RICOH
imagine. change.

MFP/Printer Security White Paper Ricoh Approach to Adopting Zero Trust Security

Based on the CISA Zero Trust Maturity Model

Version 1.00 2026/9

Table of Contents

1 Introduction P.03

- 1-1 Overview of Zero Trust Security
- 1-2 Why Zero Trust Security?
- 1-3 Goal and Target Readers of This White Paper

2 Basic Zero Trust Concepts P.04

- 2-1 Basic Zero Trust Principles
- 2-2 Zero Trust Maturity Model

Five Pillars and Three Capabilities of the CISA Zero Trust Maturity Model

3 Office Printing Realized by Ricoh in a Zero Trust Environment P.06

- 3-1 Compatibility with existing environment to achieve step-by-step migration
- 3-2 Centralized management of multiple sites
- 3-3 Functional comprehensiveness to cover the five pillars and three capabilities of the CISA Zero Trust Maturity Model

4 Requirements of Zero Trust Security (Five Pillars) P.07

- 4-1 Identity
- 4-2 Devices
- 4-3 Networks
- 4-4 Applications & Workloads
- 4-5 Data

5 Requirements of Zero Trust Security (Three Capabilities) P.12

- 5-1 Visibility & Analytics
- 5-2 Automation & Orchestration
- 5-3 Governance

6 Model Cases P.13

- Case 1 Managing Multiple Sites with a Cloud-Focused Model
- Case 2 Integrated Management of On-Premise Environment with Devices from Multiple Vendors

