Informacje techniczne

HP Sure Start

Automatyczna ochrona oraz naprawa na poziomie systemu BIOS

Może 2018 r.

Spis treści

Dlaczego ochrona na poziomie systemu BIOS jest ważna? 03

HP Sure Start zapewnia ochronę oprogramowania układowego na najwyższym poziomie 04

Przegląd architektury i możliwości 05

- Weryfikacja spójności oprogramowania układowego — zasadnicze działanie systemu HP Sure Start 05
- Unikalna spójność danych maszyny 05
- Region deskryptora 06
- Ochrona kontrolera sieci 06
- Zabezpieczenie ustawień BIOS 06
- Chroniona pamięć HP Sure Start 06
- Ochrona kluczy rozruchu bezpiecznego 07
- Wykrywanie włamań w trakcie pracy urządzenia (RTID) 07

Powiadomienia użytkownika, rejestrowanie zdarzeń, zarządzanie zasadami 08

- Powiadomienia dla użytkownika końcowego HP Sure Start 08
- Rejestrowanie zdarzeń HP Sure Start 08
- Zarządzanie zasadami HP Sure Start 09
- Zdalne zarządzanie zasadami HP Sure Start 10

Podsumowanie 11

Załącznik A — generacje HP Sure Start 11

Załącznik B — przegląd kodu System Management Mode (SMM) 12

Wprowadzenie

HP Sure Start może automatycznie wykryć atak lub uszkodzenie systemu BIOS, zatrzymać go i odzyskać sprawność systemu bez interwencji działu IT, przy nieznacznym lub zupełnym braku wpływu na pracę użytkownika. Za każdym razem, gdy komputer się włącza, HP Sure Start automatycznie weryfikuje spójność kodu BIOS, tak aby pomóc chronić komputer przed złośliwymi atakami. Gdy komputer już działa, funkcja wykrywania nieautoryzowanego dostępu stale monitoruje pamięć. W razie ataku komputer może sam się wyleczyć, korzystając z wyodrębnionej „złotej kopii" systemu BIOS w czasie poniżej minuty.

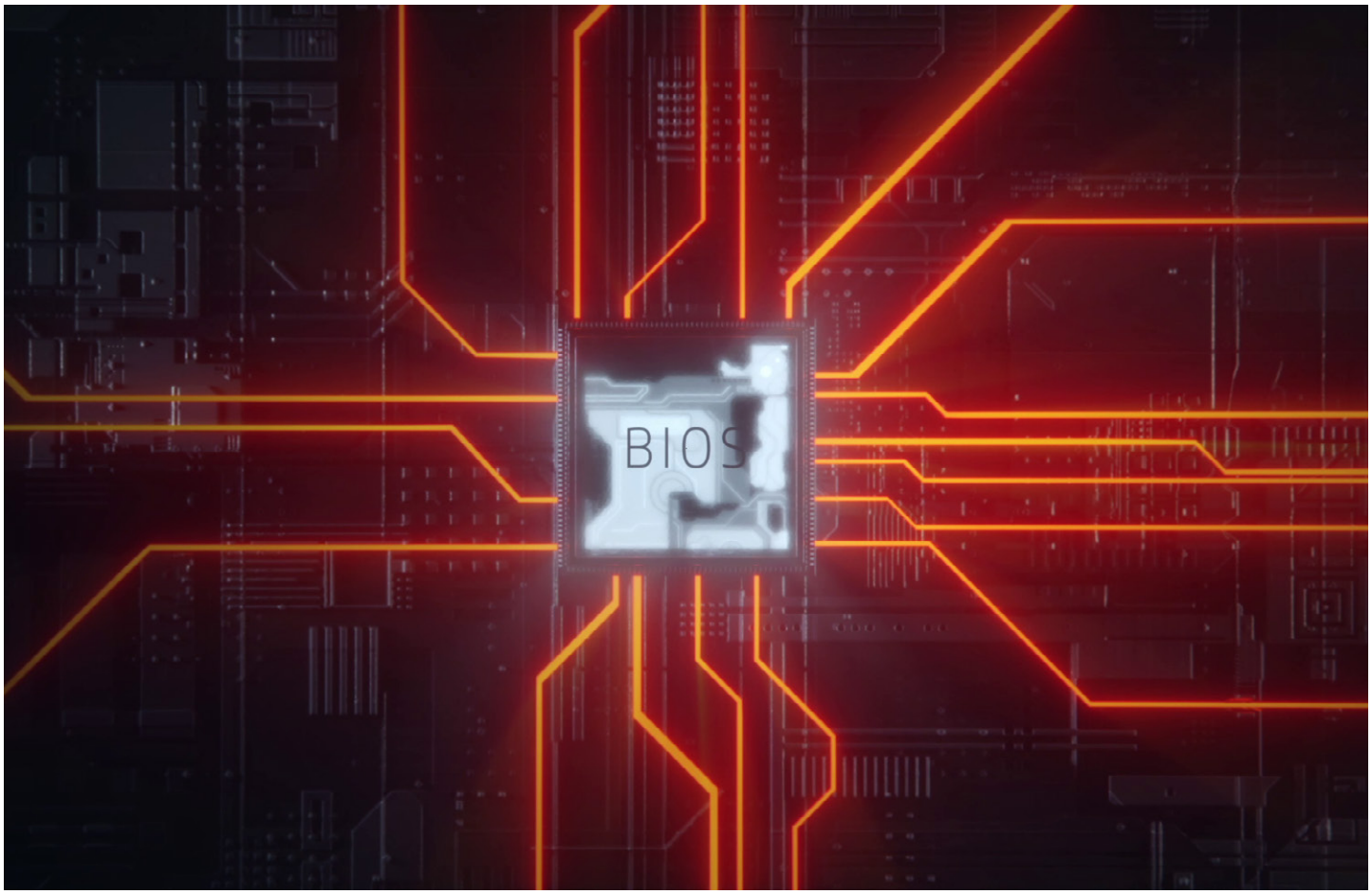
Dlaczego ochrona na poziomie systemu BIOS jest ważna?

Ponieważ nasz świat jest opleciony coraz gęstszą siecią połączeń, cyberataki na oprogramowanie układowe oraz urządzenia są coraz częstsze i coraz bardziej złożone. Narzędzia i metody ataków na oprogramowanie układowe kiedyś były rozważane tylko w aspekcie teoretycznym. Sądzono wówczas, że wyłącznie państwa dysponowałyby środkami odpowiednimi do ich przeprowadzenia. Obecnie wiadomo już, że takie narzędzia i metody nie tylko istnieją, ale są dostępne w sferze publicznej.

Oprogramowanie układowe urządzenia (czyli BIOS) to atrakcyjny cel dla hakerów ze względu na korzyści wynikające z zakończonego powodzeniem ataku.

- Trwałość: Oprogramowanie układowe jest zapisane w pamięci trwałej na płytce obwodu drukowanego i nie można go usunąć poprzez zwykłe usunięcie danych z dysku twardego.
- Kontrola: Oprogramowanie układowe działa na najwyższym poziomie uprawnień — poza domeną systemu operacyjnego, która umożliwia działanie złośliwego oprogramowania niezależne od systemu operacyjnego.
- Niewidoczność: Oprogramowanie układowe zajmuje część pamięci zupełnie niedostępną dla systemu operacyjnego oraz oprogramowania systemu. Ponieważ programy antywirusowe nie mogą skanować tej części pamięci, nie mogą też wykryć tutaj zagrożeń.
- Trudności w odzyskiwaniu: Wymienione powyżej aspekty sprawiają, że bardzo trudno odzyskać system po takim rodzaju infekcji. Zazwyczaj komputer trzeba oddać do naprawy i często wymagana jest nawet wymiana płyty systemowej.

Idealne rozwiązanie do ochrony urządzeń przed tego typu atakami powinno być przygotowane już na poziomie sprzętowym przy zastosowaniu zasad „odporności na cyberataki". Te zasady opierają się na założeniu, że przewidzenie każdego ewentualnego ataku i zapobieżenie mu jest niezwykle trudne, jeśli nie niemożliwe. Idealne rozwiązanie powinno zapewniać ulepszoną ochronę oprogramowania układowego przy jednoczesnej zdolności sprzętowej do wykrycia zakończonego sukcesem ataku, a także odzyskania sprawności po nim.



