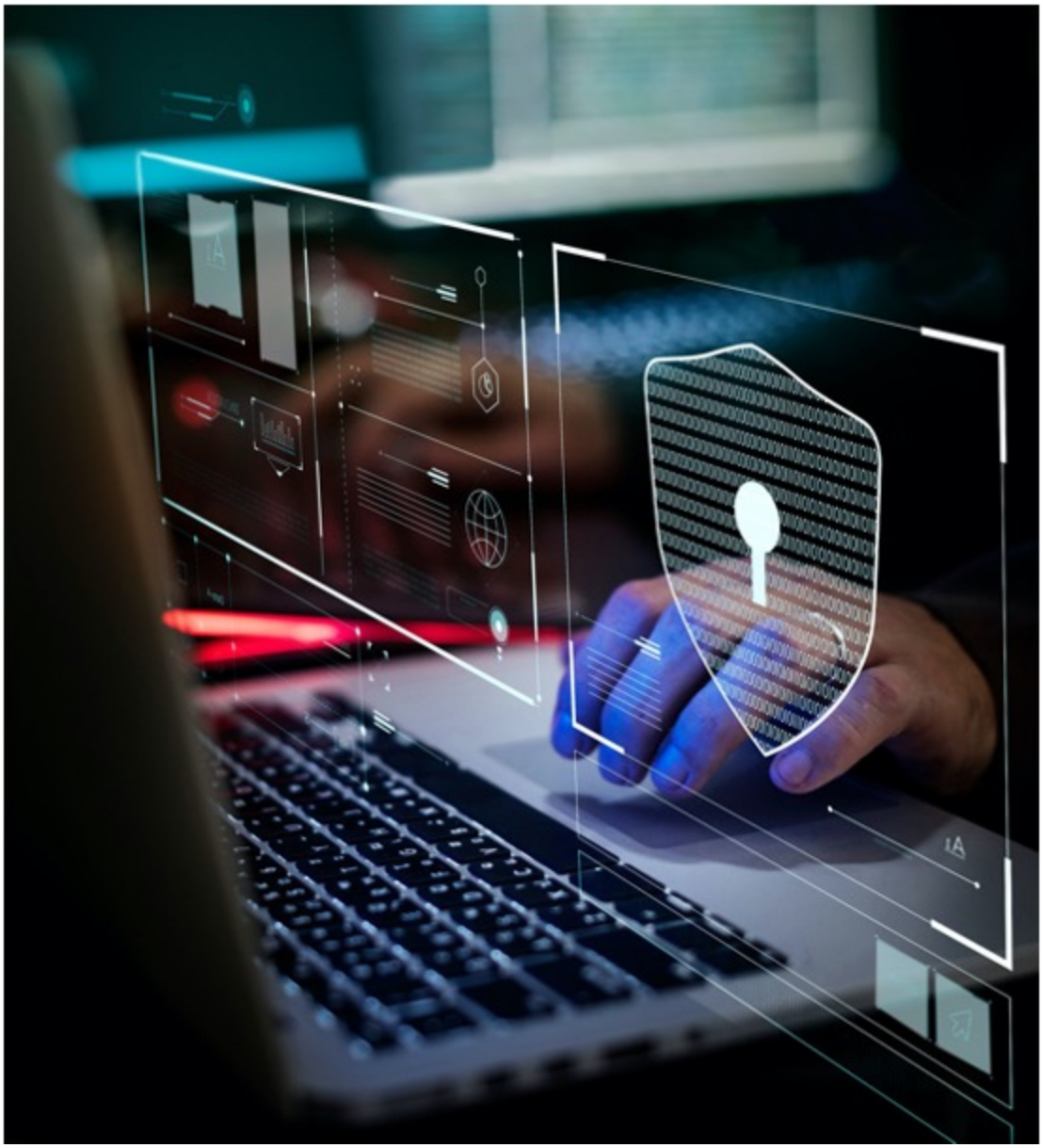


Xerox Next Generation Security: Partnering with Trellix[1]

White Paper

[1]Trellix, formerly known as McAfee Enterprise business

xerox™

Background

Today's multifunction printers (MFPs) are complex embedded systems. They contain, among other things, full-scale operating systems, embedded web servers, support for multiple protocol stacks, external hardware and software interfaces, and application programming interfaces (APIs) to interact with enterprise systems. Because of the broad capabilities and power of these MFP devices, they potentially represent a serious risk to your network and enterprise systems if they are not adequately protected.

