Panoramica della soluzione

WithSecure™ Elements **Exposure Management**

Correzione delle esposizioni dalla prospettiva dell'attaccante

Alias
www.alias.it

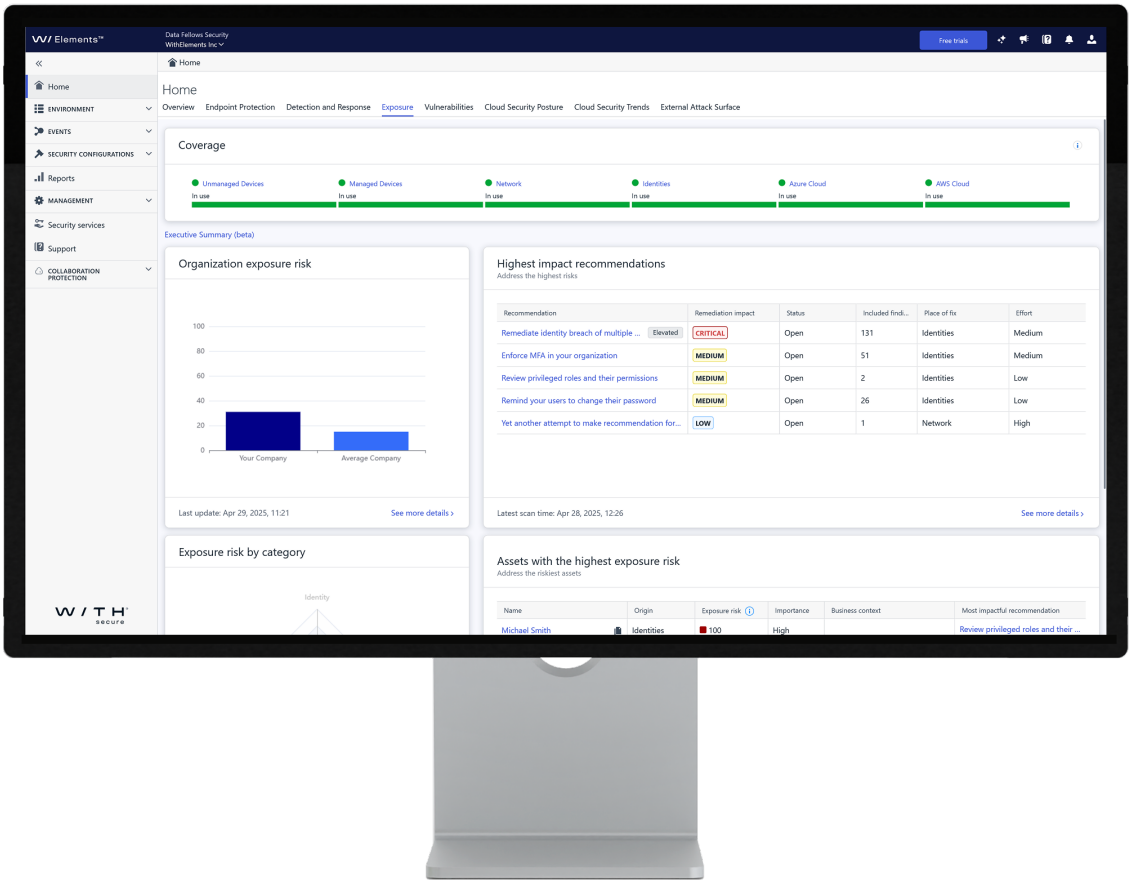
WITH secure

Indice

Ultimo aggiornamento: settembre 2025
Classificazione della sicurezza delle informazioni: pubblica
Dichiarazione di non responsabilità: il presente documento contiene una panoramica di alto livello dei principali componenti di sicurezza in WithSecure™ Elements Exposure Management. Sono stati omessi i dettagli al fine di prevenire attacchi mirati contro le nostre soluzioni. WithSecure™ migliora costantemente i propri servizi.
WithSecure™ si riserva il diritto di modificare le caratteristiche o le funzionalità del Software in conformità con le proprie pratiche relative al ciclo di vita dei prodotti.

Introduzione

WithSecure™ Elements Exposure Management (XM) è una soluzione continua e proattiva che prevede e previene le violazioni contro asset e attività della tua azienda. Elements XM fornisce visibilità sulla superficie di attacco e raccomandazioni che consentono una correzione efficace delle esposizioni ad impatto più elevato da una vista unificata. Scegli un'unica soluzione per la gestione a 360 gradi delle esposizioni digitali e per la visibilità sulla tua superficie di attacco esterna e sul profilo di sicurezza interna, per prevenire in modo proattivo i cyber attacchi.



