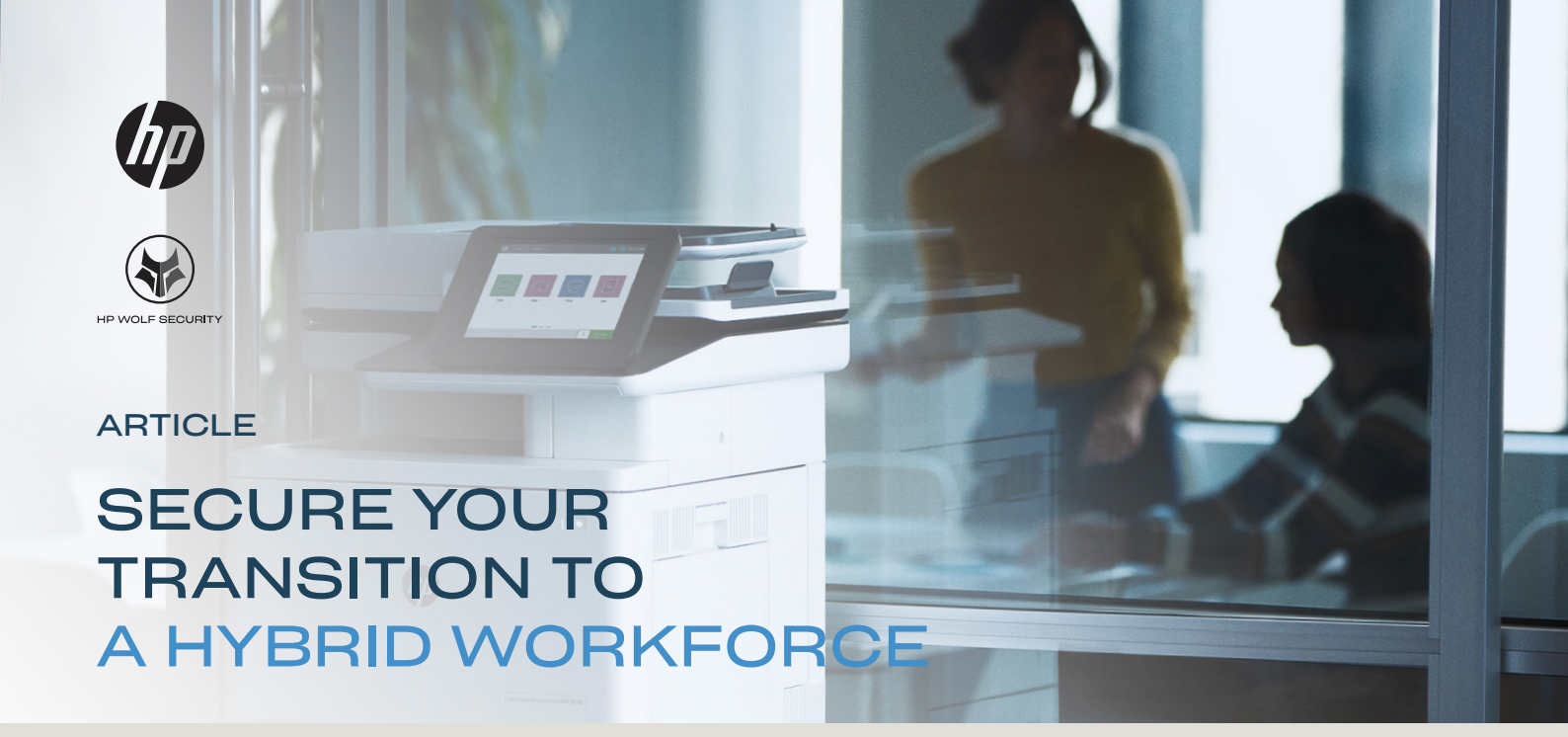


HP WOLF SECURITY

ARTICLE

SECURE YOUR TRANSITION TO A HYBRID WORKFORCE

HOW ORGANIZATIONS ARE KEEPING UP WITH CHANGES IN THE WORKFORCE

Organizations are quickly recalibrating their approach to hybrid work. This is a key driver in the adoption of new platforms and processes, which enable remote and on-site employees to collaborate seamlessly and securely.

