

CONVALIDA ECONOMICA

Analisi dei vantaggi economici di Trend Vision One


Rischio informatico minimizzato, rilevamento e risposta accelerati ed efficienza operativa complessiva migliorata con una piattaforma di sicurezza informatica comprovata

Di Nathan McAfee, analista economico senior
Enterprise Strategy Group

Gennaio 2024


Sommario

Introduzione	3
Sfide.....	3
La soluzione: Trend Vision One	4
Convalida economica di Enterprise Strategy Group	5
Panoramica economica di Trend Vision One.....	5
Rischi ridotti.....	5
Rilevamento e risposta migliorati	7
Efficienza operativa migliorata.....	8
Analisi di Enterprise Strategy Group	10
Conclusione	10




Convalida economica: Riepilogo dei risultati chiave


Vantaggi convalidati di Trend Vision One



Rischio di violazione dei dati ridotto del 17%



Costi per gli FTE della sicurezza ridotti del 70%



Tasso di abbandono dei clienti e di ricambio dei dipendenti per la sicurezza ridotti del 5% e 20%

- **Rischi ridotti:** Trend Vision One fornisce approfondimenti e chiarezza tra risorse IT, integrazioni e comportamenti degli utenti, riducendo i rischi complessivi.
- **Rilevamento e risposta migliorati:** I clienti di Trend Vision One evidenziano l'eliminazione dello stress da avvisi e possono concentrarsi sulle minacce reali e risolvere i problemi più rapidamente rispetto al passato.
- **Efficienza operativa migliorata:** ESG ha rilevato che i clienti che implementano Trend Vision One possono spostare l'attenzione degli FTE verso attività above-the-line per un migliore allineamento delle funzionalità IT con gli obiettivi aziendali.

Introduzione

Questa convalida economica realizzata da Enterprise Strategy Group (ESG) di TechTarget è incentrata sui vantaggi quantitativi e qualitativi prevedibili per le aziende che utilizzano Trend Vision One rispetto a strategie frammentate di sicurezza informatica per migliorare la sicurezza e proteggere da, rilevare e rispondere a minacce ed eventi legati alla sicurezza.

Sfide

Proteggere gli asset digitali e le risorse IT è una sfida la cui complessità cresce a una velocità che può apparire esponenziale. Ogni cambiamento nel panorama digitale comporta la creazione di vettori di attacco che devono essere localizzati, compresi e messi in sicurezza. ESG ha studiato le sfide che le aziende devono affrontare in merito alla sicurezza informatica e ne ha rilevato la coerenza tra la maggior parte delle aziende e i loro team di sicurezza informatica:

- **Stress da avvisi.** I team di sicurezza informatica si trovano spesso ad affrontare quantità di avvisi che possono superare il miliardo di log generati ogni 1000 dispositivi a settimana, con una portata di identificazione dei rischi reali che, nella maggior parte dei casi, può sovraccaricare i sistemi e i team di sicurezza.
- **Dislocamento delle risorse IT.** La ricerca ESG ha rilevato che il 60% delle aziende ha diversi team responsabili delle risorse cloud on-premise, pubbliche e private.¹ Il che implica la creazione di strategie diverse in un ecosistema IT, che spesso determinano decisioni poco lungimiranti con un conseguente debito tecnico. Inoltre, con il normalizzarsi della forza lavoro flessibile, il numero di sedi da supportare è aumentato, tanto che ogni singolo dipendente costituisce una singola sede di lavoro e si trova spesso escluso dall'area di protezione delle reti o dell'hardware aziendali.
- **Complessità crescente.** Con ambienti IT sempre più complessi, i sistemi utilizzati per rilevare, rispondere a, rimediare e contenere le minacce possono risultare congestionati e inefficaci. Il risultato è un aumento del tempo necessario a individuare e risolvere le minacce e, risolto ancora peggiore, la mancanza di visibilità dei rischi attivi. La ricerca ESG ha rilevato che quasi un quarto delle società (23%) utilizza oltre 25 diversi prodotti per la sicurezza informatica.² Ciò si traduce in silos digitali, maggiore complessità e lacune di copertura, a cui spesso si aggiungono processi decisionali non lungimiranti che comportano un debito tecnico.
- **Crescita esponenziale delle applicazioni SaaS.** Poche applicazioni sono indipendenti. Poiché l'interfunzionalità è incorporata nelle applicazioni che utilizzano API, software di terze parti e più team di sviluppo, il panorama delle minacce di tali applicazioni aumenta. La ricerca ESG mostra che il 76% delle applicazioni sviluppate ha più di 25 API associate, con una modifica fino al 75% a cadenza almeno settimanale.³ Ciò aumenta il numero di vettori di attacco e costringe le aziende ad assumersi i rischi per la sicurezza delle risorse esterne connesse tramite API.⁴
- **Rischio di risorse sconosciute.** Identificare tutte le risorse digitali, in particolare con le continue richieste di protezione della forza lavoro da remoto, rappresenta una sfida. Senza una visione chiara delle risorse che costituiscono la superficie di attacco aziendale, è impossibile proteggerle.
- **Complessità crescente dei malintenzionati.** Gli attacchi aumentano in termini di complessità e volume. ESG ha rilevato che il 68% delle aziende è stato vittima di un attacco che ha utilizzato il traffico crittografato nel tentativo di evitare il rilevamento.⁵ La crittografia è una pietra miliare della metodologia legata alla sicurezza, ma non è più la misura preventiva infallibile del passato.

