Ricoh Security Overview

RICOH
imagine. change.

Wondering if your devices are vulnerable?

Security threats are no longer limited to personal computers, servers or networks. Printing devices — even basic laser printers — need countermeasures against a diverse range of threats. As multifunction printers have evolved into true information terminals, they have become core IT assets in their own right. The computing capability of what have been traditionally categorized as "Printer/Copiers" has grown, but so too have potential threats — which can include:

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

Simply hoping you don't get hit is not the answer. Superior technology, commitment and know-how are essential. Ricoh can help you tackle potential issues caused by vulnerabilities in your devices, the data they process and the networks to which they connect.

Ricoh's layered approach

At the heart of our security model is the device itself. The Operating System (OS) at the core of our current Ricoh-designed devices has been specifically engineered and hardened by Ricoh for our equipment, and many of our MFP device models are certified to the IEEE 2600.2 Standard Protection Profile for Hardcopy Devices. Hard disk encryption and disk overwrite security come standard on some of our devices and help ensure that processed data remains confidential. Ricoh has worked hard to ensure that device security is not weakened by the introduction of the Smart Operations Panel — which also uses a Ricoh-only OS. Ricoh does not install unnecessary components, and root access is not available. Embedded applications must pass Ricoh Compatibility testing and be digitally signed before they can run on the Smart Operation Panel. Ricoh is commited to working with our customers to deliver products and services that are in sync with your IT and network security policies. We use a number of techniques to help protect against "man-in-the-middle" or "inside job" threats — including end-to-end encryption of print and scan files, encryption of data on servers and segregation of administrator duties. An industry leading range of security services — including consultancy and managed services — wraps around the other layers to monitor, optimize and effectively manage document and information security.

Embedded applications

- Providing extended features
- Tested, compatibility certified and digitally signed by Ricoh
- Examples: Authentication, secure print, encryption, workflow

Network (transport & data link layer)

- Leverage and comply with customer's network security policies and measures
- End to end encryption of scan and print files to protect against "man in the middle"

User interface (Smart Operation Panel)

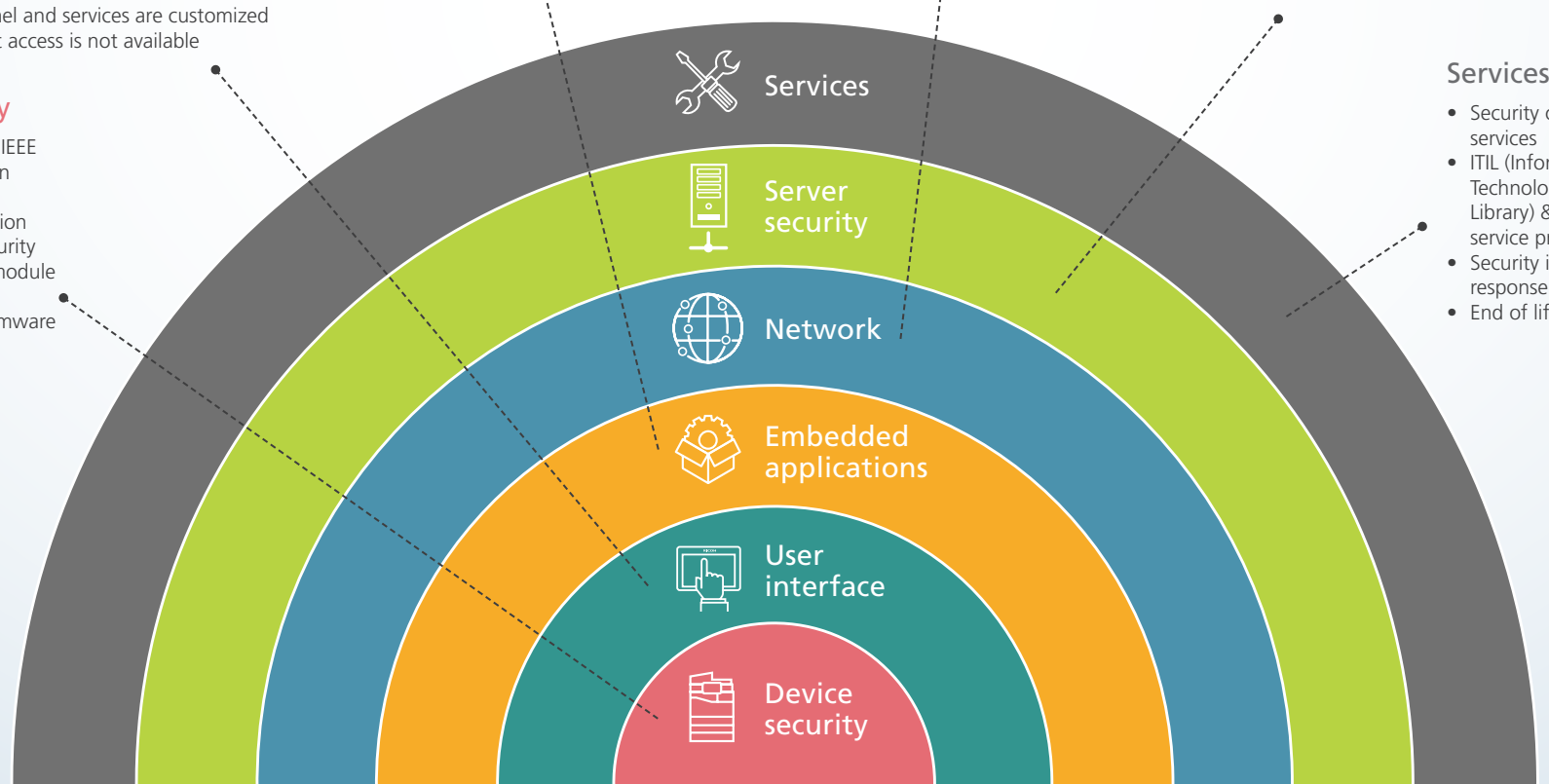
- Ricoh hardened OS based using specific modules
- Unnecessary tools and components, tools with known issues are not installed
- Kernel and services are customized
- Root access is not available

