RICOH
imagine. change.

Ricoh Security Solutions

Helping you protect your business

Cyber security is the biggest threat to the survival and success of modern businesses. Companies of all sizes are at constant risk of falling victim to disruptive attacks such as phishing, DDoS or ransomware. The real cost of these attacks runs into the millions. In 2017 the Ponemon Institute found that the global average cost of a data breach was $3.62 million. This cost will only grow in coming years as government regulation, such as the GDPR, looks to punish businesses with crippling fines for failing to secure their systems and data appropriately. To avoid these debilitating punishments a business must be able to demonstrate its ability to protect data.
This requires a holistic view of all vulnerabilities across an enterprise.

Further compounding the cyber security challenge for businesses is the expansion and digitisation of the modern workplace, as well as the explosion in data volumes. Workflows often spread across devices, networks and geographies. Information is most at risk when it is moved around a business. It must remain protected at every stage of its journey. Given the security risk this poses, modern businesses can no longer function without fundamentally secure document and data management systems. At the same time, the capabilities of office printers and multifunction devices have increased ten-fold in recent years. They are now responsible for a huge proportion of business data input, output, transfer and storage. This makes them one of the most dangerous, yet often overlooked, threat vectors in the workplace today.

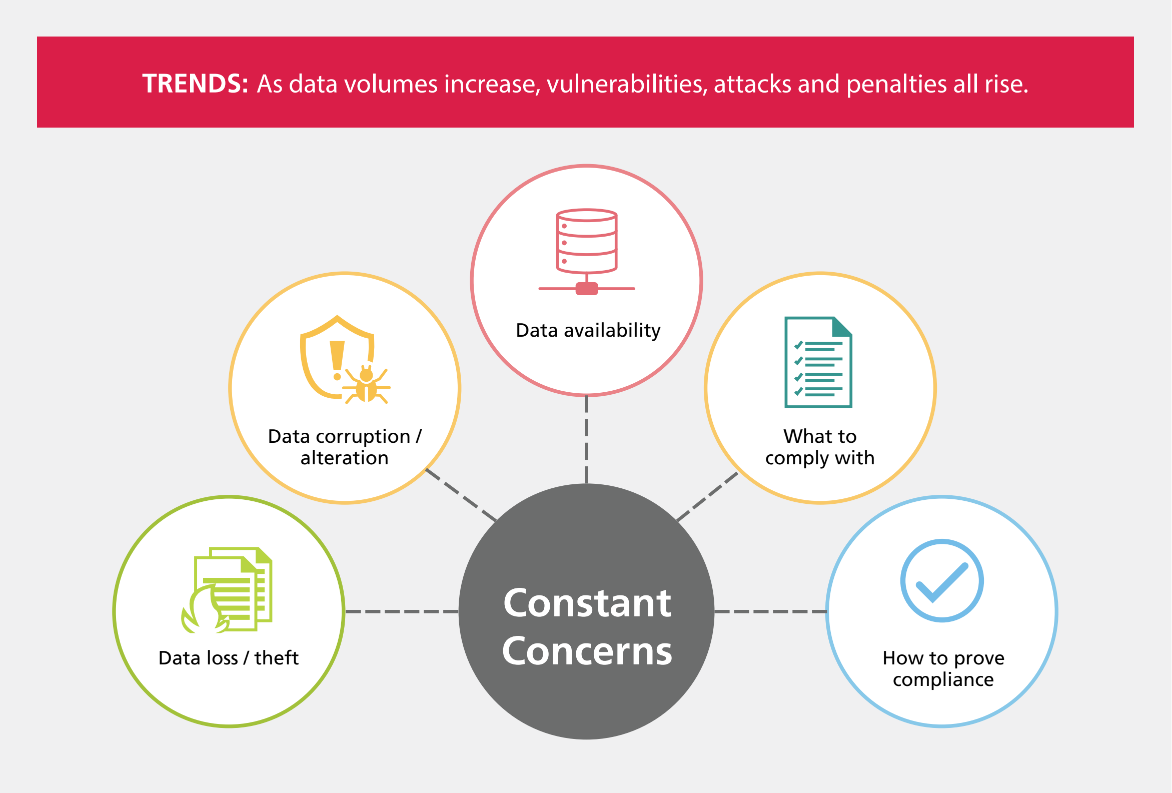
Although many companies claim to offer security capabilities, Ricoh has been developing secure workplace solutions and services for decades. Our printers, for example, have featured secure hard disk overwrite capabilities for over 20 years.

