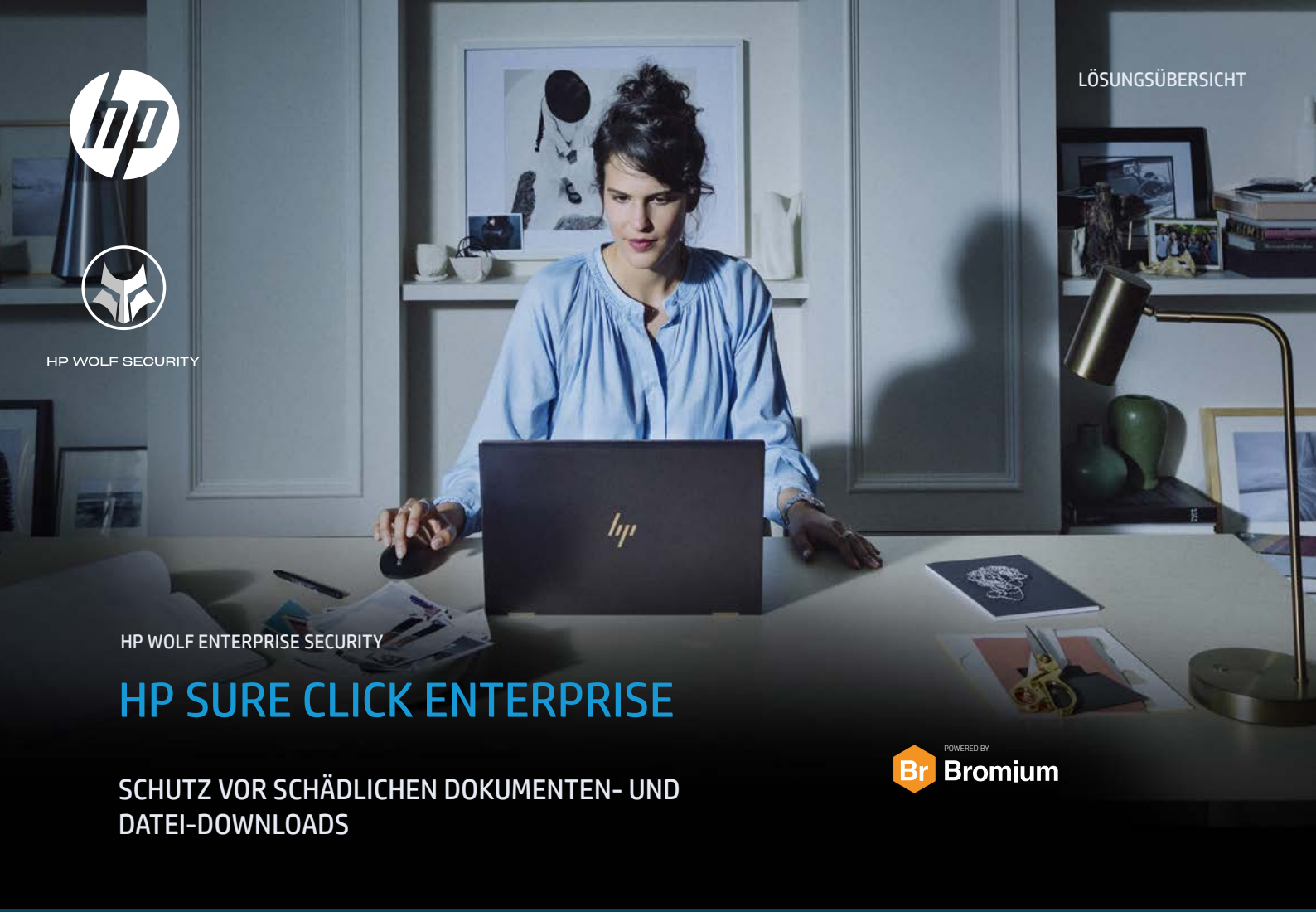

LÖSUNGSÜBERSICHT

HP WOLF SECURITY

HP WOLF ENTERPRISE SECURITY

HP SURE CLICK ENTERPRISE

SCHUTZ VOR SCHÄDLICHEN DOKUMENTEN- UND DATEI-DOWNLOADS

POWERED BY Bromium

SICHERES HERUNTERLADEN UND ÖFFNEN VON DOKUMENTEN ODER AUSFÜHRBAREN DATEIEN VON UNBEKANNTEN ODER NICHT KATEGORISIERTEN WEBSITES

SCHUTZ VOR SCHÄDLICHEN DOWNLOADS DURCH VERIFIZIERTE NATIVE ANWENDUNGSLEISTUNG UND EINE BENUTZERFREUNDLICHE LÖSUNG

VERMEIDEN RESTRIKTIVER IT-SICHERHEITSRICHTLINIEN, DIE DEN ZUGRIFF AUF HERUNTERGELADENE DATEIEN EINSCHRÄNKEN UND ABLÄUFE BEHINDERN

ANGRIFFE LAUERN ÜBERALL: SCHÄDLICHE DOWNLOADS STAMMEN AUS VIELEN QUELLEN

Um ihre Arbeit erledigen zu können, müssen Benutzer in der Lage sein, Dateien aus externen Quellen herunterzuladen. Viele Menschen neigen dazu, schnell auf geteilte Dokumente zu klicken – durchschnittlich in weniger als vier Minuten, nachdem sie sie erhalten haben. Schädliche Downloads gelangen auf unterschiedlichsten Wegen ins Unternehmen. Einige Beispiele:

- Surfen im Internet
- Klicken auf geteilte Links
- Installieren von Programmen
- Initiieren von FTP-Dateiübertragungen

Böswillige Downloads sind besonders effektiv, weil es so viele kurzlebige und böswillige Websites mit Inhalten gibt, die sich häufig ändern, um eine genaue Kategorisierung zu vermeiden. Sie nutzen einzigartige und polymorphe Malware, die sich allen herkömmlichen Erkennungsmethoden entzieht.

