Teknisk vitbok

# HP Sure Start

Automatiskt skydd och reparation på BIOS-nivå

Maj 2018

# Innehållsförteckning


Varför är BIOS-skydd viktigt? ..... 03

HP Sure Start ger ett utmärkt skydd av inbyggd programvara ..... 04

Arkitektonisk översikt och kapacitet ..... 05

- Sekretessverifiering av inbyggd programvara – kärnan i HP Sure Start ..... 05
- Datorns unika dataintegritet ..... 05
- Identifieringsområde ..... 06
- Nätverkskontrollskydd ..... 06
- BIOS-inställningsskydd ..... 06
- HP Sure Starts skyddade lagring ..... 06
- Skydd av nycklar för säker start ..... 07
- Runtime Intrusion Detection (RTID) ..... 07

Användarmeddelanden, händelselogg och policyhantering ..... 08

- HP Sure Start, meddelande till slutanvändare ..... 08
- HP Sure Start, händelselogg ..... 08
- HP Sure Start, policykontroll ..... 09
- Fjärrhantering av policykontroller för HP Sure Start ..... 10

Slutsats ..... 11

Bilaga A – HP Sure Start, generationsöversikt ..... 11

Bilaga – översikt av System Management Mode (SMM) ..... 12


# Inledning

HP Sure Start kan automatiskt upptäcka och stoppa en BIOS-attack eller ett intrång, samt återställas från detta, utan IT-ingripande och med minimala eller inga avbrott i användarproduktiviteten. Varje gång datorn startar, bekräftar HP Sure Start automatiskt BIOS-kodens integritet för att säkerställa att datorn skyddas mot skadliga attacker. När datorn är igång övervakar systemet konstant BIOS för att upptäcka försök till intrång. I händelse av en attack kan datorn självläka med hjälp av en "gyllene kopia" av BIOS på mindre än en minut.

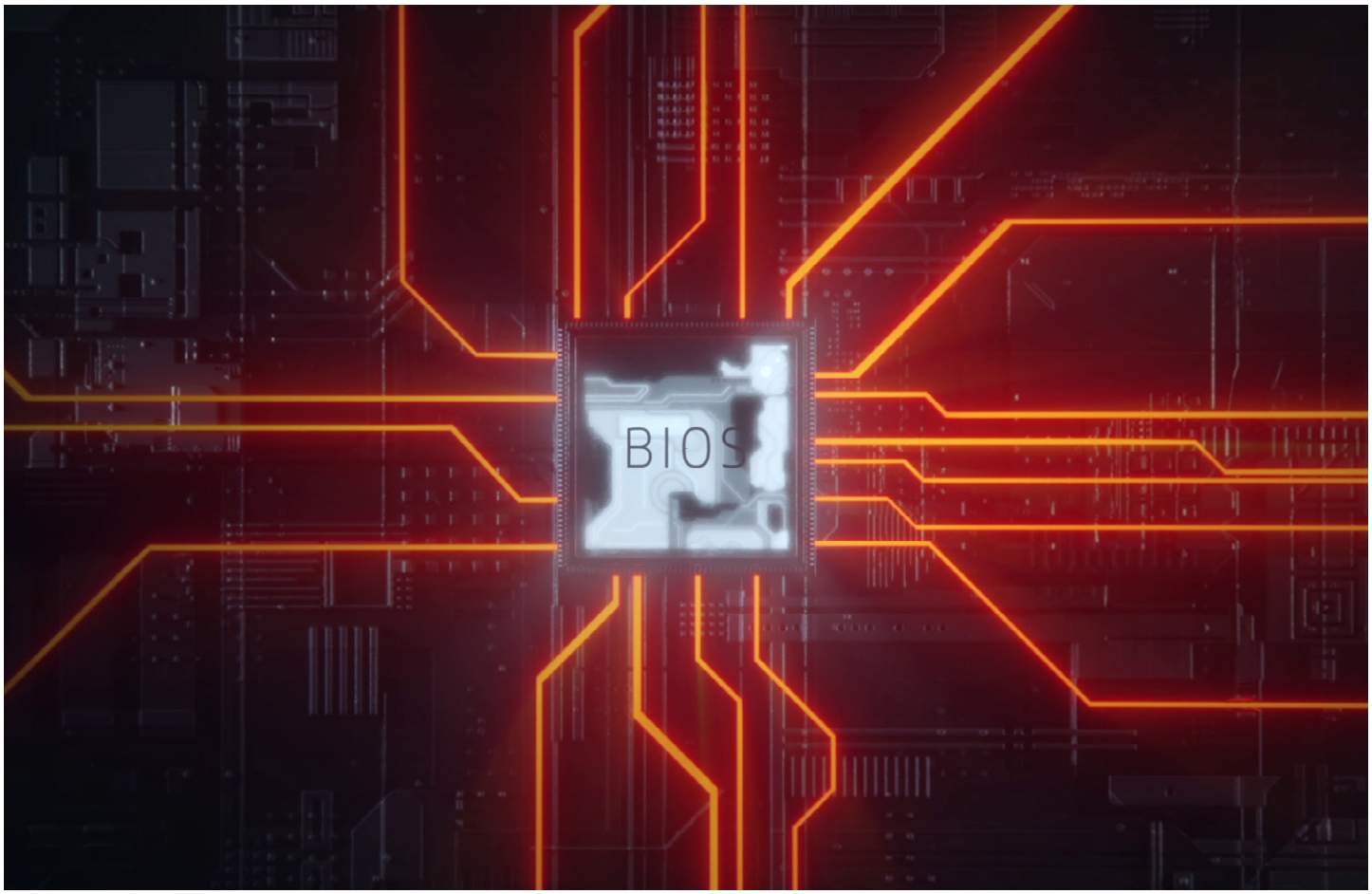
## Varför är BIOS-skydd viktigt?

**I takt med att vår värld blir alltmer uppkopplad, kommer även cyberangrepp på klientenheters inbyggda programvara och hårdvara att tillta, både vad gäller antal förekomster och sinnrikhet. Verktyg och tekniker för att attackera inbyggd programvara fanns en gång i teorin, och man trodde att dessa endast kunde utföras av nationer. Sedan dess har sådana verktyg och tekniker visat sig inte bara existera utan även vara lättillgängliga för allmänheten.**

Enhetens inbyggda programvara (eller BIOS) utgör ett attraktivt mål för angripare på grund av de potentiella vinster som ett framgångsrikt intrång kan ge angriparen:

- Uthållighet: Inbyggd programvara finns i ett icke-flyktigt minne på kretskortet och kan inte tas bort enbart genom att radera hårddisken.
- Kontroll: Inbyggd programvara körs på högsta behörighetsnivå – utanför OS-domänen, vilket möjliggör angrepp från OS-oberoende skadlig programvara.
- Smygangrepp: Inbyggd programvara upptar en del av minnet som är helt otillgängligt för operativsystemet och systemprogramvaran. Eftersom det inte kan genomsökas av antivirus finns möjligheten att det aldrig upptäcks.
- Svårighet att återställa: Alla dessa aspekter gör det extremt svårt att återställa från denna typ av angrepp utan att tillgripa en servicehändelse vilket innefattar byte av moderkortet.

