HP WOLF SECURITY

HP WOLF ENTERPRISE SECURITY

HP SURE CLICK ENTERPRISE

POWERED BY Bromium

NICHT ERKENNBARE BEDROHUNGEN ISOLIEREN UND VERMEIDEN

HP Sure Click Enterprise[1] stellt ein virtuelles Sicherheitsnetz für PC-Benutzer bereit, selbst wenn unbekannte Bedrohungen andere Schutzmaßnahmen umgehen können. Hardwareunterstützte Virtualisierung isoliert risikobehaftete Inhalte, um Benutzer-PCs, Daten und Anmeldeinformationen zu schützen, und macht Schadsoftware unschädlich, während die IT-Abteilung verwertbare Bedrohungsdaten erhält, um die Sicherheitslage des Unternehmens zu verbessern.

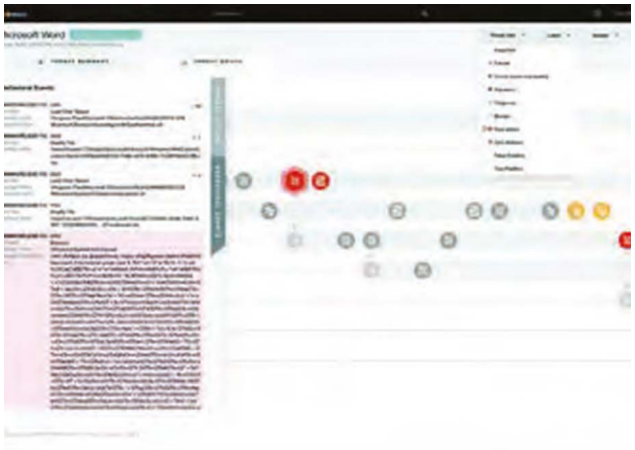
HP Sure Click Enterprise[1] blockiert Angriffe auf Endgeräte, indem mikrovirtuelle Maschinen (VMs) angelegt werden, die jede Benutzeraufgabe absichern, vom Surfen im Internet bis zum Öffnen von E-Mails und dem Herunterladen von Anhängen. Jede Aufgabe wird in der Mikro-VM vollständig isoliert. Beim Abschließen einer Aufgabe werden die Mikro-VM und die darin enthaltenen Bedrohungen entfernt, ohne dass es zu einer Sicherheitsverletzung kommt.

HP Sure Click Enterprise[1] basiert auf einzigartiger hardwaregestützter Isolationstechnologie, die hostseitig auf Virtualisierung basierende Sicherheitsfunktionen nutzt, um Bedrohungen in einzelnen löschbaren Mikro-VMs (Virtual Machines) einzuschließen. Durch diesen Ansatz wird die Angriffsfläche erheblich verkleinert, ohne dass sich für die Endbenutzer beim Zugriff auf E-Mail, Browser oder Daten etwas ändert.

RICHTLINIENBASIERTE ZUGRIFFSSTEUERUNG FÜR DIE FEINJUSTIERUNG DER SICHERHEIT

HP Sure Click Enterprise[1] bietet eine robuste Richtlinien-Engine. Administratoren können den sicheren Web- und Dateizugriff nach Benutzergruppen konfigurieren und feinkörnige Kontrollen und Standardrichtlinien für häufige Anwendungsfälle wie E-Mail-Anhänge, Phishing-Links und Downloads aus dem Internet anwenden. Die mehrstufigen Richtlinien sind einfach zu definieren und lassen sich genau auf Ihre individuellen Sicherheitsherausforderungen und Risikoprofile abstimmen.

HAUPTVORTEILE



SICHERER ZUGRIFF AUF EINGEHENDE DATEIEN

Öffnen Sie jede Datei und jedes Dokument ohne Infektionsrisiko, ganz gleich, ob diese aus dem Internet heruntergeladen, als E-Mail-Anhang empfangen oder auf tragbaren USB-Laufwerken gespeichert sind.

MALWARE-ABWEHR

Mikro-VMs isolieren schädliche Aktivität und halten diese in Schach. Die Malware verschwindet beim Schließen der Datei oder des Dokuments.

ANMELDEDATEN VOR PHISHING SCHÜTZEN

Sure Click Enterprise blockiert die Eingabe von Anmeldedaten auf bekannten böswilligen Websites und warnt die Benutzer vor potenziell riskantem Verhalten auf allen Websites mit niedriger Reputation.