Il passaggio da una cyber security reattiva a una proattiva è da tempo una priorità per i professionisti della sicurezza, ma le soluzioni soddisfacenti scarseggiano. Nell'era digitale odierna, le aziende devono affrontare un panorama di minacce in continua evoluzione, con la comparsa costante di nuove vulnerabilità, soprattutto con lo sviluppo dell'intelligenza artificiale (AI) che rende possibili nuovi tipi di cyber attacchi. Le organizzazioni hanno ambienti sempre più ibridi con confini poco definiti. La sfida non consiste solo nel proteggere i sistemi e i dati all'interno di questi confini, ma anche nel salvaguardare la continuità operativa dalle minacce esterne, come le compromissioni della supply chain digitale.

L'innovativa soluzione WithSecure™ Elements Exposure Management (XM) AI-powered affronta queste sfide fornendo funzionalità complete di gestione delle esposizioni. WithSecure™ è il fornitore leader nella gestione delle esposizioni per le piccole e medie imprese e i Managed Service Provider (MSP) europei, nonché per le organizzazioni che desiderano una cyber security in stile europeo. Elements XM fornisce strumenti e processi che valutano il grado di accessibilità e di esposizione degli asset digitali di un'organizzazione e quanto sia facile sfruttarli. Questa soluzione offre raccomandazioni continue simulando percorsi di attacco, identificando vulnerabilità critiche e offrendo risultati incentrati sul rischio per rafforzare le difese in modo proattivo.

Le organizzazioni solitamente isolano le attività di esposizione come i penetration test, la gestione della threat intelligence e la scansione delle vulnerabilità. Queste visioni compartimentate forniscono una consapevolezza scarsa o nulla della situazione complessiva relativa ai rischi effettivi che l'organizzazione deve affrontare. Elements XM abbina invece i dati provenienti dalla superficie di attacco esterna, dai sistemi di gestione delle identità (Entra ID), dai dispositivi, dalla rete e dai servizi cloud (Azure, AWS). Questa soluzione arricchisce questi dati con threat intelligence in tempo reale e contestualizzazioni aziendali per un approccio olistico alla sicurezza.

Le raccomandazioni AI-powered includono indicazioni per i team tecnici sulle azioni più efficaci da intraprendere per migliorare rapidamente il profilo di sicurezza. I percorsi di attacco visivi rendono i rischi di sicurezza facilmente comprensibili per i responsabili delle decisioni aziendali.

Il nostro servizio aggiuntivo WithSecure™ Elevate consente di inviarci una raccomandazione specifica per un'ulteriore analisi. Questa consulenza dei nostri esperti garantisce la validità e la priorità dell'elemento segnalato con Elevate, fornendo ulteriori indicazioni.

Cos'è la superficie di attacco?

"L'insieme dei punti sul confine di un sistema, di un elemento di sistema o di un ambiente in cui un attaccante può tentare di entrare, di causare un effetto o estrarre dati" *.

Cos'è un'identità?

L'identità è una presenza digitale che può essere un utente, un gruppo di utenti o un'intera organizzazione. Una persona può anche avere più identità digitali. Le identità possono rappresentare esseri umani o macchine e possono operare in ambienti locali, ibridi, regolari o privilegiati.

Nel contesto delle soluzioni WithSecure Elements, un'identità è un insieme di dati associati all'entità, protetti dalla soluzione Elements. Questi dati possono includere informazioni di identificazione personale (PII), diritti e privilegi di accesso, ruoli e gruppi a cui appartiene l'entità, asset associati all'identità, comportamento e attività online, contatti e altro ancora. La nostra attuale implementazione delle identità all'interno di Elements XM utilizza Entra ID come base.

Cosa sono i percorsi di attacco?

Un percorso di attacco simula i potenziali percorsi e le azioni che un attaccante potrebbe intraprendere all'interno dell'ambiente di un'organizzazione, con lo scopo principale di ottenere l'accesso agli asset più critici per l'azienda. Il reasoning engine di Elements XM è progettato per dare priorità alle azioni più accessibili e probabili da parte degli attaccanti, concentrandosi sui principali percorsi di attacco, per garantire un'efficace valutazione dei rischi e attività di risposta.