Den idealiska lösningen för att skydda enheter mot denna typ av angrepp är utformad med start i hårdvaran, där principerna för ”digital motståndskraft” används. Dessa principer bekräftar att det är extremt svårt, om inte omöjligt, att förutse och förebygga alla eventuella attacker. Den idealiska lösningen ger inte bara utökat skydd av inbyggd programvara, men inbegriper även en hårdvarubaserad förmåga att både upptäcka en lyckad attack och återställa från den.



# HP Sure Start ger ett utmärkt skydd av inbyggd programvara

**HP Sure Start är HPs unika och banbrytande metod som ska ge inbyggd programvara i HP-datorer avancerat skydd och motståndskraft. Den använder HP Endpoint Security Controller (HP ESC) för att skydda BIOS som når långt över gällande branschstandard och säkerställer att systemet endast startar Genuine HP BIOS. Om HP Sure Start dessutom upptäcker att BIOS, inbyggd programvara eller BIOS-koden i körmiljön System Management Mode (SMM) har manipulerats, kan den återställa systemet med en skyddad säkerhetskopia.**

### Sammanfattning av funktionerna i HP Sure Start

- HPs autenticitetshantering och manipulationsskydd av den inbyggda programvaran i kärnplattformen – HP Endpoint Security Controller-hårdvaruhantering av systemstart, så att endast autentisk och oförändrad inbyggd programvara och BIOS från HP läses in
- Hälsoövervakning och kontroll av inbyggd programvara – loggning av den inbyggda programvarans hälsorelaterade händelser via HP Endpoint Security Controller, vilket presenterar status på plattformens inbyggda programvara i kombination med eventuella avvikelser som kan vara tecken på försvagande angrepp
- Självläkande – automatisk reparation av skador tillförda inbyggd programvara och BIOS från HP med hjälp av den isolerade säkerhetskopia som HP Endpoint Security Controller har av inbyggd programvara och BIOS från HP
- BIOS-inställningsskydd – utökar det skydd som HP Endpoint Security Controller utövar på BIOS-koden till att även innefatta HP ESC-säkerhetskopia och integritetskontroll av alla BIOS-inställningar som har konfigurerats av användare eller administratör
- Intrångsidentifiering under körning – löpande övervakning av kritisk BIOS-kod i körmiljöns minne (SMM) medan operativsystemet körs
- Skydd av nycklar för säker start – väsentligt förbättrat skydd av databaser och nycklar som lagras av BIOS som är kritiska för integriteten rörande operativsystemets funktion för säker start jämfört med standardiserad UEFI BIOS-implementering
- Skyddad lagring – HP Sure Start använder starka kryptografiska metoder för att lagra BIOS-inställningar, inloggningsuppgifter och andra inställningar i hårdvaran som tillhör HP Endpoint Security Controller för att tillhandahålla integritetsskydd, manipulationsskydd och konfidentialitetsskydd för dessa data
- Skydd för inbyggda Intel® Management Engine-programvaran – utökat skydd och återställning av den inbyggda Intel Management Engine-programvaran
- Managerbarhet – administratörer kan hantera HP Sure Start-funktioner med insticksprogrammet Manageability Integration Kit (MIK) för Microsoft® System Center Configuration Manager (SCCM)

En sammanfattning av de funktioner som lagts till i varje generation av HP Sure Start finns i bilaga A på sidan 11.

### Säkerhetscertifiering av tredje part

HP Endpoint Security Controller-hårdvaran som används i HP Sure Start har genomgått en säkerhetsbedömning från tredje part och har certifierats för att tillhandahålla hårdvarubekämpning som endast auktoriserad inbyggd programvara kan starta på måldatorn.[1]

Försäkran om att en säkerhetslösning fungerar enligt anvisningar är en kritisk del av alla köpbeslut relaterade till säkerhetsprodukter. Även om HP har rykte om sig att leverera god kvalitet, har HP låtit ett oberoende och ackrediterat laboratorium utsätta de inre arbetsmekanismer som verkar i HP Endpoint Security Controller för granskning och testning, i syfte att validera att det fungerar enligt de krav som finns stipulerade enligt offentligt tillgängliga kriterier, metoder och processer.

### Design med digital motståndskraft

HP Sure Start tillhandahåller inte bara förbättrat BIOS-skydd som sträcker sig bortom branschstandard, utan det är utformat med start i hårdvaran för att ge en oöverträffad digital motståndskraft för att säkerställa att BIOS kan återställas även om ett dataintrång eller ett förödande angrepp skulle inträffa. HPs företagsdatorer med HP Sure Start överträffar riktlinjerna som är upprättade enligt Draft National Institute of Standards Technology (NIST) Platform Firmware Resiliency (Special Publication 800-193), vilket är ett av de ledande organen inom offentlig sektor med fokus på att formalisera kraven på plattformar med digital motståndskraft.

### Modeller med stöd för HP Sure Start

HP introducerade Sure Start 2014. Sedan dess har HP förbättrat Sure Start och utökat det antal produkter som innefattar den. HP Sure Start tillhandahålls över hela 2018 Elite-sortimentet, inklusive plattor, bärbara datorer, stationära datorer och allt-i-ett-lösningar (AIO). HP Sure Start Gen4 finns tillgängligt på HP Elite- och HP Pro 600-produkter utrustade med 8:e generationens processorer från Intel eller AMD®.

# Arkitektonisk översikt och kapacitet

HP Sure Start består av två huvudsakliga arkitektoniska komponenter:

- **HP Endpoint Security Controller** som kör den inbyggda programvaran HP Sure Start
- **HP Sure Start BIOS** som arbetar tillsammans med hårdvaran och den inbyggda programvaran i HP Endpoint Security Controller

## Sekretessverifiering av inbyggd programvara – kärnan i HP Sure Start

HP Endpoint Security Controller (HP ESC) är den första enheten i systemet som kör den inbyggda programvaran när systemet startar, och som är aktivt före systemstart. Aktiviteterna som HP ESC utför innefattar, men är inte begränsade till, övervakning av strömbrytaren och sekvensen för värddatorns start av CPU-körning när användaren trycker på strömbrytaren.

