RICOH
imagine. change.

Ricoh essentials security guide

Layered security to enable business transformation in today's digital workplace

The need to operate in a digital-driven world has accelerated transformational change for organizations as they modernize capabilities to meet the demands of evolving markets. This can often result in a fragmented landscape of tools and technologies that reveal security, privacy and operational gaps.

Keeping things secured and compliant — ensuring people, processes and technology are safeguarding against data breaches — is a never-ending effort that has to be addressed holistically, across every facet of the business.

Security has the power to make or break high-level business goals, and yet too often it isn't integrated into the overall business strategy. How can organizations make security strategic to their business transformation, to enable important goals such as brand trust, compliance, innovation, business continuity, and sustainability?

Brand trust	Compliance	Innovation	Business continuity	Sustainability
Design for transparency and trust	Meet regulations and exceed expectations	Confidently grow and gain a competitive advantage	Ensure success through every storm	Protect the broader community

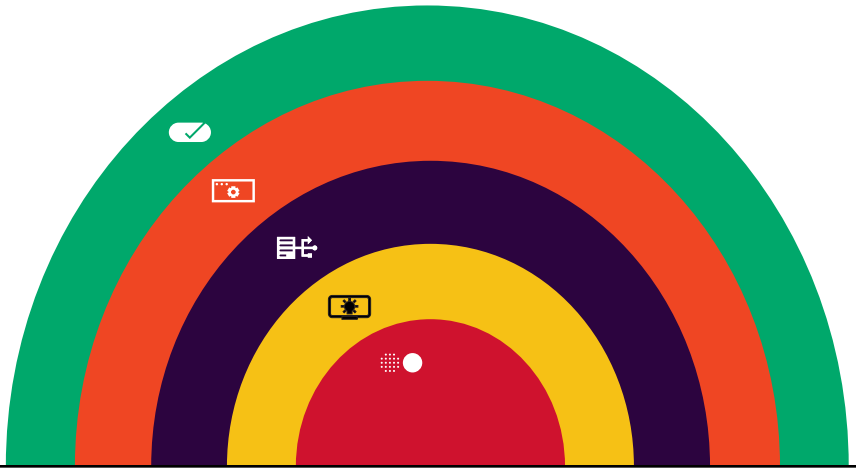
Ricoh delivers the tools and expert guidance today's organizations need to safeguard information and enable success. We do this with a strategic, multi-layered approach that governs information and covers potential vulnerabilities across all areas of business.

All our services, solutions, and devices are designed with a security-focused, data-driven approach, starting with security by design through implementation. Our industry-leading services — including consultancy and managed services — complement our device and solution security layers to optimize document, data, device, and information security.

Only when security is made a priority across many aspects of the organization can impactful and pervasive change in business transformation occur.

In this overview, learn how Ricoh uses a multi-layered approach to help organizations make security and compliance strategic to their business transformation.

- Workforce security
- Information security
- Device security
- Network security
- Application security



Layer 1 – Workforce security

Creating a secure work culture

In an age where cyber threats loom large over companies of all sizes, establishing a secured workforce culture is not just an IT concern — it's a business imperative. Organizations grapple with potential security breaches that can lead to financial loss, reputational damage, and regulatory scrutiny. Security experts know that while technology is a critical component of any security strategy, the human element cannot be overlooked.

Forging a security-first workplace and cultivating a secured organizational culture should be at the forefront of every modern organization's agenda.

The human factor: a vulnerability and an asset

While employees can be one of your greatest assets, they can inadvertently become vulnerable if not empowered with the right tools and knowledge to make smart and secure decisions. The crux of the issue is vigilance — maintaining it is as much about culture as it is about technology.

To minimize risk, it's essential to equip employees with:

- **Safe work experiences:** A seamless work environment that integrates intelligent tools and secured processes
- **Policies:** Clearly communicated information governance guidelines for accessing and handling data, and for reporting and remediation
- **Empowerment:** The capacity and confidence to identify and avoid potential security threats themselves
- **Alternatives to shadow IT:** Officially sanctioned and secured solutions that nullify the need for employees to find unsecured workarounds

Educating to empower

Cybersecurity awareness training is designed to extend an organization's security to those who often find themselves on the front lines. By making team members aware of the potential risks and educating them on best practices, employees evolve from potential liabilities into vigilant protectors of the organization's digital fortress.

Awareness training features:
- **Holistic training programs:** Ongoing education that evolves with emerging threats
- **Regular reinforcement:** Continuous prompts and refreshers that keep security top of mind
- **Effective strategies:** Leveraging anecdotes and scenarios that relate to employees' daily tasks
- **Knowledge assessment:** Tracking progress and testing comprehension to ensure readiness

A multi-layered approach to workforce security

Considering the multifaceted nature of cybersecurity threats, an overarching approach that spans security, privacy and business risk is crucial. This enables organizational leaders to:

- **Assess risk impact:** Gain a clear understanding of the potential repercussions of various threats
- **Identify vulnerabilities:** Proactively pinpoint weak areas in your security posture before they are exploited
- **Practice prevention:** Employ risk management strategies to reduce exposure to security breaches
- **Mitigate potential damage:** Develop an incident response plan and conduct regular training and drills
- **Stay current:** Maintain compliance with privacy regulations, industry regulations, insurance policies and other governance policies

By offering consultations and employing a governance framework influenced by best practices in risk and compliance, companies can build a robust, data-driven, and secure working culture. The end goal is a workforce that not only understands the mechanics of security threats but is also fully integrated into the fabric of the organization's defense mechanisms.

Building on trust

A secure work culture isn't just about defending against threats; it's also about nurturing growth and innovation within a framework of trust. When employees trust their work environment and have confidence in their organization's security policies, they are more likely to engage fully and responsibly with corporate resources and represent the brand with integrity.

The path to creating a secured culture is continuous and evolving. It requires commitment from every level of the organization, starting with the C-suite. By investing in training, incorporating best practices, and fostering a culture that values vigilance, organizations can not just defend against threats but can proactively shape a secure future.

Layer 2 – Information security

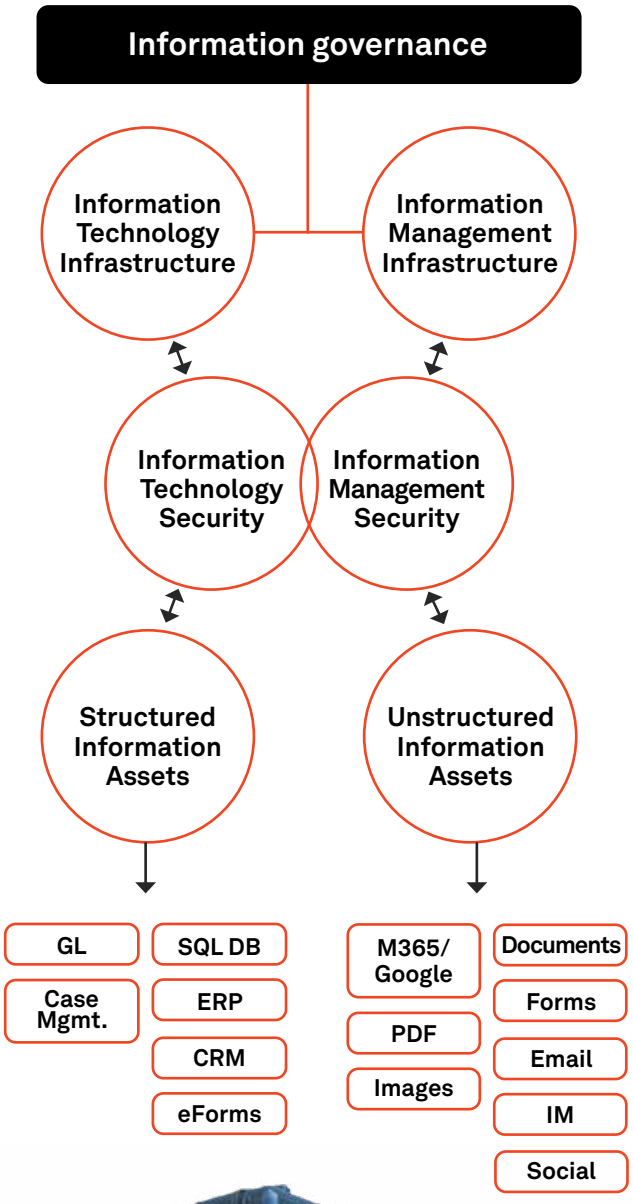
Protecting your information starts with knowing what you have, where it's located and the potential risk it could pose to your business. Turning raw data into classified, searchable, and actionable information enables you to uncover insights that empower better decision-making and implement appropriate levels of protection.