¹ Fonte: report della ricerca condotta da Enterprise Strategy Group, [Network Security Trends in Hybrid Cloud Environments](#), luglio 2022.

² Fonte: risultati completi del sondaggio condotto da Enterprise Strategy Group, [ESG/ISSA Cybersecurity Process and Technology Survey](#), giugno 2022.

³ Fonte: report della ricerca condotta da Enterprise Strategy Group, [Securing the API Attack Surface](#), agosto 2023.

⁴ Ibid.

⁵ Fonte: report della ricerca condotta da Enterprise Strategy Group, [The Evolving Role of Network Detection and Response](#), marzo 2023.

- **Impatto in aumento degli eventi di sicurezza.** L'impatto degli eventi legati alla sicurezza varia da semplici distrazioni a eventi ransomware con una media pari a 4,45 milioni di dollari per occorrenza.⁶ I dati mostrano che le aziende che subiscono attacchi andati a buon fine hanno in media un rendimento inferiore dell'11,9% rispetto al mercato nei due anni successivi a un attacco.⁷

Le sfide sono chiare. Le minacce sono in aumento in termini di quantità e complessità e le superfici di attacco si espandono con l'aggiunta di nuovi dispositivi, risorse cloud, applicazioni SaaS, posizioni di domini e IP, tipi di dati e altro ancora. Le aziende hanno bisogno di una soluzione che semplifichi la protezione proattiva basata sui rischi e il rilevamento delle minacce in tutti gli scenari di utilizzo.

La soluzione: Trend Vision One

Come mostrato nella figura 1, Trend Vision One è una piattaforma moderna appositamente realizzata per la sicurezza informatica basata su intelligenza artificiale che sfrutta la potenza combinata di soluzioni di gestione dei rischi di superficie di attacco a ciclo di vita completo, XDR, intelligence sulle minacce leader a livello globale, tecnologia AI/ML e principi zero trust per unire funzionalità complete di previsione, prevenzione, rilevamento e risposta alle minacce in vista di una protezione superiore contro le minacce informatiche.

Figura 1. Trend Vision One combina prevenzione, rilevamento, risposta e protezione



Fonte: Trend Vision One

Le aziende che adottano Trend Vision One riscontrano la capacità di questa piattaforma completa per la sicurezza informatica di apportare un cambio nella direzione della sicurezza proattiva finalizzata a rilevare, gestire e mitigare meglio le minacce alla sicurezza in tutto il proprio ambiente.

⁶ Fonte: IBM Corporation, [Cost of a Data Breach Report 2023, luglio 2023](#).

⁷ Fonte: Keman Huang et al., [Harvard Business Review, "The Devastating Business Impacts of a Cyber Breach," 4 maggio 2023](#).

Convalida economica di Enterprise Strategy Group

Enterprise Strategy Group (ESG) ha realizzato un'analisi economica quantitativa sull'impatto che Trend Vision One può avere sulla capacità di un'azienda di raggiungere obiettivi IT e di business.

Il processo di convalida economica di ESG è un metodo comprovato per comprendere, convalidare, quantificare e modellare le proposte di valore economico di un prodotto o di una soluzione. Il processo si avvale delle competenze fondamentali di ESG nel campo delle analisi di mercato e di settore, della ricerca previsionale e della convalida tecnica ed economica. ESG ha condotto interviste approfondite con utenti finali per comprendere e quantificare meglio l'impatto di Trend Vision One sulle loro aziende, in particolare rispetto alle soluzioni implementate e/o sperimentate precedentemente. I risultati qualitativi e quantitativi sono stati utilizzati come base per un semplice modello economico di comparazione dei costi preventivati per l'infrastruttura dedicata alla sicurezza e agli eventi di Trend Vision One con i tradizionali servizi on-premise e cloud.

