مستند المعلومات الفنية

HP Sure Start

حماية وصيانة تلقائيان على مستوى BIOS

ايار 2018

جدول المحتويات

مقدمة

يمكن لتقنية HP Sure Start بشكل تلقائي اكتشاف الهجمات على نظام BIOS أو حدوث تلف به، وإيقاف مثل تلك الهجمات، واسترداد BIOS، وذلك دون تدخل من مسؤولي تكنولوجيا المعلومات وفي غضون فترة توقف قصيرة للغاية أو دون توقف على الإطلاق لإنتاجية المستخدم. في كل مرة يتم فيها تشغيل الكمبيوتر الشخصي، تتحقّق تقنية HP Sure Start تلقائيًا من سلامة رمز BIOS لتساعد في ضمان أنّ الجهاز محمي من الهجمات الخبيثة. وبمجرد دخول الكمبيوتر الشخصي في وضع العمل، تبدأ تقنية كشف الاختراق بمراقبة الذاكرة بصورة مستمرة. وفي حالة حدوث هجوم، يستطيع الكمبيوتر الشخصي إصلاح نفسه خلال أقل من دقيقة باستخدام "النسخة الذهبية"، وهي نسخة معزولة من نظام BIOS.

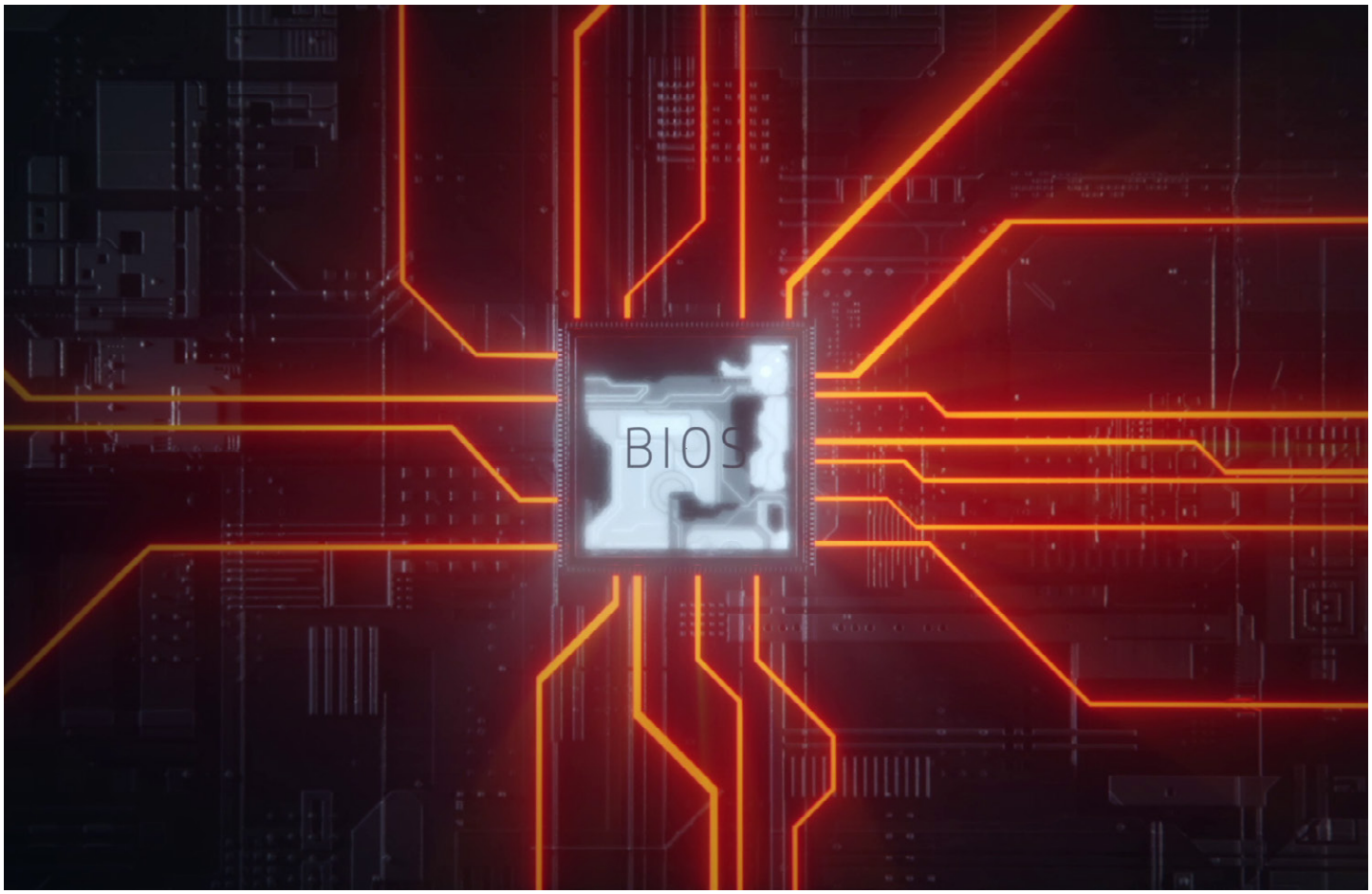
لماذا من المهم حماية BIOS؟

لأن كل شيء في عالمنا أصبح أكثر تواصلاً، تستهدف الهجمات الإلكترونية الأجهزة والبرنامج الثابت في الجهاز العميل بوتيرة متزايدة وتعقيد متصاعد. وكان الاعتقاد السائد سابقًا أنّ الأدوات والتقنيات اللازمة لاستهداف البرنامج الثابت هي فكرة نظرية ومتوفرة فقط على مستوى الحكومات والدول. ولكن هذه الأدوات والتقنيات لم يثبت وجودها فعليًا فحسب، بل تأكد كونها متوفرة بالفعل على نطاق جميع فئات المستخدمين.

تعتبر البرامج الثابتة للجهاز (أو نظام BIOS) هدفًا جذابًا للمهاجمين نظرًا لأن الاختراق الناجح لهذه الأهداف قد يتيح للمهاجم التمتع بميزات محتملة مثل:

- الاستمرارية: تتواجد البرامج الثابتة في ذاكرة مستديمة على لوحة الدوائر الكهربائية ولا يمكن إزالتها ببساطة عن طريق محو بيانات القرص الصلب.
- التحكم: يتم تشغيل البرنامج الثابت بأعلى مستويات الامتيازات - خارج نطاق نظام التشغيل، ممّا يطرح إمكانية الإضرار بالجهاز بشكلٍ مستقل عن نظام التشغيل.
- التخفّي: تشغل البرامج الثابتة منطقة من الذاكرة يتعذر الوصول إليها تمامًا من قبل نظام التشغيل وبرامج النظام؛ ونظرًا لأنه لا يمكن فحصها بواسطة برامج مكافحة الفيروسات، فقد لا يتم اكتشاف إصابتها أبدًا.
- صعوبة الاسترداد: كل هذه الجوانب تجعل من الصعب للغاية التعافي من هذا النوع من العدوى دون اللجوء إلى إجراء صيانة قد يتضمن استبدال لوحة النظام.

الحل المثالي لحماية الأجهزة ضد هذا النوع من الهجوم يعتمد في تصميمه على ترقية الأجهزة باستخدام مبادئ "الجاهزية ضد الهجمات الإلكترونية". تقر هذه المبادئ أنه من الصعب للغاية، إن لم يكن من المستحيل، التنبؤ ومنع كل هجوم محتمل. والحل المثالي هنا لا يتضمن توفير حماية مُحسّنة للبرامج الثابتة فحسب، بل يتضمّن أيضًا توفر قدرات تعتمد على أجهزة يمكنها الكشف عن هجمات نجحت بالفعل والتعافي منها.



توفر تقنية HP Sure Start حماية فائقة للبرامج الثابتة

يعتبر HP Sure Start هو المفهوم الفريد والرائد من HP لتوفير حماية متقدمة للبرامج الثابتة وتحقيق الجاهزية ضد الهجمات التي قد تتعرض لها أجهزة كمبيوتر HP. هذه التقنية تستخدم طريقة فرض التنفيذ على مستوى عمل الأجهزة من خلال وحدة HP Endpoint Security Controller وذلك لتوفير الحماية لنظام BIOS مستخدمةً في ذلك معايير فائقة تتجاوز تلك المعايير القياسية المتعارف عليها في المجال بما يضمن أن نظام التشغيل سوف يبدأ التشغيل باستخدام نظام BIOS الأصلي من HP فقط. بالإضافة إلى ذلك، إذا اكتشفت HP Sure Start العبث بنظام BIOS أو بالبرامج الثابتة أو بالتعليمات البرمجية لنظام BIOS لوضع إدارة النظام (SMM)، فيمكنها استردادها باستخدام نسخة احتياطية محمية.

