



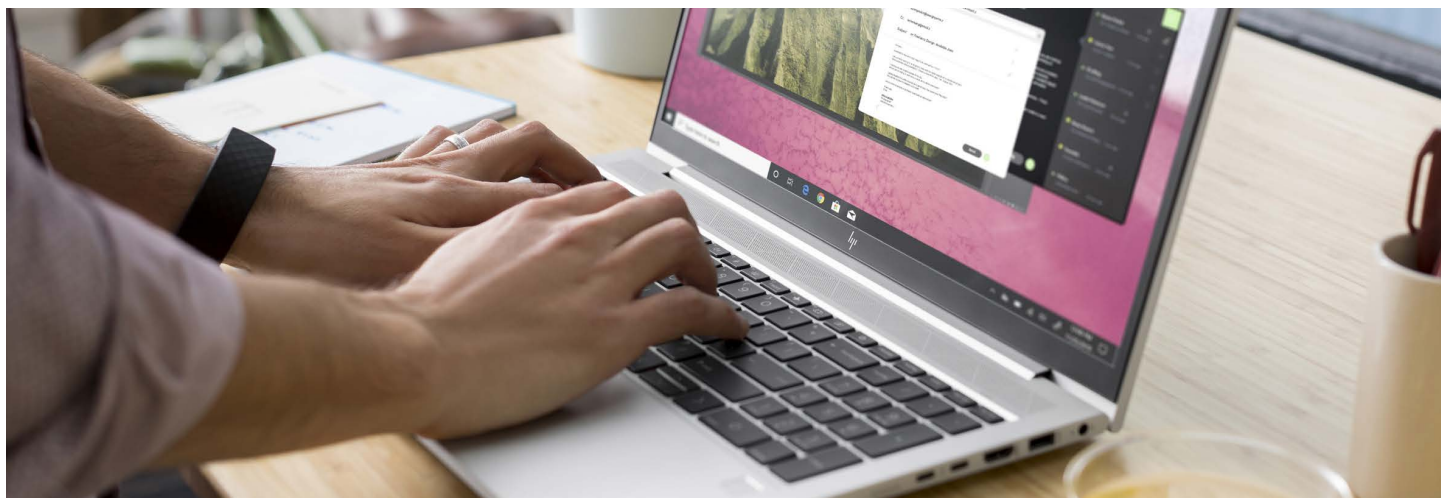
HP BIOSPHERE DER 6. GENERATION

INFOBLATT



HP WOLF SECURITY

Angriffe auf das BIOS sind häufig schwer zu erkennen. Glücklicherweise automatisiert das HP BIOSphere-Ökosystem den Schutz des BIOS und ermöglicht eine stabile PC-Verwaltbarkeit.



WARUM IST DER BIOS-SCHUTZ SO WICHTIG?

Ein ungesichertes BIOS kann Hackern einen gefährlichen Zugriff ermöglichen, und die Zahl der Cyberangriffe auf das BIOS nimmt zu. Hacker erhalten häufig über Phishing-Angriffe Zugriff auf das BIOS.

Physische Angreifer können ein System schnell zerlegen und sich direkt mit dem nichtflüchtigen Speicher auf der Platine verbinden, um Malware einzuschleusen. Malware kann auch über ungesicherte Ports eingeschleust werden.

Angriffe auf BIOS-Ebene sind nur sehr schwer zu erkennen, weil sie unterhalb der Betriebssystemebene ansetzen und das Gerät kontrollieren. Entsprechende Schadsoftware lässt sich auch nicht mithilfe von Antivirensoftware entfernen oder verändern. Eine auf das BIOS abzielende Malware kann kontinuierlich Daten senden und besitzt die Fähigkeit, sich nach einem Lösversuch durch die Sicherheitsfunktionen des Netzwerks selbstständig neu zu installieren. Ein kompromittiertes BIOS kann unentdeckt andere Sicherheitsmaßnahmen auf dem PC deaktivieren und sogar ein Löschen der Festplatte und eine Neuinstallation des Betriebssystems überstehen.

