DELL Technologies

Migliorare la maturità della sicurezza informatica e della resilienza

La maturità della sicurezza informatica è una leva strategica per ogni azienda moderna

Il panorama delle minacce informatiche di oggi è più dinamico e spietato che mai, con attacchi basati dall'AI sempre più frequenti, veloci e sofisticati. Le organizzazioni non possono più contare su difese frammentarie o aggiornamenti incrementali.

I leader aziendali devono agire come se una violazione fosse inevitabile, se non imminente. Dell Technologies aiuta i clienti ad aumentare la propria maturità in termini di sicurezza, la fiducia nel gestire l'azienda di fronte al rischio informatico. A tale scopo, promuoviamo un approccio alla sicurezza informatica e alla resilienza completo e stratificato basato su tre aree di applicazione cruciali.

Le aziende devono disporre di funzionalità per:

- **Ridurre la superficie di attacco**
- **Rilevare e rispondere alle minacce informatiche**
- **Effettuare il ripristino dagli attacchi informatici**

La sicurezza informatica efficace inizia valutando onestamente il profilo di sicurezza e la maturità attuali. Grazie a questa trasparenza, dai priorità ai miglioramenti giusti e investi in un futuro più sicuro.

Riduci la superficie di attacco

La superficie di attacco di un'organizzazione è dinamica e in rapida evoluzione, con l'introduzione di nuovi vettori di attacco da parte dell'AI. Insieme al lavoro remoto e ai sistemi legacy, estendono la superficie di attacco, creando più punti di ingresso per gli attori delle minacce. Per questo motivo, limitare questa superficie è una necessità strategica per ridurre i rischi, rispettare gli obblighi di conformità, proteggere la resilienza organizzativa e creare fiducia di base.

Migliorare la maturità della sicurezza informatica e della resilienza

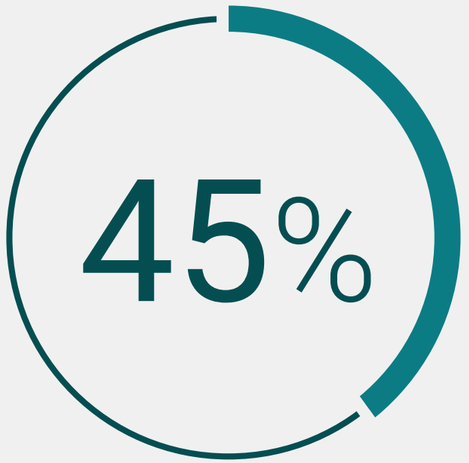
Il ridimensionamento della superficie di attacco diminuisce il rischio complessivo riducendo al minimo i punti di ingresso che gli autori degli attacchi possono sfruttare. Questo rafforza la maturità della sicurezza e semplifica le attività di conformità. Il risultato è una maggiore resilienza, una riduzione dei costi derivante dalla diminuzione degli incidenti e la capacità di muoversi più velocemente, innovare più liberamente ed entrare in nuovi mercati con la certezza che la sicurezza è integrata fin dall'inizio. Inizia con l'adozione dei principi Zero Trust (mai fidarsi, verificare sempre) e l'applicazione di privilegi minimi per utenti, dispositivi e applicazioni.

In Dell Technologies, adottiamo una mentalità basata sul concetto di "sicurezza fin dalla progettazione". La sicurezza informatica è integrata in tutto ciò che facciamo, a partire dalla nostra supply chain globale sicura e fino alle protezioni integrate nei nostri prodotti principali. Queste protezioni iniziano a livello di hardware per garantire che i dispositivi avviino ed eseguano solo software attendibili. Allineiamo le nostre soluzioni ai principi Zero Trust, aiutandoti a eliminare le vulnerabilità prima che gli autori degli attacchi possano sfruttarle. I nostri AI PC commerciali più sicuri al mondo[1], ad esempio, forniscono difese fondamentali per l'ambiente di lavoro moderno.

