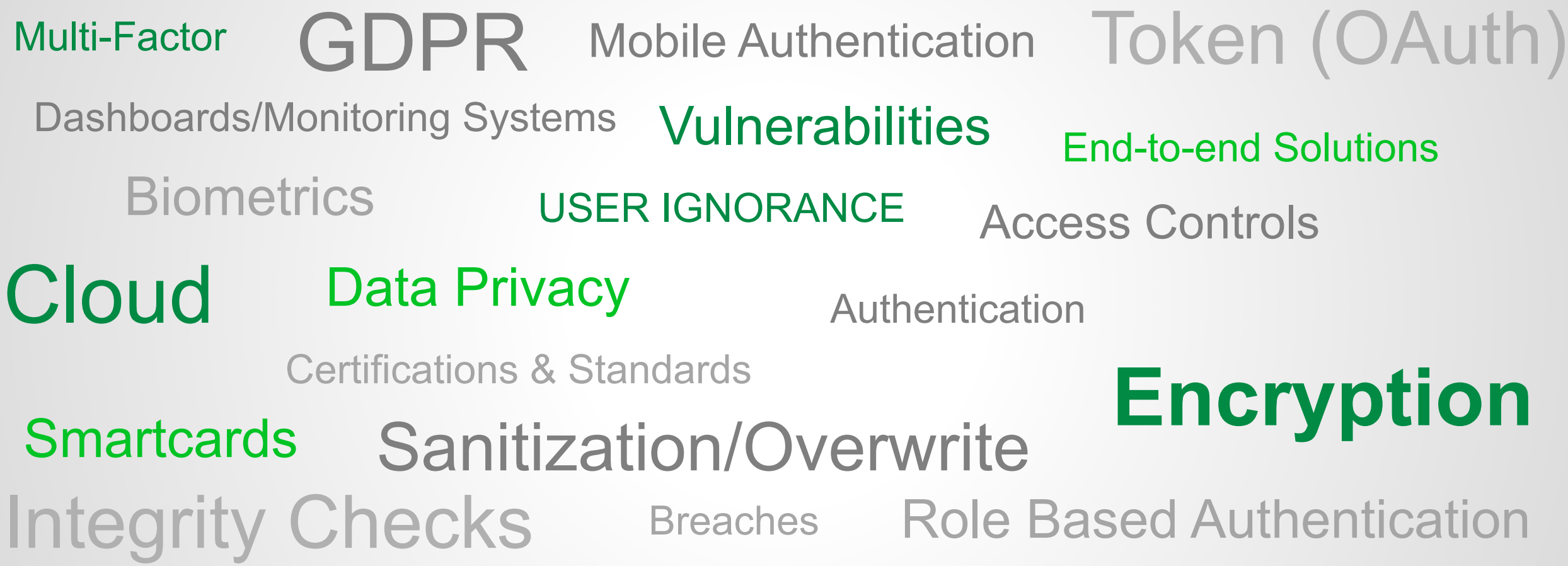
Full Spectrum Security from Lexmark

Lexmark™



© 2017 Lexmark. All rights reserved.

Unsecured print = Unsecured IT

80%* of organizations

Security policy in place for accessing documents, along with what and where information can be stored

63%* of organizations

Security policy about what printers and MFPs can be used to print, scan, fax or copy documents

61%** of large enterprises

Admitted suffering at least one data breach through insecure printing

Profile of typical enterprise fleet

54% Devices 5+ years old

52 Models

6 Manufacturers

Bottom line: Unsecured print = Unsecured IT

*Based on results from IDC's Print Security Survey, IDC #US40612015

**Quocirca 2017 report, Print security: An imperative of the IoT era

Lexmark

© 2018 Lexmark. All rights reserved.

