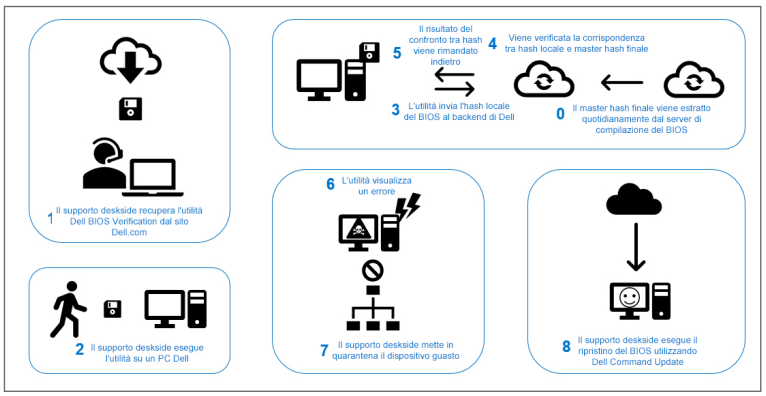
Dell SafeBIOS

PROTEZIONE INTEGRATA SUI PC COMMERCIALI PIÙ SICURI DEL SETTORE

DELL SAFEBIOS RIDUCE IL RISCHIO DI MANOMISSIONI DEL BIOS ATTRAVERSO IL RILEVAMENTO INTEGRATO DEGLI ATTACCHI AL FIRMWARE

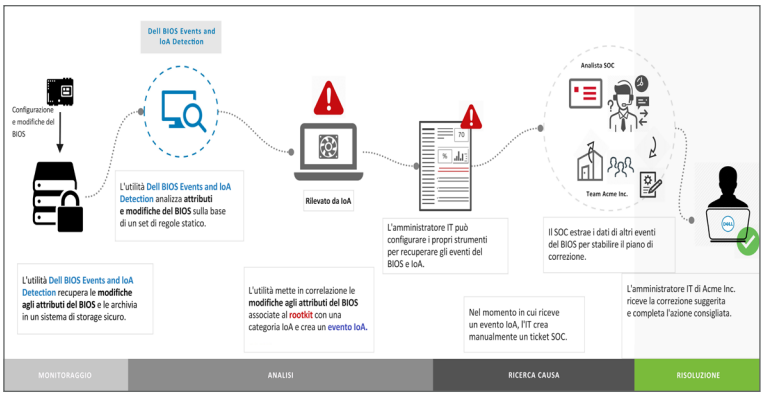
Avviso di manomissione del BIOS più efficiente

Proteggere i dati aziendali, che si tratti della proprietà intellettuale o delle informazioni di identificazione personale (PII, Personally Identifiable Information) del cliente, è di fondamentale importanza sotto il profilo della sicurezza dei dati. Dal momento che le minacce comuni vengono bloccate con maggiore frequenza, i criminali informatici sono alla continua ricerca di metodi più avanzati per acquisire le informazioni cruciali, mentre gli hacker utilizzano tecniche sempre più sofisticate. Grazie a innovative soluzioni per la sicurezza degli endpoint, come ad esempio gli antivirus di nuova generazione e i sistemi EDR (Endpoint Detection and Response) gestiti, i vettori di attacco si stanno riducendo e gli avversari sono quindi costretti a trovare punti di invasione alternativi.



La protezione del BIOS è un aspetto importante nell'ambito della strategia di sicurezza di un'organizzazione.

Le soluzioni per la sicurezza degli endpoint più comuni si concentrano principalmente sul sistema operativo locale e sulle applicazioni installate su di esso, lasciando il livello più basso dello stack informatico, ovvero il BIOS, vulnerabile ad attacchi malevoli che possono mettere fuori uso l'intero sistema. Quando un malware attacca il BIOS, prende possesso di tutto il PC e può accedere alla rete. La compromissione del BIOS ha un impatto estremamente elevato, in quanto viene attaccata la radice di attendibilità del PC e la persistenza è quindi significativa. Se un malintenzionato riesce ad accedere al BIOS, tutte le funzionalità di sicurezza degli endpoint di un dispositivo potrebbero risultare compromesse, così come l'intera rete aziendale. Questo tipo di attacco è particolarmente tecnico e, se messo in atto, crea molti danni. Tale vulnerabilità a livello di accesso desta sempre più preoccupazione in quanto i pirati informatici cercano nuovi vettori di attacco.



Dell SafeBIOS: la risposta al cambiamento paradigmatico sul fronte della sicurezza

Poiché gli attacchi che interessano direttamente il BIOS sono sempre più frequenti e i nuovi malware sono in grado di reinstallarsi all'interno del BIOS, le organizzazioni necessitano di metodi più sofisticati non solo per proteggere i sistemi in uso, ma anche per verificare che questi non siano stati compromessi.

