Technische Produktinformationen

# HP Sure Start

Automatischer Schutz auf BIOS-Stufe und dessen Reparatur

Mai 2018

# Inhaltsverzeichnis



# Einführung

HP Sure Start kann einen BIOS-Angriff oder eine Beschädigung automatisch erkennen, stoppen und das BIOS wiederherstellen, ohne dass die IT-Abteilung eingreifen muss und ohne Unterbrechung der Benutzerproduktivität. Jedes Mal, wenn der PC eingeschaltet wird, überprüft HP Sure Start automatisch die Integrität des BIOS-Codes, um sicherzustellen, dass der PC vor bösartigen Angriffen geschützt ist. Sobald der PC in Betrieb ist, überwacht die Runtime Intrusion Detection ständig den Speicher. Im Falle eines Angriffs kann sich der PC mit einer isolierten «goldenen Kopie» des BIOS in weniger als einer Minute selbst heilen.

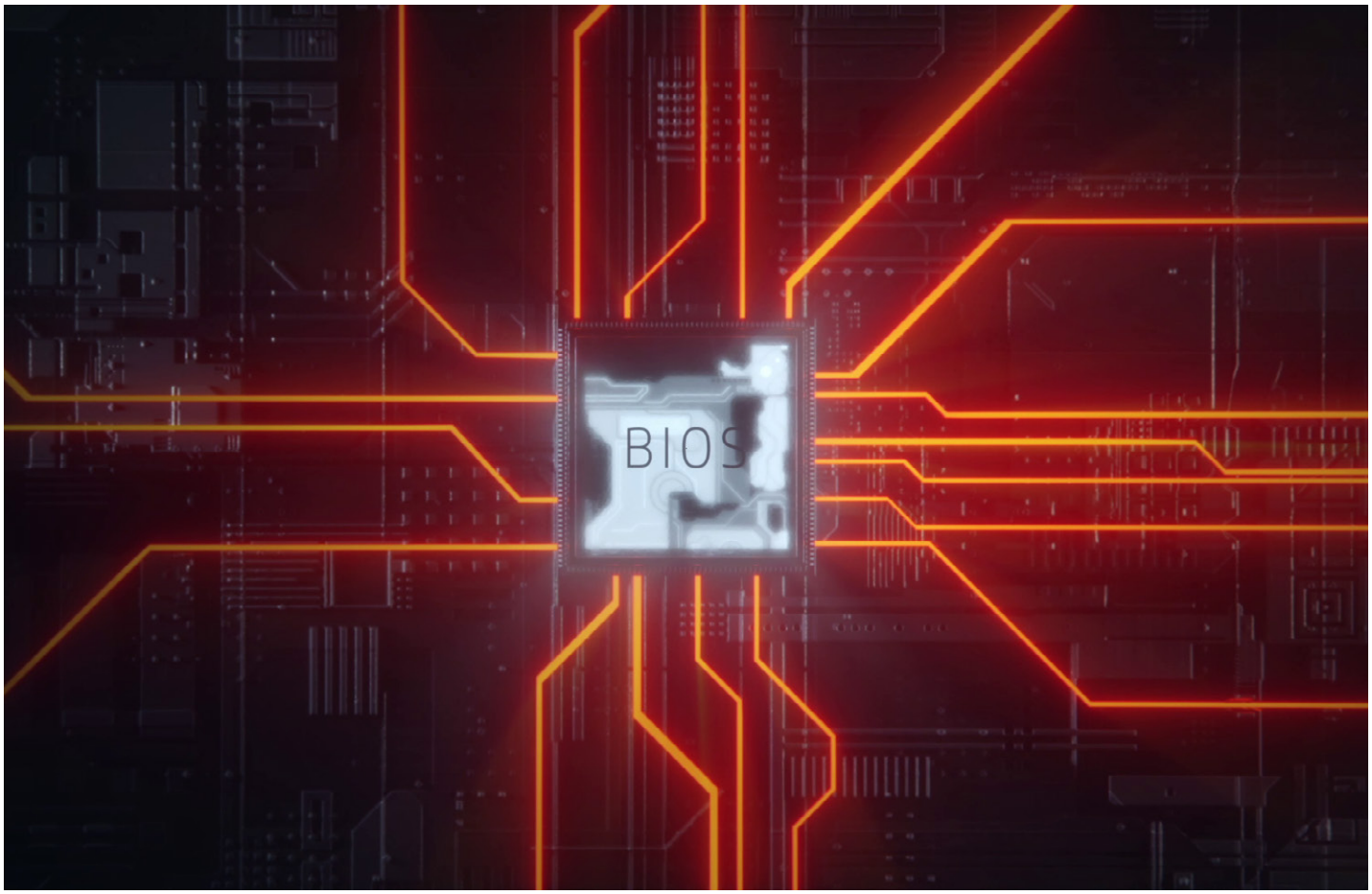
## Warum ist BIOS-Schutz wichtig?

**Mit zunehmender Vernetzung unserer Welt zielen Cyber-Angriffe immer häufiger auf die Firmware und Hardware von Client-Geräten. Tools und Techniken zum Angriff auf Firmware waren einst theoretisch und wenn, dann nur für staatliche Behörden erhältlich. Seitdem hat sich gezeigt, dass solche Tools und Techniken nicht nur existieren, sondern auch der Öffentlichkeit leicht zugänglich sind.**

Die Geräte-Firmware (oder BIOS) ist ein attraktives Ziel für Angreifer, da ein erfolgreiches Eindringen dem Angreifer potenzielle Attribute liefern könnte:

- Hartnäckigkeit: Die Firmware befindet sich in einem nichtflüchtigen Speicher auf der Platine und kann nicht einfach durch Löschen der Festplatte entfernt werden.
- Steuerung: Die Firmware wird auf der höchsten Berechtigungsebene ausgeführt – ausserhalb der Domain des Betriebssystems, was die Möglichkeit von betriebssystemunabhängiger Malware ermöglicht.
- Tarnung: Die Firmware belegt einen Speicherbereich, der für das Betriebssystem und die Systemsoftware völlig unzugänglich ist; da sie nicht von Antivirenprogrammen gescannt werden kann, werden Angriffe und Manipulationen möglicherweise nie erkannt.
- Schwierigkeit der Wiederherstellung: All diese Aspekte machen es extrem schwierig, sich von dieser Art von Infektion zu erholen, ohne auf ein Service-Ereignis zurückzugreifen, das einen Austausch der Systemplatine beinhaltet.

Die ideale Lösung zum Schutz von Geräten gegen diese Art von Angriffen ist ausgehend von der Hardware mithilfe der «Cyber-Widerstandsfähigkeit» konzipiert. Diese Grundsätze erkennen an, dass es äusserst schwierig, wenn nicht gar unmöglich ist, jeden möglichen Angriff vorherzusehen und zu verhindern. Die ideale Lösung bietet nicht nur einen verbesserten Schutz der Firmware, sondern beinhaltet auch eine hardwarebasierte Fähigkeit, einen erfolgreichen Angriff zu erkennen und sich davon zu erholen.



