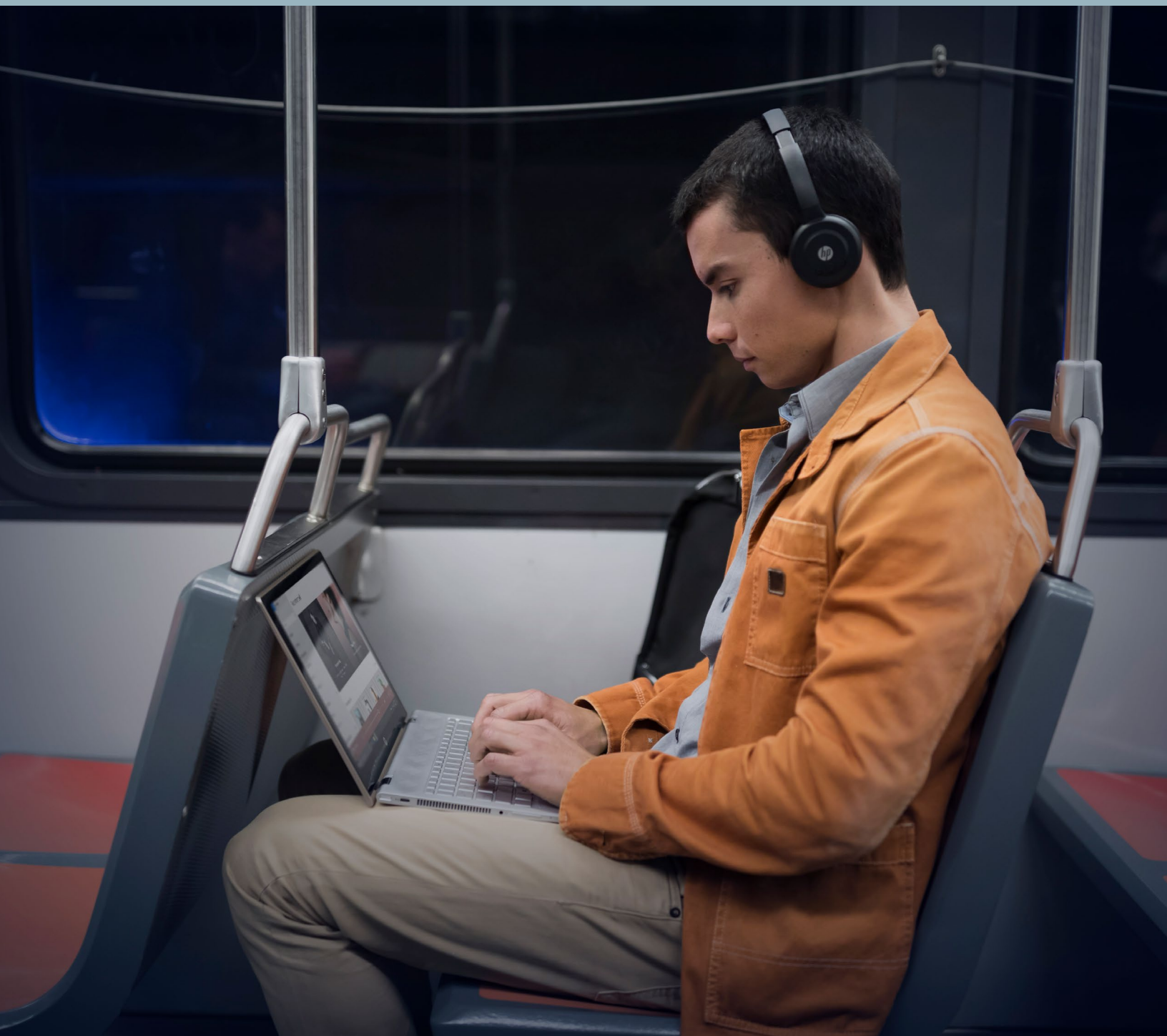
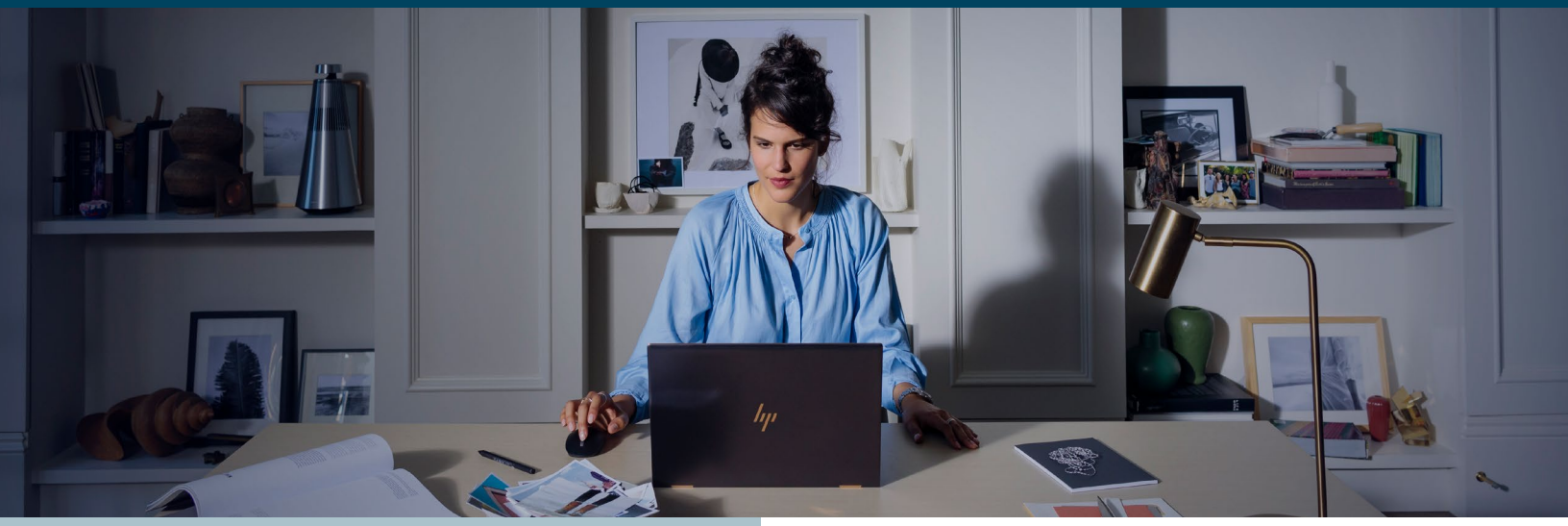
SOLUTION OVERVIEW

