# CYBER SECURITY AND YOUR PRINTING INFRASTRUCTURE

Nicolas Moerenhout
Marketing Business Developer

# CYBERSECURITY IN HEALTHCARE



# WHEN WE THINK ABOUT SECURITY, WE ALL FIRST THINK...

# A CONSTANT SEARCH FOR THE WEAKEST LINK...

# SECURITY AND PRINTING INFRASTRUCTURE

**16%**

**of organisations in 2024 are fully confident in the security of their printing infrastructure, compared with 19% in 2023.**

**67%**

**of organisations have suffered a print-related data breach in the last year**

**1.17**

**million d'euros**

**is the average cost of a printing-related data breach in 2024, compared with €870,000 in 2023.**

Source: Quocirca Print Security Landscape 2024

# SECURITY CHALLENGES

**Protect your documents and data**

**Complying with the law**

**Securing your network and peripherals**

# WHAT MAKES CANON UNIQUE

## Security Incident Response Team

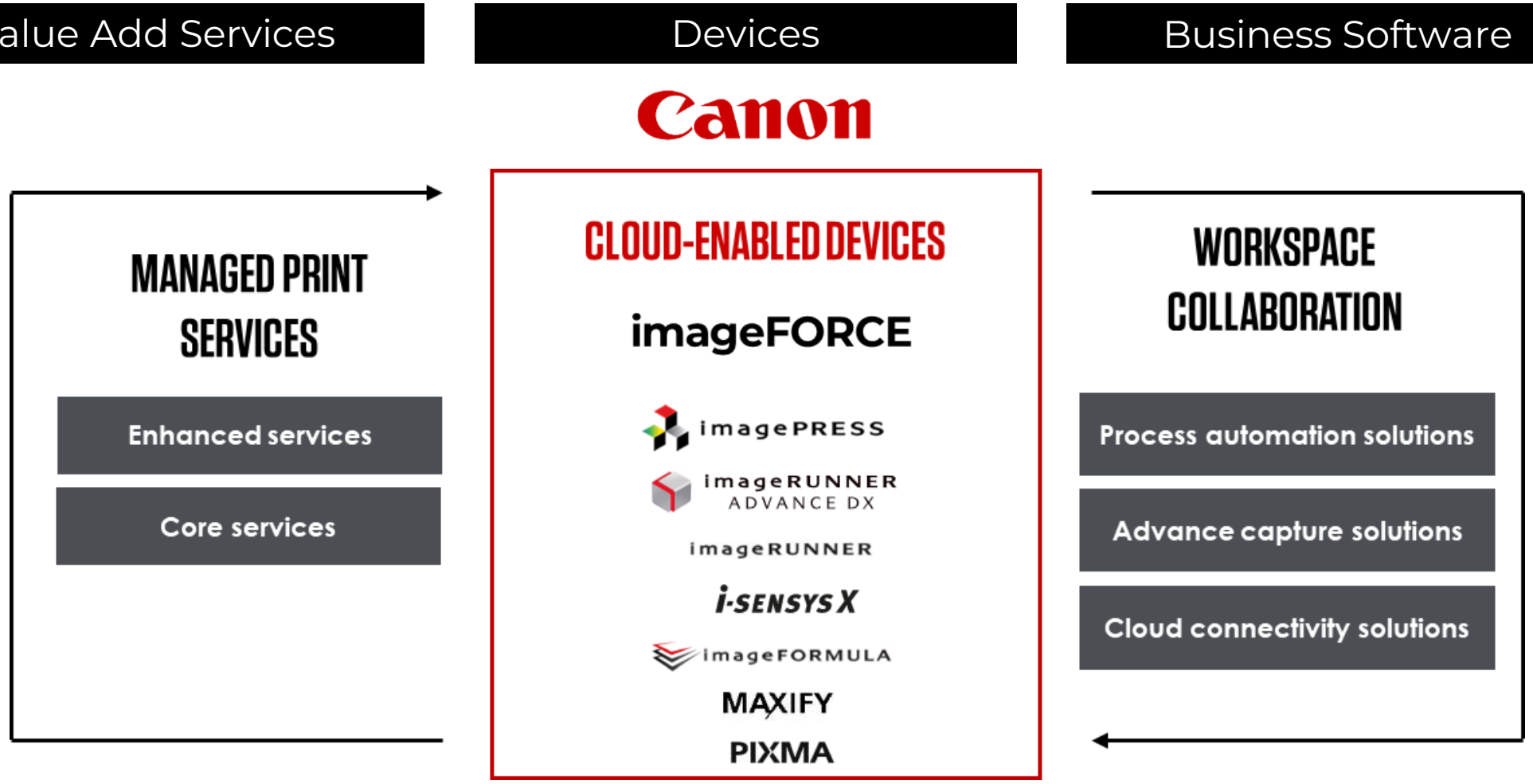
Internally focussed


## Product Security Incident Response Team

Canon

**2 teams, 1 management structure**

# CANON DIGITAL TRANSFORMATION SERVICES



# I’TS NOT JUST A PRINTER...

# 360-DEGREE SECURITY


## DOCUMENT Security

**Prevent leakage of information from documents**

Protect both documents to be printed and scanned from the MFP to prevent information leakage from documents left behind or document tampering.

## DEVICE Security

**Protect the MFP**

Protect MFP systems and data with multiple layers to guard against unknown threats.