Security is in the DNA of our entire digital workplace portfolio. We have more than 4 million office products in the field today. Every one of those products and every service we deploy alongside them features built-in security capabilities. We also employ a Ricoh-only operating system across many of our products. This is a major component of our security defences, providing control and insulation from OS-specific threats which target more widespread operating systems.

Ricoh provides a consistent worldwide service and support structure for customers that ensures threat-intelligence is efficiently shared and acted upon. Not only is IEEE 2600 certification implemented as standard across our print-output devices, Ricoh is a leading member and key author for the IEEE Standards Association. Ricoh is also ISO 27001 certified, and committed to continuing to comply with this information security management system. We keep our product development focused on customers' business needs and security concerns through a series of global customer-driven innovation programmes.

To meet the demanding requirements of effective, demonstrable cyber security best practices, security is included in every product and service in Ricoh's portfolio by design – never as an afterthought. We believe this holistic view of vulnerabilities is essential for survival in modern business.

CUSTOMER SECURITY CHALLENGE


TRENDS: As data volumes increase, vulnerabilities, attacks and penalties all rise.
Data availability
Data corruption / alteration
What to comply with
Data loss / theft
Constant Concerns
How to prove compliance

Securing and Empowering Digital Workplaces

Ricoh seeks to enable and secure digitised work, wherever people are in action. In a modern digital economy this means adding value beyond the confines of the traditional office in frontline workplaces. Remote offices and workers afford businesses great flexibility and productivity gains in day-to-day operations. They help companies to better meet customers' expectations and service requirements.

However, operating at the edge of the network poses some of the greatest risks to business security. The data these workers generate and the remote devices they use to capture it have to be appropriately secured. Employees will often operate across networks and geographies, further complicating this task. Crucially, government regulations such as the GDPR require that businesses demonstrably secure data throughout its lifetime or face severe penalties. As workplaces evolve and embrace digital workflows, the lifecycle of business data gradually becomes more complicated. Let's examine it now, stage by stage.

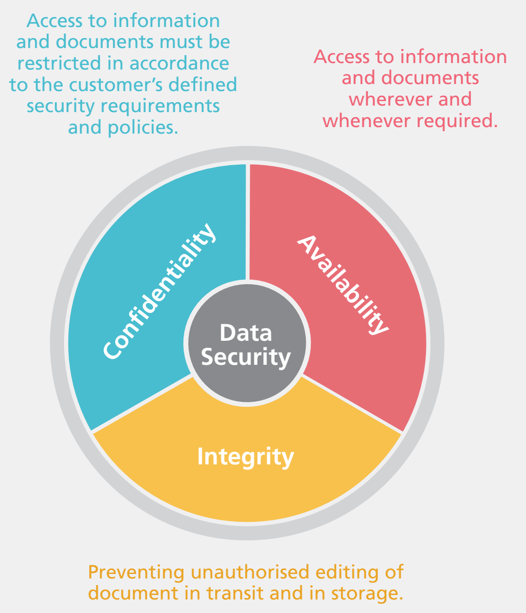
The first step is data input and capture devices – a vital component of Ricoh's security defence. From here, data must be transported across networks and stored securely. At this stage preserving data integrity is crucial. Ricoh's systems restrict user access to device and network functionality to ensure data cannot be tampered with in transport or at rest. These services include access control, encryption and copy protection. We call this Control.

Once stored, however, documents must also be readily accessible to those within the business who need them. The ability to draw on information whenever it's required and visualise it effectively depends on this availability. Data analysis is a vital component of the empowered digital workplace. It effectively provides insight for every element of the business from sales to HR. Authorisation infrastructure tools provide quick secure access, regardless of user location or device choice. It's vital that security protocols do not hamper innovation or functionality or risk pushback from employees. We call this stage Preservation.

Finally, this data must be disposed of in a secure, auditable fashion. This step is essential for complying with regulatory requirements and minimises the possibility of subsequent theft or loss. This process actually occurs throughout a document's lifetime as well as at its final deletion. Printing any file leaves a latent image on the hard drive of Multi-Function Printers (MFPs) which must be overwritten to prevent unauthorised access. Ricoh's data disposal services include hard disk cleansing, memory flushing, unprinted file deletion and delete on logout functionality to prevent hackers from compiling sensitive information from the footprints a document leaves behind. We call this Destruction.

