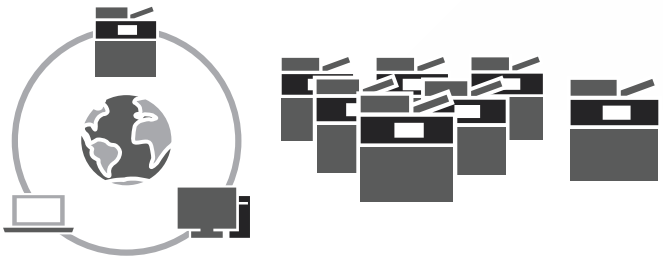
Full-spectrum security

Malicious security attacks and inadvertent vulnerabilities can lead to costly compliance breaches and business-disrupting data loss. They can also take a human toll in frustration, loss of privacy, negative financial consequences and wasted time.

Securing an enterprise environment is complex and requires a comprehensive understanding of software, hardware, network architecture, the content traveling on the network, human factors, and each organisation's specific security vulnerabilities and goals. And it requires expert knowledge and practical experience to translate theoretical security concepts into secure products and services.

Lexmark security ecosystem



Network Fleet Device

Lexmark understands the multi-faceted reality of security threats and responds with a holistic, systematic approach that encompasses the device, the fleet and the whole network infrastructure.

Security by design

That's why 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 organisations and industries on earth.

And our expertise pays off in concrete ways whether you manage your own printing infrastructure or rely on Lexmark Managed Print Services.

Keys to product security

- Secure access
- Network security
- Document security
- Secure remote management
- Security Solutions
- Hard disk security
- Standards and certifications

18KD08617

Embedded security features and architecture

Security is built into every Lexmark product, with standard security features appropriate to each product's intended use and available options to fulfil special requirements. Our comprehensive approach to product security covers a full spectrum of security capabilities.

- **Secure access** features restrict who can use your devices and what they can do.
- **Network security** features protect devices from unauthorised access over network interfaces.
- **Document security** features keep your documents—whether physical or virtual—out of the wrong hands or views.
- **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 and your environment by meeting specific objectives like print release[1], automatic security certificate and Secure Content Monitor.
- **Hard disk security** protects Lexmark printers and multifunction products that contain internal hard disks with a virtual shield to keep your organisation's secrets.
- **Encrypted and signed firmware** ensures that only firmware created by Lexmark's systems can be installed on our devices.
- **Secure boot technology** validates that the firmware installed on the printer is genuine Lexmark firmware. Should non-genuine firmware be detected, users receive notification.
- **Continuous verification** ensures the firmware has not been tampered with during operation.

And we've proven our security expertise by meeting stringent government and industry standards and certifications, including Common Criteria and FIPS.

The security ecosystem: Security and Managed Print Services (MPS)

While our embedded security features and product architecture help Lexmark smart MFPs lead the industry in defending your organisation, consider the advantages of Lexmark Managed Print Services (MPS) as both a strategic information platform emphasising security at every level:

Holistic approach—In the assessment, design and delivery of MPS, we utilise a proven methodology that focuses on security as a critical component of infrastructure optimisation, proactive services and business optimisation.

Expertise—Our security consultants and specialists work to develop policies and practices focused on output security in your unique environment, helping you to not just meet your specific goals, but get through the often-challenging change management curve.

Continuous monitoring—Our MPS tools and systems continuously monitor a deployed fleet, giving you not just security policy control, but enhanced visibility and alerts to events affecting the fleet.

Technology ownership—Lexmark owns all our core technology across services, solutions, software, hardware and firmware—the only MPS provider that does. Therefore, we can help ensure high security levels across all deployed solutions. That technology seamlessness reduces the risk of security holes between different platforms and technologies.

So Lexmark Managed Print Services are more than built around a smart MFP ecosystem. They actually form a security ecosystem.

Learn more at http://www.lexmark.com/en_gb/solutions/security. html

[1] optional

18KD08617