

CLOSE THE GAP IN DEVICE SECURITY



CONTENTS

- Endpoints are a key target
- The talent shortage isn't helping
- Innovation is necessary
- Where can you start?
- Today's RFP requirements
- Secure your process and protect your organization



YOUR COMPANY'S ENDPOINTS ARE SURROUNDED BY CYBER THREATS—

this is the new reality you live in. You're constantly fighting off cybercriminals who are always looking for the easiest way to gain control of your company's sensitive data, and unprotected endpoints have become one of their favorite attack vectors.

Are you maintaining a set of security policies to protect all your endpoints from attack? Is your organization keeping up-to-date with applying these policies to all intelligent, connected devices across the network?

If you're kept up at night thinking about the breadth of security challenges, from users to infrastructure, you're not alone. You can't control how people act, but you can control the risk posture of your organization and the follow-through of your security policies.

ENDPOINTS ARE A KEY TARGET

In 2018, there was a 17 percent increase in the number of companies compromised by attacks originating from an endpoint, according to a study by the [Ponemon Institute](#) and Barkly. This fact shouldn't come as a surprise—endpoint devices often go under-secured, because many organizations assume their networked devices are protected by a firewall.

Printers are more vulnerable than the average endpoint, because they are attached to the corporate network and accessed by many users.





ONE-THIRD

of IT professionals freely admit they don't know how many endpoints are on their network

One-third of IT professionals freely admit they don't know how many endpoints are on their network, according to a recent study by [LogMeIn](#). When surveyed further on risk, the same group of IT professionals admit their endpoint security strategy has significant room for improvement. Only approximately one in four IT security pros are using Security Information and Event Management (SIEM) software or other basic protection to understand the real-time health of their endpoint devices:

26%

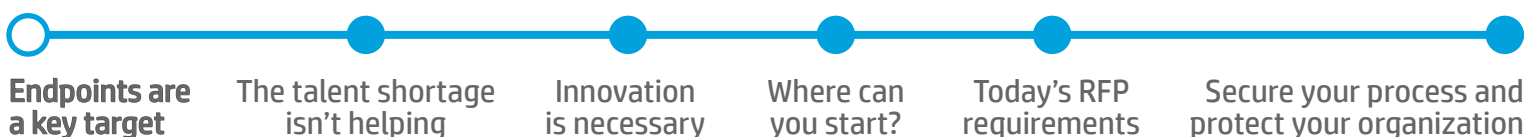
have invested in automated security event monitoring

17%

use anti-malware capabilities on endpoints

14%

use a third party for patch management

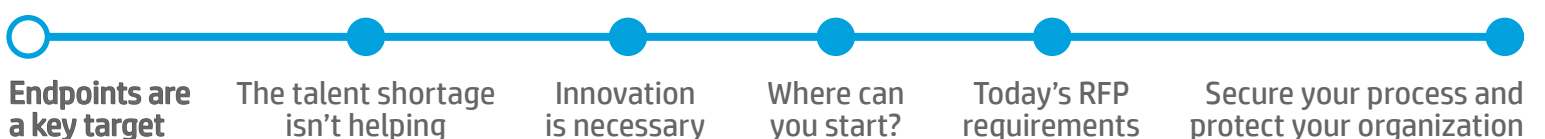


TAKE PRINTERS, FOR EXAMPLE. THE TRUTH IS YOUR PRINTERS PROBABLY AREN'T JUST UNDER-SECURED—THEY ARE LIKELY SIGNIFICANTLY UNDER-SECURED.

It's vital these intelligent, networked devices are covered by your security policies and their configuration is maintained to meet the basic principles of cyber hygiene.

To make matters worse, printers are more vulnerable than the average endpoint, because they are attached to the corporate network and accessed by many users. If an unwitting user prints a document with malicious code, a hacker can gain the ability to infect your printer with malware. And since printer alert logs are rarely integrated with SIEM software, attackers can evade detection for a long period of time. Once they're inside a printer, they can potentially move throughout your network and siphon off sensitive data without detection.

In 2018, there was a
17% INCREASE
in the number of companies
compromised by attacks
originating from an endpoint





THE TALENT SHORTAGE ISN'T HELPING

Businesses are suffering from a talent gap with respect to IT and information security professionals. [SecureWorldExpo](#) reports that there are currently 2.93 million unfilled cybersecurity jobs worldwide, including 500,000 in North America alone. And the problem will continue to get worse over time. According to a [Korn Ferry](#) study, by 2030, the global talent shortage will be

By 2030, the global talent shortage will be **85 million** workers, a figure equal to the population of Germany

85 million workers, a figure equal to the population of Germany. This will amount to a drought of internal technical expertise within many businesses.

