissbrauch und Malware greifen IT-Sicherheitsadministratoren in der Regel auf Tools wie Antiviren-Software, Anti-Malware und Netzwerkzugangs- und Inhaltsüberwachung zurück. Die meisten dieser Tools lassen sich in zwei Modelle unterteilen - Blacklists/Blocklists und Whitelists/Allowlists.

Ein Antivirenprogramm basiert auf Hashes bekannter Schadprogramme. Sobald eine bestimmte Variante eines Virus isoliert ist, wird ihr Hash zur schwarzen Liste/Blockliste hinzugefügt, die die Form von .dat-Dateien hat, die täglich heruntergeladen werden müssen. Das Problem ist, dass die Hersteller von Antivirenprogrammen durchschnittlich vier Tage brauchen, um den Virus zu isolieren und eine Aktualisierung der .dat-Dateien zu veröffentlichen. In dieser Zeit ist jeder Computer, der sich ausschließlich auf ein Antivirenprogramm verlässt, anfällig.

Der größte Nachteil dieses Ansatzes ist, dass er immer einen Schritt hinter der Bedrohung zurückbleibt. Vor allem aber sind Tools, die auf Blacklisting/Blocklisting basieren, gegen ein Ereignis wie einen Zero-Day-Angriff völlig unwirksam.

Zero-Day-Angriffe

Bei einem Zero-Day-Angriff werden Schwachstellen in Geräten ausgenutzt, für die es derzeit keine Lösung gibt. Wenn ein Softwareunternehmen einen Fehler oder ein Problem mit einer Software entdeckt, nachdem diese veröffentlicht wurde, wird normalerweise ein Patch entwickelt und angeboten, um das Problem zu beheben. Bei einem Zero-Day-Angriff wird das Problem ausgenutzt, bevor überhaupt ein Patch erstellt wird. Indem er diese Schwachstellen findet, bevor die Softwareentwickler sie entdecken, kann ein böswilliger Programmierer Folgendes schaffen
einen Virus oder Wurm, der ihn ausnutzt und ein System auf verschiedene Weise schädigt.

[1]Trellix, früher bekannt als McAfee Enterprise Business

WHITELISTING / ALLOWLISTING

Der Ansatz des Whitelisting/Allowlisting basiert im Wesentlichen auf der Identifizierung von Dateien für eine IT-Umgebung und der Erlaubnis, nur diese Dateien auf dem System auszuführen. Im Wesentlichen wird nur zugelassen, was bekanntermaßen gut ist, und alles andere, was unbekannt ist, wird gestoppt. Die Standardrichtlinie lautet die Ausführung verweigern, es sei denn, ein Softwareprogramm wurde ausdrücklich zur Whitelist/Allowlist hinzugefügt. Viele der heute verwendeten Überwachungstools fallen unter Whitelisting/Allowlisting, da sie "nur" bestimmte Benutzer, bestimmte IP-Adressen oder vordefinierte Arten von Diensten zulassen, die das System passieren oder ausführen können. Auf diese Weise können Sie sicher sein, dass eine Botnet-Armee Ihre MFPs nicht für Angriffe nutzen kann!

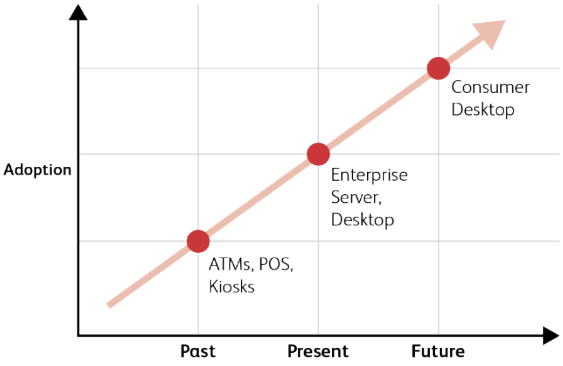
Es ist bekannt, dass Botnets aus Tausenden von infizierten Computern bestehen können. Ein Botnetz ist eine Ansammlung von Computern, die mit Malware infiziert sind, die den Computer unter dem zentralen Kommando und der Kontrolle eines Botmasters versklavt.
Jeder infizierte Computer wird als Zombie bezeichnet. Die Botnet-Malware befindet sich auf dem infizierten Computer, oft ohne das Wissen des Computerbesitzers und ohne dessen Betrieb zu beeinträchtigen. Der Botmaster verkauft die Dienste des Botnets an einen Kunden, um Spam-Werbung per E-Mail zu versenden oder einen DDOS-Angriff (Distributed Denial of Service) auszulösen. Bei einem DDOS-Angriff versuchen alle Zombies gleichzeitig, auf eine bestimmte Website zuzugreifen, die dadurch mit Datenverkehr überflutet und zum Stillstand gebracht wird. Stellen Sie sich vor, dass "Anonymous" eine Regierungswebsite oder eine Medienseite angreift, die sie nicht mögen. Die Trellix[1] Embedded Control-Software in Xerox®-Geräten würde verhindern, dass die infizierende Malware jemals auf dem Gerät Fuß fassen kann, und somit das Gerät davor schützen, in das Botnet aufgenommen zu werden.