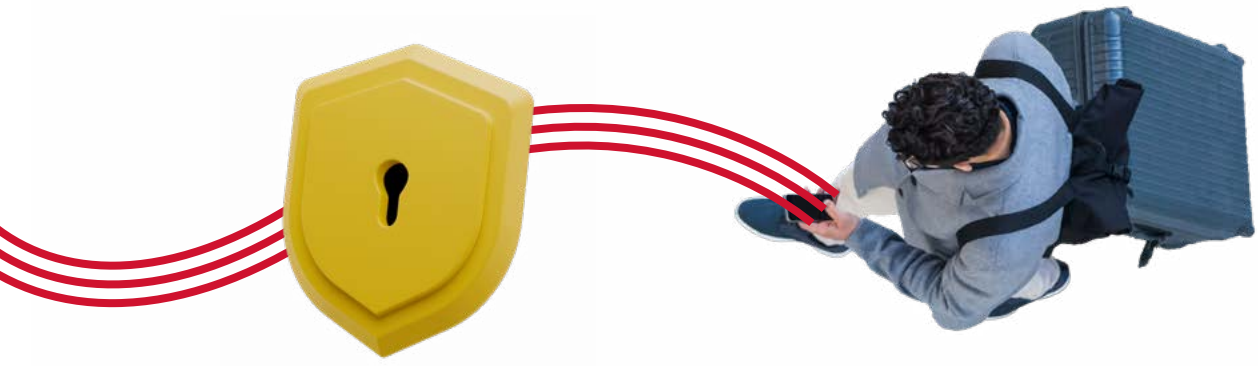
Information governance

Maintaining control of your information to maximize operations, safeguard against threats and ensure regulatory and legal compliance requires an overarching policy and program based on international standards. Information governance is the orchestration of creation, collection, management, retention and disposition of information across an organization.

The development of compliant information governance policies requires expertise from certified professionals, with practical guidelines developed to meet the needs of your business. Information governance services support organizations in meeting security policies and achieving compliance with a variety of federal, state, and industry regulations — including the ability to audit, demonstrate and defend compliance efficiently.

Every transaction between an organization and their stakeholders produces a trail of data. This may be highly sensitive, as with personally identifiable information (PII) or payment card industry (PCI) information, requiring security, privacy, and discovery controls. Other data has no value and simply takes up space, commonly referred to as ROT (redundant, obsolete or trivial) data. It is estimated that ROT data accounts for a minimum of 25-30% of an organization's data, with other sources saying it can be much higher.





90%+ of data is unstructured[1]

Unstructured data is information that hasn't been organized into a traditional, structured database format, which means it isn't accessible, tracked, or leveraged for business insights. Without managing your repository — most of which is unstructured — you're at risk of storing high quantities of ROT data and exposing your organization to risk and vulnerability if breached.

Unstructured data is a key contributor to security breaches, privacy violations, high IT costs, and compliance penalties. When considering cybersecurity, unstructured data is often the low-hanging fruit cyber criminals will target to gain access to deeper systems. They are looking for things they can monetize, such as names, addresses, dates of birth, social security numbers, passwords, credit card numbers, banking information, or contracts. Unfortunately, this sensitive data is often found throughout the infrastructure, making it difficult to track and keep secured.

Here are four key areas to mitigate risk through information governance:

1. **Records and information management program**
   Implementing a records information management (RIM) program ensures organizations can comply with regulatory and legal requirements while improving efficiency in access to information. Proper RIM practices, supported by a secured platform, help protect information through secure storage, access controls, encryption and audit trails, reducing the risk of security and privacy breaches.

   It's essential to establish governance policies, developed with certified records management experts, that encompass information across the organization, supported by practices and technologies that enable governance through the entire lifecycle, from collection to storage to disposition. By doing so, organizations can safeguard against breaches and maintain the integrity and confidentiality of critical data while bolstering trust and reliability.

2. **File analysis and classification tools**
   Data classification uses AI-based technology to categorize or index your documents so the data can then be easily extracted, exported, accessed, and protected. Implementing a system to classify your data can strengthen your security by reducing ROT data assets, proactively managing the lifecycle of your data, and ensuring compliance with privacy regulations. Data discovery also remediates data by restricting access, encrypting, archiving, redacting, or moving sensitive data to secured locations.

   It can also transform data generated from various physical and digital workflows into intelligence to enable better decision-making, more responsive customer service, and efficient operations. Ricoh security and process specialists have a deep understanding of information generated from print, mail and digital workflows as well as archiving and email security, so the right approach is applied when classifying your data.

3. **Expert-driven policy and implementation**
   Establishing an information governance policy with leadership-level endorsement provides a structured framework of controls and measures to effectively direct how information is handled. Governance helps mitigate organizational risk and ensures technologies and behaviors comply with legal and regulatory requirements. Once policies and guidelines are put in place, effective data protection procedures can be enacted across people, processes and technologies.

[1] IDC. "High Data Growth and Modern Applications Drive New Storage Requirements in Digitally Transformed Enterprises," July 2022.

Policies should cover information and records management, privacy controls and data security. Organizational guidelines will set out the procedures, workflows and safeguards through operational manuals and communications, with roles and responsibilities clearly outlined. A regular cadence for training is necessary as operations and regulations evolve. Enabling technologies can be implemented to enact controls, automate processes and measure, track and report outcomes.

4

Data lifecycle management policies and procedures

This security best practice seeks to mitigate an organization's risk through the management of data, including sensitive and valuable information throughout the entire information lifecycle. Ricoh professional services and managed services teams can assist in any step of this process.

Retention and disposal policies and procedures determine the lifecycle and handling of different classes of data. Retention policies can determine when and how data is moved from your active repositories into an archived state, moved into an off-site cloud repository, or expunged from systems as warranted by policy. Services for end-of-life disposal encompass cleansing data from multifunction devices to ensure that the NVRAM and drives of retired customer devices are wiped clean before disposal.

Business process automation

As the way we communicate, collaborate and create evolves, the need for secured and sustainable solutions becomes more apparent. The core of what we do — sourcing, creating, capturing, and managing information — is integral to success, and, therefore, must be protected from potential threats.

Automation has driven new ways of learning to work, improving efficiencies, delivering holistic analytics that enable informed decision-making, and integrating workflows for a more seamless experience.

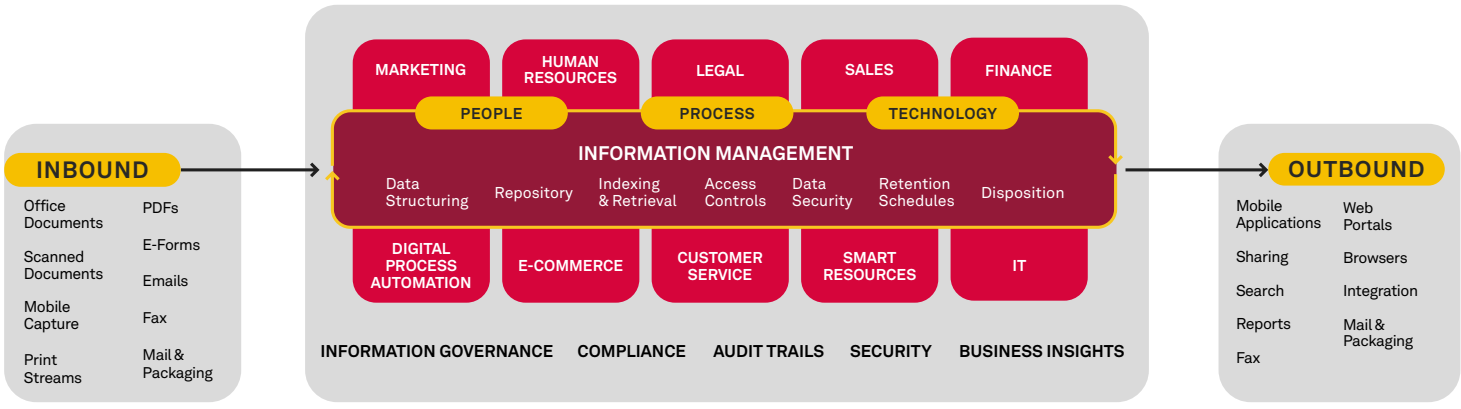
It also enables information controls, intelligent monitoring, tracking and rapid response to anomalies and threats, mitigating risks and improving compliance.

