White paper tecnico

HP Sure Start

Protezione e riparazione automatiche a livello di BIOS

Maggio 2018

Sommario

Introduzione

HP Sure Start rileva, blocca e ripara in automatico un attacco o danneggiamento del BIOS senza l'intervento del team IT e con un'interruzione minima della produttività dell'utente. Ogni volta che il PC viene avviato, HP Sure Start verifica in automatico l'integrità del codice BIOS per contribuire a garantire che il PC sia protetto da attacchi. Una volta avviato il PC, il rilevamento delle intrusioni in run-time monitora costantemente la memoria. Nel caso in cui si verificasse un attacco, il PC è in grado di auto-ripararsi utilizzando una copia fedele e isolata del BIOS in meno di un minuto.

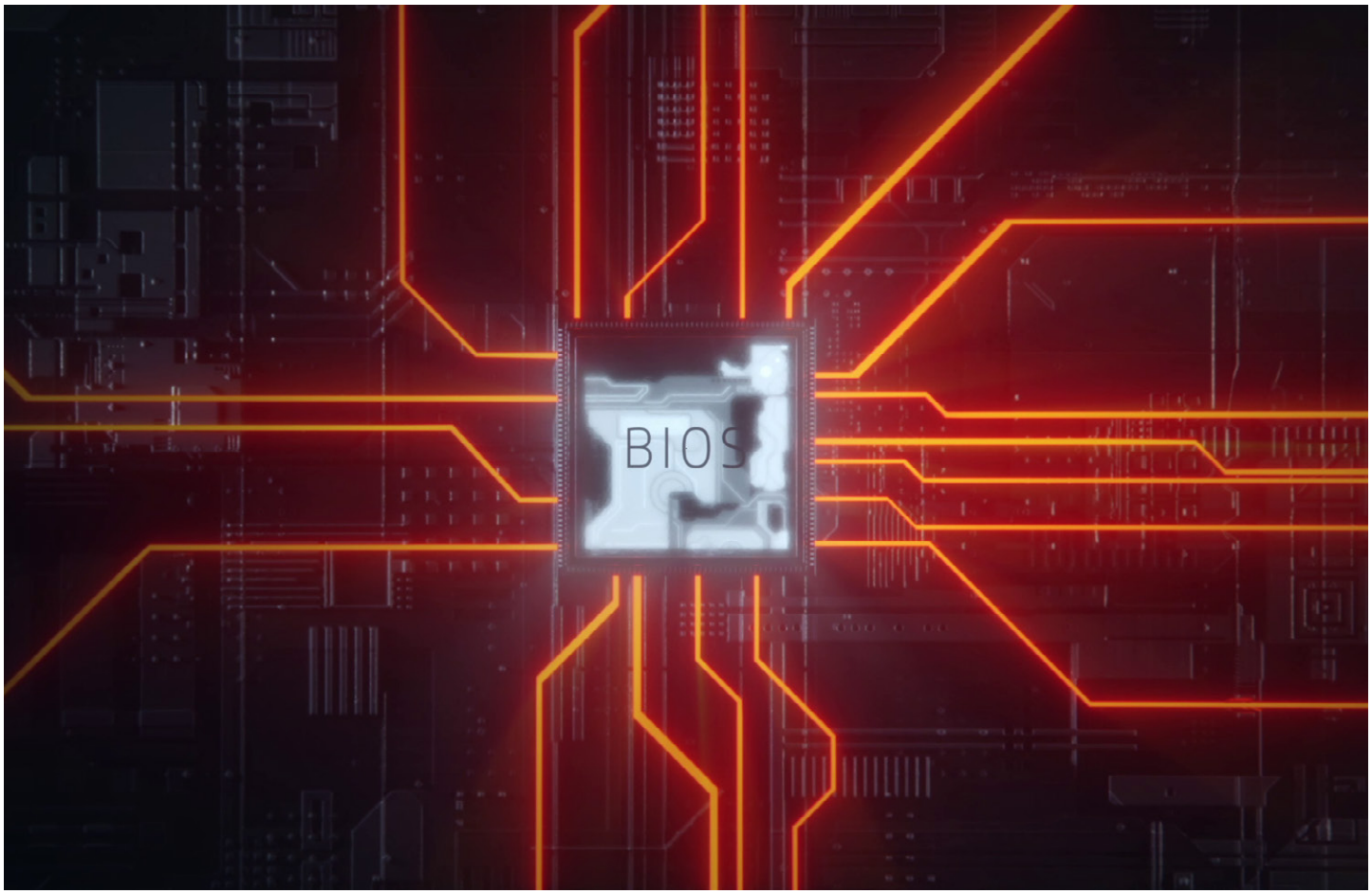
Perché è importante proteggere il BIOS?

Il nostro mondo diventa sempre più connesso, per questo gli attacchi informatici colpiscono il firmware e l'hardware dei dispositivi con crescente frequenza e una maggiore sofisticatezza. In passato gli strumenti e le tecniche di attacco al firmware erano puramente teorici e al massimo disponibili solo per enti di tipo governativo. Da allora, non solo se ne è appurata la reale esistenza, ma tali strumenti e tecniche sono diventati facilmente disponibili e di pubblico dominio.

Il firmware dei dispositivi (o BIOS) è un bersaglio ideale per gli aggressori, per le potenziali informazioni che una violazione riuscita potrebbe fornire loro.

- Persistenza: il firmware è contenuto in una memoria non volatile della scheda di circuito e non può essere rimosso semplicemente resettando l'hard drive.
- Controllo: l'esecuzione del firmware avviene con il livello più elevato di privilegi, al di fuori del dominio del SO, cosa che lo espone al malware non dipendente dai SO.
- Invisibilità: il firmware occupa una regione della memoria che è completamente inaccessibile al sistema operativo e al software del sistema, e non potendo essere scansionata dall'antivirus non potrà mai essere individuata.
- Difficoltà di recupero: tutti questi aspetti rendono estremamente difficile recuperare i danni di tali infezioni senza il ricorso a un servizio di assistenza che includa la sostituzione della scheda di sistema.

La soluzione ideale per proteggere i dispositivi da questo tipo di attacchi deve quindi partire dall'hardware, sulla base dei principi di "resilienza informatica". Tali principi riconoscono l'estrema difficoltà, se non l'impossibilità, di prevedere e prevenire ogni possibile attacco. La soluzione ideale non solo offre una protezione avanzata del firmware, ma include anche la capacità insita nell'hardware di individuare un attacco andato a segno e di ripararne i danni.



