HP'S PRODUCT SUPPLY CHAIN

HP takes Product Supply Chain Cybersecurity very seriously. We understand that strong security measures represent the best opportunity to mitigate risks associated with attempts to counterfeit or tamper with our products. We begin by thoroughly vetting our supply chain all the way from the component level to our logistics partners.

For our Suppliers to meet the expectations our customers have placed on us, we developed a Product Cybersecurity Standard that lists requirements designed to protect the integrity of our products.

Some examples of key requirements of our Product Cybersecurity Standard:

Assigning accountability: we establish a key point of contact that is responsible for implementing processes and training of on-site personnel.

Responsible electronic part sourcing: our sourcing standard requires that all electronic components meet US Department of Defense standards on a global basis.

Installing software: strict protocols and procedures for the loading of firmware, software and customer images in a controlled secure environment.

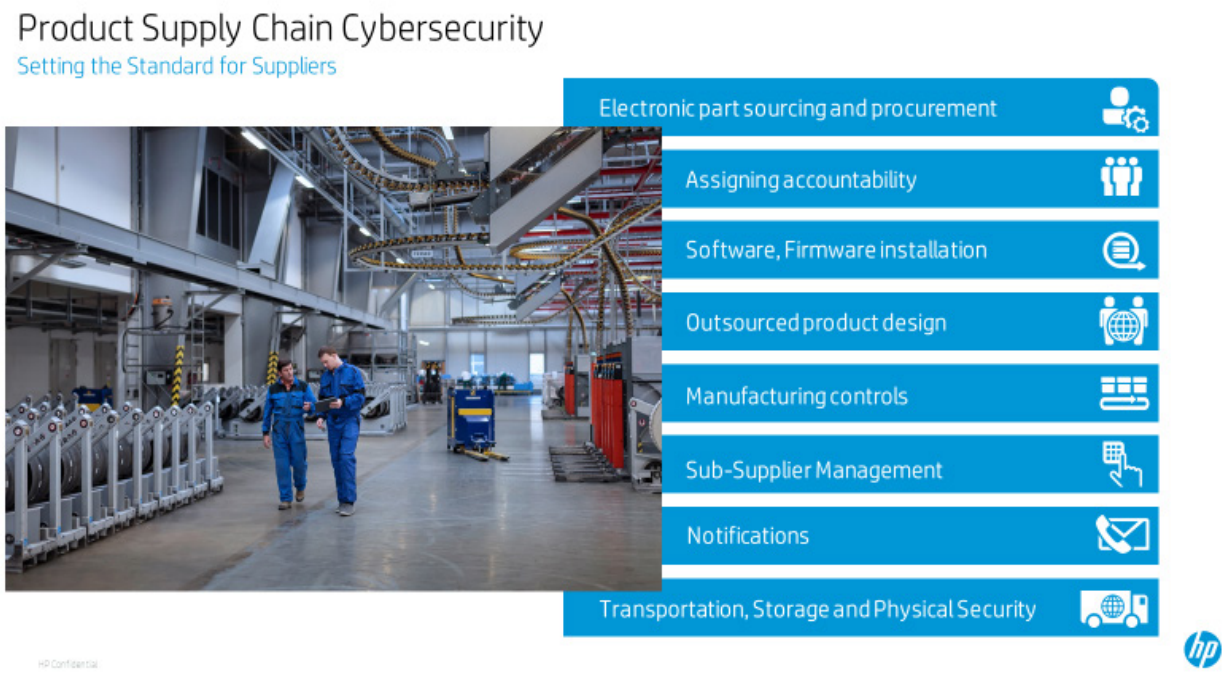
Outsourced product design: we require our original design manufacturer suppliers to follow Secure Development Life Cycle best practices and conduct penetration testing against exploitation tactics.

Manufacturing controls: running anti-malware scans on all systems used to support or produce product, using current operating systems, establishing a secure environment for information technology systems.

Sub-Supplier management: we require compliance at all levels of our supply chain.

Securing transportation and physical locations: we implement solutions to prevent loss or interference including tracking, real time monitoring of routes, schedules, alarm systems. Our suppliers deploy security guards, limit access, use video, and fence their perimeters.

Company alignment: we have a clear escalation path for all issues raised around compliance with the Product Cybersecurity Standard.

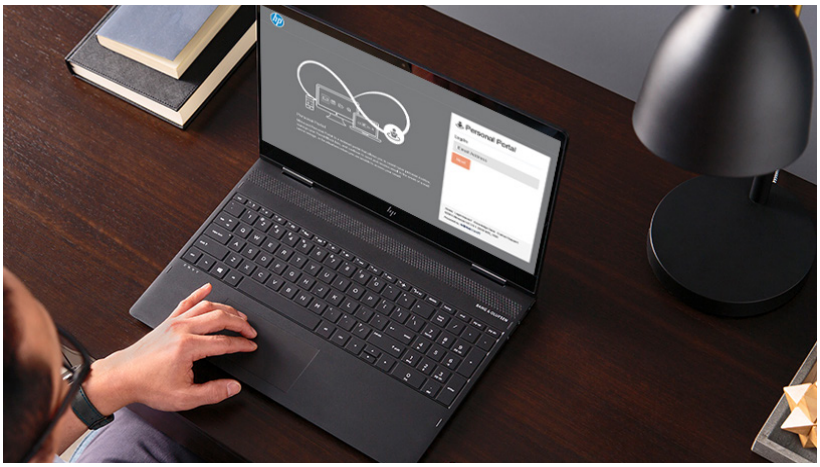


HP Product Security and Privacy

As cyberattacks become increasingly prevalent and sophisticated, security breaches are a growing concern for our customers. In response, we are continually evolving HP products, solutions, and services to offer industry-leading resiliency capabilities that anticipate an ever-evolving attack and threat landscape.