När strömmen når plattformen (innan systemet är påslaget), bekräftar HP ESC att dess egen inbyggda programvara är autentisk HP-kod innan koden läses in och körs.
HP ESC-hårdvaran använder starka kryptografiska metoder enligt branschstandard för att utföra integritetsverifiering. Metoden använder sig av en 2048-bitars HP RSA-nyckelfunktion i internt, permanent skrivskyddat minne. Därför är HP ESC den inbyggda hårdvarubaserade Root of Trust (RoT) för plattformen, vilken används för att validera dess inbyggda programvara och HP BIOS innan dessa körs. Denna hårdvarubaserade Root of Trust skyddar mot attacker som kräver utbyte av inbyggda programvara, oberoende av deras installationsmetod och fungerar som den grund på vilken HPs plattformssäkerhet är uppbyggd.

**Bild 1.** Verifieringsprocess för inbyggd programvaras integritet.

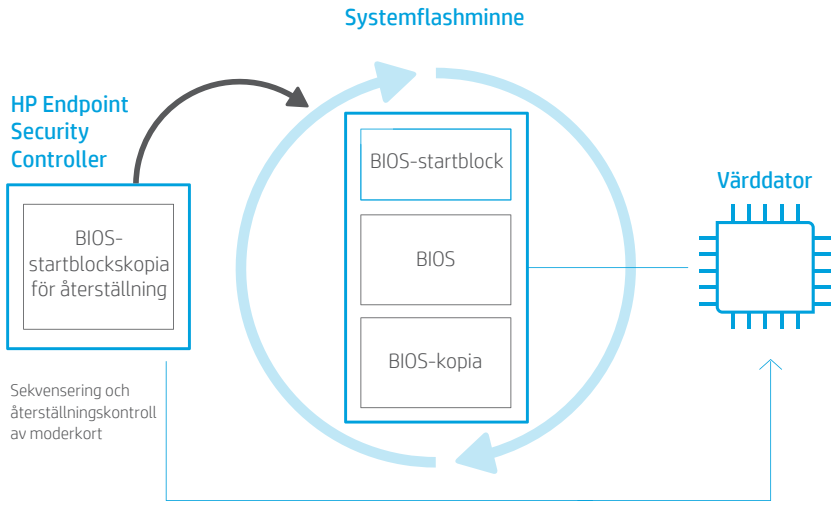



Bild 1 illustrerar verifieringsprocessen för inbyggd programvaras integritet. När HP ESC autentiserar och börjar köra den inbyggda programvaran HP Sure Start, använder denna inbyggda programvara samma starka kryptografiska processer för att verifiera integriteten för systemflashminnets BIOS-uppstartsblock. Om en enda bit är ogiltig, ersätter HP ESC systemflashinnehållet med en egen kopia av HP BIOS-startblocket som lagras i ett separat icke-flyktigt minne (NVM) dedikerat till HP ESC.

Designen av HP Sure Start säkerställer att all inbyggd programvara och BIOS-kod som körs på både HP ESC och värddatorn, är den kod som HP avser vara på enheten.

*Observera: Integritetskontrollen av systemflashminnets startblock och eventuell nödvändig återställning som utförs av HP ESC, äger rum när värddatorn är avstängd. Ur ett användarperspektiv sker därför hela processen när systemet fortfarande är avstängt, i viloläge eller strömsparläge.*

Systemflashminnets BIOS-startblock utgör grunden för HP BIOS. HP ESC-hårdvaran säkerställer att BIOS-startblocket är den första koden som CPU-enheten läser in efter en återställning. När HP ESC har fastställt att BIOS-startblocket innehåller autentisk HP-kod, tillåts systemet att starta på det sätt det normalt skulle göra.

HP ESC kontrollerar även integriteten för systemflashminnets startblockskod varje gång systemet stängs av eller försätts i viloläge eller strömsparläge. Eftersom CPU-enheten är avstängd i vart och ett av dessa tillstånd, och CPU-enheten måste köra BIOS-startblockskoden för att fortsätta, är det av yttersta vikt att kontrollera BIOS-startblockets integritet på nytt för att kontrollera om manipulering har ägt rum.

För HP Intel-modeller gäller dessutom att HP Sure Start regelbundet (var 15:e minut) kontrollerar integriteten för systemflashminnets BIOS-startblock medan systemet körs.[2]

## Datorns unika dataintegritet

HP ESC och BIOS arbetar tillsammans för att ge avancerat skydd för fabriksinställda kritiska variabler som är unika för varje dator, vilket är avsett att vara konstant under den livstid som gäller för varje specifik plattform. I fabriken sparas en säkerhetskopia av dessa variabla data i HP ESC:s icke-flyktiga minneslagringsenhet. Säkerhetskopian görs tillgänglig för HP Sure Start BIOS-komponenten i en skrivskyddad version för att utföra integritetskontroll av data vid varje start. Om någon inställning i det delade flashminnet har ändrats jämfört med fabriksinställningarna, återställer HP Sure Start BIOS-komponenterna automatiskt data i systemflashminnet med hjälp av den säkerhetskopia som tillhandahålls av HP ESC.

## Identifieringsområde

För HP Intel-modeller skyddar HP Sure Start systemflashminnets identifieringsområde. Intel-arkitekturen är dessutom ensam med att innehålla ett identifieringsområde med kritiska konfigurationsparametrar som samplas av Intel Core™-logiken vid återställning och därefter används för att konfigurera Core-logiken. Identifieringsområdet inbegriper också partitionsinformation för systemflashminnet som används av Intel Core-logiken för att avgöra var BIOS-området ligger i flashminnet och följaktligen var CPU-enheten hämtar kod för körning från återställning. HP Sure Start övervakar detta områdes integritet och återställer det till avsedd konfiguration i händelse av manipulering eller skada.

## Nätverkskontrollskydd

Dessutom skyddar HP Sure Start för HP Intel-modeller de NIC-inställningar som ingår i systemflashminnet. Vissa HP-kunder har fall som kräver legitima ändringar av fabriksinställda NIC-inställningar. Som standard förhindrar därför HP Sure Start inte ändringar av NIC-inställningar. I stället tillhandahåller HP Sure Start en funktion som, när denna är aktiverad, varnar användaren om att NIC-inställningarna har ändrats. Därtill erbjuder HP Sure Start en metod för att återställa NIC-inställningarna till fabriksinställningarna. Skyddade inställningar innefattar MAC-adressen, inställningar för Pre-boot Execution Environment (PXE), samt fjärrprogrammets startprogram (RPL). Denna återställning är möjlig via en skrivskyddad säkerhetskopia som skyddas av HP ESC

## BIOS-inställningsskydd

Så som tidigare beskrivits, bekräftar HP Sure Start HP BIOS-kodens integritet och autenticitet. Eftersom denna kod är statisk efter att den har skapats av HP kan digitala signaturer användas för att bekräfta kodens båda attribut. Då BIOS-inställningarna både är dynamiska och kan konfigureras av användaren, skapar detta dock ytterligare utmaningar när det gäller att skydda dessa inställningar. Digitala signaturer kan inte genereras av HP och användas av HP Sure Start ESC-hårdvaran för att bekräfta dessa inställningar.