## NETWORK+CLOUD Security

Protect from wire-tapping /
Protect from spoofing

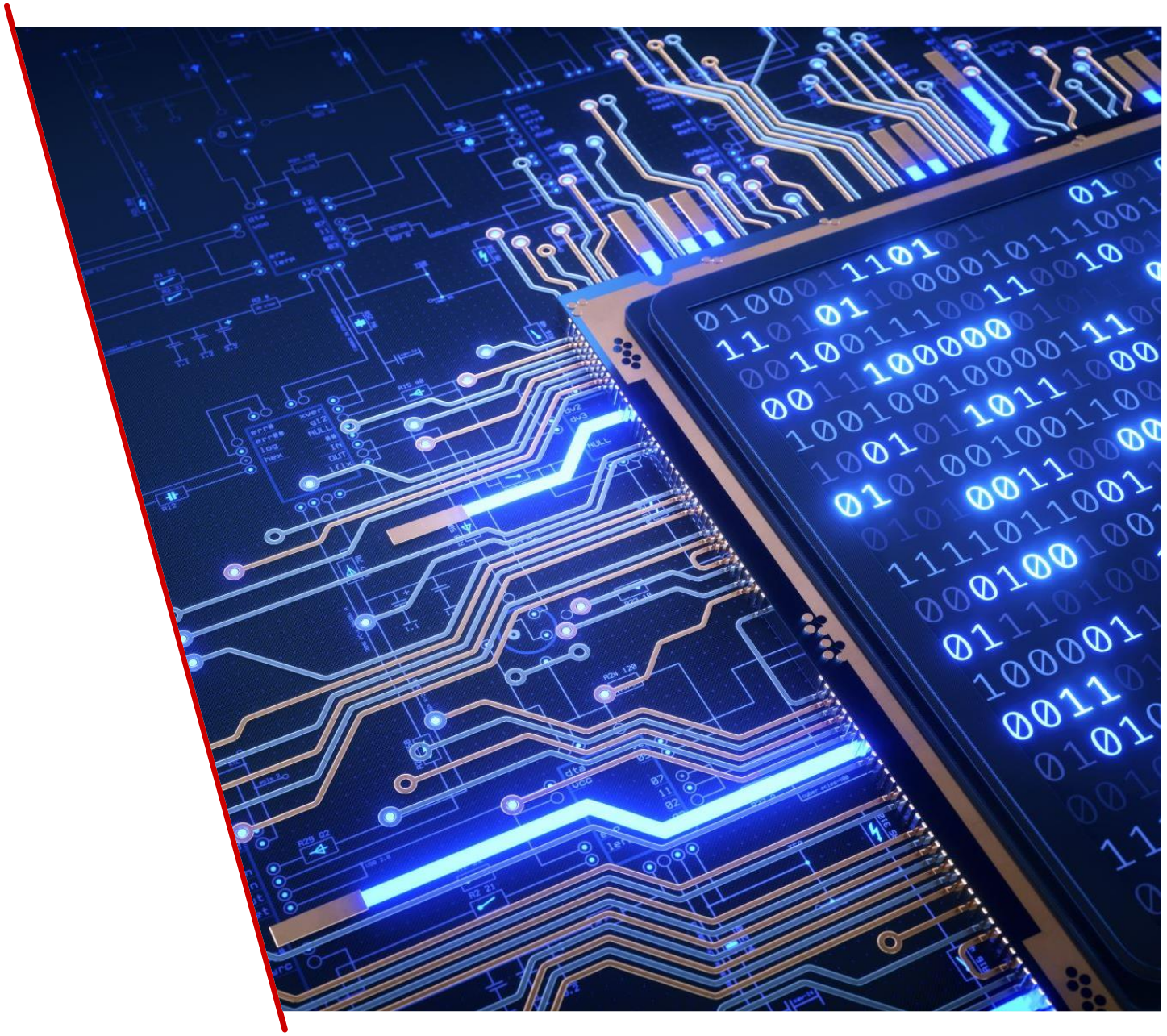
# UNIFIED FIRMWARE PLATFORM

# UNIFIED FIRMWARE PLATFORM

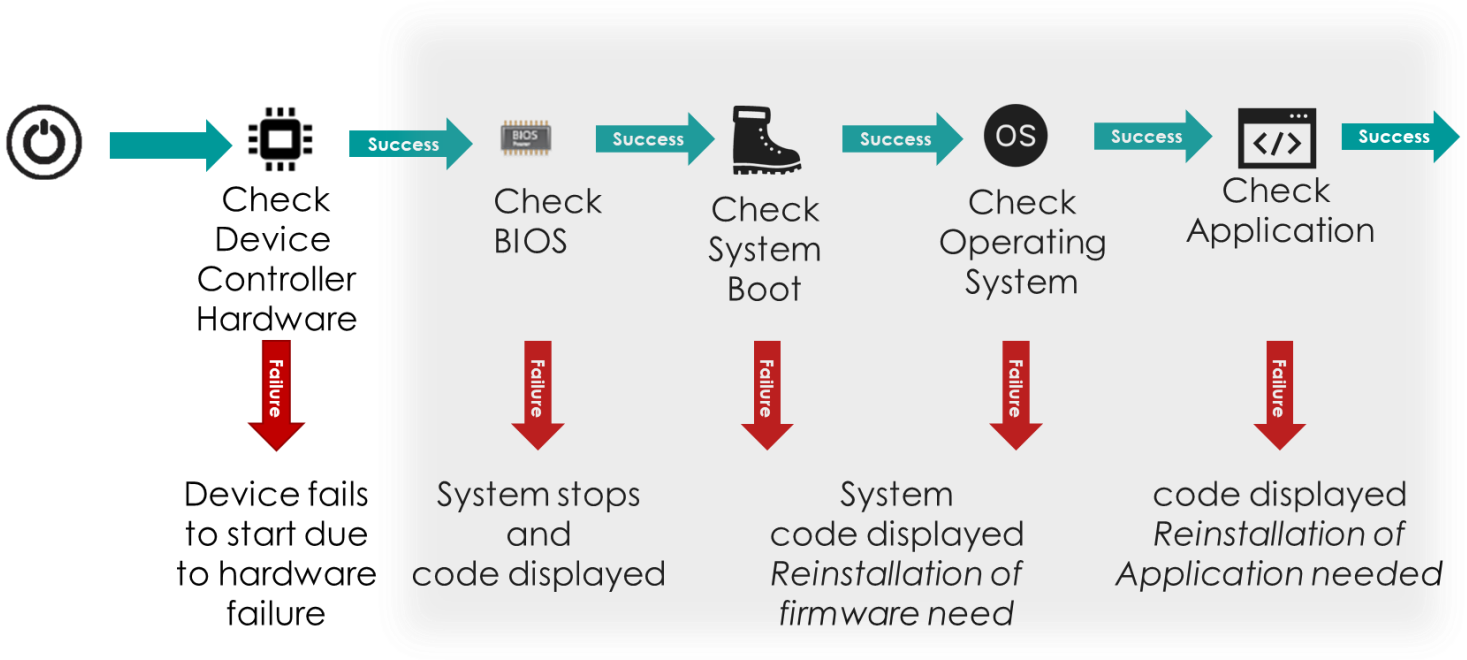
Our peripherals incorporate a unified platform that updates functionality, performance and security throughout the lifecycle of your hardware.