ملخص مزايا تقنية HP Sure Start

- فرض استخدام البرامج الثابتة الأصلية للنظام الأساسي من HP والحماية ضد العبث بالنظام - قيام وحدة HP Endpoint Security Controller بفرض عملية بدء تشغيل النظام، بما يضمن تحميل البرامج الثابتة الأصلية وغير المُعدلة من HP فقط وكذلك نظام BIOS الأصلي من HP
- مراقبة لمدى سلامة البرامج الثابتة وامتثالها للمعايير – تسجيل الأحداث المتعلقة بسلامة البرامج الثابتة من خلال وحدة HP Endpoint Security Controller منفصلة؛ بما يوفر معلومات عن حالة البرامج الثابتة للنظام مع معلومات حول أي أمور غير عادية قد تشير إلى وجود محاولات هجوم تم التصدي لها
- الإصلاح الذاتي – إصلاح تلقائي لأي تلف قد يحدث لبرامج HP الثابتة ولنظام HP BIOS باستخدام النسخة الاحتياطية المنفصلة من برامج HP الثابتة ونظام HP BIOS وذلك من خلال وحدة HP Endpoint Security Controller
- حماية إعدادات نظام BIOS – توسع من الحماية التي توفرها وحدة HP Endpoint Security Controller للتعليمات البرمجية لنظام BIOS لتشمل أيضًا توفير نسخة احتياطية من HP ESC والتحقق من سلامة جميع إعدادات نظام BIOS للمستخدمين على مستوى مسؤولي النظام والمستخدمين العاديين
- اكتشاف محاولات الاختراق أثناء التشغيل – مراقبة مستمرة للتعليمات البرمجية الحساسة لنظام BIOS في ذاكرة وقت التشغيل (SMM) وذلك أثناء عمل نظام التشغيل
- حماية مفاتيح بدء التشغيل الآمن – حماية معززة بشكل كبير لقواعد البيانات والمفاتيح المخزنة بواسطة نظام الإدخال والإخراج الأساسي (BIOS) والتي تعتبر ضرورية لسلامة ميزة بدء التشغيل الآمن لنظام التشغيل بما يتوافق مع معايير تنفيذ UEFI BIOS القياسية
- وسائط تخزين محمية – تستخدم HP Sure Start أساليب تشفير قوية لتخزين إعدادات BIOS وبيانات اعتماد المستخدمين والإعدادات الأخرى في وحدة HP Endpoint Security Controller لتوفير الحماية والسلامة إلى جانب الكشف عن التلاعب والحفاظ على سرية تلك البيانات
- حماية برامج Intel® Management Engine الثابتة – حماية مُحسنة واسترداد برامج Intel Management Engine الثابتة
- سهولة الإدارة – يمكن للمسؤولين إدارة إمكانات HP Sure Start مع المكون الإضافي Manageability Integration Kit (MIK) لبرامج Microsoft® System Center Configuration Manager (SCCM)

للاطلاع على ملخص القدرات المضافة في كل جيل من HP Sure Start، راجع الملحق أ في الصفحة 11.

شهادة أمان الجهات الخارجية

خضعت أجهزة HP Endpoint Security Controller التي يتم استخدامها في تقنية HP Sure Start إلى تقييم أمان الجهات الخارجية والذي بموجبه تم اعتماد تلك الأجهزة بحيث يمكنها فرض استخدام وتشغيل البرامج الثابتة المعتمدة والمصرح بها فقط على الكمبيوتر المستهدف.[1]

ويعتبر الجزء الأهم في أي قرار شراء متعلق بمنتجات الأمان هو ضمان عمل حل الأمان وفقًا لما تم تحديده من قِبل جهة إنتاجه. ونظرًا لأن HP تتمتع بسمعة منقطعة النظير فيما يخص الجودة، فقد وافقت HP على الكشف عن المكونات الداخلية لأجهزة HP Endpoint Security Controller وأخضعتها للمراجعة والاختبار من قِبل مختبر مستقل ومعتمد للتحقق من أنها تعمل كما هو مُعلن ووفقًا للمعايير والمنهجيات والعمليات المتعارف عليها للجميع.

تصميم يُراعي مرونة الأمان الإلكتروني

لا توفر HP Sure Start حماية متقدمة لنظام الإدخال والإخراج الأساسي (BIOS) فحسب، بل تتجاوز فيما تقدمه المعايير القياسية المتعارف عليها في تلك الصناعة، وذلك لأنها مصممة انطلاقًا من مبدأ تأمين الأنظمة من خلال حماية الأجهزة وما يتصل بها، وهو ما يوفر جاهزية لا مثيل لها للنظام ضد أي هجمات إلكترونية ولضمان القدرة على استرداد نظام BIOS حتى في حالة وقوع اختراق أو هجوم مُدمر. يتخطّى ما تُقدّمه أجهزة كومبيوتر HP المُخصّصة للأعمال والمزوّدة بتقنية HP Sure Start توجيهات جاهزية البرامج الثابتة للأنظمة الأساسية والمحددة في مسودة المعهد الوطني للمعايير التقنية والمعروفة اختصارًا باسم (NIST)، (منشور خاص 800-193)، وهي إحدى الجهود الرائدة للقطاع العام في إضفاء الطابع الرسمي على متطلبات الأنظمة التي تتمتع بالجاهزية لصد الهجمات الإلكترونية.

HP Sure Start- الطرز المدعومة

قدّمت HP تقنية Sure Start في عام 2014. ومنذ ذلك الوقت، قامت HP بتحسين تقنية Sure Start وتوسيع عدد المنتجات التي تتضمن تلك التقنية. توفرت HP Sure Start عبر مجموعة منتجات Elite لعام 2018 بالكامل، بما في ذلك الأجهزة اللوحية والمحمولة وأجهزة الكمبيوتر المكتبية والأجهزة المتكاملة متعددة الوظائف (AIOs). الجيل الرابع من تقنية HP Sure Start متوفر في أجهزة HP Elite وHP Pro 600 المجهّزة بالجيل الثامن من معالجات Intel أو AMD®.

نظرة عامة على البنية والإمكانات

تتكوّن تقنية HP Sure Start من مُكوّنيْن رئيسيّيْن:

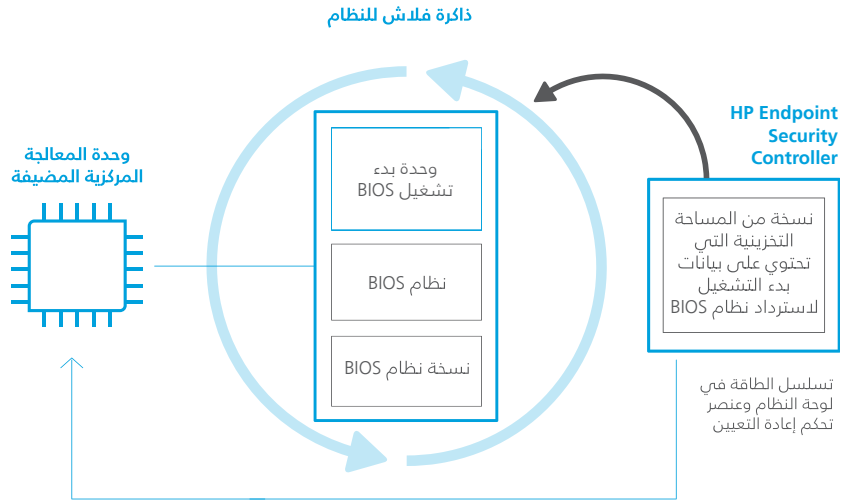
- **HP Endpoint Security Controller** التي تقوم بتشغيل البرامج الثابتة لتقنية HP Sure Start
- **HP Sure Start BIOS** يعمل بالتزامن مع البرامج الثابتة وأجهزة HP Endpoint Security Controller

التحقق من سلامة البرنامج الثابت - الوظيفة الأساسية في HP Sure Start

HP Endpoint Security Controller (HP ESC) هو أول جهاز في النظام يقوم بتشغيل البرنامج الثابت عند تشغيل النظام، ليكون نشطًا قبل بدء تشغيل النظام. وتتضمّن أنشطة HP ESC، على سبيل المثال لا الحصر، مراقبة زر تشغيل النظام وإجراء تسلسل الطاقة لبدء تشغيل وحدة المعالجة المركزية المضيفة عند ضغط المستخدم على زر تشغيل الطاقة.