Implementing AI-driven technology can further enhance resilience while maintaining efficiency and productivity. Through analysis of historical data, AI can predict potential security risks by recognizing patterns in information and user behaviors. It also plays a role in encrypting information as it moves through the organization, using data masking techniques to protect information from interception.

Robotic process automation (RPA) provides organizations with a virtual workforce or bots that tackle repetitive business tasks, accelerating the way we work. RPA tools have their set of security standards with measures such as enterprise-grade encryption, role-based and permission access, Active Directory authentication, database encryption, and more.

The flow of information:

Capture, connect and secure information coming in, through and out of your organization



Inbound information

Inbound information such as email, mail, web form submissions, document scans, and e-commerce must be received and handled securely for any business process automation initiative. Integrating them with secured, automated workflows helps ensure data is safe and assists with information governance and compliance.

Digitized data requires focused protection from the point of origin and throughout its lifecycle. Digital and scanned documents, fax transmissions, form submissions, captured images, and other data enter your organization's systems through various methods, which warrants scrutiny of how you protect that valuable information.

Automating data capture, classification, extraction, and export can accelerate the flow of information, providing convenient access to those who need it. Controlling and governing access to information — especially sensitive information in digital formats — requires formidable security capabilities across multiple touchpoints.

Sensitive data can be personally identifiable information (PII), proprietary, intellectual property (IP), or fiduciary, among others, and can lead to hefty fines if not safeguarded. However, if the data is to be protected, it must be transformed from unstructured data into actionable, structured data. Let's explore how the following areas can protect your valuable data.

1 **Intelligent document capture processes**

Intelligent capture solutions transform documents into a structured, secured format so data can be exported into any workflow, application, or repository, such as ERP, ECM, CRM, RPA, iPaaS, analytics, or line of business system.

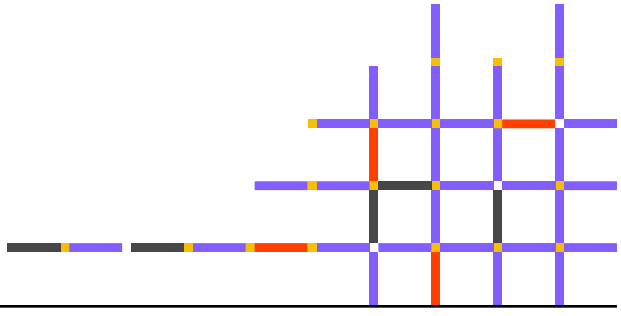
The documents must first be digitized or scanned. During the scanning process, authentication methods validate authorized users and administrators can lock down access to certain processes — even limiting what users can see — to prevent improper use. You can also protect converted files with permission settings and password control.

Most intelligent capture solutions do not store data; they simply pass the digitally transformed data through to other applications or repositories. Since information can be vulnerable to compromise if intercepted, security measures are used to protect data in use. Cloud services also make use of built-in encryption, decryption and authentication, as well as use Transport Layer Security (TLS) for transmission.

2 **Secure eForms**

Electronic forms provide a consistent way of submitting structured information into a system and can provide a secured option to the alternative paper or email approach. However, improperly coded or unprotected electronic forms can pose a security risk.

A form that has not been secured correctly can be a gateway to falsified information or attempts to introduce malicious code. Intelligent forms creation software can do the hard work for you, behind the scenes — constructing proper forms with features including electronic signature fields, location services, access control, attachment management and, most importantly, workflow management. Monitor and analyze your form-based workflows with full tracking of critical processes and approve or deny form submissions before they continue to their destination.



Outbound information

Securely managing large volumes of data while complying with regulatory controls and audits can be daunting. However, with the right technology and security in place to protect your data, remote and hybrid business processes and information can be optimized for growth and scalability.

How do you achieve this while ensuring your data is protected from outside threats, internal security breaches (accidental or deliberate), data loss, or compliance violations?

1. **Controlled print output**
   Multifunction printers bring efficient output to multiple users, along with the capability to protect printed information. Whether printing from desktop computers or mobile devices, outputting sensitive information remains in the authorized person's control. In addition, full-featured cost control tracking and chargeback provide comprehensive accountability of user behavior and a way to identify out-of-the-ordinary patterns or abuse.

2. **Secured document release**
   By incorporating Secured Document Release, sensitive information sent to centralized print servers or cloud services will not be picked up by mistake or by anyone seeking to steal confidential information. Instead of submitted print jobs going directly to a device, they are encrypted and held in the originating user's print queue on a secured server or in the cloud.

   The user can only release a print job when they are present at and logged into the device of their choice. The print queue can reside on-premises or in the cloud, and print data can be sent over a secured web connection and encrypted in transit.

3. **Mobile printing**
   With a changing workforce, mobile device printing is a critical capability in many organizations. Enabling this involves both process and technology infrastructure considerations. On the process side, users can prevent sensitive information from being left unattended at a printer by using authenticated print release with their mobile devices.

   Printer selection is handled on the mobile device, and output takes place when someone is present to securely release and retrieve the information. For infrastructure, you can protect print stream data and manage mobile printing processes with various deployment choices — depending on security policies. These can include both an on-premises mobile print server(s) or an off-premises mobile print cloud platform. Activity from mobile devices can be tracked alongside traditional printing with user/device detail reporting — so that mobile printing is tracked. Mobile device management can also be supported.

4. **Rules-based printing**
   Printing rules can include setting page limits by device, restricting color usage, enforcing duplex, restricting access to certain settings, and more. Budgetary account limits for copying and printing can be set up by the user — and include tracking walk-up activity at a multifunction printer.

   Preventing the misuse of resources reduces operating costs, restricts user activity to enforce accountability, and provides insight to spot irregularities through reporting.

   Because users must authenticate to print, the print rules you set are automatically enforced and activity is attributed back to the user. Users can associate document printing, scanning, and faxing to a specific client/matter/project for billing, which enables detailed activity reports around a project or confidential topic.

5 **Secured cloud printing solutions**

As hybrid work becomes more common, cloud printing is essential to ensure secured communication of information, reduce costs and keep workforces productive.
A combination of these security features should be considered with cloud printing:

- Zero trust
- Authentication
- Encryption
- Remote monitoring

6 **Cloud faxing**

Decrease the risks associated with stand-alone fax machines and replace manual routing with an automated delivery process. A safer method to get faxes into the hands of just the intended recipient often includes taking advantage of secured authentication, encrypted protocols, encrypting data at rest, and routing rules. This automation eliminates paper handling and reduces the risk of paper documents being picked up by unauthorized persons.

With administrative control over your fax environment, you can address compliance and policy requirements using several features — including verifiable document transmission and receipt, full audit trails of activity, and access to archived faxes of all inbound and outbound transactions.

Layer 3 – Device security

Security threats are no longer limited to personal computers, servers, or networks. Any device — even basic network printers — needs countermeasures against a diverse range of threats. As multifunction printers' (MFPs) functionality has evolved, they have become core IT assets. As the computing capability of what was traditionally categorized as "printer/copiers" has grown, so have potential threats, which can include:

- Malicious access via networks
- Tapping into and alteration of information over the network
- Information leaks from storage media
- Unauthorized access via a device's operation panel
- Improper access through fax telephone lines
- Information leaks via hardcopy
- Security policy breaches due to carelessness

Simply hoping you don't get hit is not the answer. Superior technology, diligence, and knowledge are essential, requiring a deep understanding of how to tackle potential issues caused by vulnerabilities in your devices, the data they process, and the networks to which they connect.

Device authentication

Controlling access by authentication according to your security policies is necessary. Healthy, secured devices can offer another critical level of security, including remote insight into device configuration, alerts related to usage and supplies, critical service alerts, and warnings for upcoming service issues.

1. **Device user authentication**
   The ability to track, control usage, and prevent unauthorized access is predicated on requiring users to authenticate before they can print, scan, fax, etc. Once logged in, users will only see the device functions and features they're authorized to use. Various authentication options give you the ability to control the level of capabilities granted to each user or group of users. This may include restricting the ability to change machine settings and view address book entries or granting access to scanning workflows, document servers, and other functions. In addition, the User Lock-out function — which triggers if it detects a high frequency of successful or failed login attempts — helps guard against Denial of Service attacks or brute force password cracks.