Die Verteilung von Malware per Datei-Download ist effizient, kostengünstig und entwickelt sich ständig weiter. Sie kann viele Formen annehmen:

- **Absichtliche Downloads:** Der Benutzer initiiert den Download eines Dokuments oder einer ausführbaren Datei während des normalen Surfens im Internet.
- **Gefälschte ausführbare Updates:** Der Benutzer wird beim Besuch einer Website dazu verleitet, eine böswillige Datei herunterzuladen.
- **Links zu Dokumenten**: Der Benutzer erhält in einer E-Mail oder einem Chatprogramm einen Dokumentenlink und wird zum Herunterladen eines Dokuments aufgefordert, das Malware enthält.
- **URL-Umleitungen:** Der anfängliche Link leitet den Benutzer zu einer alternativen URL um, die zum Herunterladen einer Datei auffordert.
- **DNS-Angriffe**: Wenn der DNS-Sucheintrag kompromittiert ist, lädt der Benutzer eine schädliche Datei herunter, auch wenn er nichts falsch gemacht hat.
- **Gefälschte Treiber und Dienstprogramme:** Der Benutzer wird auf eine „inoffizielle“ Download-Seite geleitet und installiert versehentlich Malware.
- **Watering-Hole-Angriffe:** Der Angreifer infiziert eine vom Opfer häufig genutzte Website und ersetzt Datei-Downloads oder leitet diese um.

HP SURE CLICK ENTERPRISE, POWERED BY BROMIUM, SETZT AUF ANWENDUNGSISOLIERUNG, UM ORGANISATIONEN VOR SCHÄDLICHEN DOWNLOADS ZU SCHÜTZEN

HP Sure Click Enterprise[3] 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.

Bei der hardwaregestützten Isolierung wird jedes heruntergeladene Dokument und jede heruntergeladene ausführbare Datei in einem eigenen sicheren Container ausgeführt. Über Datei-Downloads eingeschleuste Bedrohungen werden vollständig vom Host und von allen anderen Anwendungen isoliert, um eine Kreuzkontamination zu verhindern. Beim Schließen der Anwendung bzw. der Datei wird die Bedrohung zusammen mit der Mikro-VM beendet. Die vollständige Malware-Angriffskette wird mit allen anderen HP Sure Click Enterprise-Geräten im Netzwerk geteilt. Das sichert die Infrastruktur zusätzlich ab und verkleinert die gesamte Angriffsfläche.

ANWENDUNGSISOLIERUNG: SCHUTZ BEREITS VOR DER ERKENNUNG

ALLE WEB-DOWNLOADS AUTOMATISCH SCHÜTZEN

Sie können jedes heruntergeladene Dokument oder jede heruntergeladene ausführbare Datei unabhängig von der Quelle (HTTP/HTTPS, FTP usw.) sicher öffnen. Dank der Isolierung innerhalb der geschützten Mikro-VM können die Benutzer ihre Dateien sicher herunterladen und darauf zugreifen, wobei die vertraute Benutzeroberfläche erhalten bleibt.

IT-SICHERHEIT OPTIMIEREN UND KOSTEN SENKEN

Durch die High-Fidelity-Warnungen von HP Sure Click Enterprise können Sie die Selektierungszeit drastisch verkürzen und dafür sorgen, dass aufgrund falsch-positiver Ergebnisse keine Ressourcen mehr verschwendet werden. Sie vermeiden Reimaging, Rebuilds und Notfallkorrekturen.

INFORMATIONEN ZU SICHERHEITSBEDROHUNGEN IN ECHTZEIT TEILEN

Adaptive Intelligenz identifiziert und stoppt ausweichende Angriffe, teilt Echtzeit-Risikodaten über Ihr Netzwerk und bietet eine vollständige Angriffskettenanalyse (Kill Chain Analysis) für Ihr SOC.

DAUERHAFTEN SCHUTZ MIT HARDWAREGESTÜTZTER SICHERHEIT ERZIELEN

Nur HP Sure Click Enterprise nutzt virtualisierungsbasierte Sicherheit zum Erzielen einer hardwaregestützten Anwendungsisolierung Unsere Lösung schützt Sie sogar vor bisher unbekannten Bedrohungen und polymorpher Malware, die selbst durch fortschrittlichste Erkennungstools schlüpfen können.

38 % DER MALWARE WERDEN MITTLERWEILE ALS WORD-DOKUMENTE GETARNT.[1]

- Safety Detectives

IM JAHR 2020 KONNTEN PHISHING-SEITEN EINEN ANSTIEG VON MEHR ALS 750 % GEGENÜBER 2007 VERZEICHNEN.[2]

- Comparitech 2021

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

1. 15 (CRAZY) Malware and Virus Statistics, Trends & Facts (safetydetectives.com)
2. Malware Statistics in 2021: Frequency, impact, cost & more (comparitech.com)
3. 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.

4AA7-7469DEE, April 2021, Rev. 2

HP WOLF SECURITY