عندما تسري الطاقة في النظام الأساسي أولاً (قبل تشغيل النظام) يتحقّق HP ESC من أنّ برنامجه الثابت الخاص هو برنامج تعليمات HP البرمجية الأصلية وذلك قبل تحميل التعليمات البرمجية وتنفيذها. تستخدم أجهزة HP ESC أساليب تشفير قوية قياسية للتحقق من السلامة. ويستخدم أسلوب التشفير مفتاح RSA عام من نوع 2048 بت من HP وهو مُضمن في الذاكرة الداخلية الدائمة للقراءة فقط. وبالتالي، فإنّ HP ESC هو جذر الثقة Root of Trust (RoT) القائم على الأجهزة والمُضمن للنظام الأساسي، والمستخدم في التحقق من البرنامج الثابت للنظام والتحقق من HP BIOS قبل تشغيلهما. يوفر Root of Trust للأجهزة الحماية من الهجمات التي تستهدف استبدال البرامج الثابتة بغض النظر عن طريقة انتشارها ويعمل كأساس يُبنى عليه أمان النظام الأساسي من HP.

الشكل 1. عملية التحقق من سلامة البرامج الثابتة.



يُوضّح الشكل 1 عملية التحقق من سلامة البرامج الثابتة. بمجرد قيام HP ESC بالمصادقة وبدء تشغيل البرنامج الثابت لتقنية HP Sure Start، يقوم ذلك البرنامج الثابت باستخدام نفس عمليات التشفير القوية للتحقق من سلامة وحدة بدء تشغيل BIOS في ذاكرة فلاش للنظام. في حال تم العثور على بت واحد غير صحيح، يستبدل HP ESC محتويات ذاكرة فلاش للنظام بنسخته الخاصة من وحدة بدء تشغيل BIOS المخزّنة ضمن ذاكرة معزولة مستديمة (NVM) والمُخصّصة لجهاز HP ESC.

يضمن تصميم HP Sure Start أنّ جميع التعليمات البرمجية للبرنامج الثابت وBIOS التي يتم تشغيلها في كل من HP ESC ووحدة المعالجة المركزية المضيفة هي ذات التعليمات البرمجية المُخصّصة من HP لتعمل على الجهاز.

ملاحظة: تجري عملية التحقق من سلامة وحدة بدء التشغيل ذاكرة فلاش للنظام، وأي عمليات استرداد ضرورية يتم تنفيذها من قِبل *HP ESC*، أثناء توقف المعالج المضيف. لذلك، ومن وجهة نظر المستخدم، تجري العملية بأكملها عندما يكون النظام متوقفًا، في وضع السكون، أو وضع الإسبات.

تُشكّل وحدة بدء تشغيل BIOS في ذاكرة فلاش للنظام، الأساس لنظام HP BIOS. تضمن أجهزة HP ESC أنّ وحدة بدء تشغيل BIOS هي التعليمات البرمجية الأولى التي يقوم المعالج بتشغيلها بعد إعادة الضبط. بمجرد تأكد HP ESC من أنّ وحدة بدء تشغيل BIOS تتضمّن التعليمات البرمجية من HP الموثوق بها، يسمح بعدها ببدء تشغيل النظام بشكلٍ طبيعي.

يتحقّق HP ESC أيضًا من سلامة التعليمات البرمجية لوحدة بدء التشغيل في ذاكرة فلاش للنظام في كل مرة يتم فيها إيقاف تشغيل النظام أو وضعه في وضع الإسبات أو السكون. وبما أنّه يتم إيقاف تشغيل وحدة المعالجة المركزية في كل من هذه الحالات، وحيث إنّ وحدة المعالجة المركزية مطلوبة لإعادة تنفيذ التعليمات البرمجية لوحدة بدء تشغيل BIOS لاستئناف التشغيل، فمن الأمور بالغة الأهمية إعادة التحقق من سلامة وحدة بدء تشغيل BIOS في كل مرة وذلك للتحقق من حدوث حالات تلاعب.

بالإضافة إلى ذلك، وفيما يتعلّق بطرز أجهزة HP المزوّدة بمعالجات Intel، تقوم HP Sure Start بشكلٍ دوري (كل 15 دقيقة) بفحص سلامة وحدة بدء تشغيل BIOS في ذاكرة فلاش للنظام أثناء عمل النظام.[2]

سلامة البيانات الفريدة في الجهاز

يعمل HP ESC وBIOS سويًا لتوفير حماية فريدة متقدمة للمتغيرات الهامة التي يتم تهيئتها أثناء التصنيع لكل جهاز والتي يجب أن تظل متسقة في عملها على مدار عمر أي نظام أساسي مُحدد. وفي المصنع، يتم حفظ نسخة احتياطية من هذه البيانات المتغيرة في الذاكرة المستديمة لوحدة HP ESC. يتم توفير النسخة الاحتياطية لمكون HP Sure Start BIOS على أساس للقراءة فقط للتحقق من سلامة البيانات الموجودة في كل عملية بدء تشغيل. إذا تغير أي إعداد في ذاكرة فلاش المشتركة مقارنة بإعدادات المصنع، ستقوم مكونات HP Sure Start BIOS باستعادة البيانات تلقائيًا في ذاكرة فلاش للنظام من النسخة الاحتياطية التي توفرها HP ESC.

منطقة أداة التوصيف

بالنسبة لطرز أجهزة HP المزوّدة بمعالجات Intel، تقوم HP Sure Start بحماية منطقة توصيف ذاكرة فلاش للنظام. وبشكلٍ مُخصّص لبنية Intel، تحتوي منطقة التوصيف على معاملات تكوين بالغة الأهمية يتم اختبارها من خلال منطق ™Intel Core عند إعادة الضبط ويتم استخدامها بعد ذلك لتكوين منطق Core. تتضمّن منطقة التوصيف كذلك معلومات التقسيم لذاكرة فلاش للنظام المُستخدَمة من قِبل منطق Intel Core لتحديد مكان تواجد منطقة BIOS داخل ذاكرة فلاش وبالتالي المكان الذي تقوم وحدة المعالجة المركزية باسترداد التعليمات البرمجية منه لتشغيلها عند إعادة الضبط. تراقب HP Sure Start سلامة هذه المنطقة وتقوم باستردادها إلى حالة التكوين المطلوبة في حالة حدوث تلاعب أو عطل.

حماية وحدة تحكم الشبكة

بالإضافة إلى ذلك، وبالنسبة لطرز أجهزة HP المزوّدة بمعالجات Intel، تقوم HP Sure Start بحماية إعدادات وحدة تحكم الشبكة (NIC) الموجودة في ذاكرة فلاش للنظام. هناك بعض عملاء HP لديهم حالات استخدام تتطلب تغييرات قانونية في إعدادات المصنع لوحدة تحكم الشبكة NIC. وبالتالي، لا تمنع HP Sure Start بصورة افتراضية إجراء تغييرات على إعدادات NIC. عوضًا عن ذلك، توفر HP Sure Start ميزة تقوم، عند تفعيلها، بتحذير المستخدم عند تغيير إعدادات NIC. بالإضافة إلى ذلك، توفر HP Sure Start طريقةً لاسترجاع إعدادات NIC إلى القيم الافتراضية للمصنع. تتضمّن الإعدادات المحمية عنوان MAC، وإعدادات بيئة تنفيذ ما قبل بدء التشغيل (PXE)، وتحميل البرنامج المبدئي البعيد (RPL). عملية الاسترجاع ممكنة عبر نسخة احتياطية متوفرة للقراءة فقط ومحمية بواسطة HP ESC.

حماية إعدادات BIOS

كما هو مُبيّن مسبقًا، تتحقّق HP Sure Start من سلامة وموثوقية التعليمات البرمجية لنظام HP BIOS. وبما أنّ هذه التعليمات البرمجية تبقى ثابتة بعد أن تقوم HP بإنشائها، يمكن استخدام التوقيعات الرقمية لتأكيد كلا السمتيْن الخاصّتيْن بالتعليمات البرمجية. ومع ذلك، يعمل الطابع الديناميكي والطابع القابل للتكوين من قِبل المستخدم لإعدادات BIOS على خلق تحديات إضافية عند حماية هذه الإعدادات. لا يمكن إنشاء التوقيعات الرقمية من قِبل HP ولا يمكن استخدامها في أجهزة ESC التي تستخدم تقنية HP Sure Start للتحقق من هذه الإعدادات.

توفر حماية إعداد BIOS في HP Sure Start القدرة على تكوين النظام بحيث يتم استخدام أجهزة HP ESC في النسخ الاحتياطي وفحص السلامة لجميع إعدادات BIOS التي يفضلها المستخدم.

عند تفعيل هذه الميزة في النظام الأساسي، يتم نسخ جميع إعدادات السياسات التي يستخدمها BIOS احتياطيًا بعد ذلك وتنفيذ فحص السلامة في كل عملية بدء تشغيل وذلك لضمان عدم تعديل أي إعدادات لسياسات BIOS. في حالة الكشف عن تغيير، يستخدم النظام النسخة الاحتياطية من وحدة تخزين HP Sure Start المحمية للعودة تلقائيًا إلى إعدادات المستخدم.

تقوم ميزة حماية إعداد BIOS في HP Sure Start بإنشاء أحداث للأجهزة التي تستخدم HP Sure Start عند كشف محاولة لتعديل إعدادات BIOS. يتم تسجيل الحدث في سجل مراقبة HP Sure Start ليستقبل المستخدم المحلي إشعارًا من BIOS أثناء التشغيل.