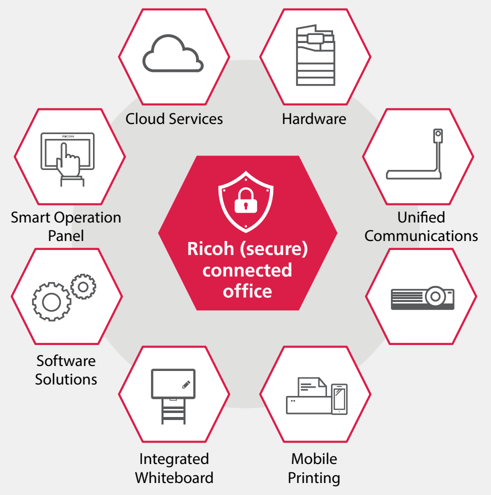
To effectively secure workplace data throughout this lifecycle, Ricoh uses the 'CIA' principles of privacy and security: Confidentiality, Availability and Integrity. These are our guiding principles in designing our products and solutions to meet the necessary standards and regulations. This approach enables workplace innovation and growth while maintaining effective, secure processes.

RICOH'S APPROACH TO SECURITY



Access to information and documents must be restricted in accordance to the customer's defined security requirements and policies.
Access to information and documents wherever and whenever required.
Confidentiality
Availability
Data Security
Integrity
Preventing unauthorised editing of document in transit and in storage.

We build around the 'CIA' principles of privacy and security: confidentiality, integrity and availability



Security is in our DNA. Every product built and service deployed by Ricoh contains built in security features and capabilities

Ricoh offers a complete suite of security products and services to secure document creation from start to finish. We will now explore each crucial stage in turn: control, preservation, destruction and support.

FOUR STAGES OF DIGITAL WORKPLACE SECURITY

1 CONTROL

Effective data controls are crucial for maintaining data confidentiality and integrity. Business information is a primary asset and needs to be protected. Today's hardware devices are information terminals that can act as vulnerable gateways to business information. As such, Ricoh employs a number of user authentication and device management tools to control and secure business data. These pertain to the settings on physical devices which permit and restrict access to certain functionalities and data. Limiting employee access to the information travelling through any office Multi-Function Printer (MFP) is a crucial best practice step for maintaining document security. The control phase also includes device malware protection through Ricoh's three-tiered approach to device firmware.

Unauthorised copy control

To guard against attempts to make unauthorised copies, Ricoh offers an elegant solution to ensure the security of hardcopy documents. The copy guard function prints or copies documents with special invisible patterns embedded across the background. If the printed or copied document is photocopied and/or scanned, the embedded patterns are visible on the copies. The unauthorised copy guard module allows the MFP to detect the embedded patterns and replace the photocopied image with a grey image to prevent information leaks. This function is useful when printing confidential information. Restricting the duplication of confidential information prevents this kind of information leak.

Locked print

A document received from a PC can be stored on the hard disk drive in the MFP. Using Ricoh's locked print function, a password is specified when a user sends the document, and that password must be entered on the MFP before it can be printed. Since the document will not be printed until the owner reaches the device, locked print ensures the document remains under the control of its owner.

Advanced capture security

Ricoh's portfolio of advanced capture solutions offers varying layers of encryption and decryption throughout the processing layers, across the stages of the capture process. Administrators can authorise access to process queues by individual user login or by group credentials. Additional layers of security include Security Assertion Markup Language (SAML) for a Single Sign On (SSO) framework, Personal Identity Verification (PIV) and Public Key Infrastructure (PKI) encryption.

Embedded authentication controls

Device access and identity authentication protocols across Ricoh products can be centrally managed. Available methods include ID card, pin number, network login or a multi-factor combination of the above. Multi-factor authentication enhances security but can slow down busy users. Single Sign On (SSO) helps this by allowing users to access a range of devices seamlessly. In addition, Ricoh's Quick Authentication, swipe-and-go card-based authentication software is pre-installed across our devices, giving users an easy way to access their documents. Using an NFC reader/writer vastly simplifies the user's login process while effectively securing and controlling access to the MFP. This form of access also works in conjunction with existing MFP permissions setting to restrict user access to device functions as determined by the customer.