It is more critical than ever to ensure every device on your network has strong embedded security and your organization becomes better versed in applying your security policies.

Endpoints are a key target

The talent shortage isn't helping

Innovation is necessary

Where can you start?

Today's RFP requirements

Secure your process and protect your organization

INNOVATION IS NECESSARY

Cybersecurity is no longer as simple as setting up perimeter defenses, like firewalls. Due to growing risks, you need to bring smart devices into the purview of your threat monitoring systems and vulnerability assessment tools. Historically, printers and copiers have been left out of these.

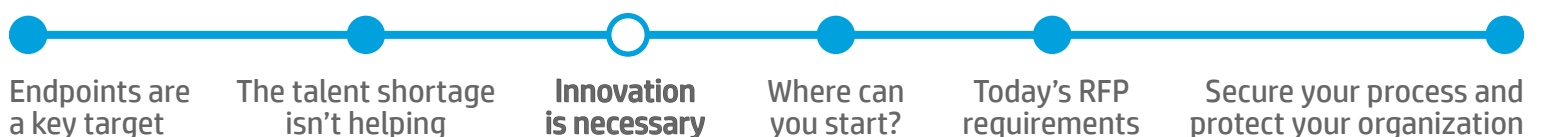
Today, security teams are constantly grappling with an extreme amount of alerts generated by endpoints and don't have the resources to separate meaningful threats from noise.

Clearly, innovation is needed, and some device manufacturers are stepping up with embedded security features and providing logs in standard formats.

IDC guidelines now recommend that all endpoint products be designed to protect both the device and the data it houses from attacks, regardless of OS type.¹ You can now request these features when purchasing devices and integrate these devices into your assessment and SIEM tools.



1. IDC Government Procurement Device Security Index 2018: Public Sector PC & Printer RFPs Lack Basic Security Consideration, sponsored by HP, May 2018



WHERE CAN YOU START?

Your first step should be to assess—or reassess—your environment for vulnerabilities. Doing so will allow you to understand the risk landscape, whether your devices are up to snuff, and if policies are being enforced.



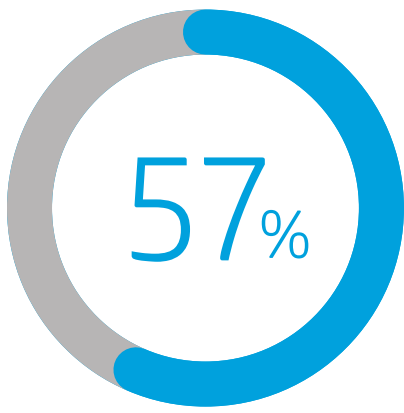
Conduct a pulse check

1. Do you have a complete inventory of endpoint devices?

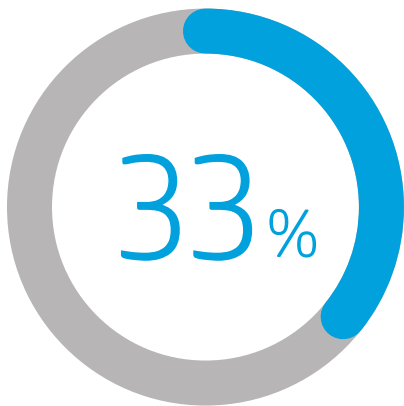
Organizations are experiencing epidemic levels of shadow IT, which can create conditions where much of the hardware and software operating on the network are acquired and maintained without the knowledge of the IT department.

Often, technology purchases are managed, defined, and controlled by other business leaders in the organization. IT needs to go out of its way to build connections with these business leaders, so they can outline the risk inherent in endpoint device procurement and communicate the importance of following security policy.





of breached firms attributed the incident to a vulnerability that could have been patched—but the patch was never applied.



of breached organizations knew the unapplied patch left their organization vulnerable.

2. Check your security policies

Evaluate your security policies to ensure your printers are being managed in the same way as any other intelligent, networked device. Specific areas to evaluate include device requirements for purchase, access control, configuration, and device disposal.

3. Check if your printer firmware is up to date

There's an industry-wide patching problem. A **Ponemon Institute** study, sponsored by ServiceNow, found the majority of organizations who suffered at least one data breach in the past two years could have prevented the incident with stronger cyber hygiene practices. Fifty-seven percent of breached firms attributed the incident to a vulnerability that could have been patched—but the patch was never applied. One-third of breached organizations knew the unapplied patch left their organization vulnerable.

