Teknik İş Raporu

HP Sure Start

Otomatik BIOS seviyesinde koruma ve onarım

Mayıs 2018

İçindekiler

Giriş

HP Sure Start, bir BIOS saldırısını otomatik olarak tespit edebilir, durdurabilir ve böyle bir saldırıya ya da bozulmaya karşı, bir IT müdahalesine gerek kalmadan ve kullanıcı üretkenliği üzerinde az miktarda kesinti ya da sıfır kesinti ile kurtarma sağlayabilir. Bilgisayar her açıldığında, HP Sure Start bilgisayarın kötücül saldırılara karşı korunduğundan emin olmak için BIOS kodu bütünlüğünü otomatik olarak doğrular. Bilgisayar faal duruma geçtiğinde, çalıştırma saldırı tespiti, sürekli olarak belleği gözlemler. Bir saldırı olması halinde, bilgisayar bir dakikadan daha kısa bir süre içerisinde BIOS'un izole edilmiş bir "altın kopyasını" kullanarak kendisini onarabilir.

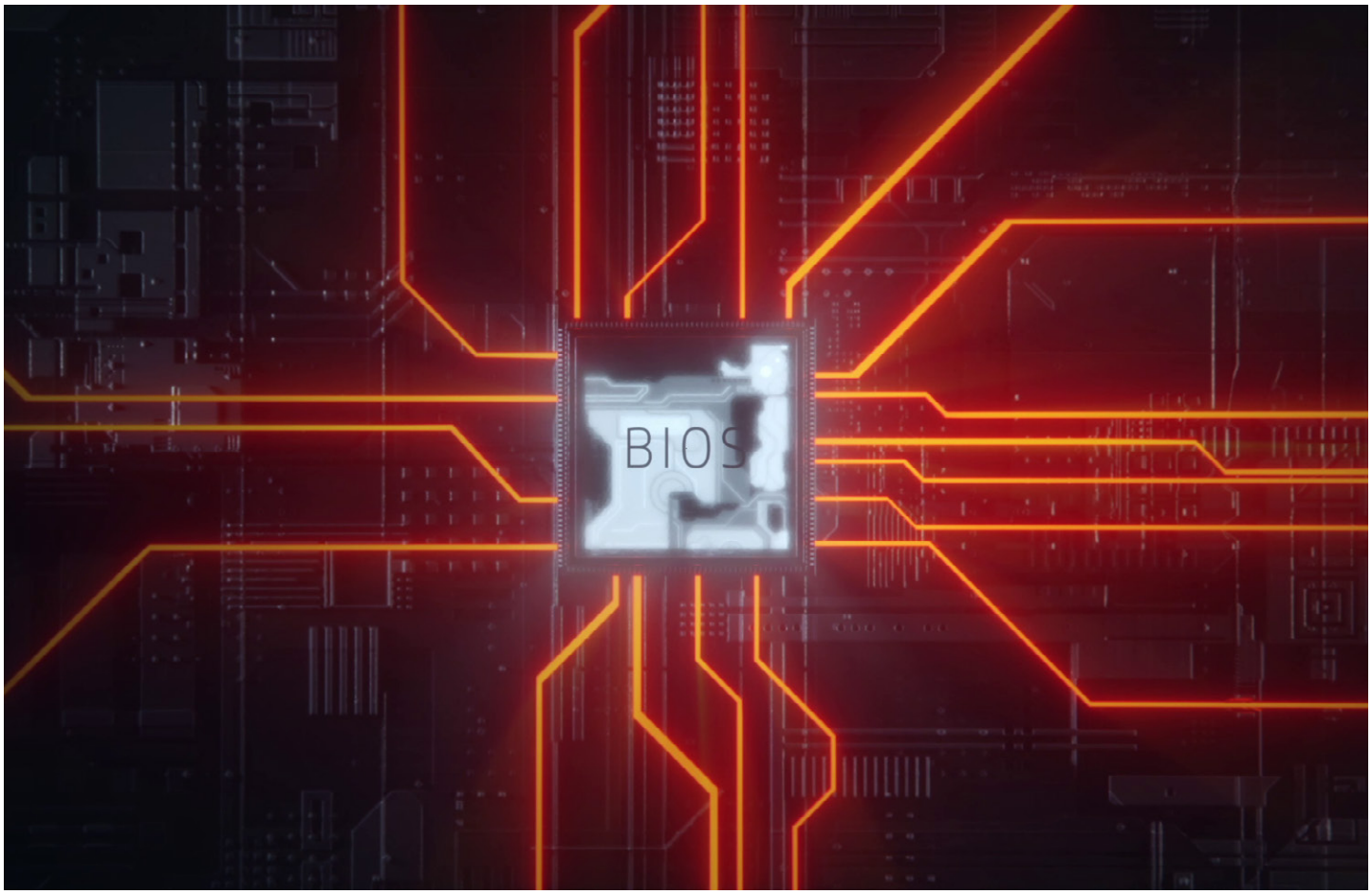
BIOS koruması neden önemlidir?

Dünyamız daha da bağlantılı hale geldikçe, siber saldırılar artan bir sıklık ve karmaşıklıkla istemci cihazı yazılım ve donanımını hedef alıyor. Yazılımlara saldırmak için kullanılan araçlar ve teknikler, bir zamanlar teorik düzeydeydiler ve sadece ulus devletlerde bulunacağı düşünülürdü. O zamanlardan günümüze, böyle araç ve tekniklerin sadece varlığı tespit edilmekle kalmadı, aynı zamanda kamuya açık bir şekilde erişilebildikleri de görüldü.

Cihaz yazılımı (veya BIOS) saldırganlara başarılı bir ihlalin sağlayabileceği aşağıdaki muhtemel nitelikler nedeniyle saldırganlar için çekici bir hedeftir:

- Kalıcılık: Aygıt yazılımı, devre kartı üzerindeki kalıcı bellekte bulunur ve sadece sabit sürücünün silinmesi ile ortadan kaldırılamaz.
- Kontrol: Aygıt yazılımı, işletim sistemi alanı dışında, en yüksek ayrıcalık düzeyinde işlem gerçekleştirmektedir. Bu da işletim sisteminden bağımsız, kötü amaçlı yazılımların varlığını mümkün kılmaktadır.
- Gizlilik: Aygıt yazılımı, işletim sistemi ve sistem yazılımı tarafından tamamen ulaşılmaz olan bir bellek bölgesini işgal eder; anti-virüs programları tarafından taranamayacağı için de, asla tespit edilemeyebilir.
- Kurtarma zorluğu: Tüm bu özellikler, sistem kartının değiştirilmesini de içeren bir hizmete başvurmadan, bu tür bir bozulmadan kurtarılmayı son derece zor kılmaktadır.

Cihazları bu tür saldırılara karşı koruyacak olan ideal çözüm, "siber dayanıklılık" prensipleri kullanılarak, donanım üzerinden tasarlanmıştır. Bu prensipler, olası her saldırıyı öngörmenin ve engellemenin, imkansız değilse de, son derece zor olduğunu kabul etmektedirler. İdeal çözüm, sadece aygıt yazılımın gelişmiş korumasını sağlamakla kalmaz, aynı zamanda hem başarılı bir saldırıyı tespit etme hem de bundan kurtulma amacıyla donanım kökenli bir kabiliyet de içermektedir.



HP Sure Start, yüksek seviyede aygıt yazılımı koruması sağlamaktadır

HP Sure Start, HP bilgisayarlarına ileri seviyede aygıt yazılımı koruması ve dayanıklılık sağlayacak olan eşsiz ve çığır açıcı bir yaklaşımdır. Endüstri standartlarının ötesine geçen bir BIOS koruması sağlamak için HP Endpoint Security Controller (HP ESC) üzerinden donanım uygulaması kullanır ve sistemin sadece Genuine HP BIOS ile başlamasını sağlar. Ek olarak, HP Sure Start'ın BIOS, aygıt yazılımı ya da çalışma System Management Mode (SMM) BIOS kodu ile oynandığını tespit etmesi halinde, korumalı bir yedek kopya kullanarak kurtarma sağlayabilir.