HP BIOSPHERE SCHÜTZT IHREN PC

HP BIOSphere greift auf mehr als zehn Jahre Erfahrung als führende BIOS-Sicherheitslösung zurück und stellt ein Verteidigungssystem für den Schutz von PCs dar. Hierzu gehören automatisierte Schutzmechanismen, anpassbare Sicherheitsmaßnahmen und einfache Verwaltbarkeit zum Schutz vor Angriffen, ohne die Mitarbeiterproduktivität zu unterbrechen.¹

HP BIOSphere kann zum Schutz vor einer Vielzahl von Angriffen oder Beschädigungen beitragen, einschließlich Angriffen, die auf den Master Boot Record (MBR) und die GUID Partition Table (GPT) abzielen. Außerdem schützt es vor Angriffen, die versuchen, über nicht autorisierte Wireless-Brücken einzudringen. Darüber hinaus bietet es Schutz vor neuen Arten von Malware, die derzeit noch unbekannt sind und auch auf das BIOS abzielen. Zudem kann es mit Funktionen wie BIOS-Kennwörtern, Portsteuerelementen und HP Secure Erase vor physischen Angriffen auf das Gerät schützen.

Seit 2015 bietet HP BIOSphere ein gemeinsames BIOS-Erlebnis für HP Notebooks und Desktops, mit einem ähnlichen Look and Feel für das (F10) Setup-Menü, mehr gemeinsamen WMI-Strings und mehr gemeinsamen Funktionen.

SCHÜTZEN SIE IHR BIOS



**AUTOMATISIER-
TER SCHUTZ**



**ANPASSBARE
SCHUTZMECHA-
NISMEN**



**EINFACHE
VERWALTBAR-
KEIT**



AUTOMATISIERTER SCHUTZ

HARDWARE-ROOT OF TRUST

Bei jedem Systemstart sorgen HP Pro und Elite PCs dafür, dass ein authentisches BIOS vorhanden ist, bevor die CPU mit der Codeausführung beginnt.¹ (Bei PCs, die außerdem HP Sure Start² enthalten, kann sich ein beschädigtes BIOS automatisch selbst heilen.)

SECURE BOOT

Bei der Herstellung von HP Business-PCs erstellt das Unified Extensible Firmware Interface (UEFI) eine Liste von Schlüsseln, die vertrauenswürdige Hardware, Firmware und Betriebssystem-Loader-Code identifizieren. Außerdem wird eine Liste von Schlüsseln angelegt, um bekannte Malware zu identifizieren. Secure Boot nutzt diese Schlüssel, um potenzielle Bedrohungen zu erkennen und abzuwehren, bevor sie den PC angreifen oder infizieren können. Secure Boot kann beispielsweise verhindern, dass PCs von illegal kopierten CDs oder DVDs starten, die den Computer beschädigen könnten. Secure Boot sperrt keine gültigen Wiederherstellungsdatenträger oder Windows®-Datenträger.

SCHUTZ VON WICHTIGER FIRMWARE

HP BIOSphere der 6. Generation orientiert sich an NIST 800-147 und ISO/IEC 19678:2015, um sicherzustellen, dass das BIOS nur authentische Updates von HP erhält. Weitere wichtige Sicherheitsstandards, die es implementiert, sind der Entwurf von NIST 800-155, UEFI Secure Boot und Trusted Computing Group.

ERFÜLLUNG VON SICHERHEITSNORMEN

Elemente wie MBR oder GPT sind vor Beschädigungen oder Löschungen geschützt, die einen Systemstart des PCs verhindern könnten.

EINFACHE BIOS-UPDATES

HP BIOSphere der 6. Generation kann BIOS- und Intel® ME-Updates über Windows Update empfangen, was so einfach ist wie ein Standard-Treiber-Update.³ Automatische Updates können sogar über das Netzwerk geplant werden, mit einstellbaren Tagen und Zeiten.



ANPASSBARE SCHUTZMASSNAHMEN VOR PHYSISCHEN ANGRIFFEN

SICHERHEIT VOR DEM SYSTEMSTART

Mit-Sicherheitsfunktionen wie Authentifizierung beim Systemstart und HP DriveLock kann verhindert werden, dass unbefugte Benutzer auf Ihre Geräte zugreifen können.

