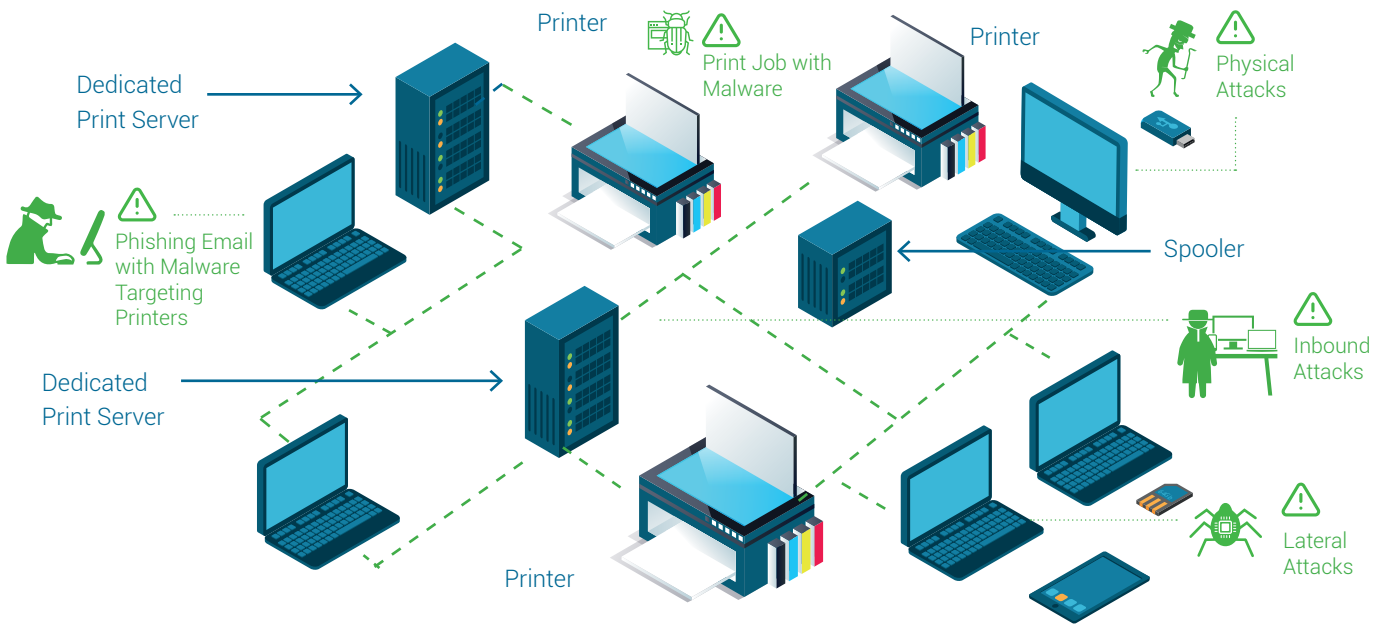
# Industry Brief: Digital Printing

MOCANA




**Digital Printing Systems Present Many Surfaces for Attack**

## Ensuring Safety, Reliability and Compliance

Perimeter-based defenses and threat detection technologies are not enough to defend against modern cyber attacks. Many business printers, multi-function printers, digital presses, scanners, copiers, 3D printers, gateways, and Internet of Things (IoT) edge devices are vulnerable due to a lack of strong cryptographic controls, including: multi-factor authentication, secure boot, secure update, and secure, encrypted communications.

Digital printer manufacturers, managed print services operators and enterprises must comply with cybersecurity standards such as NIST 800-53, Revision 4, IEC 62443-3-3, and FIPS 140-2. Keeping up with these standards as well as emerging standards from the Industrial Internet Consortium (IIC) and Industrie 4.0 is challenging. New regulations such as GDPR in Europe raise the stakes for non-compliance and privacy breaches to more than €20 million per incident. Older protocols such as Printer Job Language (PJL) can be difficult to secure.

Ensuring data privacy in printing and business systems that are vulnerable to physical compromise is critical. For printers deployed in industrial environments, compromised printers could be used to launch lateral attacks onto SCADA and industrial control system (ICS) devices. In operating technology (OT) environments, oftentimes physical human safety and uptime drive the security needs of plants and large SCADA systems.

## Mocana's Proven Cybersecurity Solution

Used by more than 200 OEMs to protect more than 100 million devices, Mocana's IoT Security Platform is a FIPS 140-2 validated embedded cybersecurity software solution that ensures device trustworthiness and secure communications by giving printer manufacturers an easy way to:

- Harden printers, scanners and digital presses with multi-factor authentication using X.509 certificates and trust chaining
- Secure the boot process to validate the firmware, OS and applications
- Enable secure, cryptographically-signed over-the-air (OTA) and over-the-web (OTW) firmware updates
- Integrate hardware or software-based roots of trust such as TPM, SGX, TrustZone, HSMs, SIMs, and MIMs
- Replace open source crypto software such as OpenSSL.

For more information on Mocana's comprehensive IoT Security Platform and how it can help you secure your critical infrastructure, visit our website at mocana.com or send us an email via sales@mocana.com.

**A:** 111 West Evelyn Avenue, Suite 210, Sunnyvale, CA 94086 **W:** www.mocana.com **T:** 415-617-0055