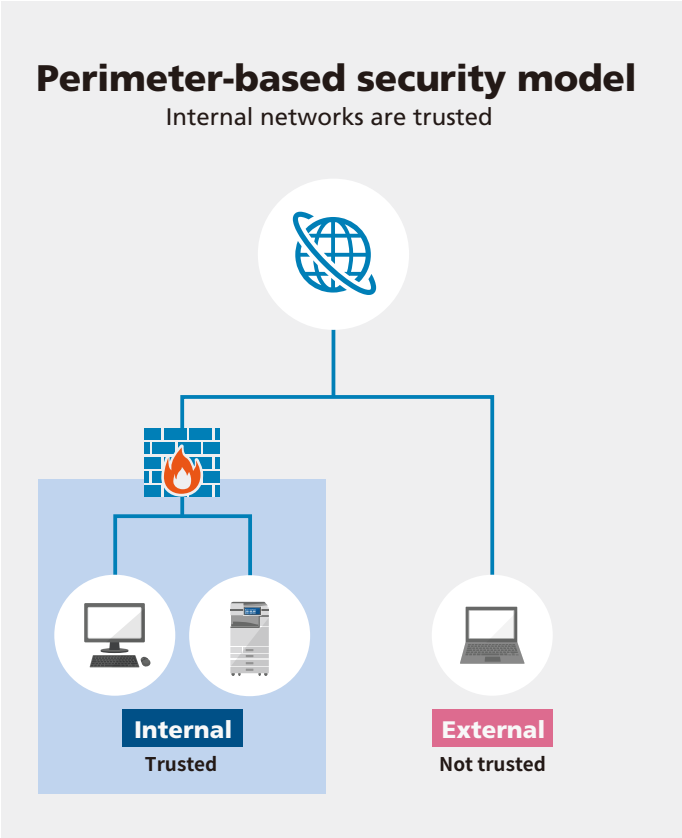
Step-by-Step Migration Flowchart

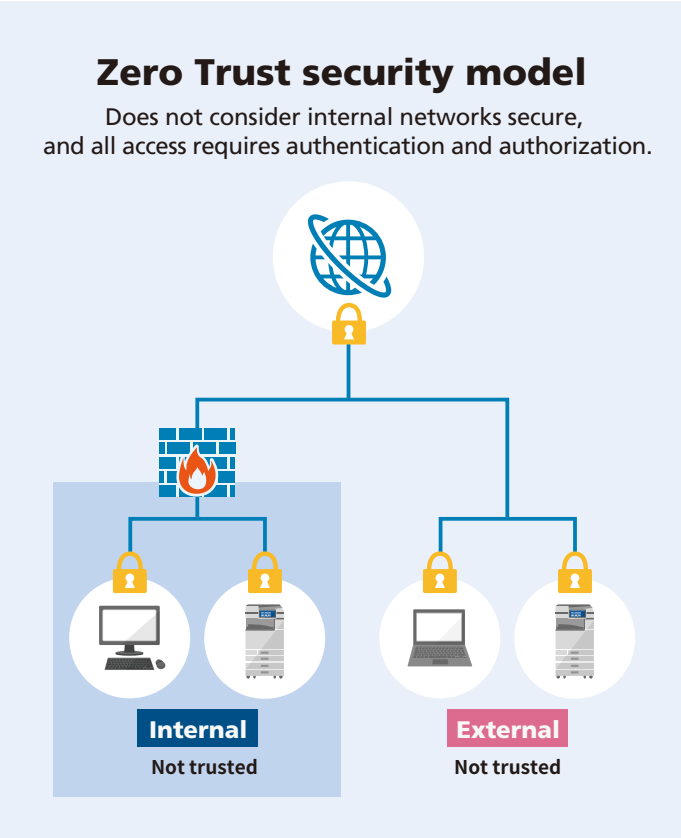
7 Summary / Next Steps to Take P.16

1 Introduction

1 - 1 Overview of Zero Trust Security

In the past, most companies adopted a perimeter-based security model. With perimeter-based security, internal networks are separated from external Internet environments, and security devices are positioned at those perimeters to protect information assets from cyberattacks. Everything inside the internal networks is deemed to be trusted. However, with Zero Trust security, internal networks are not considered secure and all access requires verification.





1 - 2 Why Zero Trust Security?

The rise of cloud services and workplace changes such as remote work have led to increased risk of unauthorized access targeting network environment vulnerabilities and the need to protect information assets saved to external environments from unauthorized access and leaks. It has become difficult to ensure security with traditional security measures alone, and this has led to the need for a new approach — Zero Trust security.

1 - 3 Goal and Target Readers of This White Paper

This white paper is intended as a reference for information security professionals at organizations that deploy and operate Ricoh MFPs and printers when building a Zero Trust environment.

2 Basic Zero Trust Concepts

This chapter introduces the basic principles of Zero Trust security and examples of Zero Trust models referenced by Ricoh.

2 - 1 Basic Zero Trust Principles

Eliminate implicit trust

Traditionally, access was implicitly trusted because the ability to access an internal network meant that authentication had already been verified once. With Zero Trust security, access is not trusted simply because it originates from an internal network or because authentication has already been verified once, and instead all access must be verified, regardless of whether it originates from an internal or external network.

Verify all access

With Zero Trust security, authenticity is verified every time access to a resource occurs. The verification process determines authenticity based not only on a user ID and password, but also a combination of other factors such as the device status, connection location, and time of day.

Assign the least privileges

With Zero Trust security, users and systems are assigned only the least privileges required to carry out their work. This limits the scope of damage if an account or device is compromised.

Design for intrusion

With Zero Trust security, systems are designed with the possibility of intrusion in mind. Access scope separation and privilege granularization are focused on to ensure a system configuration that minimizes the impact of possible security incidents.

Conduct ongoing monitoring and evaluation

Zero Trust security does not end with implementation. The status of operation must be monitored and improved on an ongoing basis. Logs and system behavior are monitored on an ongoing basis to improve access control and policies according to situational changes and new threats that arise.

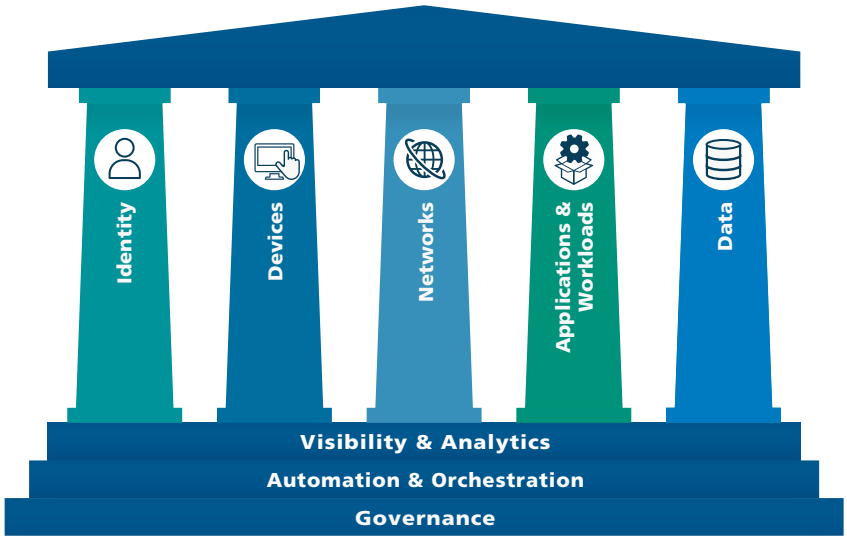
2 - 2 Zero Trust Maturity Model[*1]

The Cybersecurity and Infrastructure Security Agency (CISA) of the United States has published a maturity model for the step-by-step evaluation of Zero Trust adoption.
In the maturity model, CISA states that Zero Trust security is not completed all at once, and is instead a framework that gradually matures. The model is utilized as a guideline by companies who are planning to adopt Zero Trust security.