Streamline NX (SLNX)

The device manager module within Ricoh's Streamline NX platform is Ricoh's software for managing and monitoring devices on a network. The software enables administrators to view or configure security settings for devices using pre-packaged templates and custom parameters. Crucial security settings include enabling / disabling protocols, IP address settings, Admin user passwords, email addresses for alerts, encryption settings and more. SLNX can also report any printers that are out of compliance based on a customer's policy.

Device malware protection

Ricoh takes a triple-layered approach to malware protection on its devices. Firstly, Ricoh devices can only be operated using a Ricoh-only machine language or operating system. Secondly, to prevent malicious tampering with device software, any firmware updates must be written and approved exclusively in this Ricoh machine language. Finally, every firmware update must be digitally signed by Ricoh. Using this three-step method, unapproved firmware cannot be loaded onto Ricoh devices so malware, spyware, and viruses are effectively eliminated.

Physical document security

Security best practice isn't always complicated. Offices are busy places and hard copy documentation presents a significant business risk both in terms of theft and employee negligence. Ricoh provides a number of additional physical security options to prevent unauthorised access to hardcopy documents. For example, locking paper drawers prevents theft of sensitive paper stock such as prescription templates in a healthcare environment. Fitting blanking plates for all cables also prevents the possibility of tampering from internal threats. A secure document release (Print-to-me) solution ensures that documents are only printed when the owner is present, in order to eliminate the risk of uncollected output.

2 PRESERVATION

Under new and existing regulatory requirements, businesses must ensure both the confidentiality of information, so that it cannot be stolen or leaked, and its ongoing integrity, so that it cannot be altered. To achieve this, businesses must restrict access to sensitive documents. This prevents unauthorised modification and falsification. It also acts as protection from targeted or opportunistic threats within the business.

Mobile working adds a complexity to any cyber security scenario. Additional security measures need to be in place to accommodate file sharing from any location. Those files must be as secure in transit over networks and across devices as they are in storage. Strong encryption technology can effectively follow and protect data throughout its lifecycle. This naturally applies to documents but extends to crucial security elements such as stored passwords, macro setting and address books. With encryption in place, even if hackers were able to access your network they would struggle to extract any usable information, preserving its integrity even in the event of a breach.

Continuous up-time is paramount for many industries. Unforeseeable events such as natural disasters therefore present a direct business risk. Paper documents are particularly vulnerable in this scenario. Using a secure, cloud-based repository for digitised documents adds crucial resilience from natural and man-made disasters. However, appropriate security steps must be taken to preserve this digital data.

Essential data encryption

To protect information as it moves across devices, encryption can be enabled for any data travelling to or residing on a Ricoh MFP hard disk. Built-in software options provide end-to-end encryption for scanned and print files via the user's public key infrastructure (PKI) key. This protects against 'man in the middle' attacks inside the customer's IT environment.

For added security, print data is also continually overwritten by Ricoh's Data Overwrite Security System (DOSS) which we will discuss in more detail later in the 'destruction' phase of the data lifecycle.

Bios and operating system protection

Ricoh MFPs employ a Trusted Platform Module (TPM) which is a tamper-proof hardware security module. The TPM performs cryptographic functions and securely stores cryptographic data. Ricoh uses the TPM to store the root encryption key that protects the hard disk data encryption key and the digital certificate of MFPs. It also allows administrators to perform a trusted boot operation, validating the MFP's firmware authenticity before permitting it to operate.

Firmware validation

The root key and cryptographic functions are always contained within the TPM and cannot be altered from outside the firewall, preventing misuse of, or malicious tampering with our products. This process provides high level validation of the MFP's firmware, device identity, and hard disk security. This is another good example of how Ricoh's MFP products are designed with Ricoh's customers' security interests at the forefront.

Password management

Ricoh devices can be configured with multiple administrator users, each one with different roles on the devices and distinctive passwords. The passwords for these users can be configured remotely using web-based administration tools, and regularly verified. This enables 'segregation of duties', which is a requirement present in a number of business regulations.

User access restriction

Ricoh's user management tool allows system administrators to restrict user access privileges. For instance, the administrator can set up privileges to provide selected users with access to an MFP's registered address book. This blocks unauthorised access to personal information and records stored on office devices.

User lockout function

When wrong passwords are consecutively entered during the login process, a Ricoh MFP can assess whether someone is trying to crack the password. This triggers the lockout function blocking the username in question. The blocked username can't be authenticated even if subsequently combined with the correct password. The lockout can only be released after a certain time lapse or by an administrator, effectively thwarting would-be hackers.

