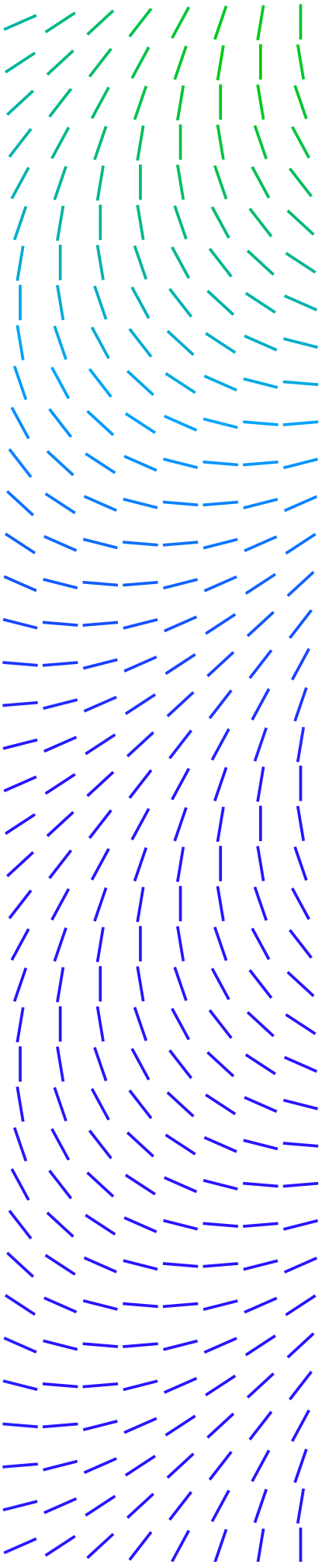
WHITE PAPER



Assumi il controllo delle operazioni di sicurezza (SecOps)

3 passi per un approccio integrato e intelligente che può aiutare a ottimizzare le SecOps

Trellix

Sintesi

Il panorama delle minacce evolve costantemente, e gli strumenti che ieri utilizzavi per proteggere la tua azienda, certamente non la manterranno al sicuro domani.

Strumenti statici e isolati non possono fare più di tanto per proteggere la tua azienda. Organizzazioni come la tua hanno bisogno di un approccio nuovo, che riunisca tutti i tuoi prodotti per la sicurezza per creare un singolo fronte unito.

> Entro il 2025, il 75% delle grandi aziende adotterà una strategia di consolidamento dei fornitori di sicurezza[1]

Con un approccio integrato e intelligente alle attività relative alla sicurezza, puoi:

1. **Migliorare la visibilità**
   Vedere più chiaramente ti consente non solo di rilevare le minacce, ma anche di prevedere gli attacchi.
2. **Accelerare la risposta**
   Integrare i tuoi prodotti e migliorare l'intelligence consente di proteggerti dagli attacchi e rispondere alle minacce in tempo reale.
3. **Migliorare l'efficienza e ridurre i costi**
   Ottimizzare la tua difesa e ridurre al minimo le spese finanziarie e operative ti consente di adattarti in modo proattivo, rafforzare la tua security posture e massimizzare i profitti.

Il momento di agire è ora e la risposta a come aumentare l'efficienza delle tue attività di sicurezza è semplice: integrazione dei prodotti e intelligence.

1. Security Vendor Consolidation Trends — Should You Pursue a Consolidation Strategy? Gartner, 2020

Un'era completamente nuova per le operazioni di sicurezza

Nel mondo dinamico di oggi, ogni giorno si presentano nuove minacce.