BIOS-inställningsskyddet i HP Sure Start gör det möjligt att konfigurera systemet så att HP ESC-hårdvaran används för att säkerhetskopiera och kontrollera integriteten för alla de BIOS-inställningar som användaren föredrar.

När den här funktionen är aktiverad på plattformen, säkerhetskopieras alla policyinställningar som används av BIOS och en integritetskontroll utförs vid varje start för att säkerställa att inga av BIOS-policyinställningarna har ändrats. I händelse av att en ändring upptäcks, använder systemet säkerhetskopian från HP Sure Starts skyddade lagring till att automatiskt återgå till de inställningar som användaren har konfigurerat.

HP Sure Starts BIOS-inställningsskydd genererar händelser till HP Sure Start ESC-hårdvaran när ett försök att modifiera BIOS-inställningarna upptäcks. Händelsen loggas i HP Sure Starts granskningslogg, och den lokala användaren får ett meddelande från BIOS vid uppstart.

## HP Sure Starts skyddade lagring

Skyddad lagring som är förankrad i hårdvaran HP Endpoint Security Controller, ger högsta skyddsnivå för BIOS/data för inbyggd programvara och inställningar som skyddas av HP Sure Start. HP Sure Starts skyddade lagring är utformad att erbjuda konfidentialitet, integritet och manipuleringsupptäckt, även i scenarier som innebär att en angripare nedmonterar systemet och upprättar en direkt anslutning till den icke-flyktiga lagringsenheten på moderkortet.

### Dataintegritet

Integriteten för de dynamiska data som lagras i icke-flyktigt minne med inbyggd programvara och används för att styra tillståndet hos olika funktioner, är avgörande för den övergripande plattformens säkerhetsställning. Dynamiska data innefattar alla BIOS-inställningar som kan modifieras av enhetens slutanvändare eller administratör. Exempel inbegriper (men är inte begränsade till) startalternativ såsom funktionen för säker start, BIOS-administratörslösenord och relaterade policyer, Trusted Platform Module-statuskontroll och policyinställningarna för HP Sure Start.

Eventuella angrepp som kringgår befintliga åtkomstbegränsningar som har upprättats för att förhindra obehöriga ändringar av dessa inställningar, kan äventyra plattformsäkerheten. Föreställ dig exempelvis ett scenario där en angripare gör en obehörig modifiering av säkert starttillstånd, och inaktiverar det utan att upptäckas. I detta scenario kommer plattformen att starta angriparens spökprogram innan operativsystemet startar, utan användarens vetskap.

BIOS för Unified Extensible Firmware Interface (UEFI) som är branschstandard, implementerar åtkomstbegränsningar som bör förhindra obehöriga modifieringar av dessa variabler, och HP implementerar dessa precis som övriga parter i datorbranschen.

Men med tanke på de risker som ett brott mot dessa mekanismer innebär på plattformen, ger HP Sure Start sekundära försvar som är starkare än grundläggande branschstandard.

BIOS-inställningar och andra dynamiska data som används av inbyggd programvara för att kontrollera det tillstånd som skyddas av HP Sure Start, lagras i det isolerade och icke-flyktiga minnet som tillhör HP Endpoint Security Controller, vilket inte är direkt tillgängligt för programvara som körs på värddatorn.

Dessutom låter HP ESC skapa och bifoga unika integritetsmätningar varje gång ett dataelement lagras i detta icke-flyktiga minnesutrymme. Integritetsmätningarna baseras på en stark kryptografisk algoritm (hash-baserad meddelandeautentiseringskod som använder SHA-256-hash) som i sin tur är knuten till en hemlighet som finns i HP ESC. Denna hemlighet är unik för varje HP ESC, så att varje styrenhet genererar en unik integritetsmätning utifrån ett identiskt element.

När detta dataelement läses in från det icke-flyktiga minnet, beräknar HP ESC integritetsmätningen på nytt för det dataelementet och jämför det med den integritetsmätning som bifogats i dessa data. Alla obehöriga ändringar av data i det icke-flyktiga minnesutrymmet resulterar i en bristande jämförelse. Med denna metod kan HP ESC upptäcka manipulering av dataelement som lagras i det icke-flyktiga minnesutrymmet.

### Datakonfidentialitet

För många av de dataelement som lagras av plattformen, är det av yttersta vikt att upprätthålla konfidentialitet. Exempel på detta är hashar för BIOS-administratörslösenord, användaruppgifter och hemligheter som eventuellt lagras av den inbyggda programvaran för användarens räkning för funktioner baserade på inbyggd programvara som HP Sure Run och HP Sure Recovery.

Skydd av dessa hemligheter är utmanande när metoder som utgår från UEFI BIOS används, eftersom det icke-flyktiga lagringsutrymmet vanligtvis kan läsas av programvara som körs på värdprocessorn. HP Sure Starts skyddade lagring avser att tillhandahålla avsevärt bättre skydd av dessa konfidentiella data än den standard som UEFI BIOS-implementering innebär.

Förutom ett separat isolerat lagringsutrymme, syftar HP Sure Starts strategi till att utnyttja hårdvarublocket Advanced Encryption Standard (AES) som finns i HP ESC för att utföra AES-256-kryptering på alla konfidentiella dataelement som är lagrade i HP Sure Starts icke-flyktiga minne, utöver de dataintegritetsmätningar som utförs för dessa element. Krypteringsnyckeln är unik för varje HP ESC och lämnar aldrig denna styrenhet, så att data som krypterats av en enskild HP ESC-komponent endast kan dekrypteras av samma HP ESC.

## Skydd av nycklar för säker start

HP Sure Start ger utökat skydd av UEFI:s databaser med säkra startnycklar som lagras av den inbyggda programvaran, jämfört med UEFI:s implementering av säker start som nu är branschstandard. Dessa variabler är kritiska för att UEFI:s funktion med säker start ska fungera korrekt, vilken verifierar integriteten och autenticiteten hos OS-starthanteraren innan den tillåter den att köras vid uppstart.

HP Sure Start skyddar UEFI:s databaser med säkra startnycklar genom att lagra en huvudkopia i HP Sure Starts skyddade lagring. Eventuella godkända ändringar av UEFI:s standarddatabaser med säkra startnycklar av operativsystemet under körning, spåras av HP Sure Start och tillämpas på huvudkopian av HP ESC. HP Sure Start använder därefter huvudkopian i HP Sure Starts skyddade lagring för att identifiera och avvisa alla obehöriga ändringar av UEFI:s standarddatabaser med säkra startnycklar.