2. **Network user authentication**
   Ricoh devices support network user authentication to limit access to authorized users.
   For example, Windows® authentication verifies a user's identity at the MFP by comparing login credentials (username and password, ID badge with or without PIN, or a combination of both) against the database of authorized users on the Windows network server. In the case of access to the global address book, LDAP authentication validates a user against the LDAP (Light-weight Directory Access Protocol) server — so only those with a valid username and password can search and select email addresses stored on the LDAP server.

For customers utilizing SmartCards for authentication, such as U.S. Government Common Access Cards (CAC) or Personal Identity Verification (PIV) IDs, Ricoh offers solutions for enabling this type of authentication.

Software such as RICOH Streamline NX — a modular suite that covers scan, fax, print, device management, security, and accounting processes — provides additional network authentication options. These include authenticating against the LDAP, Kerberos authentication, and an available SDK for custom integrations.

3 **Device network authentication**
Many Ricoh devices support the IEEE 802.1X authentication protocol, which is frequently part of zero-trust architecture (ZTA) network implementations. This port-based network access control allows a network administrator to restrict the use of a network until a device has been properly authenticated. This ensures secured communication between authenticated and authorized devices.

Device protection

When machines aren't performing as expected, there are not only costs associated with downtime, but it can negatively impact other user behavior, which may include less-than-desirable workarounds.

Keeping device firmware updated can be accomplished remotely and in batches, and updates can be set to your schedule.

1 **Firmware and driver management**
Working with your service provider, organizations can maintain a line of defense by ensuring current firmware on your devices through proactive remote management. You can prevent printer device firmware from becoming outdated via a remote cloud portal. A device's firmware can be remotely checked, and an update can be immediately pushed. Or, updates can be performed automatically on a scheduled basis.

Refreshing firmware for large numbers of devices or across an entire fleet can be handled as a batch upgrade in moments. Drivers can also be pre-configured and pushed to devices remotely. You can package drivers with the appropriate defaults according to your print and security policies — and control who has access to different driver packages.

2 **Digitally signed firmware and applications**
If an MFP or printer's built-in software — also known as firmware — is altered or compromised, that device can then be used as a method of intrusion into the corporate network to damage the device or as a platform for other malicious purposes. Many Ricoh-designed devices include a Trusted Platform Module (TPM,) a hardware security module that validates the controller core programs, Operating System, BIOS, boot loader, and application firmware.

Ricoh MFPs and printers use a digital signature to judge firmware and application validity. The public key used for this verification is stored in an overwrite-protected, non-volatile region of the TPM. A root encryption key and cryptographic functions are also contained within the TPM and cannot be altered from the outside. Ricoh uses a Trusted Boot procedure that employs two methods to verify the validity of programs/firmware:

- Detection of alterations
- Validation of digital signatures

Malicious programs and firmware cannot be installed as packages lacking a verified digital signature cannot start. Covering the range of software from boot programs to end-point functions and applications, the Trusted Boot validation process provides comprehensive, TPM-based security. When updated firmware or applications are uploaded onto a Ricoh device, a similar process checks for a valid digital signature, and if not validated, updates are aborted and the update file is deleted. At that point, the device automatically reboots and will return to running with the previous firmware. In the unlikely event that firmware is altered in some other manner, Ricoh devices will prevent the execution of malicious firmware by halting the boot process and displaying a service call code.

3 **Disable unused protocols and services**

To make it easy to add network devices, many vendors' network-enabled systems are routinely shipped to the customer with all network protocols and services set to "enabled or active" — but unused services on network devices pose a security risk. Compromised ports can lead to various threats, including the destruction or falsification of stored data, Denial of Service (DoS) attacks and viruses or malware entering the network.

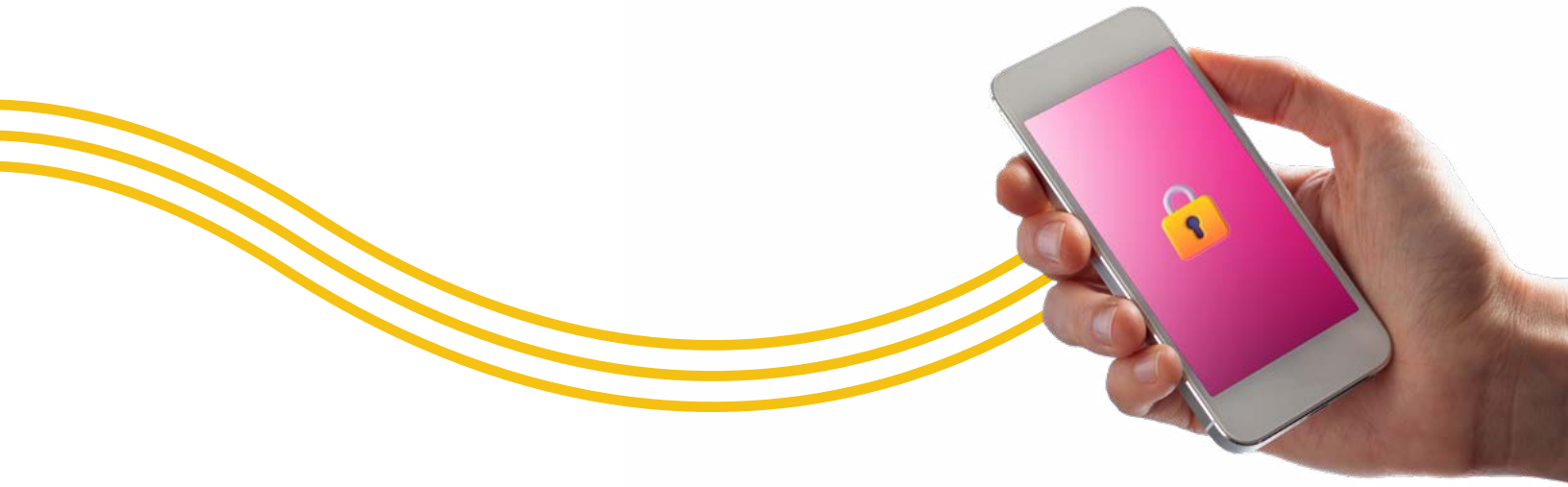
There is a simple but often overlooked solution for this particular risk source: disable all unrequired services. Ricoh device administrators can easily lock down unneeded services, helping to make devices less susceptible to hacking. In addition, specific protocols — such as SNMP or FTP — can be completely disabled to close off the risk of them being exploited.

4 **Access control**

The administrator can limit devices or protocols that can connect to the machine to avoid unintended access. Also, the administrator can select a security level at which to enable or disable a protocol and to configure the port status. They can block machine access and then allow it only from/to the IP addresses specified in reception/transmission filters. Up to five sets of filters, consisting of an IP address, a port number, and a protocol, can be defined for reception and transmission.

5 **Fax line security**

Enabling a device's fax feature may mean connecting it to the outside via a telephone line — which means that blocking potential unauthorized access via the analog fax line is critical. Ricoh embedded software is designed to only process appropriate types of data (i.e., fax data) and send that data directly to the proper functions within the device. Because only fax data can be received from the fax line, the potential for unauthorized access from the fax line to the network or programs inside the device is eliminated.



The Facsimile Control Unit (FCU) in Ricoh fax-enabled devices supports only G3 FAX protocols. Therefore, even if an initial connection is established with a terminal that does not use these protocols, the MFP will view this as a communication failure and terminate the connection. This prevents access to internal networks via telecommunication lines and ensures that no illegal data can be introduced via these lines.

6 **Simplify managing devices**

Managing devices can be time-consuming, and security gaps can emerge unintentionally when aspects of proper device management go unattended. Ricoh device management software, such as Streamline NX, gives IT managers a central control point to monitor and manage their fleet of network-connected print devices — whether spread across multiple servers or geographic regions — from a single management console.

Here's how Ricoh does it:

- SNMPv3-encrypted communications between devices and servers
- Central controls allow administrators to control access, monitor security settings, and manage device certificates
- Automated firmware update tasks reduce exposure from outdated firmware
- Deploy customer-approved firmware versions, or use the latest firmware available from Ricoh
- The Security Analyst feature for Streamline NX provides an at-a-glance dashboard for assessing device security policy compliance and offers a best practices checklist for whether devices are in policy

7 **Meters and alerts**

When an early warning enables teams to resolve a problem before it causes downtime, it helps reduce the risk of unexpected user behavior, such as unsanctioned workarounds. If machines are not operating as expected, users may choose a different, unsecured course of action. They may print or scan from a local device with no ability to audit activity or protect the data being moved.