HP Sure Start zapewnia ochronę oprogramowania układowego na najwyższym poziomie

HP Sure Start to wyjątkowe i przełomowe rozwiązanie firmy HP do zaawansowanej ochrony oprogramowania układowego komputerów marki HP oraz zapewnienia jego odporności na ataki. Rozwiązanie korzysta z wymuszania sprzętowego za pomocą HP Endpoint Security Controller (HP ESC), aby zapewnić ochronę systemu BIOS, która znacznie wykracza poza standardy branżowe i gwarantuje, że rozruch komputera będzie się odbywał wyłącznie za pomocą oryginalnego systemu BIOS firmy HP. Ponadto jeśli HP Sure Start wykryje manipulację systemem BIOS, oprogramowaniem układowym lub kodem środowiska uruchomieniowego BIOS System Management Mode (SMM), rozwiązanie może przywrócić sprawność przy wykorzystaniu chronionej kopii zapasowej.

Zestawienie funkcji rozwiązania HP Sure Start

- Ochrona oprogramowania układowego podstawowej platformy HP przed naruszeniem oraz wymuszanie autentyczności — wymuszanie sprzętowe rozruchu systemowego przez HP Endpoint Security Controller, dzięki czemu ładowane jest tylko autentyczne i niezmodyfikowane oprogramowanie układowe BIOS firmy HP
- Monitorowanie stanu i zgodność oprogramowania układowego — zapisywanie w pliku dziennika zdarzeń powiązanych ze stanem oprogramowania układowego przez odizolowany kontroler HP Endpoint Security Controller; pokazuje stan oprogramowania układowego platformy wraz z wszelkimi anomaliami, które mogłoby wskazywać na udaremnione ataki
- Samonaprawianie — automatyczna naprawa naruszenia BIOS firmy HP oraz oprogramowania układowego HP przy wykorzystaniu odizolowanej przez kontroler HP Endpoint Security Controller kopii zapasowej BIOS i oprogramowania układowego HP
- Ochrona ustawień systemu BIOS — rozszerzona ochrona kodu BIOS sprawowana przez kontroler HP Endpoint Security Controller, obejmująca kopię zapasową HP ESC oraz kontrolę spójności wszystkich ustawień użytkownika i administratora skonfigurowanych w systemie BIOS
- Wykrywanie nieautoryzowanego dostępu do środowiska uruchomieniowego — stałe monitorowanie mającego kluczowe znaczenie kodu BIOS w pamięci środowiska uruchomieniowego (SMM) podczas pracy systemu operacyjnego
- Ochrona kluczy bezpiecznego rozruchu — znacznie poprawiona ochrona bazy danych i kluczy zapisanych przez system BIOS, które są kluczowe dla spójności funkcji bezpiecznego rozruchu systemu operacyjnego w porównaniu ze standardowym UEFI BIOS
- Ochrona pamięci — HP Sure Start korzysta z silnych metod kryptograficznych do zapisywania ustawień BIOS, poświadczeń użytkownika, a także innych ustawień sprzętowych kontrolera HP Endpoint Security Controller, aby zapewnić ochronę spójności, wykrywanie naruszeń oraz ochronę poufności tych danych
- Ochrona oprogramowania układowego Intel® Management Engine (silnik zarządzania Intel®) — poprawiona ochrona i przywracanie oprogramowania układowego Intel Management Engine
- Możliwość zarządzania — administratorzy mogą zarządzać funkcjami HP Sure Start za pomocą wtyczki Manageability Integration Kit (MIK) do programu Microsoft® System Center Configuration Manager (SCCM)

Aby zapoznać się z podsumowaniem wszystkich funkcji poszczególnych generacji rozwiązania HP Sure Start, patrz załącznik A na stronie 11.

Certyfikat potwierdzający bezpieczeństwo wydany przez firmę zewnętrzną

Kontroler HP Endpoint Security Controller, działający na poziomie sprzętowym i wykorzystywany przez rozwiązanie HP Sure Start, został poddany ocenie bezpieczeństwa przeprowadzonej przez firmę zewnętrzną. Rozwiązanie uzyskało certyfikat potwierdzający, że zapewnia wymuszenie na poziomie sprzętowym, dzięki któremu autoryzowane oprogramowanie układowe może zostać uruchomione na danym komputerze.[1]

Gwarancja, że rozwiązanie w zakresie bezpieczeństwa działa zgodnie z zapewnieniami producenta ma kluczowe sprzętowym podczas podejmowania decyzji o zakupie tego typu produktów. Ponieważ opinia dotycząca jakości rozwiązania może zostać potwierdzona tylko w ten sposób, firma HP zleciła niezależnemu i akredytowanemu laboratorium ocenę oraz testy wewnętrznych mechanizmów kontrolera HP Endpoint Security. Miało to na celu potwierdzenie na podstawie ogólnie dostępnych kryteriów, metod i procesów, że produkt działa zgodnie z zapewnieniami.

Architektura odporna na cyberataki

Rozwiązanie HP Sure Start zapewnia nie tylko ulepszoną ochronę systemu BIOS wykraczającą poza standardy branżowe, ale także już na poziomie sprzętowym zostało opracowane tak, aby zapewniać niemającą sobie równych odporność na cyberataki oraz aby przywrócenie systemu BIOS było możliwe nawet w razie naruszenia zabezpieczeń lub destrukcyjnego ataku. Komputery HP wyposażone w rozwiązanie HP Sure Start wykraczają poza wymagania ustalone we wstępnych wytycznych instytutu National Institute of Standards Technology (NIST, amerykański Narodowy Instytut Standaryzacji i Technologii) dotyczących odporności oprogramowania układowego platformy na ataki (publikacja specjalna 800-193), które są jednym z głównych środków wdrażanych przez sektor publiczny w celu formalizacji wymogów wobec platform odpornych na cyberataki.

Modele zgodne z rozwiązaniem HP Sure Start

Firma HP wprowadziła rozwiązanie HP Sure Start w 2014 r. Od tamtego czasu firma HP ulepszyła HP Sure Start i rozszerzyła liczbę produktów, które są w nie wyposażone. HP Sure Start jest dostępne w całej linii produktów 2018 Elite, w tym w tabletach, notebookach, komputerach biurkowych oraz AIO (all in one, komputer wielofunkcyjny). Rozwiązanie HP Sure Start 4. generacji jest dostępne w przypadku produktów HP Elite oraz HP Pro 600 wyposażonych w procesory Intel 8. generacji lub AMD®.

Przegląd architektury i możliwości

HP Sure Start składa się z dwóch głównych komponentów:

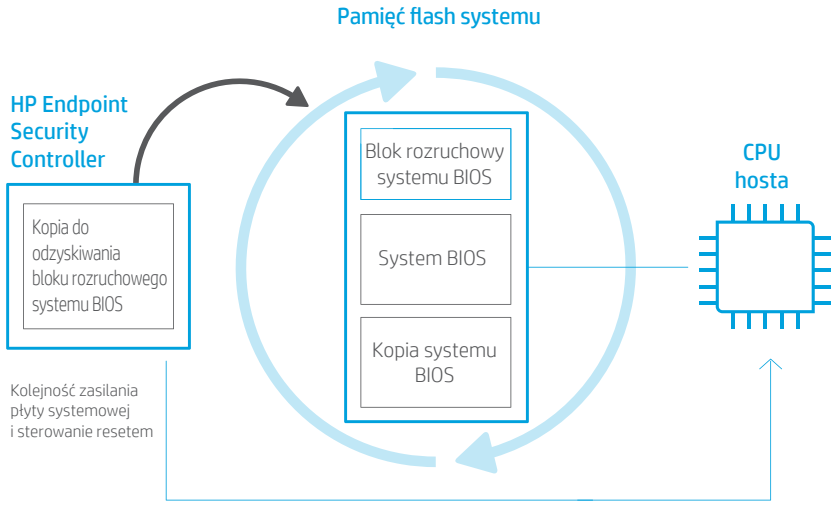
- **Kontrolera HP Endpoint Security Controller** z oprogramowaniem układowym HP Sure Start
- **HP Sure Start BIOS** współpracującego ze sprzętem i oprogramowaniem układowym HP Endpoint Security Controller

Weryfikacja spójności oprogramowania układowego — zasadnicze działanie systemu HP Sure Start

HP Endpoint Security Controller (HP ESC) to pierwsze urządzenie w systemie, które kontroluje oprogramowanie układowe w momencie włączenia zasilania systemu i jest aktywne jeszcze przed jego rozruchem. Działania wykonywane przez HP ESC obejmują m.in. monitorowanie przycisku zasilania, ustalanie kolejności zasilania CPU hosta, gdy użytkownik włącza urządzenie.