Denna funktion, som är aktiverad som standard, täcker följande databaser:

- Signaturdatabas (db)
- Databas för återkallade signaturer (dbx)
- Key Enrollment Key (KEK)
- Platform Key (PEK) som uppdateras dynamiskt vid körning av OS

## Runtime Intrusion Detection (RTID)

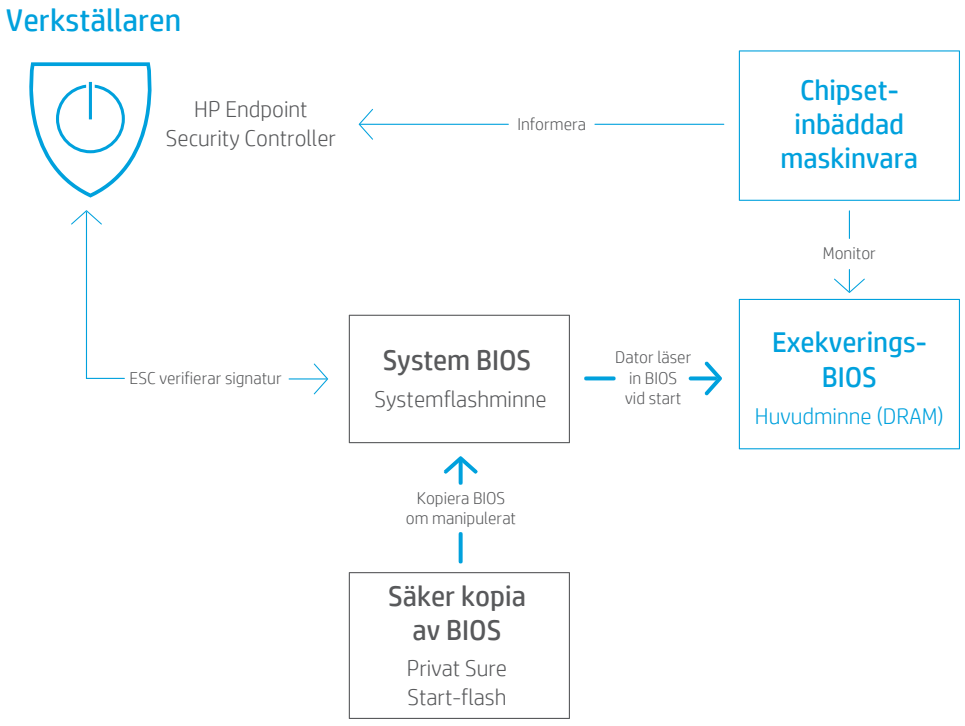
Under varje start startar BIOS-koden en körning från flashminnet vid en fast adress. Detta är känt som BIOS-startkoden och tillhandahåller ”Pre-OS”-funktioner som behövs innan operativsystemet startar. Dock förblir en del av BIOS i DRAM som behövs för att tillhandahålla avancerade energihanteringsfunktioner, operativsystemstjänster och andra OS-oberoende funktioner medan operativsystemet körs. BIOS-koden, även kallad koden för System Management Mode (SMM), ligger i ett speciellt område i DRAM som är dolt från operativsystemet. Vi refererar även till denna kod som ”Runtime”-BIOS-kod i samband med HP Sure Start-funktionen för intrångsidentifiering under körning. (Mer information om SMM och hur det fungerar finns i bilaga B på sidan 12.)

SMM-kodens integritet är avgörande för klientenhetens säkerhetsställning. HP Sure Start utför en kontroll för att säkerställa att HP SMM BIOS-koden är intakt vid start av OS. Runtime Intrusion Detection tillhandahåller mekanismer som ser till att SMM BIOS-koden förblir intakt när OS körs genom att tillföra nya skyddsfunktioner och/eller tillhandahålla metoder för att upptäcka eventuella angrepp riktade mot denna kod.

### Runtime Intrusion Detection och dess arkitektur

RTID-funktionen använder sig av specialiserad hårdvara på plattformens chipset för att upptäcka avvikelser i Runtime HP SMM BIOS. Upptäckten av eventuella avvikelser resulterar i ett meddelande till HP Endpoint Security Controller, som i sin tur kan vidta den konfigurerade policyåtgärden oberoende av CPU-enheten.

**Bild 2.** Runtime Intrusion Detecktion använder specialiserad hårdvara som är inbäddad i plattformens chipset i syfte att övervaka SMM-koden och meddela om eventuella ändringar.



# Användarmeddelanden, händelselogg och policyhantering

## HP Sure Starts meddelande till slutanvändare

Under normala driftsförhållanden är HP Sure Start osynligt för användaren. Återställningsprocesser sker automatiskt med standardinställningarna, vanligtvis utan att någon slutanvändare eller IT-interaktion krävs för återställning, när HP Sure Start identifierar ett problem.

Användare kan se körtidsmeddelanden om ett integritetsproblem i BIOS upptäcks via funktionerna HP Sure Start Dynamic Protection eller för intrångsidentifiering under körning (RID) medan operativsystemet körs. Om en viktig händelse upptäcks eller åtgärder vidtas, visar HP Sure Start ett varningsmeddelande via Windows®-meddelanden vid nästa start. HP Notifications-programvara krävs för att aktivera visning av dessa Windows-meddelanden.

## HP Sure Start, händelselogg

HP Endpoint Security Controller registrerar viktiga händelser förknippade med inbyggd programvara/BIOS-kod och data som övervakas av HP Sure Start. Dessa händelser lagras i Sure Starts icke-flyktiga minnesutrymme. Dessa händelser kopieras från HP ESC till Windows Loggboken när HP Notifications-programvara installeras för att underlätta åtkomsten till dessa händelser för den lokala användaren samt kundens valda hanteringsagent.

Följande händelser utlöser HP Notifications-programvaran så att denna samlar in alla händelser från HP Sure Starts undersystem och säkerställer att Windows Loggboken uppdateras med händelser som inte redan finns registrerade:

- Windows uppstart
- Windows återupptar från viloläge/strömsparläge
- HP Sure Start med dynamisk skyddskörning händelsemeddelanden
- HP Sure Start Runtime Intrusion Detection (RTID)

HP Notifications-programvaran fyller HP Sure Start-händelser i en unik "HP Sure Start"-programhändelselogg. Endast händelser som rör HP Sure Start inkluderas i denna loggbok. Sökvägen för Windows Loggboken till HP Sure Starts händelser är som följer: Systemverktyg/Loggboken/Program och tjänster/HP Sure Start.

Nivåkategorierna i Windows Loggboken associerade med HP Sure Starts händelser anges i tabellen nedan.

