Brochure

Blocca gli **attacchi mirati**

WithSecure™ Elements Endpoint Detection and Response

EDR

PROXIMALAB
SOLUZIONI INFORMATICHE

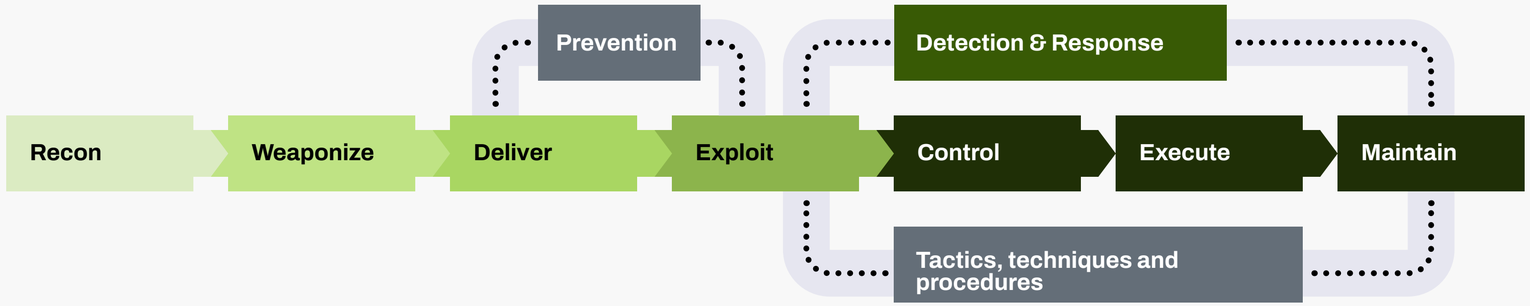
Proteggi l'azienda e i suoi dati dagli attacchi informatici avanzati

La prevenzione efficace delle minacce pre-compromissione è uno dei pilastri della cyber security. Tuttavia, le sole misure preventive non sono sufficienti per proteggere l'azienda e i suoi dati da tattiche, tecniche e procedure usate dagli avversari negli attacchi mirati.

Il panorama delle minacce in continua evoluzione e i requisiti normativi come il GDPR richiedono alle aziende di essere preparate a rilevare violazioni in fase di post-compromissione. Ciò significa garantire a un'azienda la capacità di rispondere rapidamente agli attacchi avanzati.

WithSecure™ Elements Endpoint Detection and Response solution, addestrata da un esperto team di threat hunting, permette al tuo team IT o a un service provider certificato di proteggere la tua organizzazione dalle minacce avanzate.

Con il supporto d'eccellenza degli esperti di cyber security WithSecure™, i tuoi specialisti IT potranno rispondere agli incidenti in modo rapido ed efficace. In alternativa, se fai gestire le operazioni di detection and response ad un service provider, potrai concentrarti sul tuo core business e affidarti alla guida di esperti in caso di attacco.