*1 Zero Trust Maturity Model（https://www.cisa.gov/zero-trust-maturity-model）

Five Pillars and Three Capabilities of the CISA Zero Trust Maturity Model

The Zero Trust Maturity Model published by the CISA is a framework for evaluating the Zero Trust implementation level of an organization based on five pillars and four maturity levels.
This table is a guideline to use for understanding the current level of security measures at your enterprise. It is normal for an enterprise to have some variation between maturity levels for each of the pillars. The "Optimal Stage" does not necessarily refer to the optimal choice for all organizations. When actually implementing Zero Trust security, it is important to formulate a step-by-step improvement plan that takes into consideration factors such as return on investment, operational overhead, and compatibility with existing systems.



Pillar	Description	Maturity Level			
		Traditional Stage	Initial Stage	Advanced Stage	Optimal Stage
Identity	Robust authentication and authorization of users and devices	Static authentication	Adoption of multi-factor authentication	Dynamic authorization based on context and risk	Ongoing verification and automatic application of least privilege
Devices	Ongoing verification of the integrity, authenticity, and security of devices	Asset identification only	Security configuration and compliance checks	Ongoing status evaluation	Automatic isolation, automatic response, and recovery
Networks	Monitoring, control, and encryption of communication	Perimeter firewall	Adoption of microsegmentation	Dynamic communication control based on context	Encryption of all communication and implementation of an ongoing policy
Applications & Workloads	Allow only trusted applications and services	Perimeter level protection	Access control per application	Dynamic authorization and workload protection	Ongoing monitoring, automatic response, and integrated control
Data	Classification, encryption, and lifecycle management	Static classification	Basic encryption	Labeling, confidential information removal prevention, and granular access control	Automatic lifecycle management and dynamic protection

*This table indicates a general Zero Trust maturity model and is not a list of functions achievable with any particular products or services.
*Developed by Ricoh based on the CISA Zero Trust Maturity Model Version 2.0.
*Applications & workloads refers to an application and the components involved in its execution and operation, including services, containers, virtual machines, and APIs.

Three capabilities (Visibility & Analytics, Automation & Orchestration, and Governance) support these five pillars.

Visibility & Analytics:

Visualizing and analyzing data and events across the entire organization to make policy improvement and incident handling faster while also enabling risk identification and bolstering preventive measures.

Automation & Orchestration:

Utilizing and operating automation tools and workflows to improve the efficiency of security measures for all products and services, while maintaining monitoring and control.

Governance:

Defining, implementing, and enforcing cybersecurity policies, procedures, and processes for the entire organization.

3 Office Printing Realized by Ricoh in a Zero Trust Environment

This white paper is written to describe how Ricoh products and solutions in the field of MFPs and printers are incorporated in a Zero Trust environment across an enterprise, and what kind of roles they play. From this chapter onwards, this white paper looks at the requirements for MFPs and printers based on the CISA Zero Trust Maturity Model, and introduces Ricoh solutions that help meet those requirements.

3 - 1 Compatibility with existing environment to achieve step-by-step migration

Ricoh products and solutions are compatible with an existing authentication platform and network security platform, such as Active Directory, Microsoft Entra ID, or SASE.

- Build a print environment that assumes co-existence with SASE and an existing on-premise environment.

3 - 2 Centralized management of multiple sites

Centralized management of the MFPs at multiple sites in enables the head office to remotely monitor and control the MFPs at all sites.

- **RICOH CloudStream for cloud-based management**

  RICOH CloudStream offers cloud-based centralized management of the MFPs and printers at multiple sites and provides functionality for asset information management, status monitoring, configuration management, and software/firmware distribution. It also visualizes the status of devices across the entire organization and aids ongoing device governance.

- **RICOH Streamline NX for management of both Ricoh and non-Ricoh printers with an on-premise environment**

  RICOH Streamline NX provides integrated management of printers in an on-premise environment, including those from other manufacturers, and features device discovery, log management, user management, and configuration management.

3 - 3 Functional comprehensiveness to cover the five pillars and three capabilities of the CISA Zero Trust Maturity Model

Note that an entire Zero Trust environment cannot be achieved with Ricoh products and solutions alone. When it comes to identity and access management, network security platform (such as SASE or ZTNA), monitoring platform (such as SIEM), and operation processes, Ricoh products and solutions are expected to be linked with customer environments or solutions from other companies. Ricoh mainly assists Zero Trust security in the field of MFPs and printers.
From this chapter onwards, this white paper describes the requirements for MFPs and printers and the functionality that Ricoh can help with, from the perspective of the five pillars and three capabilities defined in the CISA Zero Trust Maturity Model.

4 Requirements of Zero Trust Security (Five Pillars)

This chapter describes the security requirements for MFPs and printers based on the elements of the five pillars in the Zero Trust Maturity Model of the CISA. It also introduces examples of Ricoh solutions to support those requirements.

*The various features and services described here may be provided differently in some regions. Contact us for details.

4 - 1 Identity

Identity refers to the identification of individual users and the management of which user is accessing something, whether the user is who they say they are, and which functions and information the user is allowed to operate.