HP Sure Start per una protezione superiore del firmware

HP Sure Start è una soluzione innovativa ed esclusiva di HP che garantisce la protezione avanzata e la resilienza del firmware dei PC HP. Si avvale di un HP Endpoint Security Controller (HP ESC) basato su hardware per fornire una protezione del BIOS che supera di gran lunga gli standard di settore e garantisce che il sistema si avvierà solamente con un BIOS HP originale. Inoltre, nel caso in cui HP Sure Start rilevi una manomissione del BIOS, del firmware o del codice BIOS del System Management Mode (SMM) in run-time, esso è in grado di riparare i guasti utilizzando una copia di backup protetta.

Sintesi delle funzioni di HP Sure Start

- Esecuzione dei controlli di autenticità del firmware della piattaforma HP e protezione dalle manomissioni: esecuzione dell'Endpoint Security Controller di HP all'avvio del sistema, affinché venga caricato solo un firmware BIOS HP autentico e non alterato
- Monitoraggio e conformità dell'integrità del firmware: log degli eventi relativi all'integrità del firmware tramite un HP Endpoint Security Controller isolato; mostra lo stato del firmware di sistema insieme a eventuali anomalie che potrebbero indicare attacchi sventati
- Autoriparazione: riparazione automatica in caso di corruzione del BIOS o del firmware HP utilizzando la copia di backup isolata del BIOS o del firmware HP creata dall'Endpoint Security Controller
- Protezione delle impostazioni del BIOS: estende la protezione del codice BIOS fornita dall'Endpoint Security Controller includendo la verifica di integrità e backup di HP ESC di tutte le impostazioni del BIOS configurate da utenti o amministratori
- Individuazione delle intrusioni in run-time: monitoraggio costante del codice BIOS critico nella memoria di run-time con il sistema operativo in funzione
- Protezione delle chiavi di avvio sicuro: protezione avanzata dei database e delle chiavi salvate dal BIOS che sono di importanza critica per l'integrità della funzione di avvio sicuro del sistema operativo, rispetto a una implementazione UEFI BIOS standard
- Storage protetto: HP Sure Start utilizza dei robusti metodi di crittografia per salvare le impostazioni del BIOS, le credenziali utente e altre impostazioni nell'hardware dell'Endpoint Security Controller per garantire la protezione dell'integrità, la rilevazione di manomissioni e la riservatezza di tali dati
- Protezione del firmware di Intel® Management Engine: protezione migliorata e ripristino del firmware di Intel Management Engine
- Gestibilità: gli amministratori possono gestire le funzionalità di HP Sure Start con il plug-in del Manageability Integration Kit (MIK) di Microsoft® System Center Configuration Manager (SCCM)

Per una sintesi delle funzionalità aggiunte in ogni generazione di HP Sure Start, vedere l'Appendice A a pagina 11.

Certificato di sicurezza di parti terze

L'hardware HP Endpoint Security Controller utilizzato in HP Sure Start è stato sottoposto a valutazioni di parti terze ed è stato certificato come soluzione hardware che garantisce l'avvio esclusivo di firmware autorizzato sul PC target.[1]

La garanzia che una soluzione di sicurezza funzioni come previsto è fondamentale quando si deve decidere l'acquisto di un prodotto. Per questo, HP ha sottoposto i meccanismi interni dell'Endpoint Security Controller alla revisione e al collaudo da parte di un laboratorio indipendente accreditato per attestare il suo funzionamento secondo i criteri, metodi e processi pubblicizzati.

Design "cyber-resiliente"

HP Sure Start non offre soltanto una protezione migliorata del BIOS rispetto agli standard di settore, ma è anche progettato a partire dall'hardware per fornire una resilienza informatica senza paragoni per garantire il recupero del BIOS anche in caso di violazione o attacco distruttivo. I PC aziendali HP con HP Sure Start superano le linee guida sulla resilienza del firmware della piattaforma (pubblicazione speciale 800-193) del Draft National Institute of Standards Technology (NIST), uno dei principali sforzi compiuti nel settore pubblico per formalizzare i requisiti delle piattaforme cyber-resilienti.

Modelli supportati da HP Sure Start

HP ha lanciato Sure Start nel 2014. Da quel momento, HP ha migliorato Sure Start e ha ampliato il numero di prodotti che lo includono. HP Sure Start è fornito su tutta la linea di prodotti 2018 Elite, inclusi tablet, notebook, desktop e all-in-one (AIO). HP Sure Start Gen4 è disponibile sui prodotti HP Elite ed HP Pro 600 dotati di processori Intel o AMD® di 8ª generazione.

Architettura e funzionalità della tecnologia

L'architettura di HP Sure Start si basa su due principali componenti:

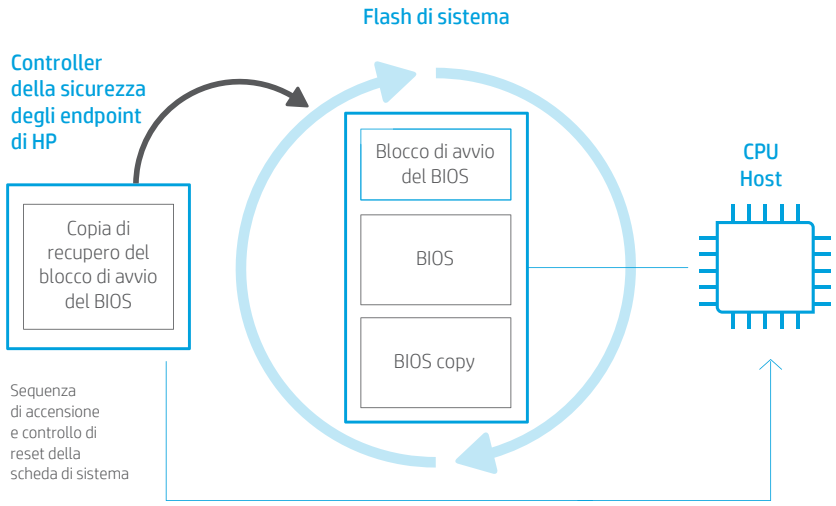
- **HP Endpoint Security Controller** che esegue il firmware di HP Sure Start
- **HP Sure Start BIOS** che lavora in sintonia con l'hardware e il firmware di HP Endpoint Security Controller

Verifica dell'integrità del firmware: il cuore di HP Sure Start

HP Endpoint Security Controller (HP ESC) è il primo dispositivo del sistema a eseguire il firmware all'accensione, ed è attivo ben prima dell'avvio del sistema. Le attività di HP ESC includono, tra le altre, il monitoraggio del pulsante di accensione del sistema e la sequenza di avviamento dell'esecuzione della CPU host nel momento in cui l'utente preme il pulsante di accensione.