Panoramica economica di Trend Vision One

L'analisi economica ESG ha rivelato che Trend Vision One offre ai propri clienti risparmi e vantaggi significativi in categorie tra cui:

- **Rischi ridotti.** ESG ha riscontrato presso i clienti Trend Vision One una minore probabilità di eventi ransomware e di violazione, nonché un impatto ridotto di eventi reali.
- **Rilevamento e risposta migliorati.** I clienti hanno segnalato un miglioramento significativo nella capacità di rilevare problemi che creano il massimo livello di rischio e di risolverli in un tempo minore con Trend Vision One.
- **Efficienza operativa migliorata.** I clienti di Trend Vision One hanno riscontrato una minore spesa complessiva per la sicurezza e la risposta agli incidenti rispetto alle soluzioni adottate in precedenza.

Rischi ridotti

La chiave di misurazione di qualsiasi piattaforma di sicurezza è la sua capacità di proteggere un ecosistema IT. Gli analisti ESG hanno studiato il prima e il dopo tra gli ambienti delle aziende che hanno adottato Trend Vision One. Oltre alle metriche comparabili fianco a fianco, ESG ha rilevato un'intera gamma di nuovi elementi misurabili da considerare per i clienti Trend Vision One. Con Trend Vision One, i clienti hanno potuto proteggere in modo proattivo intere classi di risorse digitali, tra cui dispositivi, server, indirizzi di dominio e IP, risorse cloud e API, che in passato erano sotto-protette o addirittura non protette. Inoltre, i clienti intervistati per la presente analisi hanno riferito vantaggi in termini di riduzione dei rischi, tra cui:

"Vision One non ha sostituito le vecchie funzionalità, ma ci ha permesso di vedere cose a noi totalmente sconosciute con la soluzione precedente. Scansioniamo e contrastiamo minacce di cui in passato saremmo venuti a conoscenza solo troppo tardi".

- Security Manager, sistemi bibliotecari di stato

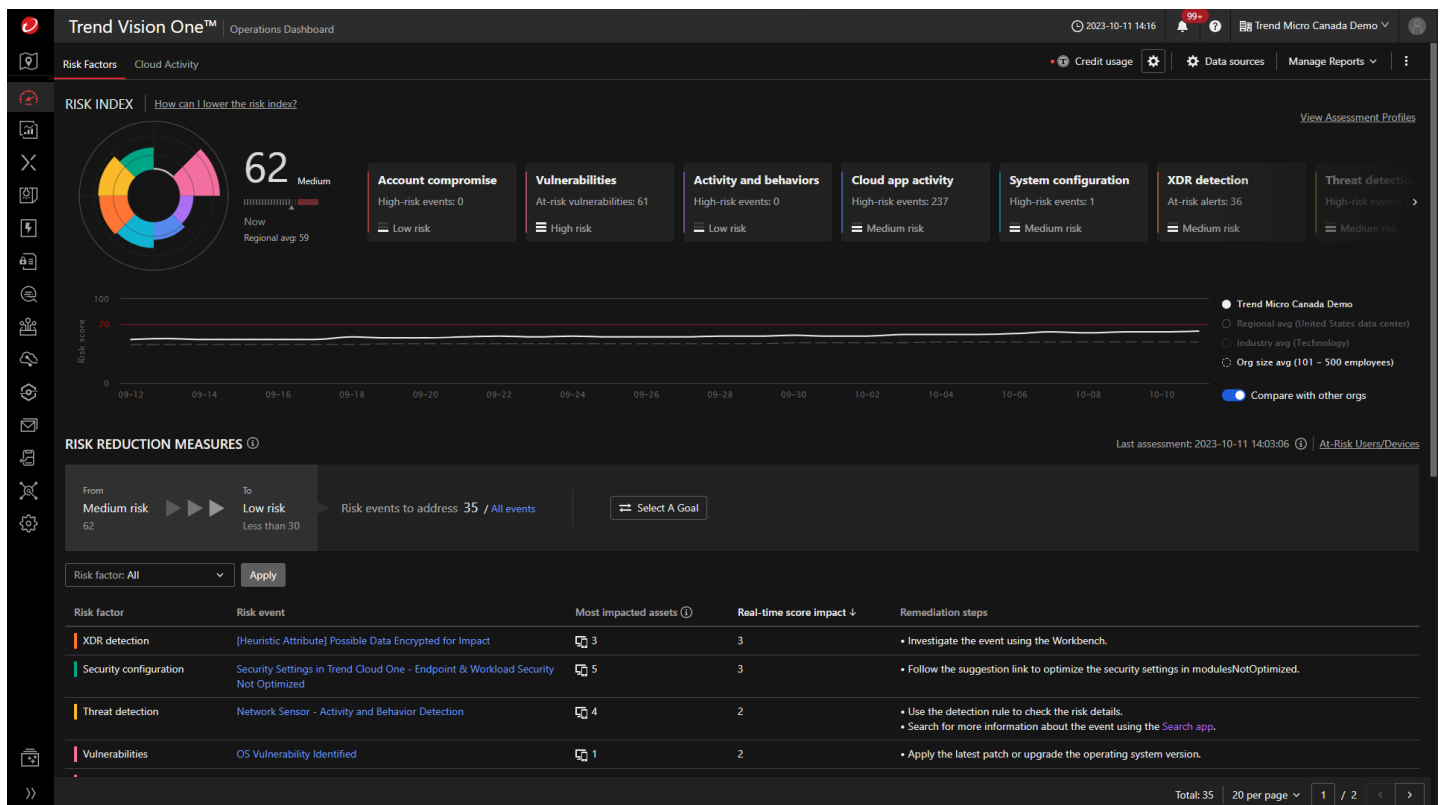
- **Rischio di violazione ridotto.** Come già menzionato, uno dei principali studi sulla quantificazione dei rischi stima che il costo medio di una violazione dei dati sia di 4,45 milioni di dollari. Il modello finanziario di ESG ha utilizzato l'11% quale valore di esposizione annuale a una violazione. In base alle interviste con i clienti, Trend Vision One ha ridotto il numero di rischi annuali all'8%, con un profitto annuale di 1,30 milioni di dollari dato dall'alleggerimento dell'esposizione ai rischi. Alla domanda sul perché ritenessero che l'esposizione al rischio fosse stata ridotta con Trend Vision One, tutti i partecipanti hanno citato una visibilità e una fedeltà degli avvisi migliorate e un dwell-time minore, che in media si è rivelato inferiore del 65% rispetto all'ambiente precedente. Un intervistato ha riferito che l'attenzione sull'impatto di una violazione dovrebbe andare ben oltre la metrica dei costi: *"Un problema di sicurezza incide sulla nostra reputazione. I numeri contano, ma il rischio reale è il modo in cui i nostri clienti guardano a noi e al nostro impegno per la sicurezza"*.

