WHITE PAPER

UNLOCKED DOORS

RESEARCH SHOWS PRINTERS ARE BEING LEFT VULNERABLE TO CYBER ATTACKS

While IT teams focus on other endpoints, security for corporate printers lags behind

Printers make easy targets: Too many network-connected printers have no restrictions and aren't securely locked down.

But the threat is real, and shouldn't be ignored. Enterprise-class printers have evolved into powerful, networked devices with the same vulnerabilities as any other endpoint on your network. These typically unsecured entry points offer the very real possibility of cyber attacks; they can also offer access to your company's financial and private data, leading to very real business consequences.

Even so, a recent Spiceworks survey of more than 300 enterprise IT decision-makers shows just 16% of respondents think printers are at high risk for a security threat/breach, significantly less than desktops/laptops and mobile devices.[1] This perception has tainted how IT staffs are approaching network security. While nearly three in five organizations have security practices in place for printers, this percentage is well below that for other endpoints—and leaves printers vulnerable, when there are easy solutions to safeguard this particular entry point.

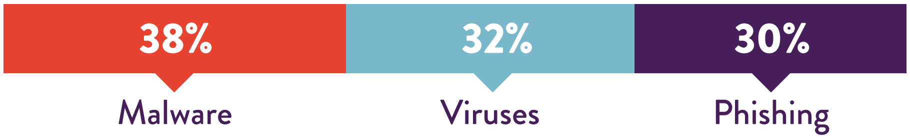
This white paper presents data on printer security based on the Spiceworks survey, the impact of security breaches, and some of the modern built-in printer security features designed to protect against cyber attacks.

JUST 16% OF RESPONDENTS THINK PRINTERS ARE AT HIGH RISK FOR A SECURITY THREAT/BREACH.[1]

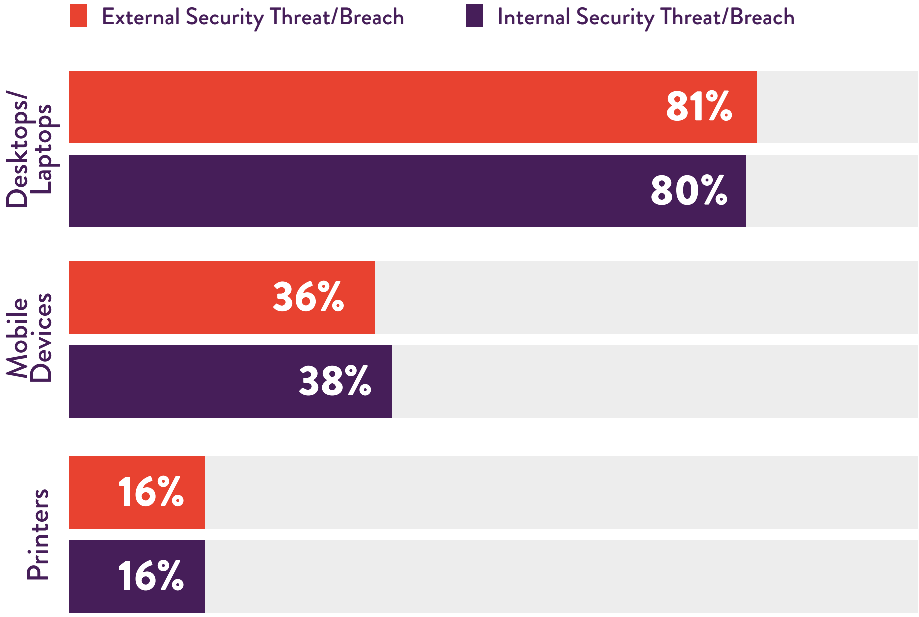
DOORWAYS FOR ATTACKS

In the Spiceworks survey, 74% of respondents (net) said their organization has experienced at least some type of external IT security threat or breach in the past year. And 70% (net) experienced an internal IT security threat or breach, most commonly from user error, the use of personal devices for work purposes, or employees using a home or public network for work purposes.[1]

TOP EXTERNAL IT SECURITY THREATS/BREACHES EXPERIENCED



The top threats snuck in primarily through desktops and laptops, with others coming through mobile devices and printers.[1] (The 16% coming in via printers is notably higher than the 4% found in a similar 2014 Spiceworks study.) It's also possible the number of attacks striking through printers is underestimated, since printers are not as closely monitored as PCs and mobile devices.



