A Comprehensive Approach to Printer Security

Single and multifunction printers are now capable of working at the heart of your business operations. With the exponential growth of wireless devices and cloud-hosted software and services, your printer not only needs to work with these new technologies, but also stay secure from them.

Prevent

Detect

Protect

External Partnerships

HOLISTIC PROTECTION FOR YOUR PRINTER

We, at Xerox, recognised and embraced the shift in technology and the evolving needs of the workplace a long time ago. We offer a comprehensive set of security features to keep your printers and your data safe. Additionally, we secure every part of the data chain, including **print, copy, scan, fax, file downloads** and **system software**. There are four key aspects to our multi-layered approach.

PREVENT

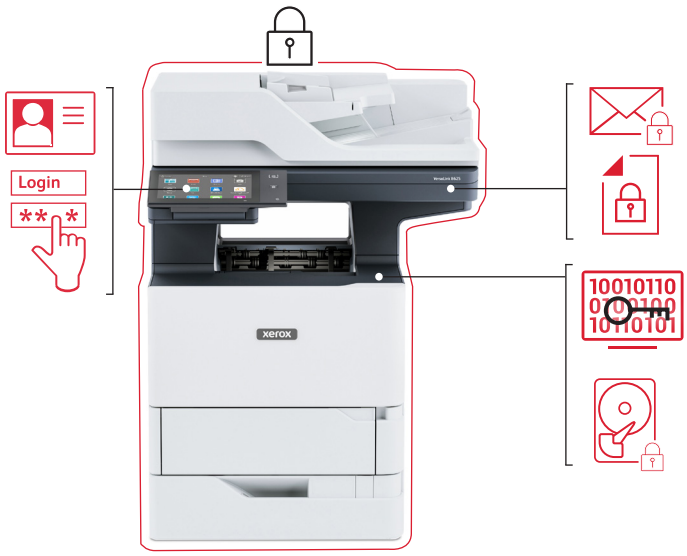
Your first and most obvious point of intrusion is the user interface, and maintaining control over who has physical access to your printer and its features is the first step. Our security measures start with intrusion prevention through **User Authentication** to ensure only authorised staff have access. Once in, **Role-based Access Control** ensures each team member only sees the features you want them to see. **Strong and complex password** enablement protects against hackers and malicious software, and support for **multi-factor authentication**[1] provides a further layer of security. Every action by each user is also logged, offering a full **Audit** trail.

Then we tackle less obvious points of intrusion – what is sent to the printer and how. Our system software is **Digitally Signed**: any attempts to install infected, non-signed versions result in the file being automatically rejected. Encrypted keys are stored on TPM chips, keeping printers secure from cyber attacks.

xerox™

DETECT

In the unlikely event that your data and network defences are bypassed, Xerox® ConnectKey® Technology will run a comprehensive **Firmware Verification** test, either at start-up[2] or when activated by authorised users. This alerts you if any harmful changes to your printer have been detected. Our most advanced built-in solutions use **Trellix* Whitelisting/ Allowlisting**[3] technology, which constantly monitors for and automatically prevents any malicious malware from running. Integration with **Cisco® Identity Services Engine (ISE)** auto-detects Xerox® Devices on the network and classifies them as printers for security policy implementation and compliance. Xerox® Devices integrate with market-leading SIEM software tools[4] to communicate security event data in real time. This aids in early breach detection and eliminates or mitigates the potential harm of security threats to the organisation.



PROTECT

Our comprehensive security solutions also protect your printed and scanned documents from unauthorised disclosure or modification. Xerox® ConnectKey® Technology helps block the deliberate or accidental transfer of key data to those not authorised to see it.

We protect print output using a **PIN Code** or **Card Release** system. We restrict scan information from reaching those who should not receive it using **digitally signed, encrypted and password-protected file formats**. ConnectKey Technology-enabled printers also let you **lock down 'to/cc/bcc' email** fields, limiting scan destinations to **internal addresses**.

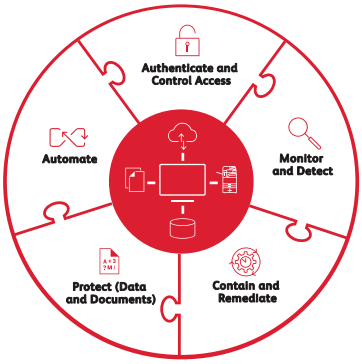
We also protect all your stored information using the highest levels of **encryption**. We delete any processed or stored data that is no longer required using the National Institute of Standards and Technology (NIST) and US Department of Defence-approved **data clearing** and **sanitisation algorithms**.[5]

EXTERNAL PARTNERSHIPS

We work with compliance testing organisations and security industry leaders such as **Trellix* and Cisco** to integrate their overarching standards and expertise into Xerox offerings.

For third-party independent proof that we achieve top levels of compliance, certification bodies like **Common Criteria (ISO/ IEC 15408)** and **FIPS 140-2/140-3** measure our performance against international standards. They recognise us for our comprehensive approach to printer security.

Our Bug Bounty[6] programme with HackerOne is another mark of confidence in our security measures, as well as an independent resource of technology validation.



XEROX SUPPORTS ZERO TRUST

With a combination of hardware, software and processes, we support your Zero Trust initiatives to make implementation simpler and more comprehensive.

Learn More: www.xerox.co.uk/en-gb/about/security-solutions/zero-trust-security

Trellix cisco LogRhythm splunk> hackerone

Learn more: **www.xerox.co.uk/en-gb/about/security-solutions**

[1] MFA is enabled through Xerox® Workplace Solutions and Cloud IdPs
[2] Xerox® VersaLink® Printers
[3] Xerox® AltaLink® MFPs, Xerox® VersaLink® 7100 MFPs, Xerox® WorkCentre® i-Series MFPs, Xerox® EC7800/8000 MFPs and Xerox® WorkCentre® EC7836/EC7856 MFP
[4] Trellix Enterprise Security Manager, LogRhythm and Splunk SIEM tools
[5] Applies to devices with Hard Disk Drives only
[6] Bug Bounty offered through HackerOne on Xerox® AltaLink® 8100 Series MFPs, with more products, solutions, and services to be added in the future
* Trellix was formerly known as McAfee Enterprise business

xerox™