Xerox:
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, cloud-hosted software and services, your printer not only needs to work with these new technologies, but also stay secure from them.

Intrusion Prevention

Device Detection

Document & Data Protection

External Partnerships

HOLISTIC PROTECTION FOR YOUR PRINTER

Xerox has long ago recognized and embraced this shift in technology and the evolving needs of the workplace. We offer a comprehensive set of security features to keep your printers and your data safe. Xerox secures 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.

INTRUSION PREVENTION

Your first and most obvious vulnerability is the user interface – who has physical access to your printer and its features. Xerox security options start with **User Authentication** to ensure only authorized staff have access. Once in, **Role Based Access Control** ensures each team member only sees the features you want them to see. 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. Xerox® ConnectKey® Technology will intercept attacks from corrupted files and malicious software[1]. Our system software is **Digitally Signed**: any attempts to install infected, non-signed versions will result in the file being automatically rejected. Print files will also get deleted if any part is not recognized as legitimate.

xerox

DEVICE DETECTION

In the unlikely event that your data and network defenses are bypassed, Xerox® ConnectKey® Technology will run a comprehensive **Firmware Verification** test, either at start-up* or when activated by authorized users. This alerts you if any harmful changes to your printer have been detected. Our most advanced built-in solutions use **McAfee® Whitelisting**** technology which constantly monitors for and automatically prevents any malicious malware from running.

DOCUMENT AND DATA PROTECTION

At Xerox, we drill down deeper. Our comprehensive security solutions also protect your printed and scanned documents from unauthorized disclosure or modification. Xerox® ConnectKey® Technology helps to prevent the deliberate or accidental transfer of key data to those not authorized to see it.

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

Xerox also protects all your stored information, using the highest levels of **encryption**. We delete any processed or stored data that is no longer required using National Institute of Standards and Technology (NIST), and U.S. Department of Defense approved **data clearing** and **sanitization algorithms**[2].

EXTERNAL PARTNERSHIPS

Xerox works with compliance testing organizations and security industry leaders such as **McAfee®** to wrap their overarching standards and knowhow around ours.

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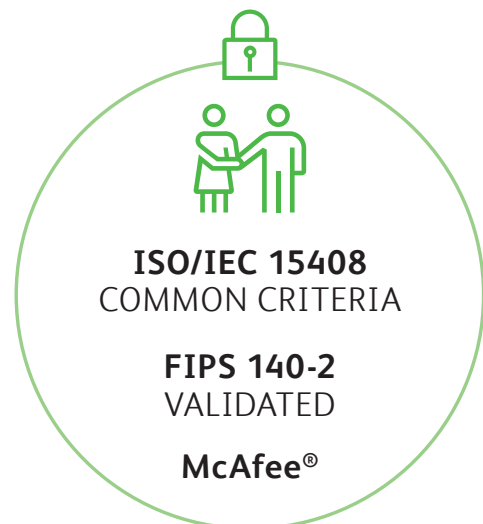
They recognize us for our comprehensive approach to printer security.

ISO/IEC 15408
COMMON CRITERIA

FIPS 140-2
VALIDATED

McAfee®

* Xerox® VersaLink® Printers
** Xerox® AltaLink® and i-Series Multifunction Printers
[1] Malware interception with McAfee® Whitelisting Technology
[2] Applies to devices with Hard Disk Drives only

Learn more: **Xerox.com/security**

xerox®