Server security

- Leverage and comply with customer's server security policies and measures
- Encrypted files
- Segregation of administrator roles

Device security

- ISO / IEEE 15408 / IEEE 2600.2 certification
- Ricoh-only OS
- Hard drive encryption
- Disk overwrite security
- Trusted platform module for secure boot
- Digitally signed firmware updates

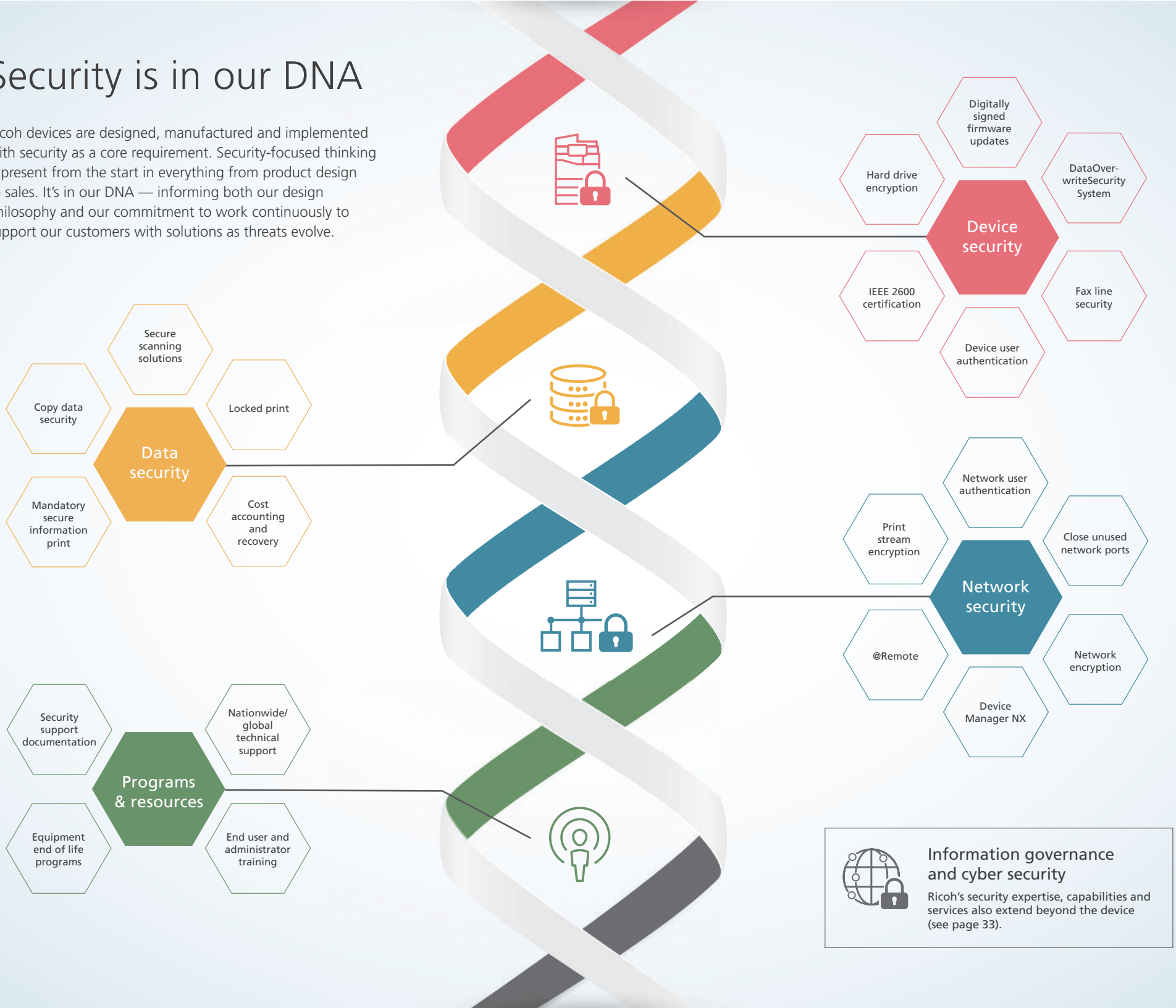


Services

- Security optimization services
- ITIL (Information Technology Infrastructure Library) & ISO certified service processes
- Security incident & response team
- End of life disposal services

Security is in our DNA

Ricoh devices are designed, manufactured and implemented with security as a core requirement. Security-focused thinking is present from the start in everything from product design to sales. It's in our DNA — informing both our design philosophy and our commitment to work continuously to support our customers with solutions as threats evolve.



Information governance and cyber security

Ricoh's security expertise, capabilities and services also extend beyond the device (see page 33).

Device security

Our device security capabilities can help protect multifunction devices and laser printers from potential threats — including compromising firmware, a device's hard disk drive, non-volatile memory, open network ports and system of authentication. Ricoh has obtained certification for a wide range of products based on Common Criteria (ISO/IEC 15408). On devices undergoing Common Criteria certification, security functions are tested by independent third-party government-licensed laboratories to ensure security features perform correctly and conform to standards set by both government and industry.

As part of our ongoing commitment to prevent your important information assets from being exposed to threats, we develop and offer security features and products to help protect your electronic and hardcopy documents — without hindering user-friendly processes and productivity.