VERSTÄRKUNG IHRER GESAMTEN DEFENSIVEN INFRASTRUKTUR

Sure Click-Indikatoren für Angriffe und Sicherheitsverletzungen helfen dabei, Dateien in Quarantäne zu verschieben und nach Malware auf Servern und auf Geräten ohne Sure Click zu suchen, auf denen Tools von Drittanbietern zum Einsatz kommen.

THREAT INTELLIGENCE

Jedes Sure Click Endgerät und jeder Server ist Teil eines ständig adaptiven Sensornetzwerks, das für Malware-Analysen und die schnelle Weitergabe von Bedrohungsindikatoren verwendet werden kann. Sicherheitsteams erhalten Informationen zu Bedrohungen und führen Kill Chain-Analysen durch, um Bedrohungen leichter auf die Spur zu kommen, Informationen im gesamten Unternehmen bereitzustellen und Probleme schnell zu lösen.

HAUPTMERKMALE

UMFASSENDER MALWARE-SCHUTZ MIT HARDWAREGESTÜTZTER ISOLATION

Isolation von eingehenden Dateien und Webinhalten vom Host-PC und aus dem internen Netzwerk mithilfe einer umfassenden Bedrohungsforensik auf der Grundlage von fortschrittlichen Techniken der Verhaltensanalyse, um schädliche Aktivitäten zu erkennen.

THREAT INTELLIGENCE

Durch die Isolation von Malware werden SOC-Analysten über Sicherheitsbedrohungen benachrichtigt und Feeds mit Informationen zu Bedrohungen an Drittsysteme gesendet, um die defensive Infrastruktur zu verstärken.

SCHNELLER SCHUTZ VOR WESENTLICHEN ANGRIFFSVEKTOREN

Sofortschutz vor wesentlichen Angriffsvektoren wie E-Mail-Anhängen, Phishing-Links und Datei-Downloads ohne Durcharbeiten von komplexen Konfigurationseinstellungen.

BEDROHUNGSPRIORISIERUNG DURCH KONTEXTBEZOGENE INTELLIGENZ

Workflow-basierte Bedrohungspriorisierung mit erweiterter Threat Intelligence ermöglicht Analysten die schnelle Erkennung von wahr-positiven Ergebnissen für die Entwicklung proaktiver Lösungen für Systeme mit und ohne Sure Click-Schutz.

DASHBOARDS MIT PRAXISRELEVANTEN INFORMATIONEN, BERICHTEN UND DRILLDOWN-FUNKTIONEN

Machen Sie den Nutzen von Sure Click in Form von Kurzübersichten für sich und andere transparent – durch CISO/CIO-Berichte, ein Betriebs-Dashboard für das Desktop-Team und ein Bedrohungs-Dashboard für Ihr Sicherheitsteam.

HP SURE CLICK ENTERPRISE[1] BESTEHT AUS DEN FOLGENDEN KOMPONENTEN:

SECURE BROWSING, SECURE FILES UND THREAT INTELLIGENCE & REPORTING

SECURE BROWSING

BENUTZERORIENTIERTES SICHERES SURFEN IM INTERNET

Beim Secure Browsing werden Bedrohungen aus dem Web und Browser-Exploits mithilfe von hardwaregestützten Mikro-VMs isoliert, sodass Sie nicht auf Erkennungstechnologie oder restriktive schwarze Listen für Websites angewiesen sind.

Jeder Browser-Tab wird vollständig von allen anderen Tabs, dem Host-PC und dem internen Netzwerk isoliert. Secure Browsing spielt sich in einem geschützten Mikro-VM ab, was die ungehinderte Ausführung von vertraulichen Dateien und Prozessen in Isolation ermöglicht. Benutzer können nativ sichere Websites in Chrome, Firefox oder Edge aufrufen, wobei zum Öffnen von risikobehafteten und unkategorisierten Websites sowie verdächtigen Phishing-Links automatisch auf isoliertes Browsing im Sure Click Secure Browser umgestellt wird.

