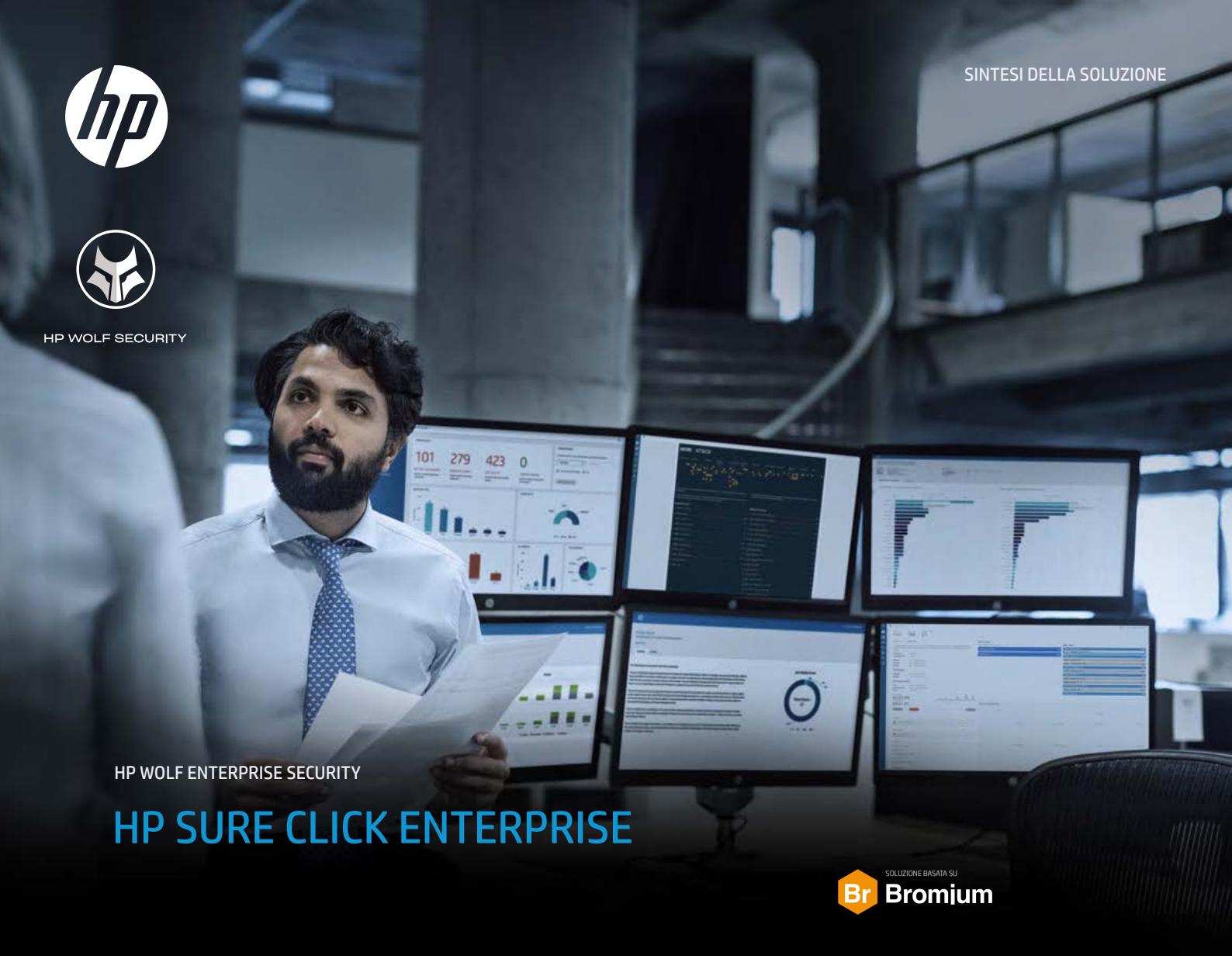
HP WOLF SECURITY



HP WOLF ENTERPRISE SECURITY

HP SURE CLICK ENTERPRISE

SOLUZIONE BASATA SU Bromium

ISOLAMENTO E PREVENZIONE DELLE MINACCE NON RILEVABILI

HP Sure Click Enterprise[1] offre una rete di sicurezza virtuale agli utenti dei PC, persino quando le minacce sconosciute riescono a superare altre difese. La virtualizzazione basata su hardware isola i contenuti ad alto rischio per proteggere il PC, i dati e le credenziali dell'utente rendendo inoffensivi i malware, mentre il personale IT ottiene una threat intelligence utile ad aumentare ulteriormente il livello di sicurezza dell'organizzazione.