When was the last time your organization checked for firmware updates and patches for your print fleet? Are patches being delayed due to a lack of resources to evaluate interoperability with your surrounding systems and software?

Firmware updates aren't always easy, but the solution lies in bringing printers and copiers in line with existing patching practices for PCs, servers, and applications.

LIKE MANY ORGANIZATIONS TODAY, YOU MAY FIND YOUR PRINT FLEET IS UNDER-SECURED



4. Are your print devices configured to your security policies?

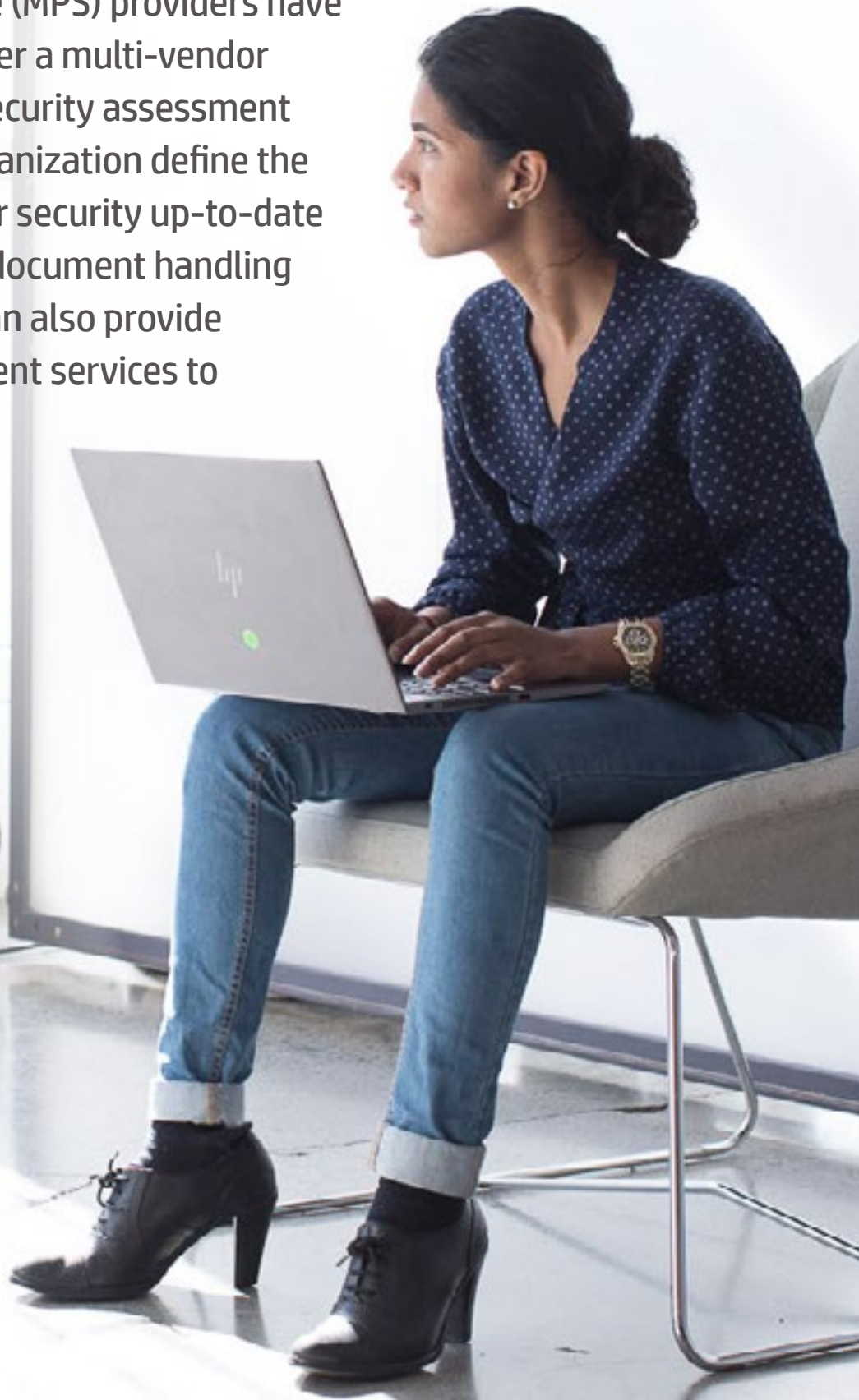
Check to see if printers have been configured with unique admin passwords and that services and protocols are closed if not needed by the organization's applications (e.g., Telnet and FTP).

After your quick pulse check, you may find your print fleet is under-secured—just like many organizations today. If so, you need to commit to fully assessing the situation and taking steps to close the gap.