* NIST (National Institute of Standards and Technology). Definizione di "superficie di attacco" (Fonti: NIST SP 800-172 da GAO-19-128).

https://csrc.nist.gov/glossary/term/attack_surface (consultato il 22.8.2024)

1. Ottimizza la tua cyber resilienza con il minimo sforzo

Individua e agisci sulle tue esposizioni digitali prima che lo facciano i cyber criminali. Elements XM offre raccomandazioni continue sul modo per migliorare il profilo di sicurezza in base ai punteggi di esposizione degli asset che valutano il contesto in cui opera l'azienda, modellazione dei percorsi di attacco e threat intelligence dinamica come input principali.

Discover
Individua il tuo perimetro digitale e identifica le identità e gli asset più critici. Da un'unica interfaccia utente puoi ottenere una visione d'insieme della tua superficie di attacco, compresi gli asset quali dispositivi, cloud (AWS, Azure) e reti, nonché della superficie di attacco esterna e delle identità (Entra ID). Una vista a 360 gradi dei cyber rischi dell'organizzazione consente di identificare le esposizioni pericolose con una visibilità completa.

Prioritize
Le nostre valutazioni sulle esposizioni da correggere in via prioritaria si basano sulla simulazione del percorso di attacco che integra dati provenienti dalla threat intelligence di WithSecure e dal contesto in cui opera l'azienda.
I nuovi attacchi non saranno più una preoccupazione grazie all'integrazione dei dati di threat intelligence più recenti nella gestione delle esposizioni e potendo contare su una soluzione su misura per le tue esigenze aziendali basata su informazioni specifiche del contesto in cui opera l'azienda.
Garantisci la sicurezza dei tuoi asset più importanti con la gestione continua delle esposizioni, in cui il nostro recommendation engine AI-powered abbina i rilevamenti correlati e fornisce raccomandazioni sulla successiva correzione da implementare in base all'impatto.

Act
Seguendo le nostre indicazioni pratiche, potrai implementare le azioni correttive prioritarie per ridurre la superficie di attacco e il livello di rischio aziendale. Inizia a proteggere la superficie di attacco ottenendo raccomandazioni AI-powered per assegnare la priorità alle esposizioni più pericolose oppure, se non c'è tempo, intervieni rapidamente sulle esposizioni di massimo impatto con il minimo sforzo. Utilizza il Software Updater di WithSecure per applicare immediatamente le patch mancanti*. Comunica le informazioni relative al processo di correzione all'interno del portale, per garantire una collaborazione fluida tra i membri del tuo team di sicurezza. Il servizio aggiuntivo WithSecure™ Elevate consente di inviarci una raccomandazione specifica per un'analisi più approfondita e la convalida. Ripeti il processo di individuazione, definizione delle priorità e intervento sulle esposizioni per migliorare continuamente il profilo di sicurezza dell'organizzazione.

* Requires a license for WithSecure™ Elements Endpoint Protection (part of WithSecure™ Elements Endpoint Security).

2. Perché WithSecure™ Elements Exposure Management?

European Exposure Management

Soluzione Europea di Exposure Management all'avanguardia con threat intelligence locale, compliance e privacy, oltre alla nostra esperienza trentennale in attacchi reali.

Modellazione visualizzata dei percorsi di attacco

Modellazione AI-powered dei percorsi di attacco, in cui il nostro reasoning engine (motore di analisi) e i percorsi di attacco sono costruiti sulla base di un punteggio euristico dal punto di vista dell'attaccante.

Affrontare i rischi legati all'identità

Tratta le identità come asset facilmente soggetti a phishing e furto. Le identità possono essere utilizzate come potenti punti critici per interrompere i percorsi di attacco.

Progettato per le medie imprese

Ottimizzato per garantire la minima sicurezza efficace e progettato per offrire una cyber security democratizzata per le organizzazioni di medie dimensioni, garantendo facilità d'uso con risorse limitate.

Raccomandazioni AI-powered

Crea raccomandazioni attuabili su cosa correggere in base ai punteggi di rischio d'esposizione che utilizzano il nostro esclusivo approccio di modellazione dei percorsi di attacco come componente chiave.

Esperienza utente di sicurezza unificata

Parte di WithSecure™ Elements Cloud che offre un'esperienza utente unificata da un unico pannello di controllo, integrata da servizi di Co-Security come WithSecure™ Elevate.

