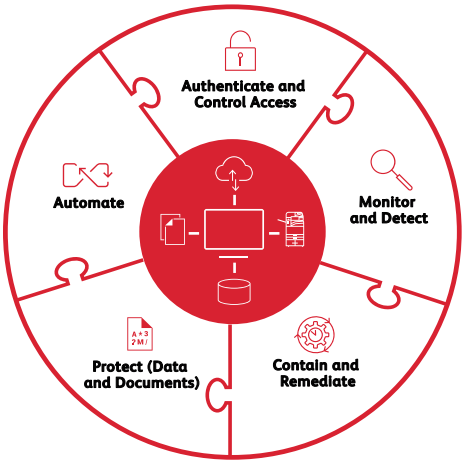
Zero Trust

Cybercrime has reached unprecedented levels globally, and is expected to continue growing. Organizations need new strategies and best practices to defend against these threats.

Today's distributed workforce needs access to their IT infrastructure anytime, from anywhere. An increasing number of digital transformation initiatives are placing business data within easy access. A multitude of IoT devices are now connected to critical business systems, which form the backbone of any business. These trends are putting security professionals under increasing pressure to enable the modern workplace, while reducing the enterprise's security attack surface.

Zero Trust has emerged as a powerful method to provide secure access to authorized users and devices, while improving the enterprise security posture.

With comprehensive security as a key focus at Xerox, we have enabled our clients with products and services that support Zero Trust initiatives. Concepts such as never trust, always verify, least privilege access, proactive threat detection and remediation, encryption, and security certifications are not new. However, when utilized in a cohesive security strategy, they represent critical features of a successful Zero Trust security program.



Implementing Zero Trust

We support your Zero Trust initiatives with the following best practices and recommendations:

AUTHENTICATE AND CONTROL ACCESS

Start with the "no implicit trust" policy and ensure all user access is verified.

Xerox® Printers ship from the factory with secure and unique passwords for the Admin account. Role Based Access Controls can be implemented with local usernames, PIN code access, card-based, and CAC/PIV secure authentication. Least privilege access and continuous revalidation can be enforced with inactivity timers/logouts. Multifactor authentication is supported via Cloud Identity Providers (IdPs) such as Ping Identity, Okta, Microsoft Azure Identity Services, as well as Xerox® Workplace Cloud/ Xerox® Workplace Suite solutions.

Xerox® Workplace Cloud Print Management Solution and Xerox® Workplace Suite Print Management Solution extend the capabilities of Xerox® Printers across a fleet of devices to provide a consistent approach. They enforce a never trust security posture by requiring users to unlock printers with cards/badges, mobile devices, or PIN codes prior to accessing the printers' available services.

Xerox® Managed Print Services implements mandatory authentication at every new connection at the user and system level. It establishes defined user role-based access, and provides password management with NIST 800-171R2 approved methods. CA/Certificate Management ensures authorized printers communicate securely across the network.

MONITOR AND DETECT

Continuously monitor and detect (potential) security threats.

Xerox® Printers are equipped with digitally signed and encrypted firmware, and with firmware verification, they are designed to protect against attempts to tamper with the system software. Trellix*[1] Whitelisting/ Allow Listing monitors for malware in real-time, rejecting and notifying users of malicious activity. Trusted Boot[4] ensures the integrity of the system start-up process.

Syslog/Audit log data generation and integration with SIEM tools[2] such as LogRhythm, Splunk, and Trellix* Security Manager provide useful insights to detect and mitigate security threats. With the help of Cisco Identity Services Engine (ISE), we can detect and prevent unauthorized printers from connecting to your network.

Xerox® Workplace Cloud and Xerox® Workplace Suite integrate with your ID management system to ensure seamless access and authentication operation. This prevents synchronization issues between the access control mechanism and the ID provider. At a local/ device level, we use tools such as reCAPTCHA to monitor and block detected brute-force entry attempts.

Xerox® Managed Print Services provide customer-defined cadence of security monitoring. We implement fleet-wide device management with Xerox® Printer Security Audit Service. It is used to intuitively manage the entire fleet's configuration by setting print and security policies remotely. It is also used as the basis for interactive dashboard style, real-time data reporting. Security patches and firmware updates are applied consistent with the customer's security policy.

xerox™

Zero Trust

CONTAIN AND REMEDIATE

In the event of a potential compromise, contain the threat and provide swift remediation to eliminate it.