MFP vendors have significantly increased their engineering efforts to tighten security controls in these devices by introducing protection improvements, including:

- Disk encryption and disk overwrite to protect end-user data
- Enablement of encrypted protocols such as Transport Layer Security (TLS), Internet Protocol Security (IPsec), and Simple Network Management Protocol Version 3 (SNMPv3) to protect any data transmitted to and from the device
- User authentication for most tasks
- Access control through the addition of firewalls and roles based on Active Directory (AD) groups
- Audit logs for traceability
- Security evaluation programs such as Common Criteria Certification

Are the MFPs embedded systems or open systems? Do these devices need an additional layer of security? If so, what is the right solution for protecting servers, desktops, and networks against current and future threats? This is a question experts in the security communities are constantly trying to answer.

We know that traditional security technologies, such as anti-virus, have limited effectiveness against today's breed of threats like advanced persistent threats (APTs) and botnets.

The reality is that despite the additional protection added by MFP vendors, security incidents continue to occur. The common theme among these security incidents is that customers find out only after the violation happens. The vendor and customer then scramble to alleviate the damage, come up with a fix, and deploy a solution. It's the equivalent of assessing the wreckage and implementing the repair after the bank vault has been broken into and the money stolen.

[1]Trellix, formerly known as McAfee Enterprise business

EMBEDDED DEVICES

An embedded system is a computer system designed for fixed functions. Embedded systems span all aspects of modern life – ATMs, medical devices, printers, point-of-sale devices, kiosks, etc.

However, today's MFPs perform more than a single fixed function, they are a hybrid between a fixed function and an IT networked server. Both of these have hard disks, operating systems, web servers, multiple input and output connections, and interfaces, and process several different types of information. Do these devices need an additional layer of security? What is the right solution that can protect servers, desktops, and networks against current and future threats? This is a question experts in the security communities are constantly trying to answer.

We know that traditional security technologies, such as anti-virus software, are not able to combat today's breed of threats like advanced persistent threats (APTs) and botnets, and there is a wider acknowledgment that Whitelisting/Allowlisting Technology may be the answer to combat these threats.

So, let's start with what are whitelists/allowlists and blacklists/blocklists.

BLACKLISTS/BLOCKLISTS

To fight against unauthorized access, misuse of information, and malwares, IT security administrators usually rely on tools such as anti-virus software, anti-malware, and network access and content monitoring. Most of the tools can be divided into two models – blacklists/blocklists and whitelists/allowlists.

An anti-virus relies on hashes of known malware. Once a particular variant of a virus is isolated, its hash is added to the blacklist/blocklist, which takes the form of the .dat files that need to be downloaded daily. The problem is that it takes anti-virus vendors an average of four days to isolate the virus and publish an update to the .dat files. During that time, any computer relying solely on anti-virus is vulnerable.

The biggest drawback of this approach is that it's always one step behind the threat. Most importantly, tools based on blacklisting/blocklisting are completely ineffective against an event like a zero-day attack.

Zero-day Attacks

A zero-day attack takes advantage of device vulnerabilities that currently do not have a solution. Typically, when a software company discovers a bug or problem with a piece of software after it has been released, they will develop and offer a patch to fix the issue. A zero-day attack takes advantage of the problem before a patch is even created. By finding these vulnerabilities before software developers find them, a malicious programmer can create a virus or worm that exploits it and harms a system in a variety of ways.

[1]Trellix, formerly known as McAfee Enterprise business

WHITELISTING/ALLOWLISTING

The whitelisting/allowlisting approach is fundamentally based on the identification of files for an IT environment and allowing only these files to execute on the system. Essentially, it's allowing only what's known to be good and stopping everything else that's unknown. The default policy is to deny execution unless a software program has been explicitly added to the whitelist/allowlist. Many of the monitoring tools used today fall under whitelisting/allowlisting since they "only allow" designated users, specific IP addresses, or predefined types of services to pass through or run on the system. With this, you can rest assured a botnet army can't recruit your MFPs to launch attacks!

