HP WOLF SECURITY

HP Sure Click Enterprise:

sicurezza zero-trust a livello di endpoint.

Per impostazione predefinita, la tecnologia di contenimento delle minacce nega l'accesso alle applicazioni più rischiose.

Che cos'è la sicurezza zero-trust

Le strategie zero-trust per la sicurezza della rete non consentono ad alcun utente o dispositivo di accedere alla rete finché la sua identità e le sue autorizzazioni non vengono verificate. Tutto quello che si connette alla rete viene considerato intrinsecamente non sicuro e potenzialmente pericoloso, pertanto la strategia richiede continuamente prove di sicurezza e autenticazione. Questo modello di sicurezza è stato adottato come best practice dalle aziende e dalle agenzie federali[1] statunitensi.

L'endpoint: il punto debole della strategia zero-trust

Nonostante il tempo, l'impegno e gli investimenti dedicati alla sicurezza zero-trust della rete, gli endpoint costituiscono ancora un punto debole. Indotti con l'inganno a interagire con contenuti nocivi espressamente progettati per eludere gli antivirus e le altre soluzioni di sicurezza, gli utenti permettono al malware di accedere ai loro dispositivi. Di fronte ad attacchi alla sicurezza informatica che diventano sempre più sofisticati, all'aumento dei costi delle violazioni dei dati e alla contrazione dei budget per la sicurezza IT, si impone l'adozione di un nuovo approccio alla sicurezza zero-trust degli endpoint.

Sicurezza zero-trust degli endpoint

HP Sure Click Enterprise adotta un approccio zero-trust alla sicurezza, presupponendo che tutti i contenuti siano potenzialmente pericolosi. In questo modo, anche se una minaccia riesce a eludere le altre misure di sicurezza (come gli antivirus e le soluzioni EDR), viene catturata e resa inoffensiva dalla tecnologia HP di isolamento, prima di poter causare qualsiasi danno.

- Il 69% delle minacce identificate dal software HP per l'isolamento delle minacce proviene dai messaggi e-mail.[2]

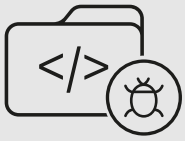
- Il 14% del malware ha eluso l'antivirus e le altre applicazioni tradizionali per la sicurezza dell'e-mail.[2]

SURE CLICK

Sure Click Enterprise[3] previene le infezioni degli endpoint, creando micro-macchine virtuali[4] (micro-VM) che proteggono le attività ad alto rischio dell'utente, come l'esplorazione del web, l'apertura dei messaggi e-mail e il download degli allegati.

La tecnologia HP per l'isolamento delle minacce isola ogni singola operazione potenzialmente rischiosa in una micro-VM dedicata, per impedirle di infettare il PC. Al termine dell'attività, la micro-VM e tutte le eventuali minacce che contiene vengono distrutte, eliminando all'istante il pericolo di una violazione. Questo approccio riduce drasticamente la superficie di attacco, senza costringere gli utenti finali a cambiare il modo di utilizzare l'e-mail, il browser o i dati. La protezione interagisce in modo trasparente con tutti i prodotti di sicurezza in uso, integrando gli investimenti attuali al fine di estendere la sicurezza zero-trust agli endpoint.

PRINCIPALI CARATTERISTICHE



SICUREZZA ZERO-TRUST BASATA SULL'ISOLAMENTO

L'isolamento garantisce un approccio zero-trust reale, perché tutto il contenuto viene racchiuso nelle micro-macchine virtuali, indipendentemente dal tipo o dal vettore di attacco.

THREAT INTELLIGENCE IN TEMPO REALE

Una volta isolato, il malware genera avvisi sulle minacce per gli analisti SOC e invia feed sulle minacce ai sistemi esterni, per contribuire a potenziare l'infrastruttura difensiva.

PROTEZIONE SUPERIORE DAI VETTORI DI ATTACCO

Protezione predefinita dai principali vettori di attacco, come allegati e-mail, collegamenti di phishing e download di file, senza richiedere complicate impostazioni di configurazione.

TRIAGE DELLE MINACCE BASATO SUL FLUSSO DI LAVORO

Potenzia la Threat Intelligence e consente agli analisti di accelerare l'identificazione dei veri positivi, affinché possano intervenire in modo proattivo sia sui sistemi protetti da Sure Click sia su quelli non coperti dal servizio.

GENERAZONE DI REPORT E INTEGRAZIONI

Gestione e conservazione dei dati on-premise o nel cloud. I report sintetici per i dirigenti (CISO/CIO) permettono di verificare e condividere facilmente il valore di Sure Click. Integrazione tramite API con gli strumenti e i processi SOC in uso.

Riepilogo

Altre risorse disponibili per ulteriori informazioni sul modo in cui HP promuove l'innovazione per la sicurezza:

Pagina delle risorse HP dedicate alla sicurezza | Sicurezza per un ambiente di lavoro ibrido | Case study su Masonicare

[1] Executive Order on Improving the Nation's Cybersecurity. Per informazioni dettagliate, visitare il sito Executive Order on Improving the Nation's Cybersecurity | The White House.
[2] Report HP sulle minacce, secondo trimestre 2022
[3] HP Sure Click Enterprise è in vendita separatamente. Gli allegati supportati includono Microsoft Office (Word, Excel, PowerPoint) e i file PDF, se sono installati Microsoft Office o Adobe Acrobat. Per i requisiti di sistema completi, visitare il sito System Requirements for HP Sure Click Enterprise, che contiene informazioni dettagliate.
[4] Definizione di micro-macchina virtuale (o micro-VM)

© Copyright 2023 HP Development Company, L.P. Le informazioni qui contenute possono subire variazioni senza preavviso. Le uniche garanzie sui prodotti e sui servizi HP sono esposte nelle dichiarazioni di garanzia esplicita che accompagnano i suddetti prodotti e servizi. Nulla di quanto qui contenuto può essere interpretato come garanzia aggiuntiva. HP declina ogni responsabilità per errori tecnici o editoriali od omissioni qui contenuti. Microsoft e Windows sono marchi di fabbrica o marchi registrati di Microsoft Corporation negli Stati Uniti e/o in altri Paesi. Intel e Core sono marchi o marchi registrati di Intel Corporation o di società controllate da Intel negli Stati Uniti e/o in altri Paesi.

4AA8-2318ITE, maggio 2023