Should I conduct a full security assessment?

The thought of producing a multi-vendor print security assessment can seem daunting, especially when you may be dealing with an overworked IT security staff. Fortunately, you can get help. Many managed print service (MPS) providers have security experts and can offer a multi-vendor assessment service. Print security assessment services could help your organization define the actions needed to bring your security up-to-date for print devices, data, and document handling processes. MPS providers can also provide ongoing security management services to address execution gaps.



TODAY'S RFP REQUIREMENTS

While you work on a full assessment, you can start to take action by ensuring your procurement department is sufficiently specifying security requirements in its MPS and hardware request for proposals (RFPs).

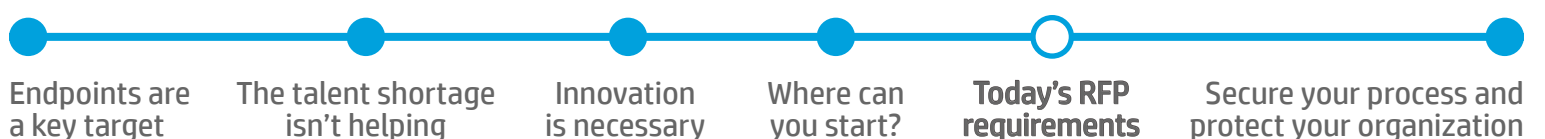
According to [IDC's Government Procurement Device Security Index](#), public sector procurement was weak in security requirements for both PCs and printers.¹ "Procurement processes within the public sector do not reflect current, modern security capabilities, nor do they account for the emerging types of threats that undermine traditional security approaches (such as malware functioning below the operating system). Almost one-third (29%) of the examined RFPs have no consideration of security at all."

Convert your security policies into clear and easy to understand RFP requirements for managed print service contracts and hardware purchases, then develop a comprehensive checklist of requirements and share it with procurement staff. Below are some examples of key requirements likely missing in RFPs today that you should consider adding to your list:

29%
of the examined
RFPs have no
consideration of
security at all.



1. IDC Government Procurement Device Security Index 2018: Public Sector PC & Printer RfPs Lack Basic Security Consideration, sponsored by HP, May 2018





Malware protection

Printer manufacturers today can provide anti-malware technologies as an embedded feature or specialized add-on software, designed for the manufacturer's devices. Some anti-malware technologies can provide recovery functions, so the IT security team doesn't need to intervene. Look for the following:

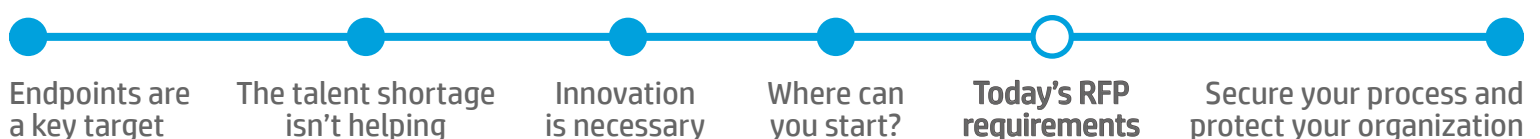
Logging

Printers should offer two types of logging: on-device logging for troubleshooting and SIEM data for the SOC. Make sure you and your department leaders ask for the following when choosing the right printers for your organization:

- Devices must log security and auditing events
- Device must be configurable to send syslogs of a user set priority level to a log server or SIEM tool
- Device must send messages in standard syslog format that can be ingested by industry (or your organization's chosen) SIEM tools

- Device must provide continuous monitoring for in-memory malware injection attacks during runtime
- Device must send a syslog message in case of memory injection anomaly being detected for threat monitoring purposes
- Device must shut down when a memory injection anomaly is detected to stop malware

ADVANCED: Device must automatically initiate a reboot to a known good condition after an anomaly is detected



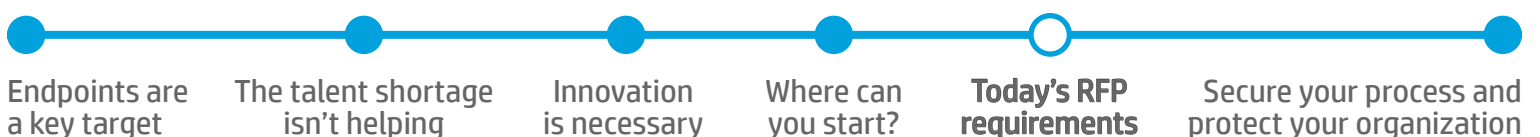
BIOS integrity

When a printer's BIOS is compromised, hackers can gain complete control over the device and evade detection. A secure boot process and continuous monitoring to protect firmware integrity can self-heal from attacks before compromised firmware spreads malware across your network.