Traditional Stage

User Management Based on Individually-Managed Authentication Information

With this method, users are managed based on an address book and local authentication information in the MFP itself. It enables the use of user code authentication and login user name + password authentication. Disadvantages include the need to change the settings of each device due to relocation, users joining or leaving the enterprise, or changes to outsourcing partners, which increases the risk of orphaned accounts and inconsistent privilege configurations.

Initial, Advanced, and Optimal Stage

Centralized Management of Authentication Information by Linking with a Directory Service

RICOH Streamline NX can be used for the centralized management of authentication information by linking with an authentication platform such as Active Directory or an LDAP server. This eliminates the need to manage authentication information for individual MFPs, and provides an authentication environment that follows the ID management policy of the entire organization.

Cloud IdP linking

Linking with a cloud authentication platform such as Microsoft Entra ID or Okta enables the centralized management of user information and authentication policies. In addition to consolidating authentication information, this provides an environment linked with an enterprise-wide identity policy that can include multi-factor authentication (MFA), conditional access, and risk-based access. Authentication platforms can be integrated because account management due to relocation, users joining or leaving the enterprise, or changes to the organization can be handled according to an ID lifecycle on the cloud side. Furthermore, because MFP authentication is incorporated in an enterprise-wide identity management mechanism, it can be expanded to conditional access and risk-based access in the future.

Role-Based Access Control (RBAC)

This mechanism controls the available functions and privileges of users according to their roles. By controlling the accessible functions according to roles such as administrator, general user, and outsourcing partner user, access management can be performed based on the principle of least privilege. For example, you can allow general users to only print and scan, but allow administrators to change device settings. This helps reduce the risk of unauthorized usage and information leaks.

Multi-Factor Authentication (MFA)

Multi-factor authentication (MFA) is a mechanism whereby individual users are checked based on a combination of something you know (password), something you have (IC card), and something you are (biometric information). Linking this with an authentication platform such as Microsoft Entra ID can enable an authentication environment compatible with an enterprise-wide multi-factor authentication policy. Compared to single-factor authentication, multi-factor authentication reduces the risk of information leaks and unauthorized access due to impersonation. Applying multi-factor authentication to MFP control panels and functions such as authenticated printing can provide more robust identity protection.

4 - 2 Devices

MFPs and printers must be managed as end points connected to a network. Zero Trust security requires a unified security policy to be applied and asset information, configurations, software status, and vulnerability status to be visualized and evaluated on an ongoing basis.

Traditional Stage

Individual Management of Devices

Traditionally, it is common for the status of MFPs to be checked and reconfigured on an individual basis. Web Image Monitor (a web-based status monitoring and configuration interface built into Ricoh MFPs and printers.) can be used to check the device status, configuration, and job history. However, as the number of devices to manage increases, so too does the workload, and this can make it easier for configuration mistakes to occur and software updates to be missed. Therefore, there is a limit to how far individual management of devices can achieve the ongoing configuration management and status evaluation required by Zero Trust security.

Initial, Advanced, and Optimal Stage

Centralized Management of Device Configurations

RICOH Streamline NX and RICOH CloudStream enable the centralized management of MFPs and printers for the following:

- Device discovery
- Asset information management
- Status monitoring
- Log management
- Configuration management
- Firmware management

This enables a unified security policy to be applied over the entire organization and allows ongoing status management.
By visualizing the asset information and configuration status, you can build the ongoing device management platform required by Zero Trust security.

Automatic Firmware Updating

Zero Trust security requires devices to be always up-to-date and secure. Automatically or systematically applying firmware updates enables known vulnerabilities to be handled and functions to be improved on an ongoing basis. This helps prevent missed updates and update delays due to manual operations, and maintains a security baseline for devices. It also systematically eliminates known vulnerabilities and helps reduce risk across the entire organization. Ricoh provides the RICOH Streamline NX and RICOH CloudStream device management solutions to enable planned firmware updates of multiple MFPs and printers.

Detecting Firmware Modifications

Zero Trust security requires the reliability of the software operating inside devices to be continuously verified. With MFPs and printers, this involves verifying the authenticity (integrity) of firmware and performing error notification if a modification is detected. Digital signing can also be used to prevent unauthorized software from being executed, which reduces the risk of malware intrusion and unauthorized modifications. This maintains reliability inside devices and supports the ongoing device verification required by Zero Trust security.

Device Authentication (IEEE 802.1X)

This mechanism performs device authentication when connecting to a network, and only allows communication with authorized devices. It can be linked with an authentication platform such as RADIUS to enact strict connection control based on device certificates and authentication information. This prevents the connection of unauthorized devices and eliminates shadow IT, while also providing ongoing verification of device authenticity.

