HP Sure Click Enterprise

Eingebaute Sicherheit: Anwendungsisolation und -Containment

WHITEPAPER

Wiederveröffentlichung von HP Inc. im Mai 2020

„Für das US-Justizministerium steht fest, dass es sich nach der Installation von Bromium keine Sorgen mehr um Endpunktsicherheit machen muss“

Kurzübersicht

IT-Sicherheitsteams in Regierungsbehörden und bei deren Auftragnehmern stehen beim Absichern ihrer Netzwerke gegen moderne Malware-Angriffe vor komplizierten Herausforderungen. Dazu zählen komplexe persistente Bedrohungen, komplexe zielgerichtete Angriffe, polymorphe Malware und dateilose Eindringversuche. Ihre Netzwerke und Infrastrukturen sind Hauptangriffsziele für Staaten, politische Agitatoren, organisierte Kriminalität und andere Hacker, die sich Zugriff auf brisante Inhalte verschaffen möchten – zu Spionagezwecken, zur politischen Destabilisierung oder um sich finanzielle Vorteile zu verschaffen. Darüber hinaus müssen Sie unzählige Bestimmungen von nationalen und internationalen Aufsichts- und Standardisierungsorganisationen erfüllen.

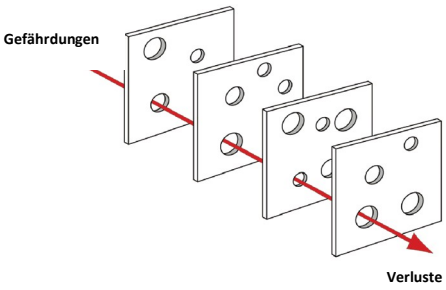
Das Problem

Der öffentliche Sektor einschließlich der für die Regierungen enorm wichtigen Verteidigungs-, Industrie- und Produktionsstandorte stellen für Angreifer, Kriminelle und Geschäftemacher aller Couleur Ziele erster Güte dar. Besonders wertvolle militärische, strategische, diplomatische und persönliche Datensätze sind einträgliche Ziele für Täter, die keine Mühen scheuen, um mit viel Geduld, hohem Zeiteinsatz und großer Ausdauer ihre Ziele zu erreichen – mit oft verheerenden Folgen.

Statistiken zu Sicherheitsverletzungen im öffentlichen Sektor bestätigen dies. Angaben aus dem Verizon Data Breach Investigations Report aus dem Jahr 2017[1]: Ungefähr 64 % der Sicherheitsverletzungen in diesem vertikalen Markt standen im Zusammenhang mit Spionage; über 85 % der Täter waren entweder Staaten oder staatsnah; und die „Verweildauer" von Malware (Zeit bis zur Entdeckung) betrug Jahre.

Frequenz	21.239 Vorfälle, 239 mit bestätigter Datenoffenlegung
Top-2-Muster	Cyber-Spionage, Privilegienmissbrauch und verschiedene andere Fehler machen 81 % der Verstöße in der öffentlichen Verwaltung aus.
Bedrohungsakteure	62 % extern, 40 % intern, 4 % mehrere Parteien, 2 % Partner (Verstöße)
Beweggründe von Akteuren	64 % Spionage, 20 % finanzielle Gründe, 13 % Spaß/Ideologie/Missgunst (Verstöße)
Beeinträchtigte Daten	41 % persönliche Daten , 41 % geheime Daten, 14 % Berechtigungsnachweise, 9 % medizinische Daten
Zusammenfassung	Fast die Hälfte der Angriffe, die zu bestätigten Datenoffenlegungen führen, haben eine staatliche Ursache. Beim Zeitrahmen vom Datenverstoß bis zur Erkennung entfallen über 50 % auf die Kategorie „Jahre".

Sicherheitsvorfälle in der öffentlichen Verwaltung, Verizon 2017 Data Breach Investigations Report.