Betrachten Sie den Unterschied zwischen Whitelisting/Allowlisting auf einem Desktop-Computer und einem eingebetteten System. Auf einem Allzweckcomputer kann der Benutzer jede beliebige Software laden, die möglicherweise völlig legitim ist. Die Desktop-Whitelisting/Allowlisting-Software muss dann den Benutzer fragen, ob die neue Software zugelassen werden soll. Bei einem eingebetteten System hingegen weiß der Softwareentwickler genau, was auf dem System laufen darf, und kann alles andere ausschließen.

Mit einer Whitelist/Allowlist legen wir fest, was passieren soll und was nicht. Das Chaos beginnt, wenn etwas, das nicht passieren sollte, möglich ist,
wie z. B. eine Adobe® Flash® Player-Anwendung, die auf ein Kernsystem zugreift.
Mit der Whitelisting/Allowlisting-Technologie können Sie verhindern, dass eine ansonsten autorisierte Anwendung auf Kerndateien zugreift, für die sie keine Rechte haben sollte.

Whitelisting/Allowlisting Übernahme

Es ist allgemein anerkannt, dass die Whitelisting/Allowlisting-Technologie ein wirksames Mittel ist, um Zero-Day-Bedrohungen abzuwehren.



WIE KANN XEROX HELFEN?

Was ist also der nächste Schritt in der Sicherheitsentwicklung, um Angriffe auf Ihr Netzwerk über Multifunktionsgeräte abzuschwächen? Xerox war schon immer führend bei der Verbesserung der Sicherheit von Druckern und Multifunktionsgeräten.

Xerox hat sich mit Trellix[1] zusammengetan, um den zunehmenden Bedrohungen für eingebettete Systeme immer einen Schritt voraus zu sein, und legt daher großen Wert auf Sicherheit. Gemeinsam haben wir die Selbstüberwachung und den Selbstschutz eingebaut, die jedes einzelne Gerät zum Schutz vor bösartigen Angriffen benötigt. Darüber hinaus kann der Trellix[1] Agent, der im Gerät läuft, direkt mit der zentralen Sicherheitsmanagement-Konsole - Trellix[1] ePolicy Orchestrator - kommunizieren, so dass Drucker und MFPs auf die gleiche Weise verwaltet werden können, wie Kunden ihre Desktops verwalten.

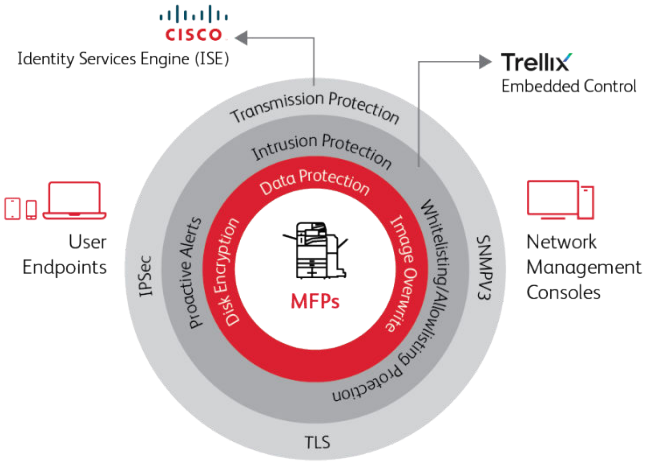
Trellix1-Sicherheitsereignisse, die auf allen bereitgestellten MFPs erzeugt werden, werden an den konfigurierten Trellix[1] ePolicy Orchestrator übermittelt. Dadurch wird die Überwachung aller bereitgestellten MFPs von Trellix[1] ePolicy Orchestrator aus vereinfacht.