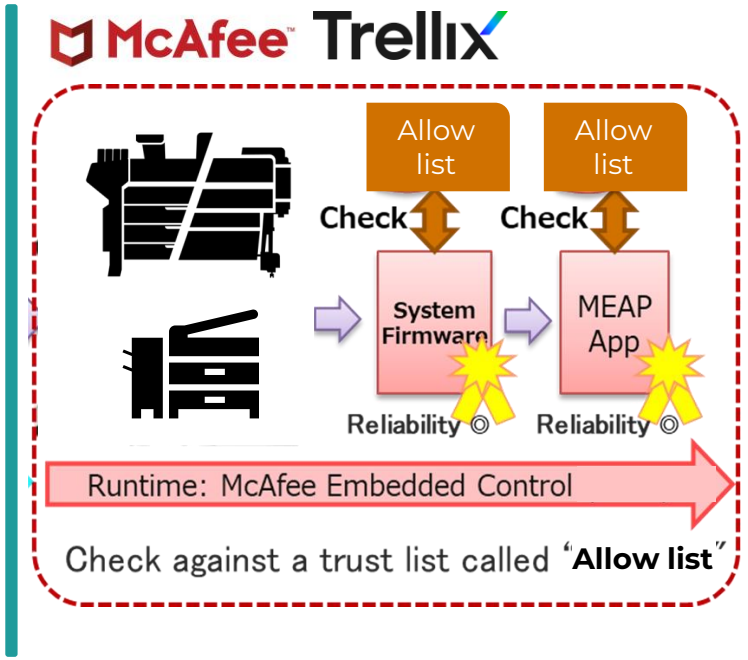
UFP
UNIFIED FIRMWARE PLATFORM

# VERIFY SYSTEM AT START-UP



# VERIFY SYSTEM AT START-UP AND TRELLIX




# SIEM INTEGRATION

# HOW DOES SIEM WORK?

**SECURITY INFORMATION EVENT MANAGEMENT (SIEM)**

SYSLOG data

Real-time information gathering from any source

Data analysis

Surveillance rules

Alert

E-mail

With details of the incident

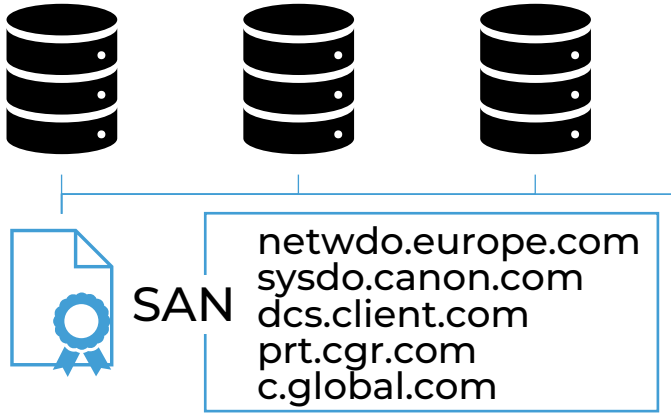
Notification administrator

# SAN (SUBJECT ALTERNATIVE NAME)

## SECURE & EFFICIENT CERTIFICATE FOR SSL / TLS COMMUNICATION

Normal certificates : **1 certificate for** 1 domain

SAN certificates : **1 certificate for** Multi-domain

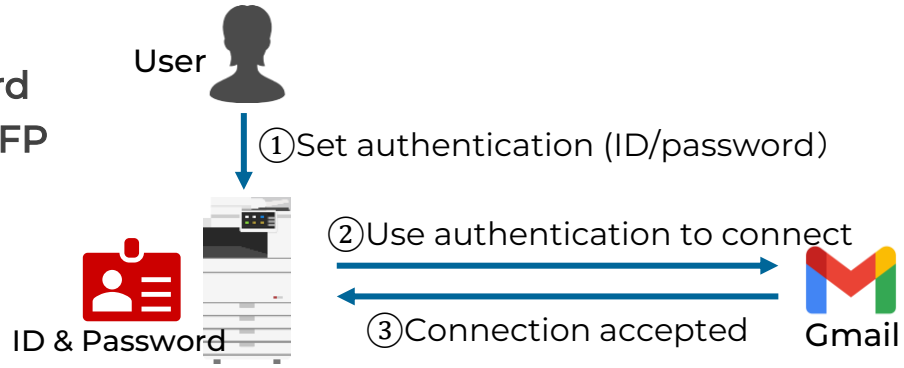



# OAUTH 2.0

## SUPPORTING CLOUD MAIL SERVERS

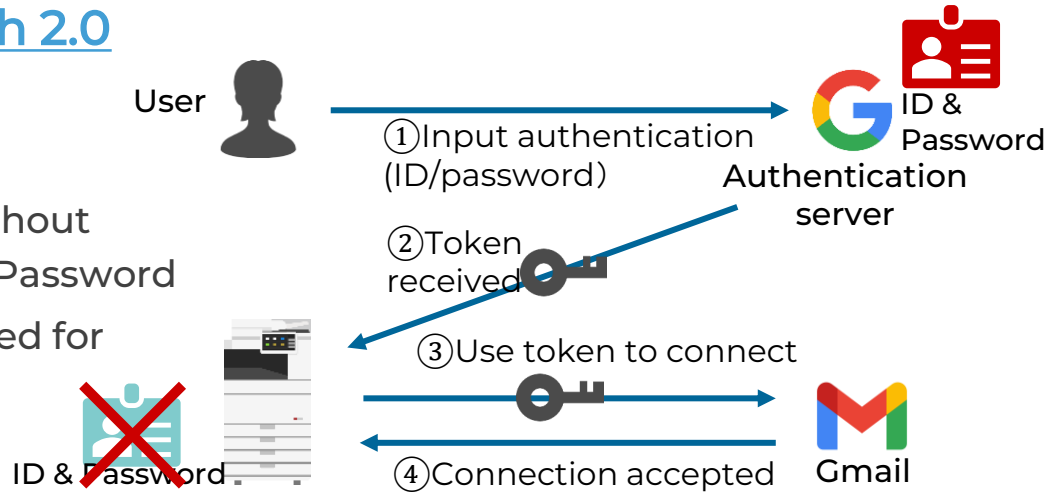
### Before : Basic Authentication

- ✓ ID & Password is saved in MFP and used for connecting.




### After : OAuth 2.0

- ✓ Connect without saving ID & Password
- ✓ **Token** needed for connecting




## WHAT'S THIS?

**OAuth 2.0 is an open standard authorization framework** for securely and selectively accessing user resources or data by client applications such as web or mobile apps.

