DELL Technologies

Dell SafeData

La piattaforma Absolute

VISUALIZZAZIONE E PROTEZIONE DEI DATI E DEI DISPOSITIVI

L'unica soluzione integrata nel firmware per l'intelligence e la resilienza degli endpoint

Nonostante l'implementazione di tutte le strategie ottimali, gli strumenti per la sicurezza e gestione degli endpoint tradizionali sono comunque soggetti a limitazioni e punti ciechi, possono essere disabilitati dagli utenti finali o devono competere per le risorse dei dispositivi, finendo quindi per non funzionare come dovrebbero.

Di conseguenza, diventa difficile visualizzare, controllare e proteggere gli endpoint. Tutto questo si traduce in imprecisione, inefficienza operativa e falle di sicurezza, compromettendo la capacità di rilevare i problemi in modo affidabile e rispondere in modo sicuro alle minacce. I risultati inevitabili sono quindi audit incerti, spreco di risorse, violazioni dei dati e infrazioni della conformità.

Dell incorpora la tecnologia brevettata Persistence® di Absolute nel firmware prima che i dispositivi lascino la fabbrica. Persistence® ripara e reinstalla automaticamente l'agent Absolute su ogni sequenza di avvio, anche se è stata ricreata l'immagine del dispositivo o se il disco rigido è stato sostituito.

Una volta attivato, Absolute fornisce la resilienza necessaria tramite un collegamento digitale indissolubile, che garantisce una visione e un controllo costanti dei dispositivi e la capacità di risolvere le falle di sicurezza, indipendentemente dalla situazione contingente.

Ulteriori informazioni sono disponibili sul sito DellEMC.com/endpointsecurity

© 2022 Dell Technologies e sue società controllate.

ABSOLUTE®

ASSET INTELLIGENCE

Visibilità persistente degli endpoint, fuori e dentro la rete

Absolute assicura che il collegamento digitale a ciascun dispositivo rimanga intatto, fornendo informazioni affidabili su tutti gli endpoint, all'interno o all'esterno della rete aziendale.

È possibile mantenere sempre aggiornato l'inventario hardware e software, semplificare la gestione del ciclo di vita dei dispositivi, velocizzare gli audit e le operazioni quotidiane, ricevere avvisi quando i dispositivi sono in movimento, rilevare le risorse sottoutilizzate per evitare gli sprechi e usare questi dati per prendere decisioni più convenienti in termini economici.

Fattori per il successo

Self-healing integrato: l'unica piattaforma con tecnologia di self-healing integrata nel firmware del dispositivo che consente di visualizzare e controllare l'intera flotta di dispositivi da un unico dashboard, indipendentemente dalla piattaforma o dalla rete

Analisi dell'hardware: consente di controllare e di creare un inventario completo e sempre aggiornato di tutti gli endpoint, con centinaia di data point per dispositivo

Geolocalizzazione: monitoraggio accurato della posizione fisica di qualsiasi dispositivo, in qualsiasi momento e sia all'interno che all'esterno della rete, inclusi i log cronologici

Gestione del ciclo di vita remota: semplificazione del provisioning, della riallocazione e della disattivazione dei dispositivi da remoto, inclusa la possibilità di automatizzare la manutenzione regolare, risolvere i problemi dei dispositivi ed eseguire una cancellazione EOL certificata

Report e avvisi software: aggiornamento dell'inventario software, eliminazione dello shadow IT e rilevamento delle app necessarie mancanti

Utilizzo dei dispositivi: consente di comprendere come vengono utilizzati i dispositivi e identifica gli asset inattivi per decidere quali riallocare e quali ritirare

SICUREZZA RESILIENTE DEGLI ENDPOINT

Valutazione del profilo di sicurezza e applicazione dei controlli di sicurezza

Da un'unica console basata sul cloud è possibile creare report sulla conformità a standard o normative e condividere queste informazioni con qualsiasi entità interessata dell'organizzazione. È possibile rilevare deviazioni e vulnerabilità della configurazione, applicare automaticamente le app di sicurezza e implementare in remoto comandi e flussi di lavoro per risolvere le falle di sicurezza e automatizzare le attività indispensabili.

Absolute è la prima e unica soluzione per la visibilità e il controllo degli endpoint che garantisce la persistenza a qualsiasi altro controllo di sicurezza. Estendendo la resilienza di Absolute ad altre applicazioni, l'intero stack di sicurezza può adottare le funzionalità di self-healing, diffondendo questa protezione avanzata all'intera flotta senza dover introdurre nuovi dispositivi. Quando gli endpoint si allontanano dall'immagine desiderata, Absolute li obbliga nuovamente ad allinearsi per evitare devastanti violazioni dei dati e mantenere la continuità aziendale.

