Bitdefender®

GravityZone

GUIDA ALLA SOLUZIONE

Semplifica le tue operazioni di sicurezza e riduci i rischi

E se tutto ciò che ci è stato detto sulla cybersecurity fosse sbagliato? E se aggiungere livelli non rende la nostra organizzazione più sicura ma aumenta la nostra vulnerabilità? La realtà è che molti dei nostri sistemi sono diventati così complessi da diventare ora le nostre maggiori debolezze.

Ogni nuovo strumento di sicurezza promette protezione, ma crea anche confusione e punti ciechi. I criminali informatici non stanno sfondando le nostre pareti, ma stanno scivolando tra le crepe che abbiamo creato. Il World Economic Forum lo conferma, affermando: "Il cyberspazio è più complesso e impegnativo che mai a causa dei rapidi progressi tecnologici, della crescente sofisticazione dei criminali informatici e delle catene di approvvigionamento profondamente interconnesse."

Il futuro della cybersecurity non è aggiungere di più. Si tratta di semplificare la sicurezza, eliminare il superfluo e concentrarsi su ciò che è davvero importante.

Perché le attuali minacce informatiche sono più difficili da rilevare e fermare

È una storia già nota: ogni giorno, le minacce di cybersecurity si evolvono, diventando sempre più avanzate e difficili da contrastare. Le organizzazioni operano in ambienti vasti e interconnessi con migliaia di asset. Ogni nuova iniziativa aziendale aggiunge più endpoint, flussi di dati e dipendenze. E sebbene aggiungano valore, introducono anche molti rischi.

Man mano che l'ambiente cresce, la visibilità dell'IT si frammenta. È quasi impossibile correlare dati tra più fonti disparate. Il tuo team di sicurezza e IT snello fatica a collegare le informazioni, rischiando di trascurare punti ciechi che gli aggressori possono sfruttare rapidamente.

Allo stesso tempo, gli aggressori hanno evoluto i loro piani di attacco. Gli aggressori non si affidano più esclusivamente alla forza bruta o agli approcci zero-day. Al contrario, hanno perfezionato le tecniche living-off-the-land, combinando le loro azioni dannose con strumenti e processi legittimi già presenti nei sistemi delle organizzazioni.

Il risultato è che le intrusioni sono molto più facili da eseguire per gli aggressori e molto più difficili da rilevare per i team IT. Anche attacchi relativamente rudimentali, quando eseguiti con precisione e furtività, possono causare conseguenze devastanti se superano le difese abbastanza a lungo. Nel frattempo, gli aggressori stanno integrando automazione e intelligenza artificiale nei propri strumenti, ampliando così la loro portata e accelerando la velocità con cui possono identificare le vulnerabilità, sfruttare le falle e intensificare le loro campagne.

Questa sfida è aggravata dal fatto che le minacce odierne raramente sono isolate a un singolo punto di attacco. Per progettazione, sono multifunzionali, agendo contemporaneamente su più livelli aziendali. Per esempio, gli hacker possono partire da un'e-mail di phishing, passare all'escalation dei privilegi, sfruttare risorse cloud configurate male e, infine, eseguire movimenti laterali tra gli endpoint. Ogni livello rinforza il successivo, creando una catena di eventi molto più difficile da rompere una volta che è iniziata.

Questo approccio multilivello significa che l'impatto di un attacco non è più confinato a un singolo sistema o dipartimento. Per esempio:

- I ransomware spesso disattivano i backup, esfiltrando contemporaneamente dati sensibili per una doppia estorsione.
- Le campagne Business Email Compromise (BEC) possono andare ben oltre una casella di posta compromessa, spesso coinvolgendo frodi finanziarie o infiltrazioni nella supply chain.

Poiché gli aggressori possono sfruttare più vettori contemporaneamente, aumenta la loro probabilità di successo e il potenziale impatto sulle attività aziendali. Il risultato è una tempesta perfetta: ambienti aziendali sempre più complessi che si scontrano con avversari sempre più efficienti. E senza la giusta visibilità, comprensione e capacità di risposta, le organizzazioni faticano a determinare il modo migliore per dare priorità agli sforzi di protezione.