3. Vantaggi

Individua la tua superficie di attacco

Individua cosa costituisce la tua superficie di attacco ottenendo una panoramica del tuo ambiente, inclusi asset, superficie di attacco esterna e identità, da un'unica interfaccia utente. Integra i dati provenienti dai dispositivi gestiti (workstation, server), dai servizi cloud (AWS, Azure), dalle identità (Entra ID), dalla rete (apparecchiature di rete, dispositivi non gestiti) e dalla superficie di attacco esterna (internet discovery, internet detections). Osserva il tuo ambiente attraverso un unico pannello di controllo.

Comprendi i percorsi di attacco

I percorsi di attacco espongono vari asset interni ai cyber attacchi. In genere, un attaccante tenterebbe di utilizzare questi percorsi di attacco per raggiungere asset aziendali critici, ad esempio nell'ambito di un attacco ransomware. Elements XM integra i dati provenienti dall'ambiente organizzativo interno ed esterno che costituiscono la superficie di attacco. Quindi integra questi dati con informazioni sul contesto in cui opera l'azienda e la più recente threat intelligence per simulare potenziali percorsi di attacco alla tua organizzazione. I nuovi attacchi non saranno più una preoccupazione grazie all'integrazione dei dati di threat intelligence più recenti nella gestione delle esposizioni. L'utilizzo delle informazioni relative al contesto in cui opera l'azienda consente di adattare la nostra modellazione del percorso di attacco e le raccomandazioni alle tue esigenze aziendali specifiche.

Elements Exposure Management rileva i percorsi di attacco dannosi che conducono agli asset cruciali prima che gli attaccanti possano sfruttarli. Identificando i punti critici in grado di bloccare gli attacchi sul nascere, Elements XM consente di migliorare notevolmente la protezione degli asset e dei dati aziendali, riducendo al minimo gli interventi correttivi necessari. In altre parole, Elements Exposure Management si concentra innanzitutto sull'interruzione della maggior parte dei percorsi di attacco pericolosi per la tua organizzazione.

Correggi in modo prioritario

Assicurati che i tuoi asset più importanti non possano essere sfruttati e mantienili al sicuro utilizzando una gestione continua delle esposizioni basata sull'intelligenza artificiale. Elements Exposure Management fornisce al tuo personale gli strumenti e i mezzi adeguati per risolvere con successo i problemi. Inizia a proteggere la tua superficie di attacco ottenendo raccomandazioni AI-powered per dare priorità alle esposizioni più dannose o, se c'è poco tempo, apportare correzioni rapide alle esposizioni che hanno il maggiore impatto con il minimo sforzo. È inoltre possibile utilizzare Software Updater di WithSecure per applicare immediatamente le patch software mancanti, con la semplice pressione di un pulsante e senza dover passare da una soluzione all'altra*.

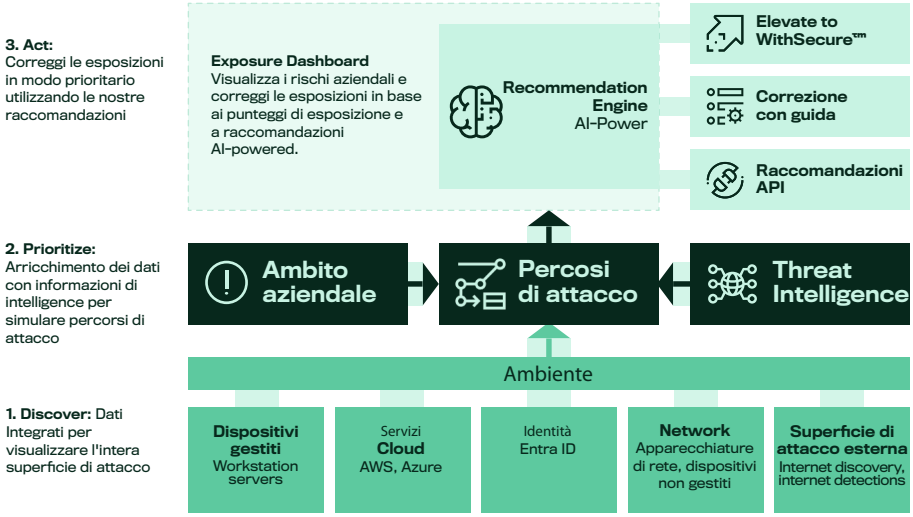
Il nostro recommendation engine funziona come un red team, un gruppo di persone che fingono di essere degli hacker, cercando potenziali vie di attacco alla tua organizzazione. Mentre il red teaming tradizionale è un'attività occasionale, Elements Exposure Management consente un "red teaming virtuale" gestito dall'intelligenza artificiale in modo continuo. Elements XM ti aiuta a riconoscere i punti deboli critici nella tua superficie di attacco, come asset o identità, che possono fungere da punti di accelerazione in un percorso di attacco – e viceversa