HP WOLF SECURITY

Security for a Hybrid Workplace

Improving IT operations while decreasing risk





Security: Factors to Consider

Availability

User Experience

IT Efficiency

Risk Management

400%

increase in cyberattacks since the pandemic began.[1]

Security plays a crucial role in enabling the hybrid workplace. IT decision-makers are well-aware of the need for IT Security, as they are confronted with near-daily reports of successful attacks targeting all types of organizations. But the composition of their security architecture has even deeper implications, as it affects four crucial areas:

- Availability: Security breach takes down PCs or applications.
- User Experience: Inconsistent access to data or performance degrades employee productivity.
- IT Efficiency: Unacceptable OpEx due to excessive staff requirements or outsourcing costs.
- Risk Management: Potential data loss, brand compromise, or compliance findings or fines.

This makes it clear that security is everyone's problem, and IT and Security must collaborate to deliver consistent outcomes across all four dimensions. Furthermore, security strategy must be part of the hardware procurement process and lifecycle to optimize outcomes. Simply "bolting on" software solutions to commoditized hardware increases both risk and operational costs.

HP's perspective is that the endpoint is the one nexus where all four considerations come together. The combination of hybrid work and cloud computing results in a patchwork of systems and connections that make it difficult to apply security policy consistently and efficiently. The endpoint device is the exception: It's where the data and user meet. And since the PC is always part of the user experience, failure can be catastrophic. For example, a control failure on a cloud application might degrade that one app. But a failure of the user's PC will prevent them from doing anything at all.