Gdy zasilanie jest najpierw doprowadzane do platformy (przed włączeniem systemu), HP ESC sprawdza, czy jego własne oprogramowanie układowe ma autentyczny kod HP przed załadowaniem i wykonaniem kodu.
Sprzęt HP ESC korzysta ze standardowych w branży, silnych metod kryptograficznych w celu przeprowadzenia weryfikacji spójności. W metodzie zastosowano 2048-bitowy publiczny klucz RSA HP, który jest zapisany w wewnętrznej, stałej pamięci tylko do odczytu. Dlatego HP ESC został zastosowany jako zintegrowane, sprzętowe Root of Trust (RoT, źródło zaufania) platformy, używane do weryfikacji jego oprogramowania układowego oraz systemu BIOS HP przed ich wykonaniem. Sprzętowe źródło zaufania chroni przed atakami polegającymi na zamianie oprogramowania układowego niezależnie od metody ich wdrożenia oraz służy za bazę, na której bezpiecznie spoczywa platforma HP.

Ilustracja 1. Proces weryfikacji spójności oprogramowania układowego.



Na ilustracji 1 przedstawiono proces weryfikacji spójności oprogramowania układowego. Po przeprowadzeniu uwierzytelniania przez kontroler HP ESC oraz uruchomieniu przez niego oprogramowania układowego HP Sure Start to oprogramowanie układowe korzysta z takich samych silnych operacji kryptograficznych do weryfikacji bloku rozruchowego BIOS w pamięci flash. Jeśli jeden z bitów jest nieprawidłowy, HP ESC zastępuje zawartość pamięci flash systemu własną kopią bloku rozruchowego systemu BIOS firmy HP, która jest zapisana w odizolowanej pamięci trwałej (NVM) dedykowanej HP ESC.

Architektura rozwiązania HP Sure Start gwarantuje, że całe oprogramowanie układowe oraz kod BIOS działający zarówno na HP ESC, jak i CPU hosta jest kodem HP przeznaczonym do zastosowania na danym urządzeniu.

Uwaga: Kontrola spójności bloku rozruchowego w pamięci flash systemu oraz wszelkie akcje odzyskiwania wykonywane przez HP ESC, odbywają się, gdy CPU jest wyłączony. Dlatego z punktu widzenia użytkownika cała operacja odbywa się, gdy system jest jeszcze wyłączony, w trybie uśpienia lub hibernacji.

Blok rozruchowy BIOS zapisany w pamięci flash jest podstawą systemu BIOS firmy HP. Sprzęt HP ESC gwarantuje, że blok rozruchowy BIOS jest pierwszym kodem wykonywanym przez CPU po resetowaniu. Gdy HP ESC ustali, że blok rozruchowy BIOS zawiera autentyczny kod HP, pozwala systemowi na rozruch, tak jak w normalnej sytuacji.

HP ESC sprawdza ponadto spójność kodu bloku rozruchowego w pamięci flash za każdym razem, gdy system jest wyłączony lub znajduje się trybie hibernacji albo uśpienia. Ponieważ CPU nie jest zasilany w każdym z tych stanów, CPU musi z tego powodu wykonać ponownie kod bloku rozruchowego BIOS. Za każdym razem niezwykle istotne jest ponowne sprawdzenie spójności bloku rozruchowego BIOS pod kątem naruszenia.

Ponadto w przypadku modeli HP Intel rozwiązanie HP Sure Start okresowo (co 15 minut) sprawdza spójność bloku rozruchowego BIOS w pamięci flash podczas pracy systemu.[2]

Unikalna spójność danych urządzenia

HP ESC i BIOS współpracują ze sobą, aby zapewnić zaawansowaną ochronę skonfigurowanych fabrycznie kluczowych zmiennych, które są unikatowe dla każdej maszyny. Powinny one być stałe w całym cyklu życia danej platformy. W fabryce kopia zapasowa tych danych zmiennych jest zapisywana w pamięci trwałej HP ESC. Kopia zapasowa jest dostępna dla komponentu BIOS HP Sure Start w trybie tylko do odczytu w celu wykonania kontroli spójności danych przy każdym rozruchu. Jeśli jedno z ustawień we współdzielonej pamięci flash zostało zmienione w porównaniu z ustawieniami fabrycznymi, komponenty BIOS HP Sure Start automatycznie przywrócą dane w pamięci flash systemu z kopii zapasowej zapewnionej przez HP ESC.

Region deskryptora

W przypadku modeli HP Intel rozwiązanie HP Sure Start chroni region deskryptora pamięci flash systemu. Region deskryptora jest unikatowy dla architektury Intel i zawiera parametry konfiguracji o kluczowym znaczeniu, które są próbkowane przez układ logiki Intel Core™ w momencie resetowania, a następnie wykorzystywane do konfiguracji układu logiki Core. Region deskryptora zawiera również informację o podziale na partycje dla pamięci flash systemu. Informacja ta jest wykorzystywana przez układ logiki Intel Core do ustalenia, gdzie w pamięci flash znajduje się region BIOS oraz w związku z tym skąd CPU uzyskuje kod do wykonania po resecie. HP Sure Start monitoruje spójność tego regionu i przywraca jego właściwą konfigurację w razie manipulacji lub uszkodzenia.

Ochrona kontrolera sieci

Ponadto w przypadku modeli HP Intel rozwiązanie HP Sure Start chroni ustawienia kontrolera sieci (NIC) zapisane w pamięci flash systemu. Niektórzy klienci HP używają sprzętu do zastosowań, które wymagają uzasadnionych zmian w fabrycznie skonfigurowanych ustawieniach NIC. Dlatego HP Sure Start nie zapobiega domyślnie zmianom w ustawieniach NIC. Zamiast tego rozwiązanie HP Sure Start zapewnia funkcję, która po jej aktywacji ostrzega użytkownika o zmianie ustawień NIC. Ponadto HP Sure Start zapewnia metodę przywrócenia ustawień NIC do wartości fabrycznych. Do ustawień chronionych należą adres MAC, ustawienia Pre-boot Execution Environment (PXE, środowisko wykonawcze przed uruchomieniem systemu) oraz zdalne ładowanie programu początkowego (remote initial program load, RPL). Przywrócenie jest możliwe za pomocą kopii zapasowej tylko do odczytu, zabezpieczonej przez HP ESC.

Zabezpieczenie ustawień BIOS

Jak już zostało to opisane powyżej, HP Sure Start weryfikuje spójność oraz autentyczność kodu systemu BIOS firmy HP. Ponieważ kod jest statyczny od momentu utworzenia go przez HP, do potwierdzenia obu tych atrybutów kodu można użyć podpisów cyfrowych. Dynamiczna natura ustawień BIOS oraz możliwość ich konfiguracji przez użytkownika stwarzają jednak dodatkowe wyzwania związane z ich ochroną. HP nie może generować podpisów cyfrowych i wykorzystywać ich w sprzęcie HP Sure Start ESC do weryfikacji tych ustawień.

Zabezpieczenie ustawień BIOS HP Sure Start zapewnia możliwość konfiguracji systemu w taki sposób, że sprzęt HP ESC jest używany do wykonania kopii zapasowej oraz sprawdzenia spójności wszystkich ustawień BIOS wybranych przez użytkownika.

Gdy ta funkcja jest włączona na platformie, wszystkie ustawienia zasad używane przez BIOS są w następstwie zapisywane jako kopia zapasowa oraz wykonywane jest kontrola spójności podczas każdego rozruchu, tak aby upewnić się, że żadne z ustawień zasad BIOS nie zostało zmodyfikowane. W razie wykrycia zmiany system korzysta z kopii zapasowej zapisanej w zabezpieczonej pamięci HP Sure Start do automatycznego przywrócenia ustawień zdefiniowanych przez użytkownika.