Werfen wir einen Blick darauf, was Trellix[1] in das System einbaut, um die bestmögliche Sicherheit für Xerox® MFPs zu gewährleisten.

[1]Trellix, früher bekannt als McAfee Enterprise Business

TRELLIX[1] EMBEDDED CONTROL TECHNOLOGY

Mit der [Trellix1] Embedded Control-Technologie auf Xerox®-Geräten können Kunden aller Größenordnungen - von kleinen bis mittleren Unternehmen (SMBs) mit begrenzten IT-Ressourcen bis hin zu globalen Unternehmen - beruhigt sein, denn sie wissen, dass ihre MFPs sicher sind, und zwar sofort nach der Auslieferung.



[Trellix1] Embedded Control nutzt die Whitelisting/Allowlisting-Technologie, um Ihre Xerox®-Geräte vor Angriffen zu schützen. Dadurch werden kritische Systeme gesperrt und unbefugte Änderungen verhindert, so dass nur Programme ausgeführt werden können, die in der von Xerox erstellten Whitelist/Allowlist enthalten sind. Andere Programme, wie z. B. .exes, .dlls und Skripte, werden als nicht autorisiert betrachtet. Versuche, in eine schreibgeschützte Datei zu schreiben oder aus einer schreibgeschützten Datei oder einem schreibgeschützten Verzeichnis zu lesen, werden verhindert und ein Ereignis wird erstellt und im Audit-Log des Geräts aufgezeichnet.
Wenn SIEM konfiguriert ist (nativ auf [AltaLink®] 8100 Series oder über [Xerox®] Device Manager for [VersaLink®]) werden alle Audit Log-Ereignisse zur Protokollierung und Analyse an einen SIEM-Server weitergeleitet. Wenn auf dem [Xerox®] -Gerät E-Mail-Warnungen konfiguriert sind, wird außerdem eine E-Mail mit den Einzelheiten des Ereignisses an die angegebene Adresse gesendet.

Das Konzept des Whitelisting/Allowlisting ist einfach: Xerox legt eine begrenzte Liste vertrauenswürdiger Anwendungen fest, und nur diese Anwendungen dürfen ausgeführt werden. Dies ist eine ideale Lösung für eingebettete Geräte mit fester Funktion. Die gleiche Technologie wird auch bei Geldautomaten eingesetzt.

Typische Funktionen wie Drucken, Kopieren, Scannen und Faxen sind Teil einer Whitelist/Zulassungsliste für vertrauenswürdige Anwendungen. Darüber hinaus werden administrative Aufgaben wie Firmware-Updates, Software-Upgrades, das Laden von Formularen und Schriftarten, Änderungen von Konfigurationsattributen und Xerox-Techniker-Diagnosen als vertrauenswürdige Vorgänge eingestuft.

Die Trellix1-Software soll Angriffe verhindern, die versuchen, die vorhandene Software des Geräts zu beschädigen oder nicht autorisierte Malware zu installieren.
In der Sicherheitssprache würde man diese Angriffe als "Code-Injektion" oder "Remote-Code-Ausführung" bezeichnen. Im Gegensatz zu anderer Software, die regelmäßige Scans durchführt, um die Integrität des Dateisatzes des Betriebssystems zu überprüfen, wird jeder Lese- und Schreibvorgang ausgeführt,

[1Trellix], früher bekannt als McAfee Enterprise Business

und Ausführungsversuche werden in Echtzeit überprüft. Darüber hinaus läuft die Trellix[1] Embedded Control Software "unterhalb" des Betriebssystems, so dass alles, was versucht, eine Infektion auf dieser Ebene zu starten, wie z. B. ein Root-Kit, entdeckt wird.