Händelserna upptas i Windows Loggboken i den ordning de skapades av HP Sure Start. Den äldsta händelsen i HP Sure Starts undersystem läggs till i Windows Loggboken först, och senare händelser läggs till sist.

Tidsstämpeln för varje post i Windows Loggboken anger den tid den lades till i denna loggbok, INTE den tid då händelsen inträffade. Varje post i Windows Loggboken förknippad med Sure Start, inkluderar detaljerade data i händelsens uppgifter, vilket inbegriper en tidsstämpel för den faktiska förekomsten.

*Observera: Händelser förblir i HP Endpoint Security Controller även efter att ha kopierats till Windows Loggboken. Om Windows Loggboken rensas, kommer programmet HP Notifications-programvaran att ersätta alla HP Sure Start-poster vid nästa händelse som utlöser en kontroll av händelseloggar relaterade till HP Sure Start.*

**Typer av händelser i Windows Loggboken förknippade med HP Sure Start**

| Händelsenivå | Definition |
|---|---|
| Info | Händelser som förväntas inträffa vid normal användning (t.ex. uppdatering av BIOS). |
| Varning | Oväntade händelser som har inträffat men som systemet kunde återställas helt från av HP Sure Start, och ingen åtgärd av användare eller administratör krävs för att plattformen ska vara fullt fungerande. Dessa händelser utgör avvikelser som användaren/administratören kanske vill titta närmare på, i synnerhet om liknande händelser inträffar på flera system. |
| Fel | Händelser som kräver att administratör/HP-tjänsten vidtar åtgärder på plattformarna för att fullständig återställning ska vara möjlig. |

## HP Sure Starts policykontroller

HP-systemets BIOS aktiverar och optimerar HP Sure Starts policyer enligt fabriksstandard för den typiska användaren. Eftersom HP Sure Start är aktiverat som standard är det inte nödvändigt för den typiska användaren att ändra de inställningar som ska skyddas av HP Sure Start. För avancerade användare ger systemets BIOS viss kontroll över HP Sure Starts beteende, med hjälp av policyinställningar i (F10) BIOS Setup. Om inte annat anges, hittas dessa inställningar och funktioner under Säkerhet/ BIOS Sure Start.

*Observera: Policyer lagras i HP ESC:s icke-flyktiga minne som inte är direkt tillgängligt för värddatorn. Därför krävs en omstart innan några Sure Start-inställningar träder i kraft.*

Följande HP Sure Start-inställningar och -funktioner finns tillgängliga:

- Verifiera startblock vid varje uppstart
- BIOS-dataåterställningspolicy
- Återställning av nätverksstyrenhetens konfiguration (endast Intel)
- Fråga vid ändring av nätverksstyrenhetens konfiguration (endast Intel)
- Dynamisk körgenomsökning av startblock (endast Intel)
- HP Sure Starts BIOS-inställningsskydd
- HP Sure Starts skydd av nycklar för säker start
- Utökad intrångsidentifiering under körning för inbyggd HP-programvara (endast Intel)
- Intrångsidentifiering under körning för inbyggd HP-programvara (endast AMD)
- HP Sure Starts policy för säkerhetshändelser
- HP Sure Starts startmeddelande för säkerhetshändelse
- Lås BIOS-version
- Spara/återställ systemdiskens MBR
- Spara/återställ systemdiskens GPT
- Återställningspolicy för startsektor (MBR/GPT)

### Verifiera startblock vid varje uppstart

HP Sure Start verifierar alltid integriteten för systemflashminnets BIOS-startblock innan du återupptar arbetet från viloläge, strömsparläge eller omstart. När detta är inställt på **aktivera**, verifierar även HP Sure Start startblockets integritet vid varje uppstart (omstart av Windows). Avvägningen att beakta är snabbare omstartstid kontra ökad säkerhet. Denna funktions standardinställning är **inaktivera**.

### BIOS-dataåterställningspolicy

När denna är inställd på **Automatisk**, reparerar HP Sure Start automatiskt BIOS eller datorns unika data när så är nödvändigt. När denna är inställd på **Manuell**, kräver HP Sure Start en särskild nyckelsekvens för att fortsätta med reparationen. I händelse av ett problem med startblockskoden, vägrar systemet att starta och systemets lysdioder initierar en unik blinkningssekvens. I händelse av ett problem med datorns unika data, visar systemet ett meddelande på skärmen. Den nyckelsekvens som krävs, och den blinkningssekvens som visas, varierar beroende på om systemet är en bärbar dator, en stationär dator eller en platta. Manuellt läge är användbart för användare som kan utföra systemanalys på systemets flash-innehåll före reparation. Vanliga användare rekommenderas inte att använda manuellt läge. Denna funktions standardinställning är **Automatisk**.

### Återställning av nätverksstyrenhetens konfiguration (endast Intel)

Denna kontroll finns endast tillgänglig på Intel-system. När denna väljs återställer HP Sure Start genast nätverksstyrenhetens konfiguration till fabriksinställningarna.

### Fråga vid ändring av nätverksstyrenhetens konfiguration (endast Intel)

Denna inställning finns endast tillgänglig på Intel-system. HP tillhandahåller en fabriksdefinierad konfiguration av nätverksstyrenheten som innehåller MAC-adressen. När denna inställning är inställd på **aktivera**, övervakar systemet statusen på nätverksstyrenhetens konfiguration och frågar användaren om en ändring av fabriksinställningarna upptäcks. Denna funktions standardinställning är **inaktivera**.

### Dynamisk körgenomsökning av startblock (endast Intel)

Denna inställning finns endast tillgänglig på Intel-system. Vid standardinställningen **aktivera** kontrollerar HP Sure Start regelbundet BIOS-startblockets integritet medan OS körs. När denna är inställd på **inaktivera**, kontrollerar HP Sure Start endast integriteten före en start eller återupptagning från viloläge eller strömsparläge.

### HP Sure Starts BIOS-inställningsskydd

Policyn för BIOS-inställningsskyddet är **inaktiverad** som standard. För att aktivera funktionen måste klientenhetens ägare/ administratör först konfigurera alla BIOS-policyer till den önskade inställningen. Ägaren/administratören behöver också konfigurera ett administratörslösenord för BIOS-konfiguration för att använda HP Sure Starts BIOS-inställningsskydd.

När detta har slutförts bör policyn för BIOS-inställningsskydd ändras till "aktiverad". Vid denna tidpunkt skapas en säkerhetskopia av alla BIOS-inställningar i HP Sure Starts skyddade lagring. Dessutom kan inga av BIOS-inställningarna ändras lokalt eller på distans. Vid varje start verifieras BIOS-policyinställningarna så att de är i önskat läge, och om någon diskrepans föreligger återställs BIOS-inställningarna från HP Sure Starts skyddade lagring.