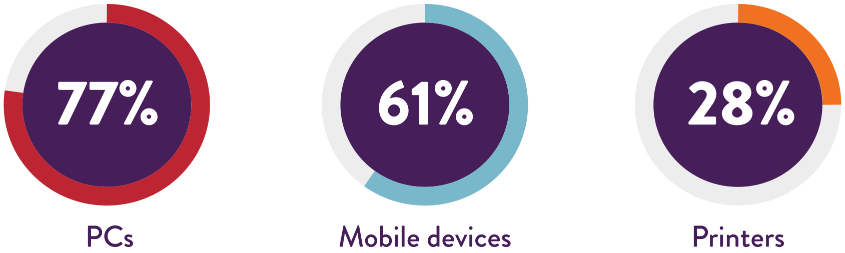
WE’RE IGNORING OUR PRINTERS

Whatever the case, the Spiceworks survey makes clear printer security is often an afterthought.

Organizations are acutely aware of the importance of network, endpoint, and data security. In fact, more than three-fourths of respondents use either network security, access control/management, data protection, or endpoint security—or a combination of these.[1]

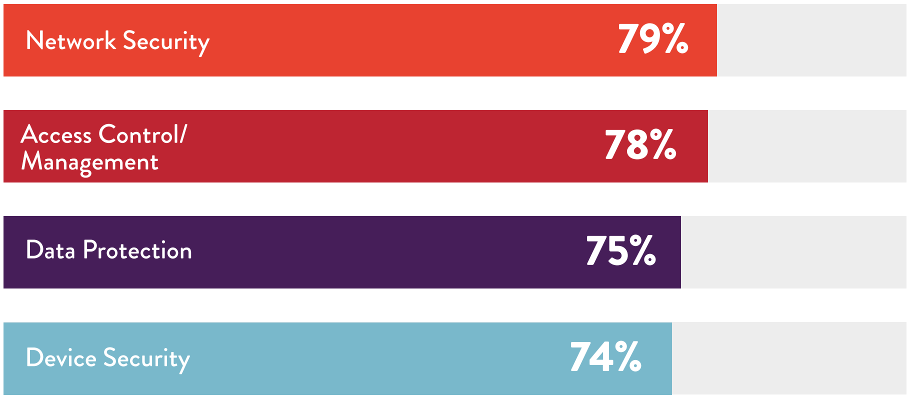
But these solutions are deployed far less often on printers. While 83% of respondents use network security on desktops/laptops and 55% on mobile devices, just 41% use it on printers.[1]

The disparity is even wider for endpoint security:



Plus, not even a third (28%) of respondents deploy security certificates for printers, as opposed to 79% for PCs and 54% for mobile devices.[1]

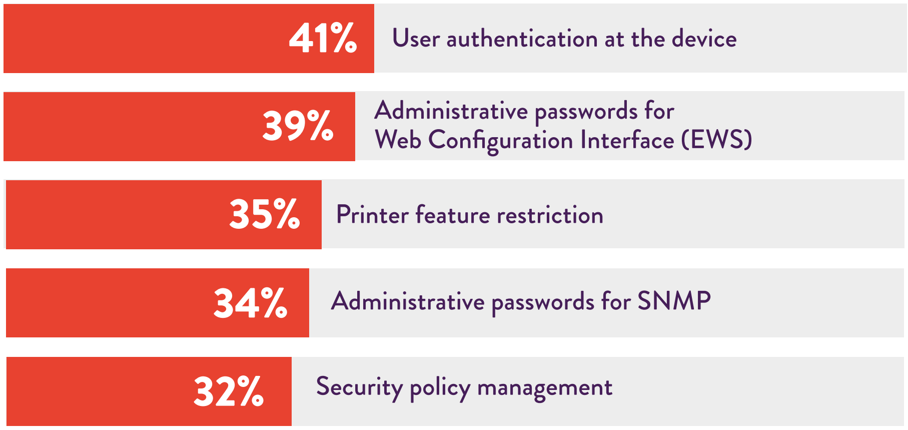
TOP ENDPOINT SECURITY PRACTICES



Among protections used on general endpoint devices, the most-used security measures for printers were document security, network security, and access control, but less than half of respondents said their organizations use any of those on their printers.[1]

