Article

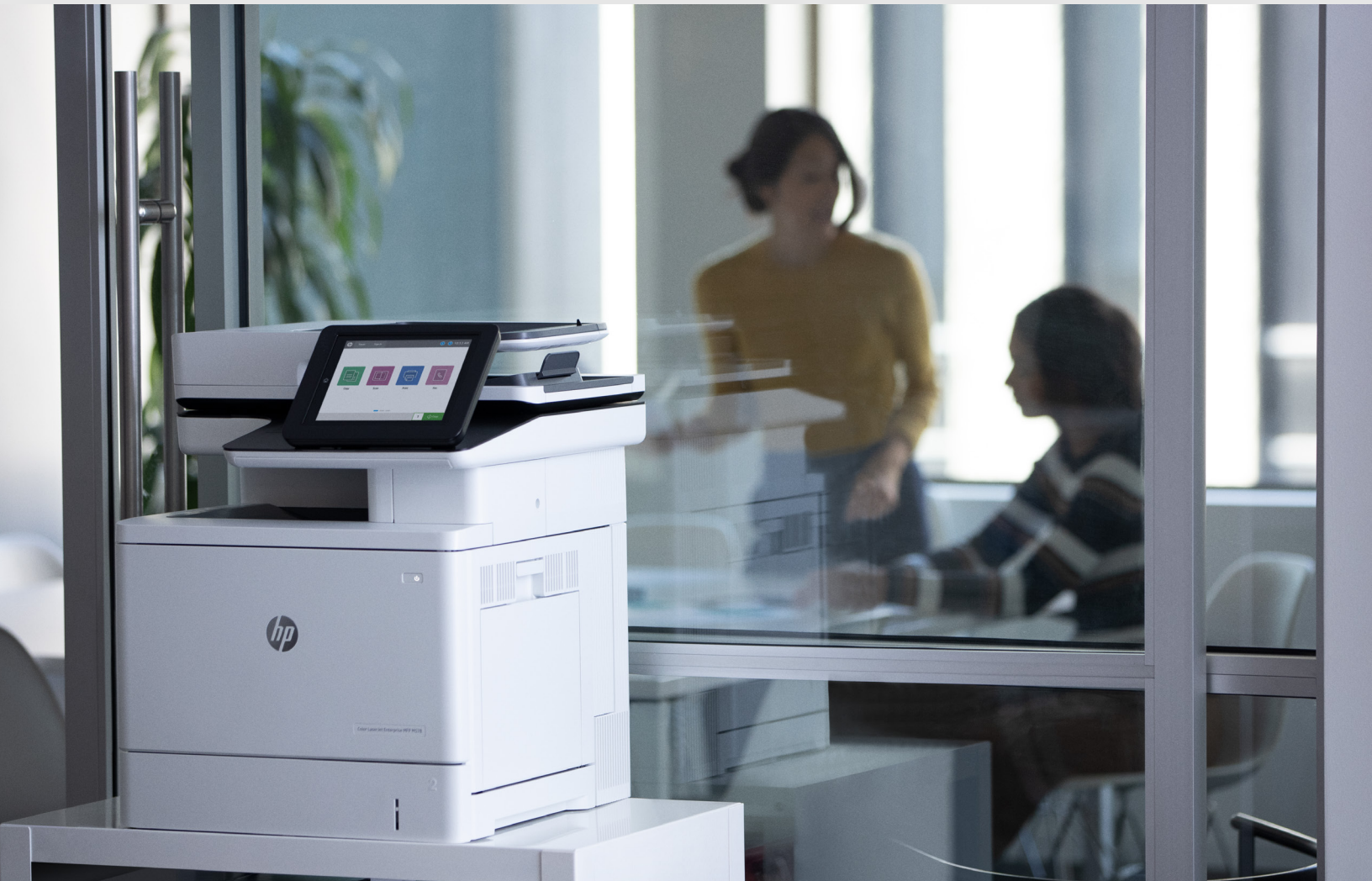
Secure your transition to the hybrid workplace

How organizations are keeping up with changes in the workplace

Organizations are quickly recalibrating their approach to virtual workplaces. This is a key driver in the adoption of new platforms and processes, which enable remote and on-site employees to collaborate more effectively and work more efficiently.

Still, many employees continue to work in the office, and providing these staff with a simple and efficient way of collaborating on paper-based workflows remains essential. This is especially true in process dependent departments, such as HR and finance, where high-volume, paper-based business processes continue to be the norm.

Much of this hinges on the capability of organizations' hardware. Endpoint devices, such as printers, can help expedite digital transformation efforts by enabling employees to stay connected and collaborating through cloud printing. Doing so ensures daily operations run smoothly and improves workplace productivity.



