

# HP PC Platform Full-Stack Security



Delivering the World's Most Secure and Manageable PCs<sup>1</sup>

## Highlights



The endpoint PC is the most crucial cyber-security battlefield.



Attackers are increasingly exploiting opportunities "Below the OS".



HP's Full-Stack risk management approach builds a resilient endpoint platform, layer by layer.



The Full-Stack approach lowers IT operational overhead while improving security and availability.

### Partner information

Website: [www.lirex.com](http://www.lirex.com)

→ Contact information:

Tel.: +359 2 9 691 691

[office@lirex.com](mailto:office@lirex.com)



## Security starts and ends with the endpoint PC

The endpoint user PC is where people, data, and the cloud converge. It's also the place cyberattackers focus their attacks. With the rise of remote working and hybrid computing, the endpoint is the crucial component that must be both highly available and secure.

However, reducing IT operational overhead is another key initiative, creating a problem: how can organizations both protect their PCs and keep operations costs under control?

HP's approach to PC risk management is Full Stack Platform Security. It is based on a fundamental premise: you can't build a secure execution environment on a weak foundation. The Full-Stack approach builds resiliency a layer at a time, so that each layer can trust the layer below it. Starting from a hardware-based root of trust and optional Factory Services, the strategy creates a resilient computing platform with lower operational overhead for either an internal IT team, or a managed services provider.

## HP's Full-Stack Approach



Users and Data



Operating System



Firmware/BIOS



Hardware



Factory Services

# HP Platform Security - Use Cases

## A Win-Win for IT Operations and Risk Management

HP has long been a leader in securing the PC platform, with over twenty years of continuous investment and innovation. That commitment has delivered a comprehensive set of security controls below the operating system, as well as integrated controls with the OS, in particular Microsoft Windows.

The Full-Stack security control set included in HP business class PCs support eight key use cases and business outcomes. These are described below: the first four being of most interest to IT/Endpoint Operations, and the last four being most relevant for Security and Risk Management.

### HP Full-Stack Security: IT Operations Use Cases












Use Case	Description	Capabilities
MODERN MANAGEMENT	Cloud-based PC management, often based on Microsoft Intune	Secure OS image management; autopilot factory enrolment; remote BIOS configuration management
LIFECYCLE MANAGEMENT	Efficient PC support from procurement to retirement	Initial installation and upgrades of custom OS images & firmware; BIOS resiliency; and device location services for PCs that leave the office
INCIDENT & DISASTER RECOVERY	Re-establish employee productivity in case of PC corruption failure or disaster scenario	Recover clean OS image at scale on remote PCs
INCREASED STAFF PRODUCTIVITY	Minimize PC downtime or upgrade service interruptions to maximize productivity	Rapid OS re-imaging; Seamless BIOS updates

### HP Full-Stack Security: Risk Management Use Cases

Threat	Risk	Capabilities
SUPPLY CHAIN RISK	Device compromise prior to onboarding renders OS level security ineffective for PCs	BIOS integrity; BIOS configuration integrity; physical integrity
PC PLATFORM INTEGRITY	Malware compromises firmware causing persistent malware presence on PCs	BIOS integrity; BIOS configuration integrity
PHYSICAL COMPROMISE	Unattended PC compromised via physical action	Secure BIOS; USB Controls
COMPLIANCE & AUDIT	Inadequate controls on in-scope infrastructure leads to audit findings	Software and configuration controls on underlying platform helps meet PCI compliance

# HP Full-Stack Platform - Capabilities

The following table describes the risk management capabilities that make up HP's Full-Stack secure PC platform. These capabilities are included with HP business class PCs<sup>2</sup> and collectively support the eight use cases described previously.