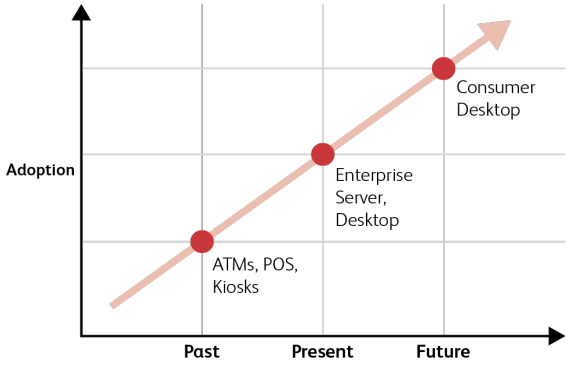
Botnets have been known to comprise thousands of infected computers. A botnet is a collection of computers infected by malware that enslaves the computer under the central command and control of a botmaster. Each infected computer is called a zombie. The botnet malware resides on the infected computer, often without the knowledge of the computer owner, and without interfering with its operations. The botmaster sells the services of the botnet to a client for the purpose of emailing spam advertising or to cause a Distributed Denial of Service (DDOS) attack. In a DDOS, all of the zombies try to simultaneously access a particular website, overwhelming it with traffic and causing it to shut down. Think in terms of "Anonymous" attacking a government website or a media site they don't like. The Trellix[1] Embedded Control software in Xerox® Devices would prevent the infecting malware from ever gaining a toehold on the device, thus protecting the device from being assimilated into the botnet.

Consider the difference between whitelisting/allowlisting on a desktop computer versus an embedded system. On a general-purpose computer, the user can load any arbitrary software, which might be totally legitimate. The desktop whitelisting/allowlisting software then has to ask the user if the new software should be allowed. Contrast that with an embedded system, where the software developer knows exactly what should be allowed to run on that system, and can lock out everything else.

Using a whitelist/allowlist, we define what should and shouldn't happen. Chaos begins when something that shouldn't happen is possible, such as an Adobe® Flash® Player application accessing a core system. With whitelisting/allowlisting technology, you can prevent an otherwise authorized application from accessing core files that it should not have rights to.

Whitelisting/Allowlisting Adoption

It is widely acknowledged that whitelisting/allowlisting technology is a powerful way to thwart zero-day threats.



HOW CAN XEROX HELP?

So what's the next step in the security evolution to mitigate attacks on your network via MFPs? Xerox has always been the leader in bringing security to printers and multifunction devices.

Consistent with our continued emphasis on security, Xerox has partnered with Trellix[1] to stay one step ahead of increasing threats to embedded systems. Together, we've built in the self-monitoring and self-protection each individual unit needs to guard against malicious attacks. In addition, the Trellix[1] Agent running in the device is able to communicate directly with the central security management console – Trellix[1] ePolicy Orchestrator – to allow printers and MFPs to be managed in just the same way customers manage their desktops.

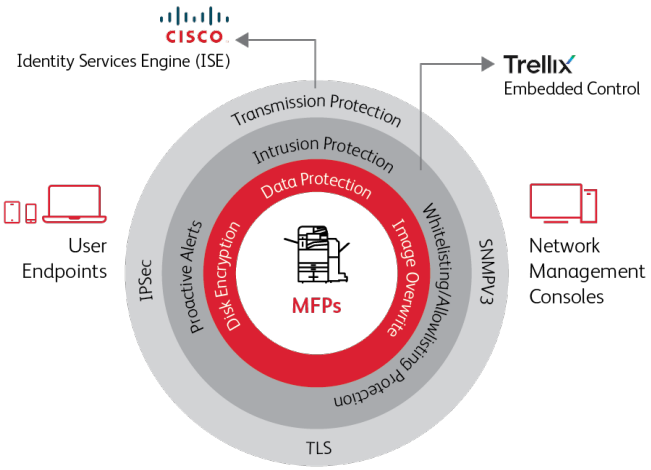
Trellix[1] security events generated on any provisioned MFPs are communicated to the configured Trellix[1] ePolicy Orchestrator. This helps simplify the monitoring of all the provisioned MFPs from Trellix[1] ePolicy Orchestrator.

Let's take a look at what Trellix[1] is putting inside to ensure the best possible security for Xerox® MFPs.

[1]Trellix, formerly known as McAfee Enterprise business

TRELLIX[1] EMBEDDED CONTROL TECHNOLOGY

With Trellix[1] Embedded Control technology on Xerox® Devices, customers of all sizes – from small to medium-sized businesses (SMBs) with limited IT resources to global enterprises – can have peace of mind, knowing their MFPs are secure, right out of the box.



