DELL Technologies

Dell Trusted Device

I PC commerciali più sicuri del settore[1]

Dell Technologies è consapevole che per affrontare le sfide di sicurezza odierne è importante gestire il panorama delle minacce in evoluzione con un ambiente di lavoro moderno. I criminali informatici sfruttano attacchi sofisticati per colpire più vulnerabilità. Una strategia di sicurezza dell'endpoint efficace deve considerare l'intera superficie di attacco. È per questo che Dell adotta un approccio completo per la protezione dei dispositivi sopra e sotto il sistema operativo per garantire una resilienza ottimale e dispositivi affidabili.

Sopra il sistema operativo:
la sicurezza integrata è parte del piano.

Protezione, rilevamento e risposta agli attacchi informatici con **Dell SafeGuard and Response**.

Protezione dei dati sul dispositivo e nel cloud con **Dell SafeData**.

Rilevamento della manomissione del BIOS con **Dell SafeBIOS**.

Garanzia di un hardware privo di manomissioni alla consegna con **Dell SafeSupply Chain**.

Sotto il sistema operativo:
la sicurezza intrinseca è inclusa nella progettazione.

Protezione delle credenziali utente con **Dell SafeID**.

Le informazioni restano private con **Dell SafeScreen** e **Dell SafeShutter**.

La protezione invisibile e continua garantisce esperienze più intelligenti e veloci.

I Dell Trusted Device creano una base sicura per la moderna forza lavoro mobile. La nostra famiglia completa di soluzioni per la sicurezza degli endpoint opera congiuntamente per proteggere i dispositivi sia sopra che sotto il sistema operativo. Questa potente combinazione mantiene i dati al sicuro e gli utenti produttivi, indipendentemente da dove scelgono di lavorare.

Sopra il sistema operativo

Contrastare gli attacchi informatici con Dell SafeGuard and Response.

Il portafoglio Dell SafeGuard and Response, basato su VMware® Carbon Black e Secureworks®, fornisce un approccio completo alla gestione delle minacce per l'endpoint. L'intelligenza artificiale e l'apprendimento automatico rilevano e bloccano in modo proattivo gli attacchi all'endpoint, mentre gli esperti di sicurezza aiutano a ricercare e neutralizzare le minacce identificate nell'endpoint, nella rete e nel cloud.

Protezione dei dati sul dispositivo e nel cloud con Dell SafeData.

Gli utenti possono collaborare in modo sicuro da qualsiasi luogo. Dell Encryption offre funzionalità di sicurezza granulari per crittografare tutti i dati sull'unità, i dati condivisi tra più utenti e i dati dei singoli utenti con più chiavi di crittografia, il tutto gestito da un'unica dashboard per soddisfare i requisiti di conformità. Netskope adotta un approccio incentrato sui dati per la sicurezza e l'accesso al cloud, proteggendo i dati e gli utenti ovunque si trovino, mentre Absolute offre all'IT visibilità, protezione e continuità al di fuori del firewall aziendale.

Sotto il sistema operativo

Rilevamento di manomissioni con Dell SafeBIOS.

Gli attacchi al BIOS sono notoriamente difficili da identificare. Dell SafeBIOS avverte l'utente in caso di manomissione del BIOS affinché possa agire rapidamente per mettere in quarantena ed esaminare il dispositivo. Con l'esclusiva verifica esterna all'host di Dell, l'immagine di confronto rimane in una posizione protetta e separata per consentire le analisi forensi successive all'attacco.[1]

Garanzia di un hardware privo di manomissioni alla consegna con Dell SafeSupply Chain.

I Dell Trusted Device sono costruiti con controlli di sicurezza e integrità leader del settore lungo tutta la supply chain. I sigilli antimanomissione assicurano che il dispositivo arrivi in uno stato non alterato. Per i sistemi ad alto valore, è possibile resettare il disco rigido alle specifiche NIST per garantire un'immagine aziendale pulita e come nuova.

Protezione delle credenziali utente con Dell SafeID.

Solo Dell protegge le credenziali utente in un chip di sicurezza dedicato, tenendole nascoste dai malware che ricercano e rubano le credenziali[1].

Le informazioni restano private con Dell SafeScreen e Dell SafeShutter.

Gli utenti possono lavorare da qualsiasi luogo mantenendo al sicuro le informazioni private.

Per ulteriori informazioni, visitare il sito: Delltechnologies.com/endpointsecurity o contattare subito il proprio esperto per la sicurezza degli endpoint Dell all'indirizzo endpointsecurity@dell.com.

[1] Dati basati su analisi interne Dell, gennaio 2020.