dal punto di vista di un difensore come punti critici per interrompere efficacemente i percorsi di attacco. Il tuo security administrator può facilmente risolvere i punti critici dei percorsi di attacco utilizzando raccomandazioni AI-powered, riducendo dunque al minimo il rischio di cyber attacchi in grado di compromettere gli asset aziendali critici.

*Richiede una licenza per WithSecure™ Elements Endpoint Protection (parte di WithSecure™ Elements Endpoint Security) che include la funzionalità Software Updater.

4. Come funziona

Ottieni una visione a 360° dei cyber rischi. Visualizza la superficie di attacco completa e correggi le vulnerabilità, le configurazioni errate e altre esposizioni che comportano il rischio maggiore di intrusione per la tua organizzazione. Proteggi i percorsi di attacco agli asset critici della tua azienda.



1. Discover: Elements Exposure Management integra i dati provenienti dai tuoi ambienti interni ed esterni per fornire una panoramica completa della tua superficie di attacco:

- Superficie di attacco esterna (compresi internet discovery e internet detections)
- Servizi cloud (Azure, AWS)
- Identità (Entra ID)
- Dispositivi gestiti (workstation e server)
- Network (apparecchiature di rete come firewall e switch, dispositivi non gestiti)

2. Prioritize: Elements XM utilizza vulnerabilità, configurazioni errate e altre esposizioni nel tuo ambiente per identificare potenziali percorsi di attacco. Abbina le conoscenze relative alla superficie di attacco esterna con informazioni sul profilo di sicurezza interna, quali le vulnerabilità degli asset e le configurazioni errate del cloud. Ciò consente di comprendere le esposizioni pericolose e i percorsi di attacco che conducono agli asset critici per l'azienda. Elements XM arricchisce i dati integrati con threat intelligence aggiornata ed informazioni sul contesto in cui opera l'azienda, simulando percorsi di attacco basati su tali informazioni. Questa soluzione visualizza i percorsi di attacco e li utilizza per fornire raccomandazioni AI-powered che aiutano a stabilire le priorità di intervento.