4 - 3 Networks

Networks must be managed as an important layer that controls access between users, devices, and applications, rather than as a simple communication route. Zero Trust security does not deem internal network traffic inherently trustworthy, and requires communication to be monitored and controlled on an ongoing basis to determine whether access is allowed based on the attributes and status of users, devices, and applications. Furthermore, encryption and certificate-based trust are important factors for protecting data in communication routes.

Traditional Stage

Static Access Control with IP Address Filtering

This mechanism controls access based on the IP addresses of the source and destination of the communication, and performs basic traffic control based on network segmentation. This enables communication to be allowed or rejected for certain network ranges or devices, which can prevent unauthorized access and restrict the scope of communication. However, because IP addresses are static attributes, it is important to use this mechanism in conjunction with control based on other authentication or context.

Initial, Advanced, and Optimal Stage

Certificate-Based Encrypted Communication

By applying certificates to devices and encrypting communication using a protocol such as TLS, the confidentiality and integrity of data on a network can be maintained. Both self-signed certificates and certificates issued by a CA (certificate authority) are supported, which enables a highly reliable communication environment to be constructed to meet the needs of the usage environment. This reduces the risk of eavesdropping and modification, and realizes the concept of protect all communication, which is required by Zero Trust security.

Print Architecture with Reduced Dependency on Internal Networks

Traditionally, MFPs were installed on an internal network, and connected to computers and servers within the same network segment. RICOH CloudStream and RICOH Streamline NX can be used to print via the cloud, which enables the construction of a print environment with reduced dependency on internal networks. This reduces unnecessary internal communication and helps reduce the impact if an intrusion happens to occur. It also makes it easier to implement a configuration that combines with a network security platform such as SASE (Secure Access Service Edge) or ZTNA (Zero Trust Network Access).

4 - 4 Applications & Workloads

Applications & Workloads refers to the protection of the printing platform, authentication platform, and related services. With Zero Trust security, functions to use, processes to execute, and communication routes are continuously verified based on the principles of explicit verification, least privilege, and expectation of intrusion. Rather than trusting access because it originates from an internal network, only the minimum required privileges are assigned and the reliability of applications and services must be checked on an ongoing basis.

Traditional Stage

Usage without Access Privilege Configuration and User Authentication

With traditional perimeter-based security, the MFPs and related systems on a network are deemed trustworthy. Therefore, it was not necessary to configure detailed access privileges or implement control to limit functions to authenticated users. However, Zero Trust security requires authentication and authorization to be performed every time access is attempted and only the minimum required privileges to be assigned.

Initial, Advanced, and Optimal Stage

Access Authorization

With Zero Trust security, access is allowed or rejected based on the authenticated ID and the functions it is allowed to use, rather than the network location. This enables the accessible functions to be controlled based on authentication and function restrictions for each user. Ricoh provides such access control with RICOH Streamline NX and RICOH CloudStream. This enables an organization to migrate from a model where users can access resources simply because they are on the internal network to one where identity and privileges are explicitly verified each time access is requested, helping prevent unauthorized access to applications and workloads.

Execute Only Trusted Software

It is also important to check the reliability of executed software, in addition to that of the applications and drivers that are used. Ricoh printer drivers have obtained Microsoft WHQL certification, which aids driver reliability checks. Furthermore, Ricoh MFPs support firmware authenticity checks and encryption key protection via a TPM (Trusted Platform Module), which helps build an environment where only verified software can be executed. Instead of allowing all available software to be executed, only software verified as trusted can be executed, which helps improve the integrity as required by the Zero Trust pillar of Applications & Workloads.

Ongoing Security Evaluation

With Zero Trust security, it is important to continuously evaluate vulnerabilities and risks, instead of continually allowing applications and services after they have been verified once. Ricoh continuously works on activities such as vulnerability management, security evaluation, and incident handling throughout the entire lifecycle of Ricoh products and cloud services. This enables Ricoh to swiftly identify potential threats and vulnerabilities, and helps improve service reliability via ongoing improvements.

Secure Application Development and Deployment

It is important to incorporate security from the stage of development, design, and release, and conduct ongoing reviews after deployment. Ricoh promotes the concept of security by design based on ISO/IEC 27034-1. This helps implement a system whereby security is incorporated from the beginning and continuously enforced, instead of only when a problem arises, which helps establish workload protection across an entire lifecycle.

4 - 5 Data

All types of data in a system (such as that on devices, applications, and networks) must be managed and protected, and data transfers must be detected.

Traditional Stage

Address Book Management inside Main Unit Storage

With this method, address information and user information is managed inside the storage of the MFP main unit. Although this is a simple management method where everything can be done on the MFP itself, the protection of the saved data itself relies on the configuration and operation of the device. In a traditional environment, it is common for data storage locations and protection settings to be located in individual devices, making it difficult to establish an enterprise-wide classification/protection policy and implement lifecycle management. Therefore, it is necessary to enhance encryption and access control to achieve the kind of environment required by Zero Trust security, where protection is focused on the data itself.