För att modifiera en BIOS-inställning måste BIOS-administratörslösenordet anges och BIOS-inställningsskyddet inaktiveras, innan ändringar kan utföras på BIOS-inställningarna.

### HP Sure Starts skydd av nycklar för säker start

Med denna fabriksinställning på **aktivera**, ger HP Sure Start utökat skydd av de databaser med säker start och nycklar som används av BIOS för att bekräfta integriteten och autenticiteten av OS-starthanteraren innan den startas. När denna är inställd på **inaktivera**, används endast standardvarianten av UEFI:s variabelskydd för säker start och ingen säkerhetskopia lagras av HP Sure Starts undersystem.

### Utökad intrångsidentifiering under körning (RTID) för inbyggda HP-programvaran (endast Intel) och intrångsidentifiering under körning för inbyggda HP-programvaran (endast AMD)

RTID-funktionen är **aktiverad** som standard för alla plattformar som lämnar HP-fabriken. Slutkunden/administratören behöver inte aktivera eller på annat sätt "sätta igång" funktionen för att dra nytta av HP Sure Start RTID.

RTID-funktionen kan alternativt ställas in på **inaktiverad** av plattformsägaren/-administratören.

### HP Sure Starts policy för säkerhetshändelser

Denna BIOS-policyinställning styr vilken åtgärd som vidtas när HP Sure Start upptäcker ett angrepp eller försök till angrepp medan operativsystemet körs. Det finns tre möjliga konfigurationer för denna policy:

- **Logga endast händelse**: När denna inställning är vald loggar HP ESC identifieringshändelser, vilka kan visas i Program- och tjänstloggar/HP Sure Start i Microsoft Windows Loggboken.[3]
- **Logga händelse och meddela användare**: Detta är standardinställningen. När denna inställning är vald loggar HP ESC identifieringshändelser, vilka kan visas i Program- och tjänstloggar/HP Sure Start i Microsoft Windows Loggboken. Användaren kan dessutom meddelas i Windows om att händelsen inträffade.[4]
- **Logga händelse och stäng av systemet**: När denna inställning är vald loggar HP ESC identifieringshändelser, vilka kan visas i Program- och tjänstloggar/HP Sure Start i Microsoft Windows Loggboken. Användaren kan dessutom meddelas i Windows om att händelsen inträffade, och att systemet är på väg att stängas av.

### HP Sure Starts startmeddelande för säkerhetshändelse

Den här BIOS-policyinställningen styr huruvida varningar och felmeddelanden från HP Sure Start som visas när systemet startas kräver att den lokala användaren bekräftar felet innan starten fortsätter. Med standardinställningen **Kräv bekräftelse** stannar systemet och visar ett felmeddelande. Den lokala användaren måste trycka på en tangent för att fortsätta uppstarten. Om detta ändras till **Avbrott efter 15 sekunder** visas meddelandet, men uppstartsprocessen fortsätter automatiskt efter att meddelandet har visats i 15 sekunder.

### Lås BIOS-version

I (F10) BIOS-konfigurationen finns denna funktion i Huvudfönster/uppdatera system-BIOS.

När denna är inställd på **inaktivera** kan du uppdatera BIOS med hjälp av någon process som stöds. När HP ESC upptäcker en giltig startblocksuppdatering i systemflashminnet, uppdaterar den startblockets säkerhetskopia.

Om denna är inställd på **aktivera** vägrar alla HP BIOS-uppdateringsverktyg att uppdatera BIOS. Dessutom skyddar HP Sure Start BIOS från försök att ändra BIOS-versionen genom att ta bort systemflashminnet via en obehörig metod. HP ESC registrerar den låsta versionen av BIOS. När HP ESC upptäcker att BIOS i systemflashminnet ändrades, skriver HP ESC över BIOS-startblocket med HP ESC:s kopia av startblocket. HP ESC:s kopia av startblocket körs och återställer det som återstår av den korrekta versionen av BIOS. Denna funktions standardinställning är **inaktivera**.

### Spara/återställ systemdiskens MBR och Spara/återställ systemdiskens GPT

I (F10) BIOS-konfigurationen finns denna funktion i Säkerhet/Hårddiskhjälpmedel. Endast en av dessa funktioner är tillgängliga, beroende på den primära enhetens partitionstyp (GPT eller MBR), som upptäckts av HP Sure Start.

När denna är inställd på **aktivera**, behåller HP Sure Start en skyddad säkerhetskopia av MBR/GPT-partitionstabellen från den primära enheten och jämför säkerhetskopian med primärenheten vid varje start. Om en skillnad upptäcks meddelas användaren och kan välja att utföra en återställning från säkerhetskopian till det ursprungliga tillståndet, eller uppdatera den skyddade säkerhetskopian med ändringarna. **Återställningspolicyn för startsektor (MBR/GPT)** kan alternativt användas för att åsidosätta användarens beslut för den åtgärd som vidtagits i händelse av att en diskrepans hittades av HP Sure Start.

När denna är inställd på **inaktivera** (standard), ger HP Sure Start inget skydd för MBR/GPT.

### Återställningspolicy för startsektor (MBR/GPT)

När denna är inställd på **Lokal användarkontroll** (standard) uppmanas användaren att vidta åtgärder när HP Sure Start upptäcker en ändring i MBR/GPT-partitionstabellen. När denna är inställd på **Återställ i händelse av skada**, återställer HP Sure Start automatiskt MBR/GPT till det sparade tillståndet de gånger skillnader påträffas.

## Fjärrhantering av policykontroller för HP Sure Start

Enligt fabriksstandard är HP Sure Starts policyer optimerade för den typiska användaren. Eftersom HP Sure Start är aktiverat som standard, behöver fjärradministratören inte vidta några åtgärder i syfte att aktivera (eller ”sätta igång”) HP Sure Start. Om en fjärradministratör önskar ändra inställningarna för HP Sure Start-policyn, kan samma Windows Management Instrumentation (WMI) API:er eller HP BIOS Configuration Utility-skript som används för att hantera andra plattformars BIOS-policyer användas för att managera HP Sure Start-policyer. Dessutom kan administratörer på distans styra HP Sure Start-funktioner med hjälp av insticksprogrammet Manageability Integration Kit (MIK) för Microsoft System Center Configuration Manager (SCCM).

Dessutom kan administratörer på distans styra HP Sure Start-funktioner och visa HP Sure Start-händelser med hjälp av insticksprogrammet Manageability Integration Kit (MIK) för Microsoft System Center Configuration Manager (SCCM).

