RICOH
imagine. change.

Ricoh's approach to device security

Security is in our DNA. Ricoh takes a layered approach to device security.

The Ricoh Philosophy - Security is in our DNA

Layered approach to device security

Multifunction Printer specific. Other devices follow a similar layered approach.

Embedded Applications

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

Network (Transport & Data Layers)

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

Smart Operation Panel

- Ricoh 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

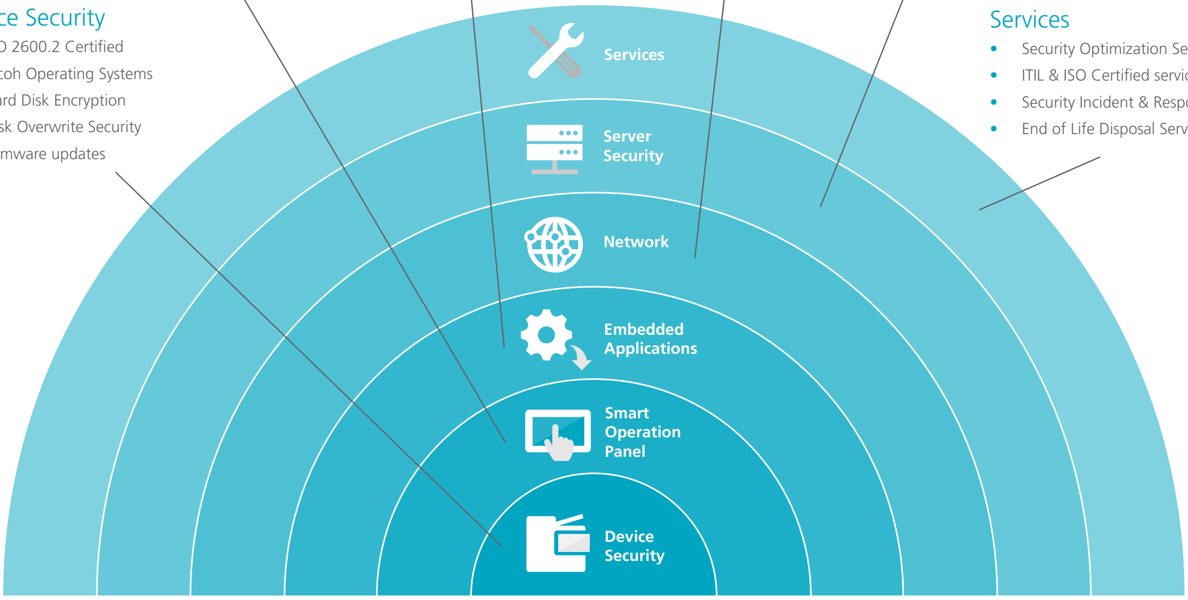
- Leverage & comply with customers server security policies & measures
- Encrypted files
- Segregation of administrator roles

Device Security

- ISO 2600.2 Certified
- Ricoh Operating Systems
- Hard Disk Encryption
- Disk Overwrite Security
- Firmware updates

Services

- Security Optimization Service
- ITIL & ISO Certified service processes
- Security Incident & Response Team
- End of Life Disposal Services



Ricoh takes a layered approach to device security. Our approach starts with each device being independently tested and verified against the IEEE or ISO 2600.2 standard.

We control our devices by having our own operating system, hard disk encryption and digitally signed firmware updates so that malware cannot be installed on our devices.

The next layer of security is our Ricoh user interface which has a custom kernel and no unnecessary modules. Root access is not available, minimising the possibility of mass market software infections and errors that cause problems.

Outside of the device, embedded applications are developed by third parties using Ricoh developer tool kits. These applications are then tested, certified and digitally signed by Ricoh. Our devices will not accept unsigned applications, preventing unknown malicious software gaining access.

Within the customer's network environment we employ end-to-end encryption of scan and print files to avoid 'man-in-the-middle' attacks where information can be intercepted over a network. At the server level we offer file encryption and segregation of administrator roles.

RICOH
imagine. change.
www.ricoh-europe.com

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.