Vorteile, die Sie bei der Abwehr von Bedrohungen erwarten können:

- Abschaffung von Notfall-Patching
- Verringerung der Anzahl und Häufigkeit von Patching-Zyklen
- Verringerung des Sicherheitsrisikos durch Zero-Day- und polymorphe Angriffe über Malware wie Würmer, Viren, Trojaner und Code-Injektionen wie Puffer

  Überlauf, Heap-Überlauf und Stack-Überlauf
- Vertrauen in die Integrität der autorisierten Dateien, indem sichergestellt wird, dass sich das System in einem bekannten und überprüften Zustand befindet
- Senkung der Betriebskosten im Zusammenhang mit ungeplanten Ausfallzeiten bei der Wiederherstellung
- Erhöhung der Systemverfügbarkeit

Trellix[1] Embedded Control erkennt Änderungsversuche in Echtzeit. Dazu gehören Versuche, den Systemstatus zu ändern, einschließlich Code, Konfiguration und Registry. Alle Änderungsereignisse werden protokolliert, sobald sie auftreten, und an den Systemcontroller gesendet.

TRELLIX[1] SORGT FÜR MEHR SICHERHEIT

Trellix[1] Enhanced Security, Standard bei neueren MFPs, ist installiert und standardmäßig aktiviert. Sie verhindert allgemeine Angriffe wie das unbefugte Lesen/Schreiben von geschützten Dateien und Verzeichnissen und das Hinzufügen zu bestimmten geschützten Verzeichnissen. Sie bewahrt die Integrität des MFP, indem sie nur die Ausführung von autorisiertem Code und die Durchführung von autorisierten Änderungen zulässt. Wird versucht, die Systemanwendungen zu ändern, mit denen das Gerät betrieben wird, wird der Administrator per E-Mail benachrichtigt. Darüber hinaus werden diese Versuche in den Audit-Protokollen aufgezeichnet und können dann, je nach Kundenkonfiguration, über die Xerox® CentreWare® Web Software oder den Xerox® Device Manager und, falls in der Umgebung vorhanden, über Trellix[1] ePolicy Orchestrator® (ePO) gemeldet werden. Wenn SIEM konfiguriert ist (nativ auf AltaLink 8100 Series oder über Xerox Device Manager für VersaLink), werden alle Audit Log-Ereignisse zur Protokollierung und Analyse an einen SIEM-Server weitergeleitet.

Whitelist/Allowlist-Updates werden von Xerox zur Verfügung gestellt, erfolgen aber nur, wenn die eingebettete Software aktualisiert wird. Bestimmte Funktionen der Software sind von vornherein vertrauenswürdig, so auch der Software-Aktualisierungsprozess. Die Xerox® Software wird mit einer digitalen Signatur versehen, um ihre Integrität und Authentizität zu gewährleisten. Wenn die Signatur gültig ist, wird die neue Software mit einer neuen Whitelist/Allowlist installiert.

Unabhängig von Ihrem Sicherheitsanbieter profitieren Sie von den integrierte Sicherheitsfunktionen von Xerox und Trellix[1] ohne zusätzliche Software. Die Whitelisting/Allowlisting-Funktion ist unabhängig von externer Software und so konzipiert, dass sie die Leistung des Systems nicht beeinträchtigt.

[1]Trellix, früher bekannt als McAfee Enterprise Business

Trellix[1] Enhanced Security wurde entwickelt, um die Probleme im Zusammenhang mit den erhöhten Sicherheitsrisiken zu beseitigen, die mit dem Einsatz kommerzieller Betriebssysteme in eingebetteten Systemen verbunden sind. Mit seinem geringen Platzbedarf und dem geringen Overhead ist es eine anwendungsunabhängige Lösung, die die benötigte Sicherheit ohne Wartung bietet.

Sie fragen sich vielleicht, wie neue Software auf dem Rechner installiert wird, da die Whitelist/Allowlist nur Software zulässt, die ihr bekannt ist. Alle autorisierte Software wird von Xerox digital signiert. Der Software-Installationsprozess prüft die digitale Signatur, bevor er mit der Installation fortfährt, und wenn die Signatur gut ist, informiert er Trellix[1] Enhanced Security, dass die neue Software sicher installiert werden kann. Da Xerox die zulässige Software während der Entwicklung festlegt, enthält jede Software eine eigene Whitelist/Allowlist. Nach der Installation der Software verwendet Trellix[1] Enhanced Security
die neue Whitelist/Allowlist, um zu bestimmen, was erlaubt ist.