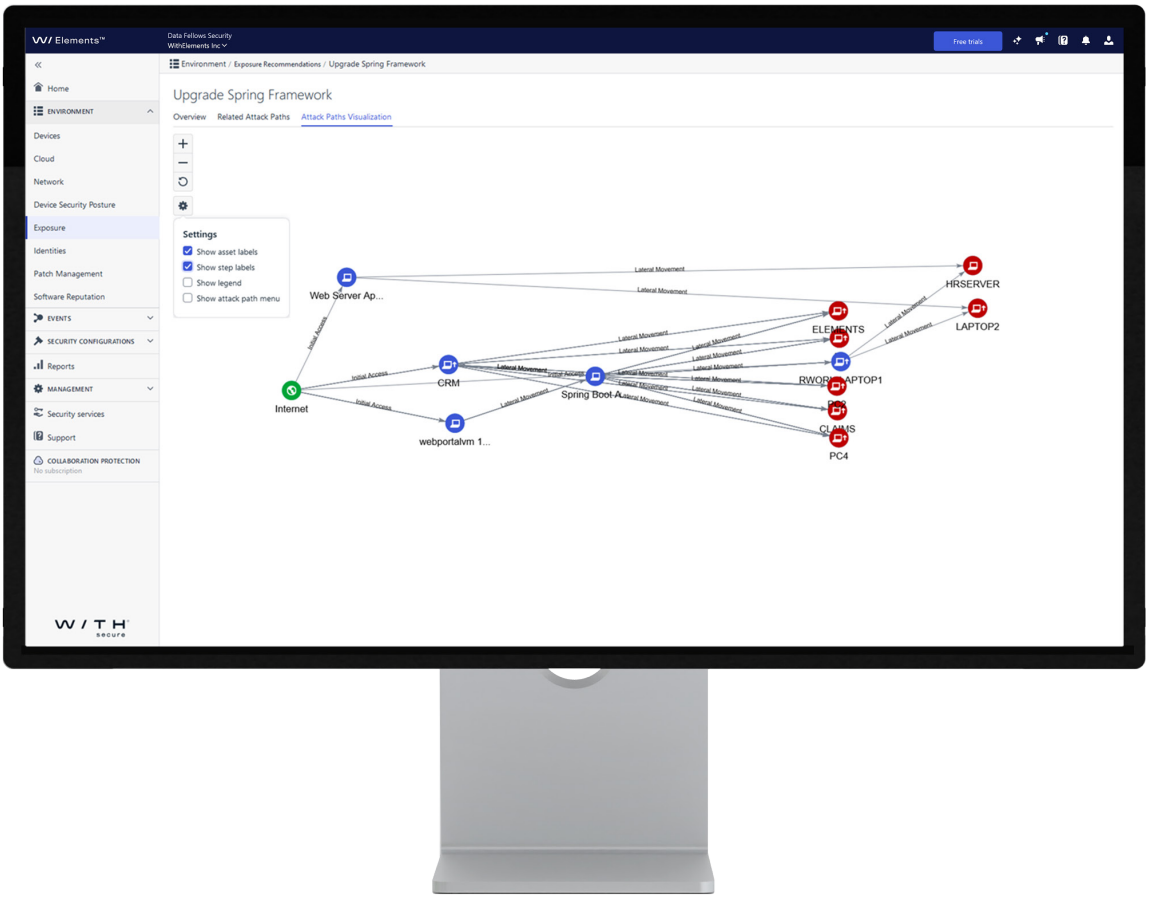
3. Act: La panoramica fornita dall'Exposure Dashboard aiuta a promuovere azioni di correzione prioritarie e offre una visione d'insieme basata sul rischio delle vulnerabilità individuate nella superficie di attacco. Il recommendation engine AI-powered ti consiglia azioni correttive in base a gruppi di risultati con un impatto elevato sulla tua esposizione complessiva. Le nostre raccomandazioni sono accompagnate da indicazioni pratiche su come intraprendere azioni correttive. Offriamo anche la possibilità di utilizzare il Software Updater di WithSecure per applicare immediatamente le patch software mancanti, con la semplice pressione di un pulsante*. Visualizzare i punteggi di esposizione della tua azienda, dei diversi tipi di asset e dei singoli asset ti aiuta ulteriormente a stabilire le priorità degli interventi correttivi. Il nostro servizio aggiuntivo WithSecure™ Elevate consente di inviarci una raccomandazione specifica per un'ulteriore analisi. Questa consulenza dei nostri esperti garantisce la validità e la priorità dell'elemento segnalato con Elevate, fornendo ulteriori indicazioni. Sfrutta la nostra integrazione Recommendations API per inviare dati da Elements XM ai tuoi sistemi SIEM e di ticketing per un'erogazione efficiente dei servizi. Questi dati includono raccomandazioni AI-powered e i relativi risultati.

*Richiede una licenza per WithSecure™ Elements Endpoint Protection (parte di WithSecure™ Elements Endpoint Security).

5. Gestisci in modo continuo le tue esposizioni digitali con la nostra tecnologia

Exposure Dashboard (Cruscotto)

Niente più affaticamento da avvisi. Mantieni la correzione delle esposizioni semplice ed efficace con la nostra dashboard Elements Exposure Management, che ti mostra dove concentrare i tuoi sforzi di correzione da un'unica schermata. Comprendi i rischi aziendali e raccomanda le azioni da intraprendere per migliorare il profilo di sicurezza. Verifica la solidità della tua superficie di attacco tramite la panoramica sulle esposizioni, che ti offre una visione d'insieme basata sul rischio delle vulnerabilità individuate nella tua superficie di attacco. Identifica gli asset aziendali critici a rischio utilizzando i punteggi di esposizione per iniziare a dare priorità alla correzione degli asset che rischiano maggiormente lo sfruttamento. Scopri i prossimi passi da compiere per migliorare le esposizioni, ottenendo consigli su cosa correggere per prima cosa e per un'azione rapida e semplice, grazie al nostro recommendation engine AI-powered.