Nel momento stesso in cui la piattaforma viene alimentata (prima ancora che il sistema venga avviato), HP ESC verifica che il proprio firmware HP sia autentico prima di caricarne ed eseguirne il codice. L'hardware di HP ESC utilizza dei metodi robusti di crittografia conformi agli standard di settore per verificare l'integrità del sistema. Il metodo impiega una chiave pubblica HP RSA a 2048 bit contenuta nella memoria permanente di sola lettura interna. Pertanto, HP ESC è la Root of Trust (RoT) integrata e basata su hardware per la piattaforma, utilizzata per convalidarne il firmware e il BIOS HP prima che vengano eseguiti. L'hardware Root of Trust protegge dagli attacchi che mirano a sostituire il firmware a prescindere dal metodo di attacco, e funge da base su cui è costruita la sicurezza della piattaforma HP.

Figura 1. Processo di verifica dell'integrità del firmware.



La figura 1 illustra il processo di verifica dell'integrità del firmware. Non appena HP ESC autentica e inizia ad eseguire il firmware di HP Sure Start, tale firmware utilizza le stesse operazioni crittografiche per verificare l'integrità del blocco di avvio del BIOS della flash di sistema. Se anche solo un singolo bit è invalido, HP ESC sostituisce i contenuti della flash di sistema con la propria copia del blocco di avvio del BIOS HP salvata all'interno della memoria non volatile isolata (NVM) dedicata a HP ESC.

La struttura di HP Sure Start garantisce che tutto il firmware e il codice BIOS eseguito sia da HP ESC che dalla CPU host formi il codice HP previsto sul dispositivo.

Nota: la verifica dell'integrità del blocco di avvio della flash di sistema e ogni eventuale recupero svolto da HP ESC vengono svolti mentre la CPU host è spenta. Quindi, dal punto di vista dell'utente, l'intera operazione viene svolta mentre il sistema è ancora spento, in modalità sospensione o ibernato.

Il blocco di avvio del BIOS della flash di sistema è la base del BIOS HP. L'hardware di HP ESC garantisce che il blocco di avvio del BIOS sia il primo codice eseguito dalla CPU dopo un riavvio. Non appena HP ESC determina che il blocco di avvio del BIOS contiene un codice HP autentico, consentirà il normale avvio del sistema.

HP ESC verifica anche l'integrità del codice del blocco di avvio della flash di sistema ogni volta che il sistema viene spento, messo in modalità sospensione o ibernato. Poiché la CPU viene spenta in ognuno di questi stati, ed è poi richiesta per eseguire nuovamente il codice del blocco di avvio del BIOS per il recupero, è cruciale che l'integrità del blocco di avvio del BIOS venga verificata ogni volta per rilevare la presenza di manomissioni.

Inoltre, nei modelli HP Intel, HP Sure Start verifica periodicamente (ogni 15 minuti) l'integrità del blocco di avvio del BIOS della flash di sistema mentre il sistema è in funzione.[2]

Monitoraggio avanzato dell'integrità del dispositivo

HP ESC e il BIOS lavorano insieme per fornire una protezione avanzata delle variabili critiche configurate di fabbrica uniche per ogni macchina e che devono rimanere costanti per tutta la vita di una specifica piattaforma. In fabbrica, viene salvata una copia di backup di tali variabili all'interno della memoria non volatile di HP ESC. Il backup è reso disponibile al componente BIOS di HP Sure Start in modalità di sola lettura per svolgere le verifiche di integrità dei dati ad ogni avvio. Se qualunque impostazione nella flash condivisa è variata rispetto alle impostazioni di fabbrica, i componenti BIOS di HP Sure Start recupereranno in automatico i dati della flash di sistema dalla copia di backup fornita da HP ESC.

Regione del descrittore

Nei modelli HP Intel, HP Sure Start protegge la regione del descrittore della flash di sistema. La regione del descrittore, secondo un'esclusiva dell'architettura Intel, contiene dei parametri di configurazione critici che vengono verificati dalla logica Intel Core™ al reset e quindi utilizzati per la configurazione. La regione del descrittore include inoltre delle informazioni sul partizionamento della flash di sistema e utilizzate dalla logica Intel Core per determinare l'ubicazione della regione del BIOS all'interno della flash, quindi da dove la CPU recupera il codice da eseguire dopo il reset. HP Sure Start monitora l'integrità di tale regione e ne ripristina la configurazione prevista in caso di manomissione o corruzione.

Protezione del controller di rete

Inoltre, nei modelli HP Intel, HP Sure Start protegge le impostazioni del controller di rete (NIC) contenute nella flash di sistema. Alcuni clienti HP hanno casi di utilizzo che richiedono modifiche legittime alle impostazioni di fabbrica del NIC. Pertanto, HP Sure Start non impedisce di default le modifiche alle impostazioni del NIC. Piuttosto, HP Sure Start offre una funzione che, se abilitata, avvisa l'utente della modifica alle impostazioni del NIC. Inoltre, HP Sure Start offre un metodo per ripristinare le impostazioni del NIC ai valori di fabbrica. Le impostazioni protette includono l'indirizzo MAC, le impostazioni del Pre-boot Execution Environment (PXE) e il caricamento iniziale dei programmi da remoto (RPL). Tale recupero è possibile grazie a una copia di backup di sola lettura protetta da HP ESC.

Protezione della configurazione del BIOS

Come precedentemente descritto, HP Sure Start verifica l'integrità e l'autenticità del codice BIOS di HP. Poiché il codice, dopo essere stato creato da HP, è statico, possono essere utilizzate delle firme digitali per confermare entrambi gli attributi del codice. Tuttavia, la natura dinamica e configurabile dall'utente delle impostazioni del BIOS le rendono ulteriormente difficili da proteggere. HP non può generare firme digitali per consentire all'hardware dell'ESC di HP Sure Start di verificare tali impostazioni.

La protezione delle impostazioni del BIOS di HP Sure Start offre la possibilità di configurare il sistema in modo che l'hardware di HP ESC venga utilizzato per eseguire il backup e verificare l'integrità di tutte le impostazioni del BIOS preferite dall'utente.

Quando tale funzione è abilitata sulla piattaforma, viene eseguito il backup di tutte le impostazioni delle policy utilizzate dal BIOS e viene eseguita una verifica di integrità a ogni avvio per garantire che nessuna delle impostazioni delle policy del BIOS sia stata modificata. Nel caso in cui si rilevi una modifica, il sistema utilizza il backup nella memoria protetta di HP Sure Start per ripristinare automaticamente le impostazioni definite dall'utente.

La funzione di protezione delle impostazioni del BIOS di HP Sure Start genera eventi per l'hardware dell'ESC di HP Sure Start quando viene rilevato un tentativo di modifica delle impostazioni del BIOS. L'evento viene memorizzato sul log di controllo di HP Sure Start e l'utente locale riceverà una notifica dal BIOS durante l'avvio.