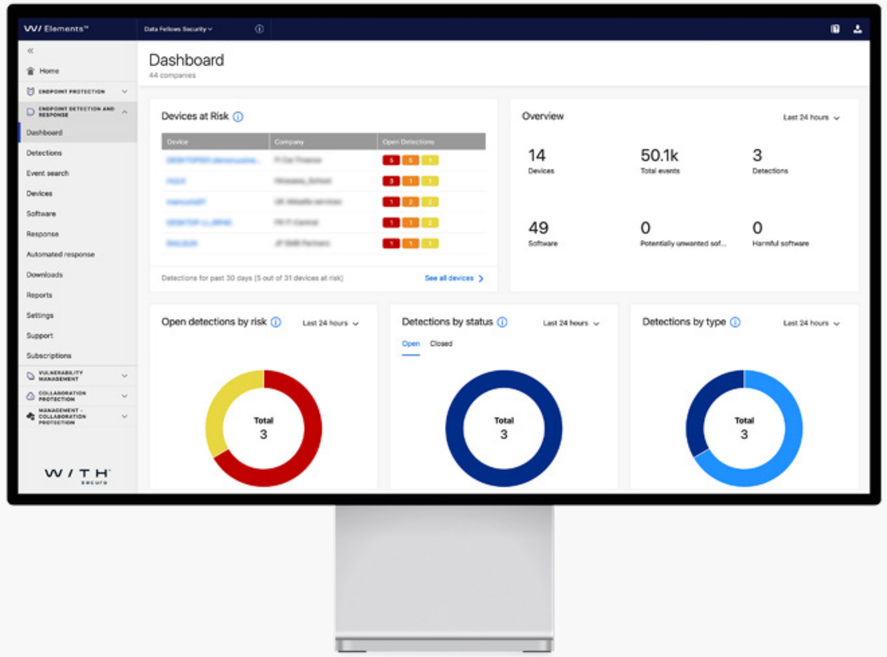


PROXIMALAB

Panoramica

Blocca rapidamente gli attacchi mirati con linee guida e automazione

Come fai a rilevare un attacco sofisticato? Impieghi le più avanzate tecnologie di analisi e machine learning per proteggere la tua organizzazione da minacce e violazioni complesse.