Unsecured firmware can be compromised

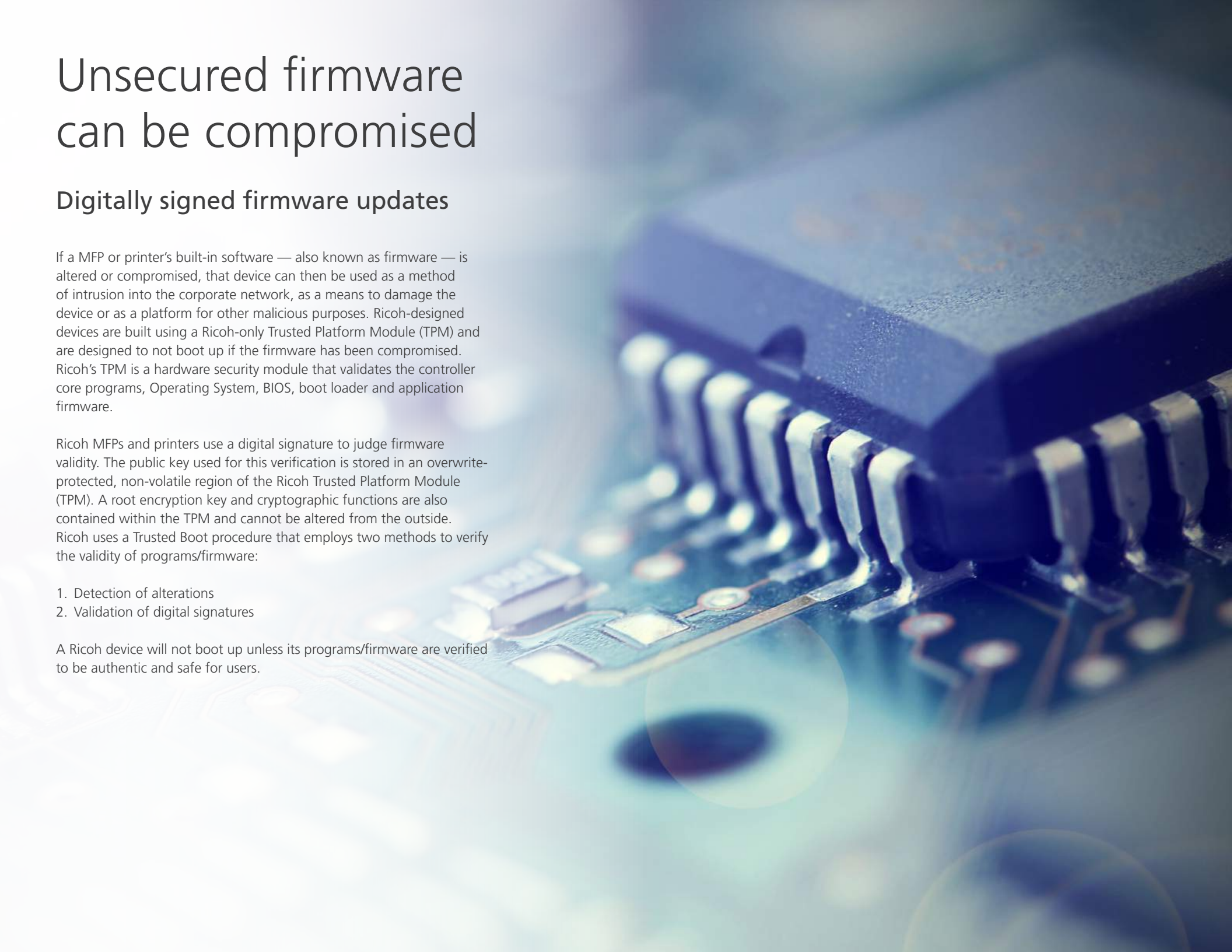
Digitally signed firmware updates

If a 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, as a means to damage the device or as a platform for other malicious purposes. Ricoh-designed devices are built using a Ricoh-only Trusted Platform Module (TPM) and are designed to not boot up if the firmware has been compromised. Ricoh's TPM is 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 validity. The public key used for this verification is stored in an overwrite-protected, non-volatile region of the Ricoh Trusted Platform Module (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:

1. Detection of alterations
2. Validation of digital signatures

A Ricoh device will not boot up unless its programs/firmware are verified to be authentic and safe for users.



Temporary data is vulnerable data

DataOverwriteSecurity System (DOSS)

When a document is scanned or when data is received from a PC, some data 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 — or "latent" — data represents a potential security vulnerability.

The RICOH DataOverwriteSecurity System (DOSS) closes this vulnerability, destroying temporary data stored on the MFP's hard drive by overwriting it with random sequences of "1's" and "0's." Temporary data is actively overwritten and thereby erased each time a job is executed.

- Conforms to National Security Agency (NSA) and Department of Defense (DoD) recommendations for handling classified information
- Makes it virtually impossible to access latent data from copy/print/scan/fax jobs once the overwrite process is complete (overwrite process can be selected from 1 to 9 times)
- Works with the RICOH Removable Hard Drive (RHD) security system, providing a multi-layered approach
- Assists customers in their compliance with HIPAA, GLBA and FERPA requirements
- Provides visual feedback regarding the overwrite process (i.e. Completed or In-Process) with a simple display panel icon

Encryption protects against data theft

Hard drive encryption

Even if the hard drive is physically removed from a Ricoh machine, the encrypted data cannot be read. The hard drive encryption function can help protect a multifunction printer's hard drive 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 and potentially targeted. The following types of data — which are stored in the non-volatile memory or hard disk drive of multifunction printers — can be encrypted:

- Address book