Das mehrschichtige Schweizer-Käse-Verteidigungsmodell

Der alte Sicherheitsansatz ist der Aufgabe nicht gewachsen

Auf Erkennung basierende Sicherheitslösungen schützen vor den bekannten 99 % der Angriffe, aber haben Probleme, die verbleibenden unbekannten, unmöglich zu erkennenden 1 % abzuwehren. Dass sich Bedrohungen Bahn brechen können, ist unvermeidbar. Dies liegt an der Abhängigkeit von alten Architekturen, die auf dem Abgleich von Signaturen, Heuristiken, Verhaltensweisen und anderen vorher identifizierten Attributen. Wie stellt sich ein Unternehmen neuen, beispiellosen Bedrohungen entgegen, beispielsweise Arten von dateiloser Malware und Schadcode, der ausschließlich im Arbeitsspeicher ausgeführt wird? Selbst Antivirenprogramme der nächsten Generation, künstliche Intelligenz und Techniken für maschinelles Lernen ermöglichen erkennungsbasierten Lösungen aufgrund von deren fundamental eingeschränkten Architekturen nicht, der schnellen Innovation von Exploits und Techniken Herr zu werden.

[1] 2017 Data Breach Investigations Report - Verizon Enterprise Solutions

Compliance ist nur der Anfang

FISMA verlangt die „Entwicklung und Aufrechterhaltung von Mindestkontrollen zum Schutz von bundesbehördlichen Informationen und Informationssystemen“ und „einen Mechanismus für einen verbesserten Überblick über bundesbehördliche Programme zur Informationssicherheit“

Compliance ist nicht mit Sicherheit gleichzusetzen. Sie dient lediglich als Referenzbasis für die eigentliche Sicherheitsdiskussion. Gesetzliche Bestimmungen führen häufig „Mindestkontrollen“ für den Erhalt von Compliance-Zertifizierung auf. Diese dienen jedem Unternehmen als Ausgangspunkt für die anschließende Implementierung ihrer Richtlinienkontrollen für geschäftskritische Anwendungsfälle. In fast allen dokumentierten Fällen, in die Organisationen aus dem öffentlichen Sektor und Auftragnehmer staatlicher Behörden involviert sind, bei denen Sicherheitsverletzungen aufgetreten sind, haben die betroffenen Opfer die ihnen auferlegten behördlichen Vorschriften vollumfänglich erfüllt und verfügten über die aktuellen Zertifizierungen.

Oftmals greifen die Vorschriften selbst zu kurz und sehen zum Beispiel die Verwendung altmodischer Antivirenprogramme als universelle Lösung vor, obwohl bereits neuere und wesentlich effektivere und fortschrittlichere Sicherheitslösungen verfügbar sind. Verschärft wird das Problem noch dadurch, dass Compliance-Vorschriften den aktuellen Taktiken, Techniken und Methoden der Angreifer um bis zu einige Jahre hinterherhinken. In Anbetracht der Tatsache, dass so viel auf dem Spiel steht, ist der Ansatz der Einhaltung von Mindestanforderungen hoffnungslos veraltet und für die Bedrohungslage von heute schlecht geeignet.

Die Patching-Herausforderung im öffentlichen Sektor

Nur 33 % der im öffentlichen Sektor verwendeten Systeme werden pünktlich gepatcht.

- VERIZON 2017 DATA BREACH INVESTIGATIONS REPORT, S.13

Laut dem 2016 erschienenen Bericht zur Cybersicherheit von HP Security Research[2] sind die 10 am häufigsten ausgenutzten Sicherheitslücken alle älter als ein Jahr. Für die meisten waren seit Monaten oder sogar Jahren Patches verfügbar. Unglücklicherweise bleiben Millionen von PCs in Regierungsbehörden und bei Service-Providern über lange Zeiträume ungepatcht. Untersuchungen von Verizon zeigen, dass nur auf 33 % der im öffentlichen Sektor eingesetzten Systeme regelmäßig Patches installiert werden, sodass kritische Systeme – sowie wertvolle Daten und geistiges Eigentum auf ihnen – durch unzählige alte und neue Sicherheitslücken bedroht sind. Nach großzügigen Schätzungen von Verizon steht „regelmäßig“ für einen Patching-Zyklus von durchschnittlich 12 Wochen – obwohl Microsoft und andere Hersteller monatliche Patches anbieten.

