HP Absolute Security

Panoramica del servizio

Insieme, HP e Absolute propongono una soluzione di sicurezza affidabile per proteggere dati e dispositivi, connessi o meno alla rete aziendale.

Absolute fornisce persistenza, intelligence e resilienza degli endpoint. La piattaforma basata su cloud mantiene una connessione costante ai dispositivi tramite la tecnologia Absolute Persistence® autoriparante. Questa piattaforma esclusiva e affidabile è incorporata in molti dispositivi HP, per consentire all'IT di monitorare, gestire e proteggere l'intero parco di endpoint.

È possibile scegliere fra tre livelli di servizio in base alle esigenze dell'IT e dell'azienda:

- Servizio Absolute Visibility
- Servizio Absolute Control
- Servizio Absolute Resilience

Vantaggi del servizio

- Persistenza: sicurezza integrata nei dispositivi per garantirne la protezione e una gestione semplificata
- Intelligence: visibilità sull'intero parco di endpoint per evitare punti ciechi e migliorare la conformità
- Protezione dei dati: localizzazione, blocco ed eliminazione dei dati dei dispositivi, connessi o meno alla rete aziendale
- Resilienza: controlli autoriparanti degli endpoint che attivano la ricompilazione, la reinstallazione o il ripristino degli agenti endpoint per garantire il corretto funzionamento delle misure di sicurezza

Principali caratteristiche del servizio

Viene applicato un livello di sicurezza per l'intero ciclo di vita di ogni dispositivo, con invio di avvisi al verificarsi di specifiche condizioni. Alcuni esempi:

- Protezione dei nuovi dispositivi in transito
- Convalida degli utenti finali
- Esecuzione di inventari hardware/software
- Certificazione dei protocolli di eliminazione dati a fine ciclo di vita

Caratteristiche del servizio e specifiche di fornitura

Tecnologia Absolute Persistence®

La tecnologia Absolute Persistence® è una soluzione di sicurezza brevettata che fornisce una connessione continua, affidabile e bidirezionale tra dispositivi, dati e la console Absolute.

La capacità di comunicare con gli endpoint, indipendentemente dall'utente o dalla posizione, consente di applicare misure di sicurezza da remoto per proteggere i dispositivi e i dati che contengono.

Absolute investe costantemente nel mantenimento di autorizzazioni, accreditamenti e certificazioni pertinenti per l'azienda e i suoi prodotti. Per maggiori informazioni, consultare https://www.absolute.com/platform/certifications/.

Valutazione del rischio

Monitoraggio delle attività e dello stato dei dispositivi, con invio di avvisi al verificarsi di specifiche condizioni. Alcuni esempi:

- Posizione dei dispositivi non conformi
- Stato non integro di crittografia, antimalware, SCCM o altre tecnologie di sicurezza complementari
- Dispositivi non connessi per un periodo di tempo prolungato
- Applicazioni in blacklist
- Dati sensibili archiviati nei dispositivi o dati che usano applicazioni di storage su cloud
- Comportamenti illeciti dei dipendenti

Risposta al rischio

Comandi di sicurezza e altre misure da remoto per mitigare gli incidenti. Alcuni esempi:

- Blocco di un dispositivo fino alla verifica del relativo stato
- Prova definitiva che i dati degli endpoint sono stati crittografati e non ne è stato eseguito l'accesso al momento dell'incidente
- Eliminazione dei dati degli endpoint da remoto
- Indagini e analisi del rischio degli endpoint
- Esecuzione di query o di script di correzione da remoto in qualsiasi numero di dispositivi per raccogliere informazioni o risolvere vulnerabilità e conferma della corretta esecuzione

Servizio Absolute Visibility

Visualizzate tutti i dispositivi, nella rete o fuori, e raccogliete automaticamente più di 500 tipologie di dati su hardware, software, sicurezza, utilizzo e geolocalizzazione, con 365 giorni di log cronologici, il tutto con conformità a SOC2 di livello 1 e 2. I dati includono:

- Dettagli dell'inventario hardware per oltre 25 OEM di PC
- Inventario delle applicazioni installate (oltre 2.000 applicazioni rilevate)
- Posizione e cronologia dei dispositivi
- Monitoraggio dell'integrità delle applicazioni
- Avvisi automatizzati e personalizzabili
- Tecnologia Persistence®
- Stato della crittografia e monitoraggio dei processi