وحدة التخزين المحمية لتقنية HP Sure Start

توفر وحدة التخزين المحمية بعمق في أجهزة HP Endpoint Security Controller أعلى مستويات الحماية لبيانات BIOS والبرامج الثابتة والإعدادات المحمية من قِبل HP Sure Start. وحدة التخزين المحمية بواسطة HP Sure Start مُصمَّمة لتوفير السرية، والسلامة، وكشف التلاعب حتى في حالات الهجوم المادي عندما يقوم المهاجم بتفكيك النظام وتأسيس اتصال مباشر بجهاز التخزين المستديم على لوحة الدوائر.

سلامة البيانات

تعتبر سلامة البيانات الديناميكية المخزنة في الذاكرة المستديمة من قبل البرامج الثابتة والتي تُستخدم للتحكم في حالة القدرات المتنوعة أمرًا هامًا بالنسبة لوضع الأمان للنظام الأساسي ككل. تتضمّن البيانات الديناميكية جميع إعدادات BIOS التي يمكن تعديلها من قِبل المستخدم النهائي أو المسؤول عن الجهاز. تتضمّن الأمثلة (على سبيل المثال لا الحصر) خيارات بدء التشغيل مثل ميزة بدء التشغيل الآمن، وكلمة مرور مسؤول BIOS والسياسات ذات الصلة، والتحكم في حالة وحدة Trusted Platform Module، وإعدادات سياسة HP Sure Start.

أي هجوم ينجح في تجاوز قيود الوصول الحالية لمنع التعديلات غير المصرح بها لهذه الإعدادات يمكنه أن يهزم أمان النظام الأساسي. كمثال، ضع في اعتبارك سيناريو يقوم فيه أحد المهاجمين بإجراء تعديل غير مصرّح به على حالة بدء التشغيل الآمن لتعطيله وذلك دون الكشف عن هذا الهجوم. في هذا السيناريو، سيقوم النظام الأساسي ببدء تشغيل برنامج الاختراق "روتكيت" للمهاجم قبل بدء تشغيل نظام التشغيل، دون معرفة المستخدم.

تقوم الواجهة القياسية Unified Extensible Firmware Interface (UEFI) بتطبيق قيود الوصول التي تمنع التعديلات غير المصرح بها على هذه المتغيرات، وتنفذ HP هذه البرامج مثلها مثل باقي أجهزة الكمبيوتر الشخصية.

ومع ذلك، وفي ضوء المخاطر التي يشكلها خرق هذه الآليات على النظام الأساسي، توفر HP Sure Start دفاعات ثانوية أقوى من معايير الصناعة القياسية المعمول بها في هذا المجال.

يتم تخزين إعدادات BIOS والبيانات الديناميكية الأخرى المستخدمة من قبل البرامج الثابتة للتحكم في الحالة المحمية بواسطة HP Sure Start في الذاكرة المستديمة المنفصلة لوحدة التحكم HP Endpoint Security Controller والتي لا يمكن الوصول إليها مباشرة من قِبل البرامج التي تعمل على وحدة المعالجة المركزية المضيفة.

بالإضافة إلى ذلك، يقوم HP ESC بإنشاء وإلحاق قياسات سلامة فريدة في كل مرة يتم فيها تخزين عنصر بيانات في مخزن الذاكرة المستديمة هذا. تستند قياسات السلامة إلى خوارزمية تشفير قوية (رمز مصادقة رسالة مجزأة يستخدم تجزئة SHA-256) لها جذر محدد لشفرة سرية داخل HP ESC. ويتفرد كل HP ESC بشفرة سرية خاصة، على سبيل المثال قيام كل وحدة تحكم بإنشاء قياس سلامة فريد في حال العناصر المتطابقة.

عندما تتم قراءة عنصر البيانات مرة أخرى من الذاكرة المستديمة، يعيد HP ESC حساب قياس السلامة لعنصر البيانات هذا ويقارنه بقياس السلامة الذي تم إلحاقه بالبيانات. أي تغييرات غير مصرح بها على البيانات في مخزن الذاكرة المستديمة يؤدي إلى عدم التطابق. باستخدام هذا الأسلوب، يمكن لوحدة HP ESC الكشف عن التلاعب بعناصر البيانات المخزنة في مخزن الذاكرة المستديمة.

سرية البيانات

بالنسبة للعديد من عناصر البيانات التي يخزنها النظام الأساسي، يعد الحفاظ على السرية أمرًا بالغ الأهمية. الأمثلة على ذلك تتضمن، تجزئة كلمة مرور مسؤول نظام الإدخال/الإخراج الأساسي (BIOS)، وبيانات اعتماد المستخدم، والشفرات السرية المخزنة اختياريًا بواسطة البرامج الثابتة نيابةً عن المستخدم للميزات القائمة على البرامج الثابتة مثل HP Sure Run وHP Sure Recovery.

تعد حماية هذه الأسرار أمرًا صعبًا باستخدام أساليب UEFI BIOS القياسية المعمول بها في المجال، نظرًا لأن التخزين المستديم يمكن قراءته عادةً بواسطة برامج تعمل على المعالج المضيف. الهدف من التخزين المحمي من HP Sure Start هو توفير حماية أكبر لهذه البيانات السرية من تلك التي يوفرها تنفيذ معيار UEFI BIOS.

بالإضافة إلى التخزين المنفصل المعزول، يتمثل نهج HP Sure Start في أن هذه التقنية تقوم بالاستفادة من كتلة أجهزة Advanced Encryption Standard (AES) الموجودة داخل HP ESC لتنفيذ تشفير AES-256 على جميع عناصر البيانات السرية المخزنة في ذاكرة HP Sure Start المستديمة، بالإضافة إلى قياسات سلامة البيانات لتلك العناصر. مفتاح التشفير المستخدم يكون فريدًا لكل جهاز HP ESC ولا يترك وحدة التحكم هذه أبدًا، لذا فالبيانات التي يتم تشفيرها بواسطة أي مكون HP ESC فردي لا يمكن فك تشفيرها إلا بواسطة مكون HP ESC هذا فقط.

حماية مفاتيح بدء التشغيل الآمن

توفر تقنية HP Sure Start حماية معززة لقواعد بيانات مفاتيح بدء التشغيل الآمن لواجهة UEFI والمخزنة بواسطة البرنامج الثابت مقارنةً بتنفيذ بدء التشغيل الآمن المحدد لواجهة UEFI والمتوافق مع معايير الصناعة. تعتبر هذه المتغيرات حاسمة في التشغيل السليم لميزة بدء التشغيل الآمن لواجهة UEFI والتي تتحقق من سلامة ومصداقية برنامج تحميل نظام التشغيل قبل السماح له بالبدء في التشغيل.

تحافظ HP Sure Start على قواعد بيانات مفاتيح بدء التشغيل الآمن لواجهة UEFI من خلال الحفاظ على نسخة رئيسية في وحدة التخزين المحمية من HP Sure Start. تراقب تقنية HP Sure Start أي تعديلات مرخصة تتم على قواعد بيانات مفاتيح بدء التشغيل الآمن لواجهة UEFI القياسية خلال وقت التشغيل من قِبل نظام التشغيل ويتم تطبيقها على النسخة الرئيسية من خلال HP ESC. تستخدم HP Sure Start بعد ذلك النسخة الرئيسية المحفوظة في وحدة التخزين المحمية بواسطة HP Sure Start لتحديد ورفض أي تغييرات غير مصرح بها على قواعد بيانات مفاتيح بدء التشغيل الآمن لواجهة UEFI القياسية.

