Přehled technických parametrů

HP Sure Start

Automatická ochrana a opravy na úrovni systému BIOS

Smět 2018

Obsah

Úvod

Funkce HP Sure Start může automaticky detekovat, zastavit a obnovit systém po útoku na BIOS nebo jeho porušení, aniž by byla třeba intervence IT, a jen s malým nebo žádným přerušením produktivity uživatele. Při každém zapnutí počítače vyhodnotí funkce HP Sure Start automaticky neporušenost kódu systému BIOS a to pomáhá ochránit počítač před zlovolnými útoky. Za provozu počítače detekce narušení trvale sleduje paměť. V případě útoku je počítač schopen se samočinně opravit pomocí izolované „zlaté kopie“ systému BIOS za méně než minutu.

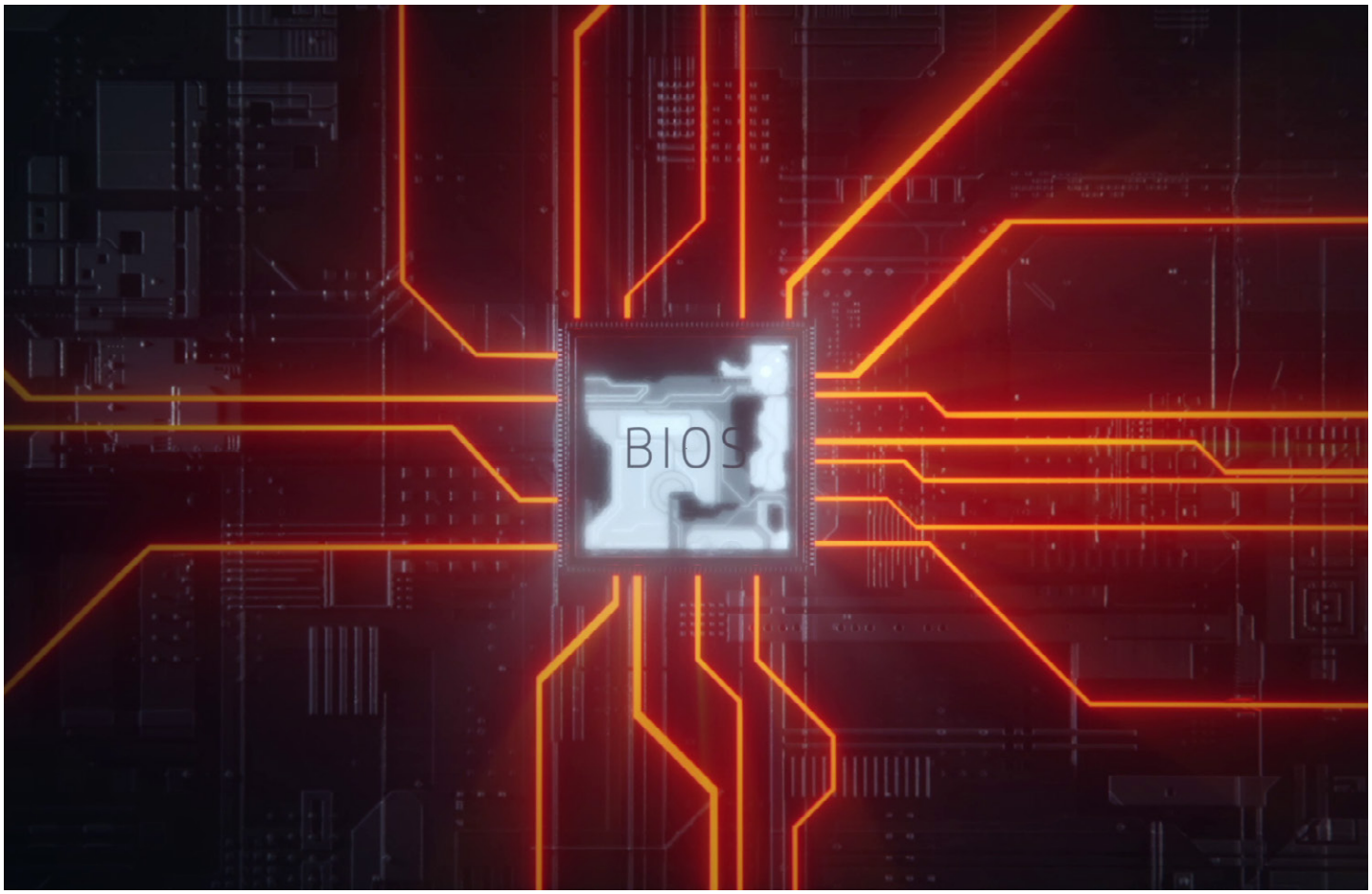
Proč je důležitá ochrana na úrovni systému BIOS?

Protože náš svět je stále více propojený, kybernetické útoky jsou stále častěji a promyšleněji zaměřeny na firmware a hardware klientských zařízení. Nástroje a techniky útoku na fimware byly kdysi jen teoretické a panoval názor, že k nim může docházet jen na národní úrovni. Od té doby se ukázalo, že podobné nástroje a techniky nejenže existují, ale jsou také snadno dostupné široké veřejnosti.

Firmware (nebo systém BIOS) přístrojů je pro útočníky lákavým cílem, protože úspěšný průnik může útočníkovi poskytnout tyto potenciální atributy:

- Trvalost: Firmware je umístěn v energeticky nezávislé, pevné paměti na desce plošných spojů a nelze ho jednoduše odstranit vymazáním pevného disku.
- Řízení: Firmware pracuje na nejvyšší úrovni oprávnění – mimo doménu operačního systému, která umožňuje existenci malwaru nezávislého na OS.
- Utajenost: Firmware zaujímá oblast paměti, která je pro operační systém a systémový software zcela nepřístupná; protože ji nemůže skenovat antivirový program, nikdy ho nelze detekovat.
- Obtížnost odstranění: Všechny tyto aspekty způsobují, že je extrémně obtížné se zotavit z tohoto typu infekce, aniž by se uživatel uchýlil k servisní události, která spočívá ve výměně základní desky.

Ideální řešení ochrany zařízení proti tomuto typu útoku vychází z hardwaru a staví na principech „kybernetické odolnosti“. Tyto principy uznávají, že je mimořádně obtížné, pokud to není přímo nemožné, předvídat každý možný útok a preventivně mu zamezit. Ideální řešení poskytuje nejen vylepšenou ochranu firmwaru, ale nese s sebou i hardwarovou schopnost detekovat úspěšný útok a zotavit se z něj.



HP Sure Start přináší vynikající ochranu firmwaru

Funkce HP Sure Start je jedinečný a průkopnický přístup společnosti HP, který poskytuje počítačům HP pokročilou ochranu a odolnost. Využívá hardwarové vynucování pomocí hardwaru HP Endpoint Security Controller (HP ESC), aby poskytl ochranu systému BIOS, která dalece přesahuje průmyslové standardy a zajišťuje, že systém spustí pouze originální systém Genuine HP BIOS. Pokud navíc funkce HP Sure Start zjistí, že došlo k neoprávněnému zásahu do systému BIOS, firmwaru nebo runtime kódu BIOSu režimu System Management Mode (SMM), dokáže se obnovit pomocí chráněné záložní kopie.