Organizations are asking for a solution

Market Trends

Ability to lock down a print device

Control use of device features

Protect confidential printing

Provide audit trails for print

Establish chain of custody for print

of companies experienced at least one data breach through printing[1]

of companies ignore printers in their endpoint security strategy[3]

1 out of 6 companies have a strategy for print security

of breaches were caused by unsecured printers or MFPs[1]

of employees have printed, copied or scanned confidential information at work[3]

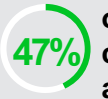
of data breaches were caused by human error[2]

of companies experienced more than one data breach through printing[1]

of all printed documents are never collected[3]

of companies place a high importance on the security of printed documents

of employees do not always follow their company's IT security policies[3]



of data breaches were caused by malicious attacks[2]

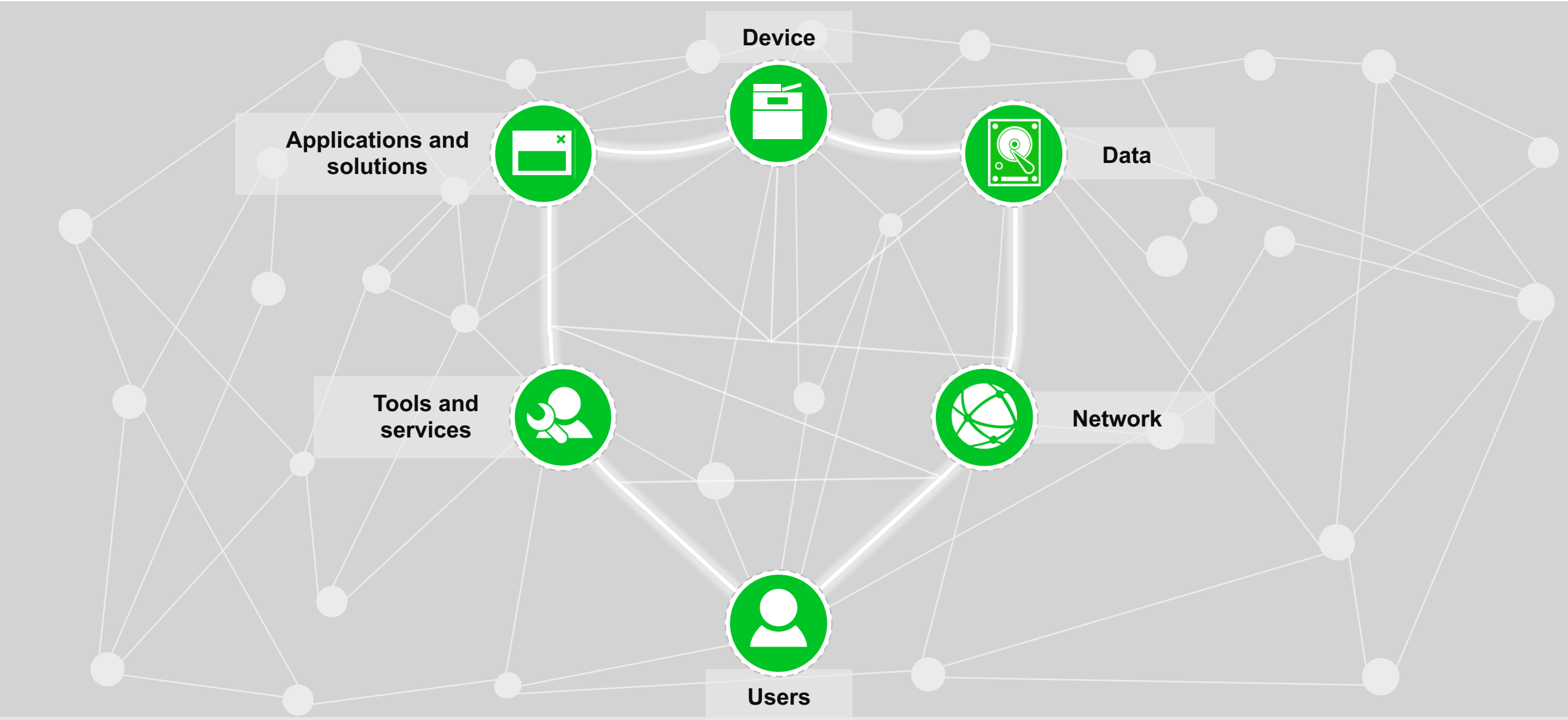
of data breaches were caused by flaws in the IT infrastructure[2]

1. 2017 Print Security Report, Quocirca Ltd.
2. 2017 Global Cost of a Data Breach Report, Ponemon Institute
3. Is printing the biggest security threat for your business? SC Media, June 2016

Lexmark

© 2017 Lexmark. All rights reserved.

