



Vantaggi del servizio

- Fermate gli attacchi “zero-day” con una difesa multilivello
- Proteggete gli endpoint con una tecnologia in linea con le direttive governative
- Contribuite alla protezione dei dipendenti dalle minacce informatiche senza creare barriere alla loro produttività

Principali caratteristiche del servizio

- Approccio incentrato sulla protezione alla sicurezza degli endpoint con difesa multilivello in tempo reale
- Gestione da parte di professionisti della sicurezza certificati ed esperti
- Analisi e informazioni preziose e tempestive

Panoramica del servizio

HP Proactive Security contribuisce alla protezione della vostra organizzazione con un servizio di sicurezza degli endpoint multilivello delle giuste dimensioni per le medie imprese.¹ Con un approccio alla gestione della sicurezza degli endpoint incentrato sulla protezione, Proactive Security riduce il rischio di attacchi e offre agli utenti la libertà di lavorare da qualsiasi luogo senza incrementare il carico di lavoro dell'IT.

Proactive Security integra una protezione anti malware multilivello e in linea con le direttive governative che combina tecnologie di deep learning e isolamento con informazioni strategiche e la gestione da parte di esperti di sicurezza informatica, il tutto offerto come servizio gestito.

Caratteristiche e specifiche

Sicurezza

HP Proactive Security fornisce una protezione multilivello avanzata per gli endpoint che include HP Sure Sense Advanced e HP Sure Click Advanced.²

La tecnologia di protezione basata su deep learning di HP Sure Sense Advanced è stata addestrata su centinaia di milioni di campioni di malware ed è ora in grado di riconoscere tempestivamente anche i file malware dissimulati più accuratamente, oltre che rilevare minacce senza file basandosi sulle loro caratteristiche, anziché su firme univoche. La soluzione è in grado di rilevare malware “zero-day” mai visto prima, oltre a fermare malware noto, tutto senza aggiornamenti necessari da parte del cliente.

HP Sure Click Advanced utilizza tecnologia di isolamento in linea con le direttive governative come ultima linea di difesa per contenere le minacce che riuscissero a superare le altre difese degli endpoint. Allegati e-mail, download di file e persino i contenuti delle unità USB vengono aperti in micro-VM separate attraverso l'isolamento delle applicazioni sui PC degli utenti per garantire la protezione dagli attacchi informatici, monitorando al contempo l'attività delle minacce durante l'isolamento. Questo consente di avere una visibilità maggiore della catena della protezione dagli attacchi.

Combinando queste due tecnologie avanzate complementari, HP Proactive Security fornisce protezione proattiva multilivello in tempo reale ai vostri dispositivi.

Caratteristiche e specifiche (continua)

Informazioni approfondite

HP Proactive Security fornisce informazioni strategiche approfondite ai clienti tramite HP TechPulse, una potente piattaforma di analisi basata su IA.³ I vostri team IT possono monitorare lo stato di protezione dei dispositivi e ricevere notifiche sui dispositivi non protetti e sull'attività relativa alle minacce bloccate, il tutto da un unico dashboard unificato.

Gestione

A differenza di semplici soluzioni software, HP Proactive Security è fornito come servizio gestito. Gli esperti di sicurezza di HP implementano e gestiscono le policy di configurazione e sicurezza, inclusa la gestione 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 catena di protezione su nuove minacce "zero-day" per identificare le fonti e favorire una protezione più efficace contro gli attacchi futuri.

Accesso a CyQu di Aon

Con HP Proactive Security, potete accedere al Cyber Quotient Evaluation (CyQu) di Aon, uno strumento di valutazione informatica online che assegna un punteggio al vostro profilo di sicurezza. Avete anche la possibilità di accedere al servizio preferenziale Incident Response Retainer (\$0, un'ora di consulenza inclusa) e di approfittare del processo semplificato per la richiesta di polizze assicurative informatiche.⁴

Categoria	Caratteristiche
Sicurezza	Prevenzione delle minacce HP Sure Sense Advanced basata su IA per dispositivi Windows 10, Mac OS e Android
	Isolamento dei download e degli allegati HP Sure Click Advanced per Windows 10
Report di sicurezza	Report sulla conformità della sicurezza aziendale
	Report sui dispositivi compromessi
	Report sulla conformità della sicurezza dei dispositivi
	Report sui dispositivi che non inviano dati
	Report sulla sicurezza di HP Sure Click Advanced
	Report sulle attività di HP Sure Recover
	Report sulle impostazioni di HP Sure Recover
	Report sulla sicurezza di HP Sure Sense Advanced
Report sull'integrità dei sistemi di HP Sure Start	
Incidenti relativi alla sicurezza	Dispositivo non protetto da HP Sure Click
	Minaccia vera positiva isolata da HP Sure Click
	Dispositivo non protetto da HP Sure Sense
	Minaccia evitata da HP Sure Sense
Gestione continua	Ottimizzazione e applicazione delle policy
	Informazioni e analisi sulle minacce
	Indagine sullo stato degli agent di sicurezza
	Aggiornamento degli agent di sicurezza
	Report approfondito sulle minacce di Sure Click Advanced ⁵
Altre caratteristiche	CyQu di Aon, uno strumento di valutazione informatica online con accesso opzionale ai servizi di assicurazione informatica e risposta agli incidenti di Aon. ⁴
	Supporto di SIEM con API HP

Specifiche di fornitura

I dispositivi gestiti da HP avranno agent software installati per fornire protezione in tempo reale e raccogliere informazioni sui dispositivi. È richiesta una connessione Internet per impostare o aggiornare le policy di sicurezza e fornire informazioni all'utente. 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.⁶

Sarà disponibile un portale dal quale accedere alle informazioni sulla sicurezza, tra cui un dashboard, i report, gli incidenti e molto altro.

