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

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

**60%**[1] of breaches in a recent study were linked to a known vulnerability where a patch was available, but not applied. Vulnerability response is a foundational step to securing your PC fleet.

As technology becomes more sophisticated, so do the threats. As a result, you should take advantage of features like Windows AutoUpdate to help secure your PC fleet with the latest security updates.

**ACTION:**
- Implement Windows AutoUpdate (see the Getting Started Guide for details).
- Keep all of your software and firmware levels up to date to help increase protection.

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

**69%**[2] of IT professionals said they needed the device PIN in order to secure a BYOD device. And **51%**[3] of hacking-related breaches are tied to passwords.

A remote workforce means new challenges when it comes to managing hardware and software updates. HP PCs feature built-in remote access capabilities that can help reduce this risk.

**ACTION:**
- Use Windows AutoUpdate to automatically update software and firmware levels.

**AVOID risks caused by ignoring common, highly destructive threats.**

**80%**[4] of IT professionals said that physical access in the event of a breach is a major concern. Sleek and light, HP Elite Notebooks offer advanced features like secure, wide-angle webcams; hardened security features like self-healing BIOS, 5G and 4G 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 services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

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 sensitive information. Keep your home network secure with devices like Windows Hello, a biometric reader and IR-camera facial recognition like Windows Hello—with policies hardened at the hardware level.

**ACTION:**
- Implement up to three factors of authentication for PC log in—including via fingerprint software and firmware levels.

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

Learn more.

---

[1] Ponemon Institute, Costs and Consequences of Gaps in Vulnerability Response, December 2019