Più strumenti = Più rumore

Gli attuali ambienti aziendali ultra-complessi hanno messo sotto pressione senza precedenti i team di sicurezza. Ogni nuovo dispositivo, applicazione o servizio cloud porta con sé il proprio insieme di avvisi, log e vulnerabilità. Per stare al passo, la maggior parte delle organizzazioni ha adottato una serie di strumenti di sicurezza, tra cui:

- Endpoint detection and response
- Firewall
- Identity protection
- Sicurezza cloud e SaaS
- Gestione delle vulnerabilità
- E altro ancora

Certamente, ogni strumento ha un determinato scopo. Ma cercare semplicemente di unirli in una difesa coesa spesso crea più problemi di quanti ne risolva. Perché?

- **Dati disparati:** ogni piattaforma genera i propri formati di dati, sistemi di avvisi e dashboard. Il tuo team di sicurezza è costretto a dedicare molto tempo a conciliare schemi incoerenti ed eventi duplicati invece di concentrarsi sulle minacce ad alta priorità.
- **Ridondanze e rumore:** la sovrapposizione delle funzionalità tra gli strumenti significa che lo stesso evento può attivare più avvisi, sovraccaricando gli analisti e prosciugando il tempo, minando al contempo la fiducia nel processo complessivo di rilevamento.
- **Sfide dell'integrazione:** l'integrazione tra gli strumenti raramente è senza intoppi. Le API cambiano, i connettori si rompono e ottimizzare le regole di correlazione richiede una sforzo ingegneristico continuo che molti team semplicemente non riescono a sostenere.

Man mano che lo stack di sicurezza cresce, la visibilità complessiva in realtà diminuisce. Il 2024 Hybrid Cloud Security Survey di Gigamon ha rilevato che il 41% dei CISO era preoccupato per la diffusione degli strumenti e per le lacune di visibilità e sicurezza che essa creano a causa della mancanza di integrazione semplificata e delle difficoltà nella gestione di ciascun strumento. Invece di vedere un quadro unificato, gli analisti devono districarsi su più console, ognuna delle quali offre una visione parziale dell'ambiente. Questa visibilità isolata rallenta le indagini. I team devono passare da una piattaforma all'altra per ricostruire la sequenza di un attacco, aumentando il tempo medio di rilevamento (MTTD) e il tempo medio di risposta (MTTR).

Per affrontare questo problema, molte aziende si affidano alle piattaforme di Security Information and Event Management (SIEM) e Security Orchestration Automation and Response (SOAR) per centralizzare i dati e automatizzare i flussi di lavoro. Tuttavia, SIEM e SOAR portano con sé complessità aggiuntive, tra cui gli alti costi per l'acquisizione dei log, regole di rilevamento fragili e la necessità di ingegneri specializzati per ottimizzarle e gestirle.

Nel rapporto "State of SIEM Detection Risk" del 2025 di CardinalOps, hanno scoperto che, nonostante l'ingestione di centinaia di fonti di log, i SIEM coprono generalmente solo una frazione delle tecniche avversarie conosciute, lasciando lacune pericolose. Le organizzazioni ancora "non vedono un aumento proporzionale della copertura" quando investono in SIEM per consolidare la diffusione dei loro strumenti.

Quindi, qual è la risposta? Chiaramente, la risposta non è aggiungere più strumenti, ma piuttosto un approccio integrato che riduca la complessità migliorando copertura e risultati.

Bitdefender

Unifica gli strumenti per semplificare la sicurezza

Con minacce in aumento, strumenti frammentati e team snelli sotto pressione, la cybersecurity ora richiede un approccio attento e ben pianificato. Aggiungere prodotti endpoint moltiplica solo il carico di integrazione e amplia il rumore dei dati. Ciò di cui il tuo team di sicurezza ha bisogno è una piattaforma unificata che semplifichi le operazioni, migliori la visibilità, automatizzi rilevamento e risposta, e fornisca le competenze giuste su richiesta.

Parlare la stessa lingua

Una piattaforma di sicurezza unificata combina l'intero spettro di strumenti e capacità di sicurezza sotto un unico tetto, assicurando che parlino tutti la stessa lingua. Invece di console separate e dati isolati, le organizzazioni possono gestire la sicurezza degli endpoint, dell'identità, del cloud, della rete e delle applicazioni SaaS attraverso un unico ambiente integrato.

Questo consolidamento:

- → Riduce la ridondanza
- → Riduce i costi operativi
- → Garantisce che avvisi, log e telemetria fluiscano in un livello centrale di intelligence dove possono essere correlati e analizzati in tempo reale

Il risultato? Operazioni di sicurezza semplificate, con capacità di rilevamento e risposta di maggiore fedeltà su tutta la superficie di attacco.

