

# HP Business PC Security

Jede PC Entscheidung ist eine Sicherheitsentscheidung.

## Fest verbaute Sicherheit

HP setzt auf hardwaregestützte, selbstheilende und verwaltbare Sicherheitsfunktionen. Diese Lösungen bieten Schutz, Angriffserkennung und Wiederherstellung und stärken somit nicht nur die Sicherheit Ihrer Geräte sondern auch die Sicherheit Ihres Unternehmens.

Verschaffen Sie sich einen Überblick über die innovativen und umfassenden Sicherheitslösungen der HP Business PCs und wie diese zu Ihrem Schutz beitragen können.



# Gemeinsam gegen zunehmende Bedrohungen

Die Bandbreite aktueller Bedrohungen hat sich in den letzten Jahren deutlich erweitert. Gleiches gilt jedoch auch für Innovationen und Entwicklungen rund um das Thema IT Sicherheitslösungen.

Mit dem **HP Endpoint Security Controller** liefert HP Geräte, die bereits beim Start mit hardwaregestützten und branchenführenden Sicherheitslösungen ausgestattet sind. Zusammen mit Windows 10 und den Intel® vPro™-Prozessoren ist damit den Geräten, Daten und der Identität nicht nur innerhalb des Betriebssystems Schutz geboten, sondern auch in allen über- und untergeordneten Prozessen.

Dank dieser hardwaregestützten Lösungen umfasst die HP Elite Familie die sichersten und verwaltungsfreundlichsten PCs der Welt.<sup>1</sup>



## Grundlegender Schutz

Wenn Sie Ihren PC hochfahren, startet immer zuerst das BIOS – noch vor dem Betriebssystem, der Firewall oder Ihrer Anti-Viren Software. Sollte das BIOS infiziert sein, lädt es die Malware bereits beim Boot-Prozess in das Betriebssystem. Und weil die Anti-Malware Software noch nicht aktiv ist, bleiben diese Angriffe auf das Betriebssystem unentdeckt. Durch die Infektion des BIOS erhält der Angreifer unbegrenzte Kontrolle über Ihren PC. Er kann ihn komplett lahmlegen, Ihre Anmeldedaten und Ihr geistiges Eigentum stehlen und Ransomware einschleusen.

**HP Sure Start** hilft solche Risiken zu vermeiden. Vier Schlüsselemente machen es so wirksam:

### 1. Selbstheilendes BIOS

Sobald das BIOS auf HP Elite PCs manipuliert wird, erkennt HP Sure Start dies automatisch und sendet eine Benachrichtigung. Anschließend stellt es das BIOS mit einer sauberen Kopie wieder her, die auf dem HP Endpoint Security Controller gespeichert ist. So erleiden Sie im Falle einer BIOS-Manipulation keine Ausfallzeiten - Ihr BIOS ist selbstheilend und Ihr Gerät startet immer mit einem echten HP BIOS.

### 2. Runtime BIOS-Intrusion Detection

Erkennt BIOS-Angriffe im Runtime-Speicher (SMM) während das Betriebssystem läuft, erstellt einen Event-Log Eintrag und stellt ein sauberes BIOS im Rahmen eines Neustarts wieder her.