Trellix[1] Embedded Control uses whitelisting/allowlisting technology to protect your Xerox® Devices from attack. This locks down critical systems and prevents unauthorized change events so that only programs contained in the Xerox-created whitelist/allowlist can execute. Other programs, such as .exes, .dlls, and scripts, are considered unauthorized. Attempts made to write to a read-only file, or read from a write-only file or directory, are prevented and an event is created and recorded in the device Audit Log. If SIEM is configured (natively on AltaLink® 8100 Series, or through Xerox® Device Manager for VersaLink®), all Audit Log events are forwarded off-box to a SIEM server for logging and analysis. Further, if email alerts are configured on the Xerox® Device, an email is sent to the designated address with details of the event.

The concept of whitelisting/allowlisting is simple – Xerox predefines a finite list of trusted applications, and only those applications are allowed to run. It's an ideal solution for fixed function embedded devices. The same technology is deployed on ATMs.

Typical functions such as print, copy, scan, and fax are a part of a trusted application whitelist/allowlist. In addition, administrative tasks, including firmware updates, software upgrades, form and font loading, configuration attribute changes, and Xerox technician diagnostics, are all comprehended as trusted operations.

The intention of the Trellix[1] software is to prevent attacks that attempt to corrupt the device's existing software, or install unauthorized malware. In security language, these would be known as "code injection" or "remote code execution" attacks. Unlike other software that performs periodic scans to validate the integrity of the operating system file set, every read, write, and execute attempt is checked in real time. In addition, the Trellix[1] Embedded Control software runs "below" the operating system so that anything, such as a root kit, that tries to launch an infection at that level would be detected.

Benefits you can expect when it comes to threat defense:

- Elimination of emergency patching
- Reduction of the number and frequency of patching cycles
- Decrease in the security risk from zero-day, polymorphic attacks via malware such as worms, viruses, Trojans, and code injections like buffer overflow, heap overflow, and stack overflow
- Confidence in the integrity of authorized files, ensuring the system is in a known and verified state
- Reduction in the cost of operations related to unplanned recovery downtime
- Increase in system availability

Trellix[1] Embedded Control detects change attempts in real time. These include attempts to change the system state, including code, configuration, and the registry. All change events are logged as they occur and sent to the system controller.

TRELLIX[1] ENHANCED SECURITY

Trellix[1] Enhanced Security, standard on newer MFPs, is installed and enabled by default. It prevents general attacks such as the unauthorized read/write of protected files and directories and adds to designated protected directories. It maintains the integrity of the MFP by only allowing authorized code to be run and authorized changes to be made. With the baseline in place, if there are any attempts to change the system applications that operate the device, the administrator is alerted via e-mail. In addition, those attempts are recorded in the audit logs and, depending on the customer setup, can then be reported through Xerox® CentreWare® Web Software or Xerox® Device Manager, and, if present in the environment, Trellix[1] ePolicy Orchestrator® (ePO). If SIEM is configured (natively on AltaLink 8100 Series, or through Xerox Device Manager for VersaLink), all Audit Log events are forwarded off-box to a SIEM server for logging and analysis.

Whitelist/allowlist updates are provided by Xerox, but occur only when the embedded software is updated. By design, certain functions of the software are trusted, including the software update process. A digital signature is applied to the Xerox® Software to guarantee its integrity and authenticity. If the signature is valid, the new software is installed with a new whitelist/allowlist.

Regardless of your security vendor, you will still benefit from the built-in Xerox and Trellix[1] security features without requiring additional software. The whitelisting/allowlisting function is independent of any external software and is designed to run without interfering with the system's performance.

[1]Trellix, formerly known as McAfee Enterprise business

Trellix[1] Enhanced Security is designed to eliminate the problems surrounding increased security risks associated with the adoption of commercial operating systems in embedded systems. With its small footprint and low overhead, it's an application-independent solution that provides the maintenance-free security you need.

You might be wondering how new software is installed on the machine, since the whitelist/allowlist will only allow software it knows about. All authorized software is digitally signed by Xerox. The software installation process checks the digital signature before proceeding with an installation, and if the signature is good, it informs Trellix[1] Enhanced Security that the new software is safe to install. Since Xerox defines the set of allowable software during development, each set of software carries its whitelist/allowlist. After the software installation, Trellix[1] Enhanced Security uses the new whitelist/allowlist to determine what is allowed.