New priorities for a new normal

But before implementing such plans, organizations must first turn their attention to security – the single most critical and urgent priority in today's landscape. Having a distributed workforce can expose organizations to higher risks. These include employees sharing data on unsecured networks, using personal devices to access company information, or installing third-party software on corporate devices even though it has not been whitelisted by IT.

Organizations face these risks amidst a diminishing capacity to monitor employees' activity and the health of their devices.

For IT, the biggest hurdle lies in ensuring that security policies are being applied equally to all devices across the network. However, one-third of IT professionals have admitted that they do not know how many endpoints are on their network[1].

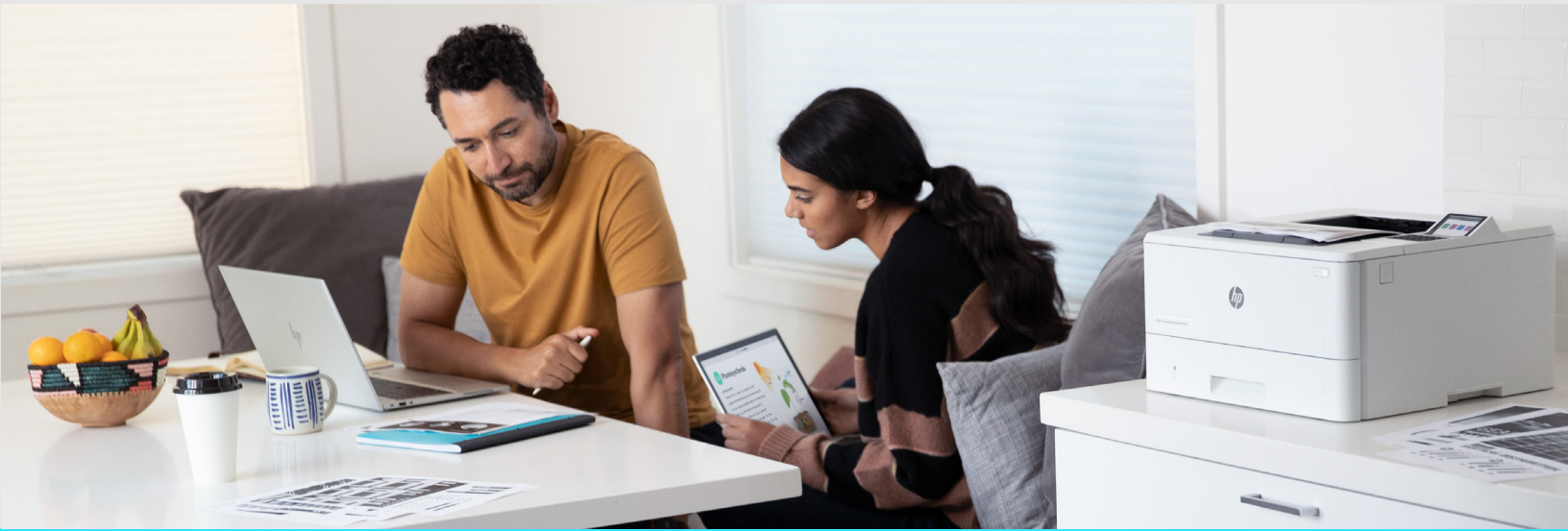
At the same time, cybercriminals are launching increasingly more sophisticated attacks. It gets even more concerning when you consider that unprotected endpoints have become one of their favorite attack vectors, and printers are some the most susceptible targets.

Printers – often overlooked and under-secured

And it is clear why. Printers are more vulnerable than the average endpoint as they are attached to the corporate network and accessed by numerous users. Many organizations also mistakenly assume that their networked devices are protected by a firewall. Furthermore, printers are often not included in threat monitoring systems and are consequently much more under-secured than other endpoints.

Now, cybercriminals can infect an organization's printer with malware when an unwitting user prints a document with malicious code. Successfully breaching one printer means they can potentially move throughout an organization's network and siphon off sensitive data without detection. Because printer alert logs are rarely integrated with Security Information and Event Management (SIEM) software, these attacks can avoid detection for long periods. Seizures are more challenging to guard against because they are continually evolving and becoming harder to detect.

Managing these threats, minimizing workflow disruptions, and ensuring the business remains resilient will be a significant challenge that organizations must overcome. But it is not impossible to do all the above – as long as organizations equip themselves with the right tools and technology.



Upgrade your security with the world's most resilient printers[2]

Don't let unseen forces hinder your organization's future-proofing efforts. Close the gap in device security with HP Enterprise printers. With the industry's strongest security from HP[3], organizations will be better positioned to keep security threats at bay without compromising transformation efforts and daily operations.