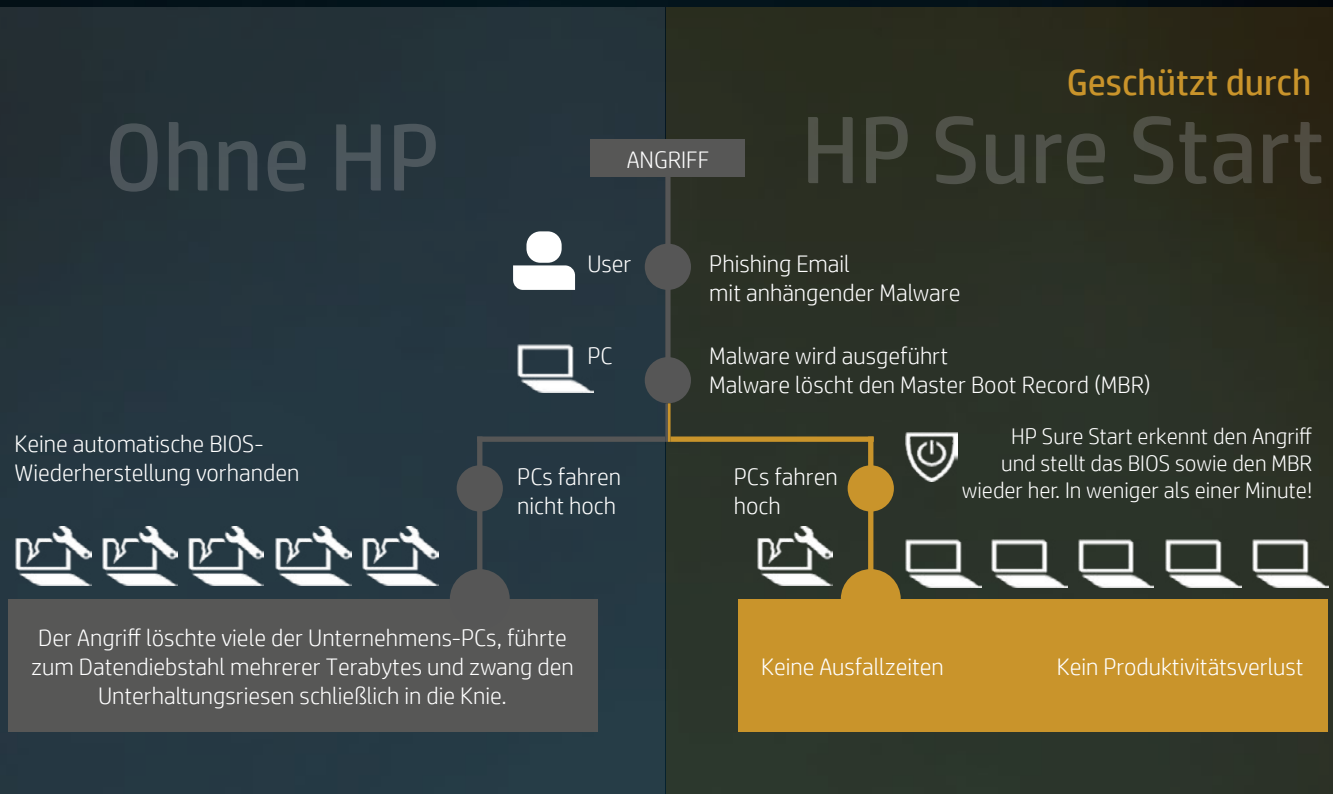
### 3. BIOS-Konfiguration und Richtlinien-Schutz

Schützt die BIOS-Einstellungen, Richtlinien und Daten. Es besteht keine Notwendigkeit, die benutzerdefinierten BIOS-Einstellungen im Falle einer Manipulation erneut einzuspielen.

### 4. Microsoft® SCCM Integration

Stärkerer BIOS-Schutz durch bessere Verwaltbarkeit in Zusammenarbeit mit Microsoft. Über das HP Manageability Integration Kit (MIK) Plug-in ist HP Sure Start mit Microsoft SCCM verwaltbar. Aktivierung und Einstellungen können so aus der Ferne eingerichtet und BIOS-Manipulationen überwacht werden.

# Ein Szenario aus dem echten Leben



## Nonstop-Schutz

Eine Vielzahl von Software-Prozessen und Anwendungen - von Antiviren- und Firewall-Software bis zu kryptografischen Diensten - schützt Ihren PC während der Arbeit. Diese Prozesse bewahren Ihren PC vor Malware, sichern Ihre Daten, und halten unbefugte Zugriffe ab. Malware versucht diese Verteidigungsmaßnahmen häufig komplett auszuschalten.