Gli esperti di sicurezza certificati 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 redazione di report di analisi approfonditi se si tratta di una minaccia nuova, originale o "zero-day" rilevata da Sure Click Advanced; la gestione degli aggiornamenti dell'agent di sicurezza; l'analisi dei problemi relativi allo stato dell'agent; 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:** assistenza in lingua inglese e spagnola disponibile dal lunedì al venerdì (esclusi i giorni festivi 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:** assistenza in lingua inglese disponibile 24 ore al giorno, in lingua giapponese dalle 09:00 alle 21:00 ora giapponese, 7 giorni alla settimana (esclusi i giorni festivi HP).

Responsabilità del Cliente

- Fornire le informazioni richieste per consentire ad HP di configurare un account
- Distribuire gli agent di Proactive Security sui dispositivi gestiti
- Richiedere l'aggiunta o rimozione di utenti e dispositivi gestiti
- Richiedere l'aggiunta in whitelist o la rimozione di siti web di download e domini e-mail (per l'isolamento dei file allegati)
- Richiedere l'aggiunta o rimozione di serie di indirizzi IP aziendali non soggetti a isolamento
- Richiedere o approvare il rilascio o l'esclusione di file in quarantena o bloccati
- Accedere alla console HP TechPulse per visualizzare dashboard, report e incidenti
- Esaminare i report di sicurezza e rispondere in base alle esigenze
- Completare l'indagine CyQu online⁴



Requisiti di sistema

Piattaforma	Requisiti del sistema operativo	Requisiti hardware ⁷
Windows	La release del sistema operativo Windows 10 più aggiornata comunemente disponibile o una delle due release precedenti più importanti	HP Sure Click Advanced^{2,8} <ul style="list-style-type: none"> • Intel Core i3, i5, i7 (o una CPU AMD moderna) con tecnologia di virtualizzazione abilitata nel BIOS/UEFI • Almeno 4 GB di RAM (8 GB consigliati) • Almeno 6 GB di spazio libero su disco HP Sure Sense Advanced <ul style="list-style-type: none"> • Almeno 4 GB di RAM
MacOS	MacOS 10.12 o versione superiore	Tecnologia HP Sure Click <ul style="list-style-type: none"> • Non supportato su dispositivi MacOS HP Sure Sense Advanced <ul style="list-style-type: none"> • Nessun particolare requisito hardware su MacOS
Android	Android v5.0 o versione superiore	Tecnologia HP Sure Click <ul style="list-style-type: none"> • Non supportato su dispositivi Android HP Sure Sense Advanced <ul style="list-style-type: none"> • Nessun particolare requisito hardware su Android

Requisiti del software di terzi

Adobe Acrobat Reader DC deve essere l'applicazione predefinita per i file PDF.

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

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

Per ulteriori informazioni, contattate il vostro partner o rappresentante commerciale HP di zona o visitate hp.com/proactive-security

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



Condividete questo documento con i colleghi

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. I requisiti completi di sistema sono disponibili su hpdaas.com/requirements.
2. La tecnologia HP Sure Click Advanced è inclusa con HP Proactive Security e richiede Windows 10 e Microsoft Internet Explorer, Google Chrome o Chromium. Gli allegati supportati includono Microsoft Office (Word, Excel, PowerPoint) e i file PDF, se sono installati Microsoft Office o Adobe Acrobat. HP Sure Click Advanced non può essere installato per la lingua cinese semplificata.
3. 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 TechPulse. HP TechPulse è conforme a GDPR e ISO 27001.
4. I servizi Aon sono disponibili solo negli Stati Uniti. Gli acquirenti del servizio HP Proactive Security negli Stati Uniti riceveranno il punteggio di sicurezza e autovalutazione CyQu di Aon. Sono inclusi un servizio "\$0 Retainer" e una consulenza di un'ora, con servizi di risposta agli incidenti opzionali disponibili da Aon. I rappresentanti dell'assistenza all'onboarding HP forniranno tutte le istruzioni.
5. L'analisi delle minacce da parte degli HP Service Expert è un processo forense che si attiva in seguito a un evento malware bloccato o isolato dal software client HP Sure Click Advanced. Non si tratta di un servizio di monitoraggio 24x7 "in tempo reale". Il client agent HP Sure Click Advanced isola automaticamente i contenuti inaffidabili o dannosi, garantendo la protezione prima dell'analisi. Inoltre, nessun piano include servizi di ripristino o mitigazione in caso di violazione. I servizi di mitigazione e ripristino sono disponibili come servizi separati erogati dai partner HP, tra cui Aon.
6. Durante il trasferimento dal client del dispositivo al server Web, i dati sono protetti tramite SSL. I dati sono accessibili solo dal server web HP DaaS.
7. Il Cliente può implementare parzialmente la tecnologia (HP Sure Sense Advanced o HP Sure Click Advanced) se il sistema non soddisfa i requisiti minimi.
8. Per un elenco completo delle versioni di Windows 10 supportate, fare riferimento alla Bromium Windows Support Policy. Si noti che Windows 7 e 8.1 non sono supportati da HP Proactive Security.

© Copyright 2020 HP Development Company, L.P. Le informazioni qui contenute possono subire variazioni senza preavviso. Le uniche garanzie sui prodotti e sui 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 contenute. Adobe e Acrobat sono marchi di fabbrica di Adobe Systems Incorporated. Apple e macOS sono marchi di Apple Inc., registrati negli Stati Uniti e in altri Paesi. Android, Google, Chrome e Chromium sono marchi registrati di Google Inc. Microsoft e Windows sono marchi registrati di Microsoft Corporation negli Stati Uniti e/o in altri Paesi.