La riduzione della superficie di attacco aumenta la maturità della sicurezza eliminando l'incertezza: meno incognite, meno punti di ingresso e meno sorprese.

Risultati principali dei clienti:

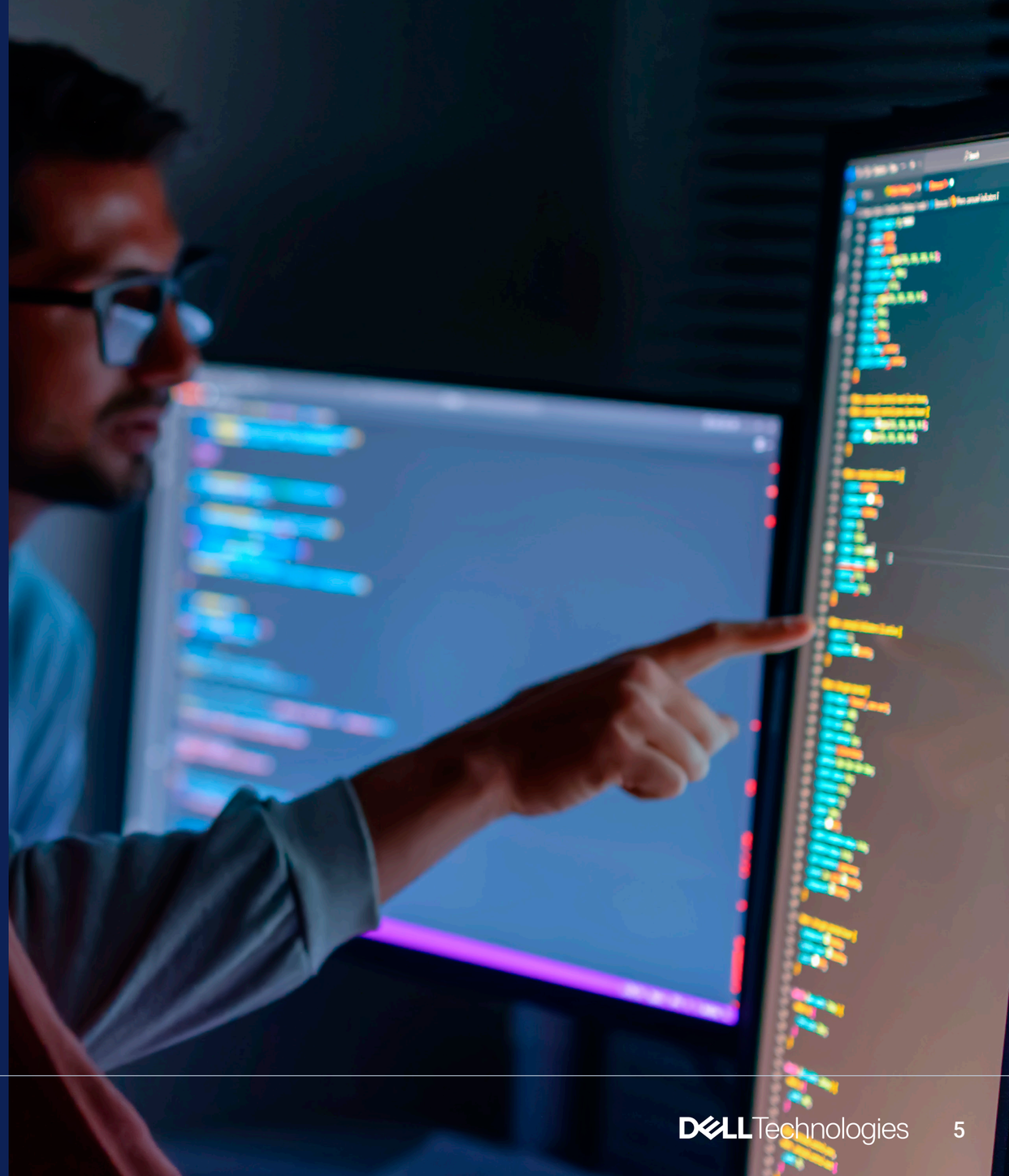
- **Riduzione al minimo delle vulnerabilità:** rafforzando in modo proattivo endpoint, infrastruttura e applicazioni, è possibile ridurre drasticamente le opportunità per gli autori di attacchi informatici.
- **Gestione della sicurezza semplificata:** meno asset esposti vuol dire meno controlli da gestire, il che determina un profilo di sicurezza più semplificato ed efficiente.
- **Fondamenta più solide per l'innovazione:** con endpoint affidabili e dati protetti, è possibile adottare nuove tecnologie come l'AI e l'edge computing in tutta sicurezza.