Storage protetto da HP Sure Start

Lo storage protetto integrato nell'hardware dell'HP Endpoint Security Controller offre il massimo livello di protezione per i dati del BIOS/firmware e per le impostazioni protette da HP Sure Start. La memoria protetta di HP Sure Start è progettata per garantire riservatezza, integrità e la rilevazione di manomissioni anche nel caso di attacchi fisici, ovvero quando un aggressore smonta il sistema e stabilisce una connessione diretta alla memoria non volatile sulla scheda del circuito.

Integrità dei dati

L'integrità dei dati dinamici salvati sulla memoria non volatile dai firmware e utilizzati per controllare lo stato di diverse funzioni è fondamentale per la sicurezza dell'intera piattaforma. I dati dinamici includono tutte le impostazioni del BIOS che possono essere modificate dall'utente finale o dall'amministratore del dispositivo. Ad esempio, opzioni di avvio quali la funzione di avvio sicuro, la password amministratore del BIOS e le relative policy, il controllo dello stato del Trusted Platform Module e le impostazioni delle policy di HP Sure Start.

Ogni attacco andato a segno che aggira le restrizioni di accesso presenti al fine di prevenire modifiche non autorizzate di tali impostazioni può compromettere la sicurezza della piattaforma. Per esempio, si consideri uno scenario nel quale un aggressore compia una modifica non autorizzata allo stato di avvio sicuro per disabilitarlo senza essere individuato. In tale scenario, la piattaforma eseguirebbe il rootkit dell'aggressore prima dell'avvio del sistema operativo, senza che l'utente ne sia a conoscenza.

Il BIOS dell'Unified Extensible Firmware Interface (UEFI), che rappresenta lo standard di settore, prevede delle restrizioni di accesso atte a prevenire modifiche non autorizzate di tali variabili, ed è implementato nei sistemi da HP come dagli altri produttori di PC.

Tuttavia, dato il rischio rappresentato per la piattaforma da una violazione che si avvalga di tali meccanismi, HP Sure Start offre anche una difesa secondaria più robusta rispetto agli standard base di settore.

Le impostazioni del BIOS e altri dati dinamici utilizzati dai firmware per controllare lo stato e protetti da HP Sure Start sono conservati nella memoria non volatile isolata dell'Endpoint Security Controller di HP, che non è direttamente accessibile al software in funzione sulla CPU host.

Inoltre, HP ESC crea e allega delle misure uniche di integrità ogni volta che un dato viene salvato in tale memoria non volatile. Le misure di integrità si basano su solidi algoritmi crittografici (un codice di autenticazione del messaggio su base hash che utilizza l'hashing SHA-256) salvati in un'ubicazione segreta all'interno di HP ESC. Tale codice segreto è unico per ciascun HP ESC, in modo che ogni controller generi una misura di integrità unica per ogni elemento identico.

Quando i dati salvati vengono recuperati dalla memoria non volatile, HP ESC ricalcola la misura di integrità per tali dati e la confronta con la misura allegata ad essi. Qualsiasi modifica non autorizzata dei dati nella memoria non volatile crea una mancata corrispondenza. Utilizzando tale approccio, HP ESC può individuare le manomissioni dei dati conservati nella memoria non volatile.

Riservatezza dei dati

Per molti dei dati salvati sulla piattaforma, mantenere la riservatezza è fondamentale. Esempi includono gli hash della password amministratore del BIOS, le credenziali utente e i dati segreti salvati opzionalmente dal firmware al posto dell'utente per delle funzioni basate su firmware quali HP Sure Run e HP Sure Recovery.

La protezione di tali dati segreti è difficile utilizzando i classici approcci al BIOS dello standard di settore UEFI, poiché la memoria non volatile può essere tipicamente letta dal software utilizzato dal processore host. La memoria protetta di HP Sure Start mira a fornire una protezione di gran lunga maggiore di tali dati riservati rispetto all'implementazione dello standard BIOS UEFI.

Oltre a una memoria separata ed isolata, l'approccio di HP Sure Start sfrutta il blocco hardware dello standard di crittografia avanzata (AES) contenuto in HP ESC per eseguire la crittografia AES-256 su tutti i dati confidenziali conservati nella memoria non volatile di HP Sure Start, oltre alle misure di integrità dei dati per tali elementi. La chiave crittografica utilizzata è unica per ciascun HP ESC e rimane costantemente associata al controller, in modo che i dati crittografati da qualsiasi componente individuale di HP ESC possano sono essere decrittati dallo stesso HP ESC.

Protezione delle chiavi di avvio sicuro

HP Sure Start offre una protezione avanzata dei database di chiavi di avvio sicuro UEFI salvati dai firmware, rispetto all'implementazione dello standard di settore rappresentato dall'avvio sicuro UEFI. Tali variabili sono critiche per il corretto funzionamento delle funzioni di avvio sicuro UEFI che verificano l'integrità e autenticità del bootloader del SO prima di consentirne l'avvio.

HP Sure Start protegge i database di chiavi di avvio sicuro UEFI mantenendo una copia master della memoria protetta di HP Sure Start. Qualsiasi modifica autorizzata dei database di chiavi di avvio sicuro dello standard UEFI da parte del SO in run-time è monitorata da HP Sure Start e applicata alla copia master da HP ESC. HP Sure Start utilizza quindi la copia master all'interno della propria memoria protetta per identificare e rifiutare qualsiasi modifica non autorizzata ai database di chiavi di avvio sicuro dello standard UEFI.

Tale funzione, abilitata di default, si applica ai seguenti database:

- Database firme (db)
- Database firme revocate (dbx)
- Chiave di iscrizione chiavi (KEK)
- Chiave piattaforma (PEK) aggiornata in maniera dinamica in run-time dal SO

Runtime Intrusion Detection (RTID)