Prevenzione, protezione, rilevamento e risposta unificate

Una piattaforma di sicurezza unificata rafforza le difese di un'organizzazione portando prevenzione, protezione, rilevamento e risposta in un unico sistema connesso. Invece di trattare queste aree come funzioni separate, la piattaforma correla continuamente la telemetria tra endpoint, identità, carichi di lavoro cloud, reti e applicazioni SaaS. Ciò consente l'identificazione precoce di vulnerabilità, configurazioni errate o attività anomale prima che gli avversari possano sfruttarle, riducendo la probabilità che gli attacchi si spingano più in profondità nell'ambiente.

Prevenzione e protezione sono ulteriormente semplificate attraverso un'applicazione unificata delle policy e la gestione delle vulnerabilità. Configurazioni di base, policy di accesso e controlli di sicurezza possono essere applicati in modo coerente in tutto l'ambiente tramite una singola console. Quando vengono introdotti aggiornamenti alla logica di rilevamento o ai feed di intelligence, vengono distribuiti simultaneamente assicurando che le difese rimangano aggiornate e sincronizzate, migliorando la copertura e semplificando la gestione dei controlli di sicurezza.

Questo consolidamento degli strumenti migliora anche la visibilità, rendendo più facile comprendere la superficie di attacco. Gli analisti possono identificare rapidamente quali risorse hanno più probabilità di essere prese di mira, dare priorità agli sforzi di bonifica basandosi sul rischio reale aziendale e utilizzare il contesto correlato per accelerare le azioni di risposta. Questa connessione end-to-end dalla prevenzione alla risposta garantisce che le minacce vengano fermate prima, le indagini semplificate e la bonifica venga eseguita con maggiore rapidità e sicurezza.

Automazione semplificata e più efficiente

Poiché tutti gli strumenti sono interconnessi, anche il rilevamento e la risposta alle minacce possono essere meglio automatizzati e semplificati, trasformando processi un tempo manuali e soggetti a errori in flussi di lavoro fluidi e affidabili. La piattaforma correla automaticamente dati, eventi e avvisi, generando rilevamenti ad alta fedeltà e avviando automaticamente le azioni di risposta.

Invece di perdere a tempo prezioso a passare da una console all'altra, a gestire avvisi sovrapposti o a tentare integrazioni personalizzate, ricevono avvisi priorizzati e ricchi di contesto. E l'automazione garantisce un enorme ROI: il rapporto 2024 Cost of a Data Breach di IBM ha rilevato che le organizzazioni con automazione della sicurezza completamente implementata contengono le violazioni 74 giorni più velocemente e risparmiano circa il 31% sui costi delle violazioni rispetto alle organizzazioni con automazione minima o nessuna della sicurezza.

Con l'automazione, il tuo team di sicurezza può rilevare le minacce più velocemente (abbassando l'MTTD), convalidare gli incidenti con maggiore confidenza e rispondere in modo più efficace su tutta la catena di attacco. Ciò include l'arricchimento degli avvisi con threat intelligence, la mappatura delle attività in base alle tecniche MITRE ATT&CK, il contenimento delle risorse compromesse e la generazione automatica di rapporti pronti per i controlli. La differenza è trasformativa per team snelli e con risorse limitate: gli analisti sono liberati dal compito ripetitivo dell'identificazione e possono concentrarsi sulla ricerca delle minacce proattiva, nonché la pianificazione della resilienza e i miglioramenti strategici della sicurezza.

L'automazione accelera il rilevamento e la risposta, semplificando al contempo le operazioni di sicurezza, riducendo la complessità e permettendo ai team snelli di operare in modo più efficace.

Rafforzare il tuo team con risorse specializzate

La tecnologia da sola non può mantenere un'organizzazione sicura. I team hanno bisogno anche di migliorare le proprie competenze ed espandere la loro capacità. Per esempio, lavorare con un unico fornitore di managed detection and response (MDR) può rafforzare la propria sicurezza fornendo monitoraggio 24/7, rilevamento delle minacce avanzato e risposta agli incidenti guidata da esperti.

Con MDR, la tua organizzazione ottiene accesso immediato ad analisti esperti, cercatori di minacce specializzati ed esperti forensi che possono convalidare gli avvisi, indagare sugli incidenti e coordinare la risposta, riducendo il tempo medio di rilevamento e risanamento. Quando tutto questo viene combinato con una threat intelligence continua, un monitoraggio del dark web e protezione dei marchi, MDR assicura che anche i team più snelli possano avere una visibilità e una protezione di livello aziendale.