يتم تفعيل هذه الإمكانية افتراضيًا، لتشمل قواعد البيانات التالية:

- قواعد بيانات التوقيع (db)
- قواعد بيانات التوقيعات التي تم إبطالها (dbx)
- مفتاح تسجيل المفاتيح (KEK)
- مفتاح النظام الأساسي (PEK) المحدث ديناميكيًا خلال وقت تشغيل بواسطة نظام التشغيل

كشف محاولات الاختراق أثناء التشغيل (RTID)

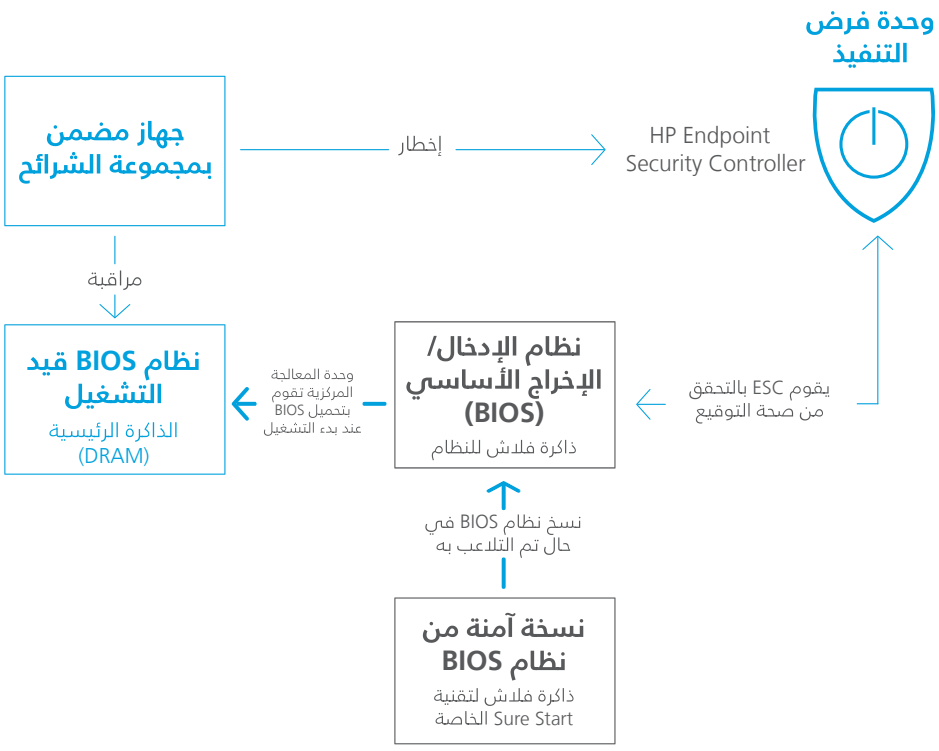
في كل عملية بدء تشغيل، تبدأ التعليمات البرمجية لنظام BIOS بالعمل من خلال ذاكرة فلاش بعنوان ثابت. ويُعرف ذلك باسم التعليمات البرمجية لبدء تشغيل BIOS، حيث توفر إمكانات "ما قبل عمل نظام التشغيل" الضرورية للمرحلة التي تسبق بدء نظام التشغيل. ولكن، هناك جزء ضروري من BIOS يبقى في ذاكرة DRAM ليوفر مزايا إدارة الطاقة المتقدمة، وخدمات نظام التشغيل، ومزايا نظام التشغيل المستقلة الأخرى أثناء عمل نظام التشغيل. هذه التعليمات البرمجية لنظام BIOS، والتي تُعرف بالتعليمات البرمجية لوضع System Management Mode أو (SMM)، توجد داخل مساحة خاصة داخل ذاكرة DRAM المخفية عن نظام التشغيل. كما نُشير إلى هذه التعليمات البرمجية كذلك باسم تعليمات BIOS في "وقت تشغيل" في سياق ميزة كشف محاولات الاختراق أثناء التشغيل الخاصة بتقنية HP Sure Start. (لمزيدٍ من التفاصيل عن SMM وكيفية عملها، يرجى الاطلاع على الملحق ب في الصفحة 12).

تعتبر سلامة التعليمات البرمجية لوضع SMM أمرًا حيويًا بالنسبة لوضع أمان الجهاز العميل. تتحقّق HP Sure Start من سلامة التعليمات البرمجية لنظام HP SMM BIOS عند بدء نظام التشغيل. توفر لك تقنية الكشف عن الاختراق أثناء وقت التشغيل (Runtime Intrusion Detection) آليات لضمان بقاء التعليمات البرمجية لنظام SMM BIOS كما هي أثناء تشغيل نظام التشغيل وذلك عن طريق إضافة إمكانات حماية جديدة و/أو توفير وسائل للكشف عن أي هجوم على هذه التعليمات البرمجية.

بنية ميزة الكشف عن الاختراق أثناء وقت التشغيل

تستخدم ميزة RTID أجهزة متخصصة في مجموعة شرائح النظام الأساسي للتعرف على الأمور غير الطبيعية التي قد تحدث في نظام HP SMM BIOS أثناء وقت التشغيل. يؤدي اكتشاف أي حالات غير طبيعية إلى إرسال إشعار إلى وحدة HP Endpoint Security Controller، والتي يمكنها التصرف وتنفيذ إجراء السياسة المكوّن بشكل مستقل عن وحدة المعالجة المركزية.

الشكل 2. تستخدم ميزة كشف الاختراق أثناء وقت التشغيل (RTID) أجهزة متخصصة مضمنة داخل مجموعة الشرائح لمراقبة التعليمات البرمجية لوضع SMM للتعرف على أية تغييرات قد تحدث لها.



إشعارات المستخدم وتسجيل الأحداث وإدارة الخصوصية

إشعارات المستخدم النهائي لتقنية HP Sure Start

في ظروف التشغيل العادية، تكون HP Sure Start غير مرئية للمستخدم. تتم عمليات الاسترداد تلقائيًا باستخدام الإعدادات الافتراضية، دون الحاجة إلى تدخل أي مستخدم نهائي أو مسؤول تكنولوجيا المعلومات وهو الأمر المطلوب عادة لاسترداد البيانات عندما تكتشف HP Sure Start وجود مشكلة.

قد يرى المستخدمون إشعارات في وقت التشغيل في حالة اكتشاف مشكلة تتعلق بسلامة نظام BIOS وذلك عبر الحماية الديناميكية من HP Sure Start. أو ميزة كشف الاختراق أثناء وقت التشغيل (RTID) أثناء عمل نظام التشغيل. عند الكشف عن أي حدث كبير أو اتخاذ إجراء، تعرض HP Sure Start رسالة تحذير باستخدام إشعارات Windows® في بدء التشغيل التالي. يتطلب تمكين عرض إشعارات Windows وجود برنامج HP Notifications.

تسجيل الأحداث في تقنية HP Sure Start

تقوم HP Endpoint Security Controller بتسجيل الأحداث الحيوية المتعلقة بالتعليمات البرمجية للبرنامج الثابت/BIOS والبيانات التي تراقبها HP Sure Start. يتم تخزين هذه الأحداث ضمن الذاكرة المستديمة لتقنية Sure Start. يتم نسخ سجلات هذه الأحداث من HP ESC إلى عارض أحداث Windows عند تثبيت برنامج HP Notifications ليوفر الوصول إلى هذه الأحداث من قِبل المستخدم المحلي وكذلك لوكيل الإدارة المفضل لدى العميل.

تقوم الأحداث التالية بتشغيل برنامج HP Notifications لجمع كل الأحداث من النظام الفرعي لتقنية HP Sure Start وضمان تحديث عارض أحداث Windows بأي أحداث ليست مسجلة لديه مسبقًا:

- بدء تشغيل Windows
- استئناف عمل Windows من وضع السكون/الإسبات
- HP Sure Start مع إشعارات أحداث وقت التشغيل للحماية الديناميكية
- كشف الاختراق أثناء وقت التشغيل (RTID) في تقنية HP Sure Start

يقوم برنامج HP Notifications بملء أحداث HP Sure Start في سجل فريد لأحداث تطبيق "HP Sure Start". سيحتوي هذا السجل على أحداث HP Sure Start فقط. ويكون مسار وصول عارض أحداث Windows إلى أحداث HP Sure Start كالتالي: أدوات النظام/عارض الأحداث/سجلات التطبيقات والخدمات/HP Sure Start.

فئات مستوى عارض أحداث Windows ذات الصلة بأحداث HP Sure Start محددة في الجدول أدناه.

يتم نشر الأحداث في عارض أحداث Windows وفق ترتيب إنشاء HP Sure Start لها. يُضاف الحدث الأقدم في النظام الفرعي لتقنية HP Sure Start أولاً إلى عارض أحداث Windows وتُضاف الأحداث الأحدث كسجلات أخيرة.

ويكون الطابع الزمني لكل إدخال في عارض أحداث Windows هو وقت إضافته إلى السجل، وليس زمن وقوع الحدث. يتضمّن كل إدخال خاص بتقنية Sure Start في عارض أحداث Windows بياناتٍ تفصيلية ضمن تفاصيل الحدث، والتي تتضمّن الطابع الزمني لوقت الحدوث الفعلي.

ملاحظة: يستمر وجود الأحداث في *HP Endpoint Security Controller* حتى بعد نسخها إلى عارض أحداث *Windows*. إذا تم مسح سجلات عارض أحداث *Windows*، يقوم برنامج *HP Notifications* باستبدال إدخالات *HP Sure Start* عند الحدث التالي الذي يقوم بتشغيله لفحص سجل أحداث *HP Sure Start*.