Initial, Advanced, and Optimal Stage

Storage Encryption

Storage encryption is a mechanism for encrypting data stored on the MFPs and printers itself, such as address book data, authentication information, stored documents, and temporary image data, to prevent information leaks stemming from unauthorized reading or the theft of recordable media.

Print Data Encryption

Print data encryption is a mechanism whereby the print jobs sent from a computer to an MFP and the print data temporarily saved and retained inside an MFP are both encrypted, to reduce the risk of confidential information leaking due to eavesdropping. Even a cloud-based print environment can be made secure by encrypting the communication route and the print data itself. This enables print jobs themselves to be protected when sent, without relying on the assumption that internal network traffic is inherently trustworthy.

Cloud-Based Printing

RICOH CloudStream and RICOH Streamline NX support printing via the cloud, and encrypt both the print data and the communication route. These services provide a secure print environment everywhere, including the office, home, or outside. They can also link with cloud services to support the use of documents based on the access control policy of the organization.

5 Requirements of Zero Trust Security (Three Capabilities)

Mechanisms for visualization, automation, and governance are essential for actually operating and continuously improving the five pillars described in Chapter 4. The three capabilities are elements that support all five pillars — Identity, Devices, Networks, Applications & Workloads, and Data.

5 - 1 Visibility & Analytics

Visibility & Analytics is the capability to collect and analyze data and events from the entire organization to aid the early detection of problems and risks. Zero Trust security requires users, devices, applications, and data to be continuously monitored in order to make improvements to access control and security policies.

Log Collection and Centralized Management

MFPs and printers should be monitored across the entire enterprise and this requires a system for continuously collecting access logs, job logs, and device events. RICOH Streamline NX is provided for collecting the following:

- Access logs
- Job logs
- Device events
- Device status
- Outage information
- Operation status
- Counter information

The collected information can be visualized in reports or on a dashboard, which allows the operation status to be monitored and aids continuous evaluations.
RICOH CloudStream is provided for continuously collecting the device status and asset information, which enables the operation status to be visualized and aids the early detection of warning signs.

5 - 2 Automation & Orchestration

With Zero Trust security, a policy defined for the entire organization must be automatically applied to continuously maintain security while reducing the work required for doing so.

- **Batch security setting configuration:**

  Applying setting templates to multiple MFPs and printers can help prevent configuration discrepancies and operational mistakes. The scheduled execution function also helps implement ongoing configuration management. RICOH Streamline NX and RICOH CloudStream can be used to increase the efficiency of distributing and managing unified security settings across an organization's entire MFPs and printers fleet.

- **Automatic firmware updates:**

  Zero Trust security requires devices to be always up-to-date and secure. Automatic firmware updates and RICOH Streamline NX and RICOH CloudStream can be used to systematically apply the latest security patches and functional improvements.

5 - 3 Governance

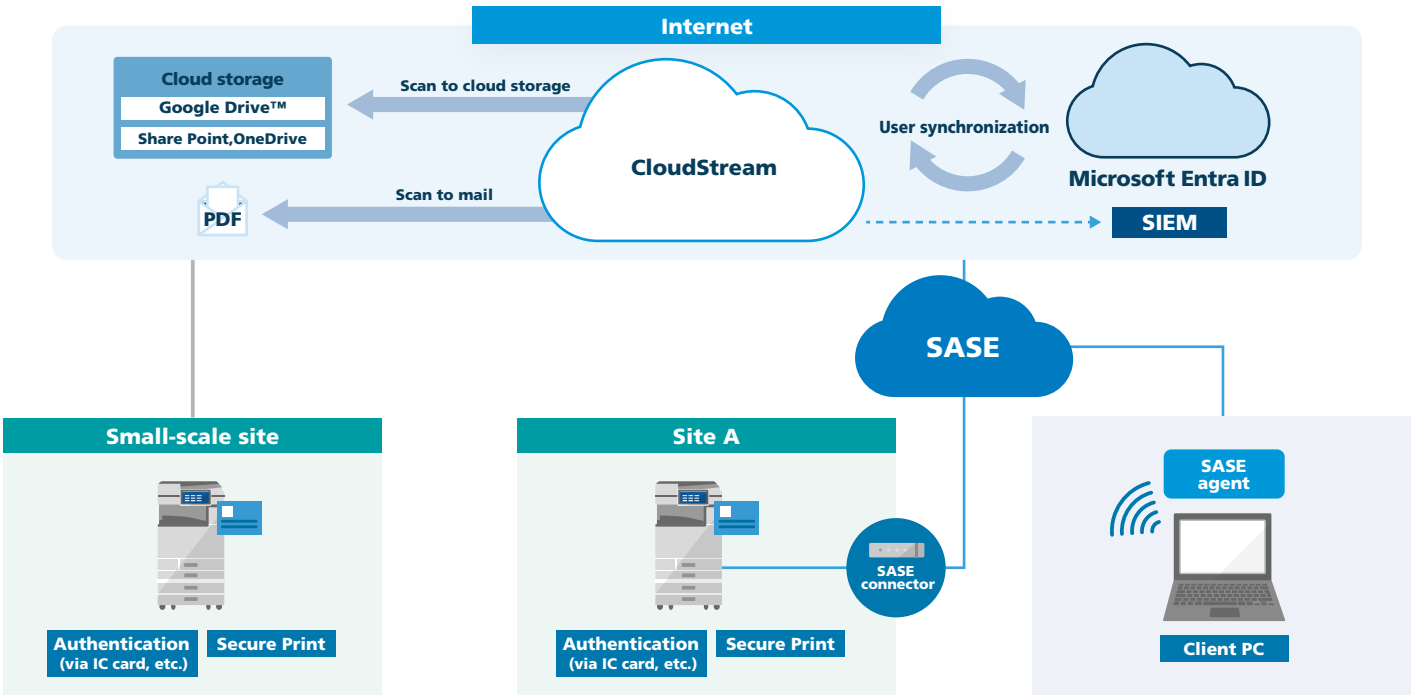
Zero Trust security requires a consistent security policy and continuous improvements to be implemented via an organizational framework including an ISMS (Information Security Management System), incident handling, and security policy management. Ricoh strives to implement ongoing improvements by handling vulnerabilities based on the PSIRT process.