Přehled funkcí HP Sure Start

- Vynucování autenticity firmwaru základní platformy HP a ochrana proti manipulacím – HP Endpoint Security Controller představuje hardwarové vynucování při zavádění systému, takže načíst lze pouze autentický a neupravený firmware a systém HP BIOS.
- Monitorování neporušenosti firmwaru a jeho shody s požadovaným stavem – Protokolování událostí souvisejících s neporušeností firmwaru prostřednictvím izolovaného hardwarového ovladače HP Endpoint Security Controller; udává stav firmwaru platformy společně se všemi anomáliemi, které by mohly indikovat zmařené útoky.
- Samoléčba – Automatická oprava porušení systému HP BIOS a firmwaru HP pomocí izolované záložní kopie systému HP BIOS a firmwaru HP pomocí hardwaru HP Endpoint Security Controller.
- Ochrana nastavení systému BIOS – Rozšiřuje ochranu kódu systému BIOS pomocí hardwaru HP Endpoint Security Controller na zálohu HP ESC a kontrolu integrity všech uživatelem nebo správcem konfigurovaných nastavení systému BIOS.
- Detekce průniku za provozu – Průběžné monitorování kriticky důležitého kódu systému BIOS v paměti (SMM) za chodu operačního systému.
- Bezpečná ochrana klíčů při načítání systému – Podstatně rozšířená ochrana databází a klíčů uložených systémem BIOS, které jsou kriticky důležité pro neporušenost funkce bezpečného načítání operačního systému ve srovnání se standardní implementací UEFI BIOS.
- Chráněné ukládání – HP Sure Start používá silné kryptografické metody ukládání nastavení systému BIOS, uživatelských pověření a dalších nastavení v hardwaru HP Endpoint Security Controller s cílem poskytnout ochranu neporušenosti, detekovat pokusy o manipulaci a poskytnout bezpečnou ochranu těchto dat.
- Ochrana firmwaru Intel® Management Engine – Rozšířená ochrana a obnova firmwaru Intel Management Engine.
- Možnosti správy – Pomocí doplňku Manageability Integration Kit (MIK) s doplňkem pro Microsoft® System Center Configuration Manager (SCCM) mohou správci spravovat možnosti funkce HP Sure Start.

Přehled schopností přidaných do jednotlivých generací funkce HP Sure Start viz příloha A na straně 11.

Certifikace zabezpečení jiných stran

Hardware HP Endpoint Security Controller používaný ve funkci HP Sure Start byl podroben hodnocení zabezpečení od jiných dodavatelů a byl certifikován proto, že přináší hardwarové vynucování toho, že na cílovém PC lze spustit pouze autorizovaný firmware.[1]

Záruka, že bezpečnostní řešení pracuje tak, jak je uvedeno, je rozhodující částí jakéhokoli rozhodnutí o koupi týkající se bezpečnostních produktů. A protože pověst kvality může jít až tak daleko, společnost HP odhalila vnitřní operace HP Endpoint Security Controller pro kontrolu a testování nezávislé a akreditované laboratoři, aby ověřila, že funguje tak, jak je uvedeno, na základě veřejně dostupných kritérií, metodiky a procesů.

Design odolný proti kybernetickým útokům

Nejenže funkce HP Sure Start poskytuje vylepšenou ochranu systému BIOS mimo standardní přístup, ale je navržena tak, aby poskytovala bezkonkurenční odolnost vůči kybernetickým útokům, aby zajistila obnovu systému BIOS i v případě prolomení nebo destruktivního útoku. Podnikové počítače HP s programem HP Sure Start překračují požadavky směrnice NIST (National Institute of Standards Technology) vztahující se k odolnosti firmwaru platforem (speciální vydání 800-193), které jsou jednou z hlavních snah veřejného sektoru o formalizaci požadavků na platformy odolné proti kybernetickým útokům.

Modely podporované funkcí HP Sure Start

Společnost HP představila funkci HP Sure Start v roce 2014. Od té doby společnost HP zdokonalila funkci Sure Start a rozšířila spektrum výrobků, které ji obsahují. Funkce HP Sure Start je zahrnuta do celé řady výrobků Elite 2018 včetně tabletů, notebooků, stolních počítačů a kompaktních počítačů All-In-One (AIO). HP Sure Start Gen4 se dodává v produktech HP Elite a HP Pro 600 vybavených procesory Intel nebo AMD® 8. generace.

Přehled a možnosti architektury

Architektura HP Sure Start sestává ze dvou hlavních komponent:

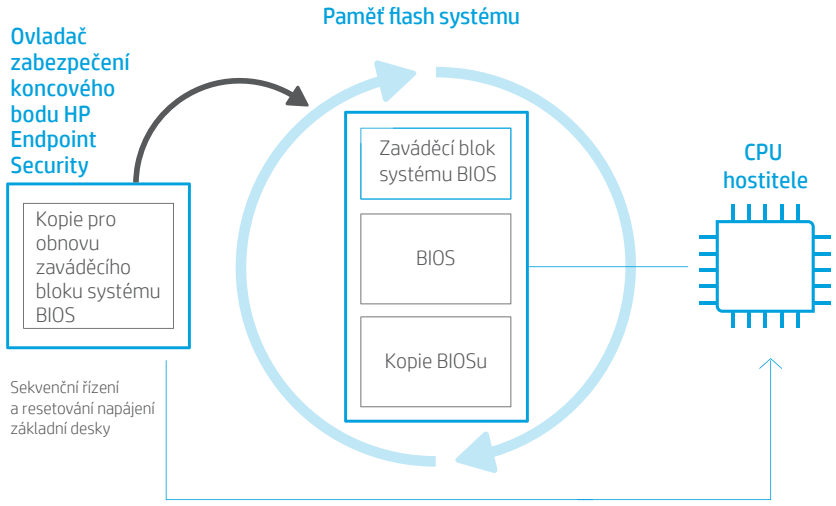
- **Hardware HP Endpoint Security Controller,** ve kterém pracuje firmware HP Sure Start.
- **HP Sure Start BIOS** spolupracující s hardwarem HP Endpoint Security Controller a firmwarem.

Ověření neporušenosti firmwaru – jádro funkce HP Sure Start

Hardware HP Endpoint Security Controller (HP ESC) je prvním zařízením v systému, které při zapínání systému spouští firmware, a je aktivní ještě před zaváděním systému. Činnosti hardwaru HP ESC zahrnují zejména sledování systémového tlačítka napájení, a když uživatel stiskne tlačítko napájení, umožní zahájení spouštění hostitelského CPU.