HP Endpoint Security

Enhancing outcomes for IT and Security with 3 core principles

1 Full-stack Security

Just as you can't build a stable building on a weak foundation, you can't securely run applications on weak infrastructure. HP takes a full-stack approach to create a solid operational environment on the endpoint:t

- User
- Applications
- Operating System
- BIOS
- Resilient PCs and Printers
- Factory Services

This methodology prevents gaps that could be exploited by attackers and simplifies hardware deployment and operations.

2 Inherent Protection

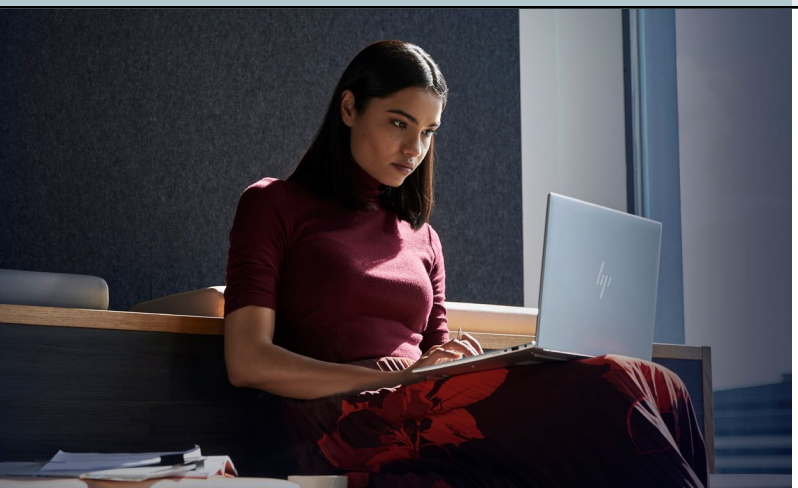
In an ideal world, you prevent all attacks all the time. Unfortunately, this is impossible in practice no matter how much money you commit to the goal. But the more prevention you do, the less risk you have, and the smaller the operational challenge. Our hardware-assisted HP Threat Containment takes this approach by isolating potentially risky tasks so that malware can't infect the PC.

HP Threat Containment reduces operational overhead by making PC remediation a less frequent occurrence. Crucially, it drives availability and maintains a consistent user experience.

3 Operational Efficiency

Security that is difficult to deploy and maintain is not acceptable in the hybrid workplace. Not only does complex security degrade user experience and increase costs, but it also increases risk through improper policy management and monitoring. HP prioritizes ease of operations across the device lifecycle and uses cloud technologies to eliminate dependency on on-premise infrastructure or physical device access.

HP's protection-first, full-stack approach delivers outcomes that help improve IT efficiency and security. This allows you to move beyond an "avoid getting hacked" mentality to one focused on process enablement.



HP's protection-first, full-stack approach delivers outcomes in support of both improving IT efficiency and security. This allows you to move beyond an "avoid getting hacked" mentality to one focused on process enablement.

IT Operational Outcomes

Incident and disaster recovery

Re-establish employee productivity in case of endpoint corruption failure or disaster scenario