**HP Sure Run<sup>3</sup>** vereitelt Angriffe, indem es Ihre Verteidigung aufrecht erhält. Von seiner sicheren, hardwaregestützten Warte aus überwacht es wichtige Sicherheitsprozesse und alarmiert den Benutzer bei Änderungen oder startet sie automatisch neu, wenn diese deaktiviert werden.



## Autonomie im Ernstfall

Unabhängig davon ob Sie einen Cyberangriff bemerken oder nicht, eine Neuinstallation des Betriebssystems ist eine effektive Methode, um softwarebasierte Malware zu eliminieren. Leider kann dies zeitraubend sein und Produktivitätsverluste für Endbenutzer und IT-Abteilungen zur Folge haben.

**HP Sure Recover**<sup>4</sup> verwendet den HP Endpoint Security Controller und bietet Mitarbeitern die Möglichkeit das neueste Betriebssystemimage über das Netzwerk selbständig und schnell wieder aufzuspielen. Sie benötigen dafür also keine Unterstützung der IT-Abteilung. Bei Geräten, die von einem häufigeren Neuimaging profitieren, ermöglicht HP Sure Recover der IT-Abteilung diesen Prozess für eine gesamte Flotte nach einem festgelegten Zeitplan durchzuführen.

Und da HP Sure Recover über den HP Endpoint Security Controller aktiviert und über das BIOS ausgeführt wird, kann es einen PC auch von einer blanken Festplatte aus neu abbilden. Dies ermöglicht also auch dann eine automatische Wiederherstellung, wenn auf dem Gerät gar kein Betriebssystem mehr gefunden wird.

---

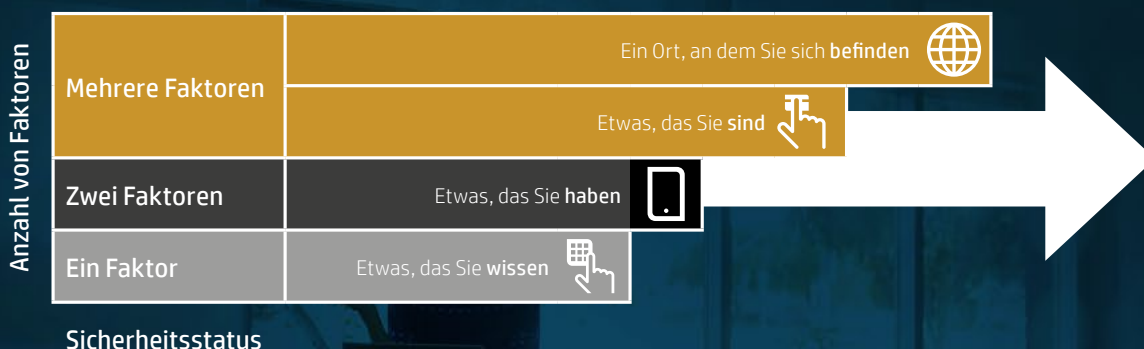
## Anfällige Passwörter

Passwörter bieten nicht mehr den Sicherheitsstandard, der effektiv vor heutigen Bedrohungen schützt.

Durch die Kombination von zwei oder mehr Authentifizierungsfaktoren steigern Sie die Sicherheit Ihres Logins um das Millionenfache.

HP nutzt **Intel® Authenticate™** angepasst, um die Authentifizierung mit Anmeldedaten und Richtlinien auf der Chip-Ebene zu optimieren. **HP Multi-Factor Authenticate**<sup>5</sup> verifiziert Identitäten mit bis zu drei von sieben hochsicheren Faktoren (z.B. PIN, Gesichtserkennung, Fingerabdruck).