- Visibilità e approfondimento migliorati.** In ogni conversazione di ESG con i clienti sull'impatto di Trend Vision One, uno dei principali vantaggi citati è stata la visibilità migliorata dell'intero approccio alla sicurezza e la nuova capacità di gestire proattivamente i rischi. La visibilità e tracciabilità dei rischi fungono da fonte centralizzata per uniformare l'approccio alla sicurezza in tutti i tipi di risorse. Dai colloqui con i clienti è emersa una sensazione unanime: *"Prima di Trend Vision One, semplicemente non sapevamo"*. In effetti, Trend Vision One ha portato alla luce diversi esempi di risorse non monitorate, o addirittura sconosciute, sulle loro reti. Un'altra funzionalità di Trend Vision One specificamente individuata come elemento rivoluzionario è la dashboard delle operazioni (mostrata nella Figura 2). Questa funzione offre una visione completa dello stato e dei rischi di sicurezza nei dispositivi e account di un'azienda, con la possibilità di analizzare ogni area per dettagli specifici. In questo modo, la dashboard delle operazioni di Trend Vision One fornisce un elenco consolidato di opportunità per migliorare l'approccio generale alla sicurezza dell'azienda.

"La dashboard delle operazioni di Trend Vision One fornisce il livello di rischio attuale, oltre a modalità dettagliate per migliorare il nostro andamento e rafforzare il nostro approccio alla sicurezza. Non potremmo permetterci di assumere le competenze necessarie per ottenere questo tipo di approfondimento, che troviamo però incluso in Trend Vision One".

- Systems Admin, governo statale

Figura 2. La dashboard delle operazioni fornisce l'andamento dell'indice di rischio e approfondimenti utili ai miglioramenti