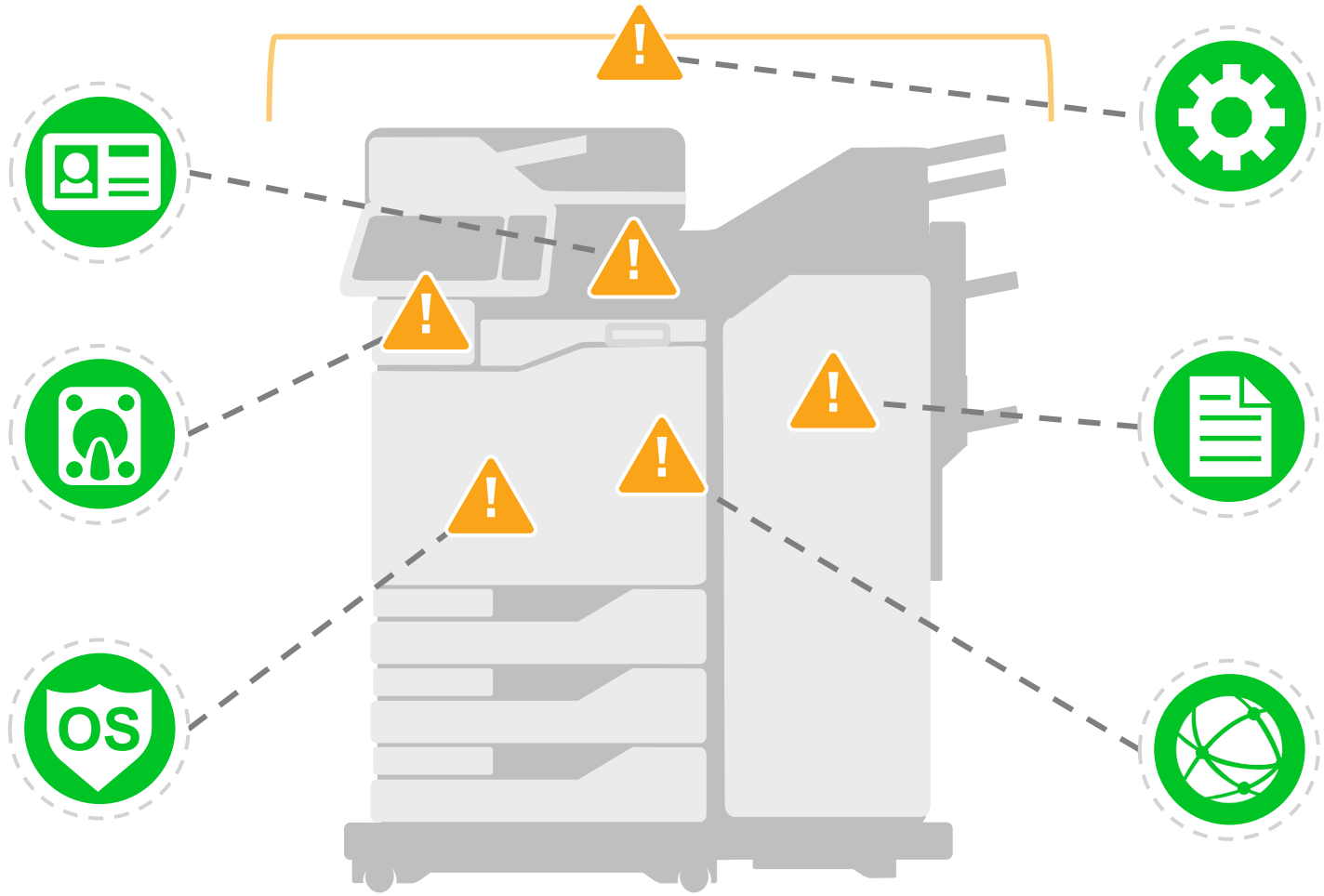
Our approach: Full-spectrum security



Lexmark
© 2017 Lexmark. All rights reserved.

Key areas of concern

Awareness around risk has increased, but most are still behind mitigating risks and protecting hardcopy output



© 2017 Lexmark. All rights reserved.