- User authentication data
- Stored documents
- Temporarily stored documents
- Logs
- Network interface settings
- Configuration info

Ricoh provides hard drive encryption using Advanced Encryption Standard (AES) methodology to 256 bits.

Is your fax line providing a way in?

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 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 to programs inside the device is eliminated.

Ricoh utilizes a number of methods to help secure fax operations:

- The Fax Controller only contains a fax modem and not a data modem, so all communication is via the G3 fax protocol.
- Image data is not saved to the Engine Controller Page Memory or Temporary Storage Area — making it impossible to access this data from the Fax Controller.
- Data stored in the Engine Controller Page Memory or the Temporary Storage Area is sent only to the Printing Unit.
- There is no active connection between the Printing/Scanning Video Buses and the Engine Controller — making it impossible to access data stored in the Engine Controller Page Memory or the Temporary Storage Area from the Fax Controller.
- Page Location data is erased at the completion of every job.

Independent security certification

IEEE 2600

The IEEE 2600 security standard defines the minimum requirements for security features used by devices that require a high level of document security — establishing a common baseline of security expectations for both MFPs and printers. To ensure that a device demonstrates conformance with the established standard, an independent third-party laboratory tests and provides verification of the manufacturer's security features.

These areas — which have been identified as the most vulnerable for possible data breach — have been validated in many Ricoh devices to the IEEE 2600 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 overwrite security operation

Ricoh offers a broad line of MFPs and printers that have been certified as conforming to the IEEE 2600 security standard — and our product line is constantly being enhanced to meet our customers' changing requirements.

Control access and reduce risks

Device user authentication

Authentication features enable authorized users to access a Ricoh multifunction printer, while preventing access for those without proper credentials. Ricoh also gives 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 particular 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 a denial of service attack or brute force password crack.