Fonte: Trend Vision One

- **Patching più rapido.** Con la forza lavoro flessibile, molte risorse IT sono fuori dal controllo dei sistemi di aggiornamento aziendali. In merito a Trend Vision One, gli intervistati segnalano un apporto di maggiore proattività, chiarezza e semplicità alla loro strategia di patching grazie alle patch virtuali informate con intelligence sulle minacce, affermando : *"Abbiamo semplificato notevolmente la gestione delle patch. Ora possiamo contare sulla chiarezza nella copertura delle patch, che implementiamo con 102 giorni di anticipo rispetto al passato".*
- **Allineamento con i principali framework di conformità.** Le aziende che operano in settori basati sulla conformità rilevano come Trend Vision One consenta loro di rispettare meglio le linee guida e monitorare costantemente lo stato della conformità. Un intervistato ha espresso la propria convinzione secondo cui Trend Vision One abbia consentito di ridurre del 60% l'esposizione alle sanzioni. Nel modello finanziario di ESG, questa riduzione del 60% corrisponde a un profitto dato dall'alleggerimento dei rischi pari a 1,2 milioni di dollari l'anno.
- **Protezione delle integrazioni di terze parti.** Ogni integrazione di terze parti comporta rischi, in quanto l'azienda deve assumersi i rischi associati al codice di tale terza parte. Sull'impatto dell'uso di API e integrazioni di terze parti, un intervistato ha affermato: *"L'integrazione di terze parti con Trend Vision One è fantastica. Spesso ci integriamo con componenti di sicurezza di altri fornitori. Trend Vision One crea elenchi dinamici esterni in modo da alimentare automaticamente il nostro firewall per bloccare una minaccia al rilevamento di un oggetto sospetto. La visibilità nelle integrazioni di terze parti è un elemento rivoluzionario che ci consente di accettare anziché rifiutare richieste commerciali.* Ogni azienda intervistata ha dichiarato di avere maggiori probabilità di trarre vantaggio dalle funzionalità di integrazione di terze parti di Trend Vision One, in particolare grazie al suo livello di approfondimento e protezione.

"Ci sentiamo più sicuri da quando abbiamo adottato Trend Vision One. Nella nostra proof of concept abbiamo riscontrato un numero enorme di falsi positivi nelle alternative prese in considerazione. Con Trend Vision One, le minacce rilevate sono molto più accurate e le informazioni nettamente più specifiche rispetto ai competitor".

- Infrastructure Manager, Home Builder USA

Rilevamento e risposta migliorati

Con milioni di log generati ogni giorno e migliaia di possibili avvisi, cercare di identificare le minacce più rilevanti è un compito molto difficile. ESG ha intervistato i clienti per comprendere le loro metriche di rilevamento e risposta prima e dopo l'adozione di Trend Vision One. Come illustrato nella tabella 1, Trend Vision One ha avuto un impatto sostanziale, riducendo il rumore e consentendo alle aziende di concentrarsi sulle questioni importanti. Inoltre, le aziende hanno scoperto di poter ricevere avvisi da risorse a cui erano totalmente ignote in passato.

Tabella 1. Confronto tra metriche di rilevamento, triage, indagine e risoluzione

	Prima di Trend Vision One	Dopo Trend Vision One
Numero di avvisi al giorno	1000	4
Tempo di rilevamento (minuti)	11520	1
Tempo di triage (minuti)	480	meno di 1
Tempo di indagine (minuti)	360	90
Tempo di risoluzione (minuti)	1860	6
FTE necessari	5,6	meno di 1

Fonte: Enterprise Strategy Group, una divisione di TechTarget, Inc.

"Abbiamo ridotto i tempi di ricerca dei problemi di oltre il 75%. Ora lavoriamo e rispondiamo alle minacce in modo più rapido. Tuttavia, non si tratta di un confronto alla pari con il nostro vecchio ambiente. Con Trend Vision One individuamo e risolviamo minacce che non avremmo potuto vedere o comprendere in passato". - Information Security Manager, sistema universitario USA