## Slutsats

HP Sure Start levererar dessa huvudfördelar:

- **Oavbruten produktivitet** – HP Sure Start upprätthåller affärskontinuitet i händelse av ett angrepp eller oavsiktlig skada genom att eliminera driftstopp i väntan på IT/service.
- **Lägre kostnad** – HP Sure Starts förmåga till automatisk återställning reducerar samtalen till IT Help Desk och förbättrar produktiviteten, vilket i slutändan bidrar till lägre underhållskostnader för plattformen.
- **Sinnesfrid** – HP Sure Start har ett flertal säkerhetsfunktioner som finns tillgängliga för många program- och hårdvaruplattformar.

Skydda kritisk inbyggd BIOS-programvara från skadlig kod med branschledande intrångsidentifiering och automatisk reparation av inbyggd programvara som erbjuds av HP Sure Start, vilket endast finns tillgängligt på utvalda HP Elite-datorer.

## Bilaga A – HP Sure Start, generationsöversikt

HP introducerade Sure Start 2014. Sedan dess har HP förbättrat Sure Start och utökat det antal produkter som använder funktionen. Tabellen nedan ger en sammanfattning av de funktioner som lagts till med varje generation.

| Generation | Utgivningsdatum | Tillagda funktioner |
|---|---|---|
| HP Sure Start | 2014 | • Autenticitetshandhavande av inbyggd programvara och BIOS, med förmågan att självläka<br>• Övervakning och överensstämmelse av inbyggd programvara |
| HP Sure Start med dynamiskt skydd | 2015 | • Stöd för Windows Loggboken<br>• Dynamiskt skydd (för utvalda Intel-produkter) |
| HP Sure Start Gen3 (utvalda Intel-produkter)[5]<br>HP Sure Start med intrångsidentifiering under körning (RTID) (utvalda AMD-produkter)[6] | 2017 | • Runtime Intrusion Detection<br>• BIOS-inställningsskydd<br>• Insticksprogrammet Manageability Integration Kit (MIK) för Microsoft SCCM |
| HP Sure Start Gen4[7] | 2018 | • Skyddad lagring – starka kryptografiska metoder för att lagra BIOS-inställningar, inloggningsuppgifter och andra inställningar i HP Endpoint Security Controller-hårdvaran för att tillhandahålla integritetsskydd, manipulationsidentifiering och konfidentialitetsskydd för dessa data<br>• Skydd för databas över säker start – utökat skydd för databaser och nycklar som lagras av BIOS som är avgörande för integriteten gällande operativsystemets funktion för säker start kontra standardvarianten av UEFI:s BIOS-implementering<br>• På Intel-plattformar, utökat skydd och återställning av inbyggd Intel Management Engine-programvara<br>• Säkerhetscertifiering av tredje part av HP Endpoint Security Controller – testning av ett oberoende och ackrediterat laboratorium för att bekräfta att HP ESC-hårdvarans kärnfunktionalitet fungerar enligt kraven på offentligt tillgängliga kriterier, metodik och processer[1]<br>• HPs företagsdatorer med HP Sure Start överträffar riktlinjerna enligt Draft NIST Platform Firmware Resiliency (Special Publication 800-193) |

## Bilaga B – översikt av System Management Mode (SMM)

System Management Mode (SMM) är en metod enligt branschstandard som används för PC-baserade avancerade energihanteringsfunktioner och andra OS-oberoende funktioner medan operativsystemet körs. Även om SMM-termen och dess implementering är specifik för x86-arkitektur, använder många moderna datorarkitekturer ett liknande arkitektoniskt upplägg.

SMM konfigureras av BIOS vid uppstart. SMM-koden upptas i huvudminnet (DRAM) och BIOS använder sedan speciella (låsbara) konfigurationsregister i chipset för att blockera åtkomst till detta område när mikroprocessorn inte exekveras i en SMM-kontext. Vid körning är inmatning i SMM-läge händelsestyrt. Chipsetet är programmerat att känna igen många olika typer av händelser och avbrott. När en sådan händelse inträffar aktiverar chipsethårdvaran ingångsstiftet System Management Interrupt (SMI). Vid nästa instruktionsgräns sparar mikroprocessorn hela sitt tillstånd och går in i SMM.

När mikroprocessorn går in i SMM aktiverar den ett utgångsstift för hårdvaran, SMI Active (SMIACT). Detta stift meddelar chipsethårdvaran att mikroprocessorn går in i SMM. En SMI kan aktiveras när som helst, under vilket processdriftläge som helst, förutom inom SMM själv. Chipsethårdvaran känner igen SMIACT-signalen och omdirigerar alla efterföljande minnescykler till ett skyddat minnesområde (ibland kallat SMRAM-området), som är reserverat särskilt för SMM. Omedelbart efter att ha mottagit SMI-inmatningen och aktiverat SMIACT-utgången börjar mikroprocessorn att spara hela sitt interna tillstånd till detta skyddade minnesområde.

När mikroprocessortillståndet har lagrats till SMRAM-minne börjar den särskilda SMM-hanterarkoden som också finns i SMRAM (vilken placerats där av system-BIOS vid uppstart) exekvering i ett speciellt SMM-driftsläge. I det här läget är de flesta hårdvaru- och minnesisoleringsmekanismer avstängda, och mikroprocessorn kan få tillgång till praktiskt taget alla plattformsresurser för att kunna utföra nödvändiga uppgifter. SMM-koden slutför den nödvändiga uppgiften, och därefter är det dags att återställa mikroprocessorn till tidigare driftsläge. Vid denna tidpunkt kör SMM-koden instruktionen Return from System Management Mode (RSM) för att lämna SMM. Denna RSM-instruktion gör att mikroprocessorn återställer sina data från sitt tidigare interna tillstånd från den kopia som sparats i SMRAM vid ingång till SMM. Efter slutförandet av RSM har hela mikroprocessortillståndet återställts till det tillstånd som gällde strax innan SMI-händelsen, och det tidigare programmet (operativsystem, program, hypervisor etc.) återupptar exekvering där det senast slutade.

[1] HP Sure Start Controller-hårdvaran har certifierats enligt CSPN:s certifieringsram.

[2] HP Sure Start med dynamiskt skydd finns tillgängligt på HP Elite-produkter utrustade med 6:e generationens Intel Core-processorer eller senare.

[3] HP Notification-programvara måste installeras för att visa HP Sure Start-händelser i Windows Loggboken.

[4] HP Notification-programvaran måste installeras för att ta emot meddelanden.

[5] HP Sure Start Gen3 finns tillgängligt på HP Elite-produkter utrustade med 7:e generationens Intel-processorer.

[6] HP Sure Start med intrångsidenfiering under körning (RTID) finns tillgängligt på HP Elite-produkter utrustade med 7:e generationens AMD-processorer.

[7] HP Sure Start Gen4 finns tillgängligt på HP Elite- och HP Pro 600-produkter utrustade med 8:e generationens processorer från Intel eller AMD.

Läs mer
hp.com/go/computersecurity



4AA7-3172SVE, Maj 2018