Look for the following when evaluating solutions:

- Device must perform a BIOS validation at startup and the device is shut down if an anomaly is present
- Device must send a syslog in case of a BIOS anomaly being detected for threat monitoring purposes
- Device must align with NIST SP 800-193 Platform Firmware Resiliency Guidelines

ADVANCED: Device must self-heal from an infected BIOS by replacing it automatically with a hardware protected golden copy and boot in a known good state without IT intervention



Firmware updates

Consider covering both manufacturer practices for testing and closing vulnerabilities, as well as getting support to update your devices.

Is the hardware manufacturer sufficiently addressing their responsibility to continually evaluate their software for vulnerabilities and releasing patches in a timely manner?

Request that the manufacturer:

- Provides documentation on adherence to secure development lifecycle processes for their firmware
- Follows OWASP secure coding practices to identify vulnerabilities
- Engages third-party researches to actively test product code for vulnerabilities
- Provides an automated way for security bulletins to be sent to opt-in users (security bulletins should describe the vulnerability, provide information on how to fix or mitigate the risk, and contain the CVE identifier, as well CVSS).



If you're looking to work with an MPS vendor who can provide firmware patching services to keep your multi-vendor fleet up to date, then you will want to ensure they will:

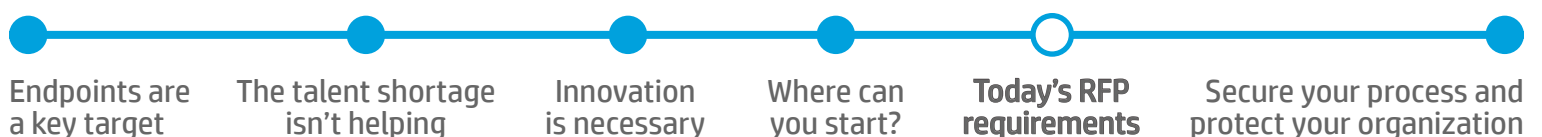
- Assess print fleet to identify any existing firmware behind in security patches
- Test firmware in a test environment to determine compatibility with company software and systems prior to pushing to the fleet
- Push firmware updates to devices to keep fleet up to date

Managed print services


If your organization is struggling to assess your printers or create an effective policy and apply it to a multi-vendor print fleet, the solution may be to engage with third-party experts. An **MPS partner** can help your organization enforce security policies.

Ensure that you ask the following questions as you prepare your MPS RFP checklist:

- What framework does the MPS vendor use to define, implement, and manage information security policies?
- Does the MPS vendor offer print fleet security assessment and remediation services?
- Does the MPS vendor offer a device security management service to maintain devices to a security policy?
- Does the MPS vendor have the experience to address regulatory compliance requirements, such as HIPAA, GDPR, and other applicable laws and regulations?



SECURE YOUR PROCESS AND PROTECT YOUR ORGANIZATION



Ultimately, the responsibility lies in the hands of the IT security organization to own and drive security policy, and make sure policy is applied across the organization. If you discover shortcomings, you can look to a partner to help you with knowledge and talent resources.

By building security into your vendor partnerships and procurement processes, you can simplify the work of the IT team and create secure partnerships that address the evolving role of cybersecurity risk in business.

ARE YOU READY TO ADDRESS THE SECURITY RISKS IN YOUR PRINT ENVIRONMENT?

Talk with HP about their **Print Security Services** to initiate a comprehensive, multi-vendor security assessment process and access expert recommendations on how your organization can improve the security of your devices, data, and documents.

Endpoints are a key target

The talent shortage isn't helping

Innovation is necessary

Where can you start?

Today's RFP requirements

Secure your process and protect your organization

WHAT YOU CAN DO RIGHT NOW TO CLOSE THE GAP IN DEVICE SECURITY

- Evaluate your organization's current RFP requirements for printer hardware and contractual print services
- Check your security policies to ensure explicit mention of printer devices
- Update security policy procedures with your printer IT administrator
- Partner with an MPS provider to fully **assess your environment** and develop a plan to close any gaps in your print security practices

Endpoints are a key target

The talent shortage isn't helping

Innovation is necessary

Where can you start?

Today's RFP requirements

Secure your process and protect your organization

Learn more about how HP can
help protect your company.

VISIT [HP.COM/GO/REINVENTSECURITY](https://www.hp.com/go/reinventsecurity)