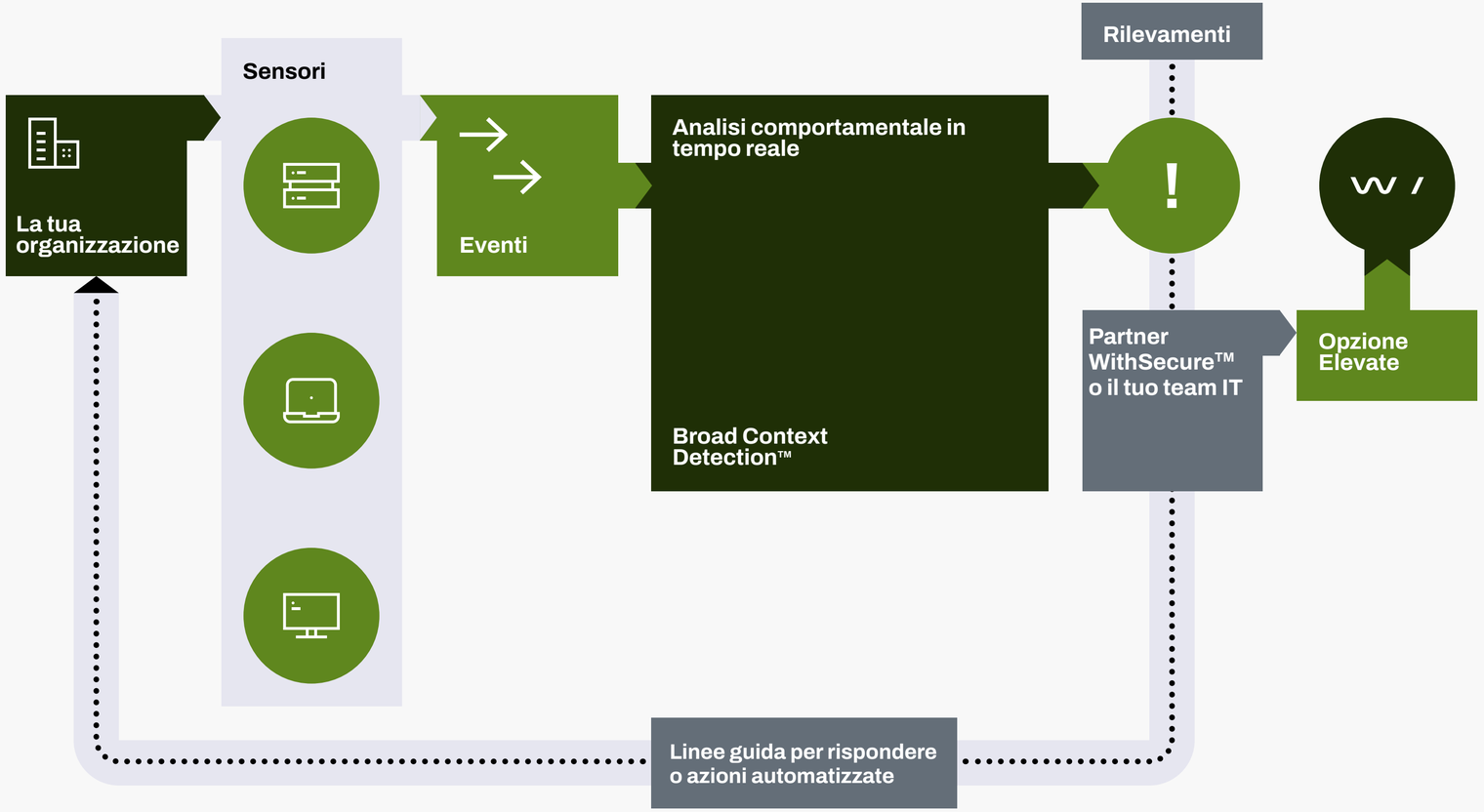


La soluzione WithSecure™ EDR (Endpoint Detection & Response) fornisce visibilità contestuale sulle minacce avanzate, consentendo di rilevare e rispondere agli attacchi mirati con automazione e linee guida.

Quando si verifica una violazione, ti serve ben più di un semplice avviso. Per pianificare la migliore risposta possibile, devi comprendere le specificità dell'attacco. I nostri meccanismi di Broad Context Detection™, insieme a service provider certificati e automazione integrata, bloccheranno rapidamente l'attacco e forniranno consigli utili per eseguire ulteriori azioni di remediation.

PROXIMALAB

Come funziona



La miglior tecnologia e gli esperti di cyber security WithSecure™ al tuo servizio

1. I sensori leggeri installati sugli endpoint monitorano gli eventi comportamentali generati dagli utenti e li inviano in tempo reale ai meccanismi di Broad Context Detection™ e di analisi dei dati comportamentali in tempo reale per distinguere i comportamenti malevoli da quelli normali.
2. Gli avvisi con punteggi di rischio e la visualizzazione del contesto più ampio su tutti gli host consentono di confermare un rilevamento in modo semplice, sia per il partner WithSecure™ sia per il team IT, con la possibilità di inoltrare le indagini complesse a WithSecure™ o di automatizzare le azioni di risposta.
3. In seguito a un rilevamento confermato, la soluzione offre consigli e suggerisce azioni per guidarti nei passaggi necessari a contenere e risolvere rapidamente l'attacco.

Come funziona

Come cercare un ago in un pagliaio: un esempio concreto

Rilevare le minacce avanzate individuando i singoli piccoli eventi causati dagli attaccanti è come cercare un ago in un pagliaio.

In un'installazione con 325 nodi presso un cliente, i nostri sensori hanno raccolto circa 500 milioni di eventi in un mese. L'analisi dei dati grezzi nei nostri sistemi di back-end ha filtrato tale numero abbassandolo a 225.000 eventi.

Gli eventi sospetti, poi, sono stati ulteriormente analizzati dal nostro meccanismo di Broad Context Detection™ per restringere ulteriormente il numero di rilevamenti a soli 24. Infine, quei 24 rilevamenti sono stati esaminati nel dettaglio e solo 7 sono stati confermati come minacce reali.

Permettere ai team IT e di sicurezza di concentrarsi su meno rilevamenti, ma più accurati, porta ad azioni di risposta più rapide ed efficaci nel caso sia in corso un reale attacco informatico.