Lexmark security spectrum

Complete security throughout and around the device and document

User authentication

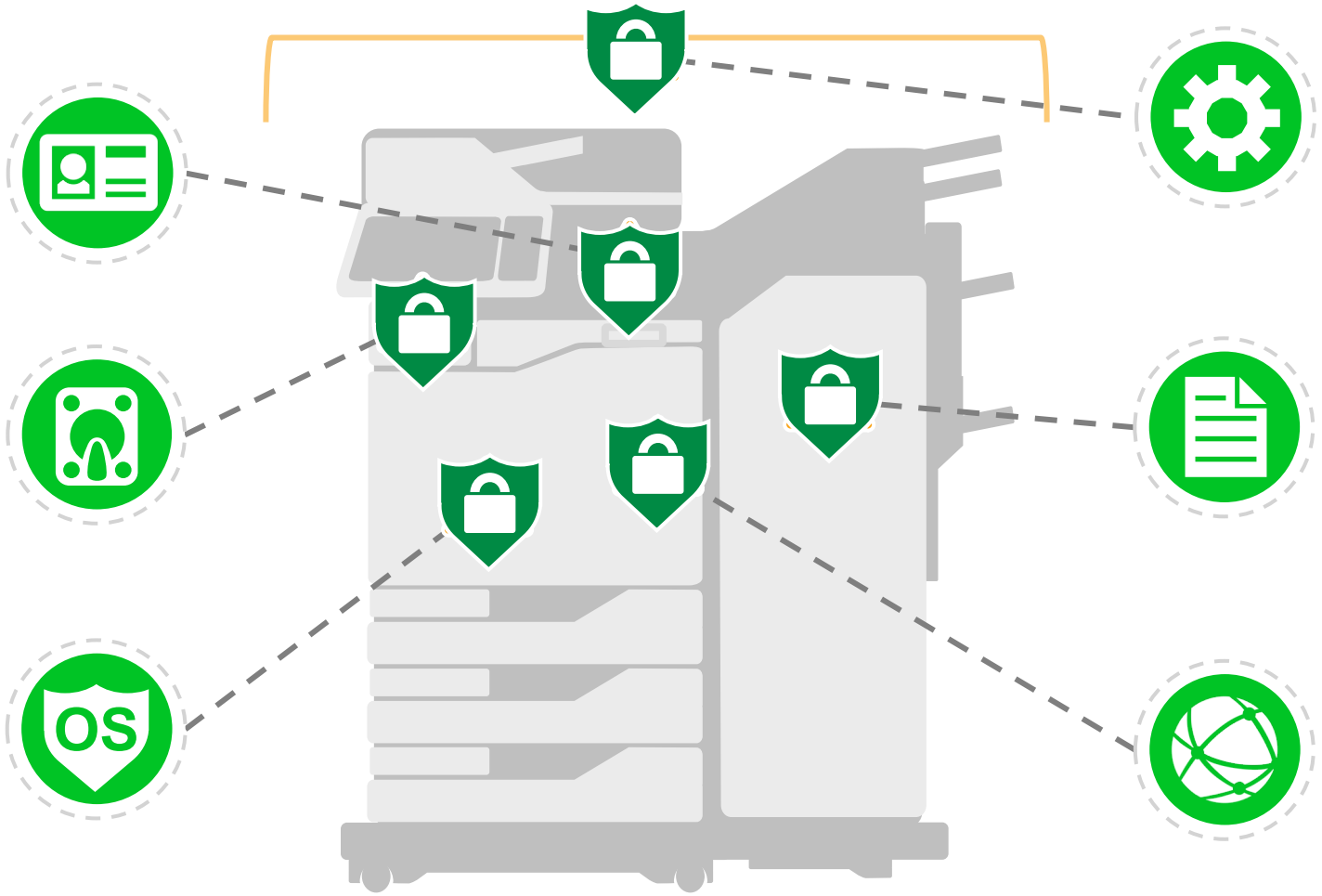
- Role based authentication
- System integration

Hard disk security

- Hard disk drive encryption and disk overwrite

Device protection

- Operating system security
- Secure firmware updates



Tools

- Device/fleet management
- Consumables management
- Asset management

Secure output

- Print Release
- Confidential Print

Network protection

- Secure network connections
- TCP / IP restrictions

© 2017 Lexmark. All rights reserved.

Secure by design…

…historically ahead of the curve

2005

Digitally signed & encrypted firmware

Embedded Encrypted HDD

White Listing

2008

Embedded Secure File Erase

Audit Logging

Function Access Controls

2010

Secure Boot

Runtime Intrusion Detection

Embedded FIPS 140

2012

Device Active Directory Integration

Remote HDD wiping & encryption

2016

Permission Based Security

SMBv3 Support

TLS 1.2

Many **vendors** are announcing **new** security features …but **not new to Lexmark**

© 2018 Lexmark International, Inc. All rights reserved.