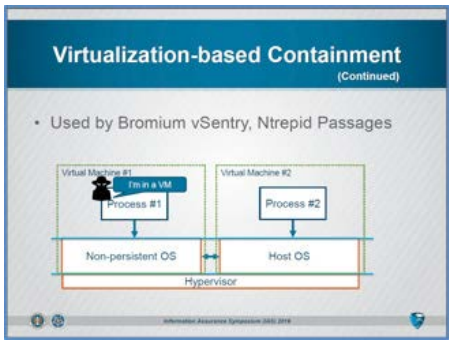
2 HPE Security Research, Cyber Risk Report 2016

„Die bei weitem effektivste Schutzlösung, die ich bislang kennen gelernt habe.“

– DIRECTOR IT GLOBAL SECURITY IN DER FERTIGUNGSINDUSTRIE

Es wird dringend ein neuer Ansatz benötigt

Das zentrale Merkmal von HP Sure Click Enterprise ist die Anwendungsisolation, eine hardwaregestützte Isolation zur Absicherung des Unternehmens gegen Unvermeidliches (z. B. Benutzerfehler, ungepatchte Systeme und hochempfindliche, mit dem Internet verbundene oder für Partner zugängliche Geräte). Wir haben die ineffektive Praxis von „hinzugefügten“ Schutz-durch-Erkennung-Sicherheitslösungen grundlegend verändert und haben ein Modell mit „integriertem“ Schutz geschaffen, das direkt am Chipsatz ansetzt. Sure Click bietet eingebauten Schutz für die dauerhafte Sicherheit von Unternehmen und ist nicht von der externen Erkennung des Unbekannten oder dem Urteil von viel beschäftigten und leicht zu täuschenden Benutzern abhängig. Durch das automatische Isolieren aller Inhalte, die aus nicht vertrauenswürdigen Quellen stammen, sind Einrichtungen des öffentlichen Sektors und Auftragnehmer staatlicher Behörden vor Lücken in ihren traditionellen Verteidigungsmechanismen und vor falschen Beurteilungen durch ihre Benutzer geschützt. Egal, ob es sich um konventionelle, fortschrittliche, gezielte oder dateilose Angriffe oder um Zero-Day-Exploits handelt – Sure Click isoliert und verhindert sie alle! Mit Sure Click gehört zudem das Notfall-Patching der Vergangenheit an.

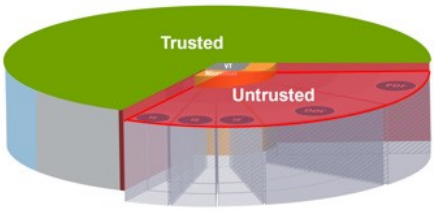


Virtualisierungstechnologie von Bromium weckt besonderes Interesse der NSA

Sicherheit durch Anwendungsisolation und -Containment

Auf dem Information Assurance Symposium (IAS) 2016[3] veröffentlichten die National Security Agency (NSA) und der Central Security Service (CSS) der USA gemeinsam eine Präsentation mit dem Titel „Application Isolation & Containment for Endpoint Protection“. Ihre Prämisse war, dass echte Sicherheit nur durch Verringerung des Schadenspotenzials eines kompromittierten Prozesses zu erreichen sei. Genau dies ist der Ansatz von Sure Click – worauf in der Präsentation explizit hingewiesen wird: die Nutzung unserer einzigartigen, mehrfach patentierten hardwaregestützten Prozessisolation und der weitestgehende Verzicht auf Beschränkungen der Zugriffsrechte für alle Tasks, die in mikrovirtualisierten Umgebungen ausgeführt werden, um High-Fidelity-Endpunkte mit geringen Sicherheitsrisiken zu schaffen.

