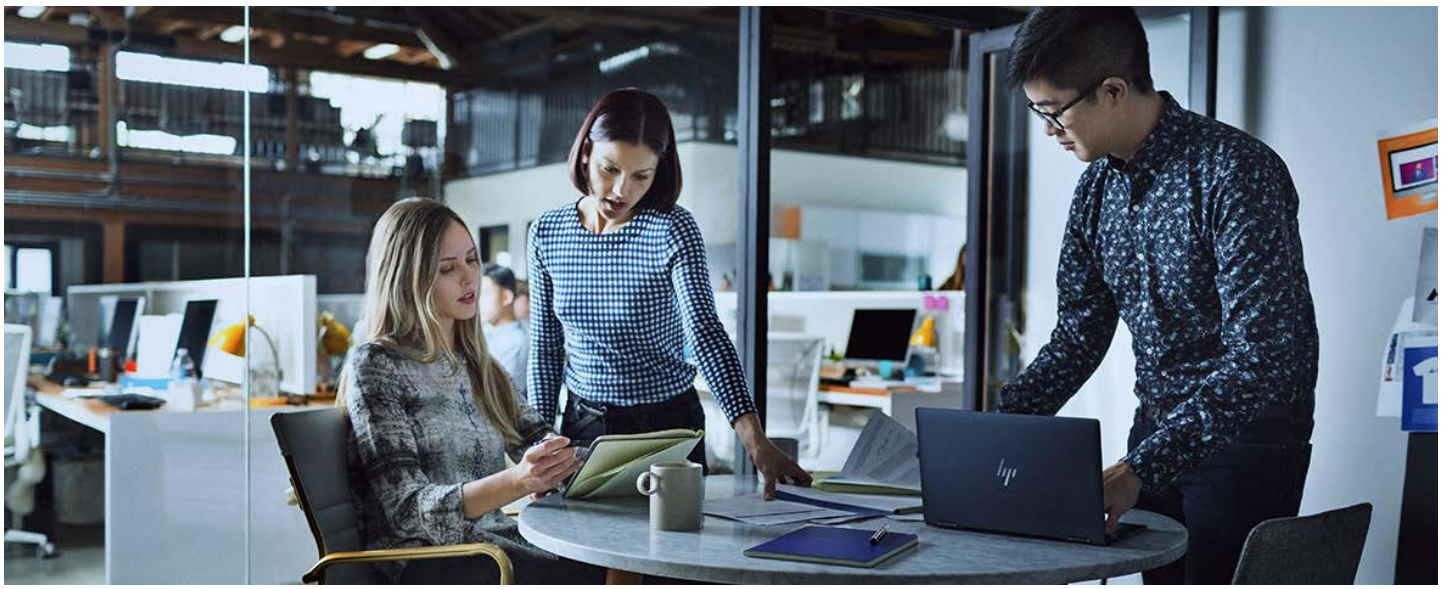
SERVIZIO HP WOLF PRO SECURITY

HP WOLF SECURITY



Vantaggi del servizio

- Bloccate gli attacchi zero-day ancora sconosciuti e il furto delle credenziali con livelli di difesa rinforzati.
- Proteggete gli endpoint con una tecnologia di isolamento di classe enterprise.
- Contribuite alla protezione dei dipendenti dalle minacce informatiche senza creare barriere alla loro produttività.

Principali caratteristiche del servizio

- Approccio protection-first per la difesa multilivello e in tempo reale degli endpoint.
- Monitoraggio e gestione competente da parte di professionisti della sicurezza certificati.
- Analisi e informazioni tempestive e fruibili.

PANORAMICA DEL SERVIZIO

Il servizio HP Wolf Pro Security contribuisce alla protezione della vostra organizzazione con un servizio di sicurezza degli endpoint a più livelli delle giuste dimensioni per le imprese in fase di crescita e consolidamento.[1] Protegge gli endpoint e riduce il rischio di attacchi con un approccio protection-first, senza impatti sulla produttività dei dipendenti e senza sovraccaricare il personale IT.