أنواع الأحداث المتعلقة بتقنية HP Sure Start في عارض أحداث Windows

مستوى الحدث	التعريف
معلومات	الأحداث المتوقعة خلال مسار التشغيل الطبيعي (مثل تحديث BIOS).
تحذير	الأحداث غير المتوقعة التي وقعت ولكن تم الإصلاح بعدها بالكامل من قبل HP Sure Start ولا يوجد أي إجراء مطلوب من قِبل المستخدم/المسؤول لتشغيل النظام الأساسي بشكل كامل. هذه الأحداث هي عمليات شاذة قد تتطلب أن يتحقق منها المستخدم/المسؤول بشكلٍ أكبر، وخاصة إذا كان هناك شيوع لهذه الأحداث على عدّة أجهزة.
خطأ	الأحداث التي تتطلب تدخُّل المسؤول/خدمة HP ليتم استرداد النظام الأساسي بالكامل.

عناصر تحكم سياسة HP Sure Start

وكإجراء غير تقليدي مبتكر، يقوم نظام BIOS من HP بتمكين وتحسين سياسات HP Sure Start للمستخدم العادي. وبما أنّ تقنية HP Sure Start مُفعّلة افتراضيًا، فليس هناك حاجة إلى قيام المستخدم العادي بتعديل الإعدادات بحيث تقوم HP Sure Start بحمايتها. وفيما يتعلّق بالمستخدمين المتقدمين، يوفر نظام BIOS بعض عناصر التحكم بسلوك HP Sure Start، باستخدام إعدادات السياسة في إعدادات BIOS (بالضغط على F10). وما لم يُذكر خِلاف ذلك، يمكن التعرف على هذه الإعدادات والمزايا في قسم الأمان/BIOS Sure Start.

ملاحظة: يتم تخزين السياسات ضمن ذاكرة *HP ESC* المستديمة والتي لا يمكن الوصول إليها مباشرةً عبر المعالج المضيف؛ ولذلك، يجب إعادة بدء التشغيل قبل تطبيق أي من إعدادات *Sure Start*.

تتوفر إعدادات ووظائف HP Sure Start التالية:

- التحقق من وحدة بدء التشغيل عند كل عملية بدء تشغيل
- سياسة استرداد بيانات BIOS
- استرداد تكوين وحدة تحكم الشبكة (في أجهزة معالجات Intel فقط)
- المطالبة باتخاذ إجراء عند تغيير تكوين وحدة تحكم الشبكة (في أجهزة معالجات Intel فقط)
- مسح ديناميكي أثناء التشغيل لوحدة بدء التشغيل (في أجهزة معالجات Intel فقط)
- حماية إعدادات HP Sure Start BIOS
- حماية HP Sure Start لمفاتيح بدء التشغيل الآمن
- الكشف والحماية المتقدمة لبرنامج HP الثابت ضد الاختراقات أثناء التشغيل (في أجهزة معالجات Intel فقط)
- كشف وحماية برنامج HP الثابت ضد الاختراقات أثناء التشغيل (في أجهزة معالجات AMD فقط)
- سياسة أحداث أمان HP Sure Start
- إشعارات بدء تشغيل لأحداث أمان HP Sure Start
- إغلاق إصدار BIOS
- حفظ/استرجاع سجل MBR من القرص الثابت للنظام
- حفظ/استرجاع سجل GPT من القرص الثابت للنظام
- سياسة استرداد قطاع بدء التشغيل (MBR/GPT)

التحقق من وحدة بدء التشغيل عند كل عملية بدء تشغيل

تتحقّق HP Sure Start بصورة دائمة من سلامة وحدة بدء تشغيل BIOS في ذاكرة فلاش للنظام قبل التنشيط من وضع السكون، أو الإسبات، أو إيقاف التشغيل. عند التعيين على **تمكين**، تقوم HP Sure Start كذلك بالتحقق من سلامة وحدة بدء التشغيل عند كل عملية تشغيل (إعادة تشغيل Windows). وتكون المفاضلة بين الحصول على بدء تشغيل أسرع مقابل مزيدٍ من الأمان. ويكون الإعداد الافتراضي لهذه الميزة **تعطيل**.

سياسية استرداد بيانات BIOS

عند تعيين الإعداد على **تلقائي**، تقوم HP Sure Start بإصلاح BIOS أو البيانات الفريدة للجهاز بصورة تلقائية عندما يكون ذلك ضروريًا. عند تعيين الإعداد على **يدوي**، تقوم HP Sure Start بطلب تسلسل مفتاحي محدد لإجراء عملية الإصلاح. في حالة وجود مشكلة في التعليمات البرمجية لوحدة بدء التشغيل، لن يقوم النظام ببدء التشغيل، وسيُومض ضوء LED في النظام بتسلسل فريد. في حالة وجود مشكلة في بيانات الجهاز الفريدة، سيعرض النظام رسالة على الشاشة. يتنوّع التسلسل المفتاحي المطلوب، والتسلسل الوميضي المعروض، حسب ما إذا كان النظام هو كمبيوتر محمول، أو كومبيوتر مكتبي، أو كومبيوتر لوحي. الوضع اليدوي مفيد في حالة المستخدمين الذين يستطيعون القيام بإجراءات استكشافية على محتويات ذاكرة فلاش للنظام قبل الإصلاح. لا يُنصح بقيام المستخدمين العاديين باستخدام الوضع اليدوي. ويكون الإعداد الافتراضي لهذه الميزة **تلقائي**.

استرداد تكوين وحدة تحكم الشبكة (الأجهزة ذات معالجات Intel فقط)

وحدة التحكم هذه متوفرة في أنظمة Intel فقط. عند اختيارها، تقوم HP Sure Start باسترداد الإعدادات الافتراضية المصنعية لتكوين وحدة تحكم الشبكة.

يُطلب تدخل المستخدم عند تغيير تكوين وحدة تحكم الشبكة (الأجهزة ذات معالجات Intel فقط)

هذا الإعداد متوفر في أنظمة Intel فقط. توفر HP التكوين الافتراضي من المصنع لوحدة تحكم الشبكة والذي يتضمّن عنوان MAC. عند تعيين هذا الإعداد على **تمكين**، يقوم النظام بمراقبة حالة تكوين وحدة تحكم الشبكة ويطلب تدخُّل المستخدم في حالة حدوث تغيير عن حالة التكوين الافتراضية من المصنع. ويكون الإعداد الافتراضي لهذه الميزة **تعطيل**.

المسح الديناميكي لوحدة بدء التشغيل أثناء التشغيل (في الأجهزة ذات معالجات Intel فقط)

هذا الإعداد متوفر في أنظمة Intel فقط. عند اختيار الإعداد الافتراضي **تفعيل**، تقوم HP Sure Start بشكلٍ دوري بتفحُّص سلامة وحدة بدء تشغيل BIOS أثناء عمل نظام التشغيل. عند التعيين على **تعطيل**، تقوم HP Sure Start بفحص السلامة فقط قبل بدء التشغيل أو التنشيط من وضع السكون أو الإسبات.

حماية إعدادات HP Sure Start BIOS

يكون الإعداد الافتراضي لسياسة حماية إعدادات BIOS **معطلة**. لتفعيل هذه الميزة، يجب أن يقوم مالك/مسؤول الجهاز العميل أولاً بضبط جميع سياسات BIOS حسب الإعدادات المفضلة. يحتاج المالك/المسؤول كذلك إلى ضبط كلمة مرور إعدادات BIOS لاستخدام حماية إعدادات HP Sure Start BIOS.

بمجرّد إتمام ذلك، يجب أن تتغيّر حالة سياسة حماية إعدادات BIOS إلى "مُفعَّل". عند هذه المرحلة، يتم إنشاء نسخة احتياطية من جميع إعدادات BIOS في وحدة التخزين المحمية من HP Sure Start. وفيما بعد، لا يمكن تعديل أيٍّ من إعدادات BIOS محليًا أو عن بُعد. يتم التحقق من إعدادات سياسة BIOS في كل عملية بدء تشغيل لتكون وفق الحالة المرغوبة، وإذا كان هناك أي تعارض، يتم استرداد إعدادات BIOS من وحدة التخزين المحمية من HP Sure Start.

لتعديل أحد إعدادات BIOS، يجب إدخال كلمة مرور مسؤول BIOS وسيتم تعطيل حماية إعداد BIOS بصورة متسلسلة، وهي المرحلة التي يمكن خلالها إجراء تغييرات على إعدادات BIOS.

حماية مفاتيح بدء التشغيل الآمن في HP Sure Start

عند اختيار هذا الإعداد بحالته الافتراضية **تمكين**، توفر HP Sure Start حماية مُحسّنة لقواعد بيانات ومفاتيح بدء التشغيل الآمن التي يستخدمها BIOS للتحقق من سلامة وموثوقية برنامج تحميل بدء التشغيل لنظام التشغيل قبل بدء تشغيل عملية بدء التشغيل. عند اختيار حالة **تعطيل**، تُستخدم حماية متغيرات بدء تشغيل UEFI الآمن فقط ولا يتم حفظ نسخة احتياطية من خلال النظام الفرعي في HP Sure Start.