**Google and Microsoft** officially announced that Basic Authentication is disallowed, and **OAuth 2.0 is mandatory**.

## BENEFIT

Users can **connect MFP with following cloud-based email services.**

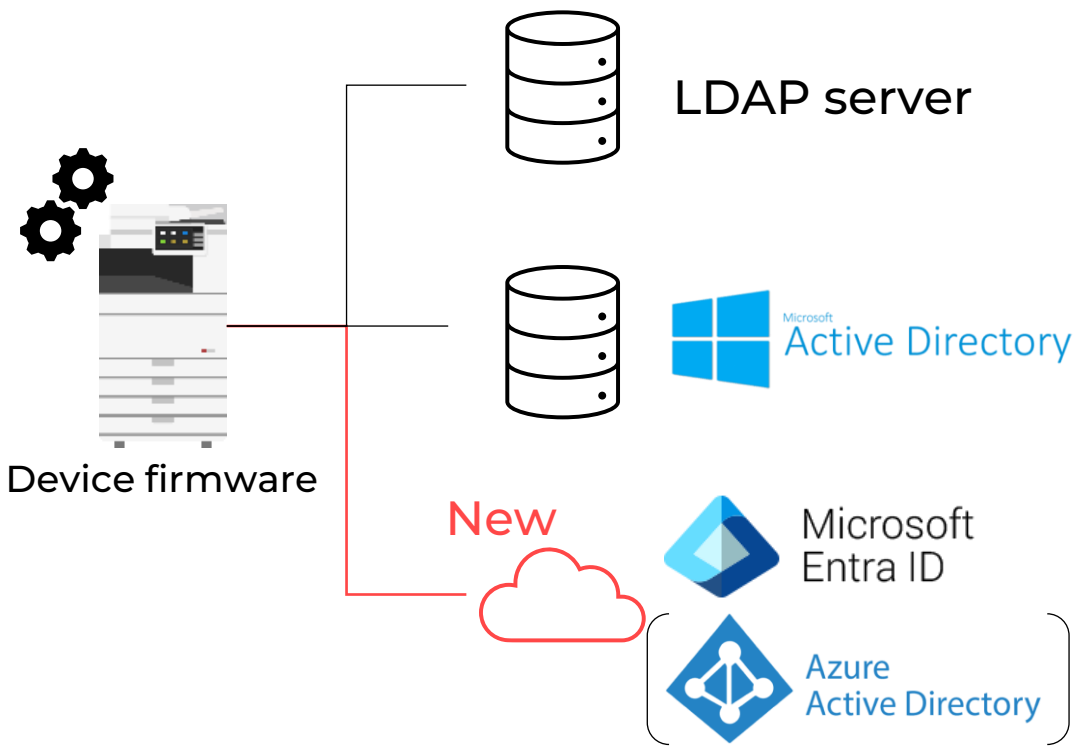
**Microsoft Exchange Online**

**Google Workspace** (formerly Google G Suite) *


*uniFLOW Online supports OAuth2.0

# MICROSOFT ENTRA ID (FORMER AZURE AD)

## SUPPORTING CLOUD BASED AUTHENTICATION




## WHAT'S THIS?

**Microsoft's cloud-based identity and access management services**

Simple access to many apps from anywhere with a single authentication (single sign-on)

More than 300,000 organizations use Microsoft Entra ID (Azure AD )

## BENEFIT

**Single Sign-On** : IT administrator can more **easily and securely** manage users by being able to link MFP authentication to their own Azure AD-based systems.

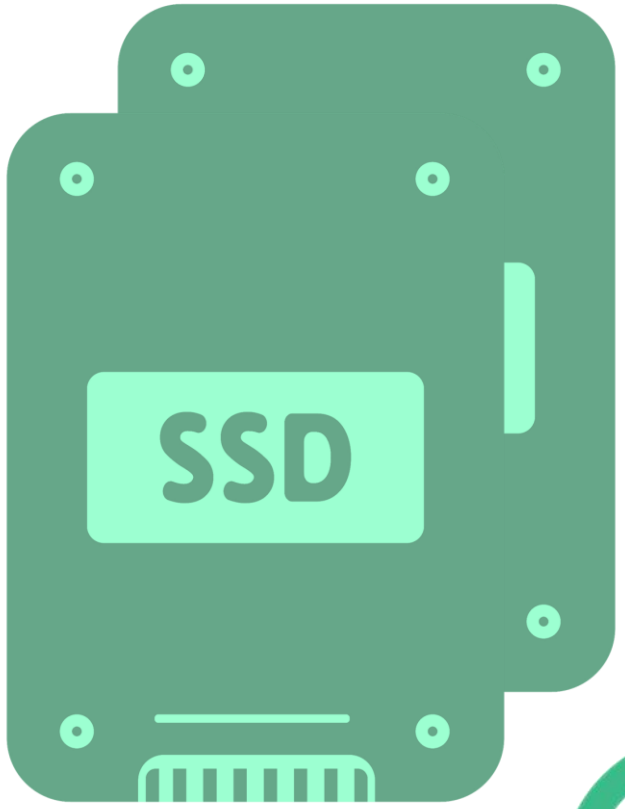
# DATA ERASE

# DATA ERASE

Canon devices feature DATA Erase, which ensures that data stored on the hard drive is securely erased after each task and at the end of the device's lifecycle.

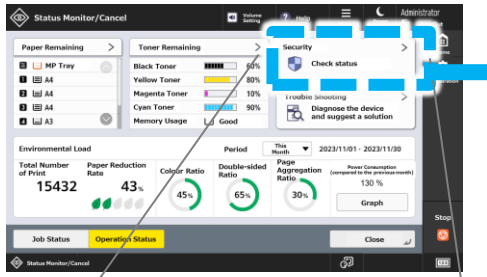
- **Protection of sensitive data**: Immediate deletion of temporary files.

- **Complete erase at end of life**: Secure hard drive reset before the device is taken out of service.