3 DESTRUCTION

Secure data disposal is an essential part of any comprehensive cyber security defence. It's easy to fall into the trap of assuming business liabilities end when data leaves an organisation. However many regulations stipulate that data destruction must be a comprehensive process, eliminating any risk of subsequent theft or misuse. Until this can be proven, a business' data obligations are not over.

End-of-life and returned office devices pose an often unrecognised risk to business information. Ricoh offers a certified and auditable service for removing data from these end-of-life printers. This includes overlooked material such as saved network settings, user data, hard drive data or even stickers left on the device. Failing to do so places businesses at significant risk of exposing confidential company and personnel information. But in order to maintain regulatory compliance this process should constantly happen throughout a device's life as well. This ensures businesses have the maximum degree of control over the data for which they are responsible.

Image overwrite: Data Overwrite Security System (DOSS)

MFP hard drives function efficiently by storing latent images of document data in their memory for job processing. Ricoh's Data Overwrite Security Solution ensures this is constantly overwritten before the next job begins. In this way if anyone were to access the hard drive maliciously they wouldn't be able to access the 'foot-print' of any data left behind from previous jobs. At Ricoh we're proud to have offered this best practice security measure for over 20 years.

End-of-life cleansing service

Ricoh offers Full Data Cleansing Service, an end-of-life service for MFPs and printers that have all memory modules and disk storage on the device erased beyond recovery using industry-certified security solutions. Ricoh's IT Services also offer a comprehensive equipment disposal service including several levels of certified data erasure services.

Hard disk replacement and removable storage

Ricoh also offers a hard drive disposal service which lets customers keep hold of their hard drive – replacing this with a new, empty hard drive when they return the equipment at lease end. This guarantees businesses complete, demonstrable control over their data environment.

4 SUPPORT

As businesses grow, the number of connections between devices and networks inevitably grows as well. Businesses need strategies to ensure this infrastructure growth doesn't pose a security risk. They must be aware of the weak points in their system taking steps to pre-empt targeted and opportunistic attacks.

Often specialised IT security expertise is required to analyse a business' infrastructure and identify these vulnerabilities. For many businesses, maintaining in-house IT staff with the necessary knowledge to manage their cyber security environment simply isn't an option. The costs and inefficiencies of this approach often force these businesses into
dangerous inaction.

Ricoh's IT support service offers IT procurement and configuration services as well as remote monitoring, service desk and transition management capabilities to further support the cyber security process. Cyber security depends on having a holistic understanding of business risks. Ricoh's Security Incident Response Team (SIRT) ensures vital threat intelligence is shared to clients around the world, and effective responses can be coordinated instantly.

Infrastructure security assessment

Ricoh's Streamline NX (SLNX) device manager functionality is designed to perform an invaluable security policy auditing function. SLNX provides a functionality that IT managers enable to set up devices based on a company's policy, distribute these settings, and analyse settings using a visualised report. SLNX can also alert management when a device is out-of-compliance with company policy.

Print security optimisation

Ricoh offers a comprehensive Print Security Optimisation (PSO) service along with professional and managed consulting services to identify device-related security gaps. This is a web-based tool with a graphical wizard that provides a view of the current state and enables Ricoh to offer product recommendations with a goal of reducing risk.

Product Security Incident Response Team (PSIRT)

Ricoh's active response to new threats and the development of effective countermeasures is managed by Ricoh's Product Security Incident Response Team (PSIRT). This is a programme that Ricoh uses to ensure our entire product suite (hardware and software) is continually updated and protected against newly identified threats and vulnerabilities. This helps us to maintain a consistently high level of service on a global scale and minimise the impact of vulnerability problems on Ricoh products.

Supporting documentation

Preparation and education is a crucial element of any cyber security set-up. Backup documentation, user guides, security whitepapers and training should all be provided to the customer. As with many elements of the cyber security environment, demonstrable compliance is crucial and this documentation plays a key role in securing a business' bottom-line.

HOW CAN RICOH HELP?

Ricoh's unique position to deliver industry leading security solutions across the entire IT and print environment is predicated, in part, on maintaining a strong understanding on changing market conditions and evolving our trajectory accordingly. Our solutions are designed to protect all information across its entire lifecycle and speak closely to the four areas of data security discussed in this report.

We have dedicated subject matter experts responsible for analysing market needs, including industry-specific requirements for which new solutions can be built or existing solutions can be tailored.