HP Sure Start özelliklerinin özeti

- HP çekirdek platformu aygıt yazılım aslına uygunluk uygulama ve kurcalamaya karşı koruma – HP Endpoint Security Controller sistem yüklemesinin donanım uygulatması, böylelikle sadece özgün ve modifiye edilmemiş HP aygıt yazılımı ve HP BIOS yüklenmesi
- Aygıt yazılım sağlıklı görüntüleme ve uyumluluk – İzole edilmiş HP Endpoint Security Controller ile sağlamlıkla ilişkili etkinliklerin aygıt yazılımı bağlanması; platformun aygıt yazılım durumunu sunar önlenmiş saldırıların belirtisi olabilecek anormallikler ile birlikte
- Kendini onarma – HP Endpoint Security Controller izole edilmiş HP BIOS ve HP aygıt yazılımı kullanarak HP BIOS ve HP aygıt yazılımı bozulmasının otomatik olarak onarılması
- BIOS ayarları koruması – HP ESC yedeklemesini dahil etme ve tüm kullanıcıların ya da admin tarafından ayarlanan BIOS ayarlarının bütünlüğünün kontrol edilmesi için, BIOS kodunun HP Endpoint Security Controller korumasını genişletme
- Program Saldırı Tespiti – İşletim sistemi çalışırken çalışma hafızası (SMM) içerisindeki kritik BIOS kodunun sürekli olarak görüntülenmesi
- Güvenli başlatma anahtar koruması – Standart UEFI BIOS uygulamalarına karşı işletim sistemi güvenli başlatma bütünlüğü için kritik olan ve BIOS tarafından saklanan veri tabanları ve anahtarların önemli ölçüde geliştirilmiş koruması
- Korumalı saklama – HP Sure Start, bütünlük korumasını sağlama, kurcalama tespit etme ve verinin gizliliğini koruma amaçlarıyla BIOS ayarlarını, kullanıcı yeterliliklerini ve diğer ayarları HP Endpoint Security Controller donanımı içerisinde saklamak için güçlü şifreleme yöntemleri kullanmaktadır
- Intel® Management Engine aygıt yazılımı koruması – Intel Management Engine aygıt yazılımı gelişmiş koruma ve kurtarması
- Yönetilebilirlik – Yöneticiler, HP Sure Start kabiliyetlerini Microsoft® System Center Configuration Manager (SCCM) eklentisi olan Manageability Integration Kit (MIK) ile yönetebilirler

HP Sure Start'ın her bir jenerasyonuna eklenmiş olan yeteneklerin bir özeti için Ek A sayfa 11'e bakın.

Üçüncü taraf güvenlik sertifikası

HP Sure Start bünyesinde kullanılan HP Endpoint Security Controller donanımı, üçüncü şahıslar tarafından güvenlik değerlendirilmesinden geçirilmiştir ve sadece yetkilendirilmiş aygıt yazılımının hedef bilgisayar üzerinde başlamasını sağlayacak donanım uygulamasını başlattığı belgelenmiştir.[1]

Bir güvenlik çözümünün belirtildiği şekilde çalıştığına dair güvence, güvenlik ürünleri ile ilgili tüm satın alma kararlarının kritik noktalarından biridir. Ayrıca, kalite itibarı sadece belli bir noktaya kadar gidebildiği için, HP, HP Endpoint Security Controller ürününün kamuya açık kriter, metodoloji ve süreçlere uygun olarak ve iddia edildiği şekilde çalıştığını onaylatmak adına, iç işleyişini, bağımsız ve akredite edilmiş bir laboratuvar tarafından incelemeye ve teste sunmuştur.

Sibere karşı dayanıklı tasarım

HP Sure Start, endüstrinin standart yaklaşımının ötesinde bir gelişmişliğe sahip BIOS koruması sağlamakla kalmaz, ayrıca bir ihlal ya da yok edici nitelikte bir saldırı durumunda dahi BIOS kurtarılmasını sağlamak amacıyla benzersiz bir sibere karşı dayanıklı platform sağlamak için donanımdan tasarlanmıştır. HP Sure Start içeren HP iş bilgisayarları, siber dayanıklı platformların gereksinimlerini biçimlendirmeye yönelik önde gelen kamu sektörü çalışmalarından olan National Institute of Standards Technology (NIST) Platform Aygıt Yazılım Sağlamlığı Taslak yönergelerinde (Özel Basım 800-193) belirtilen standartların daha da ötesine geçmektedir.

HP Sure Start destekli modeller

HP, Sure Start'ı 2014 yılında piyasaya sundu. O zamandan bu yana HP, Sure Start'ı geliştirmiş ve programı içeren ürünlerinin sayısını arttırmıştır. HP Sure Start, tabletlerin, dizüstü bilgisayarların, masaüstü bilgisayarların ve "hepsi bir arada" (AIO) ürünlerinin de dahil olduğu 2018 Elit ürünler serisinin tamamında bulunmaktadır. HP Sure Start Gen4, 8. Jenerasyon Intel ya da AMD® işlemciyle donatılmış HP Elite ve HP Pro 600 ürünlerinde bulunmaktadır.

Mimari genel bakış ve yetenekler

HP Sure Start, iki önemli mimari bileşenden oluşmaktadır:

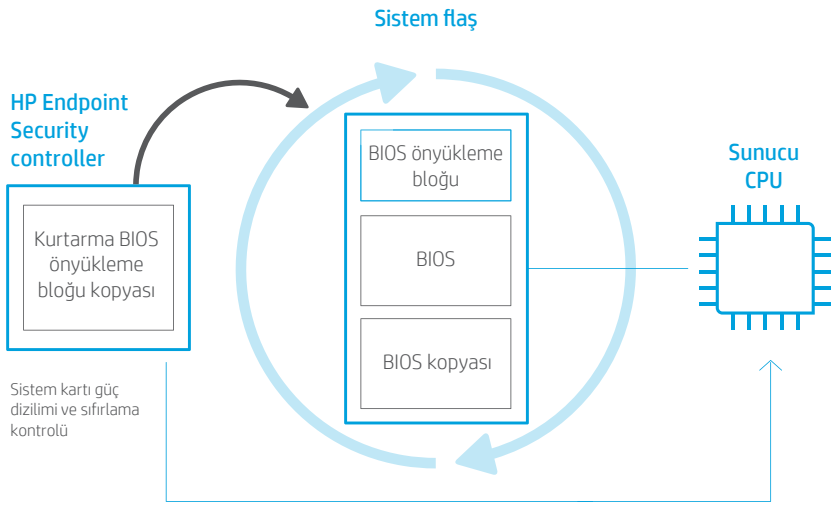
- **HP Endpoint Security Controller** HP Sure Start aygıt yazılımını çalıştırmaktadır
- **HP Sure Start BIOS** HP Endpoint Security Controller donanım ve aygıt yazılımı ile birlikte çalışmaktadır

Aygıt yazılımı bütünlüğünü doğrulama – HP Sure Start'ın temeli

HP Endpoint Security Controller (HP ESC), sistem önyüklemesinden çok önce, sistem açılıp da aktif hale geçtiği anda aygıt yazılımını çalıştıran ilk cihazdır. HP ESC etkinlikleri, sistem güç düğmesini görüntülemeyi ve kullanıcı açma düğmesine bastığında ana bilgisayar CPU uygulamasının başlangıcının güç sıralamasını oluşturmayı içerir, ancak bunlarla sınırlı değildir.

Güç platforma ilk kez ulaştırıldığında (sistem açılmadan önce), HP ESC, yükleme yapmadan ve kodu işletime almadan önce kendi aygıt yazılımının, gerçek HP kodu olduğunu doğrular. HP ESC donanımı, bütünlük doğrulamasını gerçekleştirmek için endüstri standardı olan güçlü şifreleme yöntemlerini kullanır. Yöntem, dahili kalıcı salt okunur belleğin içerisinde bulunan 2048-bit HP RSA ortak anahtarını kullanır. Bu nedenle, HP ESC, platform için, işleme alınmalarından önce, kendi aygıt yazılımını ve HP BIOS'u doğrulama amacıyla kullanılan içe yerleşik, donanım tabanlı bir Root of Trust'tır (RoT - Güven Kökü). Bu Root of Trust donanımı, yüklenme yöntemlerine bakılmaksızın, aygıt yazılımını değiştirme saldırılarına karşı koruma sağlar ve HP platform güvenliğinin de üzerine kurulacağı temeli sunmuş olur.