[3] Information Assurance Symposium (IAS) 2016 – Application Isolation Containment



Sure Click Enterprise stuft das Host-Betriebssystem und sämtliche Web- oder Dateiinhalte entweder als vertrauenswürdig oder nicht vertrauenswürdig ein.

Trennen der nicht vertrauenswürdigen Inhalte von den vertrauenswürdigen

Sure Click Enterprise teilt die Welt in vertrauenswürdige und nicht vertrauenswürdige Inhalte ein. Nicht vertrauenswürdige Inhalte stammen normalerweise aus Quellen außerhalb des Unternehmens und werden über verschiedene Vektoren für eingehenden Datenverkehr eingeschleppt, darunter Web, E-Mail, Cloud-Services und USB. Vertrauenswürdige Inhalte stammen überwiegend aus bekannten internen Quellen oder aus Dateien, die Benutzer aus dem Unternehmen selbst erstellen und verteilen. Die zwei Inhaltstypen sind unterschiedlich zu behandeln.

Nicht vertrauenswürdige Inhalte können alles Mögliche enthalten – bereits Bekanntes oder Unbekanntes, bereits Erkanntes oder Unerkanntes – und sollten daher stets als potenziell schädlich angesehen werden. Ihnen sollte niemals Zugriff auf das eigentliche Host-Betriebssystem, das Dateisystem oder das interne Netzwerk gewährt werden. Vertrauenswürdige Inhalte lassen sich hingegen sicher auf vorhandenen physischen Ressourcen ausführen. Aus Sicht der Benutzer sollten jedoch niemals Abweichungen in Bezug auf Aussehen, Verhalten oder Workflow von Anwendungen festzustellen sein.

Anwendungsisolation und -Containment in Mikro-VMs

Ransomware wird sicher in einer entfernbaren Mikro-VM abgesondert und einfach weggeklickt, wenn der Benutzer das Fenster schließt.

Hinter Anwendungsisolation und -Containment steht die einfache Idee, dass einer unbekannten Bedrohung die Möglichkeit genommen wird, Schaden anzurichten. Diese Idee umzusetzen ist jedoch alles andere als einfach. Daher sticht Sure Click Enterprise mit Technologie von Bromium und seinem einzigartigen, patentierten Ansatz der Mikrovirtualisierung auf Hardwareebene heraus. Der Host-PC wird auf der Ebene unterhalb des Windows-Systemkernels geschützt, was die Angriffsfläche erheblich verkleinert. Nicht vertrauenswürdige Anwendungsinhalte bleiben innerhalb jeder Mikro-VM zuverlässig geschützt. Der einzigartige Ansatz von Sure Click bietet eingebauten Schutz gegen Zero-Day-Bedrohungen durch Sicherheitslücken in Anwendungen, Browsern und dem Kernel und damit einen Dreifach-Schutz, den traditionelle Verteidigungslösungen und Lösungen der nächsten Generation nicht annähernd erreichen.

Auf den mit Sure Click geschützten Endpunkten werden gängige Office-Dokumente wie Word-, Excel- und PowerPoint-Dateien – sowie Adobe PDFs und andere von den Administratoren festgelegte Dateitypen – nach Anwendung voneinander und vom Host-PC direkt auf der Hardwareebene in sicheren und entfernbaren Mikro-VMs isoliert, sodass Benutzer ohne Workflow-Störungen nahtlos weiterarbeiten und jeden Inhalt mit gutem Gefühl anklicken können, weil sie wissen, dass ihre Systeme sicher sind.

RUHE BEWAHREN und Infektionen verhindern

Sure Click Kunden haben zusammen über ZWEI MILLIARDEN Mikro-VMs gestartet und bislang KEINE Malware-Einschleusung festgestellt!