We are also committed to developing our internal capacity to engineer and deploy security-centric solutions. To this end, we have created dedicated teams within our service development organisation that are focused on developing new government, risk management, compliance as well as cyber security services.

User authentication and authorisation

- Locked print
- Standard embedded S/W for authentication
- User authentication / access restriction
- Single sign-on
- Multiple administrator roles
- PDF password protection (password for scanned document)
- Unauthorised copy protection
- IP-Range based access control
- Secure device and print management
- PKI (Public Key Infrastructure) / SmartCard support
- Secure printing (print2me / locked print)

Device malware protection

- Servers
- Not/less susceptible to malware
- SOP – hardened version of Android
- Ricoh-only version of machine OS (machine control language) for MFP
- 3 layer approach – digital signature, download via Ricoh tool, needs to be written in specific control language

Hard disk disposal

- Hard disk disposal, image overwrite,
- Full Data Cleansing Service
- End-of-life service: destruction of data within memory modules, storage

Device management

- Quota setting / account limit
- DMNX – single pane of glass security auditing, password management, monitoring, alerting

Bios and operating system protection

- Secure boot using Trusted Platform Module (TPM)

Image overwrite and removable storage media

- Disk Overwrite Security System (DOSS)
- Removable hard drive

Data encryption

- Hard disk encryption via TPM
- Encryption keys via TPM
- End-to-end encryption of print and scan files using PKI key
- FIPS certified HDD (Federal Information Processing Standards)
- End-to-end encryption for printing
- End-to-end encryption for scanning

Firmware updates and password management

- Remote password audit
- User lockout function
- Firmware validation via TPM

Compliance with industry standards

- ISO 27001 Certification
- IEEE 2600.2 Certification for select products
- ISO 15408 Certification for select products
- Security documentation and training

RICOH'S LAYERED APPROACH TO DEVICE SECURITY

There's no doubt that the role of the MFP provider has evolved far beyond the transactional, one-dimensional provision of hardware to the actual management of data. The capabilities of MFPs now span the capturing of information from multichannel inputs, to the classification of the captured data and workflow integration, to its safe, secure storage and analytics. In this complex web of stringent multi-regulatory rules and retention requirements – coupled with internal and external threats putting records at risk from loss, destruction or tampering – we take a layered approach to device security to ensure your MFP and the systems it connects with provide you with the best possible protection.

1. The Device

At the heart of any Ricoh model we have the device. These are designed, manufactured and implemented with security as a core requirement. The Ricoh-only operating system does not share vulnerabilities that are present in many commercial off-the-shelf operating systems and our devices are certified to IEEE2600.2 as standard. Hard disk encryption and disk overwrite security ensure that data being processed remains confidential.

2. The Smart Operation Panel (SOP) provides the user interface

In a similar manner to the MFP, the SOP uses a Ricoh-only operating system. No unnecessary components are installed and root access is not available. Ricoh has worked hard to ensure that device security is not weakened by the introduction of the SOP.