Using monitoring and management software with devices lets you collect information and keep your device healthy with timely alerts. This includes automatic collection of meter data based on your set schedule, low/replace toner alerts, critical service alerts, and upcoming critical service issues.

8 **@Remote.NET**

Ricoh's @Remote Connector NX enhancement for Streamline NX collects approaching critical service alerts and communicates them directly to your service provider. Your provider can schedule remote firmware updates and push critical updates immediately. The @Remote Connector also collects device meters and makes them available on a pre-defined schedule — along with notifications of consumables levels — to maintain uptime and reduce administrative burden. The collected data is available via the @Remote.NET web portal.

9 **Physical port security**

On Ricoh devices, physical ports (USB, SD card, etc.) can be controlled by the device administrator, thereby preventing users from storing to or printing from external memory devices.

Types of encryption

1 **Drive and memory encryption (data at rest)**
If the drive is physically removed from a Ricoh machine, the encrypted data cannot be read. Once enabled, the drive encryption function can help protect an MFP's drive and non-volatile RAM against data theft while helping organizations comply with corporate security policies. Encryption includes data stored in a system's address book — reducing the danger of an organization's employees, customers, or vendors having their information misappropriated.

The following types of data — which are stored in non-volatile memory or on the drive of MFPs — can be encrypted:

- Address book
- User authentication data
- Permanently and temporarily stored documents
- Logs
- Network interface settings
- Configuration information

2 **Device network encryption (data in transit)**
As information moves through the network, a knowledgeable hacker can intercept raw data streams, files, and passwords. Without protection, unencrypted information can be stolen, modified, or falsified and re-inserted back into the network with malicious intent. To combat this, Ricoh uses encryption and robust network security protocols that can also be configured according to customers' needs. For example, the Transport Layer Security (TLS) protocol is used to help maintain the confidentiality and integrity of data being communicated between two endpoints. Many Ricoh devices support TLS 1.3, the most current version of that protocol.

3 **Print stream encryption**
Data sent in a print stream can be exploited if unencrypted and captured in transit. Ricoh enables the encryption of print data using Secure Sockets Layer/Transport Layer Security (SSL/TLS) via Internet Printing Protocol (IPP) — encrypting data from workstations to network devices or MFPs. Because this is a protocol that helps maintain data confidentiality, attempts to intercept encrypted print data streams in transit would only produce data that is indecipherable. Data sent to printers could be misused or attacked if it is not encrypted.

4 **End-to-end driver-based encryption**
Concerns about a malicious attack on print job data can be addressed using the Ricoh Universal Print Driver for end-to-end encryption of print data between the user's system and the Ricoh MFP. End-to-end encryption can be enabled in the print dialog so a user can set an encryption password. To release the print job, the user enters the encryption password at the Ricoh device, which then decrypts the data and prints the job. This method of print data encryption utilizes AES-256 encryption.

5 **IPsec communications**
Ricoh multifunction printers can use IPsec for encrypted communications. IPsec enables communications in units of secure packets at the IP protocol level. Even if no encryption is used by a high-order protocol or application, IPsec enhances security by preventing the communication content from being tapped into or altered.

More security features

1 **Locked print**
Printed documents sitting on the paper tray or left out in the open can be picked up by anyone. This puts the document's information at risk, and the potential impact grows dramatically when printing confidential documents. Ricoh locked print capabilities can hold encrypted documents on the device's hard drive until the document's owner arrives and enters the correct PIN code or network credentials. For even more capability, software such SLNX can provide full-featured secured document release — giving users options over their secured print queue while letting administrators maintain control.

2 **Copy data security**
Ricoh offers functions to thwart unauthorized copying of hardcopy documents — helping prevent possible information leaks. The copy guard function prints and copies documents with special invisible patterns embedded across the background. If the printed or copied document is photocopied again, the embedded patterns will become visible on the copies.

The unauthorized copy control function protects against unauthorized copying in two ways. Masked Type for Copying embeds a masking pattern and message within the original printout, safeguarding the information. If unauthorized copies are made, the embedded message appears on the copy. This might include the document author's name or a warning message. When the Ricoh device detects the masking pattern, the printed data is obscured by a gray box that covers all but a 4mm margin of the masking pattern.

3 **Compulsory security stamp**
Stamping documents with key identifying information can achieve greater accountability and management control. Mandatory security information print is a feature that forces key information — including who printed a document, when it was printed, and from which device — to be printed with a document. This feature can be enabled for copy, print, fax, and document server functions.

Administrators can select the print position and which types of information will be automatically printed on the output, which may include:

- Date and time the job was printed
- Name or login user ID of who printed the job
- IP address and/or serial number of the device used

4 **Temporary data removal**
When a document is scanned or when data is received from a PC, some may be stored temporarily on the hard disk drive or memory device. This can include scan/print/copy image data, user-entered data, and device configuration. This temporary data represents a potential security vulnerability.

The DataOverwriteSecurity System, built into most Ricoh devices, addresses this vulnerability, destroying temporary data stored on the MFP's hard disk drive by overwriting it with sequences of 1 and 0. Temporary data is actively overwritten and thereby erased each time a job is successfully completed.

The DataOverwriteSecurity System can also:

- Include options for National Security Agency (NSA) and Department of Defense (DoD) recommendations for handling sensitive information
- Make it virtually impossible to access latent data from copy/print/scan/fax jobs once the overwrite process is complete (the overwrite process can be selected from 1 to 9 times)
- Assist customers in their compliance with HIPAA, GLBA, FERPA, and other regulations
- Provide visual feedback regarding the overwrite process (i.e. Completed or In-Process) with a simple display panel icon

5 **Fax number confirmation**
People can easily make mistakes when entering a fax number directly on the keypad. Our engineers can set up the device so that the number needs to be entered twice or more for confirmation. If different numbers are entered, the transmission will not commence. This feature minimizes the risk of sending information to the wrong destination.

Independent security standards and certifications

Common Criteria is used internationally for the evaluation of information technology security. It is used for measuring whether security functions are appropriately developed for IT products. The Common Criteria Certification is a standard recognized by more than 25 nations of the world. Domestic and overseas multifunction copier vendors are eager to obtain authentication for digital multifunction copiers.

The Common Criteria Certification process verifies protection provided by multiple security technologies against various security threats. The certification covers, for example, system validity verification at the start, access control and logging, data protection by encryption and data deletion at machine disposal. Therefore, it helps protect our products from various threats — such as software alteration, invalid access, and information leakage.

1 **Protection Profile for Hardcopy Devices (PP_HCD_V1.0)**
PP_HCD_V1.0 is a U.S. government-approved protection profile for hardcopy devices such as digital MFPs. It was developed by the Multifunction Printers Technical Community with representatives from industry (including Ricoh), U.S. and Japanese government agencies, Common Criteria Test Laboratories, and international Common Criteria schemes. The purpose of this Protection Profile (PP) is to facilitate efficient procurement of Commercial Off-The-Shelf (COTS) Hardcopy Devices (HCDs) using the Common Criteria (CC) methodology for information technology security evaluation.