Il servizio HP Wolf Pro Security integra livelli di difesa rafforzati alla protezione anti-malware di livello enterprise. Combina un software antivirus avanzato e di nuova generazione basato sulla più recente tecnologia IA, con funzionalità di deep learning, prevenzione del furto di credenziali e isolamento difensivo con informazioni fruibili in tempo reale e monitoraggio continuo delle minacce da parte di esperti di sicurezza informatica.

CARATTERISTICHE E SPECIFICHE

Protezione

Il servizio HP Wolf Pro Security fornisce una protezione avanzata e a più livelli per gli endpoint di elaborazione.

Il sistema di intelligenza artificiale utilizzato nel servizio HP Wolf Pro Security sfrutta una combinazione di machine learning, deep learning e altre tecniche, con cui riconosce in tempi rapidi anche i file malware accuratamente camuffati, oltre a rilevare le minacce senza file in base alle loro caratteristiche, anziché fare affidamento su firme uniche La soluzione è in grado di rilevare malware “zero-day” sconosciuto, oltre a bloccare minacce note, il tutto senza aggiornamenti necessari da parte del cliente.

CARATTERISTICHE E SPECIFICHE (CONTINUA)

Inoltre, il servizio HP Wolf Pro Security protegge i dipendenti dal tipo di violazioni più comune: gli attacchi di phishing mirati al furto di credenziali. La funzione di protezione delle identità del servizio HP Wolf Pro Security impedisce agli utenti di inserire password nei siti web che raccolgono credenziali, accidentalmente visitati a partire da un collegamento di phishing contenuto in un'email, un client di chat, un file PDF o un altro file.

La tecnologia di isolamento di classe enterprise di HP Wolf Pro Security rappresenta l'ultima linea di difesa, in grado di rilevare anche le minacce invisibili che possono aver eluso le altre difese dell'endpoint del cliente e le rende innocue. Questa protezione di isolamento basata su hardware permette di aprire, modificare, stampare e salvare in tutta sicurezza allegati di posta elettronica, download di file e persino contenuti delle unità USB all'interno della propria micro macchina virtuale. Mentre sono aperte, le applicazioni vengono automaticamente monitorate per rilevare attività sospette e HP Wolf Security Controller fornisce un'analisi completa della kill chain di attacco delle minacce per aiutarvi a capirne meglio la natura e proteggervi dagli attacchi futuri.

Combinando queste tecnologie avanzate complementari, il servizio HP Wolf Pro Security fornisce ai vostri dispositivi protezione proattiva a più livelli in tempo reale.

Insights

Il servizio HP Wolf Pro Security offre ai clienti informazioni fruibili tramite HP Wolf Security Controller, una potente piattaforma di analisi della sicurezza.[2] I team IT possono monitorare lo stato di protezione dei dispositivi, visualizzare report e ricevere avvisi sui dispositivi non protetti e sulle attività delle minacce bloccate, il tutto da un dashboard unificato basato sul cloud.

Monitoraggio e gestione da parte di esperti[3]

Diversamente dalle soluzioni software pure, HP Wolf Pro Security viene erogato come servizio gestito. Gli esperti di sicurezza di HP implementano e gestiscono le policy di configurazione e sicurezza, inclusa l'applicazione continua dei criteri della quarantena della minacce per conto dell'utente. Una volta completato l'onboarding dei dispositivi, gli esperti di sicurezza di HP ne monitorano lo stato di protezione ed eseguono analisi forensi e della kill chain su nuove minacce zero-day per favorire una protezione più efficace contro gli attacchi futuri.

Categoria	Caratteristiche
Protezione	HP Sure Sense Pro: prevenzione delle minacce basata su IA per Windows 10[4]
	HP Sure Click Pro[5]: isolamento dei download e degli allegati per Windows 10
	La funzione di protezione delle identità di HP impedisce la divulgazione accidentale delle password degli utenti sui siti Web di furto delle credenziali
Analisi della sicurezza	Dashboard di protezione dei dispositivi
	Dati sulle minacce di HP Sure Click Pro e HP Sure Sense Pro
	Informazioni dettagliate sullo stato di protezione dei dispositivi
	Analisi completa della kill chain delle minacce con riferimento al framework MITRE ATT&CK™ [6]
Gestione costante dei servizi	Configurazione, ottimizzazione e applicazione delle policy del controller
	Informazioni e analisi sulle minacce
	Gestione di quarantene ed esclusioni
	Indagine sull'integrità dell'agente di sicurezza
	Implementazione degli agenti di protezione dell'agente di sicurezza
Altre caratteristiche	Integrazione SIEM tramite feed syslog

