Print security: know your risk, protect your assets

Did you know that unsecured print equals unsecured IT? It's true. Consider the thousands of potential security threats across an output fleet made up of varied devices and vendors, all of which must be managed separately to ensure they are secure. And each day with an outdated, multi-vendor fleet means an increased risk of security breaches to your organization.

You might not spend much time thinking about print security, yet it should be a vital part of your IT planning process. Assessing devices, network management and document solutions for potential vulnerabilities—and developing a strategy to close the gaps—are important steps in protecting information of all types across the enterprise.

An increasing number of costly security breaches reinforces the importance of assessing your current print infrastructure. Get it wrong, and you put your entire organization's performance and reputation at risk.

For over ten years, Lexmark has provided the highest level of security by delivering devices tailored to meet our customers' unique requirements that integrate seamlessly into enterprise-wide security practices. Lexmark's proven methodology focuses on security as a critical component of infrastructure optimization and can significantly reduce security gaps between documents, devices, the network and all points in between.

Secure devices: Many organizations are filled with aged, poorly secured print devices. Your best defense is to implement secure access features that restrict who can use output devices using predefined user access controls.

- **Digitally signed firmware and software updates**
  Encryption and digitally signed firmware of files ensures that only firmware created by the vendor can be installed on enterprise devices
- **Access control to device functionality**
  Individual users and groups use credentials to access the device and the authentication and authorization mechanisms can determine if a user has appropriate access to modify device settings or leverage functionality
- **Security configuration**
  Custom configurations ensure that devices match security policies and remediate automatically if a device is out of conformance
- **Physical locks on hard drives and drawers**
  Ability to provide physical protection for access to hard drives or paper trays allows for an extra level of security for confidential data and print supplies
- **Out of service**
  When devices are removed from a secure location temporarily or permanently, you can perform an out of service wipe to remove all settings/data/information stored on the hard disk or memory of the device

Secure network and device management:

With increased use of mobile devices and the need to support BYOD initiatives, IT departments must strike a balance between providing users with the tools they need to boost efficiency while minimizing the risk of intrusion across networks and connections.

Digital certificates

Certificate authority (CA) certificates allow a device to trust and validate the credentials of another system on the network

IP address filtering

Network devices are configured to allow TCP/IP connections only from a specific list of TCP/IP addresses

Secure communication protocols and capabilities

Communication with the device is not only protected via access control but the latest in network communication protocols such as Transport Layer Security (TLS) and Simple Network Management Protocol (SNMP) are being leveraged

Secure protocol restrictions

Devices are restricted to use the latest versions of secure communication protocols such as version 1.2 of TLS and/or version 3 SNMP

Port filtering

Filtering increases control over network device activity and is used to configure devices and filter out traffic on specific network ports

Device audit capabilities

The event-tracking feature proactively tracks and identifies potential risks and may be integrated with your intrusion detection system for real-time tracking

Secure document solutions

Information that is printed on or transmitted through print devices could be your organization's greatest area of vulnerability because security threats often come from within your organization rather than from outsiders.

Prohibit unauthenticated printing

Malicious printing can be prevented on a device by configuring to only allow print jobs if the user has authenticated

Contact and contactless card authentication

Administrators can grant access to device function and apps with the same magnetic stripe or proximity cards that employees use for access to physical facilities

Print Release solutions

Users can print jobs from anywhere including desktop, tablet or smartphone, and release jobs for printing when they are ready and from any location

Confidential Print

A standard part of the Lexmark Universal Print Driver, Confidential Print holds your job on a specific Lexmark printer or MFP until you release it with a PIN, preventing prying eyes from viewing documents in the output bin

Learn more at lexmark.com/security