6 Model Cases

Chapter 4 described the five pillars required by Zero Trust security and Chapter 5 described the three capabilities for supporting those pillars. This chapter introduces examples of Ricoh MFPs and printers and related solutions to achieve those requirements. It is important to note that Zero Trust security cannot be achieved simply by adopting a particular product. Ricoh solutions are one component of a Zero Trust environment built by the customer, and are used in conjunction with the authentication, device management, and monitoring platforms.

Model Case 1 Managing Multiple Sites with a Cloud-Focused Model

With a cloud-focused model, RICOH CloudStream is used to achieve cloud-based centralized management of MFPs and printers located across multiple sites. Administrators can continuously monitor the device status, asset information, and configuration at each site and systematically distribute software and firmware as required. This ensures that MFPs and printers are handled as items for device management across the entire enterprise, which reduces configuration variation and ensures updates, while also helping implement ongoing status management as required by Zero Trust security. Furthermore, collected device information can be utilized for visualizing operating status on a platform for Visibility & Analytics.

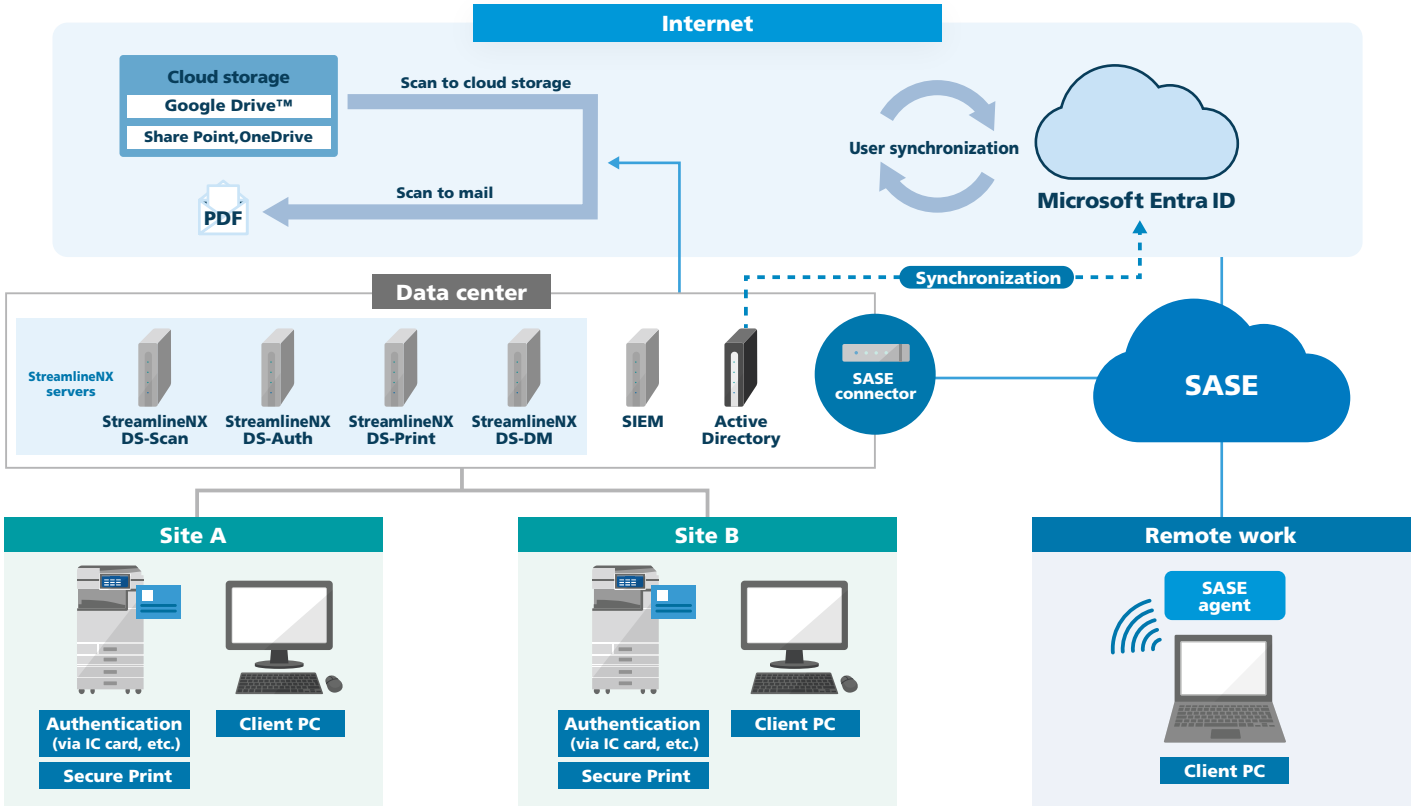


*An SASE connector is required for connecting an MFP to an SASE.

With this model, authentication is handled by an identity platform such as Microsoft Entra ID, and MFP/printer management and monitoring is handled by RICOH CloudStream. Logs can be linked with SIEM as required and integrated with the security monitoring across the entire enterprise. RICOH CloudStream does not achieve Zero Trust security by itself, and is used in conjunction with the existing identity, monitoring, and network platforms.

Model Case 2 Integrated Management of On-Premise Environment with Devices from Multiple Vendors

In on-premise environments and environments that contain printers from multiple manufacturers, RICOH Streamline NX can be used to comprehensively implement authentication linking, user management, job management, and log collection. By linking with an authentication platform such as Active Directory or LDAP, user authentication for MFPs and printers can be incorporated in the identity management of the entire enterprise. By also collecting access logs, job logs, and device events and linking this data with an analysis platform such as SIEM when necessary, it becomes easier to swiftly identify abnormal use and suspicious activity. Instead of monitoring the print environment on its own, the monitoring can be integrated in the security monitoring and analysis environment of the entire enterprise.



*An SASE connector is required for connecting an MFP to an SASE.