Reporting of Threat Alerts

Threat alerts can be communicated in several different ways depending on your particular configuration:

- **Audit Log** – Generated from the user interface on the MFP, enabled by default
- If SIEM is configured (natively on AltaLink® 8100 Series, or through Xerox® Device Manager for VersaLink®), all Audit Log events are forwarded off-box to a SIEM server for logging and analysis
- **Email Alert from the Device** – Configured through the Xerox® CentreWare® Internet Services user interface
- **Email Alerts and Reports via Xerox® CentreWare Web Software and Xerox® Device Manager** – Configured through the Xerox® CentreWare® Web Software and Xerox® Device Manager user interfaces
- **Email Alerts and Reports via Trellix[1] ePolicy Orchestrator** – Configured through the Trellix[1] ePolicy Orchestrator security management software available from Trellix[1]
- Trellix[1] security events generated on any provisioned MFPs are communicated to the configured Trellix[1] ePolicy Orchestrator. This helps simplify the monitoring of all the provisioned MFPs from Trellix[1] ePolicy Orchestrator

TRELLIX[1] INTEGRITY CONTROL

Trellix[1] Integrity Control is optional, purchasable software that combines the standard Enhanced Security features with the ability to monitor and prevent targeted attacks and the unauthorized execution of files from any location via untrusted means. It also prevents the writing of protected, executable files that are not part of the standard Xerox® Device software. It is the highest level of security, and most protection you can get for your Xerox® MFP.

Trellix[1] Integrity Control adds a layer of security by preventing new files from being executed from any location other than a trusted source. It also prevents the writing of protected, executable files, which in turn prevents the malicious overwrite of Xerox-supplied executables. It stops any unauthorized code or changes to the system in the form of malware, worms, Trojans, zero-day attacks, and even targeted attacks. Only approved software is allowed to run, heading off an attack for which a countermeasure does not yet exist.

Xerox and Trellix[1] offer whitelisting/allowlisting technology that ensures only good, executable code can run on protected systems. It ensures your devices are performing only the services you want to deliver while preventing an attacker from installing malicious code. This same technology is used to protect servers, ATMs, point-of-sale terminals, and embedded devices such as printers and mobile devices.

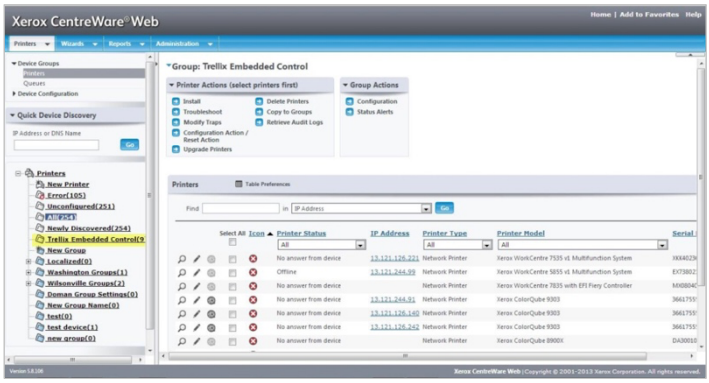
As mentioned earlier, Trellix[1] Enhanced Security is offered as a standard feature, completely installed and enabled, on certain models. For the optional Trellix[1] Integrity Control, there is no installation procedure required for customers and activation is based on a licensing key process.

MANAGING TRELLIX[1] EMBEDDED CONTROL DEVICES

There are several options for managing Trellix[1] Embedded Control devices:

Xerox® CentreWare® Web Software and Xerox® Device Manager

Xerox® CentreWare® Web Software is an innovative, web browser-based software tool that installs, configures, manages, monitors, and reports on networked printers and multifunction devices in the enterprise – regardless of the manufacturer. Xerox® Device Manager is a single tool to install print queues and configure, manage, monitor, and report on both networked and locally connected devices – regardless of vendor – across your enterprise. Functions include device discovery, configuration and management, job tracking and visualization, proactive monitoring, remote diagnostics and troubleshooting, and reporting.



Trellix[1] ePolicy Orchestrator®

This software allows IT administrators to unify security management across endpoints, networks, data, and compliance solutions from Trellix[1] and third-party solutions.

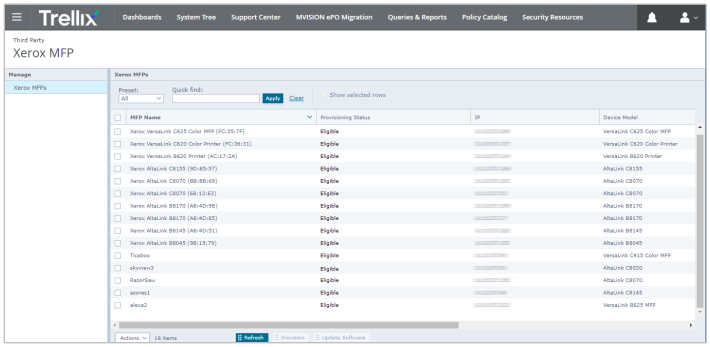
Trellix[1] ePolicy Orchestrator (ePO) is a purchasable security management software tool that makes risk and compliance management easier for organizations of all sizes. It presents users with drag-and-drop dashboards that provide security intelligence across endpoints—data, mobile, and networks, for immediate insight and faster response times. Trellix[1] ePO leverages existing IT infrastructures by connecting the management of Trellix[1] and third-party security solutions to Lightweight Directory Access Protocol (LDAP), IT operations, and configuration management tools.