Erstinfektionsabwehr und Eigenwartung

Anwendungsisolation und -Containment schützt vor allem vor der gefährlichen Patient-Zero-Infektion im Unternehmen. Über diesen zuerst kompromittierten Endpunkt versuchen Angreifer, im Unternehmen Fuß zu fassen, um dann durch Lateral Movement und Berechtigungsausweitungen das Unternehmen auszuspähen. Bei jeder Ausführung von nicht vertrauenswürdigen Inhalten in einer Bromium Mikro-VM wird eine vollständige Bedrohungsanalyse mit umfassender Kill-Chain-Analyse durchgeführt.

Neben der Verhinderung von Malware-Infektionen an Endpunkten bewirkt Sure Click auch die Eigenwartung von Endpunkten, wenn der Benutzer das Anwendungsfenster oder den Browser-Tab schließt. Dadurch werden kostspielige und zeitaufwendige manuelle Wartungsarbeiten vermieden. Beim Schließen der Mikro-VM verschwindet die Malware einfach für immer, ohne den Host-PC zu schädigen oder sich im Unternehmen zu verbreiten, wobei alle Informationen zur Bedrohung und sämtliche Kill-Chain-Analysen global geteilt und für Sicherheitsteams aufbewahrt werden.

Vermeidung der Infektionsausbreitung

Auf einem durch Sure Click geschützten Endpunkt befindliche Malware wird wie beabsichtigt in einem sicheren entfernbaren Container ausgeführt. Sie hat jedoch keine Möglichkeit, aus der Mikro-VM-Umgebung zu entkommen, um den Host-PC oder andere Netzwerkgeräte zu befallen. Nicht nur der ursprüngliche Ziel-PC ist geschützt, sondern auch alle anderen mit dem Netzwerk verbundenen Geräte, die mit dem Host interagieren, der Ziel des Angriffs war. Einfach ausgedrückt sind Sure Click Endpunkte eine absolute Sackgasse für Malware, aus der sie nicht wieder herauskommen. Schadcode kann sich nicht verbreiten und keine vertraulichen Daten oder sensible Prozesse auf dem Host, dem Netzwerk oder anderen verbundenen Geräten erreichen. Malware hat weder Zugriff auf das Intranet noch auf Dateifreigaben, da Lateral Movement und Verbreitung unterbunden werden.

Erstinfektion	Lateral Movement	Eigenwartung
Gestoppt!	Unmöglich!	Automatisiert!

Entscheidend ist das Verhalten der realen Benutzer

Sure Click Threat Intelligence führt nicht nur Kill-Chain-Analysen in Kombination mit vollständiger Malware-Absonderung in Mikro-VMs durch, sondern profitiert auch von dem Umstand, dass reale Benutzer, reale Aufgaben an realen PCs ausführen – etwas, das Sandboxing-Lösungen mit ihren verschiedenen Techniken zur „Emulation des Benutzerverhaltens“ nicht in vollem Umfang replizieren können. Gezielt eingesetzte Malware fordert Benutzer häufig zum Handeln auf oder wartet das Agieren der Benutzer ab, bevor sie ihre gesamte schädliche Nutzlast freisetzt. Reale Benutzer interagieren mit Dokumenten sowohl auf vorhersehbare als auch auf unvorhersehbare Weise. Nur Sure Click erfasst das gesamte reale Benutzerverhalten, anstatt eine generische Menge von Mausklicks, Cursorbewegungen, Texteinträgen und Dateisystemoperationen zu replizieren. Aus realem Benutzerverhalten lässt sich High-Fidelity-Intelligenz generieren.

Reales Benutzerverhalten kann von Sandboxing-Lösungen nicht exakt in vollem Umfang repliziert werden, da Benutzer unvorhersehbar handeln und bei der realen Systemnutzung auf vielfältige Weise agieren. In Kombination mit zweckgebundenen Mikro-VMs generiert SureClick ein sehr hohes Signal-Rausch-Verhältnis für jede schädliche Aktivität, die vom erwarteten realen Verhalten abweicht.