# HP Sure Start bietet hervorragenden Schutz der Firmware

**HP Sure Start ist der einzigartige und bahnbrechende Ansatz von HP, um HP PCs mit erweitertem Firmware-Schutz und hoher Ausfallsicherheit auszustatten. Es nutzt die Hardware-Erzwingung über den HP Endpoint Security Controller (HP ESC), um das BIOS zu schützen, das weit über den Industriestandard hinausgeht und sicherstellt, dass das System nur Original-BIOS von HP bootet. Wenn HP Sure Start Manipulationen am BIOS-, Firmware- oder Runtime System Management Mode (SMM)-BIOS-Code erkennt, kann es diese mit einer geschützten Sicherungskopie wiederherstellen.**

### Zusammenfassung der Funktionen von HP Sure Start

- Erzwingung der Authentizität und des Manipulationsschutzes der HP Kernplattform-Firmware – HP Endpoint Security Controller Hardware-Erzwingung des Systemstarts, sodass nur authentische und unveränderte HP Firmware und HP BIOS geladen wird
- Firmware-Zustandsüberwachung und -Compliance – Protokollierung von Firmware-Zustandsereignissen über einen isolierten HP Endpoint Security Controller; zeigt den Status der Plattform-Firmware zusammen mit allen Anomalien an, die auf Angriffe hindeuten könnten
- Selbstheilung – Automatische Reparatur von HP BIOS- und HP-Firmwarebeschädigungen mit Hilfe der isolierten HP Endpoint Security Controller-Sicherungskopie von HP-BIOS und HP-Firmware
- BIOS-Einstellungsschutz – Erweitert den HP Endpoint Security Controller-Schutz des BIOS-Codes um HP ESC-Backup und Integritätsprüfung aller vom Benutzer oder Administrator konfigurierten BIOS-Einstellungen
- Runtime Intrusion Detection – Laufende Überwachung des kritischen BIOS-Codes im Runtime Memory (SMM), während das Betriebssystem ausgeführt wird
- Sicherer Schutz von Boot-Keys – Deutlich verbesserter Schutz von Datenbanken und Schlüsseln, die vom BIOS gespeichert werden und für die Integrität der sicheren Boot-Funktion des Betriebssystems entscheidend sind, im Vergleich zur Standard-UEFI-BIOS-Implementierung
- Geschützter Speicher – HP Sure Start verwendet starke kryptografische Methoden, um BIOS-Einstellungen, Benutzer-Anmeldeinformationen und andere Einstellungen in der HP Endpoint Security Controller-Hardware zu speichern, um Integritätsschutz, Manipulationserkennung und vertraulichen Schutz für diese Daten zu bieten
- Intel® Management Engine-Firmware-Schutz – Verbesserter Schutz und verbesserte Wiederherstellung der Intel Management Engine-Firmware
- Verwaltbarkeit – Administratoren können HP Sure Start-Funktionen mit dem Manageability Integration Kit (MIK)-Plugin für Microsoft® System Center Configuration Manager (SCCM) verwalten

Eine Zusammenfassung der in jeder Generation von HP Sure Start hinzugefügten Funktionen finden Sie in Anhang A auf Seite 11.

### Sicherheitszertifizierung durch Dritte

Die HP Endpoint Security Controller-Hardware, die in HP Sure Start verwendet wird, wurde einer Sicherheitsbewertung durch Dritte unterzogen und zertifiziert, um die Hardware-Erzwingung sicherzustellen, damit nur autorisierte Firmware auf dem Ziel-PC gestartet werden kann.[1]

Die Gewissheit, dass eine Sicherheitslösung wie angegeben funktioniert, ist ein kritischer Bestandteil jeder Kaufentscheidung in Bezug auf Sicherheitsprodukte. Und weil wir unseren Ruf, hervorragende Qualität zu bieten, nicht gefährden möchten, hat HP das Innenleben des HP Endpoint Security Controllers einer Überprüfung und einem Test durch ein unabhängiges und akkreditiertes Labor unterzogen, um zu bestätigen, dass er nach öffentlich zugänglichen Kriterien, Methoden und Prozessen funktioniert.

### Cyber-robustes Design

HP Sure Start bietet nicht nur einen verbesserten BIOS-Schutz, der über den Industriestandard hinausgeht, sondern ist von der Hardware bis hin zur unübertroffenen Cyber-Robustheit der Plattform geschaffen, um eine BIOS-Wiederherstellung auch im Falle eines Eindringens oder eines destruktiven Angriffs zu gewährleisten. HP Business PCs mit HP Sure Start übertreffen die Widerstandsfähigkeitsrichtlinien des National Institute of Standards and Technology (NIST) für Platform Firmware (Special Publication 800-193), die eine der führenden Bemühungen des öffentlichen Sektors sind, die Anforderungen für cyber-robuste Plattformen zu formalisieren.

### HP Sure Start-unterstützte Modelle

HP hat Sure Start im Jahr 2014 eingeführt. Seitdem hat HP Sure Start verbessert und die Anzahl der Produkte, die es enthalten, erweitert. HP Sure Start wird für die gesamte 2018er Elite-Produktlinie angeboten, einschliesslich Tablets, Notebooks, Desktops und All-in-ones (AIOs). HP Sure Start Gen4 ist für HP Elite- und HP Pro 600-Produkte mit Intel- oder AMD®-Prozessoren der 8. Generation erhältlich.

# Übersicht über den Aufbau und die Fähigkeiten

HP Sure Start besteht hauptsächlich aus zwei Aufbaukomponenten:

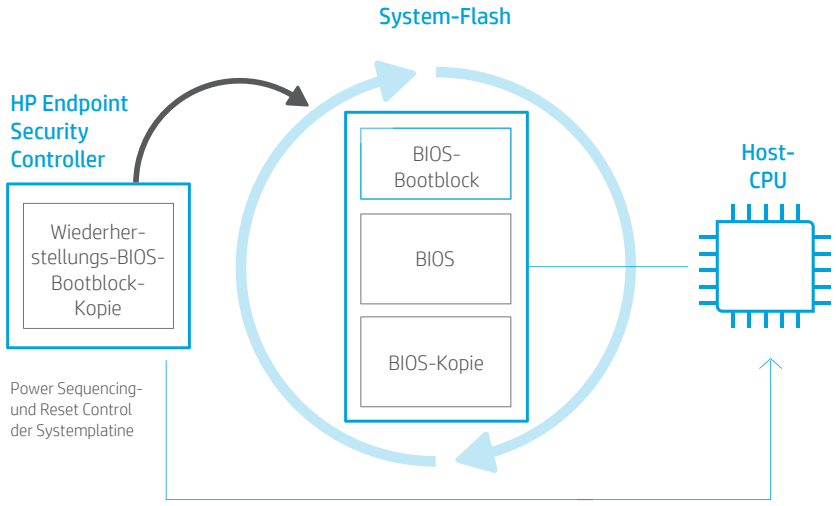
- **HP Endpoint Security Controller** unter HP Sure Start-Firmware
- **HP Sure Start BIOS** in Verbindung mit der HP Endpoint Security Controller-Hardware und -Firmware

## Firmware-Integritätsprüfung – das Kernstück von HP Sure Start

Der HP Endpoint Security Controller (HP ESC) ist das erste Gerät im System, das die Firmware ausführt, wenn das System hochgefahren wird. Die HP ESC-Aktivitäten umfassen unter anderem die Überwachung der System-Power-Taste und das Sequenzieren des Starts der Host-CPU-Ausführung, wenn der Benutzer die Power-Taste drückt.

Beim ersten Einschalten der Plattform (vor dem Einschalten des Systems) überprüft der HP ESC vor dem Laden und Ausführen des Codes, ob seine eigene Firmware authentischer HP-Code ist. Die HP ESC-Hardware verwendet branchenübliche, starke kryptografische Methoden, um die Integritätsprüfung durchzuführen. Die Methode verwendet einen öffentlichen 2048-Bit-HP-RSA-Schlüssel, der im internen permanenten schreibgeschützten Speicher enthalten ist. Daher ist der HP ESC der eingebaute hardwarebasierte Root of Trust (RoT) für die Plattform, mit dem die Firmware und das HP BIOS validiert werden, bevor sie ausgeführt werden. Diese Hardware Root of Trust schützt vor Firmware-Austauschangriffen, unabhängig von ihrer Bereitstellungsmethode, und dient als Grundlage für die Sicherheit der HP-Plattform.