Po prvním zapnutí napájení na platformě (před zapnutím systému) ověří hardware HP ESC, že před načtením a spuštěním kódu je jeho vlastní firmware autentickým kódem HP. Hardware HP ESC používá standardní, silné kryptografické metody pro provádění ověření neporušenosti. Tato metoda využívá veřejný 2048bitový klíč HP RSA uložený ve vnitřní trvalé paměti určené jen ke čtení. HP ESC je proto vestavěný hardwarový Root of Trust (RoT) pro danou platformu, který se používá k ověření svého vlastního firmwaru a systému HP BIOS ještě před jejich spuštěním. Tento hardwarový Root of Trust chrání proti útokům zaměřeným na výměnu firmwaru bez ohledu na způsob jejich zavedení a slouží jako základ, na kterém je postaveno zabezpečení platformy HP.

Obrázek 1. Proces ověření neporušenosti firmwaru.



Obrázek 1 ilustruje proces ověření neporušenosti firmwaru. Jakmile hardware HP ESC ověří firmware HP Sure Start a zahájí jeho spouštění, používá tento firmware stejné silné kryptografické operace k ověření integrity zaváděcího bloku BIOSu systémové paměti flash. Pokud zjistí, že je i jen jeden bit neplatný, program HP ESC nahradí obsah systémové paměti flash vlastní kopií spouštěcí verze systému HP BIOS, který je uložen v samostatné energeticky nezávislé paměti (NVM) určené pro HP ESC.

Koncepce HP Sure Start zajišťuje, že veškerý kód firmwaru a systému BIOS běžící jak na HP ESC, tak na hostitelském procesoru, je kódem HP, který má být v zařízení.

Poznámka: Kontrola integrity zaváděcího bloku systémové paměti flash a veškeré potřebné obnovení prováděné nástrojem HP ESC probíhají, když je hostitelská jednotka CPU vypnutá. Z uživatelského hlediska se tedy celá operace uskutečňuje, když je systém stále ještě vypnutý, v režimu spánku nebo v režimu hibernace.

Zaváděcí blok BIOSu systémové paměti flash je základem BIOSu HP. Hardware HP ESC zajišťuje, že zaváděcí blok systému BIOS je prvním kódem, který CPU provede po resetování. Jakmile HP ESC zjistí, že zaváděcí blok systému BIOS obsahuje autentický kód HP, umožní zavedení systému běžným způsobem.

HP ESC také kontroluje neporušenost kódu zaváděcího bloku systémů paměti flash při každém vypnutí systému nebo přepnutí systému do režimu hibernace nebo spánku. Vzhledem k tomu, že jednotka CPU je v každém z těchto stavů vypnutá a procesor je proto nucen znovu spustit kód zaváděcího bloku systému BIOS, je nezbytné znovu ověřit neporušenost zaváděcího bloku systému BIOS pokaždé, aby se ověřilo, že nedošlo k neoprávněnému zásahu.

U modelů HP Intel navíc kontroluje funkce HP Sure Start pravidelně (každých 15 minut) za chodu počítače neporušenost zaváděcího bloku BIOSu systémové paměti flash. [2]

Jedinečná neporušenost dat počítače

Programy HP ESC a BIOS společně poskytují pokročilou ochranu kriticky důležitých proměnných konfigurovaných ve výrobě, které jsou pro každý počítač jedinečné a musí být konstantní po celou dobu životnosti jakékoli konkrétní platformy. Ve výrobě se záložní kopie těchto variabilních dat uloží v energeticky nezávislém paměťovém úložišti HP ESC. Zálohování je k dispozici pro komponentu HP Sure Start BIOS a je pouze ke čtení, aby bylo možné provádět kontrolu neporušenosti dat při každém zavádění systému. Pokud se ve sdílené paměti flash změní nastavení ve srovnání s továrním nastavením, součásti systému HP Sure Start BIOS automaticky obnoví data v systémové paměti flash ze záložní kopie poskytnuté nástrojem HP ESC.

Oblast popisovače

U modelů HP Intel chrání program HP Sure Start oblast popisovačů systémové paměti flash. Architektura Intel jako jediná zahrnuje oblast popisovačů obsahující kriticky důležité parametry konfigurace, které jsou při resetování vzorkovány logikou Intel Core™ a následně se používají ke konfiguraci logiky Core. Oblast deskriptoru také obsahuje informace o rozdělení systémové paměti flash, kterou používá logika Intel Core, ke zjištění, kde se nachází v paměti flash oblast systému BIOS, a tudíž kde jednotka CPU načte kód pro provedení po resetování. HP Sure Start monitoruje neporušenost této oblasti a v případě manipulace nebo porušení ji obnoví do požadované konfigurace.

Ochrana síťové karty

U modelů HP Intel navíc chrání program HP Sure Start nastavení síťové karty (NIC) obsažené v systémové paměti flash. Někteří zákazníci HP používají počítače způsobem, který vyžaduje oprávněné změny nastavení konfigurace NIC z výroby. Proto HP Sure Start nebrání ve výchozím stavu změnám nastavení. Namísto toho poskytuje HP Sure Start funkci, která po své aktivaci varuje uživatele před provedenými změnami nastavení NIC. HP Sure Start navíc nabízí metodu obnovení nastavení NIC na výchozí hodnoty z výroby. Mezi chráněná nastavení patří adresa MAC, nastavení prostředí PXE (Pre-boot Execution Environment) a vzdálené počáteční načítání programu (RPL). Toto obnovení je možné prostřednictvím záložní kopie jen ke čtení, kterou chrání HP ESC

Ochrana nastavení systému BIOS

Jak jsme již popsali, ověřuje nástroj HP Sure Start neporušenost a autenticitu kódu systému HP BIOS. Protože tento kód je po vytvoření společností HP statický, lze k ověření obou atributů kódu použít digitální podpisy. Dynamická povaha nastavení systému BIOS, které může měnit i uživatel, však představuje další problémy při ochraně těchto nastavení. Digitální podpisy může generovat společnost HP a může je používat hardware HP Sure Start ESC k ověření těchto nastavení.

Ochrana nastavení HP Sure Start BIOS nabízí možnost konfigurovat systém tak, aby byl hardware HP ESC používán k zálohování a kontrole integrity všech nastavení systému BIOS, která uživatel upřednostňuje.

Je-li na platformě tato funkce povolena, všechna nastavení zásad použitá systémem BIOS jsou následně zálohována a při každém zavádění systému se provádí kontrola neporušenosti dat; tím se ověřuje, že žádná z nastavení zásad systému BIOS nebyla změněna. Pokud je zjištěna změna, systém použije zálohu z chráněného úložiště nástroje HP Sure Start, aby se automaticky vrátila k uživatelem definovanému nastavení.

Funkce ochrany nastavení systému HP Sure Start BIOS generuje pro hardware HP Sure Start ESC události při zjištění pokusu o úpravu nastavení systému BIOS. Událost je protokolována v protokolu z kontroly HP Sure Start a místní uživatel obdrží upozornění během načítání systému.