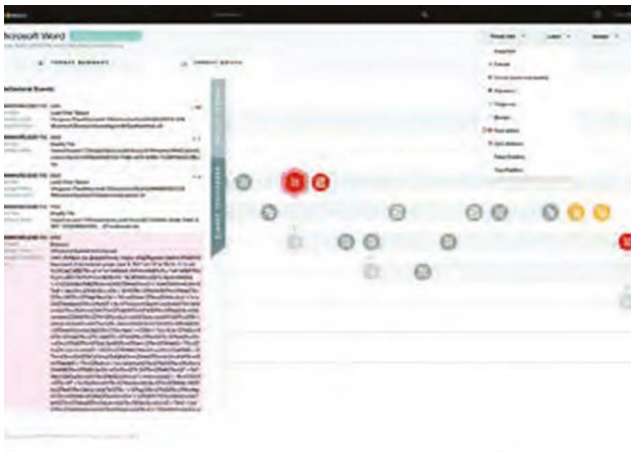
HP Sure Click Enterprise[1] impedisce gli attacchi agli endpoint creando micro-macchine virtuali (VM) che proteggono ogni attività dell'utente, dalla navigazione sul web all'apertura delle e-mail e al download degli allegati. Ogni attività viene completamente isolata all'interno della micro-VM. Al termine dell'attività, la micro-VM viene distrutta insieme a tutte le minacce che contiene, senza che avvenga alcuna violazione.

HP Sure Click Enterprise[1] sfrutta un'esclusiva tecnologia di isolamento basata su hardware, che utilizza la sicurezza basata sulla virtualizzazione nell'host per contenere le minacce all'interno di singole micro-macchine virtuali monouso. Questo approccio riduce drasticamente la superficie di attacco senza apportare alcun cambiamento alle modalità con cui gli utenti finali accedono a e-mail, browser o dati.

ACCESSO BASATO SU POLICY PER OTTIMIZZARE LA SICUREZZA

HP Sure Click Enterprise[1] include un affidabile motore di policy. Gli amministratori possono configurare l'accesso sicuro a file e al web per i diversi gruppi di utenti, con controlli accurati e policy predefinite per gli scenari di utilizzo più comuni, come gli allegati e-mail, i collegamenti di phishing e il download di file dal Web. È possibile impostare facilmente policy multilivello ottimizzabili in base ai profili di rischio e alle problematiche di sicurezza specifiche della vostra azienda.

VANTAGGI PRINCIPALI



ACCESSO SICURO AI FILE DA FONTI IN ENTRATA

È possibile aprire qualsiasi file o documento scaricato dal web, ricevuto per e-mail o salvato in un'unità USB portatile senza rischio di infettare PC o rete.

FINE ALLA MINACCIA DEI MALWARE

Le micro-VM permettono di isolare e contenere le attività dannose, eliminando i malware alla chiusura dei file o documenti.

PROTEZIONE DELLE CREDENZIALI DAGLI ATTACCHI DI PHISHING

Sure Click Enterprise impedisce agli utenti di inserire le credenziali di accesso in siti web dannosi noti, e segnala i potenziali comportamenti rischiosi in tutti i siti di scarsa reputazione.

HARDENING DELL'INTERA INFRASTRUTTURA DIFENSIVA

Utilizzando gli indicatori di attacco e compromissione di Sure Click, è possibile mettere in quarantena i file e cercare il malware nascosto nei server o nei dispositivi non protetti da Sure Click tramite strumenti di terze parti.

THREAT INTELLIGENCE

Ogni server ed endpoint Sure Click fa parte di una rete continua di sensori adattivi che può essere utilizzata per l'analisi dei malware e la condivisione istantanea degli indicatori di minaccia. I team di sicurezza ricevono la threat intelligence ed eseguono un'analisi completa delle strategie di attacco, che semplifica l'identificazione delle minacce, la condivisione delle informazioni all'interno dell'azienda e la risoluzione rapida dei problemi.

PRINCIPALI CARATTERISTICHE

PROTEZIONE DAI MALWARE PIÙ RESISTENTI GRAZIE ALL'ISOLAMENTO BASATO SU HARDWARE

I file e i contenuti web in entrata vengono isolati dal PC host e dalla rete interna utilizzando dettagliate informazioni forensi ottenute tramite avanzate tecniche di analisi comportamentale per identificare le attività dannose.

THREAT INTELLIGENCE

Un malware isolato genera avvisi sulle minacce per gli analisti SOC e invia i relativi feedback a sistemi terzi per contribuire a rinforzare l'infrastruttura difensiva.

PROTEZIONE RAPIDA DAI PRINCIPALI VETTORI DI ATTACCO

Protezione immediata dai principali vettori di attacco, come allegati e-mail, collegamenti di phishing e download di file, senza che siano necessarie complesse impostazioni di configurazione.