Le organizzazioni che si concentrano sulla riduzione della superficie di attacco diminuiscono del 45% il rischio di violazione informatica nella gestione delle esposizioni esterne.[2]

Rileva e affronta le minacce informatiche

Nel mondo della sicurezza informatica, velocità e intelligence vanno di pari passo. Rilevamento e risposte efficaci permettono di identificare e contenere rapidamente le minacce, riducendo il tempo di permanenza e limitando i danni di un attacco. Il risultato è una riduzione dei costi, un downtime ridotto e una maggiore fiducia operativa sapendo che l'azienda può continuare a operare in modo sicuro anche in caso di minacce continue.



Migliorare la maturità della sicurezza informatica e della resilienza

Tuttavia, molte organizzazioni hanno difficoltà a causa della visibilità limitata negli ambienti ibridi e un volume eccessivo di avvisi. Oggi gli autori di attacchi rimangono all'interno delle reti per una media di 11 giorni prima di essere scoperti. Per ovviare a questo problema, è necessario avere visibilità in tempo reale su endpoint, reti e sistemi attraverso monitoraggio continuo, Threat Intelligence e automazione.

I partner di sicurezza affidabili forniscono competenze specializzate su Threat Intelligence e risposta agli incidenti. Dell combina analisi avanzate, rilevamento delle minacce basato su AI/ML e servizi gestiti 24x7 con una base hardware sicura per identificare e contenere le minacce prima che causino interruzioni. I servizi opzionali come Managed Detection and Response (MDR) forniscono competenza in materia di sicurezza per espandere la visibilità, rispondere rapidamente e mitigare le minacce.

Le solide funzionalità di rilevamento e risposta aumentano la maturità della sicurezza, riducendo i tempi di permanenza e fornendo ai team la sicurezza di agire in modo deciso quando emergono minacce.

Risultati principali dei clienti:

- **Rilevamento più rapido e tempi di permanenza più brevi:** Managed Detection and Response (MDR) è in grado di ridurre del 25-49% il tempo medio di rilevamento e risposta, diminuendo la probabilità che un attacco diventi più grave.
- **Riduzione del carico operativo:** la collaborazione con esperti per la ricerca proattiva delle minacce e il monitoraggio continuo sollevano il carico dai team interni, rendendoli disponibili per attività strategiche.
- **Maggiore resilienza:** le funzionalità di rilevamento e risposta mature determinano un minor numero di incidenti di sicurezza ed evitano costi più elevati correlati alle violazioni.

$4,44M

Il costo medio di una violazione dei dati ha raggiunto $ 4,44 milioni nel 2025.[3]

Ripristino da un attacco informatico

Quando si verifica lo scenario peggiore, l'obiettivo primario è un ritorno alle operazioni il più rapidamente possibile con interruzioni minime. Il ripristino da un attacco informatico garantisce la capacità di recuperare dati e sistemi puliti in tempi rapidi, riducendo i danni alla reputazione e offrendo la certezza di un recupero affidabile e senza reinfezioni.