Over a decade of meeting customer security needs

Owning our technology allows us to adapt quicker to our customers security needs

2005

- **Digitally signed & encrypted firmware**
- **Digitally signed & encrypted Embedded Apps**
- **HDD encryption & wiping**
- IPSec capabilities
- USB whitelisting

2008

- **OS secure boot technology**
- PKI certificate management
- Role based authorization
- **Function access controls**
- Manual & scheduled HDD wiping
- Device auditing

2010

- **OS continuous run-time verification checks**
- Automatic file-based wiping
- Non-volatile memory wiping
- Customizable access controls

2012

- **Device AD integration**
- Automatic CA installation
- Auto device certificate enrollment application
- Remote HDD wiping & encryption

2016-Current

- Secure element
- Improved AD integration
- **Permission based security**
- Improved “Suite B” cryptography
- SMB 3.0 support
- Common criteria updates

Lexmark device security ecosystem

IP Address Filtering
Simple Certificate Setup Capabilities
Fax/Network Separation
Port Blocking
Improved Authentication
- Simple Bind
- Kerberos
- LDAP+GSSAPI

PrintCryption
HTTPS
802.1x
SNMPv3
USB Thumb Drive Controls
Operator Panel PIN
Improved Port Filtering
Confidential Print Improvements
Physical Locks
ISO 15408 Compliance

Additional Authentication Configuration Options
Encrypted Scan Data
Configurable Logout Timeout
Email Domain Control
Fax Lock (Schedulable)
Fax Forwarding
Device Locking
User/Advanced Passwords
Embedded Applications
Secure IPP

Password Protected Hidden Menus
Additional Badge Reading Capabilities
Additional USB Controls
Advanced EWS Controls
Secure Device Reset
Advanced Address Book Queries
SMTP Server Authentication
Secure PDFs
Secure NTP
Server Based PrintCryption
FIPS Certified Algorithms

Improved Active Directory Integration
Improved Smart Card Authentication Capabilities
Improved Access Controls for eSF
Increased IPSec Connections
Automatic Device Account Enrollment
Improved Troubleshooting Capabilities
Increased TCP Filtering Connections
Improved Auditing Capabilities
Secure Serverless Print Release Capability
FIPS 140-2 Crypto Module Validation
Advanced Role Based Account Permissions

© 2017 Lexmark. All rights reserved.

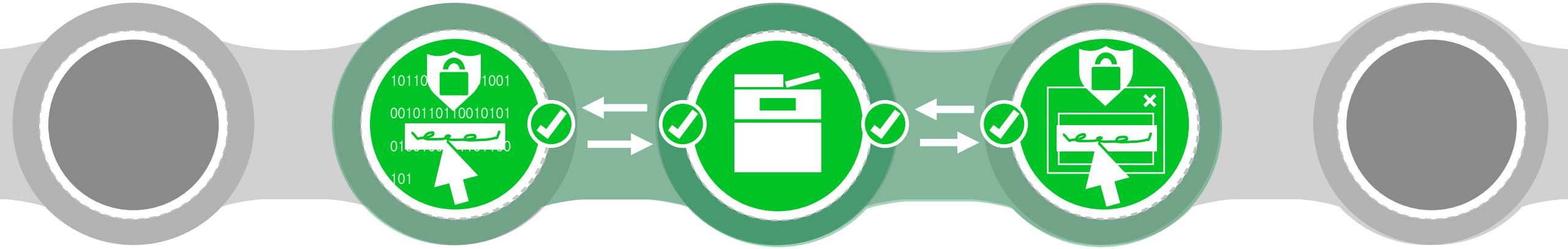
Embedded OS/firmware/solutions protections

Device operating system

- Linux based OS
- Remove standard applications
- Create custom applications
- Firewall OS after all modifications are completed

Firmware update security

- Data is encrypted
- Data is digitally signed by Lexmark
- Limited to authorized users



Boot/run chain of trust

- Physical hardware validation
- Bootloader validation
- Kernel validation
- Designed to provide continuous verification and tamper detection

Embedded solutions

- Similar protections as firmware
- Encrypted and verified by the device
- Authenticity and verification via digital signatures
- Limited to authorized users

