+ImageNet Consulting

Reduce Network Vulnerability and Data Theft With Secure Printing

Legacy printing devices give hackers who want to penetrate enterprise networks and sensitive data an open door. They are often overlooked as security concerns, but designed much like PCs — with hardware and software that can be breached. And because they're connected, any printer fleet breach can quickly spread to enterprise networks. Like any other device, printers need cybersecurity to mitigate the rising tide of threats that include:

- Exploitation of older, less secure printer firmware
- Unsecured network printer ports
- Passive network printer management with unlocked settings

Cybercrime isn't the only problem. Information access is also a challenge when corporate employees with different levels of corporate data access share office space and print devices. As information is printed, it's vulnerable to being seen or intercepted by corporate employees who aren't authorized to view it.

Due Diligence — and Compliance Challenges

As cyberthreats increase, it's critical for organizations to safeguard printers. Only 16% of companies think printers are a high security risk,[1] yet 61% of companies surveyed report at least one print-related breach in the past year.[2] Even more surprising, only 41% use access security (or security of any kind) on their printers.[1]

Maintaining current firmware on printers is a challenge and in many cases leaves organizations vulnerable to attack if best patching practices aren't applied. In fact, 57% of organizations that had at least one data breach attributed the incident to a vulnerability that could have been patched.[3] The same report stated 33% of breached organizations knew the unapplied patch left their organization at risk.[3]

Managed Print Security

Device, BIOS, and user-level security

Ongoing printer fleet management and security

Secure supply chain for printer configuration and deployment

Printer network and data protection

Secure Printing

Safeguarding corporate documents takes a three-pronged approach:

- **Upgrading legacy printers:** Printers must be upgraded to include security features that prevent unauthorized printing, viewing, and access to confidential information.
- **Safeguarding printer BIOS:** Print data must be encrypted and secured as it moves and is stored within the print queue.
- **Optimizing printer fleets:** Managed services are needed to assess, deploy, and manage secure printer fleets, including disposal of printers no longer in use.

Print With Confidence

ImageNet Consulting protects sensitive corporate documents with HP Print Security Solutions. HP offers the strongest, most secure printing in the industry.[4] These printers are designed for today's highly collaborative, cloud-based environments with built-in security features that protect printers at the device, BIOS, network, and user levels. They're designed with encryption and access control that can stop attacks the moment they start. HP Print Security Solutions have the capacity to secure your printing devices with:

- Runtime intrusion and detection to detect and stop attacks on printer memory
- HP SureStart to detect and prevent malicious code from infecting BIOS
- HP JetAdvantage Security Manager to prevent users from changing security settings

ImageNet Consulting can also help automate the best practice process of monitoring and managing printer firmware to mitigate vulnerability loopholes. We can also customize experiences for individual users (e.g., requiring badges to authenticate print jobs), which improves security and also personalizes each experience and improves usability.

HP is ranked as a leader in IDC MarketScape for print and document security solutions and services worldwide.[5]

Trust ImageNet

ImageNet Consulting provides IT solutions to improve our clients' bottom lines. Our consultants optimize and enhance the management of business processes and secure all endpoints. Our partnership with HP and our solution-led approach allows us to offer best-in-class technologies to meet our customers' needs. We strive to make it easy to do business with us. Our service is second to none, our asset management has never been easier, and our security and automation features will make you wonder how you ever managed any other way.

Contact us at www.ImageNet.com to learn more.

ImageNet Consulting | 3223 Commander Dr. | Carrollton, TX 75006 | 214-217-1410 | www.ImageNet.com

[1] Spiceworks Whitepaper, "Unlocked Doors, Research Shows Printers are Being Left Vulnerable to Cyber Attacks," accessed Feb 26, 2018.
[2] CSO, "Cozying Up to the Lonely Network Printer," Sep 29, 2017.
[3] Ponemon Institute Report: "Today's State of Vulnerability Response: Patch Work Demands Attention," Jun 2018.
[4] "HP Security claims for business printing, scanning and HP Elite PCs," HP.com, accessed Sep 30, 2019.
[5] IDC MarketScape, Worldwide Security Solutions and Services 2017 Vendor Assessment, Oct 2017.

Partner First Platinum