Migliorare la maturità della sicurezza informatica e della resilienza

Anche costruendo le difese più forti possibili, bisogna prevedere un attacco come un evento inevitabile. Disporre di un piano e di funzionalità di ripristino completi è fondamentale. Questo prevede l'esecuzione di backup puliti e immutabili dei dati critici in un vault di ripristino isolato e l'utilizzo di ambienti clean room per verificare che i sistemi ripristinati siano privi di malware prima di tornare online.

Dell integra funzionalità di ripristino all'interno dei propri prodotti, perché far tornare le aziende operative è la nostra priorità quando si verificano incidenti. Soluzioni come il vault PowerProtect Cyber Recovery isolano e proteggono le copie pulite dei dati critici per un ripristino rapido, limitando le perdite ed eliminando gli attacchi ransomware. Questa architettura aiuta a far tornare rapidamente online i carichi di lavoro critici, offrendo la massima tranquillità.

Il ripristino è spesso il momento in cui la maturità della sicurezza viene realmente messa alla prova: quando la fiducia dipende dalla rapidità e dalla pulizia con cui l'azienda riesce a tornare alla normale operatività.

Risultati principali dei clienti:

- **Impatto ridotto sul business:** le organizzazioni con un piano di risposta agli incidenti ben collaudato possono ridurre i costi delle violazioni di circa il 61%.
- **Ripresa più veloce delle operazioni:** dare priorità a un rapido ritorno al business, non solo alla rimozione delle minacce, aiuta a ripristinare le operazioni con interruzioni e costi minimi.
- **Maggiore integrità dei dati:** l'isolamento dei dati critici, l'utilizzo di copie immutabili e la convalida dell'integrità prima di un ripristino rafforzano la fiducia nel processo di recupero.

delle organizzazioni ha ammesso di avere difficoltà a eseguire il ripristino da un attacco informatico rispettando al contempo gli accordi sui livelli di servizio.[4]

Rafforzamento della maturità della sicurezza tramite partnership strategiche

I partner esperti sono essenziali per esplorare il panorama della sicurezza informatica complesso e in rapida evoluzione di oggi. Le minacce informatiche stanno diventando sempre più sofisticate e frequenti, rendendo quasi impossibile per un'organizzazione sola mantenere le competenze, le risorse e le tecnologie necessarie per rimanere al passo. Collaborando con leader della sicurezza come Dell, le aziende hanno accesso a competenze specializzate, tecnologie all'avanguardia e una rete di partner di fiducia. Queste partnership forniscono il supporto e le competenze necessarie per rilevare, prevenire e rispondere alle minacce in modo efficace, garantendo la protezione delle aziende in un ambiente digitale in continua evoluzione.

Con il giusto approccio in queste tre aree di applicazione, le organizzazioni incrementano la maturità in termini di sicurezza, creando la fiducia necessaria per operare, innovare e crescere nonostante la costante pressione informatica. Dell unisce un'infrastruttura affidabile, un ambiente di lavoro sicuro, servizi avanzati e un ecosistema dei partner per aiutare la tua organizzazione a rimanere protetta, flessibile e resiliente, pronta per il futuro.

Scopri le soluzioni per la sicurezza

Domande frequenti

1. Perché la sicurezza informatica dovrebbe essere una priorità assoluta per la mia azienda?
La sicurezza informatica non è solo protezione; è la base che permette a un'azienda di innovare e crescere, resistendo alle minacce di un panorama digitale pericoloso. Un solido profilo di sicurezza non riguarda solo la difesa, ma anche l'operatività. Le aziende con framework di sicurezza informatica maturi possono muoversi più velocemente, innovare più liberamente ed entrare in nuovi mercati in tutta sicurezza. Sono meglio attrezzate per gestire i cambiamenti normativi, le esigenze dei clienti e le pressioni dei competitor.