At Xerox, we have designed our printers with a security-first approach that prevents threats from infecting them. Layers of security features further contain potential security breaches. For example, the Configuration Watchdog[3] printer feature allows system administrators to implement up to 75 security settings, and proactively remediate (reset) them in case they are changed.

At the fleet level, Xerox® Printer Security Audit Services maintain policy compliance and proactively remediate any devices that fall out of compliance. We conduct regular reviews of configuration policies (to ensure they are up-to-date with security requirements), advise the client, and provide ongoing security recommendations.

PROTECT (DATA AND DOCUMENTS)

Use data encryption techniques and software solutions to protect data and documents from intentional and unintentional disclosure.

The storage drives on our printers are protected with 256-bit encryption. Stored data that is no longer required can be deleted using National Institute of Standards and Technology (NIST) and U.S. Department of Defense approved data clearing and sanitization algorithms. Print output is protected through the use of a PIN or card release system. And we prevent scan information from reaching those that should not receive it, using digitally signed, encrypted, and password-protected file formats.

Our printers[4] let you lock down 'to/cc/bcc' email fields, limiting scan destinations to designated domains only, such as internal ones. With the Imaging Security feature, Xerox® AltaLink® Printers use IR (Infrared) technology to mark and detect sensitive documents. This prevents their unintended duplication and creates alerts and audit logs to track duplication attempts.

Unused network services can be disabled to reduce the network's attack surface. IP Filtering can be implemented to restrict network access to only approved clients for scan, print, and device management. Secure protocols such as IPsec, HTTPS, LDAPS, and SFTP protect data in transit. FIPS mode can be enabled to ensure only the most secure protocols are allowed to interact with the device.

Xerox® Workplace Cloud solution encrypts content in transit and at rest. Content stored in the cloud at Xerox can be encrypted using a client's own encryption key. By using their own encryption management, clients gain all the benefits of moving to cloud-based print management, and keep control over who can see the content of their data. The Content Security feature of Xerox® Workplace Cloud and Workplace Suite solutions provides a capability to detect pre-defined sensitive content and generate alerts and reports based on how that data is used.

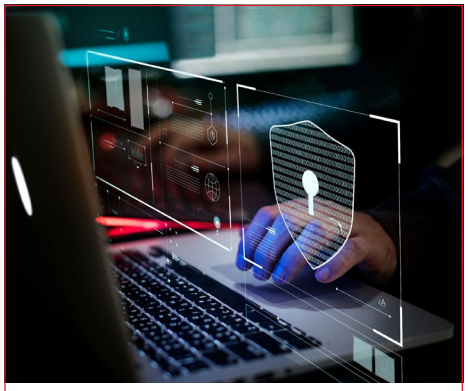
Xerox® Printer Security Audit Services ensure data and document protection features are enabled on the fleet, remediate policy violations, and report compliance.

AUTOMATE

Streamline security policy for best results.

Automation leads to simplicity and allows security teams to focus on important issues. The Fleet Orchestrator feature of Xerox® Printers automates device configuration and applies firmware updates to a network of printers. This ensures compliance while reducing the burden on IT staff. With the integration of Cisco ISE and Trellix* ePolicy Orchestrator, any printer can be automatically quarantined upon threat detection. This prevents damage to the printer, and protects the network and other endpoints.

Xerox® Printer Security Audit Services use a centralized policy mechanism and device grouping to streamline fleet management with minimal effort. Compliance enforcement and validation is fully automated. Dashboards present fleet, policy, and device compliance information in an easy-to-read, graphical format.



A successful security program depends on a simple and enforceable security policy, backed by product features and services that ensure compliance. Zero Trust is quickly becoming the security model of choice for businesses of all sizes. By implementing the Xerox security recommendations outlined in this brief, businesses can safely provide authorized user access, limit exposure in case of data breaches, and automate responses to potential security threats.

[1] Xerox® AltaLink®, EC Series and Xerox® VersaLink® 7100 Series MFPs.
[2] AltaLink® direct SIEM integration, all other devices through Xerox® Managed Print Services.
[3] Xerox® AltaLink® 8000 and 8100 Series MFPs.
[4] Xerox® AltaLink® and Xerox® VersaLink®.
*Trellix formerly known as McAfee.

To learn more about Xerox Security, visit **www.xerox.com/securitysolutions**.