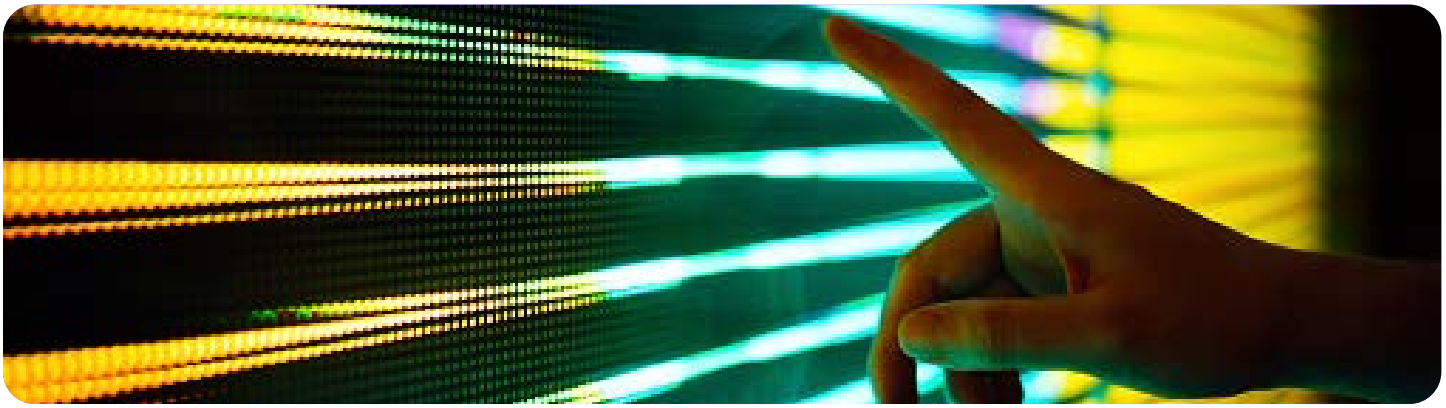
The following areas — which have been identified as among the most important for security protections — have been validated in most Ricoh devices to the PP_HCD_V1.0 standard and can be enabled:

- User identification and authentication systems
- Data encryption technology available for multifunction printers
- Validation of the system's firmware
- Separation of the analog fax line and the copy/print/scan controller
- Validation of data encryption algorithms
- Data protection

At Ricoh, our product line is constantly being enhanced to meet our customers' and regulators' changing requirements.

50+
Products with Common Criteria (ISO/IEC 15408)

Please visit the website for the complete list of Ricoh devices with ISO/IEC 15408 certifications.



2 **IEEE 2600.2**

The IEEE 2600.2 security standard pertains to hardcopy devices operating in a commercial information processing environment — with required levels of document security, network security and security assurance. It establishes a common baseline of security expectations for MFPs. To ensure that a device demonstrates conformance with the established standard, independent third-party laboratory tests provide verification of the manufacturer's security features. Ricoh offers a broad line of MFPs that have been certified as conforming to the IEEE 2600.2 security standard.

3 **FIPS 140-2/3**

The Federal Information Processing Standard (FIPS) 140-2/3 is a U.S. government security standard for validating cryptographic modules through the National Institute of Standards and Technology's (NIST) Cryptographic Module Validation Program (CMVP). Many cryptographic modules in Ricoh devices use algorithms that are recommended or approved by NIST, including algorithms validated under NIST's Cryptographic Algorithm Validation Program (CAVP). CAVP validation is a prerequisite for CMVP validation.

Customers can upgrade certain devices to a CMVP validated drive* and an MFP firmware upgrade that will incorporate CMVP validated modules elsewhere within the MFP**. Firmware-upgraded devices will implement certain device hardening measures — including turning off less secured ports, protocols and limiting some application use. When a machine is being returned at the end of its lease or lifespan, the Erase All Memory function can be used to remove stored data from various areas of the device.

* The FIPS 140-2 CMVP validated drive is available for many of our products.
** Firmware upgrade is available for selected devices.

Layer 4 – Network security

In today's fast-paced digital landscape, IT professionals are inundated with a growing array of responsibilities: delivering seamless work experiences — from anywhere — while supporting all lines of business, training and troubleshooting users, and ensuring networks, systems and data are protected. Everything in the work environment must be accessible, integrated, efficient, seamless and secured, including communications, file storage, applications, user identities, network, servers, email and more.

As threats evolve and attack surfaces grow, the margin for error grows. Robust, proactive cybersecurity is more critical than ever. Ricoh offers a large portfolio of IT services and solutions to enable seamless and secured digitalization across all areas of your business. Let's explore the options

Zero trust

In today's workplace, where users frequently work remotely and systems and data often aren't located within the physical office space, the boundaries that once defined what was inside and outside of the network have been blurred. A zero trust approach assumes threats can come from both outside and inside the network, which means it relies on verification and access controls for every user and device on the network.

1. **Multi-factor authentication**
   For years, organizations relied on credentials — a login and password — to authenticate a user and deliver access. However, cyber criminals have learned to steal credentials through targeted attacks such as phishing and keylogging, and, with the use of AI technology, they're able to crack even the strongest passwords in minutes. Introducing additional layers of authentication (multi-factor authentication or MFA) makes access more difficult for attackers.

2. **Identity and authentication management**
   Bringing a network into a unified platform, like Microsoft 365, facilitates zero trust security through powerful features such as centralized identity management, which enables consistent authentication policies across all services and applications. More granular access policies can be employed using conditional policies based on specifics such as location, users, devices, and risk level.

Security assessments

As organizations continually shift to hybrid work and allow users to regularly log into the network from outside the office or on unsecured devices, the need for securing access within the network has increased. Increased digitalization of processes means a larger volume of data in rest, motion, or use, exposing organizations to risk. That's where security and vulnerability assessments come in.

1. **Vulnerability assessments**
   A vulnerability assessment is comprised of two components:

   • Vulnerability scanning and reporting
   • Analysis and remediation planning

   Ricoh security engineers scan externally facing assets for vulnerabilities such as missing patches, outdated software versions, open ports, and operating system services. From there, we report the findings and develop a remediation plan tailored to the customer. Vulnerability assessments can be conducted regularly or as a point-in-time service.

2 **Penetration testing**
How secure is your data? The only way you can know for sure is to test your current security by trying to get in from the outside, the way a hacker would. Testing like this reveals where your network is strong — and where you require deeper security protection.

Penetration testing and assessments will uncover weaknesses in your networks, applications, and security controls. It can also confirm the effectiveness of the various security policies, procedures, and technologies.

Intrusion detection

Today's cyber threats are continually evolving, learning new ways to enter a network and wreak havoc — malware, ransomware and denial of service are some of the more popular exploits experienced by businesses of all sizes.

Intrusion detection is a game of cat and mouse, a continuous and dynamic struggle between attackers and defenders. As technology evolves, both sides adapt and develop new techniques to out-maneuver one another. As attackers innovate, defenders respond. Defenders detect, attackers evade.

1 **Firewalls**
Firewalls are designed to protect your network's infrastructure and improve site-to-site connectivity. Today's most advanced firewalls provide enhanced capabilities that allow real-time protection against malware, vulnerabilities, and network attacks. Intelligent analysis allows for deep application context, combining human and machine learning to apply rules specifically to allow or deny traffic.

2 **Anti-virus software**
Anti-virus software falls into three primary categories: signature-based, behavior-based, and machine learning.

- **Signature-based:** The signature method compares the code of a suspicious file to a database of known malware signatures. If there's a match, the file is immediately flagged and blocked, contained, or deleted.

- **Behavior-based:** This software analyzes the behaviors of a file (such as rapid encryption), which enables it to discover new malware it hasn't seen before. Because cyber criminals are constantly evolving and developing new strains of malware, this provides much stronger protection than signature-based solutions.

- **AI-based:** Machine learning-based software is the latest and most robust type of anti-virus protection, applying algorithms and datasets to detect malicious patterns in malware on individual devices and across large networks.

3 **Ransomware containment**
The days of 'set it and forget it' antivirus installations are long over with the introduction of sophisticated, malicious attacks such as ransomware, which requires a combination of prevention and mitigation. Preventative solutions detect ransomware signatures and behaviors, stopping them from getting past the perimeter. But as cyber criminals use increasingly sophisticated tactics, a second line of defence is necessary.

Ransomware containment stops illegitimate encryption at the source, isolating and containing it to prevent further spread. Ransomware containment is a critical last line of defence to an organization's security infrastructure, filling the perilous gap between devices and file shares where organizations often lack the essential defences.

Endpoint management

Being prepared starts with embedding intelligent cybersecurity services and solutions into your core business Endpoints are today's most common entry points for malware, ransomware, deep fakes, and social engineering. If a cyber criminal gains access to one of your endpoints, they can potentially find ways to burrow further into the network to access sensitive data or launch large attacks.

1. **Web filtering**
   Providing protective security and content filtering minimizes risks and maximizes safety as a critical component of defense. Filtering is commonplace for email, tools often referred to as anti-spam, email security, or email filtering. While providing email protection is important, it is only half the filtering solution.

   Managed web filtering is designed to block malicious domains that may include harmful content such as ransomware, malware, viruses, and data phishing. Optionally, specified content types may be blocked based on individual business needs to prevent access to domains that may contain adult, gambling, crypto mining, dating, or other prohibited content.