Grazie alla verifica post-avvio integrata nei PC commerciali di Dell, l'IT ha la certezza che il BIOS dei dispositivi utilizzati dai dipendenti non sia stato alterato. Anziché archiviare le informazioni del BIOS sull'hardware stesso, soggetto a possibili danneggiamenti, Dell SafeBIOS offre funzionalità di verifica off-host del BIOS. Dell SafeBIOS utilizza un ambiente cloud protetto per confrontare le singole immagini del BIOS con i dati ufficiali presenti nel BIOS Lab.

Dell SafeBIOS

Inoltre, Dell automatizza il rilevamento precoce degli eventi del BIOS, degli indicatori di attacco e delle configurazioni ad alto rischio fornendo visibilità sulla cronologia di configurazione del BIOS. I continui processi di estrazione e analisi delle configurazioni e degli eventi del BIOS fanno emergere gli endpoint vulnerabili e avvisano l'IT nel momento in cui il rischio aumenta, consentendo ai tecnici di apportare le correzioni necessarie.

In caso di danneggiamento o manomissione del BIOS, Dell offre ai clienti opzioni flessibili per ricreare l'immagine. In questo modo è possibile analizzare il BIOS contaminato allo scopo di comprendere la natura dell'attacco e permettere così ai clienti di verificare la sua integrità utilizzando procedure off-host, senza interrompere il processo di avvio. Dell SafeBIOS offre ulteriore visibilità sulle modifiche apportate al BIOS, oltre a garanzie aggiuntive per tenere a distanza le minacce.

Inoltre, nel caso in cui il BIOS venga compromesso, la relativa immagine viene acquisita automaticamente per l'analisi e la correzione in seguito al ripristino del BIOS stesso.

Integrazioni dei partner
Queste funzionalità combinate consentono di identificare e correggere più rapidamente i potenziali rischi. L'opzione standalone è attualmente disponibile con il supporto Dell.

VMware Workspace ONE fornisce ai team di gestione IT ulteriore visibilità sullo stato del BIOS per la gestione unificata degli endpoint. Grazie all'integrazione con VMware Workspace ONE, l'IT può configurare flussi di lavoro automatizzati per l'esecuzione di aggiornamenti OTA (Over the Air) e il ripristino dei dispositivi nel rispetto della conformità.

Combinati tra loro, VMware Carbon Black Audit and Remediation e Dell SafeBIOS offrono elevati livelli di sicurezza sia al di sopra che al di sotto del sistema operativo, consentendo anche la telemetria dello stato di verifica del BIOS off-host sui PC commerciali Dell. Con questa soluzione integrata, i team IT e di sicurezza possono automatizzare il reporting dello stato di verifica e intraprendere azioni per correggere eventuali problemi derivanti da manomissioni del BIOS. L'integrazione tra questi due prodotti consolida la posizione di Dell come fornitore dei PC commerciali più sicuri del settore.

Dell SafeBIOS fa parte del più ampio portafoglio di prodotti per la sicurezza degli endpoint Dell Trusted Devices, che include soluzioni che supportano gli endpoint sia al di sopra che al di sotto del sistema operativo, per un approccio completo alla protezione dei dati. Tali soluzioni comprendono:

- SafeBIOS: ottieni visibilità sugli attacchi nascosti e latenti tramite l'invio di avvisi in caso di manomissione del BIOS con le esclusive funzionalità offerte da Dell, tra cui la verifica off-host del BIOS[1], l'acquisizione dell'immagine del BIOS, i relativi eventi e gli indicatori di attacco.
- SafeID: solo Dell protegge le credenziali degli utenti finali in un chip di sicurezza dedicato, tenendole nascoste dai malware che ricercano e rubano le credenziali.
- SafeScreen: gli utenti finali possono lavorare ovunque mantenendo le loro informazioni private grazie a questa tecnologia integrata, che limita la visibilità del display a scopo di privacy.
- SafeData: proteggi i dati sensibili sui dispositivi per rispettare le normative in materia di conformità e preservare le informazioni nel cloud, offrendo agli utenti finali la possibilità di collaborare liberamente in tutta sicurezza.
- SafeGuard and Response (con tecnologia VMware Carbon Black e Secureworks): assicura la produttività ed evita eventuali interruzioni e defezioni che un attacco può causare prevenendo e rilevando malware avanzati o attacchi informatici e garantendo al contempo una risposta adeguata.

Contatta oggi stesso un esperto nella protezione degli endpoint di Dell inviando una e-mail all'indirizzo endpointsecurity@dell.com per discutere di come migliorare la strategia di sicurezza aziendale.

[1] In base ad analisi interne.