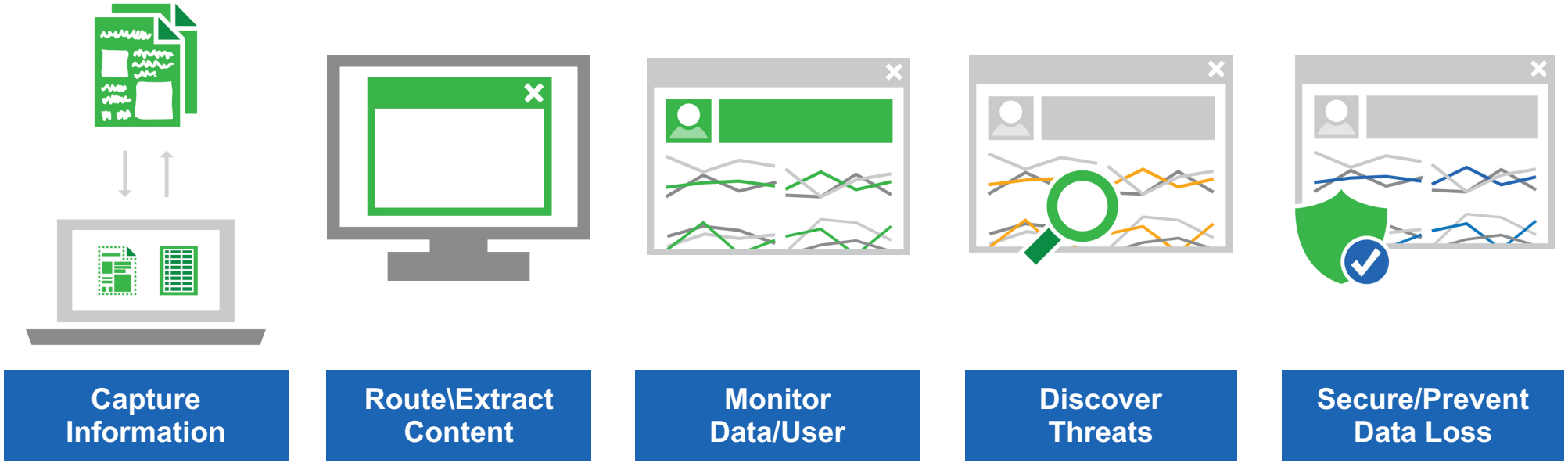
Lexmark™

© 2017 Lexmark. All rights reserved.

Solutions to the Insider Threat and Paper Problem

- Lexmark Print Management (Basic Hardcopy Security)

- Lexmark Document Monitor with Intelligent ID (Advanced Hardcopy and Digital Content Security)



Lexmark

Full Spectrum Security and Markvision Enterprise

Ensure your devices meet your security policies with printer configurations

- Ensure firmware is up to date
- Enforce functional access controls to prevent changes to security settings
- Set up devices to work with your LDAP system for authentication

Use scheduled tasks for automation and increase efficiency of support staff

- Discover new printers on the network and automatically enforce a configuration
- Check conformance of your configurations to ensure printers stay in compliance

Certified security

by recognized third parties

HARDWARE

INFORMATION

STANDARDS

INFORMATION

CYBER SECURITY

© 2018 Lexmark International, Inc. All rights reserved.

Common Criteria Certifications

Current Certificates

Protection Profile for Hardcopy Devices [HCD], version 1.0

Certificate of Product Evaluation
[PDF 200.67 KB]

Lexmark CX920, CX921, CX922, CX923, CX924, XC9235, XC9245, XC9255, and XC9265 Multi-Function Printers

Certificate of Product Evaluation
[PDF 200.30 KB]

Lexmark CX820, CX825, CX860, XC6152, XC8155, and XC8160 Multi-Function Printers

Certificate of Product Evaluation
[PDF 200.74 KB]

Lexmark CS921 and CS923 Single-Function Printers

Certificate of Product Evaluation
[PDF 200.62 KB]

Lexmark C6160 and CS820 Single-Function Printers

Certificate of Product Evaluation
[PDF 200.33 KB]

Lexmark CX725h and XC4150 Multi-Function Printers

Certificate of Product Evaluation
[PDF 200.45 KB]

Lexmark CX725 and XC4140 Multi-Function Printers

Certificate of Product Evaluation
[PDF 200.87 KB]

Lexmark C4150, CS720 and CS725 Single-Function Printers

© 2018 Lexmark International, Inc. All rights reserved.