[1]Trellix, formerly known as McAfee Enterprise business

With end-to-end visibility and powerful automations that significantly reduce incident response times, Trellix[1] ePO software enhances protection for embedded devices and reduces the cost and complexity of managing risk and security.

Trellix[1] ePO software provides comprehensive reporting capabilities for running preconfigured queries and custom queries on information about managed products on your network or user actions on your ePO server.

Report results can be displayed in different formats, such as tables or pie charts, and exported to create PDF reports.

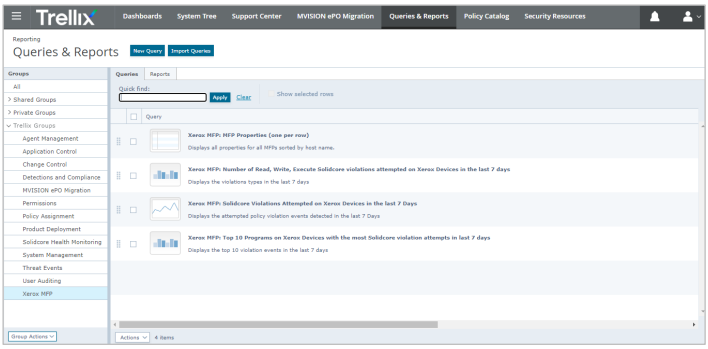


TRELLIX[1] EPOLICY ORCHESTRATOR® AND XEROX® MFP EPO EXTENSION[2]

Trellix[1] ePO is sold directly by Trellix[1] and is not part of the embedded controls' installation. However, if you are currently a Trellix[1] customer, you may already be using Trellix[1] ePO. If that's the case, you can take advantage of the Xerox® MFP ePO extension, which lets you see eligible Xerox® Devices and provisions to receive security events. View up to 60 attributes for better management and more detailed information about security configurations.

In addition, the Xerox® MFP ePO Extension provides:

- An automated response to give administrators the ability to receive automatic email notifications
- A view of approximately 60 security configuration attributes and their current settings
- The ability to view if the device firmware is current
- The ability to upload device firmware into ePO and subsequently upgrade one or more Xerox® Devices
- View in real time which listening ports are active on the Xerox® Device
- View disallowed listening ports
- View a Xerox® Device security event on the dashboard provided
- Utilize Xerox-provided queries and reports
- Customize queries or reports to perform security compliance checks quickly across your service fleet



[1]Trellix, formerly known as McAfee Enterprise business

[2]Xerox® AltaLink®, Xerox® WorkCentre® iSeries and Xerox® EC7800/8000 Series Devices

SUPPORTED DEVICES

Trellix[1] Embedded Control is available for Xerox® AltaLink® Devices, Xerox® VersaLink® 7100 Series, WorkCentre® iSeries and EC7800 and 8000 Series. More products will be added in the future.

ADDITIONAL RESOURCES

- Xerox and Trellix[1] Data Security
  https://www.xerox.com/en-us/connectkey/insights/trellix-security
- Xerox and Trellix[1] Frequently Asked Questions
  https://www.office.xerox.com/latest/SECFS-14U.PDF
- Xerox, Trellix[1], and Cisco®: Joining forces for real-time cyber threat response
  https://www.xerox.com/en-us/connectkey/insights/network-printer-security
- Trellix[1] Embedded Control Data Sheet
  https://www.trellix.com/en-us/assets/data-sheets/trellix-embedded-control-datasheet.pdf
- Zero Trust Security
  https://www.xerox.com/zerotrust
- Xerox Security Solutions
  https://www.xerox.com/securitysolutions

[1]Trellix, formerly known as McAfee Enterprise business

AUTHORS

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

For more information about Xerox® Products with Trellix[1] Embedded Control, please contact a Xerox representative or go to **www.xerox.com/en-us/connectkey/insights/trellix-security**.