Technical Whitepaper

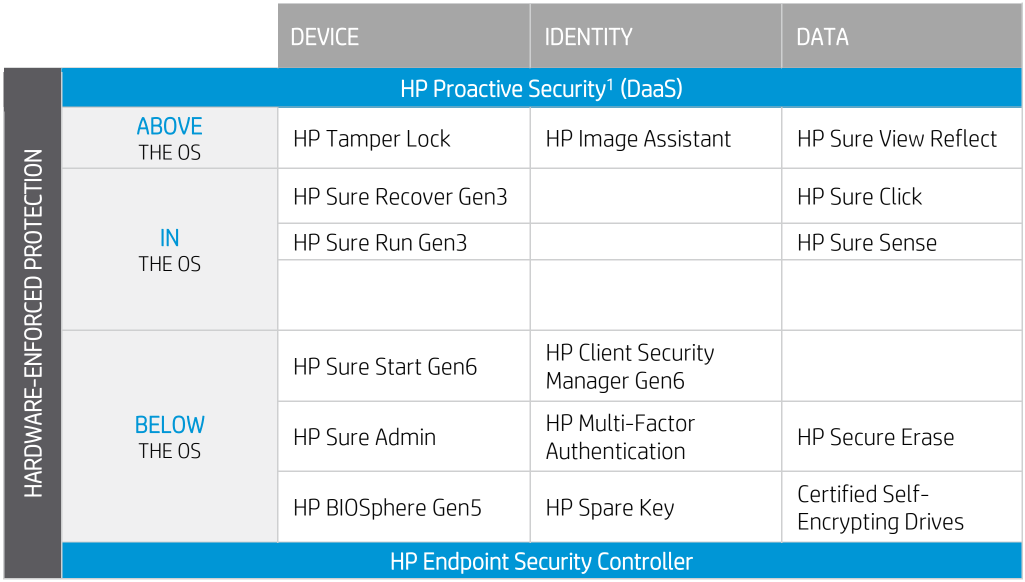
HP Essential Security Overview

HP Security Stack for Commercial PCs

In today's changing landscape, a majority of people are working from home and PC security is at risk. Business PCs are used outside of the secure office environment, and traditional network-based security alone cannot meet security needs. In these changing times, Endpoint devices are the first line of defense, and hardware-based PC security is needed more than ever. While the digital landscape keeps changing and security risks evolve, the security solutions engineered into HP Business PCs are designed to protect your business. From the moment your PC is switched on, the security products in the HP Security Stack are working together in the background to protect your business PCs.

Table of Contents

HP Essential Security Components



		DEVICE	IDENTITY	DATA
HARDWARE-ENFORCED PROTECTION	HP Proactive Security[1] (DaaS)			
	ABOVE THE OS	HP Tamper Lock	HP Image Assistant	HP Sure View Reflect
	IN THE OS	HP Sure Recover Gen3		HP Sure Click
		HP Sure Run Gen3		HP Sure Sense
	BELOW THE OS	HP Sure Start Gen6	HP Client Security Manager Gen6	
		HP Sure Admin	HP Multi-Factor Authentication	HP Secure Erase
		HP BIOSphere Gen5	HP Spare Key	Certified Self-Encrypting Drives
	HP Endpoint Security Controller			

HP Essential Security Component Details

Learn more about each component of HP Essential Security and how they protect your PC.[2]

HP Endpoint Security Controller

The HP Endpoint Security Controller is the hardware component at the foundation of the HP Business PC security architecture. This physically isolated and cryptographically protected hardware microcontroller below the OS creates the hardware root of trust that enables hardware-enforced, self-healing, manageable security solutions like the HP BIOSphere Sure Start, HP Sure Run, and HP Sure Recover.