Paměť chráněná funkcí HP Sure Start

Chráněné úložiště pevně přiřazené hardwaru HP Endpoint Security Controller poskytuje nejvyšší úroveň ochrany dat systému BIOS/firmwaru a nastavení chráněných programem HP Sure Start. Chráněné úložiště HP Sure Start je určeno k tomu, aby zaručovalo zachování důvěrnosti, celistvosti a detekci pokusů o manipulaci i ve scénářích fyzických útoků, kde útočník analyzuje systém a vytváří přímé spojení s energeticky nezávislou pamětí na desce plošných spojů.

Neporušenost dat

Neporušenost dynamických dat uložených v energeticky nezávislé paměti firmwarem a používaných k ovládání stavu různých funkcí je kriticky důležitá pro stav zabezpečení celé platformy. Mezi dynamická data patří všechna nastavení systému BIOS, která může upravovat koncový uživatel nebo správce zařízení. Mezi příklady patří zejména možnosti zavádění systému, jako je funkce zabezpečení při zavádění systému, heslo správce systému BIOS a související zásady, řízení stavu modulu Trusted Platform Module a nastavení zásad HP Sure Start.

Jakýkoli úspěšný útok, který obchází existující omezení přístupu zaměřená na ochranu proti neoprávněným změnám těchto nastavení, by mohl překonat zabezpečení platformy. Jako příklad můžeme zvažovat scénář, v němž útočník – aniž by byl detekován – provede neoprávněnou změnu stavu bezpečného zavádění, aby ho deaktivoval. V tomto scénáři by platforma spustila před zavedením operačního systému kořenovou sadu útočníka bez vědomí uživatele.

Systém BIOS odpovídající průmyslovým standardům Unified Extensible Firmware Interface (UEFI) zavádí omezení přístupu, která by měla zabránit neoprávněným změnám těchto proměnných, a společnost HP je implementuje stejně jako ostatní v tomto odvětví.

Avšak vzhledem k rizikům, která představují pro platformu porušení těchto mechanismů, poskytuje program HP Sure Start sekundární obranu, která je silnější než základní průmyslový standard.

Nastavení systému BIOS a další dynamické údaje používané firmwarem ke kontrole stavu, který je chráněn programem HP Sure Start, jsou uloženy v izolované, energeticky nezávislé paměti hardwaru HP Endpoint Security Controller, která není přímo přístupná softwaru běžícímu v hostitelské jednotce CPU.

HP ESC navíc vytváří a přidává při každém uložení datového prvku do tohoto energeticky nezávislého paměťového úložiště jednoznačné hodnoty ke kontrole neporušenosti dat. Hodnocení celistvosti je založeno na silném kryptografickém algoritmu (ověřovací kód s kontrolním součtem, využívající algoritmus SHA-256), který vychází z utajené hodnoty obsažené v HP ESC. Tato utajená hodnota je jedinečná pro každý HP ESC, takže každý řadič generuje na základě shodného prvku jedinečnou hodnotu k ověření neporušenosti dat.

Když se datový prvek přečte zpět z energeticky nezávislé paměti, HP ESC přepočítá hodnotu k ověření neporušenosti dat pro daný datový prvek a výsledek porovná s kontrolní hodnotou připojenou k datům. Jakákoli neoprávněná změna dat v energeticky nezávislém paměťovém úložišti přináší nevyhovující výsledek srovnání. Díky tomuto přístupu může HP ESC detekovat pokusy o manipulaci s datovými prvky uloženými v energeticky nezávislém paměťovém úložišti.

Důvěrnost dat

U řady prvků dat uložených platformou je kriticky důležité zachování důvěrnosti. Mezi příklady patří hash hesla správce systému BIOS, pověření uživatelů a utajené údaje volitelně uložené firmwarem jménem uživatele pro funkce firmwaru, jako jsou HP Sure Run a HP Sure Recovery.

Ochrana těchto utajených hodnot je náročná s využitím standardních přístupů systému UEFI BIOS, protože energeticky nezávislé úložiště obvykle může číst i software, který běží v hostitelském procesoru. Chráněné úložiště HP Sure Start má poskytovat mnohem větší ochranu těchto důvěrných dat než standardní implementace systému UEFI BIOS.

Vedle samostatného izolovaného úložiště má přístup HP Sure Start za cíl využívat hardwarový blok Advanced Encryption Standard (AES) obsažený v HP ESC k šifrování AES-256 všech důvěrných prvků dat uložených v energeticky nezávislé paměti nástroje HP Sure Start, kromě měření celistvosti dat pro tyto prvky. Použitý šifrovací klíč je pro každý HP ESC jedinečný a nikdy neopouští tento řadič, takže data šifrovaná libovolnou komponentou HP ESC mohou být dešifrována pouze stejným HP ESC.

Ochrana klíčů bezpečného načtení systému

Program HP Sure Start poskytuje zvýšenou ochranu databází klíčů zabezpečeného zavádění systému rozhraní UEFI, které jsou uloženy firmwarem, ve srovnání se standardní implementací zabezpečeného zavádění systému rozhraní UEFI. Tyto proměnné jsou kriticky důležité pro správnou činnost funkce zabezpečeného zavádění systému rozhraní UEFI, která ověří integritu a autentičnost zavaděče operačního systému OS dříve, než při zavádění systému umožní jeho spuštění.

HP Sure Start chrání databáze klíčů zabezpečeného zavádění systému rozhraní UEFI tím, že udržuje jejich základní kopii v chráněné paměti nástroje HP Sure Start. Veškeré schválené úpravy standardních databází klíčů zabezpečeného zavádění systému rozhraní UEFI provedené operačním systémem za chodu systému jsou sledovány programem HP Sure Start a aplikovány na hlavní kopii společností HP ESC. Program HP Sure Start pak použije hlavní kopii v chráněném úložišti HP Sure Start k identifikaci a odmítnutí všech neoprávněných změn ve standardních databázích klíčů k zabezpečenému zavádění systému rozhraní UEFI.

Tato možnost je ve výchozím stavu aktivní a vztahuje se na následující databáze:

- databáze podpisů (db),
- databáze odvolaných podpisů (dbx),
- klíč k registraci klíčů Key Enrollment Key (KEK),
- klíč platformy Platform Key (PEK) dynamicky aktualizovaný za chodu operačního systému.