TRIAGE PER LE MINACCE GRAZIE ALL'INTELLIGENCE SUL CONTESTO

Triage per le minacce basato su flussi di lavoro, con threat intelligence avanzata, rapida identificazione delle minacce effettive da parte degli analisti per la risoluzione ed eliminazione proattiva sia nei sistemi Sure Click che in quelli diversi.

DASHBOARD, REPORT E DRILL-DOWN FRUIBILI

È possibile visualizzare e condividere facilmente i vantaggi di Sure Click grazie ai report riassuntivi per i dirigenti (CISO/CIO), un dashboard operativo per il team desktop e un dashboard dedicato alle minacce per il vostro team di sicurezza.

HP SURE CLICK ENTERPRISE[1] CONSISTE NEI SEGUENTI COMPONENTI:

NAVIGAZIONE SICURA, FILE SICURI, PROTEZIONE DELLE CREDENZIALI, THREAT INTELLIGENCE E REPORT

NAVIGAZIONE SICURA

NAVIGAZIONE WEB SICURA E INCENTRATA SULL'UTENTE

La funzionalità di navigazione sicura isola le minacce provenienti dal Web e gli exploit del browser, utilizzando micro-VM basate hardware in modo che non sia necessario ricorrere a strumenti di rilevamento o blacklist di siti web restrittive.

Ogni scheda del browser è isolata da tutte le altre, dal PC host e dalla rete interna. La navigazione sicura si svolge all'interno di una micro-VM protetta, che consente di completare le attività senza alcuna limitazione in modo isolato dai file e dai processi sensibili. È disponibile l'esperienza di navigazione nativa di Chrome, Firefox o Edge per i siti sicuri, così come il trasferimento alla navigazione isolata sul browser Sure Click Secure per siti rischiosi (inclusi i presunti collegamenti di phishing e i siti web non classificati).

NEUTRALIZZAZIONE DELLE MINACCE WEB

Tutte le attività nei siti web vengono isolate nei container delle micro-VM sicure. La micro-VM e tutte le eventuali minacce vengono distrutte alla chiusura della scheda del browser; nello stesso momento viene generato un report dettagliato sulle minacce, che può essere utilizzato come traccia forense di tutte le attività dannose. La protezione Web si estende a tutte le vulnerabilità note e sconosciute, inclusi gli exploit zero-day del browser, il cross-site scripting dannoso e i malware fileless che sfruttano i punti debolezza della memoria o di Windows. L'applicazione di patch di emergenza e il controllo delle versioni diventano meno urgenti, dal momento che Secure Browsing rende persino i sistemi privi di patch sicuri per tutti gli utenti.

FILE SICURI

DOWNLOAD E ACCESSO SICURI AI FILE IN ENTRATA

La funzionalità per i file sicuri si avvale della micro-virtualizzazione basata su hardware per isolare le minacce nascoste all'interno dei file e dei documenti in entrata, inclusi allegati e-mail, download dal web e file sulle unità USB.

Ciascun file viene aperto con semplicità all'interno di una micro-VM protetta. Il processo, in cui i file vengono completamente contenuti e isolati da altri file e processi, avviene con chiarezza agli occhi dell'utente. La funzionalità per i file sicuri è utilizzabile sia online che offline, il che consente agli utenti di stampare, salvare, modificare e rinominare documenti e file in tutta sicurezza.

MINACCE CONTENUTE IN FILE E DOCUMENTI RESTANO IN ISOLAMENTO

In caso di file dannosi, tutte le attività rimangono isolate all'interno di un container sicuro e le eventuali minacce vengono distrutte alla chiusura del file. Questa protezione vale sia le vulnerabilità note che quelle sconosciute, inclusi gli exploit zero-day, le macro dannose, gli script e le tecniche di attacco avanzate che sfruttano i bug del kernel di memoria o le altre lacune di Windows.

PROTEZIONE DELLE CREDENZIALI

AVVISA GLI UTENTI E IMPEDISCE LORO DI CONDIVIDERE LE CREDENZIALI

Quando un utente visita un sito Web che richiede l'immissione di credenziali di accesso, Sure Click Enterprise utilizza HP Threat Intelligence Service per eseguire un'analisi in background su reputazione e dominio del sito, al fine di determinarne la sicurezza. In caso di siti sicuri e legittimi non viene adottata alcuna misura; in caso di siti dannosi noti, agli utenti sarà impedito di inserire le password, mentre con i siti di scarsa reputazione riceveranno un avviso.

NAVIGAZIONE SENZA PREOCCUPAZIONI

Gli amministratori possono consentire agli utenti di procedere con la navigazione sui siti di scarsa reputazione; in questo modo, tali siti saranno aggiunti alla whitelist del PC dell'utente, così che la produttività non subisca rallentamenti durante le sessioni future. Anche i siti dannosi possono essere configurati in modo da essere visibili all'utente, ma disattivando tutti i campi di acquisizione di dati. Tutte le misure relative ai siti dannosi noti e di dubbia reputazione vengono registrate e segnalate a Sure Click Controller, per consentire al personale IT di esaminare lo stato delle minacce e il comportamento degli utenti.