Authentication methods include:

- Basic Authentication — Users enter a user name and password, which are registered locally in the multifunction printer's address book.
- User Code Authentication — Users enter a code of up to 8 digits, which is compared to the registered data in the address book.
- Windows/LDAP Authentication — Access to Ricoh multifunction printers can be linked with Windows® domain controllers and LDAP servers.
- Card Authentication — Instead of entering a user name and password, a user holds a properly registered card over an optional card reader for authentication.
- Common Access Card (CAC) Authentication — The Common Access Card is a U.S. Department of Defense specialized ID card-based authentication system, designed for government users that must be compliant with Homeland Security Presidential Directive 12 (HSPD-12).
- Personal Identity Verification (PIV) — Personal Identity Verification is the civilian version of the CAC card.
- SIPRNet Token Authentication Solution — SIPRNet Token is a variation of the CAC ID, designed for controlled networks.

Data security

It's easy to accidentally leak information. A document left on the tray of a multifunction printer can become a security risk just as easily as a misappropriated digital file or the impact of human error. Ricoh multifunction printers help protect your data whether you're printing, copying, scanning or faxing. Ricoh's data encryption system — which uses a RSA BSAFE Crypto encryption module and is FIPS 140-2 validated — helps protect your data both when it is in transit and when it is at rest.

174 million

digital records were compromised by data intruders in 2011 — a more than 4,000% increase over 2010.*

*Verizon® 2012 Data Breach Investigations Report

Ricoh helps protect your data with technologies and features that are designed to support security policies, guard against misuse or carelessness and encourage compliance through accountability.

Protection for digitized documents

Secure scanning solutions

The process of digitizing hardcopy documents and routing the resulting electronic files — whether to backend systems or via email — can be a point of data compromise if not properly secured. Scanning processes, though designed to be easy for users, should also deliver robust protection for routed digital information. This starts with restricting access. Limit scanning operations to authorized users only with several authentication options — including via network login, optional Kerberos authentication or single sign-on via card.

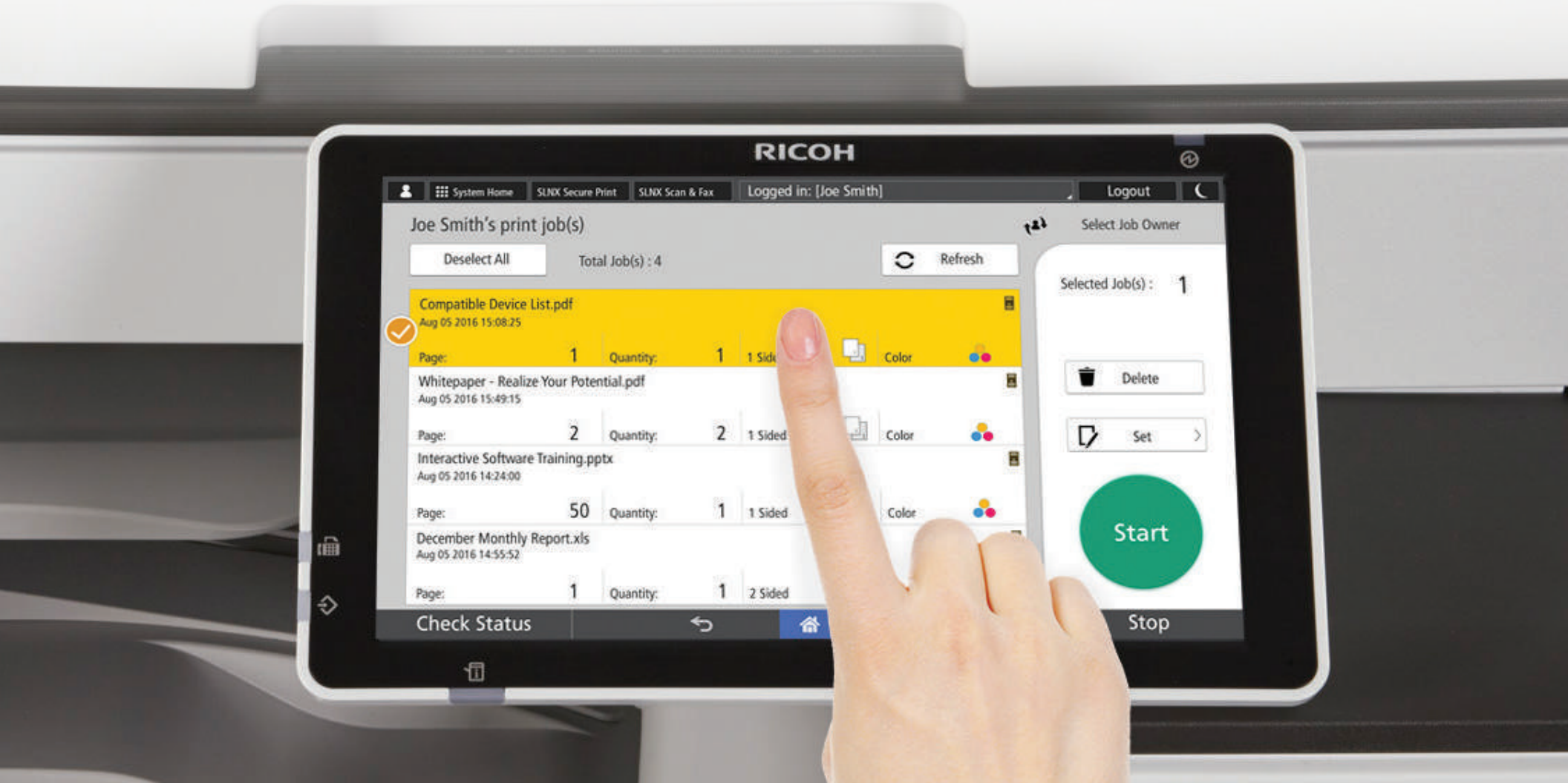
Encrypting scan-to-email communications helps reduce the risk of information compromise. Send email messages using public key cryptography and a certificate of user verification that has been registered in the scanning device's address book. You can also prevent email spoofing and message alteration by attaching an electronic signature that uses a secret key, based on a device certificate.

