Brochure

Multilayered protection to keep business moving

HP Client Security

Repel evolving threats—while maintaining productivity

Today’s information technology (IT) threats strike businesses from many places and from all angles. To keep business running smoothly, security must cover every entry point with multiple layers of protection—helping ensure perpetrators can’t break in, and accidental breaches don’t happen. To stay competitive, businesses need security solutions that are simple to deploy, manage, and customize, while also easy for employees to use.

HP Client Security

HP Client Security[1] offers a broad selection of powerful security solutions designed to outpace today’s cyber threats to your data, devices, and identity. The multilayered security you need is built right into HP business PCs and includes strong safeguards at the BIOS, hardware, and software levels. HP Client Security lets you choose the protections that matter most for defending your IT environment and maintaining a simple user experience for your employees—giving your business the peace of mind to stay protected and productive.

Defend your data

Data is at the core of your business, and it can be a costly nightmare if it falls into the wrong hands. HP Client Security helps protect data in multiple ways, while still giving authorized users simple and secure access. You can protect business data even when it is lost or stolen.

BIOS-level protection

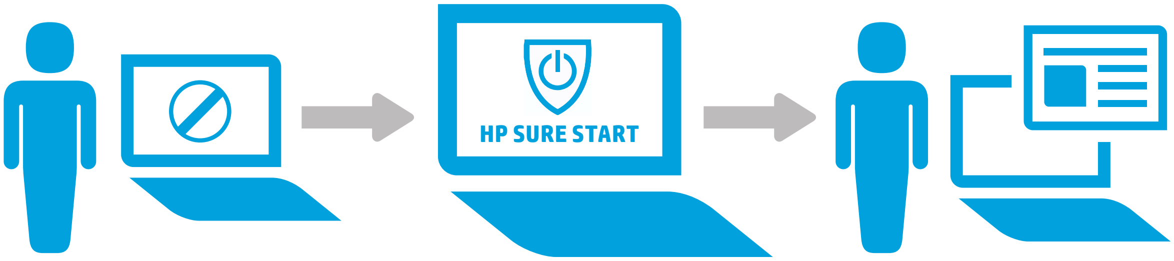
- HP DriveLock stops unauthorized users by preventing PC hard drives from running unless a password has been entered. Or choose HP Automatic DriveLock[2] to enable fast, secure access without a password.
- Help prevent confidential data leaks—use HP Disk Sanitizer to permanently erase the hard drive on PCs prior to retiring or redeploying them.[3]

Software-level protection

- Prevent unauthorized access to hard drive information—even if drives are removed. HP Drive Encryption, which is certified under Federal Information Processing Standard (FIPS) Publication 140-2, can encode all data and control access.[4]
- Keep your data out of the wrong hands. HP File Sanitizer helps you permanently delete files, folders, and identity information from PCs.[5]

Hardware-level protection

- Protect information like keys, passwords, and digital certificates stored on PCs from external software attacks and physical threats. HP uses the same Common Criteria EAL4+-certified Infineon Trusted Platform Module 1.2 that is trusted by high-security businesses like banks, governments, and insurance agencies.
- Grant users quick, safe access to their data. Self-encrypting hard drives on HP PCs deliver faster encryption performance than software-only encryption solutions.[6]
- Confidently prepare hard drives from your HP PCs for disposal or redeployment. HP Secure Erase rewrites and permanently destroys data on all hard drives, including solid-state drives—so your confidential information can’t be recovered.[7]



If a virus corrupts the BIOS on a sales representative's notebook—preventing it from booting—HP Sure Start replaces the BIOS boot block from a separate memory within seconds. The sales representative can now start his notebook and get back to work.

See how a PC's corrupted BIOS gets replaced in seconds

Problem: A stock trader's PC is attacked during the night, and the BIOS data is corrupted. He needs to boot up his PC that morning to set up a crucial client transaction that is due by noon.

Solution: HP Sure Start, the industry's first self-healing BIOS, quickly restores the PC's BIOS boot block from a clean copy that is held in a separate memory. The stock trader can get back to work with minimal downtime—and meet his trading deadline.

Safeguard your devices

Businesses need to stay a step ahead of cyber criminals, PC thieves, and unauthorized users. They also need to ensure employees make intelligent security choices guided by best practices. With HP Client Security, which includes powerful BIOS-level safeguards in HP BIOSphere, you can control everything from startup and login access to physical security for your fleet to help squash threats quickly.

BIOS-level protection

- Shield PCs against attacks. HP BIOS Protection—developed to National Institute of Standards and Technology 800-147 guidelines—helps prevent malware from updating the BIOS. If malicious code defeats the protections, HP BIOS Protection restores the BIOS to a known good state.[8]
- Rely on the industry's first and only self-healing BIOS solution. HP Sure Start can quickly restore the PC's BIOS boot block from a clean copy held in a separate memory—minimizing downtime from virus and malware attacks.[9]
- Protect your Absolute® Software Services. The built-in Absolute Persistence Module helps ensure Absolute Software Services stay active.[10]
- Master Boot Record Security helps protect essential Master Boot Record data—and recovers it after corruption incidents—reducing downtime in your office.[11]

Software-level protection

- Help protect data while simplifying access. HP Device Access Manager helps you control access to ports and storage devices, while Just in Time Authentication gives users fast, credential-protected permission to use removable storage devices for a limited time.
- Reach out to stop PC thieves from almost anywhere. Absolute Data Protect helps you locate, lock, and erase PC data remotely.[10]
- Safeguard your PCs from viruses, spyware, and other malicious software. HP PCs include a full version of Microsoft® Security Essentials[12] or Microsoft Windows® Defender to provide real-time protection.