Erkennung kostet echtes Geld für die Untersuchung und Bereinigung von infizierten Geräten und viele Alarme sind Fehlalarme oder unvollständig. Ein besserer Ansatz sieht die Erfassung aller Informationen zur Bedrohung und umfassende Kill-Chain-Analysen vor, ohne dass es im Vorfeld überhaupt zu einer Infektion kommt. Dann gibt es nichts zu bereinigen.

Niedrigere Kosten für Untersuchung und Bereinigung

Studien des Ponemon Institute zeigen, dass Unternehmen wöchentlich fast 17.000 Malware-Warnmeldungen erhalten. Nur 19 % davon sind zuverlässig und nur 4 % werden untersucht. Doch es kommt noch schlimmer: zwei Drittel der von Sicherheitsmitarbeitern investierten Zeit für die Reaktion auf Malware-Warnmeldungen ist aufgrund von fehlerhafter oder unvollständiger Intelligenz verschwendete Zeit. Das Thema Erkennung hat sich damit erledigt, denn sie ist teuer, zeitaufwendig, ineffektiv und in puncto Prämissen und Ausführung fehlerhaft. Es gibt eine bessere Lösung.

Mit Sure Click werden Untersuchung und Bereinigung weitgehend optimiert und reduziert. Da sich mit Sure Click geschützte Endpunkte automatisch selbst warten, wenn Benutzer die Mikro-VMs mit den darin enthaltenen schädlichen Dokumenten oder Webseiten schließen, kann das Unternehmen die manuelle Wartung auf die verbleibenden Endpunkte begrenzen, die nicht durch Sure Click geschützt sind, und dafür die von Sure Click bereitgestellten Indikatoren für Sicherheitsverletzungen heranziehen. Darüber hinaus bilden Sure Click Geräte ein umfangreiches Sensornetzwerk, das eine gesteuerte Bedrohungssuche und eine automatisierte Dateiquarantäne auf Unternehmensebene ermöglicht.

Besserer Schutz durch mehr Produktivität und Vereinfachung

Sure Click ermöglicht Regierungsbehörden und sicherheitsüberprüften Auftragnehmern aus der Industrie, das Sicherheitsniveau zu deutlich reduzierten Kosten erheblich zu verbessern – und all das auch noch einem deutlich geringeren Aufwand, da Sicherheitsverletzungen bei mit Sure Click geschützten Endpunkten nicht vorkommen und weil Dateien anhand der Sure Click Indikatoren für Angriffe und Sicherheitsverletzungen überall im Netzwerk gefunden und unter Quarantäne gestellt werden können. In diesem effektiven neuen Framework mit eingebauter Sicherheit spielen andere Verteidigungsmaßnahmen für Netzwerke und Endpunkte eher eine untergeordnete Rolle. Einige bedeutende HP Kunden sind allein durch Sure Click Enterprise und das unter neueren Windows-Betriebssystemen kostenlos vorinstallierte Microsoft Defender ausreichend geschützt, sodass Unternehmen ihre Verteidigungsmechanismen optimieren und die Komplexität der Sicherheitsvorkehrungen reduzieren können. Bromium, das jetzt Teil von HP Inc. Ist, hat die Gefahrenabwehr durch Mikrovirtualisierung seit 2010 immer weiter perfektioniert. MILLIARDEN von Mikro-VMs wurden in aktuellen Produktionsumgebungen von Kunden gestartet, ohne dass bisher Malware-Einschleusungen festgestellt wurden. Uns ist kein Anbieter von Sicherheitslösungen bekannt, der Ähnliches von sich behaupten kann.

Sprechen Sie mit Ihrem HP Security Ansprechpartner, um noch heute Anwendungsisolation und -Containment auf den Weg zu bringen.