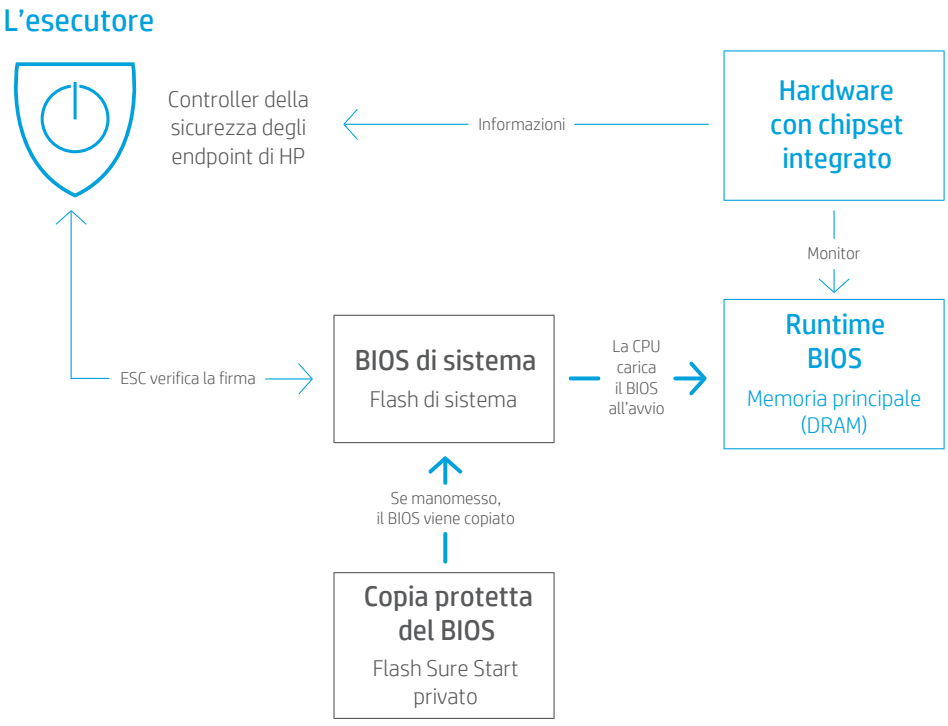
A ogni avvio, il codice BIOS inizia l'esecuzione dalla memoria flash in un indirizzo prefissato. Ciò è noto come codice di avvio del BIOS e offre le funzioni "a monte del SO" necessarie prima che il SO venga avviato. Tuttavia, esiste una parte del BIOS che rimane in DRAM e che è necessaria per fornire delle funzioni avanzate di gestione dell'alimentazione, servizi del SO e altre funzioni indipendenti dal SO mentre questo è in funzione. Il codice BIOS, noto come codice della modalità di gestione del sistema (SMM), risiede in una specifica area all'interno del DRAM, nascosta dal SO. Ci si riferisce a questo codice anche come codice BIOS in "run-time", nel contesto della funzione di individuazione delle intrusioni in run-time di HP Sure Start (per maggiori dettagli sul SMM e sul suo funzionamento si rimanda all'Appendice B a pagina 12).

L'integrità del codice SMM è critica per la sicurezza del dispositivo del cliente. HP Sure Start verifica che il codice BIOS SMM di HP sia intatto all'avvio del sistema operativo. Lo strumento Runtime Intrusion Detection offre dei meccanismi che garantiscono che il codice BIOS SMM rimanga intatto mentre il SO è in funzione, aggiungendo nuove funzionalità di protezione e/o fornendo un mezzo per rilevare eventuali attacchi a tale codice.

Architettura del Runtime Intrusion Detection

La funzione RTID utilizza un hardware specializzato nel chip della piattaforma per rilevare anomalie nel BIOS SMM di HP in run-time. La rilevazione di eventuali anomalie comporta la notifica all' HP Endpoint Security Controller che può attivare le policy configurate indipendentemente dal CPU.

Figura 2. Il Runtime Intrusion Detection utilizza un hardware specializzato integrato all'interno del chip della piattaforma per monitorare il codice SMM e rilevare alterazioni.



Notifiche utente, log degli eventi e gestione delle policy

Notifiche all'utente finale di HP Sure Start

In normali condizioni operative, HP Sure Start è invisibile all'utente. Le operazioni di recupero sono automatiche utilizzando le impostazioni di default, generalmente senza il bisogno di interazione con l'utente finale o tecnici specializzati nel caso in cui HP Sure Start identifichi un problema.

Gli utenti possono ricevere notifiche nel caso in cui venga rilevato un problema di integrità del BIOS tramite HP Sure Start Dynamic Protection o lo strumento Runtime Intrusion Detection mentre il SO è in funzione. Se viene rilevato un evento o viene intrapresa un'azione, HP Sure Start mostrerà un messaggio di avvertimento tramite le notifiche Windows® all'avvio successivo. Al fine di abilitare la visualizzazione di tali notifiche di Windows è richiesto HP Notifications Software.

Log degli eventi di HP Sure Start

L'HP Endpoint Security Controller registra eventi critici correlati ai firmware/codice BIOS e ai dati monitorati da HP Sure Start. Tali eventi sono salvati all'interno della memoria non volatile di Sure Start. Tali eventi vengono copiati da HP ESC al Windows Event Viewer quando HP Notifications Software è installato per facilitare l'accesso a tali eventi da parte dell'utente locale e dall'agente di gestibilità preferito dal cliente.

I seguenti eventi comporteranno la raccolta di tutti gli eventi da parte di HP Notifications Software dal sotto-sistema di HP Sure Start e garantiranno che il Windows Event Viewer sia aggiornato con tutti gli eventi non ancora registrati:

- Avvio di Windows
- Recupero di Windows da modalità sospensione/ibernazione
- HP Sure Start con notifiche eventi di protezione dinamica in run-time
- Runtime Intrusion Detection (RTID) di HP Sure Start

HP Notifications Software salva gli eventi di HP Sure Start all'interno di un unico log degli eventi dell'applicazione "HP Sure Start". Solo gli eventi di HP Sure Start saranno inclusi in questo log. Il percorso del Windows Event Viewer agli eventi di HP Sure Start è il seguente: System Tools/Event Viewer/Applications and Services Logs/HP Sure Start.

Le categorie di Windows Event Viewer relative agli eventi di HP Sure Start sono definiti nella tabella seguente.

Gli eventi sono salvati all'interno del Windows Event Viewer nell'ordine in cui sono stati generati da HP Sure Start. L'evento più vecchio nel sotto-sistema di HP Sure Start viene aggiunto come primo nel Windows Event Viewer, mentre l'evento più recente viene aggiunto come ultimo.

Il timestamp per ciascuna delle voci del Windows Event Viewer si riferisce al momento in cui essa è stata aggiunta al log, non al momento in cui è avvenuto l'evento a cui si riferisce. Ogni voce del Windows Event Viewer di Sure Start include dati dettagliati all'interno dei dettagli evento, incluso il timestamp di ciascun evento.

Nota: gli eventi rimangono nell'HP Endpoint Security Controller anche dopo essere stati copiati nel Windows Event Viewer. Se il Windows Event Viewer viene azzerato, l'applicazione HP Notifications Software sostituirà tutte le voci di HP Sure Start nell'evento successivo che comporterà la verifica dei log degli eventi di HP Sure Start.