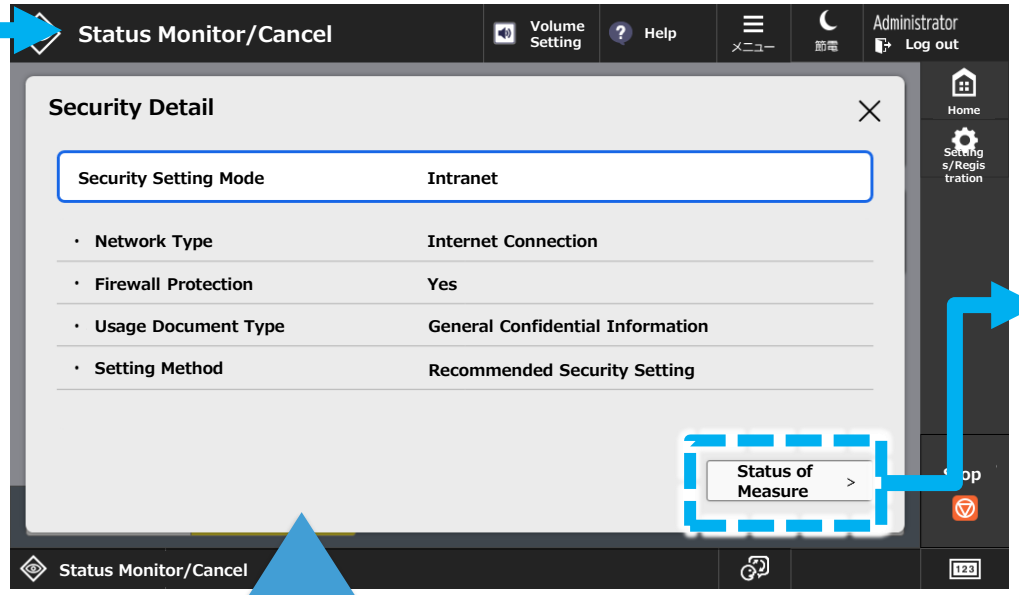



# SECURITY SCREEN

## Top screen of Dashboard for Administrators

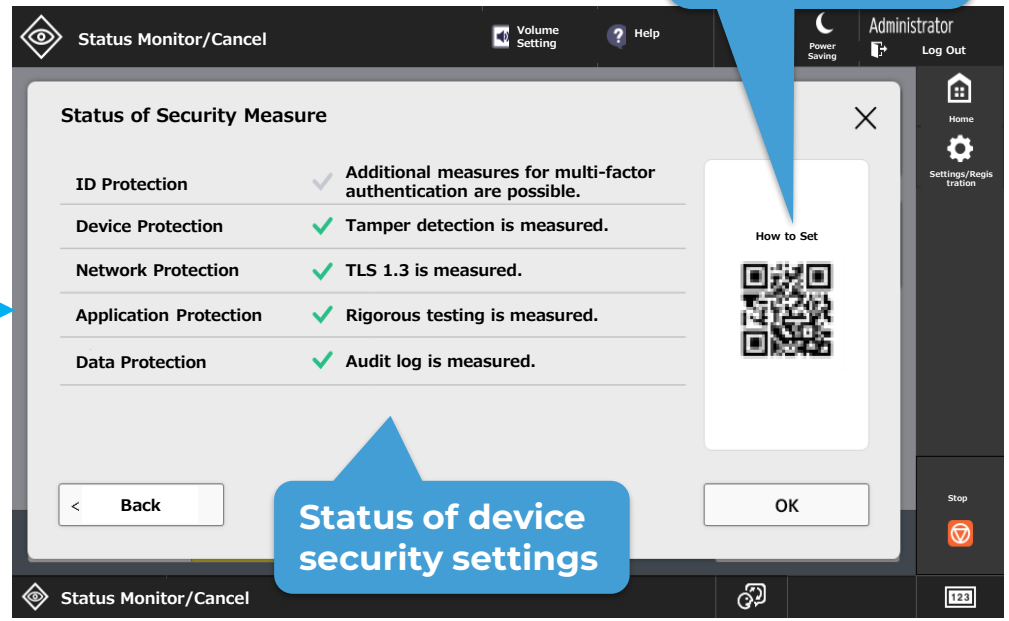



## Security detail screen




Customer environment information is displayed

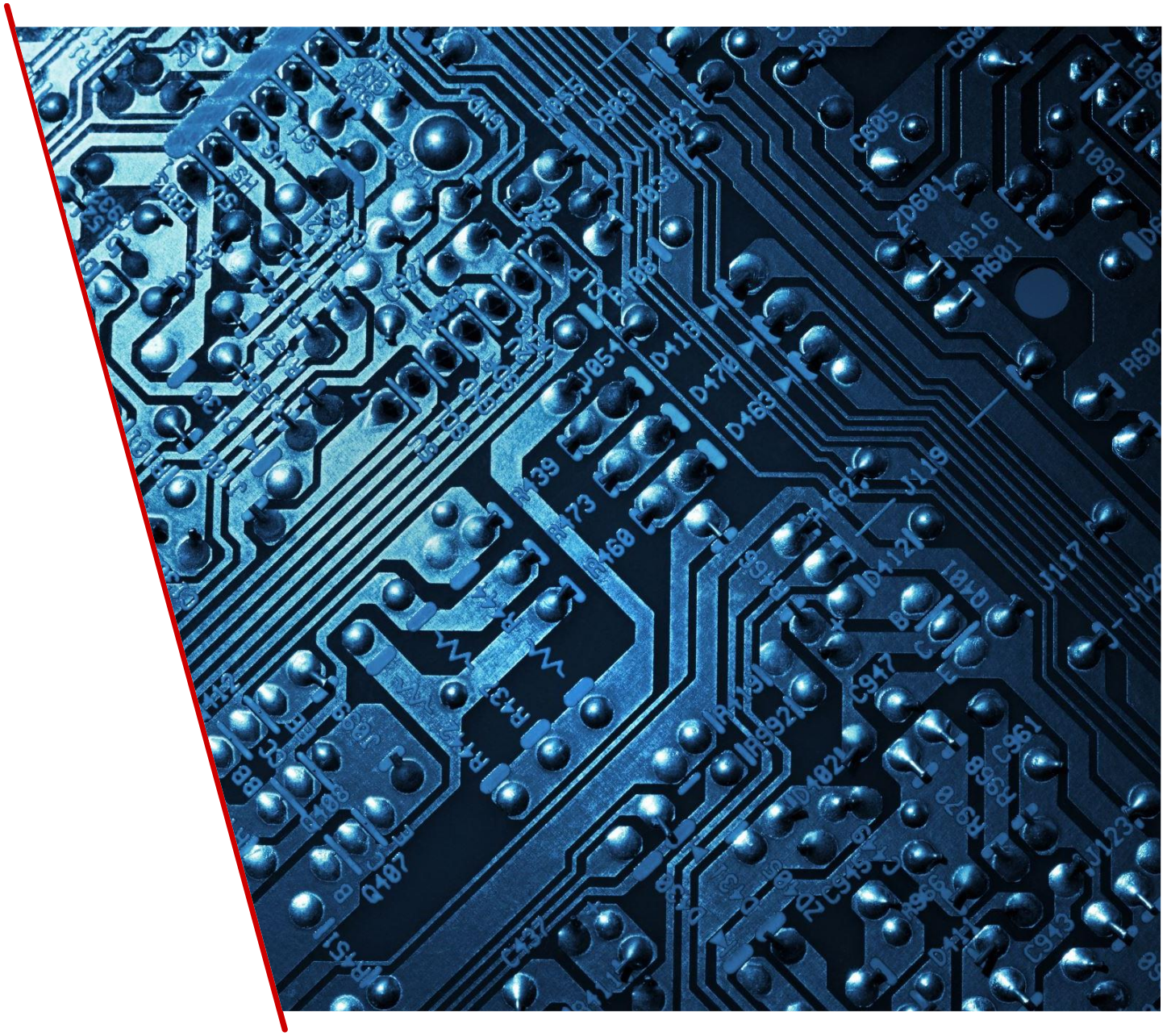
## Check the status of security measures