Meldung von Bedrohungswarnungen

Bedrohungswarnungen können je nach Ihrer speziellen Konfiguration auf verschiedene Weise übermittelt werden:

- Audit Log - Wird von der Benutzeroberfläche des MFP generiert, standardmäßig aktiviert
- Wenn SIEM konfiguriert ist (nativ auf der AltaLink® 8100 Serie oder über Xerox® Device Manager für VersaLink®), werden alle Audit Log-Ereignisse
  zur Protokollierung und Analyse off-box an einen SIEM-Server weitergeleitet
- E-Mail-Benachrichtigung vom Gerät - Konfiguriert über die Benutzeroberfläche von Xerox® CentreWare® Internet Services
- E-Mail-Warnungen und Berichte über die Xerox® CentreWare Web
  Software und
  Xerox® Device Manager - Konfiguriert über die Xerox® CentreWare®
  Web Software und Xerox® Device Manager Benutzeroberflächen
- E-Mail-Warnungen und -Berichte über Trellix[1] ePolicy Orchestrator - Konfiguriert über die Sicherheitsmanagement-Software Trellix[1] ePolicy Orchestrator
  erhältlich bei Trellix[1]
- Trellix1-Sicherheitsereignisse, die auf bereitgestellten MFPs erzeugt werden, werden an den konfigurierten Trellix[1] ePolicy Orchestrator weitergeleitet.
  Dies vereinfacht die Überwachung aller bereitgestellten MFPs von Trellix[1] ePolicy Orchestrator

TRELLIX[1] INTEG R ITY CO NTR O L

Trellix[1] Integrity Control ist eine optionale, käuflich zu erwerbende Software, die die standardmäßigen erweiterten Sicherheitsfunktionen mit der Fähigkeit kombiniert, gezielte Angriffe und die unbefugte Ausführung von Dateien aus dem Internet zu überwachen und zu verhindern.
an einem beliebigen Ort über nicht vertrauenswürdige Mittel. Sie verhindert auch das Schreiben geschützter, ausführbarer Dateien, die nicht Teil der Standardsoftware des Xerox® -Geräts sind. Dies ist die höchste Sicherheitsstufe und der beste Schutz, den Sie für Ihr Xerox® MFP-Gerät erhalten können.

Die Trellix1-Integritätskontrolle fügt eine zusätzliche Sicherheitsebene hinzu, indem sie verhindert, dass neue Dateien von einem anderen Ort als einer vertrauenswürdigen Quelle ausgeführt werden. Sie verhindert auch das Schreiben geschützter, ausführbarer Dateien, was wiederum das böswillige Überschreiben der von Xerox bereitgestellten ausführbaren Dateien verhindert. Es verhindert nicht autorisierten Code oder Änderungen am System in Form von Malware, Würmern und Trojanern,
Zero-Day-Angriffe und sogar gezielte Angriffe. Nur zugelassene Software darf ausgeführt werden, um einen Angriff abzuwehren, für den es noch keine Gegenmaßnahme gibt.

[1]Trellix, früher bekannt als McAfee Enterprise Business

Xerox und Trellix[1] bieten eine Whitelisting/Allowlisting-Technologie, die sicherstellt, dass nur guter, ausführbarer Code auf geschützten Systemen ausgeführt werden kann. Sie stellt sicher, dass Ihre Geräte nur die Dienste ausführen, die Sie bereitstellen möchten, und verhindert gleichzeitig, dass ein Angreifer bösartigen Code installieren kann. Dieselbe Technologie wird zum Schutz von Servern, Geldautomaten, Kassenterminals und eingebetteten Geräten wie Druckern und mobilen Geräten eingesetzt.

Wie bereits erwähnt, wird Trellix[1] Enhanced Security als Standardfunktion angeboten, die bei bestimmten Modellen vollständig installiert und aktiviert ist. Für die optionale Trellix1-Integritätskontrolle ist keine Installation erforderlich, und die Aktivierung basiert auf einem Lizenzschlüsselverfahren.