### Was ist Multi-Faktor-Authentifizierung (MFA)?



## Browsen ohne Risiko

Es wird immer schwieriger, zwischen sicheren und unsicheren Webseiten zu unterscheiden. **HP Sure Click<sup>8</sup>** verlagert diese Aufgabe vom Endbenutzer auf den PC und schützt ihn und Ihre Daten vor Webseiten und PDF-Dateien, die mit Malware, Ransomware oder Viren infiziert sind. Hierbei werden jeder Browser-Tab und im Browser geöffnete PDF-Dateien auf der Hardware-Ebene isoliert – auch Mikro-Virtualisierung genannt. Dadurch kann Malware nicht auf den PC oder das Unternehmensnetz übergreifen.

---

## Schutz vor visuellem Hacking

Die tägliche Arbeit findet immer öfter im öffentlichen Raum statt: Wir arbeiten beim Warten auf den nächsten Flug oder entscheiden uns für einen Abstecker ins Café um die Ecke.

Vertrauliche Daten auf dem Notebook-Bildschirm sind anfällig und an diesen Orten visuellem Hacking ausgesetzt. **HP Sure View** – die weltweit einzige integrierte Blickschutztechnologie<sup>7</sup> – lässt Ihre Mitarbeiter sicherer im öffentlichen Raum arbeiten. Der Blickschutz setzt ein, wenn der Blickwinkel mehr als 45° von der Bildschirmmitte beträgt und lässt sich ganz einfach mit einem Tastendruck einschalten.



## Einfache Integration

Selbst das weltbeste Sicherheitskonzept hilft nichts, wenn es deaktiviert ist. Darum legt HP besonderen Wert auf die Verwaltbarkeit von Sicherheitsfunktionen. **Das HP Manageability Integration Kit (MIK)** wurde speziell für Microsoft System Center Configuration Manager (SCCM) entwickelt. Dieses Tool erspart es Unternehmen, zusätzliche Plug-ins für HP PCs zu entwickeln, wenn diese über Microsoft SCCM verwaltet werden.

IT-Manager sind so in der Lage, HP Sure Start, HP Sure View, HP Multi-Factor Authenticate, HP Sure Run, HP Sure Recover und viele weitere Lösungen für eine ganze Flotte an HP PCs fernzusteuern.

# Die EliteBook 800 Serie – eine sichere Entscheidung.

Surfen Sie unbesorgt im Internet und arbeiten Sie sicher im Büro oder unterwegs - mit der Gewissheit dass Ihr HP Elite PC über hardwaregestützte Sicherheit verfügt.



## HP SURE START

Schützt Ihren PC mit der hardwaregestützten automatischen Fehlerbehebung von HP Sure Start Gen4<sup>2</sup>, die das BIOS automatisch wiederherstellen kann.



## HP SURE RUN

Hält Ihre kritischen Anwendungen und Prozesse am Laufen, selbst wenn Malware versucht diese zu beenden - dank automatischer Fehlerbehebung.



## HP SURE RECOVER

Stellt das letzte Image Ihrer PCs über eine Netzwerkverbindung schnell und sicher wieder her.



## HP SURE CLICK

Schützen Sie Ihren PC vor Websites und PDF-Dateien im Browser, die mit Malware, Ransomware oder Viren infiziert sind.<sup>8</sup>



## HP SURE VIEW

Schützen Sie Ihren Bildschirm umgehend vor visuellem Hacking – integrierter Blickschutz von HP mit nur einem Tastendruck (optional).