Hardware-level protection

- Don't let someone swipe your notebook off your desk or yank hardware components out of your desktop PC. Help stifle thieves by using physical device security tools such as chassis security kits, locks, cables, and sensors.

HP SpareKey

If an employee forgets his logon password, HP SpareKey allows him to quickly reset it by answering customized security questions.

See how a lost password is quickly reset and PC access restored

Problem: A financial advisor needs quick access to client information between appointments, but he forgot his password. He can't log on to his PC without his Microsoft Windows password, and his next client will arrive soon.

Solution: The financial advisor turns on his PC and accesses his HP SpareKey menu during startup. He quickly answers a short series of security questions that he created during the initial setup of his PC. Completing the questions unlocks his PC and lets him reset his Windows password, allowing him to serve his next client without calling for IT help.

Protect your identity information

Protecting employee and customer identities is essential to the health and productivity of your business. From BIOS-based passwords to credential management, HP Client Security offers safeguards to protect passwords and give authorized users the right level of access.

BIOS-level protection

- Stop threats before they start with built-in, pre-boot security features such as BIOS security, port control, and boot options.
- Let employees get to work quickly and securely. Enhanced pre-boot security along with Power-On Authentication requires users to log on to their PC with their Microsoft Windows password or fingerprint before any software can run.[13]

Software-level protection

- Restrict PC access to only the right users by setting up login policies, including multi-factor authentication requirements, using HP Credential Manager.
- Guard against hackers while promoting efficient user access. With HP Password Manager, employees can access websites and applications using one convenient login process—without having to remember unique usernames and passwords for each one.[14]
- Let authorized users enter just one password—One Step Logon grants employees fast PC desktop access, using their Windows password, by automatically logging them on through Power-On Authentication, HP Drive Encryption, and Windows.[15]
- Reduce downtime due to lost passwords. HP SpareKey supports custom security questions for fast, protected access to your PC and the Windows password reset process.[16]

Hardware-level protection

- Choose Smart Card Reader or Fingerprint Sensor technology to help strengthen identity protection beyond just a password, while still giving employees fast access to their PCs.

Why choose HP?

HP Client Security solutions provide a broad range of rock-solid protection for your data, devices, and identity—so you can defend your business against dangerous cybercrimes. Contact your local HP representative to get started.

To learn more, visit
hp.com/go/clientsecurity

1 Requires Microsoft® Windows® 7, Windows 8, or Windows 8.1.

2 Automatic DriveLock will work on another HP business PC when the BIOS admin passwords are the same. Requires user set up.

3 For the use cases outlined in the Department of Defense (DoD) 5220.22-M Supplement. Traditional hard drives supported. Requires HP Disk Sanitizer, External Edition for Business Desktops, from hp.com.

4 Requires Microsoft Windows. Data is protected prior to HP Drive Encryption login. Turning the PC off or into hibernate logs out of HP Drive Encryption and prevents data access.

5 For the use cases outlined in the DoD 5220.22-M Supplement.

6 Self-encrypting hard drives are not supported if the encryption personal identification number (PIN) is enabled.

7 For the methods outlined in the National Institute of Standards and Technology Special Publication 800-88. Supported on HP ElitePad 900 G1 with BIOS version F.03 and higher.

8 Requires an HP Tools partition for automatic recovery. May require a manual recovery step if all copies of BIOS are compromised or deleted. Feature not supported on HP ElitePads. HP Business Desktops introduced prior to 2013 do not support this HP BIOS Protection auto-recovery feature.

9 Available only on HP 800 series EliteBooks and HP ZBooks.

10 Absolute® agent is shipped turned off, and will be activated when customers activate a purchased subscription. Subscriptions can be purchased for terms ranging multiple years. Service is limited, check with Absolute for availability outside the United States. The Absolute Recovery Guarantee is a limited warranty. Certain conditions apply. For full details, visit absolute.com/en/about/legal/agreements/computrace-agreement. Data Delete is an optional service provided by Absolute Software. If used, the Absolute Recovery Guarantee is null and void. In order to use the Data Delete service, customers must first sign a pre-authorization agreement and either obtain a PIN or purchase one or more RSA SecurID tokens from Absolute Software.

11 Master Boot Record is only applicable to Microsoft Windows 7 and earlier versions.

12 Microsoft Windows 7 only. Internet access required. Opt-in is required to receive updates from Microsoft Security Essentials.

13 HP Business Notebooks only support fingerprint authentication.

14 Requires Microsoft Internet Explorer®. Some websites and applications may not be supported. Supported in Windows 8 desktop mode.

15 HP Business Desktops do not support One Step Logon with BIOS Power-On Authentication. One Step Logon does not support Power-On Authentication with the Trusted Platform Module. One Step Logon is disabled in Windows when software Secure Attention Sequence is disabled by Windows group policies.

16 Requires initial user setup. HP Business Desktops and ElitePads do not support HP SpareKey in BIOS.

Sign up for updates
hp.com/go/getupdated

Share with colleagues

Rate this document