SPECIFICHE DI EROGAZIONE DEL SERVIZIO

I clienti devono installare il software client di sicurezza e analisi nei dispositivi gestiti. È necessaria una connessione Internet per accedere alle analisi e ai report, nonché per ricevere gli aggiornamenti delle policy e gli upgrade del software. Questi software agent non richiedono una connessione Internet per fornire la protezione una volta completata la configurazione. I dati dell'utente considerati sensibili, ovvero credenziali, file, contenuti e dati personali, non saranno acquisiti. I dati raccolti saranno archiviati in un repository su cloud protetto.[2]

Tramite HP Wolf Security Controller HP fornirà l'accesso a informazioni dettagliate sulla sicurezza, tra cui dashboard, report, eventi e altro.

Gli esperti di sicurezza certificati HP monitoreranno e gestiranno in modo proattivo la sicurezza degli endpoint per i clienti, inclusa l'ottimizzazione e l'applicazione delle policy di sicurezza; l'analisi degli incidenti quando viene rilevata un'effettiva minaccia positiva; la gestione degli aggiornamenti dell'agente di sicurezza; l'analisi dei problemi relativi allo stato dell'agente; ed altro ancora.

Un HP Service Expert fornirà un'assistenza di primo livello al cliente e collaborerà con i team interni di HP, inclusi esperti di sicurezza, alla risoluzione dei problemi segnalati. La disponibilità degli HP Service Expert è la seguente:

Nord America: assistenza in lingua inglese disponibile dal lunedì al venerdì (esclusi i giorni festivi HP) dalle 06:00 alle 18:00 MT.

America Latina: supporto in lingua inglese e spagnola disponibile dal lunedì al venerdì (escluse le festività HP) dalle 07:00 alle 18:00 GMT - 5.

Europa, Medio Oriente e Africa: assistenza in lingua inglese, francese e tedesca disponibile dal lunedì al venerdì (esclusi i giorni festivi HP) dalle 08:00 alle 18:00 CET.

Asia Pacifico e Giappone: supporto in lingua inglese disponibile 24 al giorno in tutta l'area geografica; inglese e giapponese supportati per il Giappone dalle 9:00 alle 21:00 ora standard del Giappone, 7 giorni su 7 (escluse le festività HP).

Responsabilità del cliente

- Fornire le informazioni richieste per consentire ad HP di configurare l'account del cliente.
- Distribuire l'agente del servizio Wolf Pro Security sui dispositivi gestiti.
- Richiedere l'aggiunta o la rimozione dei siti di download nei siti Web in whitelist, delle esclusioni e delle impostazioni dei domini email (per l'isolamento di file allegati, la protezione da malware basata su IA e la prevenzione del furto di credenziali).
- Richiedere l'aggiunta o rimozione di serie di indirizzi IP aziendali interni non soggetti a isolamento.
- Richiedere o approvare il rilascio o l'esclusione di file in quarantena o bloccati.
- Accedere al portale HP Wolf Security Controller per visualizzare dashboard, report ed eventi.
- Esaminare i report di sicurezza e rispondere in base alle esigenze.

REQUISITI DI SISTEMA

HP Wolf Pro Security è compatibile con dispositivi dotati di sistemi operativi Windows 10 in esecuzione su processori Intel® o AMD supportati. Per i requisiti di sistema più aggiornati, consultare https://www.hpdaas.com/requirements

Requisiti di rete

È richiesta una connessione Internet per le comunicazioni tra il dispositivo gestito e il servizio di gestione cloud.

Prerequisiti

Per utilizzare il servizio, è necessaria la registrazione dopo l'acquisto seguendo le istruzioni di HP. Durante la procedura di onboarding, vi verrà richiesto di fornire le informazioni necessarie per impostare gli account e le policy di sicurezza.