Ricoh-designed multifunction printers, copiers and scanners are equipped with Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols and can utilize strong encryption algorithms (256-bit AES and SHA-2) — as well as provide audit trails and administrative control.

Unattended prints can leak information

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. In addition to this driver-based locked print function, Ricoh also offers enhanced locked print — which is tied to user accounts and can be coupled with card authentication. For even more capability, software such as RICOH Streamline NX (pictured) can provide full-featured secure document release — giving users options over their secure print queue while letting administrators maintain control.



Protect against unauthorized copying

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. If unauthorized copies are made, the embedded message appears on the copy. This might include the document author's name or a warning message. Data Security for Copying helps safeguard the information itself. 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.

Anonymous documents are difficult to control

Mandatory secure information print

Stamp documents with key identifying information for 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

Secure devices against misuse

Cost accounting and recovery

Uncontrolled use of imaging equipment can lead to unanticipated expenses and potential violations of company policies. Ricoh cost accounting and recovery software tracks usage down to the individual and automates the process of allocating costs back to users or departments. Create greater accountability by establishing user quotas and budgetary account limits. Establish user permissions to restrict access to certain features based on need — for example, the ability to print in color. Controlling who can use equipment via authentication and designating what they can or cannot do reduces opportunities for misuse and provides useful management insight.

Network security

Multifunction printers exchange critical information with computers and servers over networks. If left unprotected, this information is at risk of alteration by those with malicious intent who would tap into the network. Ricoh products and technologies offer features that can help protect against unauthorized access via networks. Employed techniques include encryption of network communications and print streams, network user authentication and a host of administrative countermeasures — such as closing network ports and proactive device management.

Ricoh's security features can help reduce the risk of network exploitation or information leakage stemming from a breached multifunction printer or device.

Unauthorized users can be a threat

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 multifunction printer by comparing login credentials (user name and password) 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 user name and password can search and select email addresses stored on the LDAP server.

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.

Make devices “invisible” to the outside

Close unused network ports

In an effort to make it easy to add network devices, many vendors’ network-enabled systems are routinely shipped to the customer with all ports set to “open” — but unused open ports on printers and MFPs pose a security risk. Compromised ports can lead to various outside 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: close the ports. Ricoh device administrators can easily lock down unneeded network ports — helping make devices virtually “invisible” to hacking. In addition, specific protocols — such as SNMP or FTP — can be completely disabled to close off the risk of them being exploited.

Unencrypted data on the network is at risk

Network encryption

As data moves through the network, it is possible for a knowledgeable hacker to intercept raw data streams, files and passwords. Without protection, intelligible information can be stolen, modified or falsified and re-inserted back into the network with malicious intent. Ricoh uses robust network security protocols that can also be configured according to customers' needs. The Transport Layer Security (TLS) protocol is used to help maintain the integrity of data being communicated between two end points.

Ricoh devices support WPA2, WPA2-PSK using AES Encryption (Wi-fi Protected Access), an encryption system for wireless networks that provides greater security than the conventional WEP (Wired Equivalent Privacy) encryption system. WPA2, WPA2-PSK features a user authentication function and an encryption protocol called CCMP (AES) — which automatically updates the encryption key at certain intervals.

Data sent to printers could be exploited

Print stream encryption

Data sent in a print stream can be exploited if unencrypted and captured in transit. Ricoh can enable the encryption of print data by means of Secure Sockets Layer/Transport Layer Security (SSL/TLS) via Internet Printing Protocol (IPP) — encrypting data from workstations to network devices or multifunction printers. This can be accomplished using IPP over SSL/TLS. Because this is a protocol that helps maintain data integrity, attempts to intercept encrypted print data streams in transit would only produce data that is indecipherable.