Funkcja zabezpieczenia ustawień BIOS realizowana przez rozwiązanie HP Sure Start generuje zdarzenia w sprzęcie HP Sure Start ESC w momencie wykrycia próby modyfikacji ustawień BIOS. Zdarzenie jest zapisywane w dzienniku inspekcji HP Sure Start, a lokalny użytkownik otrzymuje powiadomienie z systemu BIOS w trakcie rozruchu.

Chroniona pamięć HP Sure Start

Chroniona pamięć zawarta w sprzęcie HP Endpoint Security Controller zapewnia najwyższy stopień ochrony ustawień oraz danych systemu BIOS/oprogramowania układowego dzięki rozwiązaniu HP Sure Start. Chroniona pamięć HP Sure Start została opracowana z myślą o zapewnieniu poufności, spójności oraz wykrywania naruszeń nawet w razie ataków fizycznych, w przypadku których haker rozmontuje system i ustanowi bezpośrednie połączenie z urządzeniem pamięci trwałej na płytce obwodu drukowanego.

Spójność danych

Spójność danych dynamicznych zapisanych w pamięci trwałej przez oprogramowanie układowe i wykorzystywanych do sterowania stanem różnych funkcji ma kluczowe znaczenie dla stanu bezpieczeństwa całej platformy. Dane dynamiczne obejmują wszystkie ustawienia systemu BIOS, które mogą być modyfikowane na urządzeniu przez użytkownika końcowego lub administratora. Przykładami takich danych (nie wymieniono tutaj wszystkich możliwości) są opcje rozruchu, jak na przykład funkcja bezpiecznego rozruchu, hasło administratora w systemie BIOS oraz powiązane zasady, kontrola stanu Trusted Platform Module (TPM) oraz ustawienia zasad HP Sure Start.

Wszelkie zakończone sukcesem ataki, które omijają istniejące ograniczenia dostępu mające na celu zapobieganie nieupoważnionym modyfikacjom tych ustawień, mogą naruszyć bezpieczeństwo systemu. Przykładem jest sytuacja, gdy haker dokonuje nieupoważnionej modyfikacji stanu bezpiecznego rozruchu, aby wyłączyć tę funkcję w sposób niemożliwy do wykrycia. W takim przypadku platforma dokonałaby rozruchu rootkita hakera przed uruchomieniem systemu operacyjnego i bez wiedzy użytkownika.

Będący standardem w branży interfejs Unified Extensible Firmware Interface (UEFI, interfejs pomiędzy systemem operacyjnym a oprogramowaniem układowym) BIOS stosuje ograniczenia dostępu, które powinny zapobiegać nieautoryzowanym modyfikacjom tych zmiennych. Firma HP również stosuje ten standard, tak jak cała branża IT.

Biorąc jednak pod uwagę ryzyko dla platformy spowodowane ewentualnym złamaniem tych mechanizmów, w rozwiązaniu HP Sure Start zastosowano drugorzędny system zabezpieczeń, który jest silniejszy niż podstawowy standard branżowy.

Ustawienia BIOS oraz inne dane dynamiczne wykorzystywane przez oprogramowanie układowe w celu sterowania stanem, które są zabezpieczone przez rozwiązanie HP Sure Start, są zapisane w odizolowanej pamięci trwałej kontrolera HP Endpoint Security Controller, do których oprogramowanie działające na CPU hosta nie ma bezpośredniego dostępu.

Ponadto HP ESC tworzy i dołącza unikatowe pomiary spójności za każdym razem, gdy element danych jest zapisywany w tej pamięci trwałej. Pomiary spójności opierają się na silnym algorytmie kryptograficznym (haszowany kod uwierzytelniania wykorzystujący zestaw SHA-256), który znajduje się w tajnym zapisie w HP ESC. Ten tajny zapis jest unikatowy dla każdego HP ESC, dzięki czemu każdy kontroler generuje unikatowy pomiar spójności identycznego elementu.

Gdy element danych jest odczytywany ponownie z pamięci trwałej, HP ESC oblicza pomiar spójności dla niego i porównuje go z pomiarem spójności dołączonym do danych. Nieupoważnione zmiany danych zapisanych w pamięci trwałej dają w wyniku błąd porównania. Stosując takie podejście, HP ESC może wykrywać manipulowanie elementami danych zapisanymi w pamięci trwałej.

Poufność danych

W przypadku wielu elementów zapisanych przez platformę zachowanie poufności ma kluczowe znaczenie. Przykładami takich elementów są: skróty (hashe) hasła administratora systemu BIOS, poświadczenia użytkownika oraz tajne zapisy opcjonalnie zapisane przez oprogramowanie układowe w imieniu użytkownika w celu wykonywania takich funkcji, jak HP Sure Run i HP Sure Recover.

Ochrona tych tajnych zapisów stanowi wyzwanie w przypadku zastosowania standardowego w branży UEFI BIOS, ponieważ pamięć trwała zazwyczaj może być odczytana przez oprogramowanie działające na CPU hosta. Chroniona pamięć HP Sure Start ma na celu zapewnienie znacznie większej ochrony takich poufnych danych niż standardowy tryb UEFI systemu BIOS.

Oprócz oddzielnej, odizolowanej pamięci metoda zastosowana w HP Sure Start obejmuje wykorzystanie bloku sprzętowego Advanced Encryption Standard (AES, symetryczny szyfr blokowy), znajdującego się w HP ESC, w celu wykonania szyfrowania AES-256 na wszystkich poufnych elementach danych zapisanych w pamięci trwałej HP Sure Start. Ponadto przeprowadzane są pomiary spójności danych w przypadku tych elementów. Używany klucz szyfrowania jest unikatowy dla każdego HP ESC i nigdy nie opuszcza kontrolera, dzięki czemu dane zaszyfrowane przez indywidualny komponent HP ESC mogą być odszyfrowane tylko przy użyciu tego samego HP ESC.

Ochrona kluczy rozruchu bezpiecznego

HP Sure Start zapewnia ulepszoną — w porównaniu ze standardowo stosowanym w branży bezpiecznym rozruchem UEFI — ochronę baz danych kluczy bezpiecznego rozruchu UEFI, które są zapisane przez oprogramowanie układowe. Te zmienne są kluczowe dla prawidłowego działania funkcji bezpiecznego rozruchu UEFI, która weryfikuje spójność i autentyczność programu ładującego systemu operacyjnego, zanim pozwoli mu na uruchomienie w momencie rozruchu.

HP Sure Start chroni bazy danych kluczy bezpiecznego rozruchu UEFI, zachowując kopię główną w chronionej pamięci HP Sure Start. Wszelkie autoryzowane modyfikacje baz danych klucza bezpiecznego rozruchu standardu UEFI dokonywane przez system operacyjny w trakcie działania środowiska uruchomieniowego są śledzone przez HP Sure Start i wprowadzane do kopii głównej przez HP ESC. HP Sure Start używa następnie kopii głównej zapisanej w chronionej pamięci HP Sure Start do identyfikacji i odrzucania wszelkich nieautoryzowanych zmian w bazach danych kluczy bezpiecznego rozruchu standardu UEFI.