Fattori per il successo

Benchmarking degli standard: report sulla conformità agli standard per la sicurezza informatica o alle normative sulla privacy dei dati, segnalazione dei dispositivi privi di crittografia o di soluzioni antimalware e chiusura delle falle di conformità

Rafforzamento della configurazione: individuazione dei punti deboli e delle deviazioni rispetto alle configurazioni desiderate degli endpoint e conseguente regolazione su larga scala

Ulteriori informazioni sono disponibili sul sito DellEMC.com/endpointsecurity

© 2022 Dell Technologies e sue società controllate.

ABSOLUTE®

Continuità delle applicazioni: basta interruzioni della produttività utente e della continuità aziendale grazie alle applicazioni con self-healing

Protezione dei dati garantita: rafforzamento della protezione dei dati con controlli di sicurezza persistenti come crittografia, antimalware, VPN, gestione degli endpoint e altro ancora, senza alcun intervento umano

Rilevamento e risoluzione delle vulnerabilità: individuazione degli endpoint che eseguono versioni vulnerabili del sistema operativo, push di aggiornamenti urgenti o implementazione di soluzioni alternative di protezione, all'interno o all'esterno della rete aziendale

Flussi di lavoro automatizzati: deployment remoto di comandi e flussi di lavoro automatizzati per risolvere le falle di sicurezza rapidamente e su larga scala

RISPOSTA AFFIDABILE AI RISCHI

Rilevamento degli incidenti di sicurezza e successive attività di risposta e ripristino

Con Absolute, si possono analizzare a fondo i dispositivi per individuare i dati sensibili a rischio, nonché per rilevare dispositivi mancanti o comportamenti sospetti. In qualsiasi fase di un incidente (precursore, vulnerabilità, violazione o ripristino), Absolute offre una suite di strumenti persistenti per rispondere ai problemi e ripristinare il sistema in modo affidabile.

L'utente riceve immediatamente un avviso in caso di vulnerabilità, esposizione o nuove attività su dispositivi mancanti. Può quindi bloccare i dispositivi e cancellare i dati contenuti. Può dimostrare agli enti di controllo che i dati sono sempre stati protetti durante un incidente. Può usare in modo ottimale i log cronologici per evitare notifiche di violazione, conoscere la root cause ed evitare altri incidenti simili.

Fattori per il successo

Rilevamento dati degli endpoint: individuazione di dati sensibili, come IP, PII, PHI o PFI, a rischio o esposti a violazioni delle normative sulla privacy come HIPAA, GDPR, CJIS o CCPA

Rilevamento tempestivo degli incidenti: ricezione di avvisi se vengono rilevati controlli disabilitati e manomissioni dei dispositivi e possibilità di sapere quando i dispositivi che contengono dati finiscono nel posto sbagliato

Report sui dispositivi mancanti: rilevamento dei dispositivi rimasti offline per un certo periodo di tempo e possibilità di contrassegnarli come mancanti per ricevere un avviso appena si connettono a Internet

Protezione dei dati di emergenza: blocco o cancellazione da remoto dei dispositivi compromessi con emissione di un certificato di sanificazione, prevenzione del trasferimento dei dati ed esecuzione su larga scala di molte altre azioni correttive

Esperti in indagini: utilizzo ottimale del team Absolute di investigatori esperti che collaborano a stretto contatto con le forze dell'ordine per indagare, recuperare un dispositivo rubato o identificare l'utente tramite strumenti forensi

Prova di conformità: utilizzo ottimale dei log cronologici per convalidare che la protezione dei dati fosse attiva durante gli incidenti e per scoprire la root cause al fine di iterare le policy di sicurezza

