



HP WOLF SECURITY

SINTESI DELLA SOLUZIONE

HP WOLF PRO SECURITY SERVICE

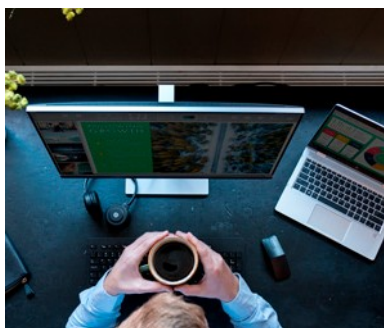
AUMENTATE LA SICUREZZA DELLA VOSTRA AZIENDA CON UN SERVIZIO DI PROTEZIONE MULTILIVELLO DEGLI ENDPOINT

Difendetevi dagli attacchi informatici senza ripercussioni sulla produttività dei dipendenti e senza aumentare il carico di lavoro del reparto IT grazie ad HP Wolf Pro Security Service, una soluzione per la protezione degli endpoint che vanta un'esperienza comprovata nel settore.¹



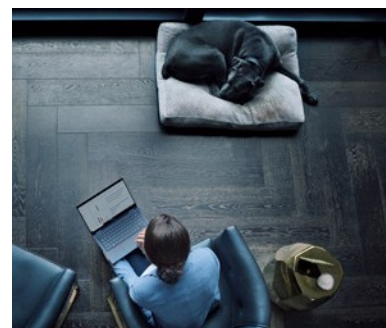
SICUREZZA SU CUI POTETE CONTARE

Impedite gli attacchi, anche quelli delle minacce ancora ignote, con livelli rafforzati di protezione proattiva basati su isolamento di livello enterprise e NGAV avanzato con tecnologie di deep learning.



GESTIONE SEMPLIFICATA DELLA SICUREZZA

Affidatevi a una gestione della sicurezza degli endpoint completa che vi offre insights strategici, anche senza disporre di personale e competenze specializzate in-house. Grazie agli esperti della sicurezza HP, i vostri tecnici IT saranno finalmente liberi di dedicarsi ai progetti più importanti per la vostra azienda.



MASSIMA PRODUTTIVITÀ DEI DIPENDENTI

Aumentate la produttività con una soluzione di sicurezza che protegge le vostre applicazioni di lavoro, i dati e le password dei dipendenti e la rete aziendale.



SICUREZZA SU CUI POTETE CONTARE

- **Un approccio che mette al centro la sicurezza**
Impedite gli attacchi zero-day con una difesa multilivello che combina un avanzato antivirus di nuova generazione basato sulle più recenti tecniche AI come il deep learning² con tecnologie di isolamento³ per proteggere i dati e i dispositivi della vostra azienda e le credenziali dei dipendenti.
- **Difesa di livello enterprise**
Difendetevi dalle minacce non rilevabili con la tecnologia di isolamento di livello enterprise³ a cui si affidano agenzie governative di tutto il mondo e adottata per la sua facilità d'uso dalle organizzazioni che hanno bisogno di solide competenze in materia di sicurezza.
- **Protezione dell'identità**
Evitate il furto di password avvisando gli utenti e impedendo loro di condividere i dati di login su siti web di cui è nota la pericolosità.



GESTIONE SEMPLIFICATA DELLA SICUREZZA

- **Gestione completa delle soluzioni**
Affidatevi agli esperti certificati HP per il monitoraggio e la gestione del profilo di sicurezza degli endpoint. Potrete così liberare le vostre risorse IT aziendali, per consentire loro di focalizzarsi sui progetti strategici che fanno davvero crescere il vostro business.
- **Gestione da parte di professionisti certificati**
Nell'ambito di un servizio cloud gestito, gli esperti della sicurezza HP provvedono alla gestione continua della soluzione con l'obiettivo di fornirvi una difesa contro i futuri attacchi attraverso il monitoraggio dello stato di protezione dei dispositivi, l'intelligence sulle minacce e l'analisi dei dati.
- **Strumenti di analytics e insights strategici**
Monitorate la sicurezza dei vostri dispositivi endpoint attraverso HP Wolf Security Controller con avvisi e informazioni in tempo reale sui tentativi di attacco.