LE ATTIVITÀ RISCHIOSE DELL'UTENTE VENGONO ISOLATE IN UNA MICRO-VM

LE MICRO-VM NON HANNO ACCESSO ALL'HOST, ALLE IMPOSTAZIONI O A INTERNET

LE MICRO-VM NON CONTENGONO DATI PERSONALI

THREAT INTELLIGENCE E REPORT

REPORT E ANALISI INTELLIGENTI

Sure Click Enterprise[1] genera avvisi in tempo reale con intelligence forense completa per ogni attacco, offrendo ai team di sicurezza visibilità degli endpoint in tempo reale.

Il controller centrale e l'applicazione endpoint di Sure Click Enterprise[1] formano una rete continua di sensori adattivi per l'analisi dei malware e la condivisione istantanea degli indicatori di minaccia. Il controller centrale di HP Sure Click Enterprise gestisce le policy a livello dell'azienda e raccoglie dati sugli attacchi in tempo reale dagli endpoint, per fornire un'analisi forense e dati di telemetria delle minacce estremamente dettagliati. I team di sicurezza ricevono avvisi in tempo reale e report completi sulle strategie di attacco per accelerare la ricerca delle minacce, ottenendo visibilità e controllo sull'intera azienda.

Implementando la soluzione su tutti i server e gli endpoint Windows a livello aziendale, i team SOC ottengono visibilità completa sulla sicurezza. Lo streaming in tempo reale dei dati degli attacchi con analisi del flusso delle applicazioni offre agli analisti SOC una visione completa e integrata dell'attacco. Migliaia di eventi di monitoraggio di basso livello vengono correlati in tempo reale presso l'endpoint o il server, evitando la necessità di lunghe attività di analisi manuale o il ricorso a costosi data center del backend.

I dati non elaborati vengono trasformati in intelligence di alto livello per consentire ai team di sicurezza di mantenersi sempre aggiornati sulle minacce. Non sarà più necessario investire denaro e risorse nell'analisi dei falsi allarmi e nelle attività di correzione, ricostruzione o applicazione di patch di emergenza.

HP SURE CLICK ENTERPRISE[1] METTE IN SICUREZZA I VETTORI DI ATTACCO CON MAGGIORI VULNERABILITÀ

ALLEGATI E-MAIL

• Ransomware • Trojan basati su macro • Malware fileless • Collegamenti dannosi

COLLEGAMENTI DI PHISHING

• Collegamenti dannosi nel corpo e negli allegati delle e-mail • Exploit del browser
• Falsi aggiornamenti Flash/Java • Download drive-by • Attacchi "watering hole"
• Malvertising • Collegamenti nei programmi di chat

DOWNLOAD E FILE EXE

• Download intenzionali • Falsi aggiornamenti degli eseguibili • Collegamenti a documenti
• Reindirizzamenti a DNS/URL dannosi • Driver e utilità fittizi • Attacchi "watering hole"

PROTEZIONE DELL'IDENTITÀ

• Phishing di credenziali • Estrazione di credenziali locali e dei domini
• Riutilizzo non autorizzato delle credenziali

RETI NON PROTETTE

• Exploit del browser • Malware fileless • Download drive-by
• Reindirizzamenti a DNS/URL dannosi • Falsi aggiornamenti (Reader, Flash, Java, ecc.)

SITI WEB NON CLASSIFICATI

• Exploit del browser • Malware fileless • Download crittografati che eludono il rilevamento

CONTENUTO DEI SUPPORTI USB

• File di produttività Office • File multimediali
• File eseguibili • Collegamenti a documenti • Preferiti web

NESSUNA VIOLAZIONE DELLE MICRO-VM

(secondo quanto riferiscono i clienti)

Implementando la piattaforma di sicurezza HP Sure Click Enterprise è possibile proteggere specifici vettori di attacco degli utenti; in alternativa, si può ottenere una sicurezza avanzata abilitando tutte le funzionalità.

Per ulteriori informazioni, consultare **https://www.hp.com/enterprisesecurity**

1. HP Sure Click Enterprise viene venduto separatamente e richiede Windows 8 o 10; sono supportati Microsoft Internet Explorer, Google Chrome, Chromium e Firefox. Gli allegati supportati includono Microsoft Office (Word, Excel, PowerPoint) e i file PDF, se sono installati Microsoft Office o Adobe Acrobat.

4AA7-7470ITE, aprile 2021, Rev 2

HP WOLF SECURITY