Şekil 1. Aygıt yazılım bütünlüğü doğrulama süreci.



Şekil 1, aygıt yazılım bütünlüğü doğrulama sürecini göstermektedir. HP ESC, HP Sure Start aygıt yazılımının doğrulunu tasdik edip işleme almaya başladığında, bu aygıt yazılımı, sistem flash BIOS önyükleme bloğunun bütünlüğünü doğrulamak için aynı güçlü şifreleme işlemlerini kullanmaktadır. Tek bir bitin geçersiz olması durumunda, HP ESC, sistem flash bileşenlerini, HP ESC için ayrılmış olan izole edilmiş kalıcı bellek (NVM) içerisinde saklanan kendi HP BIOS önyükleme bloğu ile değiştirir.

HP Sure Start tasarımı, hem HP ESC hem ana CPU'da çalışan tüm aygıt yazılımlarının ve BIOS kodunun, HP'nin cihazda bulunmasını istediği kod olmasını sağlamaktadır.

Not: Sistem hafıza önyükleme bütünlük kontrolü ve HP ESC tarafından gerçekleştirilen her türlü gerekli kurtarma, ana CPU kapalı iken gerçekleşmektedir. Böylelikle, kullanıcı bakış açısından bakıldığında, tüm işlem, sistem hala kapalı iken, uyku modunda ya da hazırda bekleme modundayken gerçekleşir.

Sistem hafızası BIOS önyükleme bloğu HP BIOS'un temelidir. HP ESC donanımı, bir sıfırlamanın ardından CPU'nun yürüttüğü ilk kodun BIOS önyükleme bloğu olmasını sağlamaktadır. HP ESC, BIOS önyükleme bloğununun gerçek HP kodu içerdiğini belirlediğinde, sistemin normal bir şekilde önyükleme yapmasına izin verir.

HP ESC, aynı zamanda, sistemin her kapanması, uyku ya da hazırda bekleme moduna alınması esnasında, sistem hafıza önyükleme blok kodunun bütünlüğünü kontrol eder. CPU'nun, bu durumların her birinde kapanması sebebiyle ve bu durumda devam etmek için CPU'nun BIOS önyükleme kodunu yeniden yürütmesi gerektiğinden, müdahaleye karşı kontrol için BIOS önyükleme bloğunun bütünlüğünün her seferinde yeniden onaylanması önem taşımaktadır.

Ek olarak, HP Intel modelleri için, HP Sure Start, sistem çalışıyorken periyodik olarak (her 15 dakikada bir) sistem hafızası BIOS önyükleme bloğunun bütünlüğünü kontrol eder.[2]

Makineye özgü veri bütünlüğü

HP ESC ve BIOS, belli bir platformun kullanım süresi boyunca değişmeden kalması hedeflenen ve her bir makinenin kendisine özgü olan fabrika ayarlı kritik değişkenlere ileri seviye koruma sağlamak için birlikte çalışırlar. Fabrikada, bu değişken verinin yedek kopyası, HP ESC silinmeyen bellek hafızasında saklanır. Yedek, HP Sure Start BIOS bileşeni için, her önyüklemede verinin bütünlük kontrolünün sağlanması amacıyla, sadece salt-okunur seviyede erişilebilir durumdadır. Paylaşılan hafızanın ayarlarında, fabrika ayarlarına kıyasla bir değişiklik olması halinde, HP Sure Start BIOS bileşenleri, HP ESC tarafından sağlanan yedek kopyayı kullanarak Sistem Hafızasındaki veriyi otomatik olarak geri getirir.

Tanımlayıcı bölge

HP Intel modelleri için, HP Sure Start, sistem hafızasının tanımlayıcı bölgesini korumaktadır. Intel mimarisine özgü olarak, tanımlayıcı bölge, yeniden başlatma esnasında Intel Core™ mantığı tarafından örneklenen ve ardından Core (Çekirdek) mantığını yapılandırmak için kullanılan tüm kritik konfigürasyon parametrelerini içermektedir. Tanımlayıcı bölge, sistem hafızası için, Intel Core mantığı tarafından BIOS bölgesinin hafıza içerisinde nereye yerleştiğini ve böylelikle sıfırlama esnasında işleme geçme için CPU'nun kodu nereden aldığını belirleme amacıyla kullanılan bellek bölümleme bilgisini de içerir. HP Sure Start, bu bölgenin bütünlüğünü izler ve bir müdahale ya da bozulma durumunda, olması gereken ayarlarına geri döndürür.

Ağ denetleyicisi koruma

Ek olarak, HP Intel modelleri için, HP Sure Start, sistem hafızası içinde bulunan ağ denetleyicisi (NIC) ayarlarını korumaktadır. Bazı HP müşterilerinin, fabrika ayarlarındaki NIC ayarlarında meşru değişiklikler yapması gereken kullanım alanları vardır. Bu sebeple, HP Sure Start, NIC ayarları üzerindeki değişiklikleri kendiliğinden engellemez. Bunun yerine HP Sure Start, etkinleştirildiğinde NIC ayarlarının değiştiğine dair kullanıcıyı uyaran bir özellik sunar. Buna ek olarak, HP Sure Start, NIC ayarlarını fabrika değerlerine döndürmek için bir yöntem sunmaktadır. Korunulan ayarlar arasında, MAC adresi, Pre-boot Execution Environment (PXE) ayarları ve uzaktan başlangıç programı yükleme (RPL) bulunmaktadır. Bu geri yükleme, HP ESC tarafından korunan bir salt okunur yedek kopya ile mümkün olmaktadır

BIOS ayarlarını koruma

Daha önce tanımlandığı gibi, HP Sure Start, HP BIOS kodunun doğruluğunu ve bütünlüğünü doğrulamaktadır. Bu kod, HP tarafından oluşturulduktan sonra sabit olduğu için, her iki özelliği de onaylamak için dijital imzalar kullanılabilir. Ancak, BIOS ayarlarının dinamik ve kullanıcı tarafından ayarlanabilir doğası, bu ayarları korumak için ek zorluklar oluşturmaktadır. Bu ayarları doğrulamak için, HP tarafından dijital imzalar oluşturulamaz ve HP Sure Start ESC donanımı tarafından kullanılamaz.

HP Sure Start BIOS ayarları koruması, sistemin ayarlarının, yapılandırılabilmesi yeteneğini sunmaktadır. Böylelikle HP ESC donanımı, yedekleme için kullanılır ve kullanıcı tarafından tercih edilen tüm BIOS ayarlarının bütünlüğünü kontrol eder.

Bu özellik platform üzerinde aktif hale getirildiğinde, bunu takiben BIOS tarafından kullanılan tüm ilke ayarları yedeklenir ve her önyüklemede, BIOS ilke ayarlarının değiştirilmediğinden emin olmak için bir bütünlük kontrolü gerçekleştirilir. Bir değişikliğin tespit edilmesi halinde, sistem kullanıcı tarafından tanımlanan ayarlara otomatik olarak geri dönmek için, HP Sure Start korumalı saklama alanındaki yedek kopyayı kullanmaktadır.

HP Sure Start BIOS ayarları koruma özelliği, BIOS ayarlarını değiştirmeye yönelik bir girişimin tespit edilmesi halinde, HP Sure Start ESC donanımı üzerinde olay oluşturur. Olay, HP Sure Start denetim kaydına kaydedilir ve yerel kullanıcı, önyükleme esnasında BIOS'dan bildirim alır.

HP Sure Start korumalı depolama

HP Endpoint Security Controller donanımı içine yerleştirilmiş korumalı depolama alanı, HP Sure Start tarafından korunan BIOS/aygıt yazılım verisi ve ayarlar için en yüksek seviyede koruma sunmaktadır. HP Sure Start korumalı saklama alanı, saldırganın sistemi parçalarına ayırdığı ve devre kartı üzerindeki geçici olmayan saklama cihazına doğrudan bağlantı kurduğu fiziksel saldırı senaryolarında dahi gizlilik, bütünlük ve müdahale tespiti sağlamak için tasarlanmıştır.

