Lexmark™

Secure by Design

Challenges with print security

Malicious security attacks and network security gaps are everywhere, leading to costly compliance breaches and business-disrupting data loss. The impact for users is wasted time and loss of privacy; for organizations, it means negative financial impacts and harm to the company's reputation.

Unfortunately, many organizations overlook their own print environment when addressing security concerns. Securing an enterprise environment against vulnerabilities is complex and requires a comprehensive understanding of software, hardware, network architecture, the content traveling on the network and each organization's specific security goals. It also requires expert knowledge and practical experience to translate theoretical security concepts into products and solutions that protect important assets.

Secure by Design

Lexmark's expertise as an industry leader in document and device security forms the backbone of our technology. This systematic, "Secure by Design" approach delivers a critical benefit to our customers: the confidence to efficiently and cost-effectively run their business, knowing devices and data are protected every step of the way. Lexmark doesn't treat security as an afterthought or optional feature, but as an integral design and engineering goal embedded in all our products and services.

Our understanding of network environments and relevant security threats, particularly in relation to printing, gives us the know-how to create unique solutions that secure your data in every possible way—a capability we've proven by working and overcoming security challenges in some of the most highly regulated organizations and industries on earth.

Product design: Lexmark's Secure Software Development Lifecycle (SSDL) is designed to address all aspects of security from planning through design and implementation, including quality assurance, release and maintenance.

Supply chain integrity: Across Lexmark's supply chain, employees and supply partners operate in full compliance with local laws and regulations. Lexmark strictly adheres to specifications ensuring that products and parts designed for the device are the same that are delivered. This eliminates the possible insertion of rogue chips or other nefarious elements not specified in the original design. In fact, Lexmark is the first print vendor with an IOS 20243 supply chain security certification for the entire printing device.

Security features: Our comprehensive approach to security delivers features and functions designed to protect every aspect of your output environment and meets the most stringent industry and government security standards.

Industry certifications: Lexmark third-party certifications include Common Criteria and FIPS (Federal Information Processing Standard) to help protect sensitive information across the network. Plus Lexmark product security posture has been recognized by IDC, Quocira and Keypoint Intelligence.

Vulnerability management: Lexmark security experts constantly monitor multiple channels to identify potential security vulnerabilities, and if the need arises, react quickly to limit exposure to threat.

Advanced security features

Security is built into every Lexmark product, with advanced standard security features designed for each product's intended use and flexible options available to meet special requirements.

Secure access features restrict who can use your devices and what they can do.

Network security features protect devices from unauthorized access over network interfaces.

Document security features keep your documents—whether physical or digital—out of the wrong hands.

Secure remote management provides a wide range of tools and device capabilities to effectively manage a fleet of networked laser printers and multifunction products.

Security solutions enhance the security of Lexmark devices by meeting specific objectives like print release and automatic security certificate deployment.

Hard disk security protects Lexmark printers and multifunction products that contain internal hard disks with a virtual shield to protect your organization's most valuable assets.

Encrypted and signed firmware ensures that only firmware created by Lexmark systems can be installed on our devices. These protections prevent malicious actors from reverse-engineering firmware and installing harmful code on Lexmark devices.

Secure boot technology validates firmware integrity several times during the boot process. If non-genuine firmware is detected, the device will revert to a known, trusted copy of the firmware.

Continuous verification ensures the device and its instructions have not been tampered with during operation.

Markvision Enterprise: solution for complete security

To enhance existing security policies, organizations need a robust fleet management software like Lexmark Markvision Enteprise 4.0. This solution is a key component of Lexmark's Secure by Design approach, engineered to ensure optimum security for every device in your network. With Markvision Enterprise, you can easily manage device configuration on a fleet of printers across a network, scalable to thousands of devices. And unlike other solutions, Markvision Enterprise manages both device configuration and security policies in a single, easy-to-use tool.

Markvision Enterprise is newly updated to give you greater visibility into your entire fleet of network printers and multifunction devices. The advanced yet intuitive toolset makes it easier than ever to configure device settings and update security policies while reducing the burden on IT staff. And because helping customers secure their print environment is a key priority, Lexmark offers Markvision software at no cost to your organization.

Learn more at www.lexmark.com/security

Industry-leading certifications

Anyone can say their products are secure. At Lexmark, we've proven our security expertise by meeting the most stringent government and industry standards and certifications, including Common Criteria, FIPS, NIST, ISO 27001, ISO 20243 and UL CAP (UL Cybersecurity Assurance Program.) These third-party validations assure our customers that industry-leading security capabilities protect every Lexmark device and solution across their organization's network.