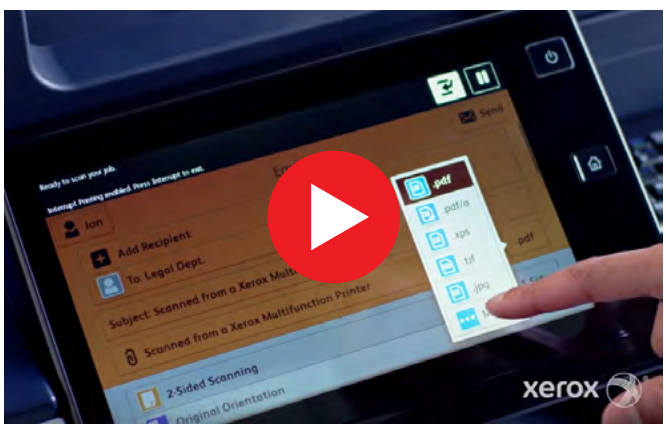
State-of-the-Art Printer and Data Security

Exceeds industry standards for security features and technologies

Security is a top priority for us, and we know it is for your business, too. That's why every **Xerox® ConnectKey® Technology-enabled device** is armed with our holistic four-point approach to security, ensuring comprehensive, all-encompassing protection for all system components and points of vulnerability.



1. Intrusion prevention

A comprehensive set of capabilities prevents malicious attacks, proliferation of malware, and misuse of unauthorised access to the printer. Whether from transmitted data or directly at the MFP, all access points are protected through user authentication and access controls.

2. Device detection

A comprehensive Firmware Verification test, either at start-up* or when activated by authorized users, provides alerts if any harmful changes to the printer have been detected. **McAfee® Whitelisting** technology** 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®

3. Document & data protection

Capabilities prevent intentional or unintentional transmission of critical data to unauthorised parties. Documents are not released until the right user is at the device and scanned information is protected from unauthorised users. Xerox also protects stored information, using the highest levels of encryption. Processed or stored data that is no longer required can be deleted using National Institute of Standards and Technology (NIST) and U.S. Department of Defense approved data clearing and sanitisation algorithms.

4. External partnerships

ConnectKey Technology provides extra security standards through our partnerships with **McAfee®*** and **Cisco®**. We measure our performance against international standards with certifications like **Common Criteria** and FIPS 140-2 to ensure our devices are trusted in even the most secure environments.