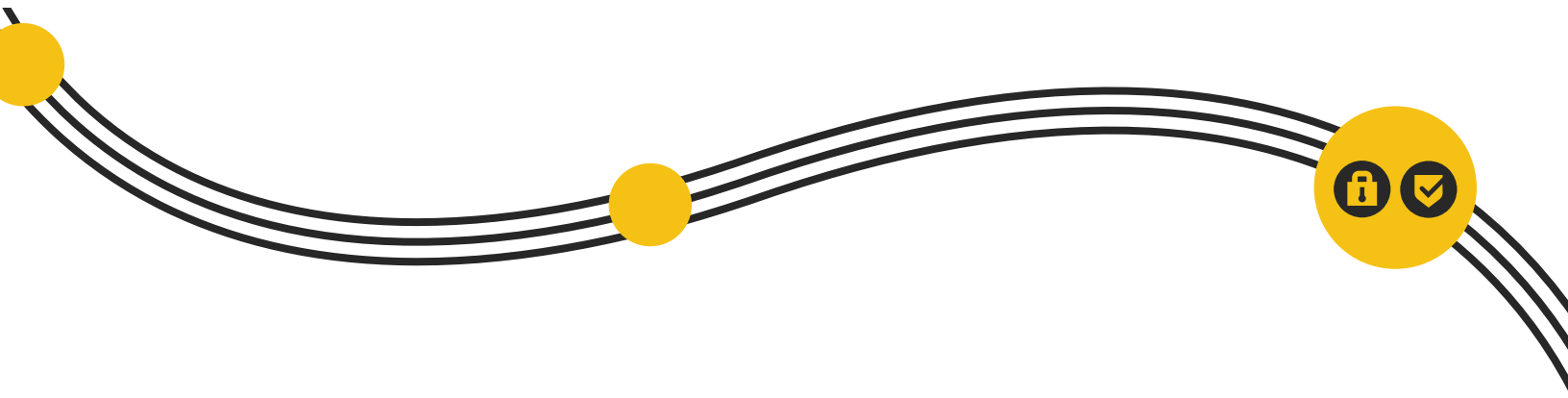
2. **Mobile device management**
   Mobile device management applications such as Microsoft Intune enable rapid deployment and application management on mobile devices, limiting data migration. It can be leveraged when securing an entire mobile device, also protecting against malware and enabling complete removal of company data in the event of a threat or employee departure.

Expert cybersecurity management services

Being prepared starts with embedding intelligent cybersecurity services and solutions into your core business processes and ensuring rigorous management by IT cybersecurity experts.

Continuously evolving threats require uncompromising and focused management of systems, devices, and environments. IT teams are under more pressure than ever to maintain operations, enable lines of business, and deliver user support. Outsourcing your cyber protection to a dedicated team of experts will free up your IT department to focus on core capabilities without their attention being diverted. A distracted, overwhelmed IT team invariably leads to gaps in security, with potentially disastrous outcomes.

Ricoh's expert-driven cybersecurity services and solutions can help you build a more resilient IT infrastructure, understand and manage your vulnerabilities, and enable you to grow with confidence.



Layer 5 – Application security

While software is designed to accelerate efficiency and productivity, it can also pose risks. Embedded software applications, installed apps, and software running as cloud services can be potential targets for breaches. Therefore, your data must be protected.

Many of the attacks perpetrated by cyber criminals are performed using software vulnerabilities. Software vulnerabilities are usually programming mistakes, design oversights or outdated scripts that leave web applications, web services or websites to be exploited on the dark web.

Steps for ensuring applications are secured:

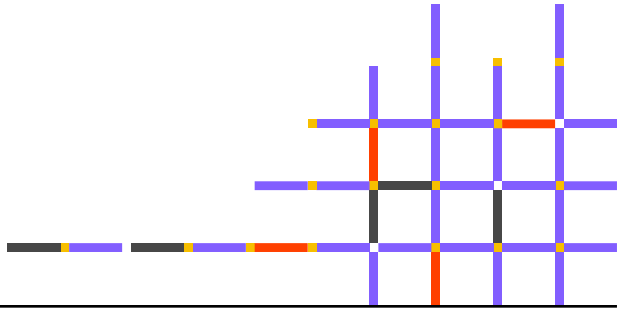
1. **Security by design**
   Applications should employ security by design, a development approach that aims to protect against cyber attacks. When implementing new applications, it's advisable to inquire about the developer's compliance with international standards such as ISO 27034.

   Ricoh practices security by design based on ISO/IEC 27034-1:2011, which considers security throughout the lifecycle of products and services from the planning and design stages. We offer various software and embedded solutions for IT systems, business process management, and multifunction devices and printers.

2. **Secured integrations**
   Secured application programming interfaces (APIs) are an integral part of an organization's IT infrastructure, enabling seamless communication between applications and systems. An API is the layer between third-party applications and your organization's data and systems, facilitating the movement of data between. Poor security management introduces what is essentially an unlocked gate to various cyber threats.

   Ensuring traffic is encrypted, maintaining a regular schedule of vulnerability scans and updating and patching, and ensuring data is encrypted at every layer is critical.

3. **Secured data**
   When working with a SaaS vendor, it's important to understand where your data will be hosted, who has access, and what controls are in place to protect it. One essential question to ask, particularly if the application will be storing sensitive data, is if the vendor has any security certifications, standard practices and controls.



4 Application security best practices

To protect against damage resulting from malicious third parties, system administrators should consider the following:

1. Read the entire license agreement for each software and embedded solutions. To continue use, you must agree to the terms.

2. Confirm your operating system and/or device firmware is the most recent version before installation and operation. Install and operate software and embedded solutions on a network protected by a firewall. To avoid inherent risks, it's suggested not to connect software and embedded solutions directly to the Internet.

3. Limit access to software and embedded solution products to only authorized users and limit access to the software and embedded solution products by access control and allowing only approved IP address ranges.

4. To prevent unauthorized access by malicious third parties, change the default administrator password for the software and embedded solution products and operating system.

5. Confirm software, software operating system, embedded solutions, and multifunction printer or printer are configured correctly to meet your desired workflow and follow your company's security policy.

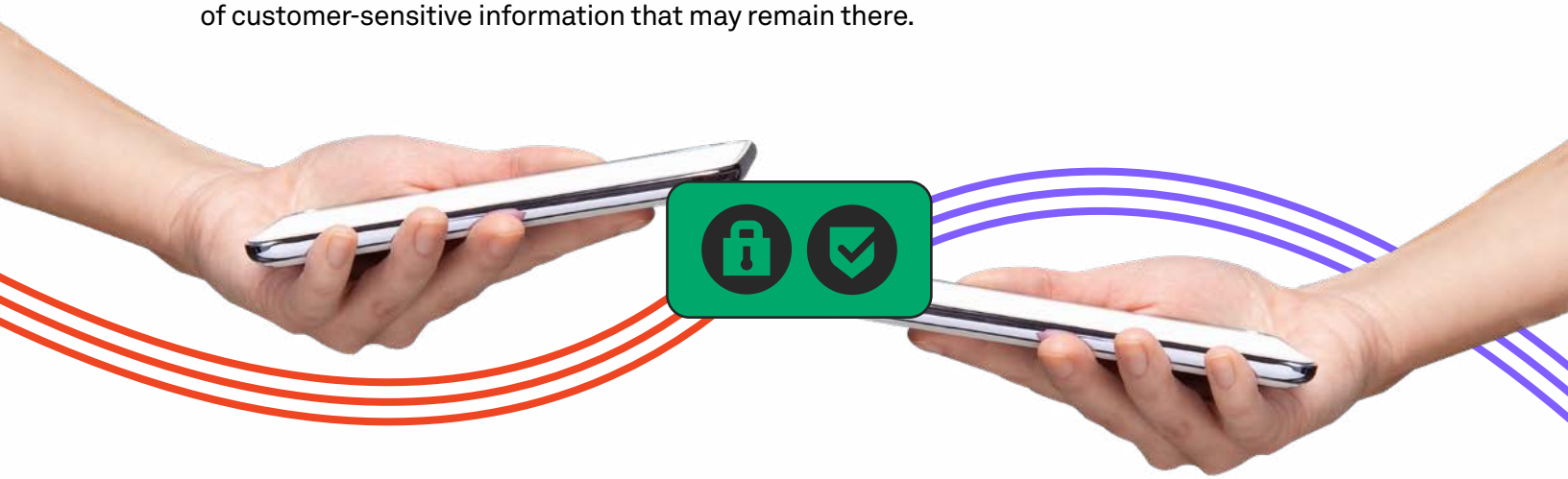
6. Multifunction printer and printer security settings should be appropriately set according to the details described in the multifunction copier or printer instruction manual or as customer policies state.