الكشف والحماية المتقدمة لبرنامج HP الثابت ضد الاختراقات أثناء التشغيل (في الأجهزة التي تعمل بمعالجات Intel فقط) وكشف وحماية برنامج HP الثابت ضد الاختراقات أثناء التشغيل (في الأجهزة التي تعمل بمعالجات AMD فقط)

ميزة RTID **مُفعَّلة** افتراضيًا لجميع الأنظمة الأساسية التي يتم إنتاجها من مصنع HP. لا يوجد حاجة لقيام العميل/المسؤول بتفعيل أو "نشر" هذه الميزة للتمتع بميزة RTID في HP Sure Start.

يمكن ضبط تعيين ميزة RTID اختياريًا على **تعطيل** من قِبل مالك/مسؤول النظام الأساسي.

سياسة أحداث الأمان في HP Sure Start

تتحكّم إعدادات سياسة BIOS بالإجراءات المتخذة عند كشف HP Sure Start لهجوم أو محاولة هجوم أثناء عمل نظام التشغيل. وهناك ثلاثة إعدادات ممكنة لهذه السياسة:

- **تسجيل الحدث فقط:** عند اختيار هذا الإعداد، يقوم HP ESC بتسجيل أحداث الكشف، والتي يمكن عرضها في سجلات التطبيقات والخدمات/في مسار HP Sure Start ضمن عارض أحداث Microsoft Windows.[3]
- **تسجيل الحدث وإخطار المستخدم:** هذا هو الإعداد الافتراضي. عند اختيار هذا الإعداد، يقوم HP ESC بتسجيل أحداث الكشف، والتي يمكن عرضها في سجلات التطبيقات والخدمات/في مسار HP Sure Start ضمن عارض أحداث Microsoft Windows. بالإضافة إلى ذلك، يُوجه المستخدم باتخاذ إجراء ضمن نظام Windows الذي وقع فيه الحدث.[4]
- **تسجيل حدث وإيقاف تشغيل النظام:** عند اختيار هذا الإعداد، يقوم HP ESC بتسجيل أحداث الكشف، والتي يمكن عرضها في سجلات التطبيقات والخدمات/في مسار HP Sure Start ضمن عارض أحداث Microsoft Windows. بالإضافة إلى ذلك، يتلقى المستخدم إشعارًا ضمن نظام Windows بوقوع الحدث، وبأن إيقاف تشغيل ذلك النظام صار وشيكًا.

إشعارات الأحداث التي تتعلق بالأمان أثناء بدء التشغيل في HP Sure Start

يتحكم هذا الإعداد الخاص بسياسة BIOS فيما إذا كانت تحذيرات HP Sure Start ورسائل الخطأ التي تظهر عند بدء تشغيل النظام تتطلّب موافقة المستخدم المحلي على الخطأ قبل استكمال بدء التشغيل. وباستخدام القيمة الافتراضية لهذا الإعداد وهي **تتطلّب الموافقة**، يتوقّف النظام ويعرض رسالة الخطأ. ويجب أن يقوم المستخدم بالضغط على مفتاح لاستكمال عملية بدء التشغيل. إذا تم تغيير حالة الإعداد إلى **انقضاء الوقت بعد 15 ثانية**، يتم عرض الرسالة، ولكن يتم استكمال عملية بدء التشغيل تلقائيًا بعد أن تظل الرسالة معروضة لمدة 15 ثانية فقط.

إغلاق إصدار BIOS

في شاشة إعدادات BIOS (يتم الدخول إليها بضغط F10)، توجد هذه الميزة في قسم رئيسي/أو تحديث BIOS.

عند ضبط إعداد هذه الميزة على **تعطيل**، يمكنك تحديث BIOS باستخدام أي عملية مدعومة. إذا قام HP ESC باكتشاف تحديث صحيح لوحدة بدء التشغيل في ذاكرة فلاش للنظام، فإنّه يقوم بتحديث النسخة الاحتياطية لوحدة بدء التشغيل.

عند ضبط إعداد هذه الميزة على **تفعيل**، فستقوم جميع أدوات تحديث HP BIOS برفض تحديث BIOS. بالإضافة إلى ذلك، تقوم HP Sure Start بحماية BIOS من محاولات تغيير إصدار BIOS بإزالة ذاكرة فلاش للنظام باستخدام طريقة غير موثوقة. يقوم HP ESC بتسجيل الإصدار المغلق من BIOS. إذا اكتشف HP ESC وجود تغيير في BIOS بذاكرة فلاش للنظام، فإنّه يقوم بإزالة وحدة بدء تشغيل BIOS ويضع مكانها نسخة من وحدة بدء تشغيل HP ESC. تقوم نسخة HP ESC الخاصة بوحدة بدء التشغيل بتنفيذ واسترداد ما تبقّى من إصدار BIOS الصحيح. ويكون الإعداد الافتراضي لهذه الميزة **تعطيل**.

حفظ/استرداد سجل MBR الخاص بالقرص الثابت للنظام وحفظ/استرداد سجل GPT الخاص بالقرص الثابت للنظام

في شاشة إعدادات BIOS (يتم الدخول إليها بضغط F10)، توجد هذه الميزة في قسم الأمان/أدوات محرك الأقراص الثابتة. تتوفر إمكانية واحدة فقط من هاتيْن الإمكانيّتيْن، حسب نوع قسم القرص الأساسي (GPT أو MBR)، الذي تقوم HP Sure Start باكتشافه.

عند ضبط الحالة على **تفعيل**، تقوم HP Sure Start بحفظ نسخة احتياطية محمية من جدول قسم GPT/MBR من محرك الأقراص الأساسي وتُقارن النسخة الاحتياطية بالنسخة الأساسية في كل عملية بدء تشغيل. وإذا تم اكتشاف اختلاف، يتم توجيه المستخدم ويمكنه اختيار استرداد الحالة الأصلية من النسخة الاحتياطية، أو تحديث النسخة الاحتياطية المحمية بالتغييرات. يمكن استخدام **سياسة استرداد قطاع بدء التشغيل (GPT/MBR)** اختياريًا لإلغاء قرار المستخدم باتخاذ إجراء في حالة عثور HP Sure Start على تعارض.

عند ضبط الإعداد على **تعطيل** (القيمة الافتراضية)، لا توفر HP Sure Start حماية لسجل GPT/MBR.

سياسة استرداد قطاع بدء التشغيل (GPT/MBR)

عند ضبط الإعداد على **تحكم المستخدم المحلي** (الإعداد الافتراضي) يُطلَب من المستخدم اتخاذ إجراء عند اكتشاف HP Sure Start لتغيير في جدول أقسام GPT/MBR.
عند ضبط الإعداد على **استرداد في حالة التلف**، تقوم HP Sure Start باسترداد GPT/MBR تلقائيًا إلى الحالة المخزنة وذلك في أي وقت يتم فيه اكتشاف اختلافات.

إدارة عناصر التحكم في سياسات HP Sure Start عن بُعد

خروجًا عن الإطار التقليدي، تم تحسين عناصر التحكم في سياسات HP Sure Start لتناسب استخدام المستخدم العادي. وبما أنّ تقنية HP Sure Start تكون مُفعَّلة افتراضيًا، فليس هناك حاجة إلى قيام المسؤول البعيد باتخاذ أي إجراء لتفعيل (أو "نشر") سياسة HP Sure Start.
في حالة رغبة المسؤول البعيد في تعديل إعدادات سياسة HP Sure Start، فيمكن استخدام نفس واجهات برمجة التطبيقات لأدوات إدارة Windows المعروفة باسم (WMI) أو البرامج النصية لأداة تكوين HP BIOS المُستخدَمة لإدارة سياسات BIOS الأخرى في النظام الأساسي، وذلك لإدارة سياسات HP Sure Start. بالإضافة إلى ذلك، يمكن للمسؤولين إدارة إمكانات HP Sure Start عن بُعد باستخدام المكون الإضافي Manageability Integration Kit المعروف اختصارًا باسم (MIK) الخاص بتطبيق Microsoft System Center Configuration Manager المعروف اختصارًا باسم (SCCM).

بالإضافة إلى ذلك، يمكن للمسؤولين إدارة إمكانات HP Sure Start عن بُعد وعرض أحداث HP Sure Start باستخدام المكون الإضافي Manageability Integration Kit المعروف اختصارًا باسم (MIK) الخاص ببرنامج Microsoft System Center Configuration Manager المعروف اختصارًا باسم (SCCM).

الخاتمة

تُوفّر HP Sure Start الفوائد الرئيسية التالية:

- **إنتاجية دون توقف -** تحافظ HP Sure Start على استمرار العمل في حالة حدوث هجوم أو عطل عرَضي من خلال محو فترة التوقف في انتظار مسؤولي تكنولوجيا المعلومات أو الخدمة المختصين.
- **تكلفة أقل -** تُقلّل إمكانية الاسترداد التلقائي في HP Sure Start من الاتصال بمكتب صيانة تكنولوجيا المعلومات كما أنها تُحسّن الإنتاجية، وهو ما يساعد في نهاية المطاف على خفض تكلفة صيانة النظام الأساسي.
- **راحة البال -** تُقدّم HP Sure Start مزايا أمان متعددة يمكن تشغيلها على مجموعة متنوعة من البرامج والأنظمة الأساسية للأجهزة.