Managing devices can be time consuming

Device Manager NX

Because managing devices can be time consuming, security gaps can emerge unintentionally when aspects of proper device management go unattended. Ricoh device management software such as Device Manager NX and Streamline NX give IT managers a central control point to monitor and manage a virtually unlimited numbers of network connected print devices — whether spread across multiple servers or geographic regions. SNMPv3-encrypted communications are used to monitor the operating status of devices and their services — incorporating user authentication and data encryption functions that help protect user data and network device information.

With central control, administrators can determine who can access and use a device or multifunction printer, monitor DataOverwriteSecurity Solution (DOSS) settings and manage device certificates. Automated tasks can also reduce exposure from outdated firmware. Ricoh device firmware is compared with either the customer approved firmware version or the latest firmware available for the device from Ricoh's Global Software Center. If the firmware is different, the correct firmware can be deployed to the device automatically.

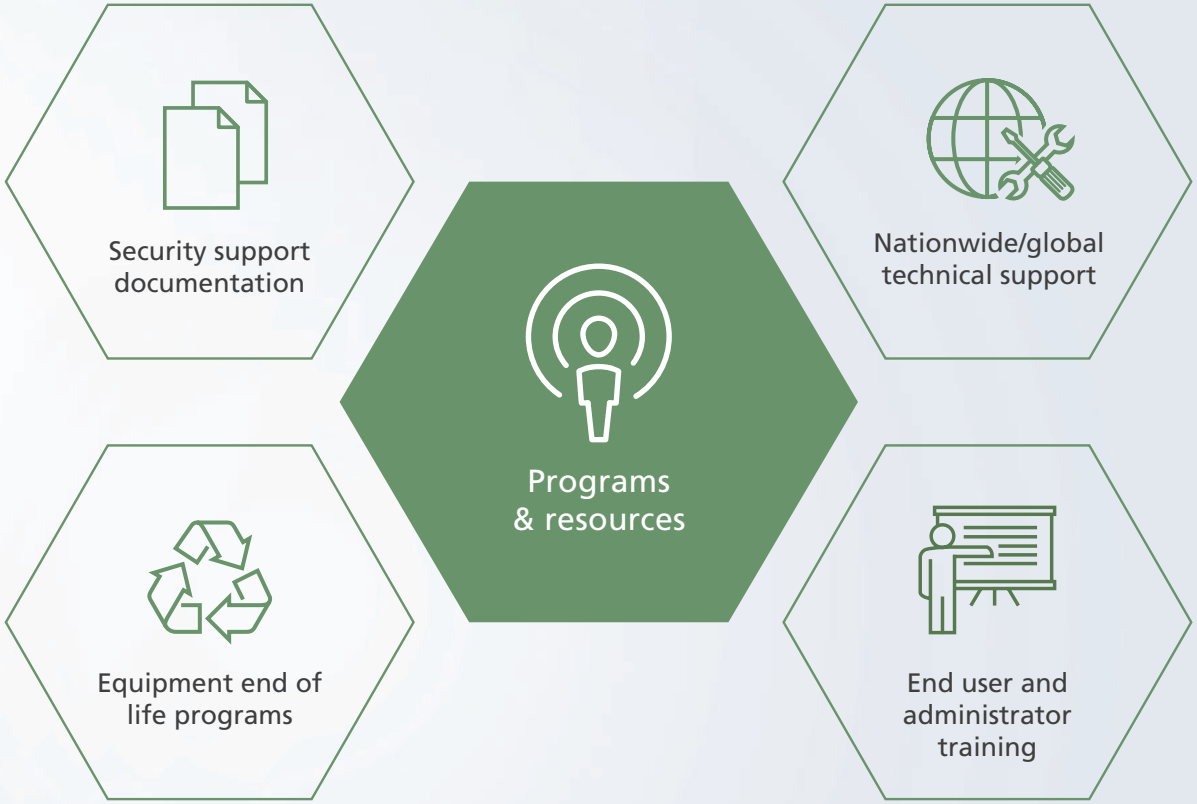
Help service providers respond fast

@Remote

Ricoh's @Remote Connector NX collects soon-to-be critical service alerts and can communicate them directly to your Service Provider using a secure method. Your Provider can schedule remote firmware updates — using the connector to 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.

Programs & resources

Organizations that use and store medical information, financial information, personally identifiable information (PII) or other types of sensitive data may be subject to various regulatory requirements — such as HIPAA, Gramm-Leach-Bliley or the Family Education Rights Privacy Act. Whether your organization needs to adhere to outside compliance or demonstrate support of your own security policies, Ricoh can help. We provide our customers with programs and resources to help satisfy their specific regulatory compliance requirements.



At Ricoh, we support our customers by providing needed technical assistance, knowledge & training and security documentation that relates to our equipment. In addition, we also offer data removal from end of life equipment as a service.