LIMITAZIONI DEL SERVIZIO

HP Wolf Pro Security non è un servizio di monitoraggio continuo in tempo reale. HP Sure Sense Pro e HP Sure Click Pro bloccano o isolano automaticamente contenuti non attendibili o dannosi, garantendo la protezione dei dispositivi. HP Wolf Pro Security non include servizi di ripristino o mitigazione in caso di violazione. Servizi di mitigazione e ripristino sono disponibili separatamente dai partner HP.

TERMINI E CONDIZIONI

I termini e le condizioni di HP Care Pack possono essere applicabili se il servizio è acquistato come HP Care Pack. I termini e le condizioni di HP TechPulse, l'Avviso sui diritti relativi ai dati personali e l'Informativa sulla privacy HP sono tutti applicabili al servizio.

PER ULTERIORI INFORMAZIONI

Contattare il responsabile vendite HP o il partner di canale di zona per i dettagli oppure consultare la pagina https://www8.hp.com/us/en/services/pro-security-service.html

1 I servizi HP sono regolati dalle condizioni e dai termini HP applicabili, in base alle indicazioni fornite al cliente al momento dell'acquisto. Il cliente potrebbe disporre di ulteriori diritti legali a seconda delle leggi locali vigenti; tali diritti non sono in alcun modo alterati dai termini e dalle condizioni di servizio HP o dalla garanzia limitata HP fornita con il prodotto HP. Per un elenco completo dei requisiti di sistema, consultare https://www.hpdaas.com/requirements.

2 HP non traccia o monitora informazioni che identificano quali URL sono visitati dagli utenti. I report si focalizzano sull'identificazione delle minacce e sulla loro fonte in HP Wolf Security Controller. HP Wolf Security Controller è conforme alla direttiva GDPR e allo standard ISO 27001. HP Wolf Security Controller non è disponibile come prodotto stand-alone e richiede il servizio HP Wolf Pro Security. Per i requisiti di sistema completi, consultare http://www.hpdaas.com/ requirements. I servizi HP sono regolati dai termini e dalle condizioni di servizio applicabili di HP, forniti o indicati al cliente al momento dell'acquisto. Il cliente potrebbe disporre di ulteriori diritti a seconda delle leggi locali vigenti; tali diritti non sono in alcun modo alterati dai termini e dalle condizioni di servizio HP o dalla Garanzia limitata HP fornita con il prodotto HP.

3 L'analisi delle minacce da parte degli esperti della sicurezza HP è un processo forense disponibile in seguito a un evento di malware bloccato o isolato dall'agente software HP Wolf Pro Security. Non si tratta di un servizio di monitoraggio 24x7 "in tempo reale". Per ulteriori informazioni su questa funzionalità del servizio, consultare il documento Definizione del servizio HP Wolf Pro Security. L'agente del servizio HP Wolf Pro Security isola automaticamente i contenuti inattendibili o dannosi, garantendo la protezione prima dell'analisi. Inoltre, nessun piano include servizi di ripristino o mitigazione in caso di violazione.

4 Per un elenco completo delle versioni supportate di Windows 10, consultare https://www.hpdaas.com/requirements. Si noti che Windows 7 e 8.1 non sono supportati dal servizio HP Wolf Pro Security.

5 La tecnologia HP Sure Click Pro è inclusa con il servizio HP Wolf Pro Security e richiede Windows 10 Pro o Enterprise; sono supportati Microsoft Internet Explorer, Google Chrome, Chromium, Mozilla Firefox e il nuovo Edge. Gli allegati supportati includono Microsoft Office (Word, Excel, PowerPoint) e i file PDF, se sono installati Microsoft Office o Adobe Acrobat. Per ulteriori dettagli, consultare https://www.hpdaas.com/requirements.

6 MITRE non afferma che ATT&CK enumeri tutte le possibilità dei tipi di azioni e comportamenti documentati come parte del suo modello e del suo framework di tecniche. L'utilizzo delle informazioni contenute in ATT&CK per affrontare o coprire tutte le categorie di tecniche non garantisce la piena copertura difensiva poiché potrebbero esistere tecniche o variazioni non divulgate nelle tecniche esistenti non documentate da ATT&CK.

Registratevi per ricevere gli aggiornamenti
hp.com/go/getupdated

Condividete questo documento con i colleghi

Valutate questo documento

© Copyright 2021 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.

4AA7-4656ITE, maggio 2021, Rev. 5

HP WOLF SECURITY