We follow security and privacy by design principles for all of our products, from design through customer use, refurbishment, and recycling. We build protection, detection, and recovery into the device, not just the software, which provides customers with separate, auditable mechanisms for managing security risks.

To protect against the malware of the future, PCs and printers must have hardware-level security that seamlessly integrates with the customers' broader IT network security infrastructure. This is the foundation of HP's strategy.



Our Security Management Review Committee, composed of business leaders from across the company, oversees and aligns our portfolio-wide approach to security and provides necessary resources to support HP's continued leadership. An external Security Advisory Board was launched in 2017 to provide insights that HP will use to reinforce its own security work. All three initial members have unique first-hand expertise in the world of hacking and the latest developments in security technology and strategies.

We employ cybersecurity specialists and conduct cybersecurity architecture reviews, penetration testing, code reviews, and automated code scanning using industry-leading tools. When issues arise, we take appropriate actions to remediate reported security vulnerabilities.

Our supply chain security group works to ensure that HP products are built to resist attacks throughout the supply chain life cycle, from component sourcing through service. We establish supply chain controls and our HP Product Cybersecurity Standard for Suppliers, enforced through periodic audits, contractually holds all suppliers to requirements which mitigate the risks of counterfeits, malware, and tampering.

Personal systems

HP's comprehensive set of security solutions for our commercial personal systems protect not only the device, but also the user's identity and data—making our PC's and work stations world class in terms of security management.

Security

Available on most of our commercial PCs, HP Multi-Factor Authenticate Gen2 integrates Intel's Authenticate technology with credentials such as a password, fingerprint, and facial recognition to make user login a million times more secure. In 2017, we announced HP Sure Click, a hardware-enforced secure browsing solution. Each browsing tab is isolated, which changes the security paradigm by isolating malware to prevent harm. New in 2018, HP Sure Click also protects PDF files and Microsoft Office documents in read mode.

HP SURE START

MULTI-FACTOR AUTHENTICATION

HP SURE VIEW

Basic Input/Output System (BIOS) security has been designed into our products since 2006. Beginning in 2018, we build our Elite and Pro 600 lines of PCs with HP Sure Start Gen4 which can detect and recover from an advanced persistent BIOS attack in less than a minute. HP Sure View Gen2 the world's only PC integrated privacy screen, makes it harder for unauthorized people to steal data by peering over the shoulders of unsuspecting users. Now in its second generation, HP Sure View enables a better visual experience in either bright or dark environments—from the plane to the café.

On our Elite PCs, beginning in 2018, HP Sure Run extends the HP Endpoint Security Controller's self-healing protection into the operating system. HP Sure Recover offers secure, automated, network-based software image recovery using the HP Endpoint Security Controller and an Internet connection.

Manageability

HP Manageability Integration Kit Gen2 the world's first and only automated management toolkit certified for Microsoft System Center Configuration Manager provides IT administrators the tools they need to enforce security policies. Previously, this was mostly a manual process.

Printers and Multifunction Devices (MFD)

HP printers and Multifunction Devices (MFD) provide the industry's strongest security features. HP's Enterprise LaserJet and PageWide Enterprise products automatically self-heal and recover from attacks, following four unique and automated steps:

HP Sure Start validates the BIOS if compromised, recovers with a safe "golden copy"

Whitelisting authenticates that the firmware is authentic and has not been tampered with before running it

Run-time intrusion detection continually monitors memory activity to detect and stop attacks, and then recover the device to a secure state

HP Connection Inspector analyzes outgoing network connections to stop suspicious traffic and recover the device to a secure state

HP Secure Managed Print Services

HP's JetAdvantage Security Manager is the industry's only policy-based printer compliance tool that assesses and remediates HP printer fleets. For security administrators in 2018, HP has expanded our position as the easiest print fleet to secure and manage with new McAfee SIEM integration to complement our certified integrations with Splunk, ArcSight, and SIEMonster tools.

HP Printer Security Plug-in

HP Printer Security Plug-in is a policy-based printer security compliance tool that integrates with the industry standard Microsoft System Center Configuration Manager (SCCM). While compliance settings in System Center Configuration Manager provide the tools and resources required to manage the configuration and compliance of devices such as computers, servers, and mobile devices, the HP Printer Security Plug-in allows for discovery of HP printers to ensure they remain compliant with desired security standards. Managing security is important to minimize data breaches and vulnerabilities across the print fleet. As technology improves, malicious users may target MFPs and other network peripherals to misuse resources or to gain access to networks or the internet. For more information, please go to HP Printer Security Plug In.

4AA7-4216ENW, December 2018