Tipi di evento di Windows Event Viewer di HP Sure Start

Livelli di evento	Definizione
Informazione	Eventi prevedibili durante il normale funzionamento (per es., aggiornamento del BIOS).
Avvertenza	Eventi inattesi che si sono verificati ma sono stati pienamente riparati da HP Sure Start e non richiedono intervento da parte dell'utente/admin perché la piattaforma torni pienamente operativa. Tali eventi sono operazioni anomale relativamente alle quali l'utente/admin potrebbe voler investigare, specialmente se si verificano in sequenza su più di una macchina.
Errore	Eventi che richiedono l'intervento dell'admin/servizio di assistenza HP per riparare totalmente la piattaforma.

Controlli delle policy di HP Sure Start

Per impostazione predefinita, il BIOS dei sistemi HP abilita e ottimizza le policy di HP Sure Start per l'utente tipico. Poiché HP Sure Start è abilitato di default, l'utente tipico non ha bisogno di modificare le impostazioni per godere della protezione di HP Sure Start. Per gli utenti avanzati, il BIOS di sistema fornisce un certo controllo del comportamento di HP Sure Start, utilizzando le impostazioni delle policy nelle Impostazioni BIOS (F10). Salvo diversamente specificato, tali impostazioni e funzioni sono ubicate sotto Sicurezza/Sure Start BIOS.

Nota: le policy sono salvate all'interno della memoria non volatile di HP ESC che non è direttamente accessibile dalla CPU host; pertanto, è necessario un riavvio prima che le impostazioni di Sure Start diventino effettive.

Sono disponibili le seguenti impostazioni e funzioni di HP Sure Start:

- Verifica blocco di avvio a ogni avvio
- Policy sul recupero dei dati del BIOS
- Ripristino delle configurazioni del Controller di rete (solo per Intel)
- Avviso in caso di modifiche delle configurazioni del Controller di rete (solo per Intel)
- Scansione dinamica in run-time del blocco di avvio (solo per Intel)
- Protezione delle impostazioni del BIOS di HP Sure Start
- Protezione delle chiavi di avvio sicuro di HP Sure Start
- Prevenzione e individuazione migliorate delle intrusioni al firmware HP in run-time (solo per Intel)
- Individuazione delle intrusioni al firmware HP in run-time (solo per AMD)
- Policy degli eventi di sicurezza di HP Sure Start
- Notifica degli eventi di HP Sure Start Security all'avvio
- Blocco versione BIOS
- Salva/Recupera l'MBR dell'hard drive di sistema
- Salva/Recupera il GPT dell'hard drive di sistema
- Policy di recupero del settore di avvio (MBR/GPT)

Verifica del blocco di avvio a ogni avvio

HP Sure Start verifica sempre l'integrità del blocco di avvio del BIOS della flash di sistema prima di ripristinarlo dalla modalità "sospensione", ibernazione o da spento. Se impostato su **abilitato**, HP Sure Start verificherà inoltre l'integrità del blocco di avvio a ogni partenza a caldo (riavvio di Windows). Il compromesso da considerare è tra tempi di riavvio più veloci e una maggiore sicurezza. L'impostazione di default di questa funzione è **disabilitata**.

Policy di recupero dei dati dal BIOS

Quando impostato su **Automatico**, HP Sure Start ripara in automatico il BIOS o i dati della macchina laddove necessario. Quando impostato su **Manuale**, HP Sure Start richiede una speciale sequenza di tasti per procedere con la riparazione. Nel caso di un problema con il codice del blocco di avvio, il sistema rifiuterà di avviarsi, e il LED di sistema si illuminerà con una sequenza di lampeggiamento specifica. Nel caso di un problema nei dati unici della macchina, il sistema mostrerà un messaggio sullo schermo. La sequenza di tasti richiesta e la sequenza di lampeggiamento eseguita variano a seconda che il sistema sia un notebook, un desktop o un tablet. La modalità manuale è utile agli utenti che possono svolgere un'indagine investigativa sui contenuti della flash di sistema prima della riparazione. Agli utenti tipici è sconsigliato utilizzare la modalità manuale. L'impostazione di default di questa funzione è **Automatica**.

Ripristino delle configurazioni del controller di rete (solo per Intel)

Questo comando è disponibile esclusivamente sui sistemi Intel. Quando selezionato, HP Sure Start ripara immediatamente le configurazioni del controller di rete ripristinando le impostazioni di fabbrica.

Avviso in caso di modifiche delle configurazioni del Controller di rete (solo per Intel)

Questa impostazione è disponibile esclusivamente sui sistemi Intel. HP fornisce una configurazione del controller di rete predefinita che include l'indirizzo MAC. Quando tale impostazione è **abilitata**, il sistema monitora lo stato della configurazione del controller di rete e avvisa l'utente nel caso di modifiche allo stato predefinito. L'impostazione di default di questa funzione è **disabilitata**.

Scansione dinamica in run-time del blocco di avvio (solo per Intel)

Questa impostazione è disponibile esclusivamente sui sistemi Intel. Se impostato sullo stato di default, ovvero **abilitato**, HP Sure Start verifica periodicamente l'integrità del blocco di avvio del BIOS mentre il SO è in funzione. Se impostato su **disabilitato**, HP Sure Start verifica soltanto l'integrità prima di un avvio o di un ripristino dalla modalità "sospensione" o ibernazione.

Protezione delle impostazioni del BIOS di HP Sure Start

La policy di protezione delle impostazioni del BIOS è **disabilitata** di default. Per abilitare la funzione, il proprietario/amministratore del dispositivo client dovrà prima configurare tutte le policy del BIOS con le impostazioni preferite. Il proprietario/amministratore dovrà anche configurare una password amministratore di impostazione del BIOS per utilizzare la protezione delle impostazioni del BIOS di HP Sure Start.

Una volta completata la configurazione, la policy di protezione delle impostazioni del BIOS dovrebbe risultare "abilitata". A questo punto, viene creata una copia di backup di tutte le impostazioni del BIOS sulla memoria protetta di HP Sure Start. Procedendo, nessuna delle impostazioni del BIOS potrà essere modificata localmente o da remoto. A ogni avvio, viene verificato che le impostazioni delle policy del BIOS siano allo stato desiderato, e se viene rilevata una discrepanza, le impostazioni del BIOS vengono ripristinate dalla memoria protetta di HP Sure Start.

Per modificare un'impostazione del BIOS, occorre fornire la password amministratore del BIOS e disabilitare la protezione delle impostazioni del BIOS.

Protezione delle chiavi di avvio sicuro di HP Sure Start

Quando questa impostazione è **abilitata** come da configurazione di default, HP Sure Start fornisce una protezione migliorata dei database e delle chiavi di avvio sicuro utilizzate dal BIOS per verificare l'integrità e autenticità del bootloader del SO prima che questo venga avviato. Se impostata su **disabilitata**, viene utilizzata solo la protezione delle variabili di avvio sicuro degli standard UEFI e il sotto-sistema di HP Sure Start non conserva alcuna copia di backup.