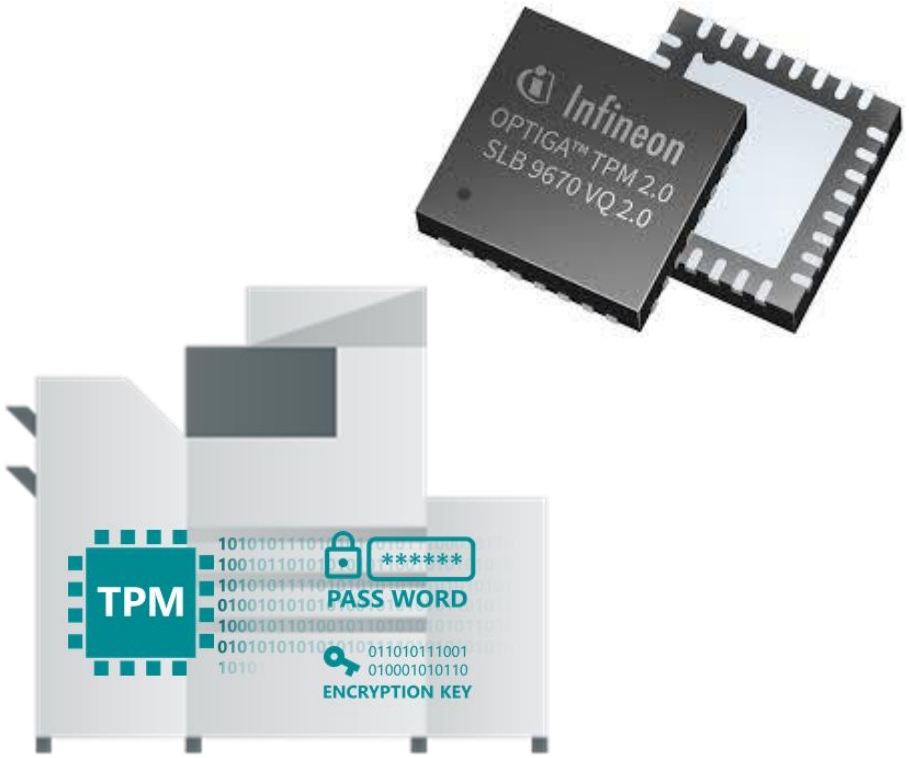

Links to settings guides

Status of device security settings

# TRUSTED PLATFORM MODULE



# TRUSTED PLATFORM MODULE




## What is TPM?

Trusted Platform Module

Secure management of "critical data" such as encryption keys stored in the MFD

Store "critical data" encrypted with the TPM

## TPM 2.0

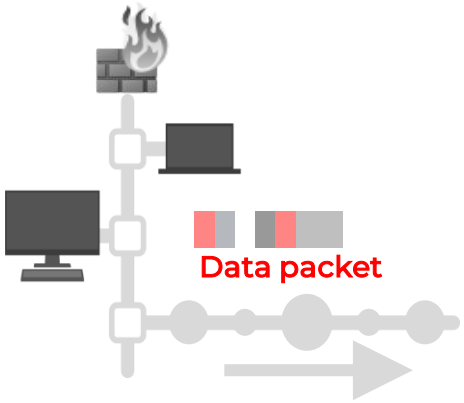
Stronger encryption technology protects critical data

# DUAL NETWORK

# DUAL NETWORK

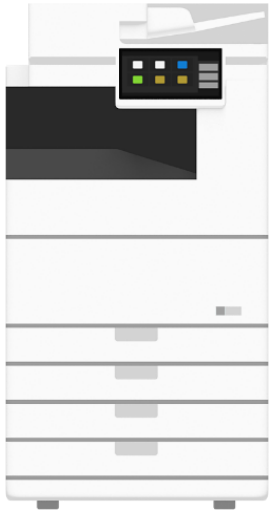

For example, the primary network should be used for secure and confidential information and secondary network for general use

# EVOLUTION OF SECURITY SETTINGS NAVIGATOR

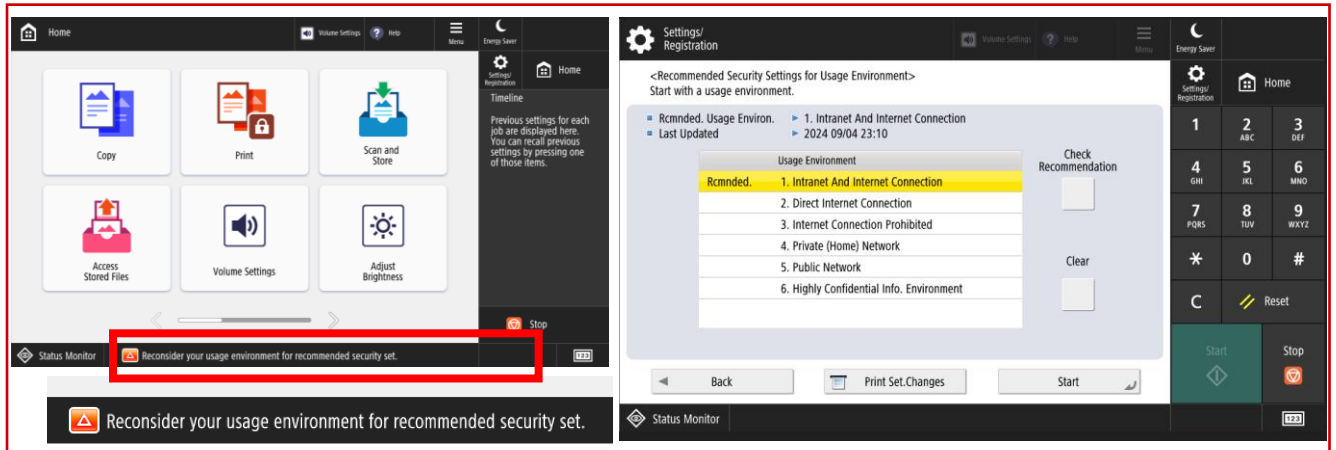



**STEP 1:**

Collect data packets from network



**STEP 2:**
Automated security settings recommendations




- Prevent missing security settings
- With AI-based assistance, users with no IT knowledge can configure the appropriate security settings
- Seamless flow completed on the device