**Abbildung 1.** Firmware-Integritätsprüfungsprozess.




Die Abbildung 1 illustriert den Firmware-Integritätsprüfungsprozess. Sobald sich der HP ESC authentifiziert und mit der Ausführung der HP Sure Start-Firmware beginnt, verwendet diese Firmware die gleichen starken kryptografischen Operationen, um die Integrität des System-Flash-BIOS-Bootblocks zu prüfen. Wenn ein einzelnes Bit ungültig ist, ersetzt der HP ESC den Inhalt des System-Flash durch eine eigene Kopie des HP BIOS-Bootblocks, der in einem isolierten nichtflüchtigen Speicher (NVM) für den HP ESC gespeichert ist.

Das HP Sure Start-Design stellt sicher, dass der gesamte Firmware- und BIOS-Code, der sowohl auf dem HP ESC als auch auf der Host-CPU läuft, der Code ist, den HP für das Gerät vorgesehen hat.

*Anmerkung: Die Integritätsprüfung des System-Flash-Bootblocks und die erforderliche Wiederherstellung durch den HP ESC erfolgen, während die Host-CPU ausgeschaltet ist. Aus der Perspektive der Benutzer erfolgt der gesamte Vorgang daher im ausgeschalteten oder im Ruhezustand.*

Der System-Flash-BIOS-Bootblock ist die Grundlage des HP-BIOS. Die HP ESC-Hardware stellt sicher, dass der BIOS-Bootblock der erste Code ist, den die CPU nach einem Neustart ausführt. Sobald der HP ESC feststellt, dass der BIOS-Bootblock authentischen HP-Code enthält, erlaubt er dem System das Booten, wie es normalerweise der Fall wäre.

Der HP ESC überprüft auch die Integrität des System-Flash-Bootblock-Codes jedes Mal, wenn das System ausgeschaltet oder in den Ruhezustand versetzt wird. Da die CPU in jedem dieser Zustände ausgeschaltet ist und die CPU daher den BIOS-Bootblock-Code erneut ausführen muss, um fortzufahren, ist es wichtig, die Integrität des BIOS-Bootblocks jedes Mal neu zu prüfen, um mögliche Manipulationen zu erkennen.

Zusätzlich überprüft HP Sure Start bei HP Intel-Modellen regelmässig (alle 15 Minuten) die Integrität des System-Flash-BIOS-Bootblocks, während das System läuft.[2]

## Eindeutige Rechnerdatenintegrität

HP ESC und BIOS arbeiten zusammen, um einen erweiterten Schutz der werkseitig konfigurierten kritischen Variablen zu bieten, die für jeden Rechner eindeutig sind und über die gesamte Lebensdauer einer bestimmten Plattform konstant sein sollen. Im Werk wird eine Sicherungskopie dieser Variablendaten im nichtflüchtigen Speicher von HP ESC gespeichert. Das Backup wird der HP Sure Start BIOS-Komponente schreibgeschützt zur Verfügung gestellt, um bei jedem Start eine Integritätsprüfung der Daten durchzuführen. Wenn sich eine Einstellung im freigegebenen Flash im Vergleich zu den Werkseinstellungen geändert hat, stellen die HP Sure Start BIOS-Komponenten die Daten im System Flash automatisch aus der vom HP ESC bereitgestellten Sicherungskopie wieder her.

## Deskriptorbereich

Bei HP Intel-Modellen schützt HP Sure Start den Deskriptorbereich des System-Flash. Einzigartig für die Intel-Architektur enthält der Deskriptorbereich kritische Konfigurationsparameter, die von der Intel Core™-Logik beim Neustart abgefragt und anschliessend zur Konfiguration der Core-Logik verwendet werden. Der Deskriptorbereich enthält auch Partitionierungsinformationen für den System-Flash, der von der Intel-Core-Logik verwendet wird, um festzustellen, wo sich die BIOS-Region im Flash befindet und wo ihre CPU Code zur Ausführung vom Neustart abruft. HP Sure Start überwacht die Integrität in diesem Bereich und stellt sie im Falle von Manipulationen oder Beschädigungen wieder her.

## Network Controller-Schutz

Darüber hinaus schützt HP Sure Start bei HP Intel-Modellen die im System-Flash enthaltenen Network Controller (NIC)-Einstellungen. Einige HP-Kunden haben Anwendungsfälle, die legitime Änderungen an den werkseitig konfigurierten NIC-Einstellungen erfordern. Daher verhindert HP Sure Start standardmässig keine Änderungen an den NIC-Einstellungen. Stattdessen bietet HP Sure Start eine Funktion, die, wenn sie aktiviert ist, den Benutzer warnt, dass die NIC-Einstellungen geändert wurden. Darüber hinaus bietet HP Sure Start eine Methode, um die NIC-Einstellungen auf die Werkseinstellungen zurückzusetzen. Zu den geschützten Einstellungen gehören die MAC-Adresse, die Pre-Boot Execution Environment (PXE)-Einstellungen und die Remote Initial Program Load (RPL). Diese Wiederherstellung ist über eine schreibgeschützte Sicherungskopie des HP ESC möglich.

## BIOS-Einstellungsschutz

Wie bereits beschrieben, überprüft HP Sure Start die Integrität und Authentizität des HP BIOS-Codes. Da dieser Code statisch ist, nachdem er von HP erstellt wurde, können digitale Signaturen verwendet werden, um beide Attribute des Codes zu bestätigen. Der dynamische und vom Benutzer konfigurierbare Charakter der BIOS-Einstellungen stellt jedoch zusätzliche Herausforderungen an den Schutz dieser Einstellungen. Digitale Signaturen können von HP nicht erzeugt und von der HP Sure Start ESC-Hardware zur Überprüfung dieser Einstellungen nicht verwendet werden.

Der HP Sure Start BIOS-Einstellungsschutz bietet die Möglichkeit, das System so zu konfigurieren, dass die HP ESC-Hardware zur Sicherung und Prüfung der Integrität aller vom Benutzer bevorzugten BIOS-Einstellungen verwendet wird.

Wenn diese Funktion auf der Plattform aktiviert ist, werden alle vom BIOS verwendeten Richtlinieneinstellungen gesichert, und bei jedem Start wird eine Integritätsprüfung durchgeführt, um sicherzustellen, dass keine der BIOS-Richtlinieneinstellungen geändert wurden. Wenn eine Änderung festgestellt wird, verwendet das System das Backup aus dem HP Sure Start geschützten Speicher, um automatisch zur benutzerdefinierten Einstellung zurückzukehren.

Der HP Sure Start BIOS-Einstellungsschutz erzeugt Ereignisse auf der HP Sure Start ESC-Hardware, wenn versucht wird, die BIOS-Einstellungen zu ändern. Das Ereignis wird im HP Sure Start Audit Log protokolliert und der lokale Benutzer erhält während des Bootvorgangs eine Benachrichtigung vom BIOS.

## HP Sure Start-geschützter Speicher

Geschützter Speicher, der auf der HP Endpoint Security Controller-Hardware basiert, bietet den höchsten Schutz für BIOS/Firmware-Daten und -Einstellungen, die durch HP Sure Start geschützt sind. HP Sure Start geschützter Speicher wurde entwickelt, um Vertraulichkeit, Integrität und Manipulationserkennung auch in physischen Angriffsszenarien zu gewährleisten, in denen ein Angreifer das System zerlegt und eine direkte Verbindung zum nichtflüchtigen Speichergerät auf der Platine herstellt.