Detekce průniku za chodu Runtime Intrusion Detection (RTID)

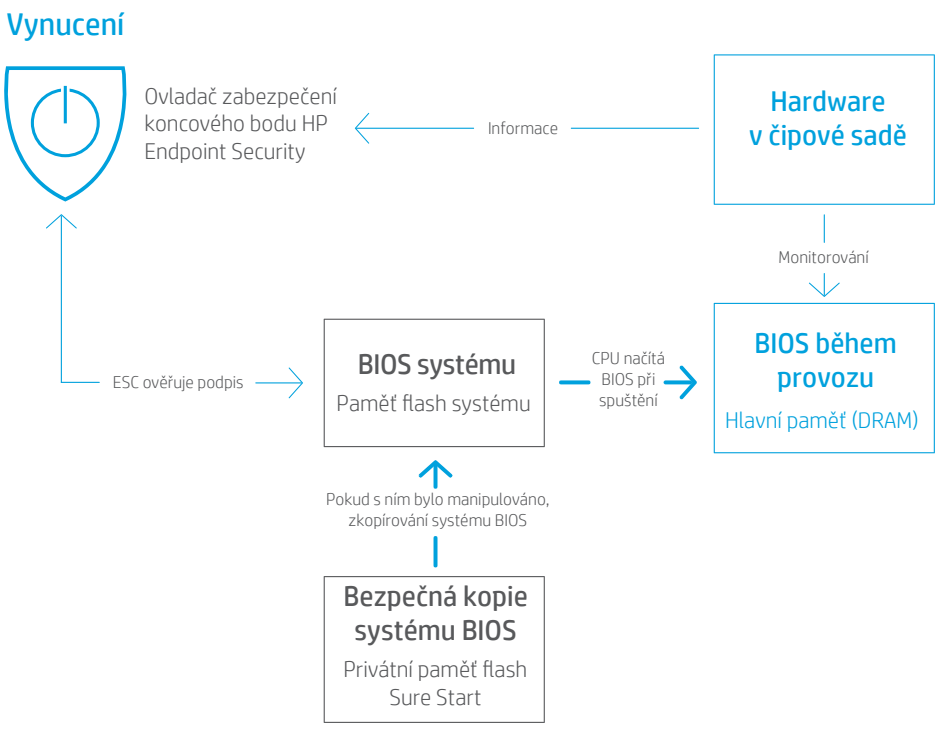
Při každém zavádění systému se začne kód systému BIOS spouštět z pevné adresy v paměti flash. To je známo jako zaváděcí kód BIOS a před spuštěním operačního systému to přináší potřebné možnosti „pre-OS“. Existuje však část systému BIOS, která zůstává v paměti DRAM a která je třeba k poskytování pokročilých funkcí správy napájení, služeb OS a dalších funkcí nezávislých na OS, zatímco systém běží. Tento kód systému BIOS, označovaný jako kód SMM (System Management Mode), je umístěn ve zvláštní oblasti v paměti DRAM, která je před operačním systémem skrytá. V kontextu funkce detekce narušení chodu – Runtime Intrusion Detection – technologie HP Sure Start nazýváme tento kód také „runtime“ kódem systému BIOS. (Další podrobnosti o režimu SMM a způsobu jeho práce viz přílohu B na straně 12.)

Neporušenost kódu SMM je pro zabezpečení klientského zařízení kriticky důležitá. HP Sure Start při spuštění operačního systému provádí kontroly neporušenosti kódu HP SMM BIOS. Funkce detekce narušení chodu poskytuje mechanismy, které zajistí, že kód BIOS systému SMM zůstane neporušený v době, kdy je systém spuštěn, přidáním nových ochranných funkcí a/nebo poskytnutím prostředků k detekci jakéhokoli útoku na tento kód.

Architektura funkce detekce narušení chodu Runtime Intrusion Detection

Funkce RTID využívá specializovaný hardware v čipové sadě platformy k odhalení anomálií v systému Runtime HP SMM BIOS. Detekce všech anomálií vede k upozornění předanému hardwaru HP Endpoint Security Controller, který může podniknout konfigurovanou taktickou akci nezávisle na CPU.

Obrázek 2. Detekce narušení chodu používá speciální hardware vložený do čipové sady platformy ke sledování jakýchkoli změn kódu SMM.



Uživatelská upozornění, protokolování událostí a správa zásad

Upozorňování koncového uživatele HP Sure Start

Za běžných provozních podmínek je nástroj HP Sure Start uživateli neviditelný. Operace obnovy jsou automatické s použitím výchozích nastavení, přičemž pokud HP Sure Start zjistí problém, při obnově obvykle nevyžaduje žádnou interakci koncového uživatele ani IT.

Uživatelé mohou vidět upozornění v případě, že je za chodu operačního systému rozpoznán problém s integritou systému BIOS pomocí dynamické ochrany HP Sure Start Dynamic Protection nebo funkce Runtime Intrusion Detection. Je-li zjištěna jakákoli významná událost nebo je provedena významná akce, program HP Sure Start zobrazí při příštím spuštění operačního systému varovnou zprávu prostřednictvím oznámení systému Windows®. K aktivaci těchto upozornění systému Windows musí být povolen software HP Notifications.

Protokolování událostí HP Sure Start

Hardware HP Endpoint Security Controller zaznamenává kritické události související s kódem firmwaru / systému BIOS a s daty sledovanými softwarem HP Sure Start. Tyto události se ukládají v energeticky nezávislém paměťovém úložišti HP Sure Start. Tyto události jsou z hardwaru HP ESC zkopírovány do Prohlížeče událostí systému Windows, je-li nainstalován software HP Notifications Software, který usnadňuje přístup místního uživatele a také zákazníkem preferovaného zástupce správy k těmto událostem.

Následující události aktivují software HP Notifications Software, aby shromáždil všechny události z podsystému HP Sure Start a zajistil, že Prohlížeč událostí systému Windows bude aktualizován veškerými událostmi, které dosud nebyly zaznamenány:

- zavedení systému Windows,
- obnovení činnosti systému Windows ze stavu spánku/hibernace,
- upozornění na události za chodu systému ze strany softwaru HP Sure Start s dynamickou ochranou,
- detekce průniku za chodu Runtime Intrusion Detection (RTID).

Software HP upozorňování zapíše události HP Sure Start do jedinečného protokolu událostí aplikace „HP Sure Start“. Do tohoto protokolu budou zahrnuty pouze události softwaru HP Sure Start. Cesta Prohlížeče událostí Windows k událostem HP Sure Start je tato: System Tools/Event Viewer/Applications and Services Logs/HP Sure Start.

Kategorie úrovní v Prohlížeči událostí Windows Event, které souvisejí s událostmi HP Sure Start, jsou definovány v tabulce dále.

Události jsou vyplněny v Prohlížeči událostí Windows v pořadí, ve kterém byly vygenerovány softwarem HP Sure Start. Nejstarší událost v podsystému HP Sure Start se do Prohlížeče událostí systému Windows přidá jako první a nejnovější událost se přidá nakonec.

Časová razítka záznamů v Prohlížeči událostí Windows obsahují čas, kdy byla událost přidána do daného protokolu, NE čas, kdy k události došlo. Každý záznam programu Sure Start v Prohlížeči událostí Windows zahrnuje podrobné údaje v rámci podrobností události; v těchto údajích je také uvedeno časové razítko skutečného výskytu události.

Poznámka: Události přetrvávají v řadiči HP Endpoint Security Controller i po jejich zkopírování do Prohlížeče událostí systému Windows. Po vymazání obsahu Prohlížeče událostí systému Windows nahradí aplikace HP Notifications Software všechny záznamy softwaru HP Sure Start při příští události, která ji spustí, aby zkontrolovala protokoly událostí HP Sure Start.