HP BIOSphere Gen5

Building on over a decade of BIOS security leadership, HP BIOSphere PC firmware automates BIOS protection and delivers improved manageability. The BIOS is a series of boot instructions used to load critical hardware components and initiate firmware. HP BIOSphere creates an ecosystem of protection around the BIOS below the OS to help defend your PC. With automated protections, customizable safeguards, and easy manageability, HP BIOSphere protects your PC against attacks without interrupting employee productivity.[3]

HP Sure Start Gen6

From the moment the PC is switched on, HP Sure Start works below the OS to protect the device by communicating with the HP BIOSphere to confirm the BIOS is unchanged. If any BIOS tampering is detected, HP Sure Start, in concert with the HP Security Controller, replaces the BIOS with a clean version and boots up the computer with clean and fully functional BIOS. HP Sure Start continues to perpetually inspect the system BIOS and automatically self-heals if the BIOS is damaged by malware, rootkits, or corruption. By ensuring that only trusted BIOS code is executed, HP Sure Start protects your PC at its most fundamental level.[4]

New for Gen6:

- Now available on extended portfolio from ProBook 400 series to EliteBook 1000 series, including AMD PCs
- Smart Flash technology provides a 91% recovery time improvement by erasing and preprogramming any 4kb block that is not as it should be
- Endpoint Security Controller runtime intrusion detection delivers Memory Protection Unit (MPU) support within Endpoint Security Controller by detecting and blocking any rogue code execution on Endpoint Security Controller
- Protects against preboot DMA attacks on internal slots with visual on the bottom of Intel PCs

HP Sure Run Gen3

HP Sure Run protects the device below the OS by using hardware-enforced protection to keep critical processes running, even if malware tries to shut them down. Backed by the HP Endpoint Security Controller, HP Sure Run monitors key processes, alerts users and IT of any changes, and restarts key processes automatically if they are stopped. As the HP hardware-enforced application persistence solution, HP Sure Run has the capability to maintain communications with the policy enforcement hardware while the OS is running. HP Sure Run continually monitors the presence of critical services and applications, even if the HP Sure Run agent in the OS is attacked or removed. HP Sure Run interfaces with the HP Endpoint Security Controller at the hardware level below the OS to ensure OS integrity. It is included at no additional charge in select HP products.[5]

New for Gen3:

- Dynamic Persistence automatically reinstalls agent if stopped
- Kill Prevention stops malware side effects

HP Sure Recover Gen3

Built into the system hardware and firmware, HP Sure Recover protects the device by empowering users to restore their machines quickly and securely to the latest image using only a network connection. With HP Sure Recover, with Embedded Reimaging[7], the user can install the operating system and drivers from a dedicated local storage device without IT intervention. HP Sure Recover boosts resilience and minimizes downtime via an automated operating system recovery solution integrated into HP computer hardware and firmware. HP Sure Recover enables you to quickly recover the operating system whenever needed, throughout the lifecycle of the computer. HP Sure Recover succeeds even if the primary drive has been completely erased. HP Sure Recover empowers IT to schedule reimaging for the entire fleet.[6]

New for Gen3:

- Provides cloud network-based recovery using Wi-Fi
- Offers efficient recovery with pause, resume, and retry

HP Client Security Manager Gen6

HP Client Security Manager provides the strength of hardware-based security authentication to support the efforts of users and IT professionals to protect their identity by configuring and controlling a variety of security features embedded in HP PCs within the OS, including HP Sure Run, HP Spare Key, Multi-Factor Authentication, and more.[8]

HP Sure Admin

HP Sure Admin provides IT professionals a path to move away from password-based BIOS management with an optional no password required BIOS management tool. HP Sure Admin offers a modern approach based on strong public key cryptography that can be use to securely manage HP business PC BIOS settings without the need to reveal the authorization secret.