Veri bütünlüğü

Geçici olmayan hafızada, aygıt yazılımı tarafından saklanan ve çeşitli yeteneklerin durumunu kumanda etmek amacıyla kullanılan dinamik verinin bütünlüğü, platform genelinde güvenlik duruşu açısından kritik önem taşımaktadır. Dinamik veri, cihazın son kullanıcısı ya da yöneticisi tarafından değiştirilebilir tüm BIOS ayarlarını içermektedir. Örnekler, bunlarla sınırlı kalmamakla birlikte, şunları içermektedir: güvenli önyükleme özelliği gibi önyükleme seçenekleri, BIOS yönetici şifresi ve ilgili ilkeler, Trusted Platform Module (Güvenilir Platform Modülü) durum kontrolü ve HP Sure Start ilke ayarları.

Bu ayarlar üzerinde yetkilendirilmemiş değişiklikleri engellemek amacıyla oluşturulan mevcut erişim sınırlandırmalarını aşan her başarılı saldırı, platform güvenliğini ortadan kaldırabilir. Örneğin, bir saldırganın, tespit edilemeden, güvenli önyükleme özelliğini devre dışı bıraktığı yetkilendirilmemiş bir değişim gerçekleştirdiği bir senaryoyu ele alalım. Bu senaryoda, kullanıcının bilgisi olmadan, işletim sistemi başlamadan önce saldırganın korsanlık programı, platform tarafından ön yüklenecektir.

Endüstri standartında Unified Extensible Firmware Interface (UEFI) BIOS, bu değişkenler üzerinde yetkilendirilmemiş değişimleri engelleyecek erişim sınırlandırmaları uygulamaktadır ve HP de bunları, bilgisayar endüstrisinin geri kalanının uyguladığı şekilde uygulamaktadır.

Ancak, platformun taşıdığı bu mekanizmalara ihlal risklerinden dolayı, HP Sure Start, temel endüstri standartlarından daha güçlü olan ikincil savunmalar sunmaktadır.

HP Sure Start tarafından korunan, aygıt yazılımı tarafından durum kontrolü için kullanılan BIOS ayarları ve diğer dinamik veriler, HP Endpoint Security Controller'ın, ana CPU üzerinde çalışan yazılım tarafından doğrudan erişilebilir durumda olmayan, izole edilmiş ve geçici olmayan bir bölgesinde saklanmaktadır.

Ek olarak, geçici olmayan bu hafıza alanına her veri parçası kaydedildiğinde, HP ESC özgün bütünlük önlemleri oluşturmakta ve eklemektedir. Bütünlük önlemleri, HP ESC içerisinde gizlenmiş ve yerleştirilmiş güçlü bir şifreleme algoritmasına (SHA-256 hashing (karma) kullanan karma-tabanlı mesaj onaylama kodu) dayandırılmaktadır. Bu sır, her bir HP ESC için özgündür, öyle ki her bir denetleyici benzer öğelere, eşsiz bir bütünlük önlemleri oluşturmaktadır.

Veri öğesi geçici olmayan hafızadan yeniden okunduğunda, HP ESC veri bileşeni için bütünlük önlemlerini yeniden hesaplar ve bunu veriye eklenmiş olan bütünlük önlemi ile kıyaslar. Bu geçici olmayan hafıza alanı içindeki verilere uygulanan her yetkilendirilmemiş değişiklik, bir yanlış eşleşme ile sonuçlanır. Bu yaklaşımı kullanarak, geçici olmayan hafıza bölgesindeki veri bileşenleri üzerinde yapılan oynamalar, HP ESC tarafından tespit edilebilir.

Veri gizliliği

Platform tarafından saklanan birçok veri bileşeni için, gizliliği korumak kritik öneme sahiptir. Örnekler arasında, BIOS yönetici şifre karmaları, kullanıcı yeterlilikleri ve isteğe bağlı olarak kullanıcı adına, HP Sure Run ve HP Sure Recovery gibi aygıtsal yazılım tabanlı özellikler için aygıtsal yazılım içerisine yüklü olan parolalar bulunmaktadır.

Bu parolaların endüstri standardı olan UEFI BIOS yaklaşımları kullanılarak okunması zorluk oluşturmaktadır zira, geçici olmayan hafıza, genel olarak ana işlemci üzerindeki yazılım tarafından okunabilmektedir. HP Sure Start korumalı saklama alanı, standart bir UEFI BIOS uygulamasına kıyasla, gizli verinin çok daha iyi bir şekilde koruması amacı taşımaktadır.

Ayrı ve izole edilmiş bir saklama alanına ek olarak, HP Sure Start yaklaşımı, HP Sure Start geçici olmayan hafızasında saklanılan tüm veri bileşenleri üzerinde AES-256 şifrelemesi uygulamak için, HP ESC içerisinde bulunan Advanced Encryption Standard (AES) yazılım bloğunun geliştirilmesi ve ilgili veri bileşenleri için veri bütünlük önlemlerinin alınmasıdır. Her bir HP ESC için kullanılan şifreleme anahtarı özgündür ve asla kumandayı bırakmaz, böylelikle her bir HP ESC bileşeni tarafından şifrelenen verinin şifresi, sadece aynı HP ESC tarafından çözülebilir.

Güvenli önyükleme anahtar koruması

HP Sure Start, endüstri standartlarındaki UEFI güvenli önyükleme uygulamalarına kıyasla, aygıt yazılımı tarafından saklanmakta olan UEFI güvenli önyükleme anahtar veritabanları için daha gelişmiş koruma sağlar. Bu değişkenler, önyüklemede başlamasına izin vermeden önce, işletim sistemi ön yükleyicisinin bütünlüğünü ve gerçekliğini doğrulayan UEFI güvenli önyükleme özelliğinin uygun şekilde işletilmesi için kritik önem taşımaktadır.

HP Sure Start, HP Sure Start korumalı alanında bir orijinal kopya tutarak, UEFI güvenli önyükleme anahtarı veritabanlarını korur. Yürütme zamanında işletim sistemi tarafından UEFI standart güvenli önyükleme veri tabanlarına yapılan yetkilendirilmiş değişiklikler, HP Sure Start tarafından takip edilir ve HP ESC tarafından orijinal kopyaya uygulanır. Ardından, HP Sure Start, HP Sure Start korumalı saklama alanındaki orijinal kopyayı, UEFI standart güvenli önyükleme anahtarı veritabanları üzerindeki yetkilendirilmemiş değişiklikleri tespit etmek ve reddetmek için kullanır.

Kendinden etkin olan bu kabiliyet, aşağıdaki veritabanlarını kapsamaktadır:

- İmza veritabanı (db)
- İptal edilen imzalar veritabanı (dbx)
- Key Enrollment Key (KEK)
- Platform Key (PEK) işletim zamanında dinamik olarak güncellenen İşletim Sistemi tarafından

Runtime Intrusion Detection (RTID)