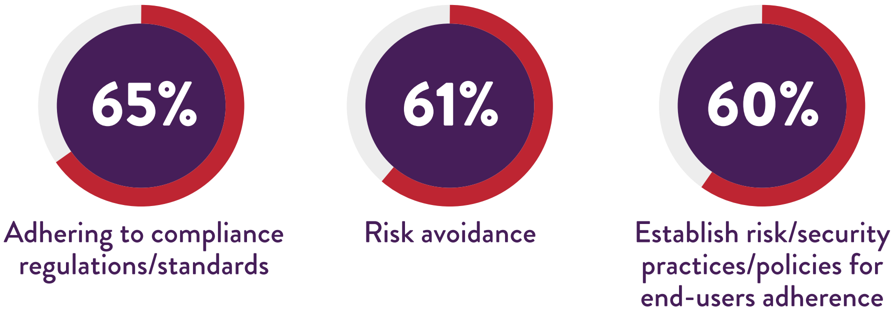
Some companies do have printer-specific security practices, but even there, the practices are widely disparate. Just over 40% of organizations deployed user authentication, and less than 40% used administrator passwords for web configuration interface.[1] For a strong defense, each organization should be using a mix of all of these approaches—and more.

TOP PRINTER-SPECIFIC SECURITY PRACTICES



When it comes to endpoint compliance and audit practices, printer security controls lag behind nearly all other endpoints. Nearly 90% of organizations have an information security policy deployed, but those policies don't typically extend to printers. For example, while 57% of respondents said they have malware defenses deployed on their PCs, only 17% had them deployed on printers.[1]

NEARLY 9 IN 10 IT PROS CITE THEIR ORGANIZATION HAS AN INFORMATION SECURITY POLICY IN PLACE, FOR THE FOLLOWING REASONS:



Clearly, organizations aren't taking printer security serious enough—but they certainly should.

"Many printers still have default passwords, or no passwords at all, or ten are using the same password," Michael Howard, chief security advisor for HP, told Computerworld in June. "A printer without password protection is a goldmine for a hacker. One of the breaches we often see is a man-in-the-middle attack, where they take over a printer and divert [incoming documents] to a laptop before they are printed. They can see everything the CEO is printing."[2]

THE POTENTIAL IMPACT OF PRINTER INTRUSIONS

According to a senior e-threat analyst at Bitdefender, Bogdan Botezatu, printers present a sizable potential security hole. "We get a lot of telemetry in our vulnerability assessment labs. The router is no longer the worst device on the internet. It's now the printer."[3]

This vulnerability can have profound effects on a business. With a single unsecured printer, you could be leaving your entire network of connected devices vulnerable to attack, giving hackers the ability to spy on your networked devices—and compromising the security of the whole network.

1. Increased help desk calls and support time
2. Reduced productivity/efficiency
3. Increased system downtime
4. Increased time on support calls
5. Increased enforcement of end-user policies

We've all seen the effects of security breaches. In the Spiceworks survey, respondents said the top five impacts of a breach are:[1]

But a printer breach can be even more severe than that, particularly if you use a multifunction printer capable of storing printed data electronically. Print jobs stored to the printer's cache make it possible for hackers to gain access to sensitive personal or business information.

Even more concerning, hackers can access the broader company network through an unsecured printer, stealing things like Social Security numbers, financial information, or internal memos and documents. This stolen information can not only affect individual employees, but be used by the competition or cause serious harm to a company's reputation.

THE EASY SOLUTION: BUILT-IN SECURITY FEATURES

Clearly, companies need to address security even with their printers. Some of today's modern enterprise-level printers feature easy-to-use, built-in security that combats printer threats. These include:

- Automatic attack detection, protection, and healing
- Tracking use to prevent unauthorized use
- Simple sign-in options such as PIN or smartcards
- A proximity card reader that lets users quickly authenticate and print securely at a printer using their identification badge
- Secure encrypted printing for sensitive documents

When considering your next printer, whether desktop or multi-function, investigate integrated security safeguards—and be sure to activate them. With simple, printer-specific features like those, there's no reason to remain vulnerable through your printers; after all, with the Internet of Things, there are plenty of other access points to worry about—**your printers don't need to be one of them.**

LOOKING FOR MORE SECURE PRINTERS?

LEARN MORE ›

Sources:

[1] Spiceworks survey of 309 IT decision-makers in North America, EMEA, and APAC, on behalf of HP, November 2016.

[2] "Printer Security: Is your company's data really safe?" *Computerworld,* June 1, 2016.
http://www.computerworld.com/article/3074902/security/printer-security-is-your-companys-data-really-safe.html

[3] "Printers Now the Least-secure Things on the Internet," *The Register*, September 8, 2016.
http://www.theregister.co.uk/2016/09/08/the_least_secure_things_on_the_internet/