1. HP Sure Start is your first layer of security. It enables a secure boot process for your printer by automatically checking the operating code (BIOS) each time it powers on. Upon detecting a compromised version, the printer can repair itself by restarting with a safe, "golden copy" of the BIOS and safeguard you from attack.[4]

2. HP Connection Inspector supports Run-Time Intrusion Detection. It uses a unique HP technology to evaluate your printer's outgoing network connections to determine what is normal, stops suspicious requests to "call home" to malicious servers, and automatically triggers a self-healing reboot. This helps to stop malware from stealing data and compromising your network.

3. Whitelisting automatically checks your printer firmware during startup to determine if it is authentic and digitally signed by HP. This helps to ensure the code that coordinates your printer's functions, controls, and security hasn't been tampered with, as compromised code could expose your whole network to an attack. If anomalies are detected, your printer will reboot to a secure, offline state and notify IT.

4. Reduce the time it takes for upgrades to be expanded across your fleet — with upgradeable firmware from HP FutureSmart. HP FutureSmart eliminates the challenges of managing a distributed fleet by making it easy to deploy the latest security enhancements and features. Old and new devices can be updated on your schedule at the touch of a button, helping to protect your investment for years to come.

5. The Run-Time Intrusion Detection feature detects anomalies in the system memory and protects the printer while it is connected to the network — when it is most vulnerable to attacks. It conducts checks for anomalies during complex firmware and memory operations, automatically stops intrusions, and reboots to initiate self-healing. Worry less about the security of your fleet with technology that conforms to the Common Criteria Information Technology Security Evaluation ISO/IEC 15408 Standard requirements.[5]

6. A comprehensive approach to printer security must go beyond technology. HP Advance secures the confidentiality of data in hard copy document printing and reduces unclaimed prints — by requiring authentication to release print jobs. Jobs can be encrypted both in transit and on the printer's secure hard drive, so only the user who sent the print job can receive it.

Take a safe approach in building your future workplace

Before organizations embark on large-scale, potentially cross-border projects to adapt to the hybrid workplace, it is important to re-examine their operational and security requirements within this new paradigm.

Here, organizations must rethink their approach to paper-based workflows, as it might impede the way employees collaborate in a distributed workforce. Evaluate whether your organization could benefit from the implementation and use of new printing and imaging technologies that may not have been previously considered.[6]

Consequently, printers must feature more prominently in the broader security strategy as well. This is particularly important as modern printers merge digital and paper-workflows, making it a key component of any organization's efforts in pivoting towards a resilient and hybrid workplace.

HP can help organizations to make this pivot more seamlessly – with cloud-powered printers that deliver leading-class security that protects your data. Capable of stopping threats, adapting to new ones, and healing itself from attacks, HP printers can enhance your overall security strategy.

Interested to know how you can make your printers a central part of your digital transformation?

Contact an HP Representative

References:

1. HP, Close the gap in device security, Jun 2019
2. "World's most secure printing" or "most resilient printers" claims include HP's most advanced embedded security features which are available on HP Enterprise and HP Managed devices with HP FutureSmart firmware 4.5 or above. The claim is based on HP review of 2019 published features of competitive in-class printers. Only HP offers a combination of security features to automatically detect, stop, and recover from attacks with a self-healing reboot, in alignment with NIST SP 800-193 guidelines for device cyber resiliency.
3. HP's most advanced embedded security features are available on HP Enterprise and HP Managed devices with HP FutureSmart firmware 4.5 or above. Claim based on HP review of 2019 published features of competitive in-class printers. Only HP offers a combination of security features to automatically detect, stop, and recover from attacks with a self-healing reboot, in alignment with NIST SP 800-193 guidelines for device cyber resiliency. For a list of compatible products, visit: hp.com/go/PrintersThatProtect. For more information, visit: hp.com/go/PrinterSecurityClaims
4. A FutureSmart service pack update may be required to activate security features. Some features will be made available as an HP FutureSmart service pack update on select existing Enterprise printer models. For a list of compatible products, please see our "Embedded security features compatibility matrix" at http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA6-1178ENW
5. Third-party certification based on Common Criteria Information Technology Security Evaluation ISO/IEC 15408 Standard requirements as of May 2019. Certification applicable to HP Enterprise and Managed devices running HP FutureSmart Firmware version 4.5.1 and later. For more information: https://www.commoncriteriaportal.org/files/epfiles/Certification%20Report%20%20HP%20Intrusion%20Detection.pdf
6. IDC, IDC FutureScape: Worldwide Imaging, Printing, and Document Solutions and 3D Printing 2021 Predictions, Oct 2020