BEDROHUNGEN AUS DEM INTERNET – NEUTRALISIERT

Die gesamte Website-Aktivität wird im sicheren Container der Mikro-VM separiert. Die Mikro-VM und alle darin enthaltenen Bedrohungen werden beim Schließen des Browser-Tab vernichtet, und ein ausführlicher Bedrohungsbericht dient als forensischer Nachweis der gesamten schädlichen Aktivität. Der Schutz vor Bedrohungen aus dem Internet erstreckt sich auf bekannte und unbekannte Sicherheitslücken wie Zero-Day-Exploits bei Browsern, schädliches webseitenübergreifendes Skripting und dateilose Malware, die Schwachstellen im Arbeitsspeicher oder andere Schwächen von Windows ausnutzt. Notfall-Patches und Versionsüberprüfungen sind weniger dringend, weil Secure Browsing sogar ungepatchte Systeme für alle Benutzer sicher macht.

SECURE FILES

SICHERER DOWNLOAD VON UND ZUGRIFF AUF EINGEHENDE DATEIEN

Secure Files nutzt hardwaregestützte Mikro-Virtualisierung zum Isolieren von schädlichen Bedrohungen, die in eingehenden Dateien und Dokumenten wie E-Mail-Anhängen, Web-Downloads und USB-Dateien verborgen sind.

Jede Datei wird reibungslos in einer geschützten Mikro-VM geöffnet. Der Prozess ist für den Benutzer transparent und die Dateien sind vollständig von anderen Dateien und Prozessen abgesondert und isoliert. Secure Files funktioniert online und offline, sodass Benutzer ihre Dokumente und Dateien sicher speichern, ändern und umbenennen können.

DATEI- UND DOKUMENTBEDROHUNGEN BLEIBEN ABGEKAPSELT

Wenn eine Datei schädlich ist, bleibt die gesamte Aktivität im sicheren Container isoliert, und sämtliche Bedrohungen werden mit dem Schließen der Datei beseitigt. Dieser Schutz erstreckt sich auf bekannte und unbekannte Sicherheitslücken wie Zero-Day-Exploits, schädliche Makros, Skripte und hochentwickelte Angriffstechniken, die Kernel-Bugs im Arbeitsspeicher oder andere Schwächen von Windows ausnutzen.

ZUGANGSDATENSCHUTZ:

BENUTZER VOR DER PREISGABE VON ANMELDEDATEN WARNEN UND SPERREN

Wenn ein Benutzer eine Website besucht und zur Eingabe von Zugangsdaten aufgefordert wird, nutzt Sure Click Enterprise den HP Threat Intelligence Service zur Durchführung einer Reputations- und Domain-Analyse im Hintergrund, mit der die Sicherheit der Website bestimmt wird. Bei legitimen, bekanntermaßen sicheren Websites werden keine Maßnahmen ergriffen, während Benutzer für die Eingabe von Kennwörtern auf bekannten böswilligen Websites gesperrt werden und für Websites mit niedriger Reputation eine Warnmeldung erhalten.

SO KÖNNEN BENUTZER UNBESORGT BROWSEN

Bei Websites mit niedriger Reputation können Administratoren den Benutzern die Freiheit geben, fortzufahren. Dadurch wird die Website auf dem PC des Benutzers auf eine Whitelist gesetzt und unnötige Produktivitätseinschränkungen bei zukünftigen Besuchen werden verhindert. Selbst für böswillige Websites kann die Software dahingehend konfiguriert werden, dass der Benutzer die Website mit deaktivierten Datenerfassungsfeldern anzeigen kann. Alle Aktionen auf bekanntermaßen böswilligen und unseriösen Websites werden aufgezeichnet und an den Sure Click Controller gemeldet, damit die IT-Abteilung den Status der Bedrohung und des Benutzerverhaltens überprüfen kann.

RISIKOREICHE BENUTZERAKTIVITÄTEN WERDEN IN EINER MIKRO-VM ISOLIERT

MIKRO-VMs HABEN KEINEN ZUGRIFF AUF DEN HOST, DIE EINSTELLUNGEN ODER DAS INTERNET

MIKRO-VMs ENTHALTEN KEINE PERSONENBEZOGENEN DATEN

THREAT INTELLIGENCE & REPORTING

INTELLIGENTE BERICHTSFUNKTIONEN UND ANALYSEN

Sure Click Enterprise[1] generiert Echtzeit-Benachrichtigungen mit umfassender forensischer Intelligenz für jeden Angriff und bietet Sicherheitsteams Echtzeit-Transparenz für Endgeräte.