HP Sure Admin remote management tools offer an innovative way to empower the Remote Administrator and Locally Present Administrator to remotely manage HP business PC BIOS settings to serve the user quickly and securely.[9]

HP Multi-Factor Authentication

HP Multi-Factor Authentication helps you keep your network and VPN safe from unauthorized access and protects your identity by requiring up to three factors of authentication for log in—including optional fingerprint reader and IR camera facial recognition—running within the OS with policies hardened at the silicon level. With the increase in data and security breaches, long and complicated passwords are no longer enough. Increasing the information required at log in can reduce the potential for identity fraud and costly data theft; however, requiring users to spend increased time typing multiple PINs or complicated passwords can lead to user frustration. HP Multi-Factor Authentication provides a way forward. HP Multi-Factor Authentication uses multiple factors or methods to verify user identity, strengthening identity security without placing an undue burden on the user. Instead of requiring the user to memorize multiple credentials of the same factor—like a password and a security question (both knowledge-based factors), HP Multi-Factor Authentication uses multiple factors—something the user knows, something the user has, and something the user is—to create a custom blend of identity authentication that is effective without being cumbersome. Something the user knows might be a password or a PIN. Something the user has might be a Bluetooth phone or a smartcard. Something the user is may be facial or fingerprint recognition. HP Multi-Factor Authentication empowers both users and IT professionals with a custom blend of easily implemented user authentication that works for them. Solutions that are more easily implemented have a higher percentage of user compliance and Multi-Factor Authentication guards against fraudulent logins by any attacker who gains access to one type of sensitive information.[10]

HP SpareKey

Forgot your Windows password? HP SpareKey works within the OS to protect identity, reset passwords, and restore access to locked PCs without intervention from IT personnel by taking the user through a series of predetermined security questions.

Certified Self-Encrypting Drives

Self-encrypting hard drives and solid-state drives employ hardware-based encryption to protect their contents even after the drive is removed from the PC. And because the data encryption process is hardware based, there's little to no discernable impact on performance.

HP Secure Erase

Simply deleting files from a hard drive doesn't make them unrecoverable. HP Secure Erase is a BIOS-level feature that protects data by permanently destroying sensitive information from hard drives and solid-state drives, ensuring the deleted information can never be recovered or compromised.[11]

HP Sure Click

Users are increasingly accessing consumer and enterprise applications on the go, on untrusted networks, and often from their own personal devices. Web browsers are a primary attack vector for malware and other online threats. HP Sure Click provides a revolutionary solution developed through the collaboration of HP and Bromium, the pioneers of application isolation using patented microvirtualization technology. HP Sure Click is a hardware-enforced, secure browsing solution within the OS that isolates web content in a CPU-isolated virtual machine, where malware cannot affect other tabs, applications, or the operating system. By effectively isolating the contained browser activity, HP Sure Click reduces the ability of a compromised process to do damage. With HP Sure Click, the endpoint device can shrug off browser-borne attacks. Malware is blocked from accessing documents, enterprise intranets, or even other websites, and automatically erased when the browser tab is closed, thereby eliminating costly remediation and downtime. HP Sure Click task isolation protects users as they work and play, delivering unparalleled security and privacy within a fast, familiar, and responsive user experience.[12]

New for 2020:

- Added Firefox and Edge browsers
- UWP/Ingress support for Office and Skype apps
- Auto add option for Trusted Sites
- Application improvements including Radio Button modifications
- Data collection on uninstall
- New support for Windows 10 IoT Enterprise 2016 & 2019 LTSC

HP Sure Sense

With an increasing risk of AI being used in malware attacks, Sure Sense is the HP solution that uses Deep Learning AI with malware protection capabilities that are light years ahead. HP Sure Sense detects zero day never-before-seen threats and protects your PC in real time. HP Sure Sense operates within the OS in concert with HP Sure Run to keep endpoints protected 24/7 whether or not the endpoint is online. The HP Sure Sense highly advanced Deep Learning algorithm scans every file on the endpoint and recognizes any new threats instinctively, even unknown zero-day attacks that traditional, signature-based antivirus software might miss. The HP Sure Sense instinctive malware recognition system needs to be updated only four times per year. HP Sure Sense ships on a select list of PCs and is also available as a Softpaq download so IT professionals can add it to the corporate image. HP Sure Sense protects against ransomware, exploits, spyware, and executable threats in real time—investigating remediating and containing the threat in less than a minute. HP Sure Sense delivers all this powerful protection with a remarkably light usage of 1% CPU system resources.[13]