### Datenintegrität

Die Integrität der dynamischen Daten, die von der Firmware im nichtflüchtigen Speicher gespeichert und zur Kontrolle des Zustands verschiedener Funktionen verwendet werden, ist entscheidend für die Sicherheitslage der gesamten Plattform. Zu den dynamischen Daten gehören alle BIOS-Einstellungen, die vom Endbenutzer oder Administrator des Geräts geändert werden können. Beispiele hierfür sind u. a. Boot-Optionen wie die sichere Boot-Funktion, das BIOS-Administrator-Passwort und zugehörige Richtlinien, die Zustandskontrolle des Trusted Platform Module und die HP Sure Start-Richtlinieneinstellungen.

Jeder erfolgreiche Angriff, der die bestehenden Zugriffsbeschränkungen umgeht, um unbefugte Änderungen an diesen Einstellungen zu verhindern, könnte die Sicherheit der Plattform gefährden. Ein Beispiel ist ein Szenario, in dem ein Angreifer eine nicht autorisierte Änderung am sicheren Boot-Zustand vornimmt, um ihn zu deaktivieren, ohne entdeckt zu werden. In diesem Szenario würde die Plattform das Rootkit des Angreifers booten, bevor das Betriebssystem startet, ohne dass der Benutzer es merkt.

Das Branchenstandard Unified Extensible Firmware Interface (UEFI) BIOS implementiert Zugriffsbeschränkungen, die unbefugte Änderungen an diesen Variablen verhindern sollen, und HP implementiert diese genau wie der Rest der PC-Branche.

Angesichts der Risiken, die eine Verletzung dieser Mechanismen für die Plattform darstellt, bietet HP Sure Start sekundäre Abwehrmassnahmen, die stärker sind als der Basisbranchenstandard.

BIOS-Einstellungen und andere dynamische Daten, die von der Firmware verwendet werden, um den durch HP Sure Start geschützten Zustand zu kontrollieren, werden im isolierten, nichtflüchtigen Speicher des HP Endpoint Security Controllers gespeichert, auf den die auf der Host-CPU laufende Software nicht direkt zugreifen kann.

Zusätzlich erstellt und fügt der HP ESC jedes Mal, wenn ein Datenelement in diesem nichtflüchtigen Speicher abgelegt wird, einzigartige Integritätsmessungen hinzu. Die Integritätsmessungen basieren auf einem starken kryptografischen Algorithmus (Hash-basierter Nachrichtenauthentifizierungscode unter Verwendung von SHA-256-Hashing), der auf einem im HP ESC enthaltenen Geheimnis basiert. Das Geheimnis ist eindeutig und einzigartig für jeden HP ESC, sodass jeder Controller eine einzigartige Integritätsmessung mit einem identischen Element erzeugt.

Wenn das Datenelement aus dem nichtflüchtigen Speicher zurückgelesen wird, berechnet der HP ESC die Integritätsmessung für dieses Datenelement neu und vergleicht sie mit der Integritätsmessung, die an die Daten angehängt wird. Unbefugte Änderungen an den Daten im nichtflüchtigen Speicher führen zu Vergleichsunterschieden. Mit diesem Ansatz kann der HP ESC Manipulationen an Datenelementen im nichtflüchtigen Speicher erkennen.

### Vertraulichkeit der Daten

Für viele der von der Plattform gespeicherten Datenelemente ist die Wahrung der Vertraulichkeit entscheidend. Beispiele sind BIOS-Administrator-Passwort-Hashes, Benutzer-Anmeldeinformationen und Geheimnisse, die optional von der Firmware im Namen des Benutzers für Firmware-basierte Funktionen wie HP Sure Run und HP Sure Recovery gespeichert werden.

Der Schutz dieser Geheimnisse ist bei Verwendung von UEFI-BIOS-Ansätzen nach Branchenstandard schwierig, da der nichtflüchtige Speicher in der Regel von Software auf dem Host-Prozessor gelesen werden kann. Der geschützte Speicher von HP Sure Start soll diese vertraulichen Daten viel besser schützen als eine Standard-BIOS-Implementierung von UEFI.

Zusätzlich zu einem separaten, isolierten Speicher dient der HP Sure Start-Ansatz dazu, den im HP ESC enthaltenen Advanced Encryption Standard (AES)-Hardwareblock einzusetzen, um zusätzlich zu den Datenintegritätsmessungen für diese Elemente eine AES-256-Verschlüsselung aller im nichtflüchtigen Speicher von HP Sure Start gespeicherten vertraulichen Datenelemente durchzuführen. Der verwendete Verschlüsselungsschlüssel ist einzigartig für jeden HP ESC und verlässt diesen Controller nie, sodass Daten, die von einer einzelnen HP ESC-Komponente verschlüsselt werden, nur von demselben HP ESC entschlüsselt werden können.

## Sicherer Schutz der Boot-Keys

HP Sure Start bietet einen verbesserten Schutz der UEFI Secure Boot Key-Datenbanken, die von der Firmware gespeichert werden, im Vergleich zur UEFI Secure Boot-Implementierung nach Branchenstandard. Diese Variablen sind entscheidend für den ordnungsgemässen Betrieb der UEFI Secure Boot-Funktion, die die Integrität und Authentizität des Betriebssystem-Bootloaders prüft, bevor er beim Booten gestartet wird.

HP Sure Start schützt UEFI-sichere Boot-Key-Datenbanken, indem eine Master-Kopie im von HP Sure Start geschützten Speicher aufbewahrt wird. Alle autorisierten Änderungen an den sicheren UEFI-Standard-Boot-Key-Datenbanken durch das Betriebssystem während der Laufzeit werden von HP Sure Start verfolgt und vom HP ESC auf die Master-Kopie angewendet. HP Sure Start verwendet dann die Master-Kopie im geschützten Speicher von HP Sure Start, um nicht autorisierte Änderungen an den UEFI-Standard-Datenbanken für sichere Boot-Keys zu identifizieren und abzulehnen.

Diese Funktion, die standardmässig aktiviert ist, deckt die folgenden Datenbanken ab:

- Signaturdatenbank (db)
- Datenbank für widerrufene Signaturen (dbx)
- Key Enrollment Key (KEK)
- Platform Key (PEK) wird dynamisch zur Laufzeit durch das Betriebssystems aktualisiert