Despite the push towards digitization, many paper-based workflows remain essential. This is especially true for employees in 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 employees stay connected and collaborate through cloud printing. Doing so can help daily operations run smoothly and improves workforce performance.

NEW PRIORITIES FOR THE NO NORMAL

But before implementing such plans, organizations must first turn their attention to security – the number one priority in a business landscape defined by constant, unpredictable changes. To thrive, businesses need to ensure that their employees are ready and able to do their best work from anywhere, without compromising on security.

For IT, this means building the capacity to monitor employees' activities and the health of their devices, while ensuring that security policies are enforced on all devices across the network - regardless of location.

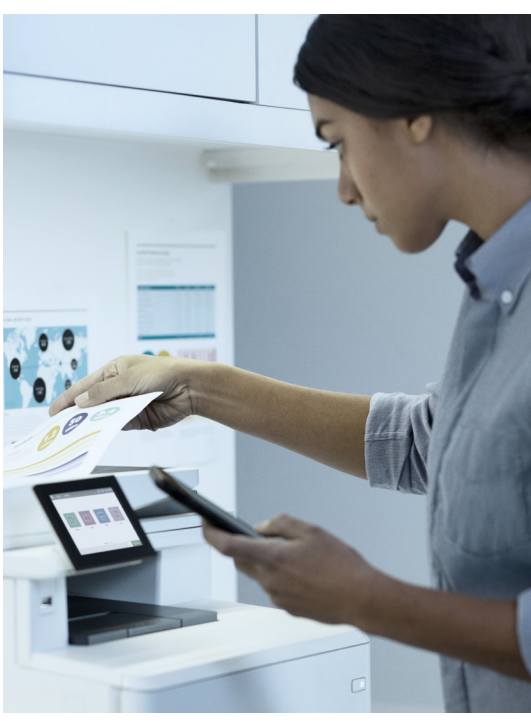
At the same time, IT also needs to defend against increasingly sophisticated attacks. As organizations make the transition to hybrid work, they must ensure that their endpoints - especially printers - remain protected at all times.

PRINT SECURITY SHOULD NOT BE OVERLOOKED

And it is clear why. Printers make for attractive attack vectors as they are attached to the corporate network and accessed by numerous users. Additionally, printers are often not included in threat monitoring systems, and rely exclusively on the manufacturer to build security into the printer's hardware and firmware.

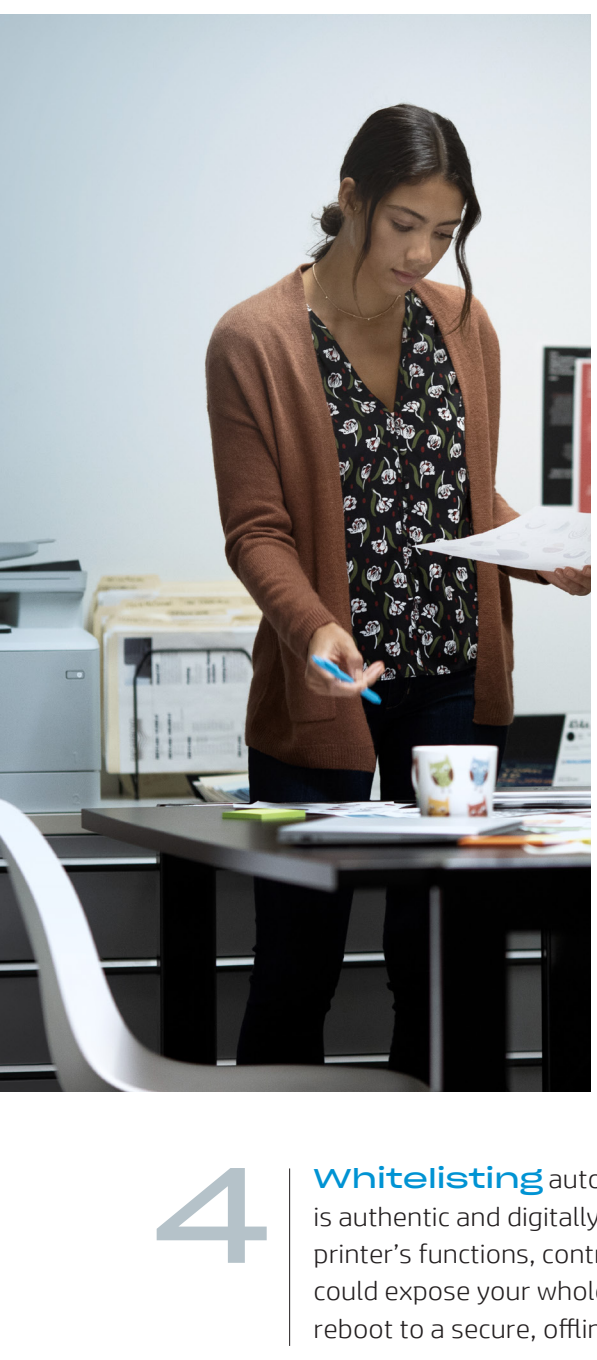
One possible route of attack involves infecting a printer with malware when an unwitting user prints a document with malicious code. Successfully breaching one printer means they can potentially move throughout an organization's network and siphon off sensitive data without detection. Because printer alert logs are rarely integrated with Security Information and Event Management (SIEM) software, these attacks can avoid detection for long periods.