# ALL-ROUND PROACTIVE SECURITY

**Secure Print/Forced Hold Print**
Prevent loss of documents

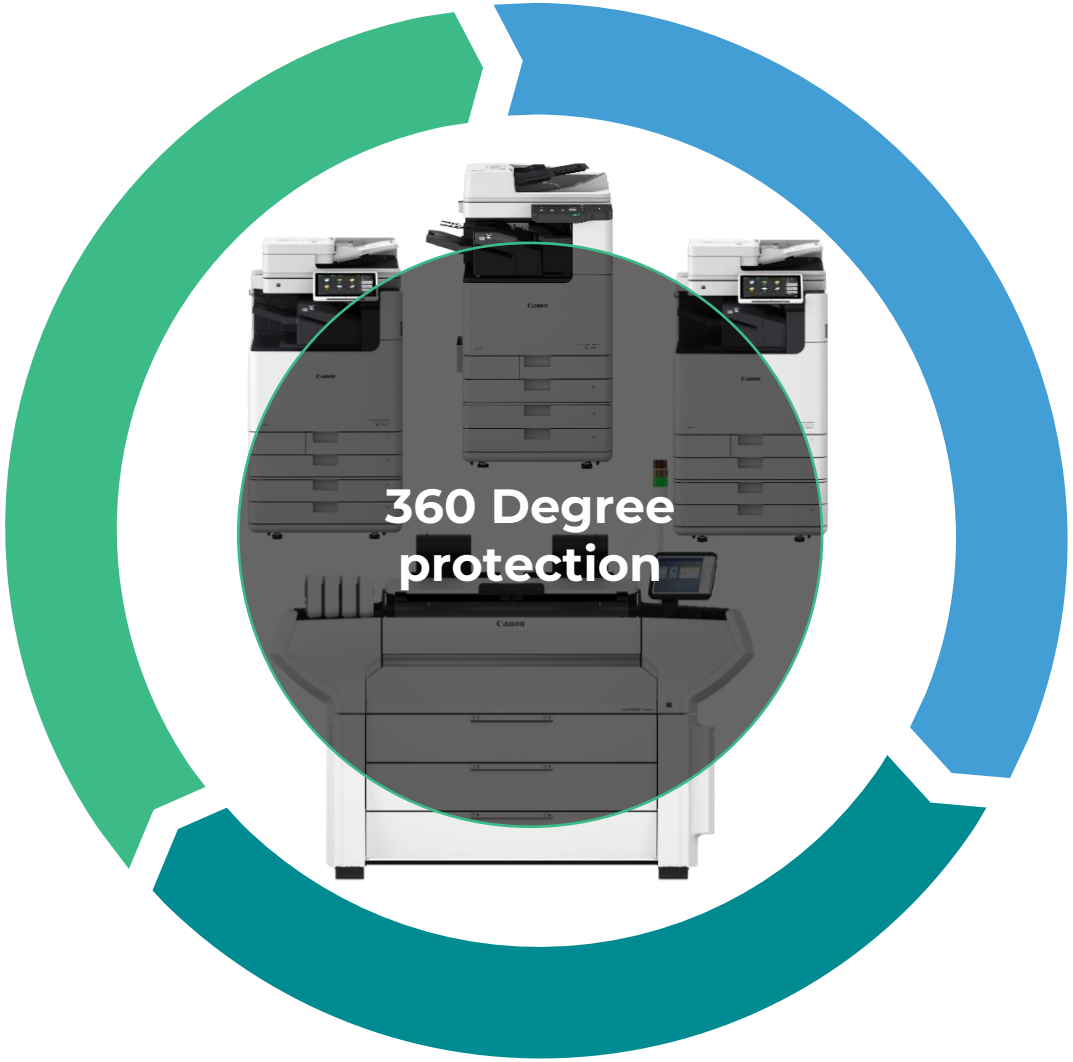
**NIST Purge data erase**
Protection against data leaks

**Encrypted PDF**
Protect data from unauthorised view

**Multi-factor authentication**
Access control

**0Auth 2.0**
Open standard authorisation

**Microsoft Entra ID**
**Cloud based authentication**




**Verify System at Start-up**
Prevent unauthorised changes

**Trellix McAfee Embedded Control**
Device protection from malware

**TPM 2.0**
Robust data encryption

**FIPS 140 Level 3**
Storage data protection

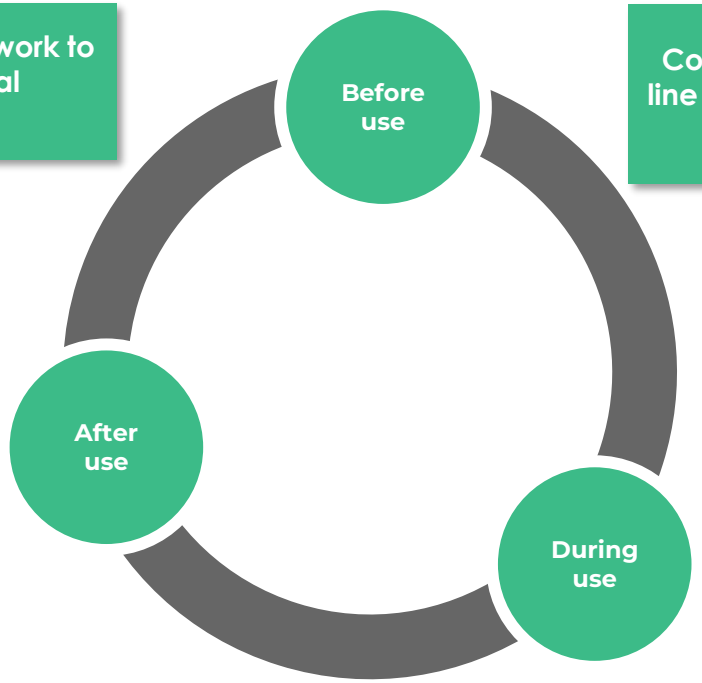
**SIEM Integration**
Real-time threat detection detection

**SAN**
Multi domain certificate

**WPA3-SAE**
**Password protection**

# A CONSTANT SEARCH FOR THE WEAKEST LINK...

# CANONS INFORMATION SECURITY SERVICES




**OFFICE HEALTH CHECK**

Scan your office network to identify potential vulnerabilities

**DEVICE HARDENING**

Configure your devices in line with the recommended hardening baseline

**DATA REMOVAL SERVICE**

Removal of data from your EOL devices

**DEVICE MANAGEMENT**

Additional security with remote firmware and application updates

**SECURE PROFILE MANAGEMENT**

Proactive monitoring and management of security configurations

**UNIFLOW & ZERO TRUST**

Assume no one can be trusted

# OFFICE HEALTH CHECK

A security analysis of your IT environment :

## ✓ Scan

A scan of your IT infrastructure, including of your firewall configuration.