Servizio Absolute Control

Oltre al monitoraggio dei dispositivi, avete la possibilità di intraprendere azioni da remoto per correggere immediatamente i rischi per gli endpoint. Tutte le caratteristiche di Absolute Visibility, oltre a:

- Blocco dei dispositivi, on-demand o offline
- Eliminazione completa o selettiva dei dati, confermata dalle certificazioni di settore pertinenti
- Geofence specifici per uffici, edifici, città e Paesi in oltre 120 Paesi
- Geofencing per rilevare lo spostamento dei dispositivi, avviare interventi e creare azioni automatizzate con messaggi personalizzati
- Interventi ServiceNow con integrazione di altre API di terze parti

Servizio Absolute Resilience

Stabilite misure di sicurezza resilienti assicurandovi che le applicazioni critiche di terze parti rimangano sempre attive. Identificate e proteggete i dati sensibili da remoto, raccogliete informazioni precise o correggete le vulnerabilità degli endpoint. Tutte le caratteristiche di Absolute Visibility e Control, oltre a:

- Conformità GDPR
- Analisi e recupero dei dispositivi rubati
- Autoriparazione delle applicazioni di terze parti tra aziende diverse
- Scansione da remoto dei file sensibili e a rischio, in locale e nel cloud
- Integrazione di SCIM 2.0, che offre una migliore conformità agli enti normativi
- Esecuzione di script di PowerShell o BASH in qualsiasi dispositivo
- Esecuzione dell'analisi dei rischi in dispositivi sospetti con raccomandazioni di esperti

Consultare absolute.com/platform/editions per un confronto dettagliato tra Absolute Visibility, Absolute Control e Absolute Resilience. Per richiedere una demo, visitate la pagina absolute.com/hp.

Absolute si impegna a fornire supporto di altissimo livello. Soluzioni e assistenza per i prodotti Absolute sono disponibili alla pagina relativa alle risorse di assistenza online di Absolute (absolute.com/support).

Absolute Investigations

I clienti Absolute che si rivolgono al team Absolute Investigations potranno intervenire sulla propria infrastruttura ed eliminare immediatamente i punti deboli, riducendo i rischi per l'azienda.

I clienti Absolute potranno sfruttare l'esperienza del team Absolute Investigations per eseguire indagini sugli endpoint. Il team aiuterà i clienti a:

- Determinare le cause degli incidenti di sicurezza degli endpoint
- Identificare ed eliminare le minacce interne
- Ottimizzare le best practice per evitare il ripetersi dell'incidente
- Determinare se l'incidente abbia causato l'accesso ai dati e se sia necessaria una notifica di violazione dei dati
- Recuperare i dispositivi rubati

Per maggiori informazioni, scaricate la scheda tecnica di Absolute Investigations:
absolute.com/resources/datasheets/absolute-investigative-services

Responsabilità del cliente

Subito dopo l'acquisto, il cliente dovrà registrare l'hardware oggetto del servizio, e il servizio HP Care Pack utilizzando le istruzioni per la registrazione fornite da HP. Per motivi di sicurezza e conformità, durante il processo di registrazione è possibile immettere solo l'indirizzo email del cliente finale (account amministratore), in modo che Absolute completi l'assegnazione della licenza. Se la registrazione non viene eseguita con l'indirizzo email del cliente finale, la licenza potrebbe non essere assegnata.

Inoltre, per ottenere l'idoneità per il servizio HP Absolute Security, il cliente dovrà collaborare con Absolute per installare il software necessario nel dispositivo richiesto. Non verrà fornito alcun servizio prima dell'installazione dell'agente software Absolute. Il cliente riceverà un'email di benvenuto da Absolute (fulfillment@absolute.com) contenente le istruzioni per il download e l'installazione dell'agente software Absolute.

In alternativa, HP potrà preinstallare Absolute in fabbrica sui dispositivi del cliente prima della distribuzione. Per maggiori informazioni su questa opzione, contattate un rappresentante commerciale HP.

Prima che il servizio possa essere attivato, è necessario installare l'agente software Absolute. Al fine di utilizzare funzionalità di sicurezza come la geotecnologia e la risposta al rischio, il cliente deve innanzitutto firmare un accordo di pre-autorizzazione e seguire le altre istruzioni.

Si applicano termini e condizioni.

Vedere i termini e condizioni completi di Care Pack.
Per maggiori informazioni sui servizi HP, contattate i nostri uffici vendita o visitate il nostro sito web:
hp.com/go/services

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

4AA2-1087ITE, maggio 2024