Ulteriori informazioni sono disponibili sul sito DellEMC.com/endpointsecurity

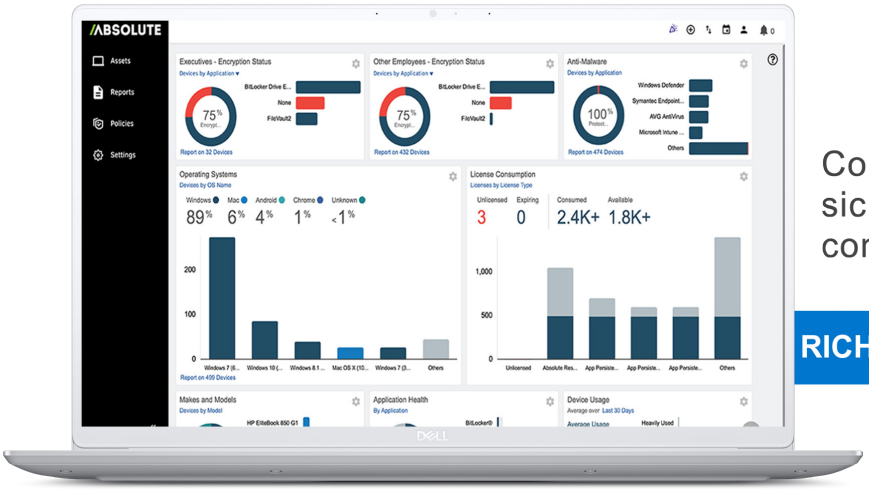
© 2022 Dell Technologies e sue società controllate.

ABSOLUTE®

MASSIMA SICUREZZA GARANTITA DEGLI ENDPOINT

Le organizzazioni distribuite di oggi richiedono visibilità e controllo persistenti degli endpoint. Per stare al passo con la forza lavoro mobile e rendere resiliente l'organizzazione, i team IT e addetti alla sicurezza si affidano alla potente combinazione di asset intelligence, sicurezza resiliente degli endpoint e risposta affidabile ai rischi. Contano sulla piattaforma Absolute.

Per ulteriori informazioni sulle funzionalità di Absolute, visitare il sito absolute.com/platform



Come trasformare l'IT e la sicurezza dell'organizzazione con Absolute

RICHIESTA DI UNA DEMO

Absolute Resilience: una soluzione unica per rendere indistruttibili app e strumenti per la sicurezza

Absolute Resilience contiene tutte le funzioni di visibilità e controllo, tra cui un flusso persistente di dati, inventari automatizzati e la capacità di cancellare i dati o bloccare i dispositivi a rischio.

Persistenza delle applicazioni

Le applicazioni mission-critical possono eseguire le attività di correzione e reinstallazione automatiche dopo un tentativo di disabilitarle, rimuoverle o riconfigurarle.

Rilevamento dati degli endpoint

Impostazione di policy per analizzare i dispositivi Windows e Mac o i dati sensibili a rischio, inclusi PII, PHI, PFI, SSN, GDPR e proprietà intellettuale, all'interno o all'esterno della rete, e successiva stima del costo dell'esposizione.

Portata di Absolute

Valutazione e adozione di azioni correttive in tutti i dispositivi Windows e Mac con una libreria di script predefiniti e personalizzati.

Indagini

Il team Absolute, composto da ex professionisti delle forze dell'ordine, rintraccia i dispositivi smarriti o rubati, quindi collabora con le agenzie locali per recuperarli.

Ulteriori informazioni sono disponibili sul sito DellEMC.com/endpointsecurity

© 2022 Dell Technologies e sue società controllate.

ABSOLUTE®

	Absolute Visibility	Absolute Control	Absolute Resilience
Console Absolute	●	●	●
Monitoraggio dell'hardware	●	●	●
Misurazione dell'utilizzo dei dispositivi	●	●	●
Monitoraggio del software installato	●	●	●
Valutazione del profilo di sicurezza	●	●	●
Monitoraggio dello stato delle applicazioni critiche	●	●	●
Integrazione con terze parti	●	●	●
Rilevamento dello spostamento non autorizzato dei dispositivi		●	●
Blocco remoto dei dispositivi		●	●
Eliminazione remota dei dati		●	●
Abilitazione della protezione del firmware		●	●
Self-healing delle applicazioni critiche			●
Individuazione di informazioni sensibili sui dispositivi			●
Esecuzione di query e correzione da remoto dei dispositivi su larga scala			●
Ricerca e ripristino dei dispositivi rubati			●

Piattaforme supportate:

Contattare gli esperti per la sicurezza degli endpoint Dell dedicati all'indirizzo endpointsecurity@dell.com per saperne di più sui prodotti Dell SafeData che possono migliorare il profilo di sicurezza dell'azienda

Ulteriori informazioni sono disponibili sul sito DellEMC.com/endpointsecurity

© 2022 Dell Technologies e sue società controllate.

ABSOLUTE®

DELL Technologies