hp × Windows

Setting up remote workers? Avoid these security risks.

intel
Intel vPro® platform

HP recommends Windows 10 Pro for business.

When you're setting up remote workers, there are three risk areas you can act on right away to reduce exposures and strengthen protections across your business.

AVOID risks caused by security gaps across your organization's PC fleet.

60%

of breaches in a recent study were linked to a known vulnerability where a patch was available, but not applied.[1]

When workers take unpatched devices off the corporate network, they become extremely vulnerable to security breaches, especially if the OS is out of date.

✓ **ACTION:**

Implement the single most important security setting for any Windows 10 PC: Ensuring that updates are being installed on a regular, predictable schedule.

As cyberattacks grow increasingly more sophisticated, they carry greater consequences for hybrid workers. Modern PCs can help you create resiliency instead of risk.

✓ **ACTION:**

Add hardware-enabled security to your device strategy, along with encryption at both the software and firmware levels.

AVOID risks caused by legacy management models that rely on hands-on intervention.

69%

of IT professionals said they required physical access in order to secure a BYOD device[2]

51%

need the device PIN[2]

In the world of cybersecurity, after-market add-ons can be the equivalent of an unlocked door. And when you have to install security products physically, it slows you down and introduces point solutions that all have to be updated separately.

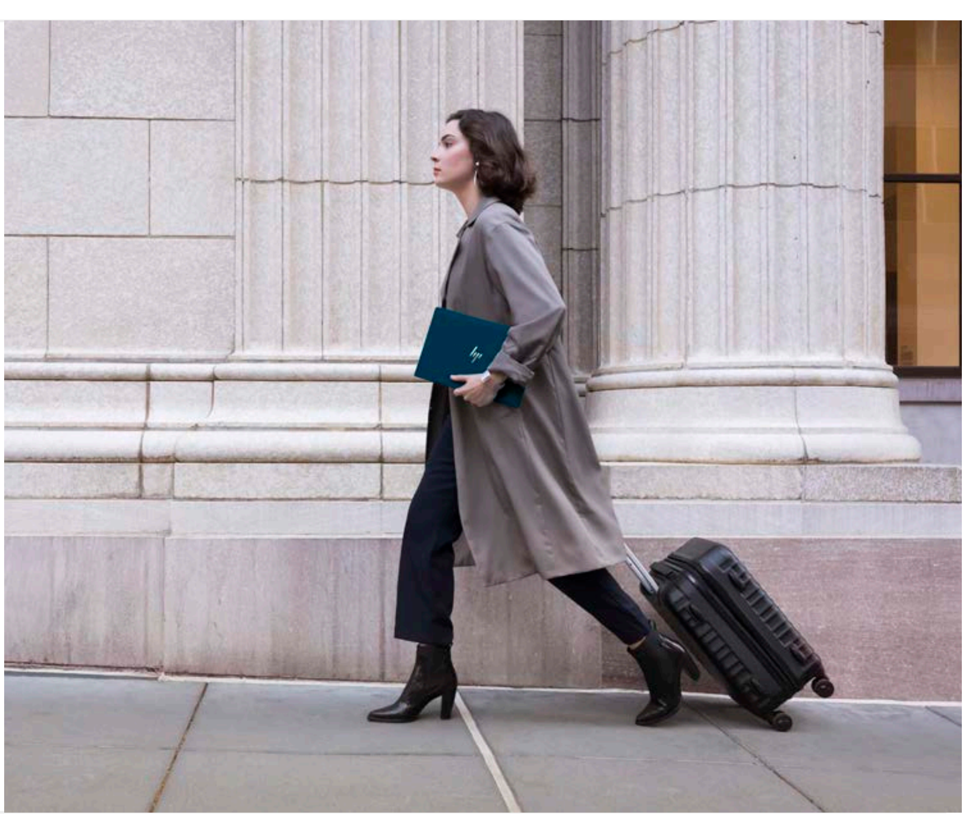
✓ **ACTION:**

Choose PCs that provide robust protections straight out of the box to make onboarding faster and easier, allowing you to drop-ship secure devices directly to employees and maintain updates without physical contact.

In case of an incident, remote access control allows you to quickly limit damage. You need the ability to remediate devices, recover from errors, and prevent DoS attacks on PCs that could be located anywhere.

✓ **ACTION:**

Enable remote access and manageability control when you set up new PCs. With faster security patch deployment and remote remediation for infected devices, you can solve issues fast—even if devices aren't powered on.



AVOID risks caused by ignoring common, highly destructive threats.

30%

of malware is disguised as a trusted attachment[3]

80%

of hacking-related breaches are tied to passwords[4]

Malware continues to pose a major threat to individuals and businesses alike. Malware comes in all forms, from email to ransomware to nefarious code inserted at the hardware level.

✓ **ACTION:**

Take advantage of built-in protections in Windows 10 Pro and the Intel® vPro® platform, which minimize the risk of malicious code injection by locking down system-critical resources to help prevent planted malware from compromising the OS.

Help keep your network and VPN safe from unauthorized access. Remote workers may have insecure home networks that inadvertently create opportunities for hackers to access corporate resources.

✓ **ACTION:**

Implement up to three factors of authentication for PC log in—including via fingerprint reader and IR-camera facial recognition like Windows Hello—with policies hardened at the silicon level.

Improve security and protection for your remote workforce.

HP offers the world's most secure and manageable PCs.[5] HP Elite Notebooks are made for today's challenges—with hardware-enforced security features and layers of protection below, inside, and above the OS to prevent threats and proactively recover quickly in the event of a breach. Sleek and light, Elite Notebooks offer advanced features like secure, wide-angle webcams; hardened security features like self-healing BIOS, 5G and 4G LTE connectivity, Audio by Bang & Olufsen, HP Noise Cancellation, and the power and performance needed for smooth virtual collaboration. Together with Windows 10 Pro and the Intel® vPro® platform, you get the latest software and out-of-the-box hardware security features to help defend your devices and your business.

When your IT is at its best, so are your people. Learn more.

HP EliteBook 830 Series

Meet the demands of your multi-task, multi-place workday with a beautifully designed, powerful and highly secure EliteBook 800 Series.

HP EliteBook 1000 Series

Powerful, precision-crafted, and versatile PCs that adapt to the way you get life done.

[1] Ponemon Institute, Costs and Consequences of Gaps in Vulnerability Response, December 2019
[2] Infosecurity Magazine, Organizations' Security Measures Failing to Keep Pace with BYOD Use, July 2020
[3] TechJury, The Most Telling Cyber Security Statistics in 2020, June, 2020.
[4] Verizon, 2020 Data Breach Investigations Report, 2020.
[5] Based on HP's unique and comprehensive security capabilities at no additional cost and HP's Manageability Integration Kit's management of every aspect of a PC including hardware, BIOS and software management using Microsoft System Center Configuration Manager on HP Elite PCs with Windows and 8th Gen and higher Intel® processors; and HP ProDesk 600 G6 with Intel® 10th Gen and higher processors.