Prevenzione e individuazione migliorate delle intrusioni al firmware in run-time di HP (solo per Intel) e individuazione delle intrusioni al firmware in run-time di HP (solo per AMD)

La funzione RTID è **abilitata** di default su tutte le piattaforme che lasciano lo stabilimento HP. L'utente finale/amministratore non dovrà eseguire alcun'altra procedura per abilitare o avviare la funzione e godere della protezione RTID di HP Sure Start.

La funzione RTID può essere opzionalmente **disabilitata** dal proprietario/amministratore della piattaforma.

Policy eventi sulla sicurezza di HP Sure Start

Le impostazioni delle policy del BIOS controllano le azioni intraprese nel caso in cui HP Sure Start rilevi un attacco o tentativo di attacco mentre il SO è in funzione. Sono possibili tre diverse configurazioni per questa policy:

- **Solo log degli eventi**: Quando questa impostazione è selezionata, HP ESC crea un log degli eventi individuati, che potranno essere visualizzati nei Log applicazioni e servizi/nel Microsoft Windows Event Viewer di HP Sure Start.[3]
- **Log evento e notifica utente**: Questa è l'impostazione di default. Quando questa impostazione è selezionata, HP ESC crea un log degli eventi individuati, che potranno essere visualizzati nei Log applicazioni e servizi/nel Microsoft Windows Event Viewer di HP Sure Start. Inoltre, l'utente viene informato all'interno di Windows dell'evento avvenuto.[4]
- **Log evento e spegnimento sistema**: Quando questa impostazione è selezionata, HP ESC crea un log degli eventi individuati, che potranno essere visualizzati nei Log applicazioni e servizi/nel Microsoft Windows Event Viewer di HP Sure Start. Inoltre, l'utente viene informato all'interno di Windows dell'evento avvenuto e dell'imminente spegnimento del sistema.

Notifica di eventi di sicurezza all'avvio di HP Sure Start

Questa impostazione delle policy del BIOS controlla se gli avvertimenti e i messaggi di errore mostrati da HP Sure Start all'avvio del sistema richiedono o meno il riconoscimento dell'errore da parte dell'utente locale prima di continuare l'avvio. Con l'impostazione di default, **Richiedi riconoscimento**, il sistema si arresta e visualizza il messaggio di errore. L'utente locale dovrà premere un tasto per continuare l'avvio. Se viene selezionata l'impostazione **Sospendi per 15 secondi**, il messaggio viene visualizzato, ma il processo di avvio viene ripreso automaticamente dopo che il messaggio è stato visualizzato per 15 secondi.

Blocco versione BIOS

Nelle impostazioni del BIOS (F10), questa funzione si trova in Principale/Aggiorna BIOS di sistema.

Se impostata su **disabilitata**, è possibile aggiornare il BIOS utilizzando qualsiasi processo supportato. Quando HP ESC rileva un valido aggiornamento del blocco di avvio nella flash di sistema, aggiorna la copia di backup del blocco di avvio.

Se impostata su **abilitata**, tutti gli strumenti di aggiornamento del BIOS HP si rifiuteranno di aggiornare il BIOS. Inoltre, HP Sure Start protegge il BIOS da tentativi di modifica della versione del BIOS tramite rimozione della flash di sistema con metodi non autorizzati. HP ESC registra la versione bloccata del BIOS. Quando HP ESC rileva che il BIOS nella flash di sistema è stato modificato, sovrascriverà il blocco di avvio del BIOS con la copia del blocco di avvio salvata da HP ESC. La copia del blocco di avvio salvata da HP ESC verrà eseguita e ripristinerà la versione corretta del BIOS. L'impostazione di default di questa funzione è **disabilitata**.

Salva/Ripristina l'MBR dell'hard drive di sistema e Salva/Ripristina il GPT dell'hard drive di sistema

Nelle impostazioni del BIOS (F10), questa funzione si trova in Sicurezza/Utility hard-drive. Solo una di queste funzioni è disponibile a seconda del tipo di partizione dell'unità principale (GPT o MBR) rilevato da HP Sure Start.

Se impostata su **abilitata**, HP Sure Start conserverà in memoria una copia di backup protetta della tabella delle partizioni MBR/GPT dall'unità primaria e la confronterà con la copia primaria a ogni avvio. Se viene riscontrata una differenza, viene chiesto all'utente se preferisce ripristinare lo stato originario dalla copia di backup o aggiornare la copia di backup protetta con le modifiche apportate. La **Policy di recupero del Boot Sector (MBR/GPT)** può essere opzionalmente utilizzata per rimuovere la decisione dell'utente sull'azione da intraprendere nel caso di discrepanze rilevate da HP Sure Start.

Se impostata su **disabilitata** (default), HP Sure Start non fornirà alcuna protezione del MBR/GPT.

Policy sul recupero del Boot Sector (MBR/GPT)

Se impostata su **Controllo utente locale** (default), verrà chiesta conferma all'utente sull'azione da intraprendere nel caso in cui HP Sure Start rilevi una modifica nella tabella delle partizioni del MBR/GPT. Se impostata su **Ripristino in caso di corruzione**, ogni volta che verranno rilevate differenze HP Sure Start ripristinerà in automatico lo stato salvato del MBR/GPT.

Gestione da remoto dei controlli delle policy di HP Sure Start

Di serie, le policy di HP Sure Start sono ottimizzate per l'utente tipico. Poiché HP Sure Start è abilitato di default, l'amministratore da remoto non dovrà intraprendere nessun'altra procedura per attivare o avviare HP Sure Start. Qualora un amministratore da remoto desideri modificare le impostazioni alle policy di HP Sure Start, potranno essere utilizzati gli stessi script di configurazione del BIOS API o HP di Windows Management Instrumentation (WMI) che vengono utilizzati per gestire altre policy del BIOS della piattaforma. Inoltre, gli amministratori possono gestire da remoto le funzioni di HP Sure Start con il plugin del Manageability Integration Kit (MIK) per Microsoft System Center Configuration Manager (SCCM).

Inoltre, gli amministratori possono gestire da remoto le funzioni di HP Sure Start e visualizzare gli eventi di HP Sure Start con il plugin del Manageability Integration Kit (MIK) per Microsoft System Center Configuration Manager (SCCM).