MASSIMA PRODUTTIVITÀ DEI DIPENDENTI

- **Livelli di protezione invisibili**
Contribuite alla protezione dei dipendenti dalle minacce informatiche senza ostacolare la loro produttività quotidiana, con una protezione trasparente che lavora dietro le quinte.
- **Produttività ed efficienza**
Consentite ai vostri dipendenti di lavorare liberamente e senza preoccupazioni con i documenti Microsoft Office e PDF.⁶

HP WOLF PRO SECURITY SERVICE INCLUDE:

PROTEZIONE ANTIMALWARE AVANZATA CON DEEP LEARNING²

- Rilevamento di minacce note e ignote
- Protezione dai file malware statici e dalle minacce senza file
- Analisi della reputazione dei file basata su cloud
- Rilevamento delle tecniche di evasione del malware
- Nessun aggiornamento delle firme richiesto

ANALISI E REPORT DI SICUREZZA IN TEMPO REALE

- Dashboard unificata per visualizzare gli interventi di prevenzione del malware, minacce isolate e phishing delle credenziali
- Visualizzazioni e report in tempo reale degli elementi in quarantena e dell'attività delle minacce, tra cui analisi kill-chain mappata al framework MITRE ATT&CK⁵
- Visualizzazione delle impostazioni di policy, siti attendibili e whitelisting
- Integrazione diretta del syslog nel SIEM esistente

ISOLAMENTO DELLE MINACCE IN TEMPO REALE³

- Isolamento degli allegati e-mail
- Protezione per link e condivisione di file via chat
- Protezione dai documenti inviati da e-mail di phishing
- Protezione delle password dai siti web che raccolgono le credenziali
- Protezione dai download di file
- Supporto all'IT per il whitelisting del sito web aziendale

GESTIONE DA PARTE DEGLI ESPERTI DI SICUREZZA HP

- Monitoraggio e analisi continui delle minacce e dello stato di protezione dei dispositivi
- Indicazioni sulle azioni associate alle minacce prevenute e ai problemi configurazione per i dispositivi non protetti
- Amministrazione centralizzata basata su policy e gestione delle impostazioni
- Hosting e gestione di HP Wolf Security Controller

Ulteriori informazioni alla pagina [HP.com/pro-security-service](https://www.hp.com/pro-security-service)

1. HP Wolf Pro Security Service è venduto separatamente. Per i requisiti completi del sistema, 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 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 i requisiti di sistema completi, consultare www.hpdaas.com/requirements.
2. HP Sure Sense è disponibile su PC HP selezionati e non è disponibile con Windows 10 Home.
3. La tecnologia di isolamento HP Sure Click Pro è inclusa in HP Proactive Security e richiede Windows 10 Pro o Enterprise. Sono supportati Microsoft Internet Explorer, Google Chrome, Chromium, Mozilla Firefox e la nuova versione di Edge. Gli allegati supportati includono i file Microsoft Office (Word, Excel, PowerPoint) e PDF, se sono installati Microsoft Office o Adobe Acrobat.
4. HP TechPulse è una piattaforma di telemetria e analisi che fornisce dati critici su dispositivi e applicazioni. I report di HP TechPulse sono incentrati sull'identificazione delle minacce e delle loro fonti. HP TechPulse è conforme a GDPR e ISO 27001.
5. 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.
6. HP Wolf Pro Security Service richiede Windows 10. HP Wolf Pro Security Service non supporta il sistema operativo Windows per i dispositivi RPOS e thin client, nonché VDI e altre implementazioni di virtualizzazione desktop. Attualmente non supporta Android o macOS.



HP WOLF SECURITY

© Copyright 2021 HP Development Company, L.P. Le informazioni qui contenute possono subire variazioni senza preavviso. Le uniche garanzie per i prodotti e servizi HP sono espresse 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. Adobe e Acrobat sono marchi registrati di Adobe negli Stati Uniti e/o in altri Paesi. Google, Chrome e Chromium sono marchi registrati di Google Inc. Microsoft, Windows, Skype e Skype for Business sono marchi registrati di Microsoft Corporation negli Stati Uniti e/o in altri Paesi. The MITRE Corporation. Questo documento è riprodotto e distribuito con l'autorizzazione di MITRE Corporation.