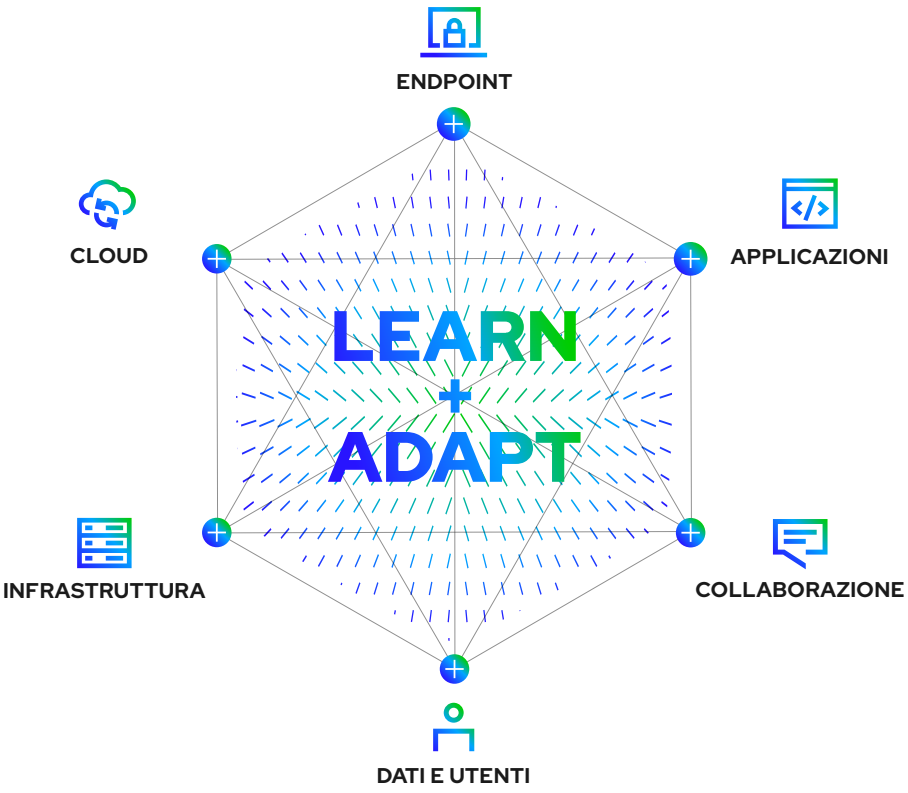
Per prevenirle, molte aziende stanno investendo per migliorare il loro approccio alla sicurezza.

Naturalmente, rafforzare la sicurezza non è facile. Spesso questo comporta notevoli risorse finanziarie, ulteriori risorse umane, maggiore complessità, un numero superiore di processi manuali e - ciò che è peggio - un aumento del rischio se le nuove misure di sicurezza vengono implementate in modo sbagliato.

Fortunatamente, ora esiste un nuovo approccio, più olistico.

Con un approccio integrato alla sicurezza cyber, la tua azienda è meglio preparata per prevedere e prevenire gli attacchi. Ma riunire i prodotti per la sicurezza in una singola soluzione non significa solo protezione, bensì sbloccare efficienze.

In questo white paper scoprirai tre modi attraverso i quali un approccio integrato e intelligente può ottimizzare le attività di sicurezza.



1. Migliora la tua visibilità

Vedere significa proteggere. Punti ciechi nell'infrastruttura possono causare problemi gravi. Una visibilità insufficiente può impedire il rilevamento delle minacce, impedendoti di comprendere meglio gli alert. Ti può impedire di valutare accuratamente l'impatto degli attacchi.

> Il 45% degli avvisi di sicurezza alla fine sono dei falsi positivi[2]

Mentre il panorama delle minacce cyber evolve, possono emergere nuove lacune per quanto riguarda la visibilità - nei punti di connessione con i vendor, nelle aziende affiliate, e altrove.

Anche l'uso sempre più diffuso del cloud comporta vulnerabilità. Le aziende che utilizzano il cloud per applicazioni di business essenziali e per archiviare dati confidenziali corrono il rischio di gestire in modo errato i dati o anche di essere esposti a violazione della privacy dei dati.

Un approccio integrato e intelligente alla sicurezza può aiutarti a migliorare la visibilità, consentendoti di:

Determinare velocemente che si è verificata una violazione

In un mondo dove ogni minuto in cui si manifesta una violazione può comportare un costo di migliaia di dollari, è vitale risalire alla causa della violazione il più presto possibile. Un'integrazione migliore dei prodotti offre capacità di rilevamento veloce, per cui puoi rilevare le minacce, misurare l'esposizione al rischio e utilizzare le informazioni così ottenute per prevenire attacchi – nell'arco di minuti, non di giorni.

Comprendere appieno il volume degli avvisi

Alert fuorvianti non sono solo inutili, ma anche costosi. Le aziende possono impiegare numerose ore dei dipendenti indagando avvisi inaccurati o irrilevanti. Con l'ecosistema integrato adatto, puoi validare automaticamente gli avvisi ed eliminare i falsi positivi, facendo risparmiare alla tua azienda tempo e denaro.

Comprendere e anticipare le mosse degli hacker

Prevedere il comportamento degli hacker è un problema costante, in modo particolare se si considera la velocità con la quale gli attaccanti possono mimetizzarsi e nascondere la loro identità. L'intelligence che si può ottenere grazie a una soluzione di sicurezza integrata consente di rilevare minacce mai viste prima. Inoltre, l'intelligence utilizza analitycs sofisticati per modellare il comportamento futuro degli hacker. Grazie al machine learning e ad altre funzionalità innovative, puoi prioritizzare le minacce, isolarle e scegliere le tattiche di risoluzione adatte.