HP Sure View Reflect

Even the best security software can't prevent visual hacking—unauthorized users viewing confidential information on an unguarded display. HP has a solution to prevent data being compromised visually. At the touch of a button, HP Sure View Reflect protects data by activating an integrated privacy screen that makes data visible only to the user sitting directly in front of it. HP Sure View Reflect allows users to work confidently from any location without fear of on-screen data being compromised by prying eyes, yet users maintain the flexibility to share their screen with clients and colleagues with a single quick keystroke, toggling the feature on and off. No matter where you use your PC—on an airplane, in a healthcare setting, or at any remote location—HP Sure View Reflect empowers employees with the power of privacy. With HP Sure View Reflect, your screen is your own and you can choose to share the view or not.[14]

HP Tamper Lock

Due to open source information sharing among attackers, detailed instructions on how to perform attacks are now readily available to would-be attackers. It's becoming much more common for attackers to physically open a PC chassis and hack into components to remove logon passwords, modify traffic, or detect keystrokes. HP Tamper Lock detects when the PC chassis has been opened or tampered with, then generates a request for the HP Sure Admin BIOS password to be entered in order to boot the PC.[15]

Conclusion

As the creator of the world's most secure PCs, HP takes Business PC Security seriously. HP has engineered a robust suite of security tools that work synergistically to relentlessly protect your endpoint assets and your data, so you can focus on your business.

Learn more about these HP Security Solutions in the HP Security Center online.

1. HP Proactive Security System requirements for HP Proactive Security are: multi-vendor client devices running Windows 10 1703 or later with a minimum of 8 GB memory and 6 GB free hard drive space to install the software client. HP Proactive Security requires HP TechPulse, which is included in any HP DaaS or HP Proactive Management plan.
2. HP Essential Security requires Windows 10, includes various HP Sure security features and is available on HP Elite and Workstation products. See product details for included security features.
3. HP BIOSphere Gen5 is available on select HP Pro and Elite PCs. Features may vary depending on the platform and configurations.
4. HP Sure Start Gen6 is available on select HP PCs.
5. HP Sure Run Gen3 is available on select Windows 10 based HP Pro, Elite and Workstation PCs with select Intel® or AMD processors.
6. HP Sure Recover Gen3 is available on select HP PCs and requires an open network connection. Not available on platforms with multiple internal storage drives. You must back up important files, data, photos, videos, etc. before using HP Sure Recover to avoid loss of data.
7. HP Sure Recover Gen3 with Embedded Reimaging is an optional feature which must be configured at purchase. Not available on platforms with multiple internal storage drives. You must back up important files, data, photos, videos, etc. before use to avoid loss of data. HP Sure Recover with Embedded Reimaging (Gen1) does not support platforms with Intel® Optane™.
8. HP Client Security Manager Gen6 requires Windows and is available on the select HP Elite and Pro PCs.
9. HP Sure Admin requires Windows 10, HP BIOS, HP Manageability Integration Kit from http://www.hp.com/go/clientmanagement and HP Sure Admin Local Access Authenticator smartphone app from the Android or Apple store.
10. HP Multi Factor Authentication Gen3 is available on select HP PCs and requires Intel® Core™ processor, Intel® integrated graphics, and Intel® WLAN. Three authentication factors require Intel® vPro™. (If facial recognition is mentioned: Authentication factors may require optional hardware.
11. HP Secure Erase - For the methods outlined in the National Institute of Standards and Technology Special Publication 800-88 "Clear" sanitation method. HP Secure Erase does not support platforms with Intel® Optane™.
12. HP Sure Click Pro requires Windows 10 and Microsoft Internet Explorer, Google Chrome, or Chromium are supported. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed.
13. HP Sure Sense requires Windows 10. See product specifications for availability.
14. HP Sure View Reflect integrated privacy screen is an optional feature that must be configured at purchase and is designed to function in landscape orientation.
15. HP Tamper Lock is an optional feature that must be configured at the factory and requires a supervisor password be established prior to use.

Sign up for updates: hp.com/go/getupdated

4AA7-7264ENW, June 2020