Ta funkcjonalność, domyślnie włączona, dotyczy następujących baz danych:

- Baza danych podpisów (db)
- Baza danych podpisów odwołanych (dbx)
- Key Enrollment Key (KEK, klucz dostępu)
- Platform Key (PEK, klucz platformy) aktualizowany dynamicznie w trakcie działania środowiska uruchomieniowego przez system operacyjny

Wykrywanie włamań w trakcie pracy urządzenia (RTID)

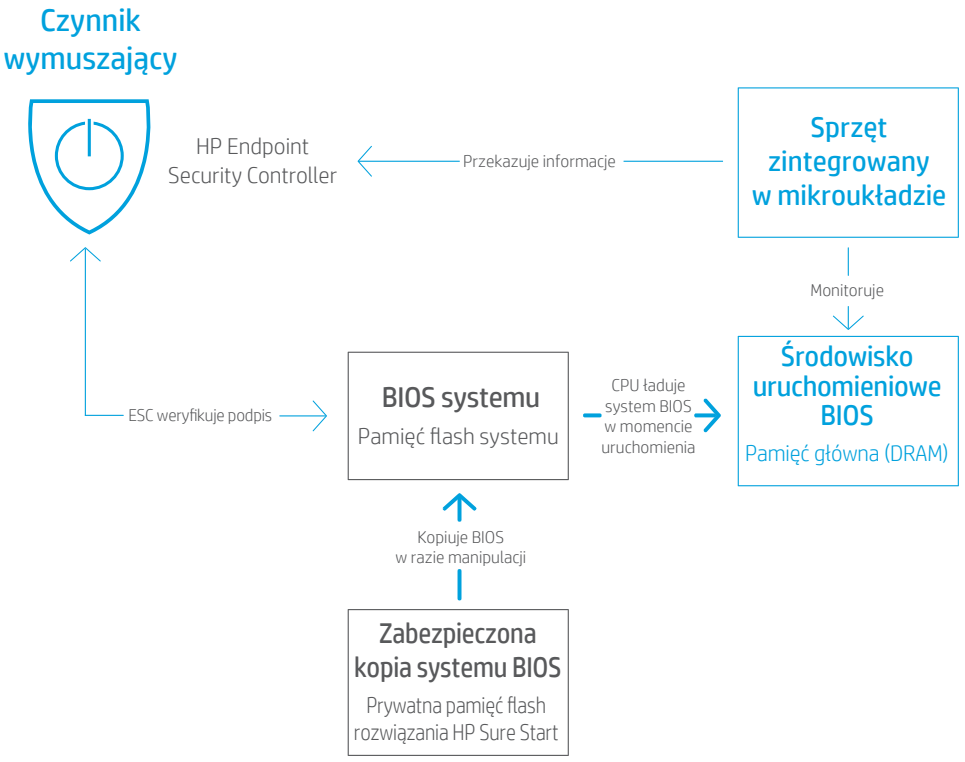
Podczas każdego rozruchu kod BIOS rozpoczyna wykonywanie z pamięci flash w ustalonym adresie. Proces ten nazywany jest kodem rozruchowym BIOS i zapewnia funkcje potrzebne jeszcze przed uruchomieniem systemu operacyjnego. Pewna część systemu BIOS pozostaje jednak w pamięci DRAM, co jest potrzebne do zapewnienia zaawansowanych funkcji zarządzania zasilaniem, usług systemu operacyjnego oraz innych funkcji niezależnych od systemu operacyjnego w trakcie jego działania. Kod BIOS, nazywany inaczej kodem System Management Mode (SMM), jest zapisany w specjalnym obszarze pamięci DRAM, który jest niewidoczny z poziomu systemu operacyjnego. Ten kod jest także czasem określany mianem „środowiska uruchomieniowego" BIOS w kontekście funkcji Runtime Intrusion Detection rozwiązania HP Sure Start (aby dowiedzieć się więcej na temat kodu SMM oraz jego sposobu działania, patrz załącznik B na stronie 12).

Spójność kodu SMM ma kluczowe znaczenie dla stanu bezpieczeństwa urządzenia klienta. HP Sure Start sprawdza, czy kod SMM BIOS firmy HP jest nienaruszony w monecie uruchomienia systemu operacyjnego. Funkcja Runtime Intrusion Detection zapewnia mechanizmy, które gwarantują, że kod SMM systemu BIOS pozostaje nienaruszony w trakcie działania systemu operacyjnego, dodając nowe możliwości zabezpieczenia i/lub zapewniając środki umożliwiające wykrycie wszelkich ataków na kod.

Architektura Runtime Intrusion Detection

Funkcja RTID korzysta z wyspecjalizowanego sprzętu będącego częścią mikroukładu platformy do wykrywania anomalii w środowisku uruchomieniowym SMM BIOS firmy HP. Wykrycie ewentualnych anomalii skutkuje powiadomieniem kontrolera HP Endpoint Security Controller, który może podjąć niezależne od CPU działanie zgodne ze skonfigurowanymi zasadami.

Ilustracja 2. Runtime Intrusion Detection korzysta z wyspecjalizowanego sprzętu zintegrowanego w mikroukładzie platformy do monitorowania kodu SMM pod kątem wszelkich zmian.



Powiadomienia użytkownika, rejestrowanie zdarzeń, zarządzanie zasadami

Powiadomienia HP Sure Start dla użytkownika końcowego

W normalnych warunkach działania rozwiązanie HP Sure Start nie jest widoczne dla użytkownika. Operacje przywracania są wykonywane automatycznie przy zastosowaniu ustawień domyślnych, gdy HP Sure Start zidentyfikuje problem. Zazwyczaj nie ma konieczności działań ze strony użytkownika końcowego ani działu IT.

Użytkownicy mogą widzieć powiadomienia środowiska uruchomieniowego w razie wykrycia problemu ze spójnością BIOS przez funkcje HP Sure Start Dynamic Protection lub Runtime Intrusion Detection w trakcie pracy systemu operacyjnego. W razie wykrycia znaczącego zdarzenia lub podjęcia działania rozwiązanie HP Sure Start wyświetla przy kolejnym rozruchu komunikat z ostrzeżeniem za pomocą powiadomień systemu Windows®. Aby wyświetlanie tych powiadomień systemu Windows było możliwe, konieczny jest program HP Notifications.

Rejestrowanie zdarzeń HP Sure Start

Kontroler HP Endpoint Security Controller rejestruje kluczowe zdarzenia powiązane z oprogramowaniem układowym/kodem BIOS, a dane są monitorowane przez rozwiązanie HP Sure Start. Te zdarzenia są zapisywane w pamięci trwałej HP Sure Start. Te zdarzenia są kopiowane z HP ESC do podglądu zdarzeń systemu Windows, gdy program HP Notifications jest zainstalowany, aby umożliwić dostęp do tych zdarzeń użytkownikowi lokalnemu, a także wybranemu przez klienta agentowi zarządzania.

Następujące zdarzenia spowodują zebranie wszystkich zdarzeń przez program HP Notifications z podsystemu HP Sure Start oraz zagwarantują, że podgląd zdarzeń systemu Windows będzie zaktualizowany o wszystkie zdarzenia, które nie zostały w nim jeszcze zarejestrowane:

- Rozruch systemu Windows
- Wznowienie systemu Windows z trybu uśpienia/hibernacji
- Powiadomienia o zdarzeniach środowiska uruchomieniowego HP Sure Start Dynamic Protection
- HP Sure Start Runtime Intrusion Detection (RTID)

Program HP Notifications wpisuje zdarzenia HP Sure Start do unikatowego dziennika zdarzeń aplikacji „HP Sure Start". W tym dzienniku będą rejestrowane wyłącznie zdarzenia HP Sure Start. Ścieżka podglądu zdarzeń systemu Windows do zdarzeń HP Sure Start jest następująca: Narzędzia systemowe/Podgląd zdarzeń/Dziennik aplikacji i usług/HP Sure Start.

Kategorie poziomów podglądu zdarzeń systemu Windows powiązane ze zdarzeniami HP Sure Start zostały zdefiniowane w poniższej tabeli.

Zdarzenia są wpisywane do podglądu zdarzeń systemu Windows w takiej kolejności, w jakiej zostały wygenerowane przez HP Sure Start. Najstarsze zdarzenie w podsystemie HP Sure Start jest dodawane do podglądu zdarzeń systemu Windows jako pierwsze, a najnowsze jako ostatnie.

Sygnatura czasowa dla każdego wpisu podglądu zdarzeń systemu Windows to czas, w którym zdarzenie zostało dodane do tego dziennika, a NIE czas, w którym zdarzenie wystąpiło. Każdy wpis HP Sure Start do podglądu zdarzeń systemu Windows zawiera szczegółowe dane w informacjach o zdarzeniu, takie jak sygnaturę czasową faktycznego zdarzenia.

Uwaga: Zdarzenia pozostają zapisane w kontrolerze HP Endpoint Security Controller nawet po ich skopiowaniu do podglądu zdarzeń systemu Windows. Po wyczyszczeniu podglądu zdarzeń systemu Windows aplikacja HP Notifications zastąpi wszystkie wpisy HP Sure Start podczas wystąpienia kolejnego zdarzenia, które spowoduje, że aplikacja przeprowadzi kontrolę dzienników zdarzeń HP Sure Start.