Typy událostí HP Sure Start v Prohlížeči událostí Windows:

Úroveň události	Definice
Informace	Události, u kterých se očekává, že se vyskytnou za běžného provozu (například aktualizace systému BIOS).
Varování	Neočekávané události, které se vyskytly, ale byly plně obnoveny softwarem HP Sure Start a není třeba, aby uživatel/správce provedl jakoukoli akci, aby byla daná platforma plně funkční. Tyto události jsou anomální operace, které uživatel/správce může chtít dále prošetřit, zejména pokud existuje trend těchto událostí ve více počítačích.
Chyba	Události, které vyžadují, aby správce/servis HP jednal na dané platformě, aby se plně zotavila.

Ovládání zásad HP Sure Start

Při dodání umožňuje systém HP BIOS stanovení zásad softwaru HP Sure Start pro typického uživatele a optimalizuje je. Protože software HP Sure Start je ve výchozím stavu aktivní, není třeba, aby běžný uživatel upravoval nastavení, aby byl chráněn softwarem HP Sure Start. Pokročilým uživatelům poskytuje systém BIOS několik ovládacích prvků, které řídí chování softwaru HP Sure Start, a to pomocí nastavení zásad v nastavení systému BIOS (F10). Není-li uvedeno jinak, tato nastavení a funkce se nacházejí v části Zabezpečení / BIOS Sure Start.

Poznámka: Zásady jsou uloženy v energeticky nezávislé paměti HP ESC, která není přímo přístupná z hostitelské jednotky CPU; proto je vždy třeba znovu spustit systém, aby se mohla nastavení Sure Start projevit.

K dispozici jsou následující nastavení a funkce softwaru HP Sure Start:

- ověření zaváděcího bloku při každém zavádění systému,
- zásady obnovy dat systému BIOS,
- obnovení konfigurace síťového adaptéru (pouze Intel),
- výzva ke změně konfigurace síťového adaptéru (pouze Intel),
- dynamické skenování zaváděcího bloku za chodu systému (pouze Intel),
- ochrana nastavení systému BIOS v softwaru HP Sure Start,
- ochrana klíčů bezpečného zavádění systému v softwaru HP Sure Start,
- rozšířená prevence a detekce průniku do firmwaru HP za chodu systému (pouze Intel),
- detekce průniku do firmwaru HP za chodu systému (pouze AMD),
- zásady událostí zabezpečení softwaru HP Sure Start,
- upozornění na událost zabezpečení při zavádění systému v softwaru HP Sure Start,
- uzamčení verze systému BIOS,
- uložení/obnovení MBR pevného disku systému,
- uložení/obnovení GPT pevného disku systému,
- zásady obnovení zaváděcího sektoru (MBR/GPT).

Ověření zaváděcího bloku při každém zavádění systému

Před obnovením činnosti počítače ze spánku, hibernace nebo vypnutého stavu software HP Sure Start vždy ověří neporušenost zaváděcího bloku BIOS v systémové paměti flash. Je-li nastaven jako **aktivní**, ověří software HP Sure Start také neporušenost zaváděcího bloku při každém měkkém rebootu (restart systému Windows). Co je třeba zvažovat, je rychlejší restart systému proti vyššímu zabezpečení. Výchozím nastavením této funkce je **neaktivní**.

Zásady obnovení dat systému BIOS

Je-li software HP Sure Start nastaven na **Automaticky**, je-li to třeba, opravuje automaticky systém BIOS nebo jednoznačná data počítače (Machine Unique Data). Je-li software HP Sure Start nastaven na **Ručně**, vyžaduje speciální posloupnost kláves, aby pokračoval s opravou. V případě problémů s kódem zaváděcího bloku se systém odmítne zavést a systémová kontrolka LED bude blikat jednoznačnou posloupností záblesků. V případě problému s jednoznačnými daty počítače Machine Unique Data zobrazí systém na obrazovce odpovídající zprávu. Požadovaná posloupnost kláves a posloupnost zobrazených záblesků se liší podle toho, zda je daný systém notebook, stolní počítač nebo tablet. Ruční režim je užitečný pro uživatele, kteří mohou před opravou provádět forenzní výzkum obsahu systémové paměti flash. Typičtí uživatelé by neměli používat ruční režim ovládání. Výchozím nastavením této funkce je **Automaticky**.

Obnovení konfigurace síťového adaptéru (pouze Intel)

Tento ovládací prvek je dostupný jen v systémech Intel. Pokud tuto možnost vyberete, software HP Sure Start okamžitě obnoví konfiguraci síťového adaptéru na výchozí nastavení z výroby.

Výzva ke změně konfigurace síťového adaptéru (pouze Intel)

Toto nastavení je dostupné jen v systémech Intel. HP poskytuje z výroby definovanou konfiguraci síťového adaptéru, která zahrnuje adresu MAC. Je-li toto nastavení **aktivní**, systém monitoruje stav konfigurace síťové karty a vyzve uživatele v případě změny ze stavu konfigurovaného ve výrobě. Výchozím nastavením této funkce je **neaktivní**.

Dynamické skenování zaváděcího bloku za chodu systému (pouze Intel)

Toto nastavení je dostupné jen v systémech Intel. Je-li výchozí nastavení **aktivní**, software HP Sure Start pravidelně kontroluje za chodu operačního systému neporušenost zaváděcího bloku systému BIOS. Je-li nastavení **neaktivní**, software HP Sure Start kontroluje neporušenost pouze před zaváděním systému nebo obnovením jeho činnosti v režimu spánku nebo hibernace.

Ochrana nastavení systému BIOS softwarem HP Sure Start

Výchozím nastavením této zásady ochrany systému BIOS funkce je **neaktivní**. Chcete-li tuto funkci aktivovat, vlastník/správce klientského zařízení musí nejdříve konfigurovat všechny zásady systému BIOS na preferovaná nastavení. Vlastník/správce také musí konfigurovat heslo správce systému BIOS, aby mohl používat ochranu nastavení systému BIOS v softwaru HP Sure Start.

Po skončení je třeba změnit zásadu ochrany nastavení systému BIOS na „aktivní“. V tomto okamžiku se v chráněné paměti softwaru HP Sure Start vytvoří záložní kopie všech nastavení systému BIOS. Při dalším postupu nelze upravit žádné nastavení systému BIOS lokálně a ani ze vzdáleného místa. Při každém zavádění systému se ověřují nastavení zásad systému BIOS, zda jsou v požadovaném stavu, a v případě nesrovnalosti se nastavení systému BIOS obnoví z chráněného úložiště HP Sure Start.

Chcete-li změnit nastavení systému BIOS, musí být zadáno heslo správce systému BIOS a ochrana nastavení systému BIOS později zakázána. V tomto okamžiku lze provést změny nastavení systému BIOS.

Ochrana klíčů bezpečného zavádění systému v softwaru HP Sure Start

Toto nastavení je ve výchozím stavu z výroby **povoleno** a HP Sure Start tak poskytuje rozšířenou ochranu bezpečných zaváděcích databází a klíčů používaných systémem BIOS k ověření neporušenosti a autenticity zavaděče operačního systému před jeho spuštěním při zavádění. Je-li nastavena možnost **zakázat**, použije se pouze standardní ochrana proměnné bezpečného zavádění UEFI a podsystém HP Sure Start nezachovává žádnou záložní kopii.