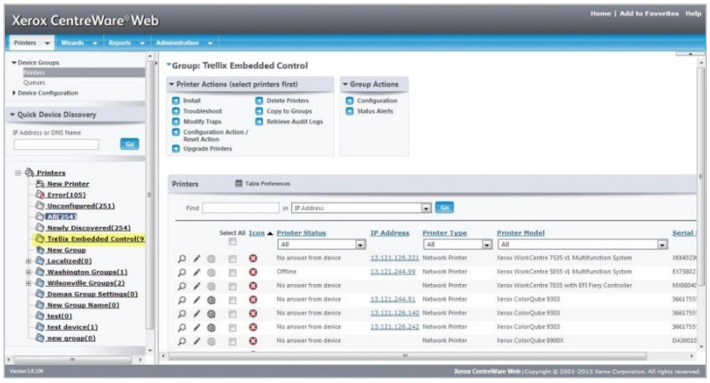
MAN G ING TRELLIX[1] EMBEDDED CO NTRO L DEVICES

Es gibt mehrere Möglichkeiten, Trellix[1] Embedded Control Geräte zu verwalten:

Xerox® CentreWare® Web Software und Xerox® Device Manager

Xerox® CentreWare® Web Software ist ein innovatives, webbrowserbasiertes Softwaretool, das vernetzte Drucker und Multifunktionsgeräte im Unternehmen installiert, konfiguriert, verwaltet, überwacht und Berichte erstellt - unabhängig vom Hersteller. Xerox® Device Manager ist ein einziges Tool zur Installation von Druckwarteschlangen und zur Konfiguration, Verwaltung, Überwachung und Berichterstellung für vernetzte und lokal angeschlossene Geräte - unabhängig vom Hersteller - im gesamten Unternehmen.

Zu den Funktionen gehören Geräteerkennung, Konfiguration und Verwaltung, Auftragsverfolgung und -visualisierung, proaktive Überwachung, Ferndiagnose und Fehlerbehebung sowie Berichterstellung.



Trellix[1] ePolicy Orchestrator®

Diese Software ermöglicht es IT-Administratoren, das Sicherheitsmanagement für Endgeräte, Netzwerke, Daten und Compliance-Lösungen von Trellix[1] und Lösungen von Drittanbietern.

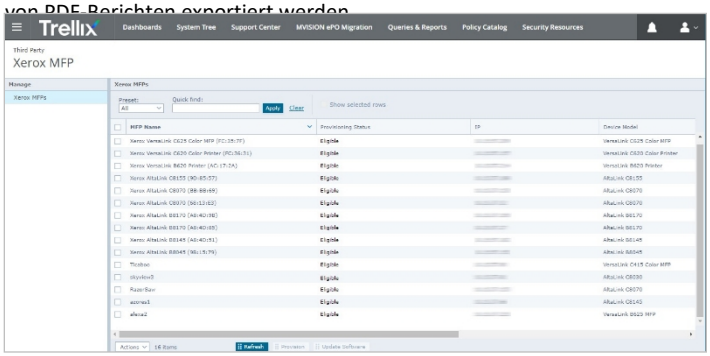
Trellix[1] ePolicy Orchestrator (ePO) ist ein kostenpflichtiges Software-Tool für das Sicherheitsmanagement, das Unternehmen jeder Größe die Verwaltung von Risiken und Compliance erleichtert. Es bietet Anwendern Drag-and-Drop-Dashboards, die Sicherheitsinformationen für alle Endpunkte - Daten, Mobilgeräte und Netzwerke - bereitstellen und so einen sofortigen Einblick und schnellere Reaktionszeiten ermöglichen. Trellix[1] ePO nutzt bestehende IT-Infrastrukturen, indem es die Verwaltung von Trellix[1] und Sicherheitslösungen von Drittanbietern mit Lightweight Directory Access Protocol (LDAP), IT-Betriebs- und Konfigurationsmanagement-Tools verbindet.

[1]Trellix, früher bekannt als McAfee Enterprise Business

Mit durchgängiger Transparenz und leistungsstarken Automatisierungen, die die Reaktionszeiten auf Vorfälle erheblich verkürzen, verbessert die Trellix[1] ePO-Software den Schutz für eingebettete Geräte und reduziert die Kosten und die Komplexität der Risiko- und Sicherheitsverwaltung.

Die Trellix[1] ePO-Software bietet umfassende Reporting-Funktionen für die Ausführung vorkonfigurierter und benutzerdefinierter Abfragen zu Informationen über verwaltete Produkte in Ihrem Netzwerk oder Benutzeraktionen auf Ihrem ePO-Server.

Die Berichtsergebnisse können in verschiedenen Formaten angezeigt werden, z. B. als Tabellen oder Tortendiagramme, und zur Erstellung von PDF-Berichten exportiert werden.