Equipment end of life programs

Latent information on decommissioned equipment can present a security risk until it is completely destroyed. If compromised, malicious third parties could use acquired information towards a larger security breach. Ricoh's programs clean information from equipment at the end of its useful life or when being returned at the conclusion of a lease or rental contact.

Hard drive overwrite services

Typically performed when a device is decommissioned or at the conclusion of an equipment lease, the Data Overwrite Service completely overwrites customer data on the machine's hard drive. Various methods of data overwrite are available — including National Security Agency (NSA) and Department of Defense (DoD) compliant methods. In addition, NV-RAM is initialized to default values to prevent identifiable information — such as IP addresses, address books, and other administrative data — from being exposed to third parties.

Hard drive disposal services

The Hard Drive Surrender Program allows customers to retain their MFP or printer's hard drive at the end of a lease or the machine's useful life. A Ricoh certified technician removes the hard drive before it leaves the customer's site and transfers it to the custody of a customer representative. Customers keep control of their information and can choose to have it destroyed via a method of their choosing.

MFP cleansing services

Ricoh's MFP Cleansing Service is designed to remove all identifying information from a MFP or printer before that device leaves a customer's location. Information stored in the device's memory — such as address books and network address information — is deleted. Identifying marks like labels listing department names, IP addresses and service desk information is also removed — along with any customer-specific paper or form stock. Removing such information can help prevent malicious attempts to gather an organization's IT information.

Nationwide/global technical support

Ricoh has established Technology Centers in every region to provide technical support to our customers across the globe, responding to their needs quickly and efficiently. The Ricoh Global Services team provides standardized, consistent, end-to-end solutions. With coverage in approximately 200 countries and territories around the world, Ricoh employs over 30,000 service delivery professionals. Our unrivaled direct sales and dealer partner support network has the capability to service 95% of Fortune Global 500 company employees — 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 — wherever they may be.

Security support documentation

Ricoh provides technical documentation to support our customers' information security requirements — including IEEE 2600 and ISO 15408 Certification Documents 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 devices and network settings and Device Security Installation Guides 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.

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 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 policies.

Security beyond the device

Security best practices demand a "defense-in-depth" that goes beyond the device. Ricoh is addressing our customers' expanding security concerns through Governance, Risk and Compliance (GRC) and Managed Security Services. These services encompass data lifecycle and risk assessment & management, eDiscovery, end-point and server security, identity access, email security and protections against advanced network threats.

Look to Ricoh for help with your top security challenges

Data loss / theft

Data loss is at the core of C-level leadership concerns, and keeping data confidential and secure is a constant struggle. Attackers are continually seeking a gap in your armor that can be exploited. Ricoh imaging equipment can be a key component of data loss prevention.

Data corruption / alteration

Virus attacks making global headlines highlight how vulnerable all organizations are to cyber attacks. Malware, Viruses, Trojans and Worms attack widely implemented platforms with well known vulnerabilities. Ricoh's platforms, although widely implemented, utilize proprietary Operating Systems to thwart attempts at tampering.

Data availability

Information and data availability is a multifaceted balancing act between allowing and preventing access. Ricoh products address both by speeding up the sanctioned exchange of information through printing, copying, scanning and routing, enforcing controls of those processes, encrypting data in transit and determining who can consume the information processed by our equipment.

Understanding regulations

Organizations must observe numerous global, national and industry regulations — not to mention internally mandated company security policies and audit requirements. Ricoh provides tools and expertise to support our customers' compliance-related needs.

Proving compliance

Penalties for non-compliance can be severe, and new regulations are raising the bar on potential adverse business impact. Proper documentation is at the heart of effectively demonstrating compliance. IEEE 2600 certification provides independent third-party validation that IT security claims operate as advertised. Ricoh can provide this certification, along with other documentation, to support our customers.

Initiate a Security Risk Assessment

A Ricoh-performed Security Risk Assessment encompasses hardware, software and data and is built upon accepted NIST* standards. Risk scores from low to high are calculated based on U.S. Federal Government and DoD** standards — along with an annual loss expectancy (ALE) for data assets, findings and recommendations. The Security Risk Assessment informs the subsequent Risk Management Plan, Policy Creation, Risk Remediation actions and independent third-party audit.

Engage our security professionals

Customers are looking for organizations they can trust and who can help them to stay secure and prove compliance. Ricoh is committed to providing our customers with the finest technology, services, programs and resources — along with the willingness to assist our customers in meeting their security policy requirements. If you have questions or would like more information, contact your Ricoh sales professional or visit our website.

Learn more at **www.Ricoh-USA.com**.

** National Institute of Standards and Technology*
*** Department of Defense*

RICOH
imagine. change.

Ricoh USA, Inc., 70 Valley Stream Parkway, Malvern, PA 19355, 1-800-63-RICOH

090717