Rozšířená prevence a detekce průniku do firmwaru HP za chodu systému (pouze Intel) a Detekce průniku do firmwaru HP za chodu systému (pouze AMD)

Funkce RTID je ve výchozím stavu **aktivní** pro všechny platformy dodávané z výrobních závodů HP. Není třeba, aby koncový uživatel/správce aktivoval nebo jinak „využíval“ tuto funkci, aby mohl s výhodou využívat HP Sure Start RTID.

Funkci RTID může vlastník/správce volitelně nastavit na **zakázat**.

Zásady událostí zabezpečení softwaru HP Sure Start

Toto nastavení zásad systému BIOS řídí, jaká akce bude podniknuta, pokud software HP Sure Start detekuje útok nebo pokus o útok za chodu operačního systému. Pro tuto zásadu se nabízejí tři možné konfigurace:

- **Log event only** (Pouze protokolovat události): Když je vybráno toto nastavení, HP ESC zaznamená detekované události, které si lze prohlížet v Prohlížeči událostí systému Microsoft Windows na cestě protokolů aplikací a služeb Applications and Services Logs/HP Sure Start.[3]
- **Log event and notify user** (Protokolovat a informovat uživatele): Toto je výchozí nastavení. Když je vybráno toto nastavení, HP ESC zaznamená detekované události, které si lze prohlížet v Prohlížeči událostí systému Microsoft Windows na cestě protokolů aplikací a služeb Applications and Services Logs / HP Sure Start. Systém navíc v systému Windows upozorní uživatele, že došlo k dané události.[4]
- **Log event and power off system** (Protokolovat událost a vypnout systém): Když je vybráno toto nastavení, HP ESC zaznamená detekované události, které si lze prohlížet v Prohlížeči událostí systému Microsoft Windows na cestě protokolů aplikací a služeb Applications and Services Logs / HP Sure Start. Navíc je uživatel v systému Windows upozorněn, že nastala předmětná událost, a systém se okamžitě vypne.

Upozornění na událost zabezpečení při zavádění systému v softwaru HP Sure Start

Tato zásada systému BIOS řídí, zda varování a chybové zprávy softwaru HP Sure Start, které se zobrazují při zavádění systému, vyžadují potvrzení chyby od uživatele, než bude zavádění systému pokračovat. S výchozím nastavením **Require Acknowledgement** (Požadovat potvrzení) se systém zastaví se zobrazenou chybovou zprávou. Aby zavádění systému pokračovalo, musí místní uživatel stisknout klávesu. Jestliže bude nastavení změněno na **Time out after 15 seconds** (Časová prodleva uplyne po 15 sekundách), zobrazí se zpráva, ale proces zavádění systému automaticky pokračuje po zobrazení dané zprávy na 15 sekund.

Uzamčení verze systému

V nastavení systému BIOS (F10) je tato funkce součástí Main/Update System BIOS.

Je-li nastavena na **zakázat**, můžete aktualizovat systém BIOS kterýmkoli podporovaným procesem. Jestliže HP ESC detekuje platnou aktualizaci zaváděcího bloku v systémové paměti flash, aktualizuje záložní kopii zaváděcího bloku.

Je-li nastavena na **aktivní**, všechny nástroje aktualizace systému HP BIOS odmítají aktualizovat BIOS. Software HP Sure Start navíc chrání systém BIOS před pokusy o změnu verze odstraněním systémové paměti flash neoprávněným způsobem. HP ESC zaznamenává uzamčenou verzi systému BIOS. Jestliže HP ESC detekuje změnu systému BIOS v systémové paměti flash, přepíše zaváděcí blok systému BIOS kopií zaváděcího bloku HP ESC. Kopie zaváděcího bloku HP ESC spustí a obnoví zbytek správné verze systému BIOS. Výchozím nastavením této funkce je **neaktivní**.

Uložení/obnovení MBR pevného disku systému a Uložení/obnovení GPT pevného disku systému

V nastavení systému BIOS (F10) je tato funkce součástí nabídky Security / Hard Drive Utilities (Zabezpečení / Nástroje pevného disku) K dispozici je jen jedna z těchto možností, a to v závislosti na typu diskového oddílu sekce primárního disku (GPT nebo MBR), jak se detekuje v softwaru HP Sure Start.

Je-li nastavena možnost **povolit**, program HP Sure Start uchovává chráněnou záložní kopii tabulky oddílů MBR/GPT z primární jednotky a porovná záložní kopii s primární hodnotou v každém zavádění systému. Jestliže zjistí rozdíl, vyzve uživatele a ten se může rozhodnout, zda se provede obnovení na původní stav ze zálohy, nebo zda se bude změnami aktualizovat chráněná záložní kopie. Zásady **Boot Sector (MBR/GPT) Recovery Policy** (Zásady obnovení zaváděcího sektoru (MBR/GPT)) lze používat volitelně o odebrání rozhodnutí uživatele v souvislosti s akcí, která byla provedena v případě rozdílu zjištěného softwarem Sure Start.

Je-li nastavena možnost **zakázat** (výchozí), nebude software HP Sure Start poskytovat žádnou ochranu MBR/GPT.

Zásady obnovení zaváděcího sektoru (MBR/GPT)

Je-li tato zásada nastavena na **Local User Control** (Kontrola místního uživatele) (výchozí nastavení), systém vyzve uživatele, aby zvolil akci, která bude provedena, když software HP Sure Start detekuje změnu v tabulce diskového oddílu MBR/GPT. Je-li nastavena na **Recover in the event of corruption** (Při porušení obnovit), software HP Sure Start při zjištění rozdílů vždy automaticky obnoví MBR/GPT na uložený stav.

Vzdálená správa ovládání zásad HP Sure Start

Při dodání jsou zásady softwaru HP Sure Start optimalizovány pro typického uživatele. Protože software HP Sure Start je ve výchozím stavu aktivní, není třeba, aby vzdálený správce zaváděl jakékoli akce k aktivaci (nebo „zavedení“) softwaru HP Sure Start. Pokud chce vzdálený správce změnit nastavení zásad softwaru HP Sure Start, lze ke správě zásad HP Sure Start používat stejné rozhraní API systému Windows Management Instrumentation (WMI) nebo skripty konfigurace HP BIOS Configuration Utility, které se používají ke správě jiných zásad platformy BIOS. Správci navíc mohou vzdáleně spravovat funkce softwaru HP Sure Start pomocí modulu doplňku Manageability Integration Kit (MIK) pro správce konfigurace systému Microsoft System Center Configuration Manager (SCCM).

Správci navíc mohou vzdáleně spravovat funkce softwaru HP Sure Start a zobrazovat události HP Sure Start pomocí modulu doplňku Manageability Integration Kit (MIK) pro správce konfigurace systému Microsoft System Center Configuration Manager (SCCM).