Staff productivity

Minimize downtime or upgrade service interruptions to maximize productivity

Modern endpoint management

Cloud-based endpoint management, often based on Microsoft Intune

Lifecycle management

Efficient PC support from procurement to retirement

Risk Management Outcomes

Safer supply chain

Factory oversight helps prevent device compromise

Data theft protection

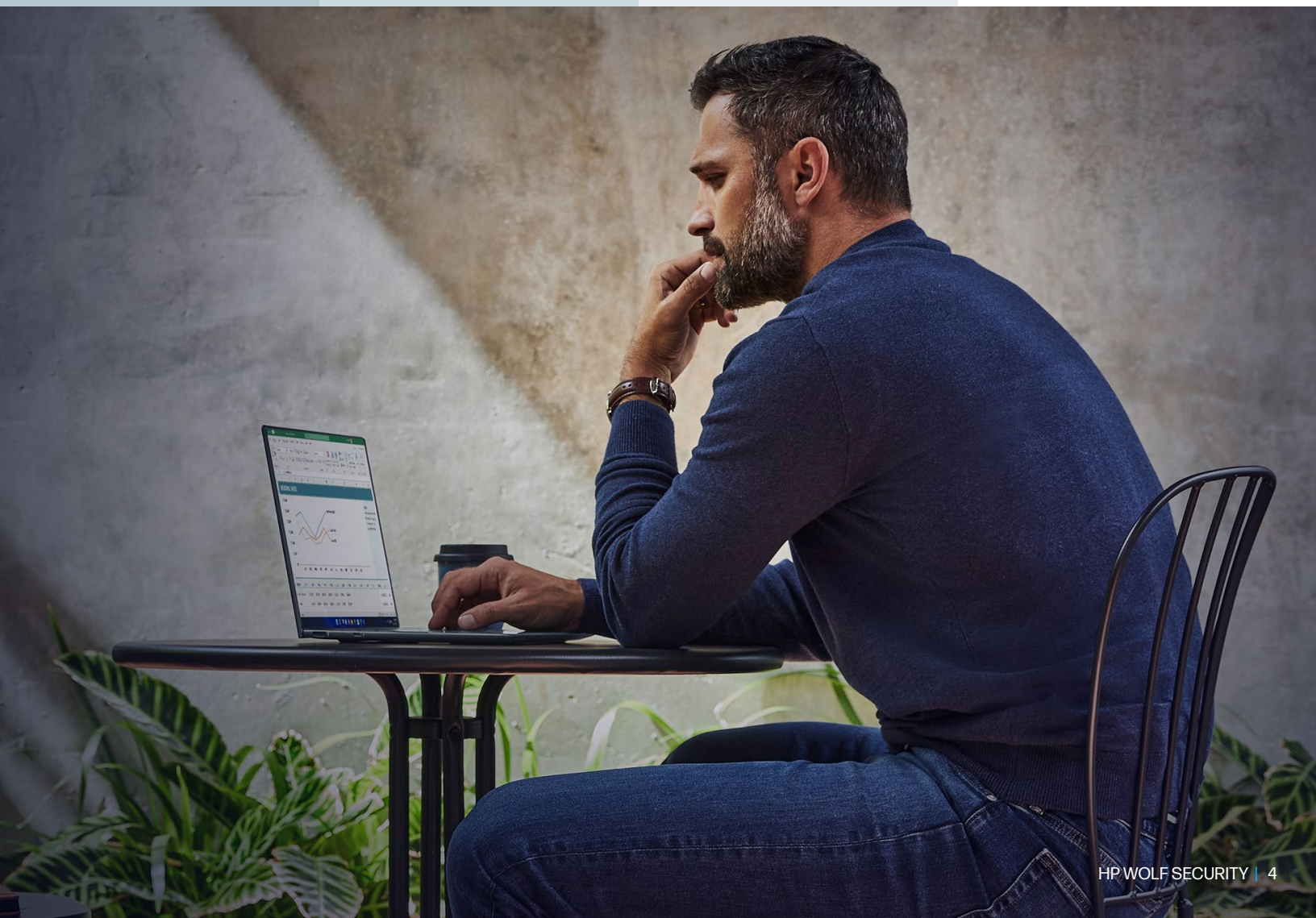
Device security helps protect data in the event of loss or theft