## Runtime Intrusion Detection (RTID)

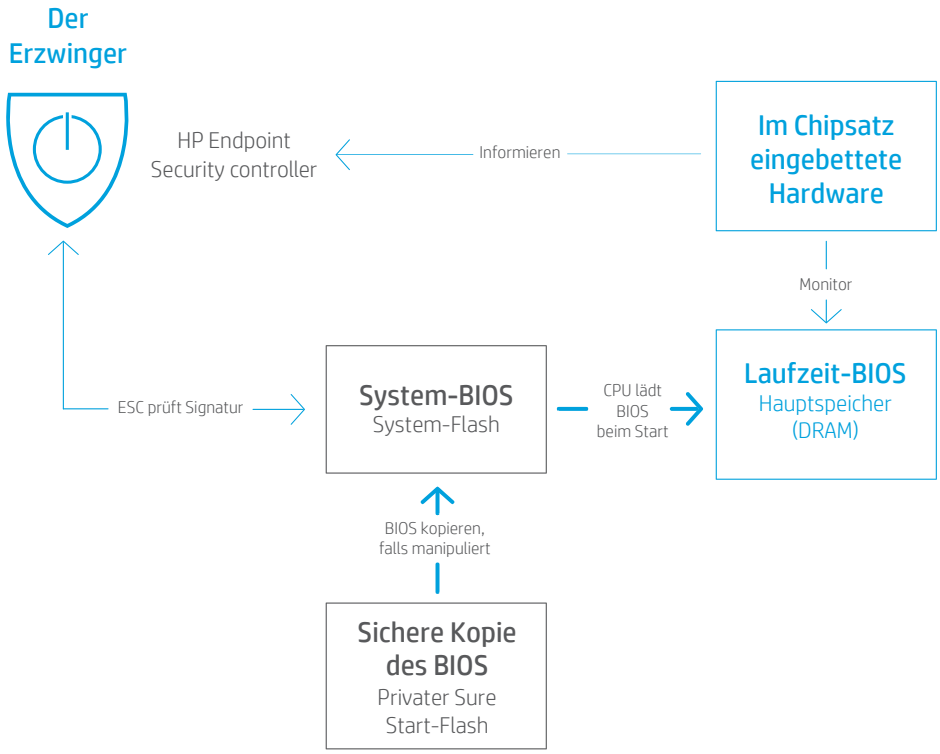
Bei jedem Start startet der BIOS-Code die Ausführung aus dem Flash-Speicher an einer festen Adresse. Dies wird als BIOS-Bootcode bezeichnet und bietet «Fähigkeiten vor dem Betriebssystem», die vor dem Start des Betriebssystems benötigt werden. Es gibt jedoch einen Teil des BIOS, der im DRAM verbleibt und benötigt wird, um erweiterte Power-Management-Funktionen, Betriebssystemdienste und andere betriebssystem-unabhängige Funktionen bereitzustellen, während das Betriebssystem läuft. Dieser BIOS-Code, der als System Management Mode (SMM)-Code bezeichnet wird, befindet sich in einem speziellen Bereich innerhalb des DRAM, der vor dem Betriebssystem verborgen ist. Wir bezeichnen diesen Code auch als «Runtime»-BIOS-Code im Zusammenhang mit der Runtime Intrusion Detection (Einbruchmeldungs)-Funktion von HP Sure Start. (Weitere Informationen zu SMM und seiner Funktionsweise finden Sie in Anhang B auf Seite 12).

Die Integrität des SMM-Codes ist entscheidend für die Sicherheitslage des Client-Geräts. HP Sure Start prüft, ob der HP SMM BIOS-Code beim Start des Betriebssystems intakt ist. Runtime Intrusion Detection bietet Mechanismen, um sicherzustellen, dass der SMM-BIOS-Code intakt bleibt, während das Betriebssystem läuft, indem neue Schutzfunktionen hinzugefügt werden und/oder ein Mittel bereitgestellt wird, um jeden Angriff auf diesen Code zu erkennen.

### Runtime Intrusion Detection-Architektur

Die RTID-Funktion verwendet spezielle Hardware im Plattform-Chipsatz, um Anomalien im Runtime HP SMM BIOS zu erkennen. Die Erkennung von Anomalien führt zu einer Benachrichtigung an den HP Endpoint Security Controller, der die konfigurierte Richtlinienaktion unabhängig von der CPU durchführen kann.

**Abbildung 2.** Runtime Intrusion Detection verwendet spezielle Hardware, die in den Chipsatz der Plattform eingebettet ist, um den SMM-Code auf Änderungen zu überwachen.



# Benutzerbenachrichtigungen, Ereignisprotokollierung und Richtlinienverwaltung

## HP Sure Start-Endbenutzerbenachrichtigungen

Unter normalen Betriebsbedingungen ist HP Sure Start für den Benutzer unsichtbar. Die Wiederherstellungsvorgänge erfolgen automatisch mit den Standardeinstellungen, ohne dass für die Wiederherstellung eine Interaktion mit dem Endbenutzer oder der IT-Abteilung erforderlich ist, wenn HP Sure Start ein Problem erkennt.

Benutzer können Runtime-Benachrichtigungen sehen, wenn ein BIOS-Integritätsproblem über den HP Sure Start Dynamic Protection oder die Runtime Intrusion Detection-Funktionen erkannt wird, während das Betriebssystem läuft. Wenn ein bedeutendes Ereignis erkannt wird oder Massnahmen ergriffen werden, zeigt HP Sure Start beim nächsten Start eine Warnmeldung über Windows®-Benachrichtigungen an. HP Notifications Software wird benötigt, um die Anzeige dieser Windows-Benachrichtigungen zu ermöglichen.

## HP Sure Start-Ereignisprotokollierung

Der HP Endpoint Security Controller zeichnet kritische Ereignisse im Zusammenhang mit dem Firmware/BIOS-Code und den von HP Sure Start überwachten Daten auf. Diese Ereignisse werden im nichtflüchtigen Speicher von Sure Start gespeichert. Diese Ereignisse werden vom HP ESC in den Windows Event Viewer kopiert, wenn die HP Notifications Software installiert ist, um den Zugriff auf diese Ereignisse für den lokalen Benutzer und den vom Kunden bevorzugten Verwaltbarkeitsagenten zu erleichtern.

Die folgenden Ereignisse veranlassen die HP Notifications Software, alle Ereignisse aus dem HP Sure Start-Subsystem zu sammeln und sicherzustellen, dass der Windows Event Viewer mit allen Ereignissen aktualisiert wird, die nicht bereits dort aufgezeichnet sind:

- Windows-Boot
- Windows-Fortsetzen nach Ruhemodus
- HP Sure Start mit dynamischen Protection Runtime-Ereignisbenachrichtigungen
- HP Sure Start Runtime Intrusion Detection (RTID)

HP Notifications Software schreibt HP Sure Start-Ereignisse in ein einzigartiges «HP Sure Start»-Anwendungsereignisprotokoll. Nur HP Sure Start-Ereignisse werden in dieses Protokoll aufgenommen. Der Windows Event Viewer-Pfad zu den HP Sure Start-Ereignissen ist der folgende: System Tools/Event Viewer/ Anwendungen und Services Logs/HP Sure Start.

Die Kategorien der Windows-Ereignisanzeige, die sich auf HP Sure Start-Ereignisse beziehen, sind in der folgenden Tabelle definiert.

Die Ereignisse werden in der Reihenfolge, in der sie von HP Sure Start generiert wurden, in den Windows Event Viewer eingefügt. Das älteste Ereignis im HP Sure Start-Subsystem wird zuerst dem Windows Event Viewer hinzugefügt und das neuere Ereignis wird zuletzt hinzugefügt.

Der Zeitstempel für jeden Windows-Ereignisanzeigeeintrag ist die Zeit, zu der er zu diesem Protokoll hinzugefügt wurde, NICHT die Zeit, zu der das Ereignis aufgetreten ist. Jeder Sure Start Windows Event Viewer-Eintrag enthält detaillierte Daten innerhalb der Ereignisdetails, die den Zeitstempel des tatsächlichen Ereignisses enthalten.

*Anmerkung: Ereignisse sind im HP Endpoint Security Controller auch nach dem Kopieren in den Windows Event Viewer persistent. Wenn die Windows-Ereignisanzeige deaktiviert ist, ersetzt die HP Notification Software alle HP Sure Start-Einträge beim nächsten Ereignis, das sie dazu veranlasst, nach HP Sure Start-Ereignisprotokollen zu suchen.*

Arten von HP Sure Start Windows Event Viewer-Ereignissen

| Ereignisstufe | Definition |
|---|---|
| Info | Ereignisse, die während des normalen Ablaufs erwartet werden (z. B. Aktualisierung des BIOS). |
| Warnung | Unerwartete Ereignisse, die aufgetreten sind, aber von HP Sure Start vollständig gelöst wurden, und es ist keine Benutzer-/Administratoraktion erforderlich, damit die Plattform voll funktionsfähig ist. Diese Ereignisse sind anomale Operationen, die der Benutzer/Administrator möglicherweise weiter untersuchen möchte, insbesondere wenn es einen Trend dieser Ereignisse über mehrere Rechner hinweg gibt. |
| Fehler | Ereignisse, bei denen der Admin/HP-Service auf den Plattformen aktiv werden muss, damit sie sich vollständig erholen. |

## HP Sure Start-Richtliniensteuerungen

Laut Werkeinstellungen aktiviert und optimiert das HP System BIOS HP Sure Start-Richtlinien für den typischen Benutzer. Da HP Sure Start standardmässig aktiviert ist, braucht der typische Benutzer die Einstellungen, die durch HP Sure Start geschützt werden sollen, nicht zu ändern. Für fortgeschrittene Benutzer bietet das System-BIOS eine gewisse Kontrolle über das Verhalten von HP Sure Start unter Verwendung von Richtlinieneinstellungen im (F10) BIOS Setup. Sofern nicht anders angegeben, befinden sich diese Einstellungen und Funktionen unter Security/BIOS Sure Start.