PORT-STEUERUNGEN

Schützt Ports vor bösartigen USB-Laufwerken oder Datendiebstahl. Mit HP Biosphere der 6. Generation können Benutzer einzelne Ports aktivieren/deaktivieren und die Möglichkeit zum Starten über USB blockieren. (Viele Geräte verwenden jetzt USB-C®, um Benutzergeräte aufzuladen. Wenn diese Option deaktiviert ist, wird USB-C® weiterhin genutzt und kann zur Stromversorgung des PCs verwendet werden. Nur bei bestimmten HP PCs verfügbar.)

SECURE ERASE

Dauerhaftes Löschen von Daten auf Festplatten oder Solid-State-Laufwerken (SSD), um Datendiebstahl zu verhindern, wenn alte Geräte entsorgt oder wiederverwendet werden.⁴



FLEXIBLE UND ANPASSUNGSFÄHIGE VERWALTBARKEIT

REPLIZIERTE INSTALLATION

Die replizierte Installation ermöglicht kleinen Unternehmen eine einfache Speicherung von BIOS-Einstellungen in einer Datei (z. B. einem USB-Stick) und das Klonen von Konfigurationen auf anderen Computern.

REMOTE-VERWALTUNG DES BIOS

Unternehmen mit verwalteter IT können mit dem HP BIOS-Konfigurationsprogramm die BIOS-Einstellungen ihrer PC-Flotte in wenigen Minuten zentral konfigurieren und aktualisieren.⁵ Dieses skriptgesteuerte Tool bietet Administratoren die Möglichkeit, BIOS-Einstellungen auf PCs aus der Ferne zu verwalten.

- Lesen der verfügbaren BIOS-Einstellungen und ihrer Werte von einem unterstützten Desktop-, Workstation- oder Notebook-Computer aus
- Festlegen oder Zurücksetzen des Setup-Kennworts auf einem unterstützten Desktop-, Workstation- oder Notebook-Computer
- Replizieren von BIOS-Einstellungen auf mehreren Client-Computern

HP BIOSphere Einstellungen und Kennwörter können auch per Fernzugriff mit dem HP Manageability Integration Kit (MIK) für Microsoft® System Center Configuration Manager (SCCM) verwaltet werden. Die BIOS-Konfigurationsschnittstelle des MIK ermöglicht es dem IT-Administrator, BIOS-Einstellungsrichtlinien für Client-Computer festzulegen und bereitzustellen.

HP BIOSphere der 6. Generation

¹Der Funktionsumfang von HP BIOSphere der 6. Generation kann je nach Plattform und Konfiguration variieren.

²HP Sure Start der 6. Generation ist für ausgewählte HP PCs verfügbar.

³BIOS-Aktualisierungen über Windows Update sind auf allen HP Elite- und HP Pro-PCs mit Intel®- oder AMD®-Prozessoren der 6. Generation oder höher verfügbar. Intel® ME-Aktualisierungen über Windows Update sind auf HP Elite- und HP Pro-PCs mit Intel®-Prozessoren der 11. Generation verfügbar.

⁴Für Methoden vorgesehen, die in der „Clear“-Löschmethode in der National Institute of Standards and Technology Special Publication 800-88 beschrieben sind. Plattformen mit Intel® Optane™ werden von HP Secure Erase nicht unterstützt.

⁵Das HP BIOS-Konfigurationsdienstprogramm kann hier heruntergeladen werden: https://ftp.hp.com/pub/caps-softpaq/cmit/HP_BCU.html.



HP WOLF SECURITY

© Copyright 2021 HP Development Company, L.P. Änderungen vorbehalten. Neben der gesetzlichen Gewährleistung gilt für HP Produkte und Dienstleistungen ausschließlich die Herstellergarantie, die in den Garantieerklärungen für die jeweiligen Produkte und Dienstleistungen explizit genannt wird. Aus den Informationen in diesem Dokument ergeben sich keinerlei zusätzliche Gewährleistungsansprüche. HP haftet nicht für technische bzw. redaktionelle Fehler oder fehlende Informationen.

4AA7-9151DEE, Juni 2021