Security in the news for Lexmark

IDC Analyze the Future

IDC MarketScape

IDC MarketScape: Worldwide Security Solutions and Services Hardcopy 2017 Vendor Assessment

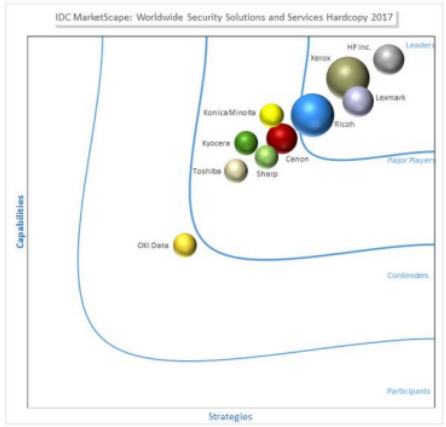
Robert Palmer Allison Correia

THIS IDC MARKETSCAPE EXCERPT FEATURES: LEXMARK

IDC MARKETSCAPE FIGURE

FIGURE 1

IDC MarketScape Worldwide Security Solutions and Services Hardcopy Vendor Assessment



Source: IDC, 2017

Please see the Appendix for detailed methodology, market definition, and scoring criteria.

October 2017, IDC #US41988517e

KEYPOINT INTELLIGENCE Buyers Lab

2017–2018 PaceSetter Award

Lexmark™

BLI PaceSetter 2017–2018:
Document Imaging Security

Lexmark International, Inc., has been honored with a prestigious BLI PaceSetter award in the Document Imaging Security category from the analysts at Keypoint Intelligence - Buyers Lab (BLI) thanks to its...

- Top-tier scores in almost every category in the study, including those covering device authentication, hard drive security, and firmware integrity
- Security features on its single-function printers that generally match those found on its more advanced MFPs
- Experience and strength in securely tying printers and MFPs to workflow software
- Excellent device-management security features found in the company's Markvision Enterprise platform

Document and device security is a concern in every organization, but printers and MFPs can often be the weak link in the document chain of custody. Fortunately, manufacturers of office document technology have tightened and improved their hardware, software solutions, and services to mitigate security gaps. To determine which OEMs lead the market, analysts at Keypoint Intelligence conducted an in-depth evaluation of the security ecosystems of 13 document imaging OEMs. The granular study drilled down into 140 points of potential differentiation spread across eight categories. Based on these findings, the analysts at BLI have recognized Lexmark International, Inc. with a BLI PaceSetter award in the Document Imaging Security arena.

In the study, Lexmark stood out in key hardware areas such as device authentication and hard drive security. It also scored very well in firmware and app integrity, an area that proved to be a challenge for the industry as a whole. On the software front, Lexmark's Markvision Enterprise device management software also earned high marks when it comes to security: The solution continuously checks devices on the network and can automatically remedy any security settings that are out of conformance.

KEYPOINT INTELLIGENCE Buyers Lab

©2017 Keypoint Intelligence. Reproduced with permission. For reprints, contact info@keypointintelligence.com.

Lexmark™

Printers Supplies & Accessories Industries & Solutions Services Customer Support

Lexmark Newsroom
News Releases
Lexmark in the News
News Alerts
New Products
Analyst Insights
Success Stories
August 2017: A3 Color Laser Printer and Smart MFP Launch
New: April 2018: A4 SMB Monochrome Launch
Lexmark Logo

News Releases

Lexmark Devices Achieve Latest Common Criteria Certification

Certification validates Lexmark devices meet the latest international security requirements for printers to assure device, document and network security.

May 10, 2018

Lexmark, a global imaging solutions leader, today announced it has achieved certification against the latest Common Criteria Security Protection Profile, Hardcopy Devices v1.0 (HCD-PP v1.0). The Protection Profile for HCD-PPv1.0 is based on security requirements specified by the U.S. and Japanese governments for printers, designed to assure device, document and network security.

Common Criteria provides a framework to validate the security functionality of a system by performing a set of rigorous and repeatable tests. This framework provides participating countries assurance that tested products meet internationally accepted security functional criteria. The compliance of Lexmark devices with the standards is validated by an internationally approved independent laboratory using the latest policy guidance.