تتم حماية البرنامج الثابت الهام لنظام BIOS من البرامج الخبيثة من خلال الميزة الرائدة في كشف محاولات الاختراق في البرنامج الثابت والإصلاح التلقائي له، والتي تُقدّمها HP Sure Start، حيث إنها متوفرة حصريًا على أجهزة HP Elite.

الملحق أ - تقنية HP Sure Start، جيلاً بعد جيل

قدّمت HP تقنية Sure Start في عام 2014. ومنذ ذلك الوقت، قامت HP بتحسين Sure Start وتوسيع عدد المنتجات التي تستخدمها. يُوضّح الجدول أدناه ملخصًا عن الإمكانيات التي تمت إضافتها لكل جيل.

الجيل	تاريخ الإصدار	الإمكانيات المضافة
HP Sure Start	2014	• فرض موثوقية البرنامج الثابت ونظام BIOS، مع إمكانية الإصلاح الذاتي • مراقبة البرنامج الثابت ومدى توافقه
HP Sure Start مع الحماية الديناميكية	2015	• دعم عارض أحداث Windows • الحماية الديناميكية (عند اختيار الأجهزة المُزوّدة بمعالجات Intel)
الجيل الثالث من HP Sure Start (عند اختيار الأجهزة المُزوّدة بمعالجات Intel)[5] تقنية HP Sure Start مع ميزة كشف محاولات الاختراق أثناء التشغيل (عند اختيار الأجهزة المُزوّدة بمعالجات AMD)[6]	2017	• ميزة كشف محاولات الاختراق أثناء التشغيل • حماية إعدادات BIOS • استخدام المكون الإضافي Manageability Integration Kit المعروف اختصارًا باسم (MIK) الخاص برنامج Microsoft SCCM
HP Sure Start الجيل الرابع[7]	2018	• مساحة تخزين محمية - أساليب تشفير قوية لتخزين إعدادات BIOS، وبيانات اعتماد المستخدمين، والإعدادات الأخرى في أجهزة HP Endpoint Security Controller لتوفير حماية السلامة، وكشف محاولات التلاعب، وحماية سرية البيانات • حماية قواعد بيانات بدء التشغيل الآمن - حماية مُحسّنة لقواعد البيانات والمفاتيح التي يُخزّنها BIOS والهامة لسلامة مزايا بدء التشغيل الآمن لنظام التشغيل مقارنة بتنفيذ UEFI BIOS • على الأنظمة التي تعمل بمعالجات Intel، حماية مُحسّنة واسترداد للبرنامج الثابت لـ Intel Management Engine • شهادة أمان من جهة خارجية لوحدة HP Endpoint Security Controller - اجتياز اختبارات مختبر مستقل ومعتمد للتحقق من أنّ الوظائف الأساسية لأجهزة HP ESC تعمل وفقًا لما أعلنته HP ووفقًا للمعايير والمنهجيات والعمليات المتعارف عليها بشكل عام[1] • تتجاوز مزايا أجهزة HP المزودة بتقنية HP Sure Start ما هو منصوص عليه في مسودة إرشادات NIST لمرونة أمان الإنترنت للبرامج الثابتة للأنظمة الأساسية (المنشور الخاص 800-193)

الملحق ب - نظرة عامة على System Management Mode (SMM)

وضع إدارة النظام (SMM) هو أسلوب قياسي في الصناعة يستخدم لميزات إدارة الطاقة المتقدمة للكمبيوتر الشخصي وغيرها من وظائف نظام التشغيل المستقلة أثناء تشغيل نظام التشغيل. في حين أن مصطلح SMM وتطبيقه مخصصان لأنظمة x86، فإن العديد من أنظمة الحوسبة الحديثة تستخدم مفهومًا هيكليًا مشابهًا.

يتم تكوين SMM بواسطة BIOS عند بدء التشغيل. يتم تحميل التعليمات البرمجية لوضع SMM في الذاكرة الرئيسية (DRAM) ثم يستخدم BIOS سجلات تكوين خاصة (قابلة للقفل) داخل مجموعة الشرائح لحظر الوصول إلى هذه المنطقة عندما لا يتم تشغيل معالجات البيانات الدقيقة في سياق SMM. أثناء وقت التشغيل، يكون الدخول إلى وضع SMM معتمدًا على الحدث. تمت برمجة مجموعة الشرائح بحيث تدرك العديد من أنواع الأحداث والمُهل الزمنية. عند وقوع مثل هذا الحدث، يقوم جهاز مجموعة الشرائح بتثبيت رقم التعريف الشخصي (PIN) لإدخالات مقاطعة إدارة النظام (SMI). عند حدود الإرشاد التالي، يقوم معالج البيانات الدقيق بحفظ حالته بالكامل ويدخل في وضع SMM.

عند دخول معالج البيانات الدقيق في وضع SMM، يقوم بالتأكيد على رقم التعريف الشخصي لمخرجات الجهاز SMI Active (SMIACT). يُوجّه هذا التثبيت رسالةً إلى أجهزة مجموعة الشرائح لإعلان دخول معالج البيانات الدقيق في وضع SMM. يمكن تأكيد إدخال SMI في أي وقت، وخلال أي وضع عملية تشغيلية، باستثناء ما يأتي من SMM نفسها. يتعرف جهاز مجموعة الشرائح على إشارة SMIACT ويعيد توجيه كل دورات الذاكرة اللاحقة إلى منطقة محمية من الذاكرة (يشار إليها أحيانًا بمنطقة SMRAM)، محجوزة خصيصًا لوضع SMM. ويبدأ معالج البيانات الدقيق بحفظ حالته الداخلية بأكملها في هذه المنطقة المحمية من الذاكرة فور استلام مدخلات SMI وتأكيد مخرجات SMIACT.

بعد تخزين حالة معالج البيانات الدقيق على ذاكرة SMRAM، يبدأ تشغيل التعليمات البرمجية لمعالج SMM الخاص الذي يتواجد أيضًا في SMRAM (تم وضعه من خلال BIOS الخاص بالنظام في وقت بدء التشغيل) في وضع تشغيل SMM خاص. أثناء التشغيل في هذا الوضع، يتم تعليق معظم آليات عزل الأجهزة والذاكرة، ويمكن لمعالج البيانات الدقيق الوصول إلى جميع الموارد في النظام الأساسي لتمكينه من تنفيذ المهام المطلوبة. تقوم التعليمات البرمجية لوضع SMM بإكمال المهمة المطلوبة، ثم يحين وقت إعادة المعالج إلى وضع التشغيل السابق. عند هذه النقطة، تقوم التعليمات البرمجية لوضع SMM بتشغيل تعليمات العودة من وضع إدارة النظام (RSM) وذلك لإنهاء وضع SMM. تؤدي إرشادات RSM إلى جعل معالج البيانات الدقيق يقوم باستعادة بيانات الحالة الداخلية السابقة الخاصة به من النسخة المحفوظة في SMRAM عند الدخول في وضع SMM. عند الانتهاء من تنفيذ إرشادات RSM، تكون قد تمت استعادة حالة معالج البيانات الدقيق بالكامل إلى الحالة التي كان عليها قبل حدث SMI، ويتم استئناف عمل البرنامج السابق (نظام التشغيل، والتطبيقات، وبرنامج hypervisor، وما إلى ذلك) من عند النقطة التي توقف عندها تمامًا.

[1] تم اعتماد أجهزة تحكم HP Sure Start وفقًا لإطار شهادة CSPN.

[2] تتوفر تقنية HP Sure Start مع الحماية الديناميكية في أجهزة HP Elite المجهّزة بالجيل السادس وأحدث من معالجات Intel Core.

[3] يلزم تثبيت برنامج HP Notification لعرض أحداث HP Sure Start في عارض أحداث Windows.

[4] يلزم تثبيت برنامج HP Notification ليتم استلام الإشعارات.

[5] يتوفر الجيل الثالث من تقنية HP Sure Start في أجهزة HP Elite المجهّزة بالجيل السابع من معالجات Intel.

[6] تتوفر تقنية HP Sure Start مع ميزة كشف الاختراق أثناء وقت التشغيل (Runtime Intrusion Detection) في أجهزة HP Elite المجهّزة بالجيل السابع من معالجات AMD.

[7] الجيل الرابع من تقنية HP Sure Start متوفر في أجهزة HP Elite و600 HP Pro المجهّزة بالجيل الثامن من معالجات Intel أو AMD.

لمعرفة المزيد تفضل بزيارة الرابط
hp.com/go/computersecurity

4AA7-3172ARE، ايار 2018