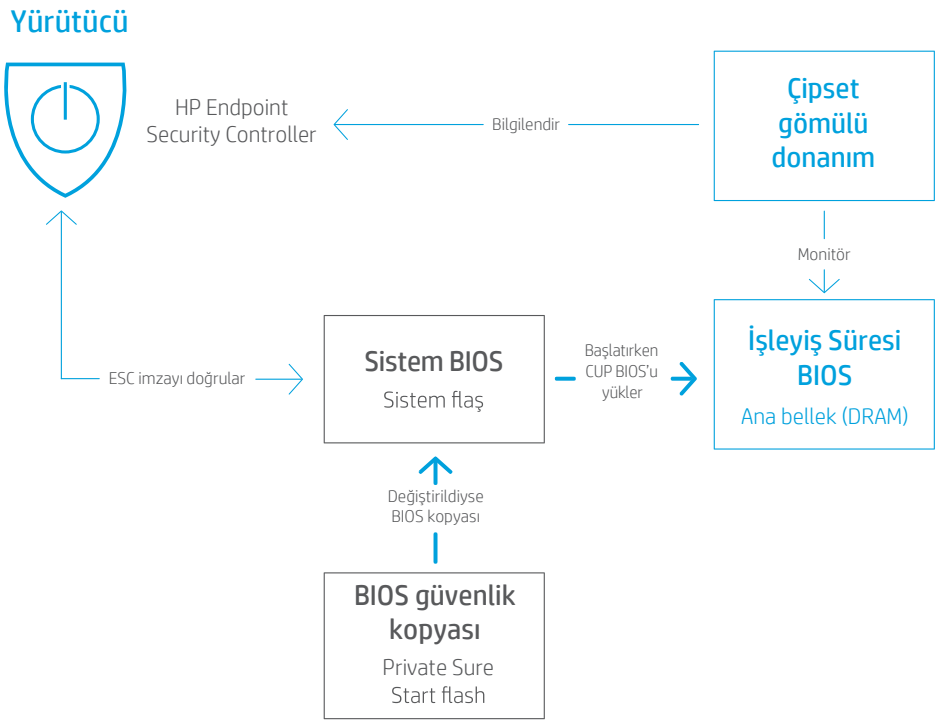
Her önyüklemede, BIOS kodu, sabitlenmiş bir adres üzerinde hafıza belleğinden işlemi başlatır. Bu, BIOS önyükleme kodu olarak bilinir ve "İşletim Sistemi Öncesi (Pre-OS)" yetenekler sunar, bunlara İşletim Sistemi başlatılmadan önce ihtiyaç duyulur. Ancak, BIOS'un DRAM içerisinde kalan bir bölümü vardır, bu bölüme gelişmiş güç yönetimi özellikleri, işletim sistemi hizmetleri ve işletim sistemi çalışmaktayken, işletim sisteminden bağımsız olarak çalışan diğer hizmetleri sağlamak için ihtiyaç duyulur. System Management Mode (SMM) olarak da bilinen bu BIOS kodu, DRAM içerisinde işletim sisteminden saklı tutulan özel bir bölgede bulunmaktadır. Bu koda, aynı zamanda, HP Sure Start'ın Runtime Intrusion Detection özelliği bağlamında "İşletim Zamanı" BIOS kodu da diyoruz. (SMM ve nasıl çalıştığına dair daha fazla detay için, lütfen sayfa 12'de bulunan Ek B'ye bakın).

SMM kodunun bütünlüğü, istemci aygıtı güvenlik postürü için de kritik önem taşımaktadır. HP Sure Start, HP SMM BIOS koduna, işletim sistemi başlatma anında dokunulmamış olduğundan emin olmak için kontrol gerçekleştirir. Runtime Intrusion Detection, yeni koruma kabiliyetleri ekleyerek ve/veya bu koda gerçekleşecek her türlü saldırıyı tespit etmek için yollar sunarak, işletim sistemi çalışmaktayken SMM BIOS koduna dokunulmadığından emin olmak için mekanizmalar sağlar.

Runtime Intrusion Detection mimarisi

RTID özelliği, İşletim Zamanı HP SMM BIOS içerisindeki anomalileri tespit etmek için platform yonga seti içerisinde bulunan özelleştirilmiş bir donanım kullanır. Anomalilerin tespit edilmesi sonucu, HP Endpoint Security Controller'a bir ileti gönderilir, o da CPU'dan bağımsız olarak yapılandırılmış ilke eylemini gerçekleştirebilir.

Şekil 2. Program Saldırı Tespiti, herhangi bir değişiklik karşısında SMM kodunu görüntülemek için platform yonga seti içerisine gömülü, özelleştirilmiş bir donanım kullanır.



Kullanıcı bildirimleri, olay günlüğü ve ilke yönetimi

HP Sure Start son kullanıcı bildirimleri

Normal işletim koşulları altında, HP Sure Start kullanıcıya görünmezdir. Kurtarma işlemleri, varsayılan ayarları kullanarak otomatik olarak gerçekleşir, genellikle HP Sure Start bir problem tespit ettiğinde, kurtarma işlemi için son kullanıcı ya da IT etkileşimine ihtiyaç duyulmaz.

Kullanıcılar, İşletim Sistemi çalışırken, HP Sure Start Dynamic Protection ya da Runtime Intrusion Detection özellikleri yoluyla, BIOS bütünlüğü ile ilgili bir problem tespit edildiğinde çalışma bildirimleri görebilirler. Önemli bir eylemin tespit edilmesi ya da aksiyon alınması halinde, HP Sure Start, bir sonraki önyükleme esnasında Windows® bildirimi yoluyla bir uyarı mesajı gösterir. HP Notifications Software (Bildirim Yazılımları), bu Windows bildirimlerini görüntülemeyi etkinleştirmek için gerekmektedir.

HP Sure Start olay günlüğü

HP Endpoint Security Controller, HP Sure Start tarafından görüntülenen aygıt yazılımı/BIOS kodu ve verilerle ilgili kritik olayları kaydeder. Bu olaylar, Sure Start geçici olmayan hafızası içerisine kaydedilirler. Bu olaylar, ilgili olaylara erişimin başlatılması için, HP Notifications Software (Bildirim Yazılımı) programının yerel kullanıcı tarafından ve bunun yanı sıra müşterinin tercih ettiği yönetilebilirlik acentesi tarafından kurulduğu anda, HP ESC'den Windows Event Viewer'a kopyalanır.

Aşağıdaki olaylar, HP Notifications Software'ın HP Sure Start alt sisteminden tüm olayları almasını tetikleyecektir ve Windows Event Viewer'ın, halihazırda kendisine kaydedilmemiş olaylarla güncellenmiş olmasını sağlayacaktır:

- Windows Önyükleme
- Windows Uyku/Bekleme Modundan Dönüş
- Dinamik koruma işletim zamanlı HP Sure Start olay bildirimleri
- HP Sure Start Runtime Intrusion Detection (RTID)

HP Bildirim Yazılımları, HP Sure Start içerisine, özgün bir "HP Sure Start" uygulama olay günlüğü yerleştirmektedir. Bu kayıtlarda sadece, HP Sure Start olayları yer alacaktır. HP Sure Start olaylarına uzanan Windows Event Viewer yolu, aşağıdaki gibidir: Sistem Araçları/Olay Görüntüleyici/Uygulama ve Hizmetler Kaydı/HP Sure Start.

HP Sure Start olayları ile ilgili Windows Event Viewer seviyesindeki kategoriler, aşağıdaki tabloda tanımlanmışlardır.

Olaylar, Windows Event Viewer içerisine, HP Sure Start tarafından oluşturuldukları sıra ile dizilirler. HP Sure Start altsistemi içindeki en eski olay, Windows Event Viewer içerisine öncelikle eklenir ve en yeni olay da en son eklenir.

Her bir Windows Event Viewer girişi için zaman pulu, olayın gerçekleştiği zaman DEĞİL, bu kayıtlara eklendiği zamandır. Her bir Sure Start Windows Event Viewer girişi, olay detayları içerisinde detaylı veri içermektedir, bu da olayın gerçekten olduğu zaman bilgisini de vermektedir.

Not: Olaylar, Windows Event Viewer'a kopyalandıktan sonra dahi HP Endpoint Security Controller içerisinde kalıcıdırlar. Windows Event Viewer programının temizlenmesi halinde, HP Notifications Software uygulaması, tüm HP Sure Start girdilerini, kendisini, HP Sure Start olay kayıtlarını incelemek için tetikleyen bir sonraki olayda yenileyecektir.

HP Sure Start Windows Event Viewer olay çeşitleri

Olay Seviyesi	Tanım
Bilgi	İşletimin normal seyri esnasında gerçekleşmesi beklenen olaylar (ör., BIOS'u güncellemek).
Uyarı	Gerçekleşen ama beklenmeyen, ancak HP Sure Start ile tamamen kurtarılan, platformun tamamen işlemsel hale dönmesi için bir kullanıcı/yönetici eyleminin gerçekleşmesine gerek duyulmayan olaylar. Bu olaylar, kullanıcı/yöneticinin, özellikle de bu olaylar birden fazla makinede yaşanma eğilimi gösteriyorsa, daha fazla incelemesini isteyebileceği olaylardır.
Hata	Tamamen kurtarılma sağlanması için, yöneticinin/HP servisinin platform üzerinde işlem gerçekleştirmesini gerektiren olaylar.