## ✓ Analysis and validation

Based on the latest known vulnerabilities and guidelines from system vendors.

## ✓ Reporting

Detailed report, with risk descriptions and concrete recommendations.

# DEVICE HARDENING

- ✓ Device Hardening Service is a security service for Canon imageRUNNER ADVANCE and imageFORCE devices.
- ✓ 'Hardening' helps to improve a printer's performance and make it resistant to security issues.
- ✓ Our service enhances the security provided as standard from the factory, allowing you to benefit from additional protection.

# DEVICE MANAGEMENT SERVICE

- ✓ Device Management Service consists of various services such as:
- ✓ Fetching counter readings.
- ✓ Toner management.
- ✓ Proactive and remote services.
- ✓ **Content Delivery Service.**
  - ➢ **firmware update.**
  - ➢ **security updates.**

# SECURE PROFILE MANAGEMENT

- ✓ Secure Profile Management focuses on keeping devices secure throughout the contract duration.
- ✓ The agreed configurations and security parameters are constantly monitored.
- ✓ In case of detected changes, the parameters are reset to the pre-agreed configuration.
- ✓ The manner and timing of repair are determined in advance.

# UNIFLOW & ZERO TRUST

uniFLOW Online uses industry-leading Zero Trust principles.

## Explicit verification

Always authenticate and authorise based on all available data points.

## Assume breaches

Verify and analyse to improve threat detection and defence.

## Access with the fewest privileges

Limit user access with 'Just-In-Time' and 'Just-Enough-Access'.


bsi ISO/IEC 27001 Information Security Management CERTIFIED

bsi ISO/IEC 27017 Cloud Security Management CERTIFIED

# DATA REMOVAL SERVICE

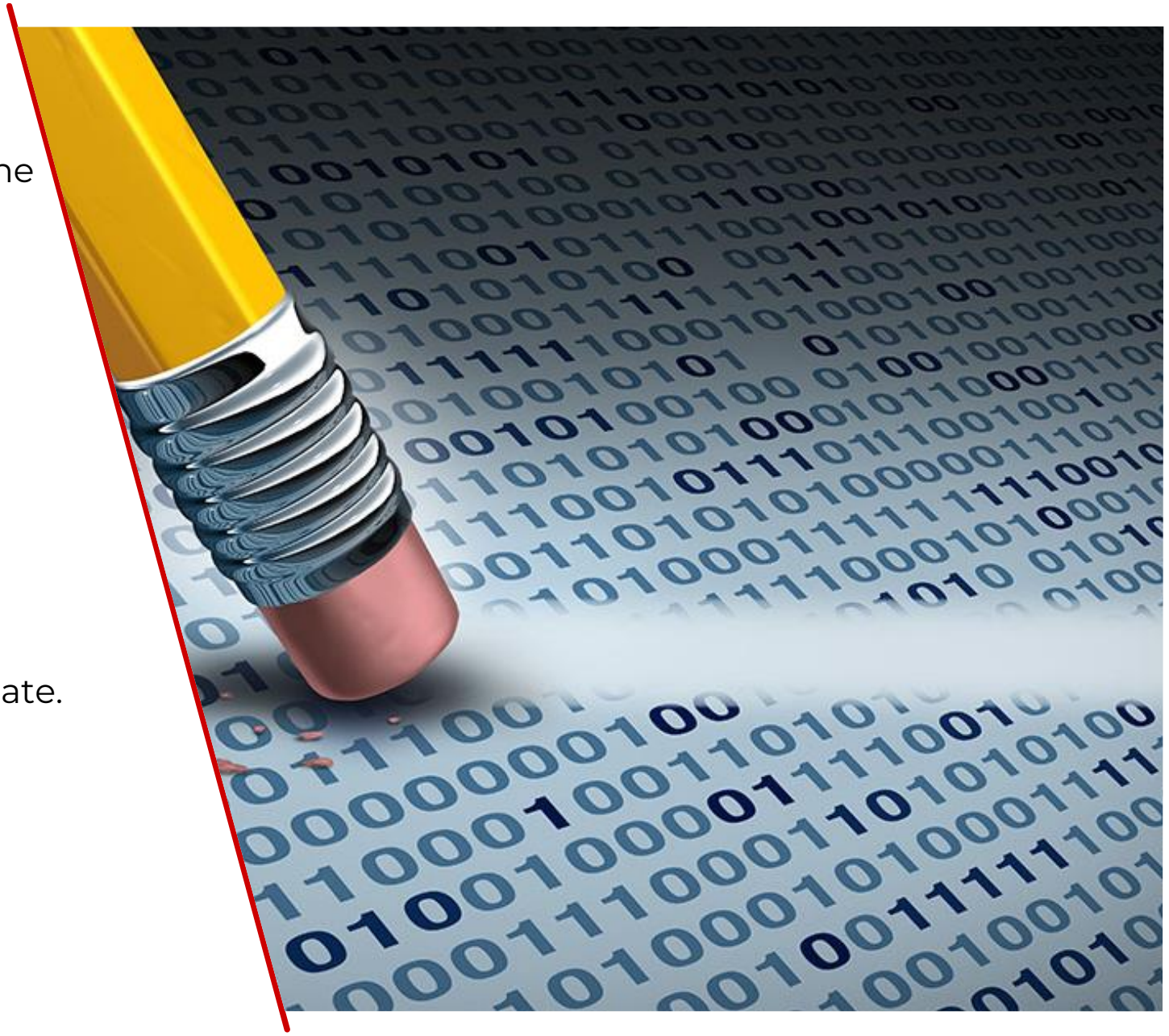
Data stored in printers is often overlooked at the end of a contract.

There are three options:

1. Secure Data Erase
2. Hard Disk Handover
3. Hard Disk Destruction

A physical inspection also takes place.

As proof of Data Removal, we provide a certificate.




BY COMBINING THE RIGHT TECHNOLOGY WITH OUR TAILORED SOLUTIONS AND SERVICES, WE STRENGTHEN EVERY LINK IN YOUR PRINTING INFRASTRUCTURE...

# THANK YOU...