SECURE YOUR ARTICLE

References:
1. HP’s most advanced embedded security features are available on HP Enterprise and HP Managed devices with an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

TRANSITION TO A HYBRID WORKFORCE

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

OVERVIEW

When it comes to managing a distributed workforce, IT departments now have to defend against increasing threats to their devices and networks. The lack of embedded security can expose a network to all sorts of vulnerabilities. Malware can make its way onto a network through unsecured printers and copy machines and can potentially spread throughout your entire network, helping to expose your whole network to an attack. If anomalies are detected, your printer will automatically check your printer firmware during startup to determine if it conforms to the Common Criteria Information Assurance Rating Level (CIRL) and is updated with the latest version of the operating code (BIOS), which is your first layer of security.

Printers are everywhere, which makes them a critical entry point to your network. Yet, 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 operations run smoothly and improves workforce performance. Doing so can help daily operations run smoothly and improves workforce performance.

A comprehensive approach to printer security must go beyond technology. HP is helping organizations take back control of their printer fleet by making it easy to deploy the latest security technologies and manage a distributed fleet of printers — by requiring authentication to release print jobs. Job Whitelisting ensures the confidentiality of data in hard copy document printing and reduces unclaimed prints — by requiring authentication to release print jobs. Job Whitelisting

EMBEDDING SECURITY INTO YOUR HYBRID WORKFORCE

But before organizations can truly scale their printer projects in mobile-friendly environments, it is important to see that such environments are powered by secure devices.

Here, organizations must think outside the box and apply concepts such as cloud printing. By integrating cloud printing into their overall security strategy, organizations can help employees stay connected and collaborate through cloud printing. Doing so helps to build security into the printer’s hardware and firmware.

Easily onboard and integrate new platforms and processes, which enable remote and on-site employees to collaborate seamlessly and securely. With cloud-based printers, organizations can help eliminate isolated workforce silos by providing a single, unified experience across all locations.

NEW PRIORITIES FOR THE NO NORMAL

But for organizations planning such shifts, on-premises printers must first be transformed into a secure component of any organization’s efforts in pivoting towards a hybrid workforce.

But before implementing such plans, organizations must first turn to cloud printing. It’s a critical component of any organization’s efforts in pivoting towards a hybrid workforce. For IT, this means building the capacity to support cloud printing and ensuring that all of your devices are up-to-date with the latest security technologies.

Printers are everywhere, which makes them a critical entry point to your network. Yet, 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 operations run smoothly and improves workforce performance. Doing so can help daily operations run smoothly and improves workforce performance.

How Organizations are keeping up with changes in the workforce

HP FutureSmart benefits organizations through embedded security features, which enable decentralized management of your printer fleet. For example, HP Sure Start helps to prevent your printer from falling prey to malware when an unwitting user prints a document with malicious code. Successfully breaching one printer means they can potentially siphon off sensitive information and use cloud-based printers to distribute malware.

Here, organizations must rethink their approach to paper-based projects to enable hybrid work, it is important to re-examine their overall security strategy.

UPGRADE YOUR SECURITY WITH HP WOLF ENTERPRISE SECURITY FOR THE WORLD’S MOST SECURE PRINTERS:

1. HP Sure Start is your first layer of security. Every time your printer powers on, a self-healing reboot automatically checks your printer’s operating code (BIOS) and updates it if required. This helps to protect your printer from malware.

2. Run-Time Intrusion Detection reduces risks by monitoring your printer’s activity and immediately shutting down any intrusions, and reboots to initiate self-healing. Worry less about the security of your fleet with technology to evaluate your printer’s outgoing network connections to determine what is normal, and alert you to any intrusions quickly. (Run-Time Intrusion Detection requires an internet connection)

3. HP FutureSmart eliminates the challenges of managing a distributed fleet by helping to automate your printer’s deployment and management processes for IT administrators. HP FutureSmart also allows you to manage your printers from virtually anywhere.

4. Whitelisting allows you to quickly activate your printer for frequent use. Simply configure your printer to allow only trusted users to print.

5. Automatic Configuration leverages cloud printing and your organization’s integrated security platforms to automatically calculate the optimal printer configuration for your business.

6. 4AA6-1178ENW

Finding out more about HP’s endpoint security offering at hp.com/wolfenterprisesecurity

Print Security should not be overlooked