HP Sure Start ilke kontrolleri

Norm dışı, HP sistemi BIOS, olağan kullanıcı için HP Sure Start ilkelerini mümkün kılmakta ve optimize etmektedir. HP Sure Start'ın kendiliğinden aktif olması sebebiyle, olağan kullanıcının, HP Sure Start tarafından korunmak için ayarlarla oynaması gerekmemektedir. İleri seviye kullanıcılar için, sistem BIOS, (F10) BIOS Setup içinde bulunan ilke seçeneklerini kullanarak, HP Sure Start davranışı üzerinde bir miktar kontrol sağlamaktadır. Aksi belirtilmediği sürece, bu ayarlar ve fonksiyonlar Security (Güvenlik) /BIOS Sure Start altında bulunurlar.

Not: Politikalar, ana CPU tarafından doğrudan erişilebilir olmayan HP ESC geçici olmayan hafızasında saklanırlar; bu sebeple, herhangi bir Sure Start seçeneği aktif hala geçmeden önce, yeniden başlatma gerekmektedir.

Aşağıdaki HP Sure Start seçenekleri ve fonksiyonları mevcuttur:

- Her Önyüklemede Önyükleme Bloğunu Doğrulamak
- BIOS Veri Kurtarma Politikası
- Ağ Kumanda Konfigürasyon Geri Yüklemesi (sadece Intel)
- Ağ Kumanda Konfigürasyon Değişimi Komut İstemi (sadece Intel)
- Önyükleme Bloğunun Dinamik İşletim Zamanı Taraması (sadece Intel)
- HP Sure Start BIOS Ayarları Koruma
- HP Sure Start Güvenli Önyükleme Anahtarları Koruması
- Gelişmiş HP Aygıt Yazılımı Program Saldırı Önlenmesi ve Tespiti (sadece Intel)
- HP Aygıt Yazılım Runtime Intrusion Detection (sadece AMD)
- HP Sure Start Güvenlik Olayı Politikası
- HP Sure Start Güvenlik Olay Önyükleme Bildirimi
- Kilit BIOS Versiyonu
- Sistem Sabit Sürücü MBR Kurtarma/Onarımı
- Sistem Sabit Sürücü GPT Kurtarma/Onarımı
- Önyükleme Kesimi (MBR/GPT) Kurtarma Politikası

Her Önyüklemede Önyükleme Bloğunun Doğrulanması

HP Sure Start, uyku, bekleme ya da kapalı moddan dönmeden önce, her zaman sistem hafızası BIOS önyükleme bloğunun bütünlüğünü doğrulamaktadır. **Etkin** olarak ayarlandığında, HP Sure Start, her ılık önyüklemede (Windows yeniden başlatma) önyükleme bloğununun bütünlüğünü de doğrulamaktadır. Değerlendirmeye alınacak olan dengeleme faktörü, daha hızlı başlangıç süresi ile daha fazla güvenliğin kıyaslanması olacaktır. Bu özelliğin varsayılan ayarı **devre dışı bırak** ayarıdır.

BIOS Veri Kurtarma Politikası

Otomatik olarak ayarlandığında, HP Sure Start gerektiği durumlarda otomatik olarak BIOS ya da Machine Unique Data (Makine Özgün Verilerini) otomatik olarak onarır. **Manüel** olarak ayarlandığında, HP Sure Start onarıma geçmek için özel bir tuş bileşimine ihtiyaç duymaktadır. Önyükleme blok kodu ile ilgili bir sorun yaşanması halinde, sistem önyükleme yapmayı reddedecektir ve sistem LED ışığı üstünde özgün bir ışık uyarısı olacaktır. Machine Unique Data (Makineye Özgü Veri) ile ilgili bir sorun yaşandığında, sistem ekran üstünde bir mesaj gösterecektir. Gereken tuş kombinasyonu ve yanacak olan ışıklar, sistemin bir dizüstü bilgisayar, masaüstü bilgisayar ya da bir tablet olmasına göre farklılıklar gösterecektir. Manüel modu, tamir öncesi sistem hafızası üzerinde karartma (adli bilişim) uygulayabilecek olan kullanıcılar için faydalı olacaktır. Olağan kullanıcıların manüel modu kullanması tavsiye edilmez. Bu özelliğin, varsayılan ayarı **Otomatik** ayardır.

Ağ Denetleyicisi Konfigürasyon Yenilemesi (sadece Intel)

Bu kontrol, sadece Intel sistemlerinde mevcuttur. Seçildiğinde, HP Sure Start ağ denetleyici konfigürasyonunu anında fabrika ayarlarına döndürür.

Ağ Denetleyicisi Konfigürasyon Değişim Sevki (sadece Intel)

Bu seçenek, sadece Intel sistemlerinde mevcuttur. HP, MAC adresini de içeren, fabrika tarafından tanımlanmış ağ denetleyicisi konfigürasyonu sunmaktadır. Bu seçenek **etkin** olarak ayarlandığında, sistem, ağ denetleyicisi konfigürasyonunun durumunu görüntüler ve fabrika ayarlarının olduğu durumdan bir değişiklik olması halinde, kullanıcıyı uyarır. Bu özelliğin varsayılan ayarı **devre dışı bırak** ayarıdır.

Dinamik Önyükleme Bloğu İşletim Zamanı Taraması (sadece Intel)

Bu seçenek, sadece Intel sistemlerinde mevcuttur. Varsayılan ayarlarında **etkin** durumdayken, HP Sure Start, işletim sistemi çalışıyorken, periyodik olarak BIOS önyükleme bloğunun bütünlüğünü kontrol etmektedir. **Kapalı** olarak ayarlandığında, HP Sure Start, sadece bir önyüklemeden önce ve ya uyku ya da bekleme modundan dönerken bütünlüğü kontrol etmektedir.

HP Sure Start BIOS Ayarları Koruması

Varsayılan ayar olarak, BIOS ayarları koruması ilkesi **kapalı** durumundadır. Özelliği etkin hale getirmek için, istemci cihazın sahibi/yöneticisi, öncelikle tüm BIOS ilkelerini, tercih edilen ayarlara getirmeleri gerekmektedir. Sahibin/yöneticinin ayrıca, HP Sure Start BIOS ayarları korumasını kullanmak için bir BIOS kurulum yönetici şifresi oluşturmaya ihtiyacı vardır.

Bu işlem tamamlandıktan sonra, BIOS ayarları koruma ilkesi "etkin" olarak değiştirilmelidir. Bu noktada, tüm BIOS ayarlarının bir yedek kopyası, HP Sure Start korumalı saklama alanında oluşturulur. İleriye dönük, hiçbir BIOS ayarı yerel olarak ya da uzaktan değiştirilemez. Her bir önyüklemede, BIOS ilke ayarları, istenen durumda olup olmadıkları açısından onaylanır ve herhangi bir uyumsuzluk varsa, BIOS ayarları, HP Sure Start korumalı saklama alanından yeniden yüklenir.

Bir BIOS ayarını değiştirmek için, BIOS yönetici şifresi sağlanmalıdır ve bunun akabinde BIOS ayarları koruması kapatılmalıdır, bu noktada BIOS ayarları üzerinde değişiklikler yapılabilir.

HP Sure Start Güvenli Önyükleme Anahtarları Koruması

Bu seçenek fabrika ayarı olan **etkin** durumda iken, HP Sure Start, önyükleme esnasında başlatılmadan önce, işletim sisteminin önyükleyici programının bütünlüğünü ve gerçekliğini doğrulamak için, BIOS tarafından kullanılan güvenli önyükleme veritabanları ve anahtarlarına geliştirilmiş koruma sunmaktadır. **Kapalı** olarak ayarlandığında, sadece standart UEFI güvenli önyükleme değişkenleri koruması kullanılmaktadır ve HP Sure Start alt sistemi tarafından da bir yedek kopya saklanmamaktadır.