Rodzaje zdarzeń HP Sure Start w podglądzie zdarzeń systemu Windows

Poziom zdarzenia	Definicja
Informacja	Zdarzenia, które powinny wystąpić w trakcie normalnego działania (np. aktualizacja BIOS).
Ostrzeżenie	Nieoczekiwane zdarzenia, które wystąpiły, ale po których system został w pełni przywrócony przez HP Sure Start i nie jest wymagane żadne działanie ze strony użytkownika/administratora, aby platforma była w pełni sprawna. Tymi zdarzeniami są nietypowe operacje, którym użytkownik/administrator może zechcieć się przyjrzeć później, szczególnie jeśli takie zdarzenia występują częściej na różnych maszynach.
Błąd	Zdarzenia, które wymagają działania ze strony administratora/serwisu HP w celu przywrócenia pełnej sprawności platformy.

Kontrole zasad HP Sure Start

BIOS firmy HP aktywuje i optymalizuje zasady HP Sure Start dla typowego użytkownika — nie jest tutaj wymagana wstępna konfiguracja. Ponieważ rozwiązanie HP Sure Start jest domyślnie włączone, typowy użytkownik nie musi modyfikować ustawień, aby rozwiązanie HP Sure Start chroniło jego urządzenie. W przypadku użytkowników zaawansowanych system BIOS udostępnia pewną kontrolę nad sterowaniem zachowaniem HP Sure Start przy wykorzystaniu ustawień zasad w konfiguracji BIOS (F10). Te ustawienia i funkcje znajdują się w menu Zabezpieczenia/BIOS Sure Start, chyba że dostępna jest informacja o ich innej lokalizacji.

Uwaga: Zasady są zapisane w pamięci trwałej HP ESC, która nie jest dostępna bezpośrednio dla CPU hosta. Dlatego wymagane jest ponowne uruchomienie, aby ustawienia HP Sure Start zostały zastosowane.

Dostępne są następujące ustawienia i funkcje HP Sure Start:

- Verify Boot Block on Every Boot (weryfikacja bloku rozruchowego przy każdym rozruchu)
- BIOS Data Recovery Policy (zasady odzyskiwania danych BIOS)
- Network Controller Configuration Restore (przywracanie konfiguracji kontrolera sieci) (tylko Intel)
- Prompt on Network Controller Configuration Change (powiadomienie w przypadku zmiany konfiguracji kontrolera) (tylko Intel)
- Funkcja Dynamic Runtime Scanning (dynamiczne skanowanie środowiska uruchomieniowego) dla bloku rozruchowego (tylko Intel)
- HP Sure Start BIOS Setting Protection (ochrona ustawień systemu BIOS przez HP Sure Start)
- HP Sure Start Secure Boot Keys Protection (ochrona kluczy bezpiecznego rozruchu HP Sure Start)
- Enhanced HP Firmware Runtime Intrusion Prevention and Detection (ulepszone zapobieganie i wykrywanie nieautoryzowanego dostępu do oprogramowania układowego HP środowiska uruchomieniowego) (tylko Intel)
- HP Firmware Runtime Intrusion Detection (wykrywanie nieautoryzowanego dostępu do oprogramowania układowego HP środowiska uruchomieniowego) (tylko AMD)
- HP Sure Start Security Event Policy (zasady zdarzeń powiązanych z bezpieczeństwem)
- HP Sure Start Security Event Boot Notification (powiadomienia o zdarzeniach powiązanych z bezpieczeństwem podczas rozruchu)
- Lock BIOS Version (blokada wersji BIOS)
- Save/Restore MBR of System Hard Drive (zapisanie/przywrócenie głównego rekordu rozruchowego (MBR) systemowego dysku twardego)
- Save/Restore GPT of System Hard Drive (zapisanie/przywrócenie GPT systemowego dysku twardego)
- Boot Sector (MBR/GPT) Recovery Policy (zasady przywracania sektora rozruchowego MBR/GPT)

Verify Boot Block on Every Boot

HP Sure Start zawsze sprawdza spójność bloku rozruchowego BIOS w pamięci flash przed wznowieniem systemu z trybu uśpienia, hibernacji lub po wyłączeniu. Gdy ta opcja zostanie **włączona**, HP Sure Start będzie również sprawdzać spójność bloku rozruchowego przy każdym ponownym uruchomieniu bez wyłączania zasilania (restart systemu Windows). Rozważając włączenie tej opcji, należy wziąć pod uwagę, że co prawda przedłuży ona czas ponownego uruchomienia, ale zapewni jednak większe bezpieczeństwo. Ta funkcja jest domyślnie **wyłączona**.

BIOS Data Recovery Policy

Po wybraniu w przypadku tej funkcji opcji **Automatic** (automatycznie), HP Sure Start automatycznie naprawia BIOS lub unikatowe dane maszyny, gdy jest to konieczne. Jeśli w przypadku tej funkcji wybrano opcję **Manual** (ręcznie), HP Sure Start wymaga użycia specjalnego skrótu klawiaturowego, aby wykonać naprawę. W razie problemów z kodem bloku rozruchowego system odmówi wykonania rozruchu, a diody systemu zaświecą się w unikatowej sekwencji. W razie problemów z unikatowymi danymi maszyny system wyświetli komunikat na ekranie. Wymagany skrót klawiaturowy oraz sekwencja diod różnią się w zależności od tego, czy urządzeniem jest notebook, komputer biurkowy czy tablet. Tryb ręczny jest korzystny dla użytkowników, którzy potrafią przeprowadzić analizę zawartości pamięci flash systemu przed naprawą. Odradzamy korzystanie z trybu ręcznego typowemu użytkownikowi. W przypadku tej funkcji domyślnym ustawieniem jest **Automatic** (automatycznie).

Network Controller Configuration Restore (tylko Intel)

Ta opcja sterowania jest dostępna tylko w systemach Intel. Po jej wybraniu rozwiązanie HP Sure Start natychmiast przywraca konfigurację kontrolera sieci do domyślnych wartości fabrycznych.

Prompt on Network Controller Configuration Change (tylko Intel)

To ustawienie jest dostępne tylko w systemach Intel. HP udostępnia zdefiniowaną fabrycznie konfigurację kontrolera sieci, która zawiera adres MAC. Gdy to ustawienie jest **włączone**, system monitoruje stan konfiguracji kontrolera sieci i powiadamia użytkownika w razie zmiany odbiegającej od stanu fabrycznego. Ta funkcja jest domyślnie **wyłączona**.

Dynamic Runtime Scanning of Boot Block (tylko Intel)

To ustawienie jest dostępne tylko w systemach Intel. Jeśli funkcja jest **włączona** (jest to ustawienie domyślne), HP Sure Start regularnie sprawdza spójność bloku rozruchowego BIOS w trakcie pracy systemu operacyjnego. Jeśli funkcja jest **wyłączona**, HP Sure Start sprawdza spójność jedynie przed rozruchem lub przywróceniem systemu z trybu uśpienia lub hibernacji.

HP Sure Start BIOS Setting Protection

Ochrona ustawień systemu BIOS jest domyślnie **wyłączona**. Aby włączyć tę funkcję, właściciel/administrator urządzenia klienckiego powinien najpierw skonfigurować wszystkie zasady BIOS zgodnie z preferowanymi ustawieniami. Właściciel/administrator musi również skonfigurować hasło administratora konfiguracji BIOS, aby korzystać z funkcji ochrony ustawień BIOS HP Sure Start.

Po wykonaniu tych czynności zasady ochrony ustawień BIOS powinny zostać „włączone". W tym momencie w chronionej pamięci HP Sure Start zostanie utworzona kopia wszystkich ustawień BIOS. Od tej pory żadnego z ustawień BIOS nie będzie można zmienić lokalnie ani zdalnie. Przy każdym rozruchu ustawienia zasad BIOS będą sprawdzane pod kątem zgodności z wymaganym stanem. Jeśli wystąpi niezgodność, ustawienia BIOS zostaną przywrócone z chronionej pamięci HP Sure Start.