Efficienza operativa migliorata

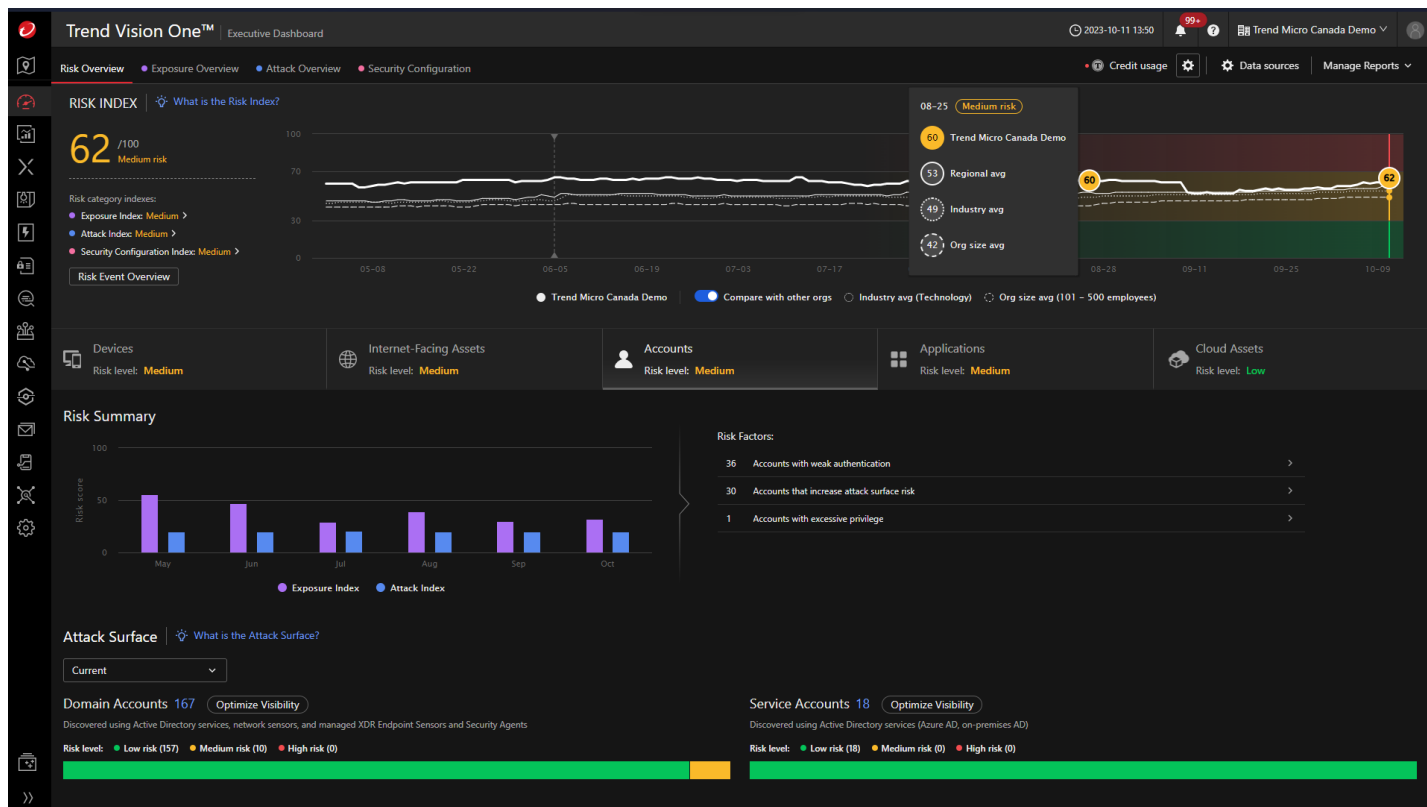
Ogni azienda deve affrontare la sfida di ottenere il maggior impatto possibile da ogni dollaro speso. Con Trend Vision One, i team IT e di sicurezza informatica hanno potuto adottare un approccio più proattivo grazie a una strategia di sicurezza basata su piattaforma. Questo impatto ha consentito di ottenere vantaggi nelle seguenti aree:

- **Efficienza degli FTE migliorata.** Grazie a Trend Vision One, tutti gli intervistati di ogni azienda hanno riscontrato una riduzione media del 70% del personale preposto alla piattaforma di sicurezza informatica. Uno tra questi ha affermato: *"In passato necessitavamo di otto analisti della sicurezza per un livello di protezione molto inferiore a quello ottenibile con due persone con Trend Vision One, le quali sono peraltro molto più indipendenti"*. Nel modello economico di ESG, ciò si traduce in un risparmio annuo di 1,04 milioni di dollari. Passando ai costi legati al supporto, con Trend Vision One il modello ha visto il personale di supporto ridursi da 28 a 17 impiegati, con un conseguente risparmio annuale di 864.000 dollari.
- **Approfondimenti per il management.** Trend Vision One dispone di un dashboard esecutivo integrato che consente a CIO, CISO e manager di accedere rapidamente a una panoramica aziendale completa delle tendenze e delle minacce legate ai rischi informatici, oltre che di esplorare ogni metrica al grado di approfondimento desiderato. Secondo un intervistato: *"La dashboard esecutiva è uno strumento fantastico per permettere ai dirigenti di avere visibilità istantanea sul nostro stato e di approfondire i dettagli a loro discrezione, senza dover sottrarre tempo a uno dei nostri dipendenti. Già solo questo ci consente di risparmiare diverse ore settimanalmente e di prendere decisioni più informate"*. Come illustrato nella figura 3, la chiarezza e gli approfondimenti forniti dal dashboard possono essere modificati per adattarsi al livello e alle esigenze dei manager e semplificano la comunicazione dei responsabili della sicurezza informatica con colleghi di unità non tecniche e consigli di amministrazione.
- **Soddisfazione dei clienti migliorata.** I clienti si concentrano sulle violazioni della sicurezza e sulle interazioni di valore sicure, mantenendo al contempo un'esperienza utente fluida. I clienti intervistati stimano di aver ridotto il tasso di abbandono dei clienti dal 6% al 5,7%, in particolare grazie alle protezioni e alla modalità di integrazione di terze parti fornita da Trend Vision One. Nel modello economico di ESG, questo miglioramento dello 0,3% nel tasso di abbandono dei clienti si traduce in un profitto annuale di 2,43 milioni di dollari.