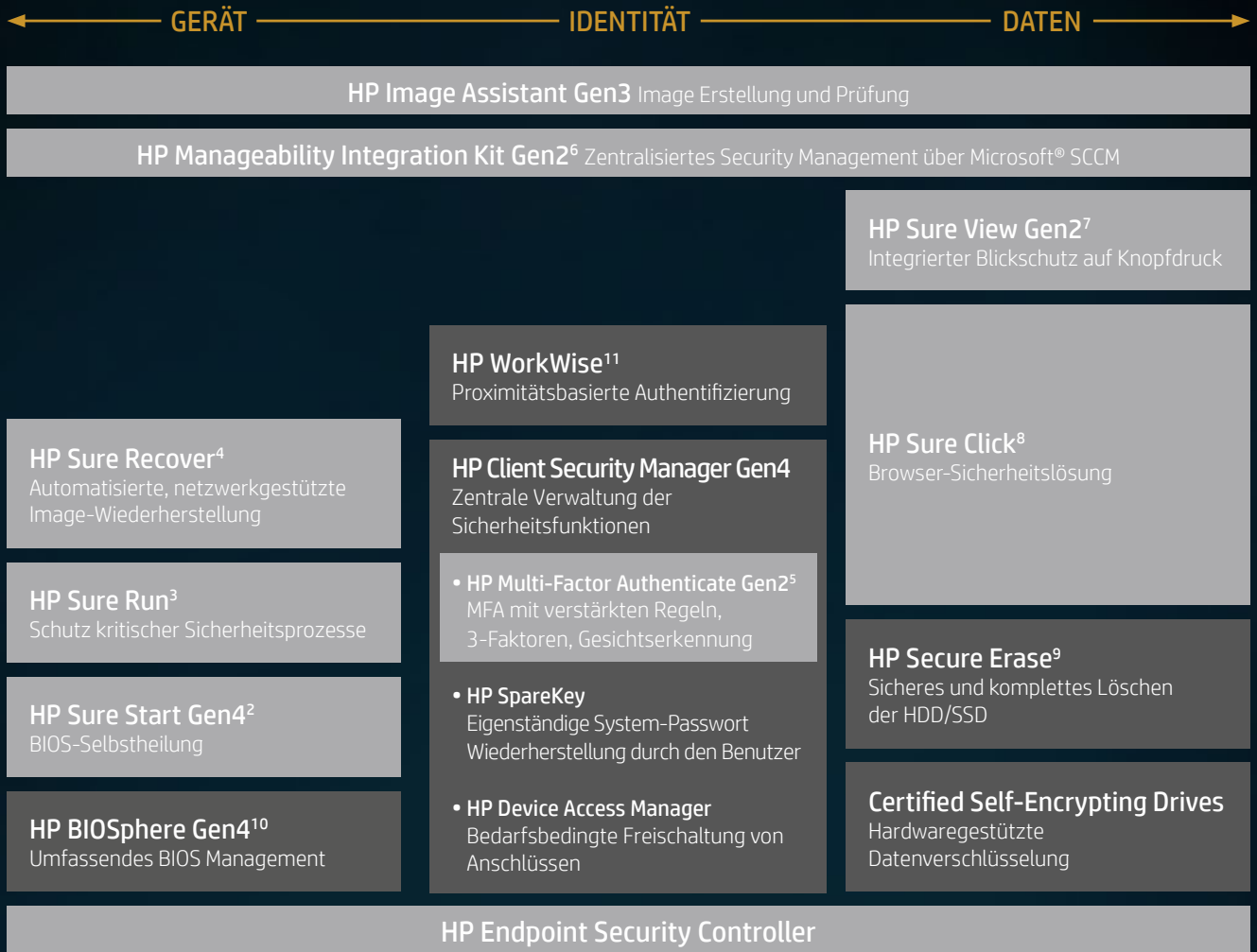


## HP MULTI-FACTOR AUTHENTICATE

Setzen Sie bis zu drei Authentifizierungsfaktoren ein, die durch Intel® Authenticate Technologie verstärkt werden.<sup>5</sup>



# Die wichtigsten HP Sicherheitslösungen auf einen Blick.



● Neue Features und Updates  
(HP Elite PCs mit Intel Prozessoren der 8. Generation)





Jede PC Entscheidung ist eine Sicherheitsentscheidung.