Geliştirilmiş HP Aygıt Yazılımı Program Saldırı Önleme ve Tespiti (sadece Intel) ve HP Aygıt Yazılımı Runtime Intrusion Detection (sadece AMD)

HP fabrikasından gönderilen tüm platformlarda, RTID özelliği için varsayılan ayar **etkin** konumdur. HP Sure Start RTID özelliğinden faydalanmak için son kullanıcı/yöneticinin bu özelliği etkinleştirmesine ya da "dağıtmasına" gerek duyulmamaktadır.

RTID özelliği, platform sahibi/yöneticisi tarafından, seçeneğe bağlı olarak **etkin değil** şekilde ayarlanabilir.

HP Sure Start Güvenlik Olayı Politikası (Security Event Policy)

Bu BIOS ilke ayarı, işletim sistemi çalışıyorken HP Sure Start'ın bir saldırı ya da saldırı girişimi tespit etmesi durumunda hangi eylemin gerçekleştirileceğini yönetir. Bu ilke için olası üç konfigürasyon vardır:

- **Sadece olayı kaydet**: Bu seçenek seçildiğinde, HP ESC tespit olaylarını kaydeder, bu olaylar Microsoft Windows Event Viewer'ın HP Sure Start yolu üzerinde Applications and Services Logs (Uygulama ve Hizmet Kayıtları) içinde incelenebilir.[3]
- **Olayı kaydet ve kullanıcıya bildir**: Bu varsayılan ayardır. Bu seçenek seçildiğinde, HP ESC tespit olaylarını kaydeder, bu olaylar Microsoft Windows Event Viewer'ın HP Sure Start yolu üzerinde Applications and Services Logs (Uygulama ve Hizmet Kayıtları) içinde incelenebilir. Buna ek olarak, kullanıcı Windows içerisinde, olayın gerçekleştiğine dair bilgilendirilir. [4]
- **Olayı kaydet ve sistemi kapat**: Bu seçenek seçildiğinde, HP ESC tespit olaylarını kaydeder, bu olaylar Microsoft Windows Event Viewer'ın HP Sure Start yolu üzerinde Applications and Services Logs (Uygulama ve Hizmet Kayıtları) içinde incelenebilir. Buna ek olarak, kullanıcı Windows içerisinde, olayın gerçekleştiğine dair bilgilendirilir ve sistem kapanmaya doğru yol alır.

HP Sure Start Güvenlik Olayı Önyükleme Bildirimi

Bu BIOS ilke ayarı sistem önyüklemesi esnasında gösterilen HP Sure Start uyarıları ve hata mesajlarının, önyükleme devam etmeden önce yerel kullanıcı tarafından ilgili hatanın onaylanmasını gerektirip gerektirmediğini kontrol eder. Varsayılan ayar olan **Onaylama Gerektir** ayarında, hata mesajı gösterilirken sistem durur. Yerel kullanıcı, önyüklemenin devam etmesi için bir tuşa basmak zorundadır. **15 saniye sonra zaman aşımı** seçeneği seçildiğinde ise, mesaj gösterilir, ancak önyükleme süreci, mesaj ekranda 15 saniye gösterildikten sonra otomatik olarak devam eder.

BIOS Versiyonu Kilitle

(F10) BIOS ayarları içerisinde, bu özellik, Main/Update System BIOS (Ana/BIOS Sistemini Güncelle) içerisinde bulunmaktadır.

Bu ayar, **etkin değil** olarak ayarlandığında, herhangi bir desteklenen süreç kullanılarak BIOS güncellenebilir. HP ESC, sistem belleğinde geçerli bir önyükleme bloğu tespit ettiğinde, önyükleme bloğunun yedek kopyasını günceller.

Bu seçenek **etkin** olarak ayarlandığında, tüm HP BIOS güncelleme cihazları, BIOS'u güncellemeyi reddeder. Buna ek olarak, HP Sure Start yetkilendirilmemiş bir metot yoluyla sistem belleğinin çıkartılarak BIOS versiyonunun değiştirilmesine karşı girişimlerden BIOS'u korumaktadır. HP ESC, BIOS'un kilitlenen versiyonunu kaydeder. HP ESC'in, sistem belleği içerisindeki BIOS'un değiştirildiğini tespit etmesi halinde, HP ESC, önyükleme bloğunun HP ESC kopyası ile BIOS önyükleme bloğunun üstüne yazar. Önyükleme bloğunun HP ESC kopyası, BIOS'un doğru versiyonunun geri kalanını işleme alır ve kurtarır. Bu özelliğin varsayılan ayarı **devre dışı bırak** ayarıdır.

Sistem Sabit Sürücünün MBR ve GPT Kaydedilmesi / Yeniden Kurulması

(F10) BIOS ayarları içerisinde, bu özellik, Güvenlik/Sabit Sürücü Hizmet Programları içerisinde bulunmaktadır. HP Sure Start tarafından tespit edildiği şekilde, birincil sürücünün bölüntü tipine (GPT ya da MBR) bağlı olarak, bu yeteneklerden sadece bir tanesi mevcuttur.

Etkin duruma getirildiğinde, HP Sure Start birincil sürücüden MBR/GPT bölüntü tablosunun korumalı bir yedek kopyasını çıkartarak, yedek kopyayı, her önyüklemede birincil olan ile kıyaslar. Bir farklılık tespit edilmesi halinde, bu kullanıcıya bildirilir ve kullanıcı da yedekleme üzerinden orijinal duruma geçmeyi seçebilir ya da değişiklikler ile birlikte korumalı yedek kopyayı güncelleyebilir. **Önyükleme Kesimi (MBR/GPT) Kurtarma Politikası**, HP Sure Start tarafından bir uyuşmazlık tespit edilmesi halinde, opsiyonel olarak, gerçekleştirilen eyleme dair kullanıcı kararını kaldırmak için de kullanılabilir.

Etkin değil olarak ayarlandığında (varsayılan), HP Sure Start tarafından sağlanan bir MBR/GPT koruması olmaz.

Önyükleme Kesimi (MBR/GPT) Kurtarma Politikası

Yerel Kullanıcı Kontrolü (varsayılan) olarak ayarlandığında, HP Sure Start'ın MBR/GPT bölüntüleme tablosunda bir değişiklik tespit etmesi durumunda, gerçekleştirilecek eylem için kullanıcı bilgilendirilir. **Bozulma durumunda kurtar** olarak ayarlandığında, HP Sure Start, farklılıklar ile karşılaşıldığı durumlarda, MBR/GPT durumunu otomatik olarak kayıtlı haline döndürür.

HP Sure Start ilke kontrollerinin uzaktan yönetimi

Norm dışı olarak, HP Sure Start ilkeleri, olağan kullanıcı için optimize edilmişlerdir. HP Sure Start, varsayılan durumda etkinleştirildiğinden, uzaktan yönetici için HP Sure Start'ı etkinleştirmek (ya da "devreye sokmak") için herhangi bir eylem gerçekleştirmeye gerek yoktur. Uzaktan bir yöneticinin HP Sure Start ilke ayarlarını değiştirmek istemesi halinde, diğer platform BIOS ilkelerini yönetmek için kullanılan aynı Windows Management Instrumentation (Yönetim Cihazları) (WMI) APIs ya da HP BIOS Configuration Utility (Konfigürasyon Uygulamaları) komutları, HP Sure Start ilkelerini yönetmek için de kullanılabilir. Buna ek olarak, yöneticiler HP Sure Start kabiliyetlerini uzaktan yönetebilmek için Microsoft System Center Configuration Manager (SCCM) eklentisi olan Manageability Integration Kit (MIK) da kullanabilirler.

Buna ek olarak, yöneticiler HP Sure Start kabiliyetlerini uzaktan yönetmek ve HP Sure Start olaylarını görüntülemek için Microsoft System Center Configuration Manager (SCCM) eklentisi olan Manageability Integration Kit (MIK) da kullanabilirler.