 <p><b>Factory Services<sup>3</sup></b></p> <p>Pre-populate PCs with customer-specific data and credentials to ensure supply chain resilience and to ease device deployment.</p>	 <p><b>Endpoint Security Controller</b></p> <p>Custom silicon provides hardware root-of-trust and secure storage for higher-layer controls, such as Sure Start.</p>	 <p><b>BIOSphere<sup>4</sup></b></p> <p>Enhanced firmware protection from first booted up, guarding against malicious attacks and accidental errors that can compromise the BIOS includes secure boot, firmware protection and simplified BIOS updates.</p>	 <p><b>Sure Start<sup>5</sup></b></p> <p>Protects PCs BIOS firmware from malware or corruption by ensuring only trusted code is executed.</p>
 <p><b>Sure Admin<sup>6</sup></b></p> <p>Eliminates the need for BIOS passwords by creating a digital signature that allows IT administrators to securely manage PCs BIOS configurations locally or remotely.</p>	 <p><b>Seamless Firmware Update<sup>7</sup></b></p> <p>Enable BIOS and Firmware updates while end users remain productive.</p>	 <p><b>Sure Run<sup>8</sup></b></p> <p>Keeps critical processes running when users or even advanced malware tries to shut them down.</p>	 <p><b>Sure Recover<sup>9</sup></b></p> <p>Reduces downtime and lost productivity by leveraging the power of the HP Endpoint Security Controller to quickly restore the operating system when the hard drive has been compromised or corrupted.</p>
 <p><b>Tamper Lock<sup>10</sup></b></p> <p>Protects the PC from physical intrusion and component tampering while in transit or unattended.</p>	 <p><b>Sure View<sup>11</sup></b></p> <p>An integrated privacy screen built directly into select HP business PCs ensuring the protection of your confidential information from unauthorized viewers.</p>	 <p><b>Sure Shutter<sup>12</sup></b></p> <p>A built-in electronic shutter covering your PC webcam protecting you from any malicious webcam surveillance.</p>	

## Optional Use Case: PC Loss or Theft



### Protect & Trace<sup>13</sup>

The security and operational impacts from a missing or stolen PC can be massive. To mitigate these impacts, HP offers Protect & Trace. Available as a software option for HP PCs, Protect and Trace provides three capabilities to enable organizations to better cope with a lost PC:

- Locate the PC
- Temporarily lock access to the PC while it is being recovered
- Remotely wipe the data on the PC if deemed appropriate to protect data

---

# Summary

Companies have long known that strong security is fundamental to business success. However, the continued success of cyberattacks on these organizations suggest that new approaches are needed. HP Wolf Security helps provide some of the most secure PCs by building security from the hardware up through each layer of the stack. HP PC Platform Security is designed to increase IT operational efficiency, improve availability and deliver end user productivity while meeting company risk management goals.

---

<sup>1</sup>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; HP ProDesk 600 G6 with Intel® 10th Gen and higher processors; and HP ProBook 600 with Intel® 11th Gen processors and higher.

<sup>2</sup> Feature support may vary by PC model.

<sup>3</sup>Factory Services - HP Services are sold separately. HP services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product.

<sup>4</sup>HP BIOSphere Gen6 features may vary depending on the platform and configuration.

<sup>5</sup> HP Sure Start is available on select HP products.

<sup>6</sup> HP Sure Admin requires HP Manageability Integration Kit and HP Sure Admin Local Access Authenticator smartphone app from the Android or Apple store.

<sup>7</sup> Seamless Firmware Update is supported on HP Intel G9 platforms.

<sup>8</sup> HP Sure Run is available on select Windows 10 and 11 Pro, Windows for IoT, and higher HP products.

<sup>9</sup> HP Sure Recover is available on select HP products and requires an open network connection. You must back up important files, data, photos, videos, etc. before using HP Sure Recover to avoid loss of data.

<sup>10</sup> HP Tamper Lock must be enabled by the customer or your administrator.

<sup>11</sup> HP Sure View is an optional feature that must be configured at purchase and is designed to function in landscape orientation.

<sup>12</sup> HP Sure Shutter only available PCs equipped with HD or IR camera and must be installed at the factory.

<sup>13</sup> HP Services are sold separately. HP services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product.