Aby zmienić ustawienie BIOS, należy podać hasło administratora systemu BIOS, a ochrona ustawień BIOS musi zostać następnie wyłączona. Po spełnieniu tych wymagań będzie można wprowadzić zmiany w ustawieniach BIOS.

HP Sure Start Secure Boot Keys Protection

Gdy ta funkcja jest **włączona** (domyślne ustawienie fabryczne), HP Sure Start zapewnia ulepszoną ochronę baz danych bezpiecznego rozruchu oraz kluczy używanych przez system BIOS do weryfikacji spójności i autentyczności programu ładującego systemu operacyjnego przed uruchomieniem go w przypadku rozruchu. Gdy ta opcja jest **wyłączona**, używana jest wyłącznie standardowa ochrona zmiennych bezpiecznego rozruchu UEFI. Podsystem HP Sure Start nie przechowuje kopii zapasowej.

Enhanced HP Firmware Runtime Intrusion Prevention and Detection (tylko Intel) i HP Firmware Runtime Intrusion Detection (tylko AMD)

Funkcja RTID jest domyślnie **włączona** dla wszystkich platform dostarczanych z fabryk HP. Użytkownik końcowy/administrator nie muszą włączać ani w inny sposób aktywować tej funkcji, aby z niej korzystać.

Właściciel/administrator platformy może opcjonalnie **wyłączyć** funkcję RTID.

HP Sure Start Security Event Policy

To ustawienie zasad BIOS wpływa na to, jakie działanie zostanie podjęte, gdy HP Sure Start wykryje atak lub próbę ataku w trakcie pracy systemu operacyjnego. Dostępne są trzy konfiguracje tej funkcji:

- **Log event only** (zapisuj tylko zdarzenia): W przypadku wybrania tego ustawienia HP ESC rejestruje zdarzenia wykrycia ataków, które można wyświetlić, przechodząc do ścieżki Dzienniki aplikacji i usług/HP Sure Start w podglądzie zdarzeń systemu Microsoft Windows.[3]
- **Log event and notify user** (rejestrowanie zdarzeń i powiadamianie użytkownika): Jest to ustawienie domyślne. W przypadku wybrania tego ustawienia HP ESC rejestruje zdarzenia wykrycia ataków, które można wyświetlić, przechodząc do ścieżki Dzienniki aplikacji i usług/HP Sure Start w podglądzie zdarzeń systemu Microsoft Windows. Ponadto użytkownik otrzymuje w systemie Windows powiadomienie, że miało miejsce dane zdarzenie.[4]
- **Log event and power off system** (rejestrowanie zdarzeń i wyłączenie systemu): W przypadku wybrania tego ustawienia HP ESC rejestruje zdarzenia wykrycia ataków, które można wyświetlić, przechodząc do ścieżki Dzienniki aplikacji i usług/HP Sure Start w podglądzie zdarzeń systemu Microsoft Windows. Ponadto użytkownik otrzymuje w systemie Windows powiadomienie o tym, że takie zdarzenie miało miejsce oraz że wkrótce nastąpi wyłączenie systemu.

HP Sure Start Security Event Boot Notification

To ustawienie zasad BIOS wpływa na to, czy ostrzeżenia i komunikaty o błędach HP Sure Start, które są wyświetlane, gdy system jest uruchamiany, wymagają zatwierdzenia lokalnego błędu przez użytkownika, zanim kontynuowanie uruchamiania systemu będzie możliwe. Domyślnym ustawieniem tej funkcji jest **Require Acknowledgement** (wymagaj potwierdzenia). System zatrzymuje się wówczas i wyświetla błąd. Użytkownik lokalny musi nacisnąć klawisz na klawiaturze, aby kontynuować rozruch. Jeśli ustawienie zostanie zmienione na **Time out after 15 seconds** (czas oczekiwania: maks. 15 s), komunikat będzie wyświetlany, ale proces rozruchu będzie automatycznie kontynuowany po 15 sekundach od momentu wyświetlenia komunikatu.

Lock BIOS Version

W konfiguracji systemu BIOS (F10) ta funkcja znajduje się w Menu główne/Aktualizacja systemu BIOS.

Gdy ta opcja jest **wyłączona**, możesz zaktualizować BIOS, korzystając z dowolnego obsługiwanego procesu. Gdy HP ESC wykryje prawidłową aktualizację bloku rozruchowego w pamięci flash systemu, aktualizuje kopię zapasową bloku rozruchowego.

Gdy ta opcja jest **włączona**, wszystkie narzędzia do aktualizacji HP BIOS odmówią aktualizacji BIOS. Ponadto HP Sure Start będzie chronić BIOS przed próbami zmian wersji BIOS poprzez usunięcie pamięci flash systemu za pomocą niezatwierdzonej metody. HP ESC rejestruje zablokowaną wersję BIOS. Gdy HP ESC wykryje zmianę w pamięci flash systemu BIOS, nadpisuje blok rozruchowy BIOS kopią bloku rozruchowego HP ESC. Kopia bloku rozruchowego HP ESC wykonuje i odzyskuje pozostałą część prawidłowej wersji BIOS. Ta funkcja jest domyślnie **wyłączona**.

Save/Restore MBR of System Hard Drive i Save/Restore GPT of System Hard Drive

W konfiguracji BIOS (F10) ta funkcja znajduje się w menu Zabezpieczenia/Narzędzia dysku twardego. Tylko jedna z tych funkcji jest dostępna, w zależności od rodzaju partycji głównego dysku (GPT lub MBR) wykrytego przez HP Sure Start.

Gdy ta opcja jest **włączona**, HP Sure Start zachowuje chronioną kopię zapasową tabeli partycji MBR/GPT z głównego dysku i porównuje kopię zapasową z partycją podstawową przy każdym rozruchu. W razie wykrycia różnicy użytkownik otrzymuje powiadomienie i może zdecydować się na przywrócenie pierwotnego stanu z kopii zapasowej lub na wprowadzenie zmian do chronionej kopii zapasowej. Funkcji **Boot Sector (MBR/GPT) Recovery Policy** można użyć opcjonalnie do usunięcia decyzji użytkownika dotyczącej wyboru działania wykonywanego w razie znalezienia różnic przez rozwiązanie HP Sure Start.

Gdy opcja jest **wyłączona** (ustawienie domyślne), HP Sure Start nie zapewnia ochrony MBR/GPT.

Boot Sector (MBR/GPT) Recovery Policy

Gdy w przypadku tej opcji wybrane jest domyślne ustawienie **Local User Control** (sterowanie przez użytkownika lokalnego), użytkownik otrzymuje powiadomienie o konieczności podjęcia działania, gdy HP Sure Start wykryje zmianę w tabeli partycji MBR/GPT. Gdy w przypadku tej opcji wybrane jest ustawienie **Recover in the event of corruption** (przywracaj w przypadku uszkodzenia), HP Sure Start automatycznie przywraca MBR/GPT do zapisanego stanu w razie wykrycia różnić.

Zdalne zarządzanie zasadami HP Sure Start

Domyślnie zasady HP Sure Start są zoptymalizowane pod kątem typowego użytkownika. Ponieważ rozwiązanie HP Sure Start jest domyślnie włączone, administrator zdalny nie musi podejmować żadnych działań, aby włączyć (lub „zastosować") rozwiązanie HP Sure Start. Jeśli administrator zdalny chce zmodyfikować ustawienia zasad HP Sure Start, może użyć tych samych interfejsów API Windows Management Instrumentation (WMI, instrumentacja zarządzania Windows) lub skryptów HP BIOS Configuration Utility (narzędzie konfiguracyjne systemu BIOS firmy HP), które służą do zarządzania innymi zasadami systemu BIOS platformy.

Ponadto administratorzy mogą zdalnie zarządzać funkcjami HP Sure Start oraz wyświetlać zdarzenia HP Sure Start za pomocą wtyczki Manageability Integration Kit (MIK) do programu Configuration Manager w pakiecie System Center firmy Microsoft (SCCM).