With this model, user authentication is performed in conjunction with Active Directory and Entra ID, and Streamline NX handles the authentication linking, log management, and job management of the print environment. By linking the collected logs with SIEM, they can be integrated with the visualization and analysis platform of the entire enterprise.

Step-by-Step Migration Flowchart

Phase 1 Preparation and Evaluation

Identify high-value assets, classify risks, and define requirements. Prioritize MFPs at departments that handle sensitive documents, and determine the confidentiality level and priority of the handled documents.

Phase 2 Planning and Selection

Prioritize countermeasures, select adoption scenarios, and create a step-by-step roadmap. Start from the fundamental security baseline (ID control, device protection, and data encryption).

Phase 3 Implementation

Roll out Ricoh solutions based on system requirements and check their effectiveness.

Phase 4 Operation and Monitoring

It is recommended to continuously monitor job logs and device events in SIEM, periodically evaluate the security status, and incorporate the results into the security plan.

7 Summary / Next Steps to Take

Rather than something that is completed with a single implementation, Zero Trust security is an ongoing effort for making improvements according to the maturity level and business requirements of an enterprise. It is recommended that you first identify the current situation at your enterprise, then clarify the challenges and points for improvement in the various fields of Identity, Devices, Networks, Applications & Workloads, and Data.

By incorporating MFPs and printers in a Zero Trust strategy, the security maturity level of an entire organization can be raised. Ricoh mainly assists Zero Trust security in the field of MFPs and printers via its products, solutions, and services. Overall architecture including an identity platform, network security platform, and monitoring platform is configured according to the customer environment and the solutions currently in use. Ricoh helps improve security and operations regarding print environments.

* Active Directory, Microsoft, Microsoft Entra, OneDrive, and SharePoint are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries
* Google Drive™ is a trademark of Google Inc. Use of this trademark is subject to Google Permissions.
* Okta is a trademark or registered trademark of Okta, Inc. and its affiliates in the United States and other countries.
* Wi-Fi™, WPA2™, and WPA3™ are trademarks of Wi-Fi Alliance.
* IEEE is a trademark of The Institute of Electrical and Electronics Engineers, Inc.
* All other product and service names mentioned herein are the marks of their respective owners.

RICOH
imagine. change.

https://www.ricoh.com/

The information contained in this white paper is current as of September 2026.