Ma le piattaforme unificate dovrebbero andare oltre il rilevamento e la risposta per offrire servizi preventivi e di consulenza. Considera di sfruttare le offerte di sicurezza offensiva come penetration testing, red teaming e tabletop exercises. Queste misure aiutano le organizzazioni a identificare proattivamente i punti deboli prima che gli aggressori li sfruttino.

I servizi di consulenza possono guidare il tuo team nella costruzione e nella maturazione dei programmi di cybersecurity. Garantiscono inoltre che policy, processi e controlli siano in linea con le esigenze aziendali e i requisiti di conformità.

Favorire una chiara comunicazione e un valore concreto

Infine, una piattaforma unificata non solo semplifica il lavoro dei professionisti della sicurezza, ma trasforma anche il modo in cui le informazioni vengono comunicate in tutta l'azienda. Poiché tutta la telemetria, gli avvisi e i risultati fluiscono in un livello di intelligence centralizzato, la piattaforma può presentare le informazioni in formati su misura per vari tipi di pubblico. Gli analisti beneficiano di avvisi ricchi di contesto e dati forensi dettagliati, mentre dirigenti, membri del consiglio di amministrazione e responsabili della conformità vedono dashboard chiare che evidenziano tendenze, KPI e la postura generale del rischio.

Grazie a questa chiarezza, i non addetti ai lavori possono adempiere ai propri compiti in modo più efficace. I dirigenti possono facilmente comprendere la posizione dell'organizzazione, i consigli di amministrazione possono valutare gli investimenti nella sicurezza con fiducia e i team di conformità possono produrre prove pronte per l'audit senza necessità di traduzione tecnica. La capacità di presentare i risultati di sicurezza in termini semplici e accessibili garantisce che il valore della funzione di sicurezza non sia solo realizzato internamente, ma anche dimostrato esternamente a stakeholder e autorità di regolamentazione.

Il risultato è un programma di sicurezza che non solo è più solido, ma anche più trasparente, responsabile e strategicamente allineato con gli obiettivi aziendali. Grazie alla semplificazione della fruizione delle informazioni, le piattaforme unificate permettono alla sicurezza di trasformarsi da una disciplina puramente tecnica a uno strumento integrato dell'attività.

Progettato appositamente per i team di sicurezza snelli

A differenza di set di strumenti assemblati dai più disparati prodotti di sicurezza, le piattaforme unificate enfatizzano la semplicità, l'integrazione e i risultati misurabili. Questa filosofia di progettazione significa meno interfacce da apprendere, implementazioni più rapide e un livello di automazione che amplifica le capacità dei piccoli team. I team di sicurezza ottengono accesso a capacità di livello aziendale senza il peso di gestire una complessità su scala aziendale. Fornisce capacità di visibilità, prevenzione, protezione, rilevamento e risposta necessarie per difendersi dalle minacce moderne, ma in modo fruibile e sostenibile per team con risorse umane limitate.

I risultati includono un contenimento più rapido delle minacce, una riduzione più proattiva delle vulnerabilità e la garanzia che gli sforzi di sicurezza siano direttamente allineati al rischio aziendale. Riducendo il tempo trascorso sull'identificazione manuale e la manutenzione degli strumenti, i team snelli possono dedicare più energie a iniziative strategiche come la pianificazione della resilienza, la conformità normativa e la reportistica per la dirigenza.

Concentrati su cosa conta di più

Pronti a fare di più con meno? Crea una piattaforma di sicurezza unificata consolidando strumenti tecnologici e collaborando con fornitori di servizi esperti. Invece di essere sommersi da dati e avvisi frammentati, potrai concentrarti su ciò che conta di più: mantenere al sicuro i dati e i sistemi della tua organizzazione.

Cerchi una sicurezza di livello aziendale senza la complessità? Le soluzioni di sicurezza aziendale di Bitdefender possono aiutarti a difenderti dalle minacce e mitigare i rischi in modo proattivo.

LEARN MORE

Data di uscita: ottobre 2025

Per maggiori informazioni, visitare https://www.bitdefender.com.

Sede centrale - Romania
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071

T: +40 21 4412452

Sede centrale - Stati Uniti
(Regus): Bastioni di
Porta Nuova 21,
office no. 308 and 309,
Milan, 20121, Italy