*Anmerkung: Richtlinien werden im nichtflüchtigen Speicher von HP ESC gespeichert, auf den die Host-CPU nicht direkt zugreifen kann; daher ist ein Neustart erforderlich, bevor die Sure-Start-Einstellungen wirksam werden.*

Die folgenden HP Sure Start-Einstellungen und -Funktionen sind verfügbar:

- Bootblock bei jedem Boot prüfen
- BIOS-Datenwiederherstellungsrichtlinie
- Network Controller-Konfigurationswiederherstellung (nur Intel)
- Eingabeaufforderung bei Änderung an der Network Controller-Konfiguration (nur Intel)
- Dynamischer Runtime Scan auf Bootblock (nur Intel)
- HP Sure Start BIOS-Einstellungsschutz
- Sicherer Schutz der Boot-Keys von HP Sure Start
- Verbesserte(r) HP-Firmware-Eindringungsschutz und -Eindringungserkennung zur Laufzeit (nur Intel)
- HP Firmware-Eindringerkennung (nur AMD)
- HP Sure Start-Sicherheitsereignisrichtlinie
- HP Sure Start-Sicherheitsereignis-Boot-Benachrichtigung
- Sperren der BIOS-Version
- MBR der Systemfestplatte speichern/wiederherstellen
- GPT der Systemfestplatte speichern/wiederherstellen
- Wiederherstellungsrichtlinie für den Boot-Sektor (MBR/GPT)

### Bootblock bei jedem Boot prüfen

HP Sure Start überprüft immer die Integrität des System-Flash-BIOS-Bootblocks, bevor er aus dem Ruhezustand oder dem Ausschalten fortgesetzt wird. Wenn auf **aktivieren** gestellt, überprüft HP Sure Start auch die Integrität des Bootblocks bei jedem Warmstart (Windows-Neustart). Der zu berücksichtigende Kompromiss ist eine schnellere Wiederanlaufzeit im Vergleich zu mehr Sicherheit. Die Standardeinstellung dieser Funktion ist **deaktivieren**.

### BIOS-Datenwiederherstellungsrichtlinie

Wenn auf **Automatisch** gesetzt, repariert HP Sure Start bei Bedarf automatisch das BIOS oder die Machine Unique Data (einzigartigen Maschinendaten). Wenn auf **Manuell** gesetzt, benötigt HP Sure Start eine spezielle Tastenfolge, um mit der Reparatur fortzufahren. Im Falle eines Problems mit dem Bootblock-Code verweigert das System das Booten und eine eindeutige Blinksequenz blinkt auf der System-LED. Im Falle eines Problems mit den Machine Unique Data zeigt das System eine Meldung auf dem Bildschirm an. Die erforderliche Tastenfolge und die angezeigte Blinkfolge variieren je nachdem, ob es sich um ein Notebook, einen Desktop oder ein Tablet handelt. Der manuelle Modus ist nützlich für Benutzer, die vor der Reparatur Forensik am System-Flash-Inhalt durchführen können. Typische Benutzer sollten den automatischen Modus verwenden. Die Standardeinstellung dieser Funktion ist **Automatisch**.

### Network Controller-Konfigurationswiederherstellung (nur Intel)

Diese Steuerung ist nur auf Intel-Systemen verfügbar. Wenn ausgewählt, stellt HP Sure Start die Werkseinstellungen der Netzwerk-Controller-Konfiguration sofort wieder her.

### Eingabeaufforderung bei Änderung an der Network Controller-Konfiguration (nur Intel)

Diese Einstellung ist nur auf Intel-Systemen verfügbar. HP stellt eine werkseitig definierte Network Controller-Konfiguration zur Verfügung, die die MAC-Adresse enthält. Wenn diese Einstellung auf **aktivieren** gesetzt ist, überwacht das System den Zustand der Netzwerk-Steuerungskonfiguration und zeigt dem Benutzer bei einer Änderung vom werkseitig konfigurierten Zustand eine Eingabeaufforderung an. Die Standardeinstellung dieser Funktion ist **deaktivieren**.

### Dynamischer Runtime Scan auf Bootblock (nur Intel)

Diese Einstellung ist nur auf Intel-Systemen verfügbar. Bei der Standardeinstellung **aktivieren** überprüft HP Sure Start regelmässig die Integrität des BIOS-Bootblocks, während das Betriebssystem ausgeführt wird. Bei der Einstellung **deaktivieren** prüft HP Sure Start nur die Integrität vor dem Booten oder dem Fortsetzen aus dem Ruhezustand.

### HP Sure Start BIOS-Einstellungsschutz

Die BIOS-Einstellungsschutzrichtlinie ist standardmässig **deaktiviert**. Um die Funktion zu aktivieren, sollte der Besitzer/Administrator des Client-Geräts zunächst alle BIOS-Richtlinien auf die bevorzugte Einstellung konfigurieren. Der Besitzer/Administrator muss ausserdem ein BIOS-Einrichtungsadministrator-Passwort konfigurieren, um den HP Sure Start BIOS-Einstellungsschutz zu verwenden.

Sobald dies abgeschlossen ist, sollte die BIOS-Schutzrichtlinie auf «aktiviert» gewechselt werden. Zu diesem Zeitpunkt wird eine Sicherungskopie aller BIOS-Einstellungen im geschützten Speicher von HP Sure Start erstellt. Zukünftig kann keine der BIOS-Einstellungen lokal oder fernbedient geändert werden. Bei jedem Neustart werden die BIOS-Richtlinieneinstellungen auf den gewünschten Zustand überprüft, und wenn es Abweichungen gibt, werden die BIOS-Einstellungen aus dem geschützten Speicher von HP Sure Start wiederhergestellt.

Um eine BIOS-Einstellung zu ändern, muss das BIOS-Administrator-Passwort eingegeben und der BIOS-Einstellungsschutz anschliessend deaktiviert werden, wodurch Änderungen an den BIOS-Einstellungen vorgenommen werden können.

### Sicherer Schutz der Boot-Keys von HP Sure Start

Mit dieser Einstellung in der Werkseinstellung **aktivieren** bietet HP Sure Start einen verbesserten Schutz der vom BIOS verwendeten sicheren Boot-Datenbanken und -Schlüssel, um die Integrität und Authentizität des Betriebssystem-Bootloaders vor dem Start zu überprüfen. Wenn auf **deaktivieren** gesetzt, wird nur der standardmässige UEFI-Variablenschutz für sicheres Starten verwendet und vom HP Sure Start-Subsystem keine Sicherungskopie aufbewahrt.