Die Sure Click Enterprise[1] Endgeräteanwendung und der zentrale Controller bilden ein ständig adaptives Sensornetzwerk für Malware-Analysen und die schnelle Weitergabe von Bedrohungsindikatoren. Der zentrale HP Sure Click Enterprise Controller verwaltet unternehmensweit geltende Richtlinien und sammelt in Echtzeit Angriffsdaten von Endgeräten für unübertroffene forensische Analysen und die Bereitstellung von Telemetriedaten zu Bedrohungen. Sicherheitsteams erhalten in Echtzeit Benachrichtigungen und führen Kill-Chain-Analysen durch, um Bedrohungen schneller zu erkennen, sodass eine unternehmensweite Transparenz und Kontrolle sichergestellt ist.

SOC-Teams profitieren von umfassender Sicherheitstransparenz, wenn Sure Click Enterprise auf Windows-Endgeräten und -Servern im Unternehmen implementiert wird. Das Echtzeit-Streaming von Angriffsdaten in Kombination mit Analysen von Anwendungs-Workflows verschafft SOC-Analysten eine vollständige integrierte Übersicht über den Angriff. Tausende von Low-Level-Überwachungsereignissen werden in Echtzeit am Endgerät oder Server korreliert, wodurch zeitaufwendige manuelle Analysen oder teure Backend-Rechenzentren überflüssig werden.

Die Rohdaten werden in höhere Intelligenz transformiert, damit gewährleistet ist, dass die Sicherheitsteams stets in Echtzeit über die allgemeine Bedrohungslage informiert bleiben. Sie müssen nicht länger Geld und Ressourcen für Fehlalarme, Problembehandlungen, Rebuilds oder Notfall-Patches aufwenden.

MIT HP SURE CLICK ENTERPRISE[1] SCHÜTZEN SIE SICH GEGEN IHRE ANFÄLLIGSTEN ANGRIFFSVEKTOREN

E-MAIL-ANHÄNGE

• Ransomware • Makro-fähiger Trojaner • Dateilose Malware • Schädliche Links

PHISHING-LINKS

• Schädliche Links in E-Mail-Text und -Anhängen • Browser-Exploits • Gefälschte Flash/Java-Updates
• Drive-by-Downloads • Watering-Hole-Angriffe • Malvertising • Links in Chat-Programmen

DOWNLOADS UND AUSFÜHRBARE DATEIEN

• Absichtliche Downloads • Gefälschte ausführbare Updates • Links zu Dokumenten
• Falsche DNS/URL-Umleitungen • Falsche Treiber und Dienstprogramme • Watering-Hole-Angriffe

IDENTITÄTSSCHUTZ

• Phishing von Zugangsdaten • Extraktion von lokalen und Domain-Anmeldeinformationen • Unbefugte Wiederverwendung von Anmeldeinformationen

UNGESCHÜTZTE NETZWERKE

• Browser-Exploits • Dateilose Malware • Drive-by-Downloads
• Falsche DNS/URL-Umleitungen • Fake-Updates (z. B. Reader, Flash und Java)

UNKATEGORISIERTE WEBSITES

• Browser-Exploits • Dateilose Malware • Verschlüsselte Downloads, die sich der Erkennung entziehen

INHALTE AUF USB-MEDIEN

• Büroproduktivitätsdateien • Multimediadateien
• Ausführbare Dateien • Dokument-Links • Web-Lesezeichen

NULL SICHERHEITSVERLETZUNGEN BEI MIKRO-VMs

(von Kunden gemeldet)

Implementieren Sie die HP Sure Click Enterprise Secure-Plattform, um ins Visier genommene Benutzer-Angriffsvektoren zu schützen oder um alle Funktionen für echte Hochsicherheit zu aktivieren.

Weitere Informationen finden Sie unter **https://www.hp.com/enterprisesecurity**

1. HP Sure Click Enterprise ist separat erhältlich und erfordert Windows 8 oder Windows 10. Microsoft Internet Explorer, Google Chrome, Chromium und Firefox werden unterstützt. Zu den unterstützten Anhängen gehören u. a. Microsoft Office (Word, Excel, PowerPoint) und PDF-Dateien, wenn Microsoft Office bzw. Adobe Acrobat installiert ist.

4AA7-7470DEE, April 2021, Rev. 2

HP WOLF SECURITY