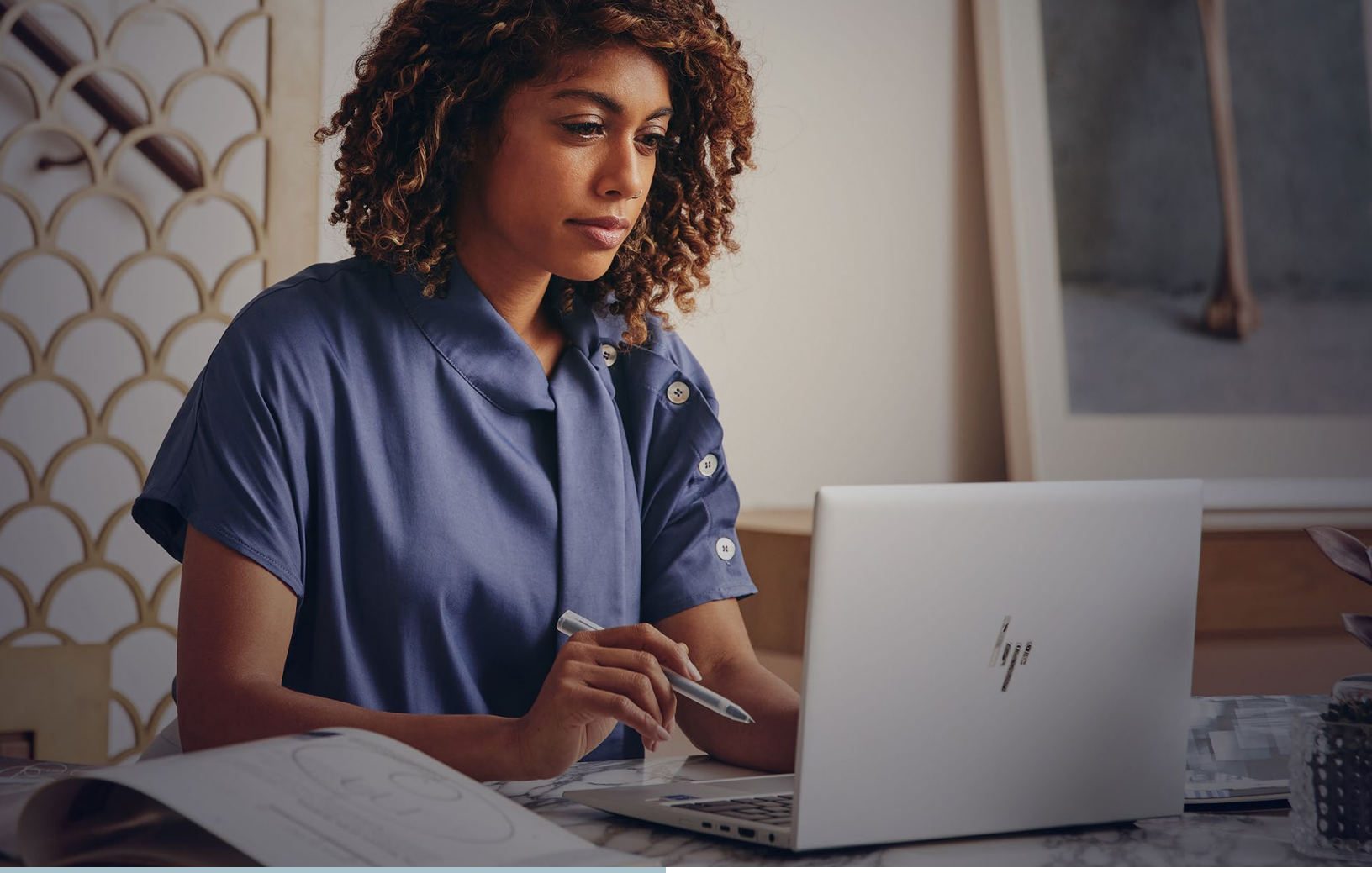
Compliance controls

Robust controls on infrastructure avoid unnecessary risks

PC system integrity

Hardware-assisted threat containment isolates risky tasks





A Simpler Approach to Securing Hybrid Work

Unlike point security solutions which add complexity, HP's approach – including our hardware-enforced HP Wolf Security for Business[2] – simplifies life for the IT Operations and Security teams. We believe that the pursuit of "zero-trust" security cannot come at the expense of user experience or IT overhead. With hardware and software that work in concert, HP delivers zero-trust risk management while also improving operational efficiencies throughout the device lifecycle.

The result is a hybrid workplace that is robust, cost-effective, and enables staff productivity.

Explore hybrid work and security solutions →

1. ZDNet. "FBI says cybercrime reports quadrupled during COVID-19 pandemic." https://www.zdnet.com/article/fbi-says-cybercrime-reports-quadrupled-during-covid-19-pandemic/

2. HP Wolf Security for Business is included on select HP PCs and requires Windows 10 or 11 Pro and higher, includes various HP security features, and is available on HP Pro, Elite, RPOS and Workstation products. See product details for included security features.