Conclusione

HP Sure Start offre i seguenti tre vantaggi principali:

- **Produttività senza interruzioni**: HP Sure Start mantiene la continuità dell'attività nel caso di attacchi o corruzione accidentale eliminando i tempi di fermo in attesa dell'assistenza tecnica.
- **Costo ridotto**: la capacità di recupero di HP Sure Start riduce automaticamente le chiamate all'Help Desk informatico e migliora la produttività, contribuendo in ultima analisi a ridurre il costo di manutenzione della piattaforma.
- **Nessuna preoccupazione**: HP Sure Start include molteplici funzioni di sicurezza che operano su un'ampia varietà di piattaforme software e hardware.

Proteggete il firmware fondamentale del BIOS dai malware con il sistema leader di settore per la rilevazione e la riparazione automatica delle intrusioni al firmware offerto da HP Sure Start, in esclusiva su PC HP Elite selezionati.

Appendice A: HP Sure Start, generazione dopo generazione

HP ha lanciato Sure Start nel 2014. Da quel momento, HP ha migliorato Sure Start e ha ampliato il numero di prodotti che lo utilizzano. La tabella seguente offre una sintesi delle funzioni aggiunte in ciascuna generazione.

Generazione	Data di lancio	Funzionalità aggiunte
HP Sure Start	2014	• Esecuzione di autenticità di firmware e BIOS, con capacità di auto-riparazione • Monitoraggio e conformità del firmware.
HP Sure Start con protezione dinamica	2015	• Supporto Windows Event Viewer • Protezione dinamica (per prodotti Intel selezionati)
HP Sure Start Gen3 (prodotti Intel selezionati)[5] HP Sure Start con Runtime Intrusion Detection (prodotti AMD selezionati)[6]	2017	• Runtime Intrusion Detection • Protezione delle impostazioni del BIOS • Plugin del Manageability Integration Kit (MIK) per Microsoft SCCM
HP Sure Start Gen4[7]	2018	• Memoria protetta: solido metodo crittografico per salvare impostazioni del BIOS, credenziali utente e altre impostazioni nell'hardware dell'HP Endpoint Security Controller per offrire protezione dell'integrità, individuazione delle manomissioni e protezione della riservatezza dei dati • Protezione dei database di avvio sicuro: protezione migliorata dei database e delle chiavi salvati dal BIOS e critiche per l'integrità della funzione di avvio sicuro del SO rispetto all'implementazione del BIOS secondo lo standard UEFI • Sulle piattaforme Intel, protezione e recupero migliorati del firmware dell'Intel Management Engine • Certificato di sicurezza rilasciato da parti terze dell'HP Endpoint Security Controller: verifica da parte di un laboratorio indipendente accreditato per confermare che le funzionalità principali dell'hardware di HP ESC funzionino come dichiarato in base a criteri, metodologie e processi disponibili al pubblico[1] • I PC aziendali HP con HP Sure Start superano le linee guida sulla resilienza del firmware delle piattaforme del Draft NIST (Pubblicazione speciale 800-193)

Appendice B: Panoramica del System Management Mode (SMM)

Il System Management Mode (SMM) è un approccio standard del settore utilizzato per funzioni avanzate di gestione dell'alimentazione dei PC e altre funzioni indipendenti dal SO mentre questo è in funzione. Sebbene i termini e l'implementazione del SMM siano specifici per le architetture x86, molte moderne architetture di calcolo utilizzano un concetto architettonico simile.

Il SMM è configurato dal BIOS al momento dell'avvio. Il codice SMM viene popolato all'interno della memoria principale (DRAM) e in seguito il BIOS utilizza degli speciali registri di configurazione (bloccabili) all'interno del chip per bloccare l'accesso a quest'area quando il microprocessore non viene eseguito all'interno del contesto SMM. In run-time, la modalità SMM viene impostata in base agli eventi. Il chip è programmato per riconoscere diversi tipi di eventi e timeout. Quando si verifica uno di questi eventi, l'hardware del chip crea il pin di ingresso del System Management Interrupt (SMI). Al limite successivo dell'istruzione, il microprocessore salva l'intero stato ed entra in modalità SMM.

Non appena il microprocessore entra in modalità SMM, crea un pin di uscita dell'hardware, SMI Active (SMIACT). Tale pin notifica all'hardware del chip che il microprocessore sta entrando in modalità SMM. Un SMI può essere creato in qualunque momento, in qualsiasi modalità operativa del processo, eccetto che in modalità SMM. L'hardware del chip riconosce il segnale SMIACT e reindirizza tutti i seguenti cicli di memoria ad un'area protetta della memoria (alle volte denominata area SMRAM), specificamente riservata al SMM. Subito dopo aver ricevuto il segnale SMI e aver creato l'uscita SMIACT, il microprocessore inizia a salvare tutto il proprio stato interno in tale area protetta della memoria.

Una volta salvato lo stato del microprocessore nella memoria SMRAM, viene eseguito lo speciale codice di gestione del SMM salvato nella SMRAM dal BIOS del sistema all'avvio, in una modalità operativa speciale del SMM. Durante il funzionamento in tale modalità, molti meccanismi di isolamento dell'hardware o della memoria sono sospesi, e il microprocessore può accedere virtualmente a tutte le risorse della piattaforma per abilitarle a svolgere le attività richieste. Il codice SMM completa l'attività richiesta, quindi riporta il microprocessore alla modalità operativa precedente. A questo punto, il codice SMM esegue l'istruzione della modalità Return from System Management (RSM) ed esce dal SMM. L'istruzione RSM implica che il microprocessore recuperi i dati precedenti sullo stato interno dalla copia salvata nella SMRAM al momento dell'avvio del SMM. Al completamento della modalità RSM, l'intero stato del microprocessore è stato ripristinato allo stato immediatamente precedente all'evento SMI, e il programma precedente (SO, applicazioni, hypervisor, ecc.) riprende l'esecuzione da dove l'aveva interrotta.

[1] L'hardware del controller di HP Sure Start è stato certificato in base al quadro di certificazione CSPN.

[2] HP Sure Start con protezione dinamica è disponibile sui prodotti HP Elite dotati di processori Intel Core di 6ª generazione o superiore.

[3] Per visualizzare gli eventi di HP Sure Start sul Windows Event Viewer è necessario installare HP Notification Software.

[4] Per poter ricevere notifiche è necessario installare HP Notification Software.

[5] HP Sure Start Gen3 è disponibile sui prodotti HP Elite dotati di processori Intel di 7ª generazione.

[6] HP Sure Start con Individuazione delle intrusioni in run-time è disponibile sui prodotti HP Elite dotati di processori AMD di 7ª generazione.

[7] HP Sure Start Gen4 è disponibile sui prodotti HP Elite ed HP Pro 600 dotati di processori Intel o AMD di 8ª generazione.

Scoprite di più
hp.com/go/computersecurity

4AA7-3172ITE, Maggio 2018