500 milioni
Dati su eventi/mese
Raccolti da 325 sensori endpoint

225 000
Eventi sospetti
Dopo l'analisi comportamentale in tempo reale degli eventi

24
Rilevamenti
Dopo aver aggiunto un contesto più ampio agli eventi sospetti

7
Minacce reali
Dopo aver confermato i rilevamenti come minacce reali

PROXIMALAB

Vantaggi

Visibilità

Ottieni visibilità immediata sull'ambiente IT e sullo stato della sicurezza

- Migliora la visibilità su ambiente IT e stato della sicurezza tramite un inventario di applicazioni ed endpoint
- Identifica le attività sospette raccogliendo e correlando eventi comportamentali al di là del malware tradizionale
- Fornisce avvisi con informazioni sul contesto più ampio e criticità degli asset, facilitando la risposta agli incidenti

Detection

Proteggi business e dati sensibili rilevando rapidamente le violazioni

- Rileva e blocca rapidamente gli attacchi mirati per minimizzare le interruzioni di business e gli impatti negativi sul brand
- Puoi avere la soluzione installata in poche ore, per essere subito pronto in caso di violazioni
- Soddisfa i requisiti normativi di PCI, HIPAA e GDPR che richiedono di notificare le violazioni entro 72 ore

Response

Rispondi rapidamente con linee guida e automazione in caso di attacco

- L'automazione e l'intelligence integrate aiutano il tuo team a concentrarsi solo sugli attacchi reali
- Gli avvisi includono linee guida per la risposta più adeguata, con la possibilità di automatizzare le azioni in ogni momento
- Supera i limiti di competenze o risorse rispondendo agli attacchi con un service provider certificato supportato da WithSecure™

Caratteristiche

Sensori endpoint

Strumenti di monitoraggio leggeri e discreti, progettati per funzionare con ogni soluzione di protezione degli endpoint

- I sensori vengono implementati su tutti i computer pertinenti nell'organizzazione
- Infrastruttura single-client e di gestione con le soluzioni di sicurezza endpoint WithSecure™
- I sensori raccolgono dati comportamentali da dispositivi Windows, Mac e Linux senza compromettere la privacy degli utenti.

Risposta guidata

Ti prepara a gestire anche gli attacchi informatici più avanzati con le risorse esistenti

- Linee guida alla risposta e azioni remote integrate passo per passo per bloccare gli attacchi
- I service provider certificati ti guidano e supportano nelle azioni di risposta
- Servizio esclusivo "Elevate to WithSecure™" per analisi delle minacce e linee guida esperte a tua disposizione

Broad Context Detection™

La tecnologia di rilevamento proprietaria di WithSecure™ facilita la comprensione della portata di un attacco mirato

- Analisi comportamentale in tempo reale, analisi reputazionale e dei big data con machine learning
- Posiziona automaticamente i rilevamenti in un contesto visualizzato su una linea temporale
- Include livelli di rischio, criticità degli host coinvolti e il panorama delle minacce prevalenti

Risposta automatizzata

Riduci l'impatto degli attacchi informatici mirati automatizzando le azioni di risposta in ogni momento

- Azioni di risposta automatizzate basate su criticità, livelli di rischio e pianificazione predefinita
- I livelli di rischio e criticità forniti dalla soluzione consentono di assegnare le priorità alle azioni di risposta
- Contieni gli attacchi rapidamente anche se il tuo team è disponibile solo durante l'orario lavorativo