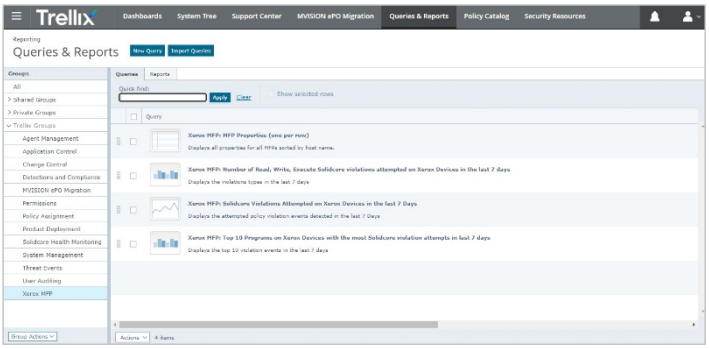


TRELLIX[1] EPO LICY ODER CHESTRA TOR® UND XER OX® MFP EPO EXTENSIO N[2]

Trellix[1] ePO wird direkt von Trellix[1] verkauft und ist nicht Teil der Installation der eingebetteten Steuerelemente. Wenn Sie jedoch bereits Trellix1-Kunde sind, verwenden Sie möglicherweise bereits Trellix[1] ePO. In diesem Fall können Sie die Vorteile der Xerox® MFP ePO-Erweiterung nutzen, mit der Sie in Frage kommende Xerox®-Geräte anzeigen und Sicherheitsereignisse empfangen können. Sie können bis zu 60 Attribute für eine bessere Verwaltung und detailliertere Informationen über Sicherheitskonfigurationen anzeigen.

Darüber hinaus bietet die Xerox® MFP ePO Extension:

- Eine automatische Antwort, um Administratoren die Möglichkeit zu geben, automatische E-Mail-Benachrichtigungen zu erhalten
- Eine Ansicht von etwa 60 Sicherheitskonfigurationsattributen und deren aktuellen Einstellungen
- Die Möglichkeit zu sehen, ob die Gerätefirmware aktuell ist
- Die Möglichkeit, Gerätefirmware in ePO hochzuladen und anschließend ein oder mehrere Xerox®-Geräte zu aktualisieren
- Anzeige in Echtzeit, welche Ports auf dem Xerox®-Gerät aktiv sind
- Nicht erlaubte abhörende Ports anzeigen
- Anzeigen eines Xerox®-Geräte-Sicherheitsereignisses auf dem bereitgestellten Dashboard
- Nutzung der von Xerox bereitgestellten Abfragen und Berichte
- Anpassen von Abfragen oder Berichten zur schnellen Durchführung von Sicherheitsprüfungen in Ihrer Serviceflotte



[1]Trellix, früher bekannt als McAfee Enterprise Business

[2] Xerox® AltaLink®, Xerox® WorkCentre® iSeries und Xerox® EC7800/8000 Series Geräte

[1] McAfee, früher bekannt als McAfee Enterprise Business

UNTERSTÜTZTE GERÄTE

Trellix[1] Embedded Control ist für Xerox® AltaLink® Geräte, Xerox® VersaLink® 7100 Serie, WorkCentre® iSeries und EC7800 und 8000 Serie verfügbar. Weitere Produkte werden in Zukunft hinzukommen.

ZUSA TZLICHE R ESO UR CES

- Xerox und Trellix[1] Datensicherheit
  https://www.xerox.com/en-us/connectkey/insights/trellix-security
- Xerox und Trellix[1] Häufig gestellte Fragen
  https://www.office.xerox.com/latest/SECFS-14U.PDF
- Xerox, Trellix[1] und Cisco®: Gemeinsame Anstrengungen für Echtzeit-Reaktionen auf Cyber-Bedrohungen https://www.xerox.com/en-us/connectkey/insights/network-printer-security
- Datenblatt Trellix[1] Embedded Control
  https://www.trellix.com/en-us/assets/data-sheets/trellix-embedded-kontroll-datenblatt.pdf
- Zero Trust Sicherheit
  https://www.xerox.com/zerotrust
- Xerox Sicherheitslösungen
  https://www.xerox.com/securitysolutions

[1]Trellix, früher bekannt als McAfee Enterprise Business

AUTHO R S

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

Für weitere Informationen über Xerox®-Produkte mit Trellix[1] Embedded Control wenden Sie sich bitte an einen Xerox-Vertreter oder besuchen Sie www.xerox.com/en-us/connectkey/ insights/trellix-security.