"I nostri team di sicurezza si trovavano costantemente ad affrontare un backlog di nuovi elementi da implementare sulla nostra rete. Il solo eseguire valutazioni dei rischi su questi nuovi elementi ha richiesto più tempo di quello a disposizione. Grazie a Trend Vision One, il carico di lavoro si è ridotto del 70%, e il maggior tempo a disposizione ci ha consentito di lavorare con le nostre unità aziendali a un migliore allineamento degli obiettivi con le funzionalità IT".

- Information Security Manager, sistema universitario USA

Figura 3. La dashboard esecutiva fornisce uno stato aggiornato con possibilità di approfondire dettagli



Fonte: Trend Vision One

- **Soddisfazione dei dipendenti migliorata.** Gli intervistati riferiscono un notevole cambiamento nella soddisfazione dei dipendenti con Trend Vision One. ESG ha rivelato numerose storie di impiegati più indipendenti, che dedicano meno tempo a mansioni ordinarie e spostano l'attenzione da attività below-the-line, come il monitoraggio dei log e le ricerche di base, ad attività above-the-line, che risolvono problemi IT e aziendali. Le aziende intervistate hanno stimato una diminuzione di oltre il 20% del ricambio del personale IT a partire dall'adozione di Trend Vision One. Come ha dichiarato un intervistato, *"I nostri dipendenti amano lavorare in questo ambiente. Abbiamo la flessibilità di esporli al giusto livello di sfida in base alle loro competenze e siamo in grado di eliminare completamente gran parte dei compiti ordinari tradizionalmente associati ai prodotti per la sicurezza grazie a un approccio basato su piattaforma e a flussi di lavoro supportati dall'intelligenza artificiale"*. Il modello economico di ESG ha quantificato questo profitto a 75.000 dollari l'anno.
- **Costi di sicurezza minori.** Trend Vision One offre funzionalità complete di sicurezza informatica su un'unica piattaforma nell'intero ambiente del cliente. Alcune di queste funzionalità sostituiscono specifiche soluzioni esistenti isolate, mentre altre includono innovazioni di categoria che contribuiscono a rafforzare l'approccio generale alla sicurezza. Diverse aziende hanno alleggerito la spesa legata ai prodotti, il 40% di quelle intervistate dichiarando di aver ridotto di oltre 500.000 dollari l'anno i costi legati alla sicurezza informatica.
- **Carico di controlli ridotto.** ESG ha riscontrato vantaggi sostanziali nella riduzione dei costi per il lavoro legato alla conformità e ai controlli, con una riduzione dei costi annuali in quest'area pari a 207.000 dollari, come mostrato nel nostro modello finanziario. Un'azienda ha affermato: *"In passato avevamo quattro dipendenti preposti ai soli controlli. Con Trend Vision One, ne serve meno di una"*.

Analisi di Enterprise Strategy Group

ESG ha sfruttato le informazioni raccolte attraverso materiali procurati dai fornitori, la conoscenza pubblica e industriale di economia e tecnologie e i risultati delle interviste ai clienti per creare un modello triennale di TCO/ROI che confronti i costi e i vantaggi di Trend Vision One con un'azienda modello che utilizza più prodotti per la protezione informatica. Le interviste di ESG ai clienti che hanno recentemente effettuato la transizione, combinate con l'esperienza e la competenza nella modellazione economica e nella convalida tecnica, hanno contribuito a formare la base del nostro scenario modellato.

L'azienda modello di ESG è nel settore high-tech con 15.000 dipendenti e 34.950 endpoint e produce 2,7 miliardi di dollari di fatturato annuo. Ha 8,4 dipendenti a tempo pieno (FTE) che gestiscono la sicurezza informatica e 28 analisti di supporto. Supporta 84 sedi a livello internazionale e ha un tasso di crescita annuo pari al 3% circa.

Perché conta

Ogni cliente intervistato ha riferito che Trend Vision One non ha costituito solo un valido sostituto di prodotti esistenti, ma anche una nuova piattaforma di funzionalità che ha sostituito le implementazioni di specifiche soluzioni esistenti, aggiungendo al contempo innumerevoli nuove funzionalità per rafforzare il proprio approccio alla sicurezza in modo molto più proattivo rispetto al passato. ESG non ha cercato di creare un ambiente già esistente (as-is) con tutte queste funzionalità aggiuntive per confronto; al contrario, ha utilizzato scenari descritti dai clienti per quantificare l'impatto del passaggio a Trend Vision One.