„Bromium macht eindeutig den Unterschied in meinem Sicherheitsumfeld.“

– V.JAY LAROSA, VP, GLOBAL SECURITY ARCHITECTURE, AUTOMATIC DATA PROCESSING

HP Sure Click Enterprise

Secure Files

Wegen ihrer Effektivität werden schädliche Dokumente bei Angreifern immer beliebter. Ransomware wird üblicherweise über schädliche Bürodokumente oder PDFs eingeschleust. Secure Files isoliert auf der Hardwareebene jedes unterstützte Dokument aus dem Betriebssystem und dem Kernel. Wird ein schädliches Dokument über eine Ingress-Anwendung wie Skype, E-Mail oder USB gespeichert, wird es auf der Hardwareebene in einem Mikro-VM isoliert. Beim Schließen des Dokuments wird die Bedrohung zusammen mit der Mikro-VM beendet. Die vollständige Kill-Chain wird an die Threat Cloud gesendet und über das Sensornetzwerk an alle anderen Sure Click-Geräte weitergegeben.

Secure Monitoring

Secure Monitoring unterstützt Unternehmen beim Erkennen von persistenten Bedrohungen im Netzwerk und sorgt für entsprechende Reaktionen. Dazu werden die vom Benutzer ausgeführten Tasks auf schädliche Aktivität geprüft. Schädliche Dateien können unter Quarantäne gestellt werden und werden anhand von Einstellungen für eine Blacklist-Richtlinie automatisch an allen Orten im Netzwerk entfernt. Über das Sensornetzwerk können extrem verlässliche Benachrichtigungen an die Threat Cloud gesendet werden, wann immer ein schädliches Verhalten auf einem geschützten Host festgestellt wird. SOC-Analysten können mithilfe der Sure Click Informationen zu Bedrohungen eine schnelle Katalogisierung vornehmen und nach Indikatoren für Sicherheitsverletzungen und Angriffe suchen. Secure Monitoring unterstützt Endpunkte und Server.

Über Bromium und HP Inc.

Mit seiner revolutionären Isolationstechnologie zur Bekämpfung von Cyberangriffen hat Bromium die Endpunktsicherheit von Grund auf neu definiert. Im Gegensatz zu Antivirenprogrammen oder anderen erkennungsbasierten Verteidigungsstrategien, die moderne Angriffe nicht abwehren können, nutzt Bromium die Mikrovirtualisierung zur Verbesserung der Benutzersicherheit und ermöglicht gleichzeitig massive Kosteneinsparungen durch die fast vollständige Vermeidung von Fehlalarmen, Notfall-Patches und Problembehebungen. Das Ergebnis ist eine Transformation des traditionellen Sicherheitslebenszyklus.

Bromium Inc. und HP Inc. gingen 2016 eine formelle OEM-Beziehung ein. HP erkannte die Notwendigkeit, sein Angebot für Plattformsicherheit durch hardwarebasierte Sicherheitslösungen zu differenzieren. Ab 2017 begann HP mit dem erfolgreichen Vertrieb einer OEM-Version der Bromium Isolationslösung unter dem Markennamen Sure Click auf Millionen von Geräten der Enterprise-Klasse.

Wegen des großen Erfolgs von Sure Click hat HP am 19. September 2019 Bromium übernommen. In der Folge hat HP mit HP Security einen neuen globalen Geschäftsbereich geschaffen, der vom ehemaligen Bromium Team geleitet wird. Die Übernahme führte dazu, dass HP den Namen des Produkts Bromium Secure Platform geändert hat, damit dieser besser zur Marke HP Sure Click passt. HP setzt sich dafür ein, dass die Sure Click Lösung herstellerunabhängig auf jedem Windows 10-PC unterstützt wird. Heute ist die Legacy Bromium Secure Platform unter dem Namen HP Sure Click Enterprise bekannt.

Weitere Informationen

Weitere Informationen über die revolutionäre Sicherheitsarchitektur von Sure Click finden Sie unter **www.hp.com/proactive-security**.

4AA7-7517DEE