Sonuç

HP Sure Start, şu temel faydaları sağlamaktadır:

- **Kesintisiz Üretkenlik** – HP Sure Start, bir saldırı ya da kaza sonucu bozulma karşısında, IT/Hizmet gelmesini bekleme süresini ortadan kaldırarak, çalışmanın/işin devam etmesini sağlar.
- **Daha düşük masraflar** – HP Sure Start'ın kurtarma kabiliyeti otomatik olarak IT Yardım Masasına yardım için yapılan aramaları azaltır ve üretkenliği arttırır, bu da nihai olarak platform için bakım masraflarının azaltılmasına katkı sağlar.
- **İç Rahatlığı** – HP Sure Start, geniş bir yazılım ve donanım platformu çeşitliliği üzerinde çalışan birçok güvenlik özelliğine sahiptir.

Seçili HP Elite PC'lerine özel olarak mevcut bulunan HP Sure Start'ın sunduğu, endüstri lideri aygıt yazılımına müdahale tespit ve otomatik tamir olanağıyla, kritik öneme sahip BIOS aygıt yazılımını, zararlı yazılımlardan koruyun.

Ek A – HP Sure Start, Gen by Gen

HP, Sure Start'ı 2014 yılında piyasaya sundu. O zamandan bu zamana, HP, Sure Start'ı geliştirdi ve onu kullanan ürünlerinin sayısını artırdı. Aşağıdaki tabloda, her bir jenerasyon ile gelen yeteneklerin bir özeti sunulmaktadır.

Jenerasyon	Çıkış Tarihi	Eklenen Yetenekler
HP Sure Start	2014	• Kendini onarma özelliği ile birlikte aygıt yazılımı ve BIOS güvenilirliğini sağlama • Aygıt yazılımı görüntüleme ve uyumluluğu
Dinamik Korumalı HP Sure Start	2015	• Windows Event Viewer (Windows Olay İnceleme) desteği • Dinamik Koruma (seçili Intel ürünleri için)
HP Sure Start Gen3 (seçili Intel ürünleri)[5] Runtime Intrusion Detection ile HP Sure Start (seçili AMD ürünleri)[6]	2017	• Runtime Intrusion Detection • BIOS ayarlarını koruma • Manageability Integration Kit (MIK) Microsoft SCCM için Yönetilebilirlik Entegrasyon Kiti eklentisi
HP Sure Start Gen4[7]	2018	• Korumalı saklama alanı – İlgili veri için bütünlüğün korunması, müdahalenin tespiti ve gizliliğin korunması amaçlarıyla, BIOS ayarlarını, kullanıcı yeterlilik bilgilerini ve diğer ayarları HP Endpoint Security Controller donanımı içinde saklamak için güçlü şifreleme metotları • Güvenli önyükleme veritabanı koruması – İşletim sistemi güvenli önyükleme bütünlüğü için kritik öneme sahip ve BIOS tarafından saklanan veritabanları ile anahtarların, standart UEFI BIOS uygulamalarına kıyasla daha geliştirilmiş bir şekilde korunması • Intel platformları üzerinde, Intel Yönetim Motoru Aygıt Yazılımı geliştirilmiş koruma ve kurtarılması • HP Endpoint Security Controller için üçüncü şahıs güvenlik belgelendirilmesi – HP ESC donanımının temel özelliklerinin, kamuya açık beyan edilen kriterler, metodoloji ve süreçler ile uygun olarak çalıştığını onaylamak için bağımsız ve akredite edilmiş bir laboratuvar tarafından test edilmesi [1] • HP Sure Start'a sahip HP iş bilgisayarları NIST Platformu Aygıt Yazılımı Dayanıklılık Taslağı (Özel Basım 800-193) rehberlerini aşmıştır

EK B - System Management Mode genel bakış

System Management Mode (SMM), işletim sisteminin çalışması esnasında, bilgisayar için ileri seviye güç kontrolü özellikleri ve diğer işletim sisteminden bağımsız fonksiyonlar için kullanılan endüstri standardı bir yaklaşımdır. SMM terimi ve uygulamaları x86 mimarisine özel olmakla birlikte, birçok modern bilgisayar mimari yapısı da, benzer bir mimari konsept kullanmaktadır.

SMM, önyükleme zamanında BIOS tarafından yapılandırılır. SMM kodu ana (DRAM) belleğine yerleştirilir ve ardından, BIOS bu bölgeye erişimi engellemek için, mikroişlemci bir SMM bağlamı içerisinde çalışmadığında, yonga seti içerisinde özel (kilitlenebilir) konfigürasyon kayıtları kullanır. Yürütme zamanında, SMM moduna giriş, olaya dayalıdır. Bu yonga seti, bir çok olay ve zaman aşımını tanımaya programlanmıştır. Böyle bir olay olduğunda, yonca döngüsü donanımı, System Management Interrupt (SMI) girdi pinini sürer. Bir sonraki talimat sınırında, mikroişlemci tüm durumunu kaydeder ve SMM girer.

Mikroişlemci, SMM'e girerken, SMI Active (SMIACT) adlı bir donanım çıktı pini sürer. Bu pin, mikroişlemcinin SMM'e girdiği bildirisini yonca döngüsü donanımına iletir. Bir SMI, SMM'in kendi içinden hariç, herhangi bir süreç işletim modunda, ileri sürülebilir. Yonca döngüsü donanımı, SMIACT sinyalini tanır ve takip eden tüm bellek döngülerini, SMM için özel ayrılmış olan bellekteki korumalı bir alana yeniden yönlendirir (bazen, bu alan SMRAM adını alır). SMI girdisini aldıktan ve SMIACT çıktısını öne sürdükten hemen sonra, mikroişlemci, tüm dahili durumunu bu korumalı bellek alanına kaydetmeye başlar.

Mikroişlemci durumu, SMRAM belleğine kaydedildikten sonra, kendisi de SMRAM içinde bulunan SMM idare edici kod (bu alana sistem BIOS önyükleme tarafından yerleştirilir) özel bir SMM işlem modu yürütmeye başlar. Bu mod içinde işlem yapılırken, birçok donanım ve bellek izolasyon mekanizması askıya alınır ve mikro-işlemciler, gerekli işlemleri yapmasını mümkün kılmak için, platform içindeki tüm kaynaklara sanal olarak erişebilirler. SMM kodu, gerekli görevi tamamlar ve ardından mikro-işlemciyi, önceki işletim moduna döndürme zamanı gelir. Bu noktada, SMM kodu, SMM'den çıkmak için Return from System Management Mode (RSM) talimatını yürütür. RSM talimatı, mikroişlemcinin, SMRAM içinde bulunan önceki dahili hal verisini, SMM girişinde yeniden yüklemesini sağlar. RSM'nin tamamlanması üzerine, tüm mikro-işlemci durumu, tam SMI olayı öncesindeki haline döndürülür ve önceki program (işletim sistemi, uygulamalar, misafir sistem arakatmanı vb.) kaldığı yerden yürütmeye devam eder.

[1] HP Sure Start denetleyici donanımı, CSPN sertifikalandırma çerçevesinde belgelendirilmiştir.

[2] Dinamik Koruma özellikli HP Sure Start, 6. Nesil Intel Core ya da daha yüksek işlemcili, HP Elite ürünlerinde mevcuttur.

[3] HP Sure Start olaylarını, Windows Event Viewer içerisinde inceleyebilmek için HP Notification Software donanımının kurulması gerekmektedir.

[4] Bildirim almak için HP Notification Software yazılımının kurulması gerekmektedir.

[5] HP Sure Start Gen3, Intel 7. nesil ya da daha yüksek işlemcili HP Elite ürünlerinde mevcuttur.

[6] Runtime Intrusion Detection özelliği bulunan HP Sure Start, 7. Nesil AMD işlemcisi bulunan HP Elite ürünlerinde mevcuttur.

[7] HP Sure Start Gen4, 8. nesil Intel ya da AMD işlemcili HP Elite ya da HP Pro 600 ürünlerinde mevcuttur.

Daha fazla bilgi için:
hp.com/go/computersecurity

4AA7-3172TRE, Mayıs 2018