Conclusione

Le minacce informatiche sono sempre più frequenti e sofisticate, mentre le superfici di attacco sono in aumento con nuove sedi, tipi di dati, fonti di dati e scenari di utilizzo. Le aziende alla ricerca di una soluzione per la sicurezza informatica si ritrovavano troppo spesso con una rete di prodotti che creano silos in alcuni casi e lasciano lacune in altri. Il che può tradursi in un atteggiamento protezionistico che costringe le unità aziendali a lavorare entro determinati vincoli anziché utilizzare l'IT per supportare nuove opportunità di business. In questi scenari, le aziende incorrono in rischi inutili e prendono decisioni non lungimiranti che richiedono un rimedio continuo, creando un debito tecnico che sottrae parte dei futuri budget IT. Trend Vision One è una piattaforma di sicurezza informatica che offre funzionalità complete di prevenzione, rilevamento e risposta per proteggere utenti, endpoint, e-mail, applicazioni, reti, cloud, infrastrutture e dati. Trend Vision One è supportato da una delle principali intelligence sulle minacce globali con pochi eguali e consente agli analisti della sicurezza di ogni livello di maturità di ottenere indicazioni basate sull'AI per rafforzare in modo più efficace la sicurezza e sventare gli attacchi informatici.

Enterprise Strategy Group (ESG) ha analizzato il possibile impatto di Trend Vision One sulla capacità di un'azienda di creare un ambiente dalla sicurezza informatica proattiva e completa. Durante questo processo, ESG ha intervistato gli attuali clienti Trend Vision One per comprendere le sfide del loro precedente ambiente di sicurezza informatica e i cambiamenti nelle funzionalità riscontrati con Trend Vision One. ESG ha riscontrato vantaggi sostanziali nella propria capacità di ridurre l'esposizione ai rischi, semplificare le funzionalità di rilevamento e risposta, allineare meglio l'IT alle esigenze aziendali e fornire ai manager un livello di approfondimento tale da poter prendere decisioni informate senza dover distrarre il personale per ottenere aggiornamenti.

Se siete alla ricerca di una piattaforma di sicurezza informatica aziendale che consenta a dirigenti, manager e team di sicurezza informatica/IT di comprendere e proteggere il vostro intero ambiente, ESG raccomanda vivamente di esplorare le funzionalità di Trend Vision One.

©TechTarget, Inc. o sue consociate. Tutti i diritti riservati. TechTarget e il logo TechTarget sono marchi o marchi registrati di TechTarget, Inc. e sono registrati in giurisdizioni di tutto il mondo. Altri nomi e loghi di prodotti e servizi, inclusi BrightTALK, Xtelligent ed Enterprise Strategy Group, potrebbero essere marchi di TechTarget o di sue consociate. Tutti gli altri marchi, loghi e nomi commerciali appartengono ai rispettivi proprietari.

Le informazioni contenute in questa pubblicazione sono state ottenute da fonti che TechTarget considera affidabili ma non sono garantite da TechTarget. La presente pubblicazione può contenere opinioni di TechTarget che sono soggette a modifiche. Questa pubblicazione può includere previsioni, proiezioni e altre dichiarazioni predittive che rappresentano presupposti e aspettative di TechTarget alla luce delle informazioni attualmente disponibili. Queste previsioni si basano sulle tendenze del settore e implicano variabili e incertezze. Di conseguenza, TechTarget non fornisce alcuna garanzia in merito all'accuratezza di previsioni, proiezioni o dichiarazioni predittive specifiche contenute nel presente documento.

Qualsiasi riproduzione o redistribuzione della presente pubblicazione, in toto o in parte, in formato cartaceo, elettronico o in altro modo a persone non autorizzate a riceverla, senza l'esplicito consenso di TechTarget, viola la legge sul copyright degli Stati Uniti e sarà soggetta ad azioni per danni civili e, se applicabile, ad azioni penali. In caso di domande, contattare il Servizio Clienti all'indirizzo cr@esg-global.com.

Informazioni su Enterprise Strategy Group

Enterprise Strategy Group di TechTarget fornisce informazioni di mercato mirate e implementabili, ricerche sul fronte della domanda, servizi di consulenza di analisti, guida alla strategia GTM, convalide di soluzioni e contenuti personalizzati a supporto dell'acquisto e della vendita di tecnologie di livello enterprise.

 contact@esg-global.com www.esg-global.com