### Verbesserte(r) HP Firmware-Eindringungsschutz und -erkennung zur Laufzeit (nur Intel) und HP Firmware-Eindringungserkennung (nur AMD)

Der/die Eindringungsschutz- und -erkennung zur Laufzeit-Funktion ist für alle von HP ausgelieferten Plattformen standardmässig **aktiviert**. Der Endkunde/Administrator muss die Funktion nicht aktivieren oder anderweitig «bereitstellen», um die Vorteile von HP Sure Start-Eindringungsschutz und -erkennung zur Laufzeit nutzen zu können.

Diese Funktion kann vom Plattformverantwortlichen/Administrator optional auf **deaktivieren** gesetzt werden.

### HP Sure Start-Sicherheitsereignisrichtlinie

Diese BIOS-Richtlinieneinstellung steuert, welche Aktion ausgeführt wird, wenn HP Sure Start einen Angriff oder versuchten Angriff erkennt, während das Betriebssystem läuft. Es gibt drei mögliche Konfigurationen für diese Richtlinie:

- **Nur Ereignis protokollieren**: Wenn diese Einstellung ausgewählt ist, protokolliert der HP ESC Erkennungsereignisse, die im Pfad «Applications and Services Logs/HP Sure Start» des Microsoft Windows Event Viewers angezeigt werden können.[3]
- **Ereignis protokollieren und Benutzer benachrichtigen**: Hierbei handelt es sich um die Standardeinstellung. Wenn diese Einstellung ausgewählt ist, protokolliert der HP ESC Erkennungsereignisse, die im Pfad «Applications and Services Logs/HP Sure Start» des Microsoft Windows Event Viewers angezeigt werden können. Zusätzlich dazu wird der Benutzer über Windows benachrichtigt, dass das Ereignis aufgetreten ist.[4]
- **Ereignis protokollieren und System herunterfahren**: Wenn diese Einstellung ausgewählt ist, protokolliert der HP ESC Erkennungsereignisse, die im Pfad «Applications and Services Logs/HP Sure Start» des Microsoft Windows Event Viewers angezeigt werden können. Zusätzlich wird der Benutzer über Windows benachrichtigt, dass das Ereignis aufgetreten ist und dass das Herunterfahren des Systems unmittelbar bevorsteht.

### HP Sure Start-Sicherheitsereignis-Boot-Benachrichtigung

Diese BIOS-Richtlinieneinstellung steuert, ob HP Sure Start Warnungen und Fehlermeldungen, die beim Booten des Systems angezeigt werden, vom lokalen Benutzer bestätigt werden müssen, bevor der Boot-Vorgang fortgesetzt wird. Mit der Standardeinstellung **Require Acknowledgement (Bestätigung erforderlich)** stoppt das System mit der angezeigten Fehlermeldung. Der lokale Benutzer muss eine Taste drücken, um den Boot-Vorgang fortzusetzen. Bei Änderung zu **Time out after 15 seconds (Timeout nach 15 Sekunden)** wird die Meldung angezeigt, aber der Bootvorgang wird automatisch fortgesetzt, nachdem die Meldung 15 Sekunden lang angezeigt wurde.

### Sperren der BIOS-Version

In der (F10) BIOS-Einrichtung befindet sich diese Funktion in «Haupt/Update System BIOS».

Wenn auf **deaktivieren** gesetzt, können Sie das BIOS mit jedem unterstützten Prozess aktualisieren. Wenn der HP ESC ein gültiges Bootblock-Update im System-Flash erkennt, aktualisiert er die Sicherungskopie des Bootblocks.

Wenn auf **aktivieren** gesetzt, weigern sich alle HP BIOS-Update-Tools, das BIOS zu aktualisieren. Darüber hinaus schützt HP Sure Start das BIOS vor Versuchen, die BIOS-Version zu ändern, indem es den System-Flash über eine nicht autorisierte Methode entfernt. Der HP ESC zeichnet die geschützte Version des BIOS auf. Wenn der HP ESC erkennt, dass sich das BIOS im System-Flash geändert hat, überschreibt der HP ESC den BIOS-Bootblock mit der HP ESC-Kopie des Bootblocks. Die HP ESC-Kopie des Bootblocks wird ausgeführt und stellt den Rest der korrekten Version des BIOS wieder her. Die Standardeinstellung dieser Funktion ist **deaktivieren**.

### MBR der Systemfestplatte speichern/wiederherstellen und GPT der Systemfestplatte speichern/wiederherstellen

Im BIOS-Setup (F10) befindet sich diese Funktion unter Security/Hard Drive Utilities. Je nach Partitionstyp des primären Laufwerks (GPT oder MBR), wie von HP Sure Start erkannt, ist nur eine dieser Funktionen verfügbar.

Wenn auf **aktivieren** gesetzt, verwaltet HP Sure Start eine geschützte Sicherungskopie der MBR/GPT-Partitionstabelle vom primären Laufwerk und vergleicht bei jedem Start die Sicherungskopie mit der primären. Wenn ein Unterschied festgestellt wird, wird der Benutzer aufgefordert und kann wählen, ob er von der Sicherung in den Originalzustand zurückkehren oder die geschützte Sicherungskopie mit den Änderungen aktualisieren möchte. Die **Wiederherstellungsrichtlinie für den Boot-Sektor (MBR/GPT)** kann optional verwendet werden, um die Benutzerentscheidung für die Aktion zu entfernen, die im Falle einer von HP Sure Start gefundenen Diskrepanz getroffen wird.

Bei Einstellung auf **deaktivieren** (Standard) wird von HP Sure Start kein MBR/GPT-Schutz bereitgestellt.

### Wiederherstellungsrichtlinie für den Boot-Sektor (MBR/GPT)

Wenn auf **Local User Control (Lokale Benutzersteuerung)** (Standard) gesetzt, wird der Benutzer aufgefordert, die Aktion auszuführen, wenn HP Sure Start eine Änderung in der MBR/GPT-Partitionstabelle erkennt. Wenn auf **Recover in the event of corruption (Bei Manipulation wiederherstellen)** gesetzt, stellt HP Sure Start MBR/GPT automatisch in den gespeicherten Zustand zurück, wenn Unterschiede auftreten.

## Fernverwaltung der Richtliniensteuerungen von HP Sure Start

Werksseitig sind die HP Sure Start-Richtlinien für den typischen Benutzer optimiert. Da HP Sure Start standardmässig aktiviert ist, muss der Remote-Administrator keine Massnahmen ergreifen, um HP Sure Start zu aktivieren (oder «bereitzustellen»). Für den Fall, dass ein Remote-Administrator die Richtlinieneinstellungen von HP Sure Start ändern möchte, können dieselben Windows Management Instrumentation (WMI)-APIs oder HP BIOS-Konfigurationsprogramm-Skripte verwendet werden, die für die Verwaltung von BIOS-Richtlinien anderer Plattformen verwendet werden. Darüber hinaus können Administratoren mit dem MIK-Plugin (Manageability Integration Kit) für den Microsoft System Center Configuration Manager (SCCM) die HP Sure Start-Funktionen remote verwalten.

Darüber hinaus können Administratoren mit dem MIK-Plugin (Manageability Integration Kit) für den Microsoft System Center Configuration Manager (SCCM) HP Sure Start Funktionen remote verwalten und HP Sure Start Ereignisse anzeigen.

## Fazit

HP Sure Start liefert folgende Hauptvorteile:

- **Ununterbrochene Produktivität** – HP Sure Start erhält die Geschäftskontinuität im Falle eines Angriffs oder versehentlicher Beschädigung aufrecht, und zwar durch die Beseitigung von Ausfallzeiten, die auf ein IT/Service-Ereignis warten.
- **Niedrigere Kosten** – Die Fähigkeit von HP Sure Start, das System automatisch wiederherzustellen, senkt die Anzahl der Anrufe an den IT-Helpdesk und steigert die Produktivität, was letztendlich die Wartungskosten für die Plattform senkt.
- **Schutz vor Malware** – HP Sure Start hat mehrere Sicherheitsfunktionen, die über eine Vielzahl von Software- und Hardware-Plattformen laufen.