Migliorare la tua preparazione prima di un attacco

Ci saranno sempre delle minacce cyber all'orizzonte. Esiste però un modo semplice per difendersi: essere preparati. Stando al passo con l'attuale panorama delle minacce e le emergenti tendenze nel campo della cyber security, la tua azienda sarà preparata per fronteggiare eventuali attacchi. E dotando il tuo ecosistema integrato di tattiche, strategie difensive e contromisure, potrai prevenire gli attacchi.

2. The Voice of the Analysts, IDC, 2021

2. Accelera la tua risposta

Ogni volta che ti lasci alle spalle un'emergenza, c'è un nuovo e grave attacco cyber al telegiornale. Abbiamo raggiunto un punto di piena consapevolezza, ovvero anche le persone che non lavorano nell'ambito della sicurezza sanno che rispondere a un incidente è tanto importante quanto proteggersi da esso.

Per rispondere agli incidenti e proteggersi, le aziende devono dare la massima priorità a un flusso di lavoro che funzioni correttamente. I processi più efficienti ed efficaci consistono in alert di alta qualità, una coda di lavoro ordinata, analisi precise e gestione dei casi regolare.

Il consolidamento dei prodotti per la sicurezza, in combinazione con funzionalità di nuova generazione come IA e machine learning, può aiutare ad accelerare la tua risposta, preparandoti meglio a:

> 287 giorni è il tempo medio necessario per individuare e contenere una violazione di dati[3]

Integrare tutti gli aspetti delle tue attività di sicurezza

Una risposta veloce in genere dipende dalla rapidità con la quale i team responsabili della sicurezza riescono a comprendere appieno gli alert. Se questi ultimi hanno diverse origini senza contesto o correlazione, l'origine del log non ha pressoché alcun valore. Unificare le origini dei log può migliorare il tempo di risposta, consentendo di combinarli più facilmente con la threat intelligence e gli analytics per individuare rapidamente i punti in cui emergono nuove minacce.

Completare la tua risposta con l'intelligence

L'intelligence è una componente essenziale delle attività di sicurezza. Ma qual è il suo valore se non la si può applicare direttamente al tuo ambiente operativo? Se non puoi utilizzarla agevolmente per difendere la tua azienda, è inutile. Quando i tuoi prodotti per la sicurezza sono integrati in una singola soluzione intelligente, hai accesso a una intelligence pertinente, contestuale, applicabile specificamente a ogni violazione e facilmente disponibile per agevolare i tuoi team nelle indagini sugli incidenti.

Attuare la gestione dei casi

Rilevare e analizzare un attacco comporta molte operazioni e l'intervento di numerosi membri del team. Sfortunatamente, gli strumenti tradizionali di gestione e comunicazione spesso non hanno le qualità necessarie richieste dai team responsabili della sicurezza per coordinare queste attività. Un approccio unificato alle SecOps rende più facile fornire ai tuoi team strumenti semplici per assegnare le attività e tenerne traccia, gestire la coda di lavoro e facilitare la condivisione delle informazioni ai fini di una risoluzione rapida.

Aumentare l'efficienza dei dipendenti

Mentre le minacce evolvono, le aziende fanno a gara per assumere risorse adatte a ricoprire ruoli nel campo della sicurezza cyber. In questo contesto, la domanda supera largamente la disponibilità. Oltre ad essere a corto di personale per quanto riguarda i team responsabili della sicurezza, troppe aziende si affidano a singoli strumenti insufficienti, che conducono a processi manuali soggetti ad errori. Grazie a una piattaforma di sicurezza olistica e intelligente, la tua azienda può automatizzare attività ripetitive, che richiedono molto tempo, consentendo al personale di focalizzarsi su attività più importanti e con maggiore efficienza.

3. Cost of a Data Breach, IBM, 2021

Quasi i 2/3 dei partecipanti al sondaggio sostiene di avere risparmiato oltre 25.000 dollari ogni anno rivolgendosi a un singolo vendor XDR[4]

3. Incrementa l'efficienza ed ottimizza i costi

Quanto vale per te la sicurezza della tua azienda? Questa è una domanda fondamentale da porsi ogni volta che si sta per adottare un nuovo approccio alla sicurezza. Proteggere le tue risorse più preziose è indispensabile. Inoltre hai bisogno di sapere con precisione quanto sei disposto a spendere per mantenere la tua azienda sicura.