An evaluation that finds a product in compliance with the Common Criteria requirements is accepted as valid by all bodies that have signed the Common Criteria Recognition Agreement (CCRA). Signatories include the U.S. National Information Assurance Partnership (NIAP). Membership in the CCRA can, in practice, result in common procurement requirements among participating governments.

" This latest Common Criteria certification further recognizes the effectiveness of Lexmark's full-spectrum security approach, validating that our customers across the globe can rely on Lexmark to meet the world's most stringent security standards. "

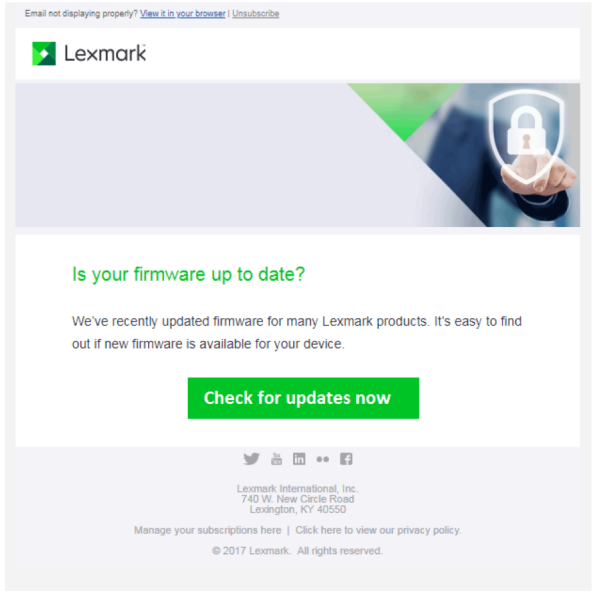
"Building a secure bridge between digital and hardcopy information is at the core of what we do at Lexmark," said Allen Waugerman, senior vice president and chief technology officer. "This latest Common Criteria certification further recognizes the effectiveness of Lexmark's full-spectrum security approach, validating that our customers across the globe can rely on Lexmark to meet the world's most stringent security standards."

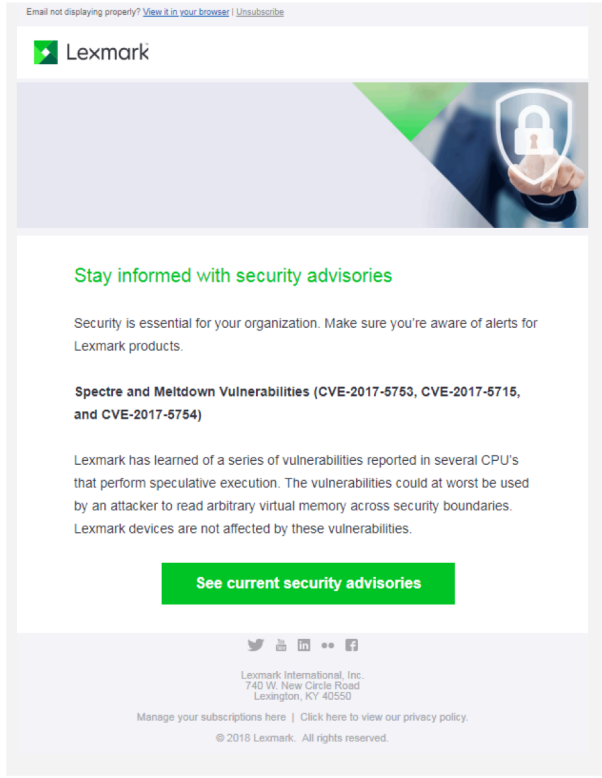
© 2018 Lexmark International, Inc. All rights reserved.

Update Email

Lexmark now has an automated method through email to send alerts to anyone who registers for Firmware and/or Security updates. This email will direct them to support.lexmark.com for latest firmware and to the alerts page for security.

https://www.lexmark.com/en_us/GlobalPreferenceCenter.html





What makes Lexmark different?

In-house development

- Ability to customize
- React with speed

Industry experience and insight to technology

- Holistic approach that focuses on device, data, network, user, software/solutions and services
- Security is developed as part of a solution not an add-on

Understand customer needs/requirements

- Develop a security strategy
- Flexibility to change as the customer environment changes

Third-party certifications

- NIAP common criteria validation
- FIPS algorithm validation

Lexmark™