Závěr

HP Sure Start přináší tyto klíčové výhody:

- **Nepřerušovaná produktivita** – HP Sure Start udržuje kontinuitu v podniku v případě útoku nebo náhodného porušení tím, že eliminuje dobu výpadku při čekání na událost IT/servisu.
- **Nižší náklady** – Schopnost obnovy softwaru HP Sure Start automaticky snižuje počet volání pracovníkům IT Help Desk a zvyšuje produktivitu, což zase jednoznačně pomáhá snižovat náklady na údržbu dané platformy.
- **Klidná mysl** – Software HP Sure Start nabízí několik funkcí zabezpečení, které pracují v širokém spektru softwarových a hardwarových platforem.

Chraňte kriticky důležitý firmware systému BIOS před malwarem používáním špičkového firmwaru k detekci a automatickým opravám, jaké nabízí software HP Sure Start, který je k dostání výhradně na vybraných počítačích HP Elite.

Příloha A – HP Sure Start, podrobné informace

Společnost HP představila funkci HP Sure Start v roce 2014. Od té doby společnost HP zdokonalila software Sure Start a rozšířila spektrum výrobků, které ho využívají. Tabulka dole přináší přehled možností, které byly přidány do jednotlivých generací softwaru.

Generace	Datum uvedení na trh	Přidané možnosti
HP Sure Start	2014	• Vynucování autenticity firmwaru a systému BIOS se schopností samostatné léčby • Sledování a shoda firmwaru
Software HP Sure Start s dynamickou ochranou Dynamic Protection	2015	• Podpora Prohlížeče událostí systému Windows • Dynamická ochrana (pro vybrané produkty Intel)
HP Sure Start Gen3 (vybrané produkty Intel)[5] HP Sure Start s detekcí průniku za chodu systému (vybrané produkty AMD)[6]	2017	• Detekce průniku za chodu systému • Ochrana nastavení systému BIOS • Doplněk Manageability Integration Kit (MIK) pro Microsoft SCCM
HP Sure Start Gen4[7]	2018	• Chráněná paměť – silné kryptografické metody k ukládání nastavení systému BIOS, uživatelských oprávnění a dalších nastavení v hardwaru HP Endpoint Security Controller k zajištění ochrany integrity, detekci pokusu o manipulaci a ochraně důvěrnosti těchto dat • Ochrana bezpečné databáze zavádění – rozšířená ochrana databází a klíčů uložených systémem BIOS, kriticky důležitých k zajištěné neporušenosti funkce bezpečného zavádění operačního systému ve srovnání se standardní implementací UEFI BIOS • Na platformách Intel zvýšená ochrana a obnovení firmwaru správy počítače Intel Management Engine • Certifikace hardwaru HP Endpoint Security Controller nezávislou institucí – testování nezávislou a akreditovanou laboratoří, která potvrdila základní funkčnost hardwaru HP ESC na základě veřejně dostupných kritérií, metodiky a procesů[1] • Podnikové počítače HP se softwarem HP Sure Start překonaly požadavky směrnice odolnosti firmwaru platforem Draft NIST Platform Firmware Resiliency (speciální vydání 800-193)

Příloha B – přehled režimu správy SMM (System Management Mode)

System Management Mode (SMM) je standardní přístup používaný v tomto odvětví pro pokročilé funkce řízení napájení počítačů a dalších funkcí nezávislých na operačním systému za chodu operačního systému. Třebaže pojem SMM a jeho implementace jsou specifické pro architektury x86, mnoho moderních výpočetních konfigurací používá podobné koncepce architektury.

SMM je konfigurován systémem BIOS během zavádění systému. Kód SMM se přenese do hlavní paměti (DRAM) a poté použije BIOS speciální (uzamykatelné) registry konfigurace uvnitř čipové sady k zablokování přístupu do dané oblasti, pokud mikroprocesor nepracuje v kontextu SMM. Za chodu systému je vstup do režimu SMM řízen událostmi. Čipová sada je naprogramována tak, aby rozpoznávala řadu typů událostí a prodlev. Pokud nastane taková událost, hardware čipové sady nastaví vstupní kontakt přerušení SMI (System Management Interrupt). V mezích další instrukce uloží mikroprocesor celý svůj stav a vstoupí do režimu SMM.

Jakmile mikroprocesor vstoupí do režimu SMM, nastaví výstupní hardwarový kontakt jako SMI Active (SMIACT). Tento kontakt slouží jako upozornění pro hardware čipové sady, že mikroprocesor vstupuje do režimu SMM. SMI lze nastavit kdykoli, během libovolného provozního režimu procesu s výjimkou samotného režimu SMM. Hardware čipové sady rozpozná signál SMIACT a přesměruje všechny následující paměťové cykly do chráněné oblasti paměti (někdy označované jako oblast SMRAM), která je rezervována speciálně pro SMM. Bezprostředně po přijetí vstupu SMI a nastavení výstupu SMIACT začne mikroprocesor ukládat celý svůj vnitřní stav do této chráněné oblasti paměti.

Po uložení stavu mikroprocesoru do paměti SMRAM se začne provádět speciální kód zpracování SMM, který je rovněž uložen v paměti SMRAM (který byl uložen systémem BIOS v době zavádění); zpracování probíhá ve speciálním provozním režimu SMM. Během práce v tomto režimu je většina mechanizmů izolace hardwaru a paměti pozastavena a mikroprocesor může přistupovat prakticky ke všem zdrojům v platformě, aby mohl provádět požadované úlohy. Kód SMM dokončí požadovaný úkol a pak je čas vrátit mikroprocesor do předchozího provozního režimu. V tomto okamžiku kód SMM provede příkaz Return from System Management Mode (RSM) a ukončí tak zpracování v režimu SMM. Instrukce RSM způsobí, že mikroprocesor obnoví své předchozí interní stavové údaje z kopie uložené v paměti SMRAM po vstupu do režimu SMM. Po dokončení RSM byl celý stav mikroprocesoru obnoven do stavu těsně před událostí SMI a předchozí program (OS, aplikace, hypervizor apod.) pokračuje v provádění přesně v místě, kde byl přerušen.

[1] Hardware řadiče HP Sure Start byl certifikován podle certifikačního rámce CSPN.

[2] Program HP Sure Start s dynamickou ochranou je k dispozici v produktech HP Elite vybavených procesory Intel Core 6. generace a vyššími.

[3] Chcete-li zobrazovat události HP Sure Start v Prohlížeči událostí systému Windows, je třeba nainstalovat software HP Notification Software.

[4] Software HP Notification musí být instalován, aby bylo možné přijímat upozornění.

[5] HP Sure Start Gen3 se dodává v produktech HP Elite vybavených procesory Intel 7. generace.

[6] HP Sure Start Gen3 s detekcí průniku za chodu operačního systému se dodává v produktech HP Elite vybavených procesory AMD 7. generace.

[7] HP Sure Start Gen4 se dodává v produktech HP Elite a HP Pro 600 vybavených procesory Intel nebo AMD 8. generace.

Podrobnější informace viz
hp.com/go/computersecurity

4AA7-3172CSCI, Směr 2018