7. Use encryption for all data in transit. Furthermore, certificates should be signed by either a company-hosted or public third-party Certificate Authority. Inherent risks exist if using self-signed certificates.

8. Instruction and training should be given to people who use the software and embedded solutions.

9. To limit outside threats, ensure browser security is enabled on computers used to manage software and embedded solutions. Additionally, do not use the same browser or browser session to manage/access software and embedded solutions while accessing outside network resources at the same time. Completely log off any software and embedded solutions before accessing outside network resources.

10. For software and embedded solutions that are discontinued, uninstall the software and remove any personal or sensitive data used in previous workflows. This will prevent leakage of customer-sensitive information that may remain there.

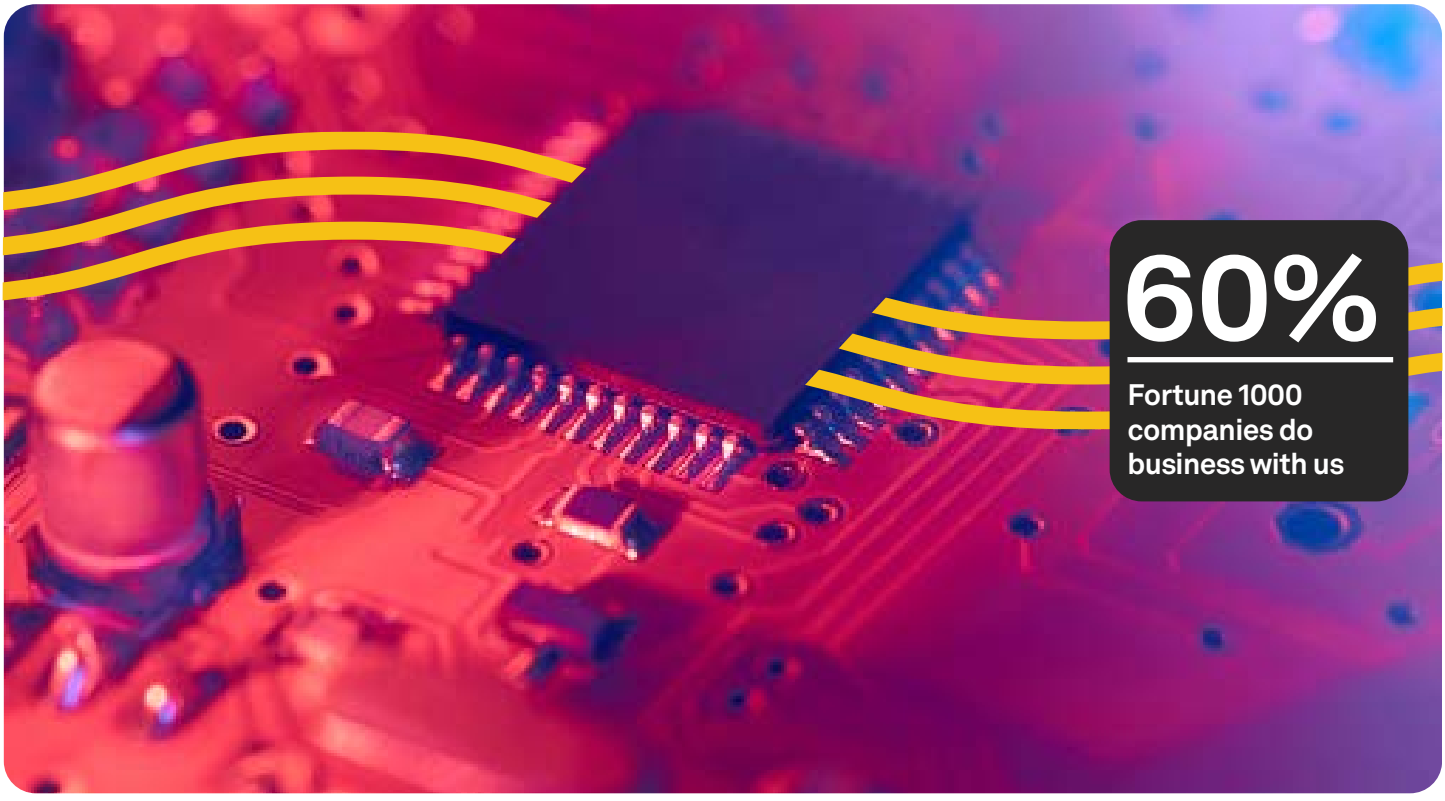


Strategic guidance and support

Security consultations
Transform your business strategy from reactive to proactive by implementing security by design policies and plans. Ricoh's virtual technology consultants and security specialists can help you build a comprehensive security strategy that's assessed, tested, and retested before disaster strikes. Our approach, based on governance, risk, and compliance best practices, quickly identifies vulnerabilities for security breaches, gaps that can result in cyberattacks, and other internal technology exposures before they impact your business.

Information governance consulting
Many organizations struggle with several aspects of information management, such as security and privacy, retention and disposition, legal and regulatory compliance, reliability, and authenticity. Ricoh's Information Governance (IG) consultants address these aspects, helping organizations break down silos and establish long-term, sustainable programs. We look at information as both the problem and the solution and take a proactive approach to your information challenges, setting your organization up for success to make sound business decisions.

Nationwide and global technical support
Ricoh has established Technology Centers in every region to provide technical support to our customers around the globe, responding to their needs quickly and efficiently. The Ricoh Global Services team provides standardized, consistent, end-to-end solutions. With coverage in about 200 countries and territories worldwide, Ricoh employs over 9,000 service delivery and technician professionals. Our unrivaled direct sales and dealer partner support network has the capability to do business with 60% of Fortune 1000 companies — which means that you can rely on one partner for all your global needs. By having offices and service delivery professionals in so many countries worldwide, we can respond quickly to customer requests.



Security support documentation
Ricoh provides technical documentation to support our customers' information security requirements — including Common Criteria Validation Reports and Certificates for select product offerings. This documentation provides independent third-party validation of security claims and can be provided upon request. In addition, security white papers covering device and network settings and the Device Security Administrators Guide required by Common Criteria are also available to customers. These guides provide detailed information about how Ricoh equipment communicates data inside of the device and how the device interacts with the network. Click here to see more documentation.

End user and administrator training
Maintaining a high degree of vigilance and adhering to security best practices involves more than just technology — it involves people. Ricoh offers training on our devices — and third-party partner vendors — aimed at both end users and administrators. With the right knowledge at their fingertips, your team can understand available security capabilities and learn how their appropriate use can help your organization protect its information and comply with regulations.

Ricoh's security commitment
Security is ingrained in our values — a commitment we do not take lightly. Whether you're stuck in a data deluge, work in a highly regulated industry, lack resources or experience, or want the assurance of utilizing highly secured services, software, and devices, we aim to gain your trust by having the highest security standards in the industry. Our goal is to stay ahead of cyber criminals — and if they do encroach into our systems, we have a plan and systems in place to mitigate a breach.

Our pledge to every customer is to adhere to current security standards and guidelines in our products and services, work diligently to protect our customers' data, and enable them to protect themselves. We commit to always evaluate, learn and innovate with every initiative, looking toward the best future for our customers and partners.

Information security threats are becoming more advanced and stealthier every day. Ricoh is committed to offering secured products that protect your information assets and harmonize with your office environment and security policies. Ensuring security requires correct settings and implementation in your specific environment.

Our depth of experience and multi-layered approach can be leveraged across your organization from strategy, devices, software, services, support, training, and more. Let us help you in your digital information services journey.

RICOH
imagine. change.

Ricoh, a trusted partner

At Ricoh, we're empowering our customers to respond to our changing world with actionable insights. We believe having access to the right information translates to better business agility, more human experiences, and the ability to thrive in today's age of hybrid and borderless work. Through our people, experience, and solutions, we create a competitive advantage every day for over 1.4 million businesses around the globe. To us, there's no such thing as too much information.

Have questions? Visit ricoh-usa.com or contact a Ricoh security expert today.

RICOH
imagine. change.