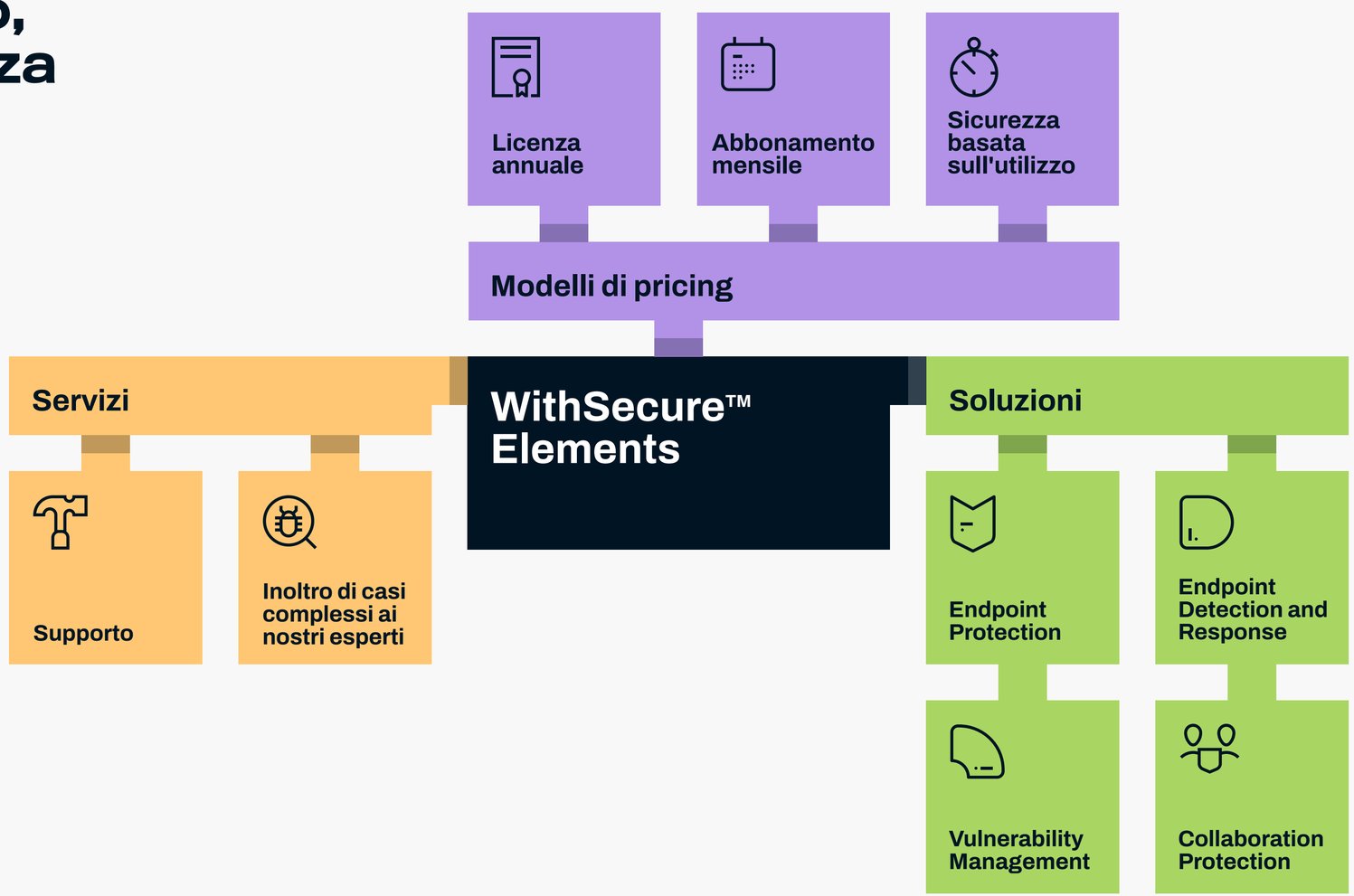
Visibilità delle applicazioni

Ottenere visibilità sull'ambiente di IT e sul relativo stato di sicurezza non è mai stato così semplice

- Identifica tutte le applicazioni pericolose o indesiderate e le destinazioni estranee di vari servizi cloud
- Sfrutta i dati reputazionali di WithSecure™ per identificare applicazioni potenzialmente dannose
- Limita le applicazioni e i servizi cloud potenzialmente pericolosi prima che si verifichi un data breach

WithSecure™ Elements – Riduci rischio informatico, complessità ed inefficienza

WithSecure™ Elements Endpoint Detection and Response è disponibile come soluzione stand-alone o come funzionalità integrate nella piattaforma di sicurezza informatica WithSecure™ Elements.



PROXIMALAB