Mit der branchenführenden Firmware-Angriffserkennung und automatischen Reparatur von HP Sure Start schützen Sie kritische BIOS-Firmware vor Malware. HP Sure Start ist ausschliesslich auf ausgewählten HP Elite PCs verfügbar.

## Anhang A – HP Sure Start, Generation nach Generation

HP hat Sure Start im Jahr 2014 eingeführt. Seitdem hat HP Sure Start verbessert und die Anzahl der Produkte, die es verwenden, erweitert. Die folgende Tabelle gibt einen Überblick über die Fähigkeiten, die mit jeder Generation hinzugefügt wurden.

| Generation | Freigabedatum | Hinzugefügte Fähigkeiten |
|---|---|---|
| HP Sure Start | 2014 | • Firmware und BIOS-Echtheitserzwingung, mit der Fähigkeit zur Selbstheilung<br>• Firmware-Überwachung und -Compliance |
| HP Sure Start mit Dynamic Protection (dynamischem Schutz) | 2015 | • Windows Event Viewer-Unterstützung<br>• Dynamic Protection (für ausgewählte Intel-Produkte) |
| HP Sure Start Gen3 (für ausgewählte Intel-Produkte)[5]<br>HP Sure Start mit Runtime Intrusion Detection (Angriffserkennung) (für ausgewählte AMD-Produkte)[6] | 2017 | • Runtime Intrusion Detection<br>• BIOS-Einstellungsschutz<br>• Manageability Integration Kit (MIK)-Plugin für Microsoft SCCM |
| HP Sure Start Gen4[7] | 2018 | • Geschützter Speicher – Starke kryptografische Methoden zum Speichern von BIOS-Einstellungen, Zugangsdaten und anderen Einstellungen in der HP Endpoint Security Controller-Hardware, um Integritätsschutz, Manipulationserkennung und vertraulichen Schutz für diese Daten zu bieten<br>• Sicherer Schutz der Boot-Datenbank – Erweiterter Schutz von Datenbanken und Schlüsseln, die vom BIOS gespeichert werden und für die Integrität der sicheren Boot-Funktion des Betriebssystems im Vergleich zum Standard-BIOS von UEFI entscheidend sind<br>• Auf Intel-Plattformen erweiterter Schutz und Wiederherstellung der Intel Management Engine Firmware<br>• Sicherheitszertifizierung von HP Endpoint Security Controller durch ein unabhängiges und akkreditiertes Labor, um zu bestätigen, dass die HP ESC-Hardware-Kernfunktionalität gemäss den öffentlich zugänglichen Kriterien, Methoden und Prozessen funktioniert[1]<br>• HP Business-PCs mit HP Sure Start übertreffen die Widerstandsfähigkeitsrichtlinien für Firmware der Draft NIST Plattform (Sonderveröffentlichung 800-193) |

## Anhang B – Übersicht über den System Management Modus (SMM)

Der System Management Modus (SMM) ist ein Branchenstandard-ansatz, der für erweiterte Power-Management-Funktionen und andere betriebssystem-unabhängige Funktionen verwendet wird, während das Betriebssystem läuft. Während der SMM-Begriff und die Implementierung spezifisch für x86-Architekturen ist, verwenden viele moderne Computerarchitekturen ein ähnliches Architekturkonzept.

SMM wird vom BIOS beim Booten konfiguriert. Der SMM-Code wird in den Hauptspeicher (DRAM) eingefüllt, und dann verwendet das BIOS spezielle (sperrfähige) Konfigurationsregister innerhalb des Chipsatzes, um den Zugriff auf diesen Bereich zu sperren, wenn der Mikroprozessor nicht in einem SMM-Kontext ausgeführt wird. Zur Laufzeit erfolgt der Einstieg in den SMM-Modus ereignisgesteuert. Der Chipsatz ist so programmiert, dass er viele Arten von Ereignissen und Zeitüberschreitungen erkennt. Wenn ein solches Ereignis eintritt, setzt die Chipsatz-Hardware den System Management Interrupt (SMI)-Eingangs-Pin durch. An der nächsten Anweisungsgrenze speichert der Mikroprozessor seinen gesamten Zustand und geht in den SMM.

Wenn der Mikroprozessor in den SMM eintritt, wird ein Hardware-Ausgangs-Pin, SMI Active (SMIACT), verwendet. Dieser Pin weist die Chipsatz-Hardware darauf hin, dass der Mikroprozessor in den SMM eintritt. Ein SMI kann jederzeit, in jeder Prozessbetriebsart, ausser innerhalb des SMM selbst, durchgesetzt werden. Die Chipsatz-Hardware erkennt das SMIACT-Signal und leitet alle nachfolgenden Speicherzyklen in einen geschützten Speicherbereich (manchmal auch als SMRAM-Bereich bezeichnet) um, der speziell für SMM reserviert ist. Unmittelbar nach dem Empfang des SMI-Eingangs und der Bestätigung des SMIACT-Ausgangs beginnt der Mikroprozessor, seinen gesamten internen Zustand in diesem geschützten Speicherbereich zu speichern.

Nachdem der Zustand des Mikroprozessors im SMRAM-Speicher gespeichert wurde, beginnt der spezielle SMM-Handler-Code, der sich ebenfalls im SMRAM befindet (vom System-BIOS beim Booten platziert), in einer speziellen SMM-Betriebsart ausgeführt zu werden. Während des Betriebs in diesem Modus sind die meisten Hardware- und Speicherisolationsmechanismen ausgesetzt, und der Mikroprozessor kann auf praktisch alle Ressourcen der Plattform zugreifen, um die erforderlichen Aufgaben ausführen zu können. Der SMM-Code vervollständigt die erforderliche Aufgabe, und dann ist es an der Zeit, den Mikroprozessor wieder in den vorherigen Betriebsmodus zu versetzen. Zu diesem Zeitpunkt führt der SMM-Code die Anweisung «Return from System Management Mode» (zurück vom System-Management-Modus [RSM]) aus, um SMM zu beenden. Der Befehl RSM veranlasst den Mikroprozessor, seine vorherigen internen Zustandsdaten aus der in SMRAM gespeicherten Kopie bei SMM-Eintrag wiederherzustellen. Nach Abschluss des RSM wurde der gesamte Zustand des Mikroprozessors kurz vor dem SMI-Ereignis wiederhergestellt, und das vorherige Programm (Betriebssystem, Anwendungen, Hypervisor usw.) setzt die Ausführung dort fort, wo es aufgehört hat.

[1] Die HP Sure Start Controller-Hardware wurde nach dem CSPN-Zertifizierungssystem zertifiziert.

[2] HP Sure Start mit Dynamic Protection ist für HP Elite-Produkte mit Intel Core-Prozessoren der 6. Generation und höher verfügbar.

[3] Die HP Notification Software muss installiert sein, um HP Sure Start-Ereignisse im Windows Event Viewer anzeigen zu können.

[4] HP Notification Software muss installiert sein, um Benachrichtigungen zu erhalten.

[5] HP Sure Start Gen3 ist für HP Elite-Produkte mit Intel -Prozessoren der 7. Generation verfügbar.

[6] HP Sure Start mit Runtime Intrusion Detection ist für HP Elite-Produkte mit AMD-Prozessoren der 7. Generation verfügbar.

[7] HP Sure Start Gen4 ist für HP Elite- und HP Pro 600-Produkte mit Intel- oder AMD-Prozessoren der 8. Generation verfügbar.

Mehr erfahren
hp.com/go/computersecurity



4AA7-3172DECH, Mai 2018