Kontaktieren Sie uns für weitere Informationen  
[hp.de/computersecurity](http://hp.de/computersecurity)

- 1 Basierend auf den einzigartigen und umfassenden Sicherheitsfunktionen von HP ohne zusätzliche Kosten und der Verwaltung durch das HP Manageability Integration Kit von sämtlichen Aspekten eines PCs, einschließlich Hardware, BIOS und Softwareverwaltung mithilfe des Microsoft System Center Configuration Manager unter Anbietern mit > 1 Million verkaufter Einheiten pro Jahr (Stand: November 2016) von HP Elite PCs mit Intel® Core®-Prozessoren ab der 7. Generation, integrierter Intel®-Grafikkarte und Intel®-WLAN. <http://h20195.www2.hp.com/v2/GetDocument.aspx?dorname=c05934743>
- 2 HP Sure Start Gen4 ist auf HP Elite- und HP Pro 600-Produkten mit Intel®- oder AMD®-Prozessoren ab der 8. Generation verfügbar.
- 3 HP Sure Run ist auf HP Elite-Produkten mit Intel®- oder AMD®-Prozessoren ab der 8. Generation verfügbar.
- 4 HP Sure Recover ist auf HP Elite-PCs mit Intel®- oder AMD®-Prozessoren der 8. Generation verfügbar und erfordert eine offene, kabelgebundene Netzwerkverbindung. Zur Vermeidung von Datenverlusten müssen Sie wichtige Dateien, Daten, Fotos, Videos usw. sichern, bevor Sie HP Sure Recover verwenden
- 5 HP Multi Factor Authenticate erfordert Intel® Core™-Prozessoren der 7. oder 8. Generation, integrierte Intel®-Grafikkarten und Intel®-WLAN. Für die Implementierung ist Microsoft System Center Configuration Manager erforderlich. Drei Authentifizierungsfaktoren erfordern Intel® vPro™. Authentifizierungsfaktoren können zusätzliche Hardware erfordern. HP Manageability Integration Kit kann unter <http://www.hp.com/go/clientmanagement> heruntergeladen werden.
- 6 Das HP Manageability Integration Kit kann unter <http://www.hp.com/go/clientmanagement> heruntergeladen werden.
- 7 Basierend auf derzeit im Markt verfügbaren PCs mit physisch eingebautem, hardware-basierendem Blickschutz, Stand August 2016. Der integrierte HP Sure View-Blickschutz ist eine optionale Funktion, die beim Kauf von ausgewählten HP Notebooks konfiguriert werden muss.
- 8 HP Sure Click ist auf ausgewählten HP Plattformen verfügbar und unterstützt Microsoft® Internet Explorer und Chromium™. Alle kompatiblen Plattformen finden Sie ab dem Zeitpunkt ihrer Verfügbarkeit unter <http://h20195.www2.hp.com/v2/GetDocument.aspx?dorname=4AA7-0922ENW> (PDF; 252KB).
- 9 HP Secure Erase | Gilt für in der Sonderveröffentlichung 800-88 des National Institute of Standards and Technology beschriebenen Methoden. Unterstützt auf Elite-Plattformen mit BIOS-Version F.03 oder höher
- 10 HP BIOSphere Gen4 benötigt Intel® oder AMD Prozessoren der 8. Generation.
- 11 HP Work Wise Smartphone-App ist als kostenloser Download bei Google Play verfügbar.
- 12 Quelle: InfoSecurity, F-Secure Labs, 2017
- 13 Quelle: Ponemon Institute, 2017 Cost of Cyber Crime Study, 2017

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Bluetooth is a trademark of its proprietor used by HP Inc. under license.

Intel, das Intel-Logo, Intel Core, Intel vPro, Core Inside and vPro Inside sind Marken der Intel Corporation oder ihrer Tochtergesellschaften in den USA und/oder anderen Ländern. USB Type-C™ und USB-C™ sind Marken des USB Implementers Forum.