2. Come si può bilanciare la necessità di una sicurezza rigorosa con la libertà di innovare?
Non è necessario scegliere tra sicurezza e innovazione. Crediamo che una solida sicurezza favorisca effettivamente l'innovazione. Quando si dispone di una base "sicura fin dalla progettazione", in cui la sicurezza è integrata nei dispositivi, nell'infrastruttura e nei dati fin dall'inizio, i team hanno la possibilità di adottare nuove tecnologie come l'AI e l'edge computing con piena fiducia.

3. Perché la sicurezza della supply chain è così fondamentale?
La vera protezione nasce molto prima di premere il pulsante di accensione. Man mano che l'impronta digitale aumenta, cresce anche l'esposizione e l'affidabilità diventa la prima linea di difesa. Ogni collegamento della supply chain deve essere protetto, poiché un singolo componente compromesso può mettere a repentaglio anche il software più avanzato. È per questo che costruiamo la sicurezza partendo dalle fondamenta, proteggendo ogni fase, dalla produzione alla distribuzione. Dalla fabbrica alla consegna, la tecnologia arriva affidabile, verificata e progettata per funzionare in tutta sicurezza.

4. In che modo Dell ci aiuta a eseguire il ripristino dopo un attacco informatico?
Ridurre al minimo il downtime e le interruzioni è fondamentale quando si verificano incidenti. La preparazione è la chiave. Il nostro vault PowerProtect Cyber Recovery isola una copia pulita e immutabile dei dati più critici, separata in modo sicuro dall'ambiente primario. In caso di incidente, è possibile ripristinare le operazioni in modo veloce e sicuro senza compromessi e senza pagare un riscatto.
Dell offre una varietà di prodotti e servizi progettati per aiutarti a implementare una strategia di ripristino completa. La gamma di servizi offerti va dalla consulenza per la creazione di un piano di recupero e formazione alle funzionalità di protezione dei dati che possono mantenere al sicuro i dati critici. Dell adotta un approccio incentrato sulle persone e sulla tecnologia, garantendo la collaborazione tra dipendenti e tecnologia per un ripristino rapido.

5. Dell può fornire assistenza per il rilevamento delle minacce in tempo reale?
Assolutamente. La velocità è fondamentale quando si tratta di fermare una minaccia informatica. Combiniamo funzionalità di protezione integrate con servizi avanzati come Managed Detection and Response (MDR) per monitorare l'ambiente 24 ore su 24, 7 giorni su 7. Attraverso l'analisi di dati basata su AI/ML e le competenze umane, ti aiutiamo a rilevare immediatamente potenziali anomalie e minacce, per rispondere tempestivamente e arginare i problemi prima che influiscano sulla tua attività.

Fonti

[1] Dati basati su analisi interne Dell, ottobre 2024 (Intel) e marzo 2025 (AMD). Applicabile ai PC con processori Intel e AMD. Non tutte le funzionalità sono disponibili per tutti i PC. Sono necessari ulteriori acquisti per alcune funzionalità. PC basati su Intel convalidati da Principled Technologies, luglio 2025 Infografica Anatomia di un dispositivo affidabile

[2] Forrester Consulting, "The Total Economic Impact™ of BitSight: Cost Savings and Business Benefits Enabled by BitSight", ottobre 2024.

[3] IBM e Ponemon Institute, "Cost of a Data Breach Report 2025: The AI Oversight Gap", 2025.

[4] Dell Technologies, "Advance Cybersecurity Maturity: Technology Infrastructure is the Heartbeat of Every Modern Business", febbraio 2025.

Informazioni su Dell Technologies

Dell Technologies (NYSE: DELL) supporta aziende e privati nel creare il proprio futuro digitale e trasformare il proprio modo di lavorare, esistere e interagire. L'azienda fornisce ai clienti il portafoglio di tecnologie e servizi più ampio e innovativo del settore per l'era dell'AI.

Ulteriori informazioni sono disponibili sul sito Dell.com