Managing these threats, minimizing workflow disruptions, and ensuring seamless, secure collaboration across their hybrid workforce will be the key priorities for organizations moving forward. It's quite a handful, but it is possible to do all the above – as long as organizations equip themselves with the right tools and technology.



UPGRADE YOUR SECURITY WITH HP WOLF ENTERPRISE SECURITY FOR THE WORLD'S MOST SECURE PRINTERS[1]

Don't let unseen forces hinder your hybrid workforce. Close the gap in device security with HP Enterprise printers. With HP Wolf Security, organizations will be better positioned to keep security threats at bay without compromising their employees' ability to collaborate and excel while working from virtually anywhere.



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.[1]

2 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.[2]

3 **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.

4 **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.

5 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.[3]

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.

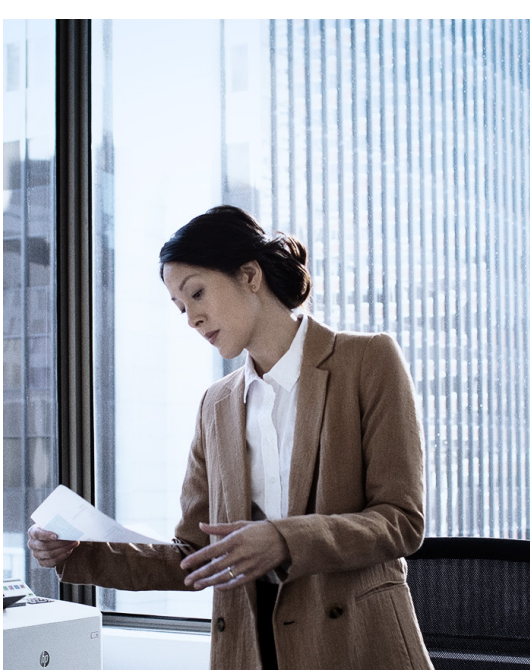
EMBEDDING SECURITY INTO THE HEART OF YOUR HYBRID WORKFORCE

Before organizations embark on large-scale, potentially cross-border projects to enable hybrid work, 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, to enable seamless collaboration between employees in their hybrid 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.[4]

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 hybrid workforce.

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.



Find out more about HP's endpoint security offering at hp.com/wolfenterprisesecurity

HP WOLF SECURITY

References:

[1] 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 2021 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.

[2] Third-party certification based on Common Criteria Information Technology Security Evaluation ISO/IEC 15408 Standard requirements as of May 2019-2024. 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%20Re- port%20-%20HP%20Intrusion%20Detection.pdf.

[3] 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

[4] IDC, IDC FutureScape: Worldwide Imaging, Printing, and Document Solutions and 3D Printing 2021 Predictions, Oct 2020