Wnioski

HP Sure Start zapewnia następujące kluczowe zalety:

- **Nieprzerwana produktywność** — HP Sure Start pozwala zachować ciągłość działalności biznesowej w razie ataku lub przypadkowego uszkodzenia, ponieważ nie trzeba czekać na to, aż dział IT/serwis zajmą się tą kwestią.
- **Niższe koszty** — ponieważ rozwiązanie HP Sure Start umożliwia natychmiastowe przywrócenie sprawności automatycznie zmniejsza to liczbę zgłoszeń do działu wsparcia IT oraz zwiększa produktywność, co w rezultacie pozwala obniżyć koszty konserwacji platformy.
- **Poczucie bezpieczeństwa** — rozwiązanie HP Sure Start jest wyposażone w różnorodne funkcje zabezpieczające, które działają w różnych programach oraz platformach sprzętowych.

Ochrona kluczowego oprogramowania układowego przed złośliwym oprogramowaniem za pomocą wiodącej w branży funkcji wykrywania nieautoryzowanego dostępu do oprogramowania układowego oraz automatycznej naprawy oferowanych przez rozwiązanie HP Sure Start, dostępne w przypadku wybranych komputerów HP Elite.

Załącznik A — generacje HP Sure Start

Firma HP wprowadziła rozwiązanie HP Sure Start w 2014 r. Od tamtego czasu firma HP ulepszyła rozwiązanie HP Sure Start i rozszerzyła liczbę produktów, które są w nie wyposażone. W poniższej tabeli można znaleźć zestawienie funkcji, które były dodawane w poszczególnych generacjach rozwiązania.

Generacja	Data wydania	Dodane funkcje
HP Sure Start	2014	• Wymuszanie autentyczności oprogramowania układowego i systemu BIOS, z możliwością samonaprawy • Monitorowanie i zapewnianie zgodności oprogramowania układowego
HP Sure Start z funkcją Dynamic Protection	2015	• Zgodność z podglądem zdarzeń systemu Windows • Dynamic Protection (w przypadku wybranych produktów Intel)
HP Sure Start 3. generacji (wybrane produkty Intel)[5] HP Sure Start z funkcją Runtime Intrusion Detection (wybrane produkty AMD)[6]	2017	• Wykrywanie ataków w trakcie pracy urządzenia • Ochrona ustawień systemu BIOS • Wtyczka Manageability Integration Kit (MIK) do Microsoft SCCM
HP Sure Start 4. generacji[7]	2018	• Chroniona pamięć — silne metody kryptograficzne do zapisywania ustawień BIOS, poświadczeń użytkowników oraz innych ustawień w sprzęcie kontrolera HP Endpoint Security Controller w celu zapewnienia ochrony spójności, wykrywania manipulacji oraz ochrony poufności tych danych • Ochrona bazy danych rozruchu bezpiecznego — ulepszona ochrona baz danych i kluczy zapisanych przez system BIOS, które mają kluczowe znaczenie dla spójności funkcji bezpiecznego rozruchu systemu operacyjnego w porównaniu ze standardowym UEFI BIOS • W przypadku platform Intel — ulepszona ochrona i odzyskiwanie oprogramowania układowego Intel® Management Engine (silnik zarządzania Intel®) • Certyfikat bezpieczeństwa przyznawany przez stronę trzecią dla HP Endpoint Security Controller — kontroler został przetestowany przez niezależne i akredytowane laboratorium w celu sprawdzenia sprawności głównej funkcjonalności sprzętu HP ESC zgodnie z zapewnieniami oraz na podstawie ogólnie dostępnych kryteriów, metod i procesów[1] • Komputery biznesowe HP z rozwiązaniem HP Sure Start wykraczają poza wymagania ustalone we wstępnych wytycznych instytutu National Institute of Standards Technology (NIST, Narodowy Instytut Standaryzacji i Technologii) (publikacja specjalna 800-193)

Załącznik B — przegląd kodu System Management Mode (SMM)

System Management Mode (SMM) to standardowa w branży metoda realizacji zaawansowanych funkcji zarządzania zasilaniem komputera oraz innych niezależnych od systemu operacyjnego funkcji w trakcie jego działania. Chociaż określenie SMM oraz jego zastosowanie jest charakterystyczne dla architektury x86, wiele nowoczesnych architektur wykorzystuje podobne rozwiązanie.

System BIOS konfiguruje SMM w trakcie rozruchu. Kod SMM jest zapisywany w pamięci głównej (DRAM), a następnie system BIOS korzysta ze specjalnych (podlegających blokowaniu) rejestrów konfiguracji w mikroukładzie w celu zablokowania dostępu do tego obszaru, gdy mikroprocesor nie wykonuje kontekstu SMM. W trakcie działania środowiska uruchomieniowego wejście do trybu SMM jest zależne od zdarzeń. Mikroukład jest zaprogramowany pod kątem rozpoznawania wielu typów zdarzeń i limitów czasu. Gdy takie zdarzenie ma miejsce, sprzęt mikroukładu przyznaje pin wejścia System Management Interrupt (SMI, przerwanie zarządzania systemem). Przy kolejnej granicy rozkazu mikroprocesor zapisuje cały stan i przechodzi do trybu SMM.

Gdy mikroprocesor przechodzi do trybu SMM, przyznaje sprzętowy pin wyjścia, SMI Active (SMIACT). Pin powiadamia sprzęt mikroukładu, że mikroprocesor przechodzi do trybu SMM. SMI może zostać przyznany w dowolnym momencie, w trakcie każdego z trybów działania, za wyjątkiem trybu SMM. Sprzęt mikroukładu rozpoznaje sygnał SMIACT i przekierowuje wszystkie dalsze cykle pamięci do chronionego obszaru pamięci (czasem określanego terminem „obszar SMRAM"), zarezerwowanego specjalnie dla SMM. Natychmiast po otrzymaniu wejścia SMI oraz po przyznaniu wyjścia SMIACT mikroprocesor rozpoczyna zapisywanie całego wewnętrznego stanu w tym chronionym obszarze pamięci.

Po zapisaniu stanu mikroprocesora w pamięci SMRAM specjalny kod obsługi SMM, który również znajduje się w SMRAM (jest on tam umieszczany przez BIOS podczas rozruchu), rozpoczyna wykonywanie w specjalnym trybie działania. Podczas pracy w tym trybie większość mechanizmów izolacji sprzętu i pamięci jest zawieszona, a mikroprocesor może uzyskać wirtualnie dostęp do wszystkich zasobów platformy, aby umożliwić wykonanie wymaganych zadań. Kod SMM wykonuje wymagane zadanie, a następnie mikroprocesor wraca do poprzedniego trybu działania. Teraz kod SMM wykonuje instrukcję Return from System Management Mode (RSM, powrót z trybu zarządzania systemem), aby opuścić SMM. Instrukcja RSM powoduje, że mikroprocesor przywraca poprzednie dane stanu wewnętrznego z kopii zapisanej w SMRAM w momencie przejścia do trybu SMM. Po ukończeniu RSM cały stan mikroprocesora jest przywrócony do stanu z chwili przed zdarzeniem SMI, a poprzedni program (system operacyjny, aplikacje, hypervisor itp.) wznawia wykonywanie dokładnie w miejscu, w którym zostało ono przerwane.

[1] Sprzęt kontrolera HP Sure Start posiada certyfikat zgodnie z wymogami certyfikacji CSPN.

[2] Rozwiązanie HP Sure Start z funkcją Dynamic Protection jest dostępne w przypadku produktów HP Elite wyposażonych w procesory Intel Core 6. generacji lub nowsze.

[3] Program HP Notification musi być zainstalowany, aby można było wyświetlać zdarzenia HP Sure Start w podglądzie zdarzeń systemu Windows.

[4] Program HP Notification musi być zainstalowany, aby możliwe było otrzymywanie powiadomień.

[5] Rozwiązanie HP Sure Start 3. generacji jest dostępne w przypadku produktów HP Elite wyposażonych w procesory Intel 7. generacji.

[6] Rozwiązanie HP Sure Start z funkcją Runtime Intrusion Detection jest dostępne w przypadku produktów HP Elite wyposażonych w procesory AMD 7. generacji.

[7] Rozwiązanie HP Sure Start 4. generacji jest dostępne w przypadku produktów HP Elite oraz HP Pro 600 wyposażonych w procesory Intel 8. generacji lub AMD.

Dowiedz się więcej na stronie
hp.com/go/computersecurity

4AA7-3172PLE, Może 2018 r.