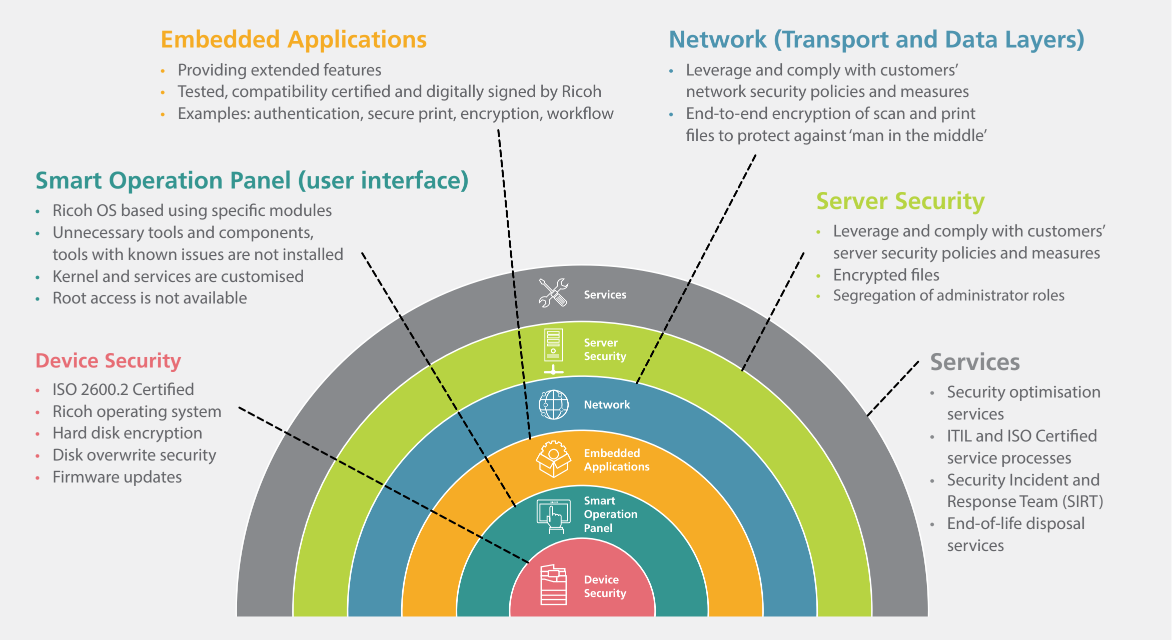
3. Smart Applications

These can be embedded on the SOP providing additional functionality to the user, including workflow and data capture. Some applications provide essential security features. These include secure print capability, card access and encryption. Applications are developed by Ricoh or Ricoh Developer Programme members and all applications must pass Ricoh Compatibility testing and be digitally signed before they can run on the SOP.

4. Network and Servers

Irrespective of who manages the IT infrastructure, Ricoh ensures that our products and services comply with your IT and network security policies. End-to-end encryption of print and scan files, encryption of data on servers and segregation of administrator duties are techniques used to protect against 'man-in-the-middle' or 'inside jobs'.

A comprehensive range of security services encompasses our entire offering. This includes consultancy and managed services to assist customers to monitor, optimise and manage their document and information security. We also have a range of end-of-life services which will ensure that the RAM and HDD of retired customer devices are wiped clean before disposal.



Embedded Applications

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

Network (Transport and Data Layers)

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

Smart Operation Panel (user interface)

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

Server Security

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

Device Security

- ISO 2600.2 Certified
- Ricoh operating system
- Hard disk encryption
- Disk overwrite security
- Firmware updates

Services

- Security optimisation services
- ITIL and ISO Certified service processes
- Security Incident and Response Team (SIRT)
- End-of-life disposal services

HOW RICOH PROTECTS THE DIGITAL WORKPLACE

Our customers have a number of core security concerns, all underpinned by the business truth that as data volumes increase, vulnerabilities, attacks and legislative penalties all rise. Keeping data confidential, secure and tamper-free is a constant struggle. For example, at Ricoh we repel around 8 billion firewall attacks per month. There are tens of thousands of global, national and industry data regulations and businesses must be able to continually prove their compliance with each of them. Understandably, organisations of all sizes are looking for a partner they can trust – one that can help them to stay secure across a portfolio that covers the entire digital workplace.

Ricoh has developed a wide range of solutions to mitigate the various risks faced by businesses. As the information security threat landscape evolves incredibly quickly, Ricoh draws on its 'voice of the customer' programmes to further develop and deliver our services.

Our Customer Advisory Boards operate as key strategic focus groups. We use these to gain a better understanding of the trends, drivers and priorities shaping our customers' businesses. Our Technology Advisory Conferences provide vital intelligence from key decision makers. Ricoh's engineering and R&D teams use these conferences to gain valuable customer feedback on ideas, concepts and proto-types. Finally, Ricoh collaborates with individual customers to develop new and advanced security features for vertical and general market customers. This customer-driven approach helps us to validate our product roadmap and helps our customers benefit from a global network of services and support.

The modern digital workplace must be as dynamic as the cyber threats it faces and as flexible as the working practices within it. That's why we believe that cyber security should operate seamlessly across the technology our customers choose to enable their workplace. Our commitment to ISO 27001 throughout our organisation, and IEEE 2600 certification across our products alongside the
Ricoh-only operating system we deploy within them means that best practice security controls are in place, however you choose to structure and grow your business.

A combination of security threats, legislative requirements and complex industry standards means the potential for reputational and fiscal damage from cyber risk has never been greater. Now is the time to work with a trusted partner to help you secure your business' most vulnerable assets and protect your future ambitions.

RICOH
imagine. change.

www.ricoh.ie

The facts and figures shown in this brochure relate to specific business cases. Individual circumstances may produce different results. All company, brand, product and service names are the property of and are registered trademarks of their respective owners.