Spesso, le aziende sono interessate a confrontare fra di loro i prezzi dei prodotti, anche se questi ultimi sono molto differenti. Ma quando si trovano a dover valutare il costo totale di proprietà, le aziende devono pensare in modo più ampio e strategico. Non basta considerare solo i costi finanziari, occorre soppesare anche quelli operativi.

Un approccio integrato e intelligente alle SecOps può aiutare a:

Ottimizzare i costi finanziari

Hardware e software. Abbonamenti e upgrade. Implementazione e manutenzione. I prezzi di questi elementi possono sembrare abbastanza semplici, ma spesso comportano costi "invisibili" - dalle sovrapposizioni con soluzioni preesistenti a una mancanza di integrazione con singoli prodotti. Riunire un'ampia gamma di endpoint, dispositivi cloud e altri prodotti per la sicurezza in una singola soluzione ti consente di evidenziare quali siano i prodotti ridondanti, e scegliere quelli di cui fare a meno, riducendo i costi.

Ridurre al minimo l'impatto sui costi

La sicurezza cyber è un business soggetto a rischi. Un'organizzazione che non è in grado di proteggersi dagli attacchi aumenta la propria esposizione al rischio e a perdite di fatturato. Perdita di produttività. Perdita di reputazione. E altro ancora. Essere in grado di integrare le proprie attività di sicurezza consente di mettere al sicuro il proprio business e affrontare le criticità e i rischi. Grazie a maggiore visibilità e controllo, è possibile ridurre al minimo le interruzioni delle attività di business e l'impatto negativo che un evento può avere sull'opinione dei clienti.

Tenere sotto controllo i costi operativi

Il tempo è denaro. Ogni minuto speso per assumere talenti nella tua azienda, formare il personale o supportare costantemente le attività di sicurezza è un costo. Una piattaforma unificata adatta può aiutare a contenere le spese operative in diversi modi. Offre funzionalità più ampie, consentendo di ridurre il tempo che solitamente viene dedicato alla formazione del personale sui molteplici tool aziendali. Automatizza i flussi di lavoro, cosicché il personale può concentrarsi di più su attività più rilevanti anziché su compiti meno importanti. E permette ai membri del team di sfruttare le loro competenze per svolgere il lavoro a loro assegnato, riducendo al minimo il tasso di abbondono del personale.

4. Future of Extended Detection and Response (XDR), Cisco, 2021

WHITE PAPER

La fase successiva dell'evoluzione delle SecOps

Un'azienda dovrebbe sempre fare ogni sforzo per diventare più intelligente. Più solida. Più agile.

Un modo sicuro per riuscirci consiste nel riunire tutti i prodotti per la sicurezza in una singola soluzione intelligente. Solo allora potrai veramente dare vita alla tua sicurezza.

Con la giusta piattaforma integrata, puoi sfruttare la potenza dell'intelligenza artificiale, del machine learning e dell'automazione per acquisire informazioni preziose e ottimizzare i flussi di lavoro. In tal modo la tua azienda potrà non solo aumentare l'efficienza dei dipendenti, ma anche apprendere e adattarsi costantemente per fronteggiare minacce nuove e in evoluzione.

Inoltre, un ecosistema integrato offre vantaggi per la tua azienda grazie a un approccio alla protezione più unificato, integrando strumenti nativi ed aperti, per consentirti di configurare la sicurezza in base alle tue specifiche esigenze.

E integrando una piattaforma olistica e intelligente nelle tue attività, potrai beneficiare dei vantaggi di una sicurezza che è ora parte integrante e viva del tuo sistema, cosi come lo sono il rilevamento, la risposta e la risoluzione in tempo reale.

Vuoi saperne di più su come unire i tuoi prodotti in un'unica soluzione e dare vita alla tua sicurezza? Visita trellix.com oggi stesso.

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com

Informazioni su Trellix

Trellix è un'azienda globale che sta ridefinendo il futuro della sicurezza informatica. La sua piattaforma XDR (Extended Detection and Response) nativa e aperta aiuta le aziende che devono far fronte alle minacce più avanzate d'oggi a ottenere fiducia nella protezione e resilienza delle loro operazioni. Gli esperti della sicurezza Trellix, insieme a un vasto ecosistema di partner, accelerano l'innovazione tecnologica tramite il machine learning e l'automazione per mettere in grado oltre 40.000 clienti aziendali e governativi di operare autonomamente e al meglio.