Percorsi di attacco

Elements XM simula i percorsi di attacco che un attaccante potrebbe seguire per compromettere il patrimonio di un cliente. Anziché creare percorsi di attacco ottimizzati per il tragitto più breve dalla superficie di attacco esterna agli asset critici per l'azienda, il nostro reasoning engine (motore di analisi) e i percorsi di attacco si basano su un punteggio euristico dal punto di vista dell'attaccante. Ciò significa che il nostro motore di intelligenza artificiale analizza l'ambiente del cliente dal punto di vista di un attaccante, cercando di individuare i punti deboli e individuando il percorso da un asset all'altro che causa il massimo danno. La nostra logica decisionale si basa su decenni di esperienza nell'analisi di attacchi reali e sulla nostra telemetria di rilevamento Extended Detection and Response (XDR).

Questo è ciò che significa il vero red teaming basato su AI. Il nostro recommendation engine funziona come un red team, ovvero un gruppo di persone che fingono di essere degli hacker, cercando potenziali percorsi di attacco nella tua organizzazione. Mentre il red teaming tradizionale è un esercizio che occasionalmente può rappresentare un investimento utile per alcune aziende, il nostro Elements Exposure Management consente un red teaming virtuale continuo basato su AI.

Visualizzazione del percorso di attacco

Elements XM visualizza i percorsi di attacco relativi a una raccomandazione, consentendo di approfondire il ragionamento sottostante. La visualizzazione del percorso di attacco fornisce informazioni dettagliate sugli asset, le fasi e le identità coinvolte nel percorso di attacco, comprendendo anche le tecniche utilizzate, gli accessi ottenuti e le risorse correlate. Di seguito sono riportati i principali casi d'uso della visualizzazione dei percorsi di attacco:

- **Convalida:** i percorsi di attacco convalidano le raccomandazioni fornite dal nostro motore AI-powered, consentendoti di stabilire priorità di risposta informate per un processo decisionale trasparente.
- **Collaborazione tra gli stakeholder:** facilita la comunicazione di informazioni dettagliate sui percorsi di attacco agli stakeholder, inclusi clienti, responsabili delle decisioni aziendali e amministratori IT, grazie a immagini di facile comprensione.
- **Valutazione dei rischi:** fornisce prospettive alternative sul rischio, migliorando le attività di valutazione dei rischi.

Recommendation Engine AI-powered

WithSecure utilizza da quasi un decennio diversi modelli di machine learning per supportare le funzionalità di rilevamento e risposta e il nostro progetto pluriennale di ricerca sull'AI "Blackfin" è stato premiato con l'AI Excellence Award per le tecniche di intelligenza collettiva. Grazie al nostro recommendation engine AI-powered che individua i percorsi di attacco tra gli asset, Elements XM contribuisce a ridurre il livello di rischio di esposizione fornendo raccomandazioni su quali esposizioni affrontare per prime. Le nostre raccomandazioni si basano su punteggi di esposizione che utilizzano elementi quali la nostra raccolta di dati di threat intelligence, le informazioni sul contesto specifico in cui opera l'azienda e il nostro approccio all'avanguardia AI-powered per la modellazione dei percorsi di attacco.

Gestione della superficie di attacco esterna (EASM)

Proteggi i tuoi domini, IP e asset pubblici. Exposure Management utilizza l'internet discovery tramite crawling e la mappatura delle porte per raccogliere dati sui sistemi pubblici. È possibile utilizzare i dati sulla base di posizione, dominio di primo livello, dominio di livello pay, parole chiave, nome host e indirizzo IP. Le internet detections aiutano ad individuare il rischio di takeover dei domini e la divulgazione delle informazioni dall'elenco delle directory. Aggiungiamo continuamente nuove internet detctions basate sull'attuale panorama delle minacce. Inoltre, il nostro nodo di scansione cloud consente la scansione da parte del sistema e delle applicazioni web degli asset accessibili via Internet per individuare eventuali vulnerabilità.

Esposizioni a rischi per le identità

Utilizza i dati relativi alle identità digitali, siano esse umane o non umane, e affronta i rischi legati alle identità integrando i tuoi dati Entra ID in Elements XM. Ciò fornisce un contesto delle identità per ogni esposizione e include dati relativi alle identità come input per identificare percorsi di attacco pericolosi. Comprende i vettori di attacco alle identità che consentono la potenziale escalation dei diritti di accesso alle identità. La nostra funzionalità di individuazione dell'esposizione per i rischi legati alle identità fornisce una valutazione continua dei rischi basati sulle identità nel tuo ambiente e contribuisce a prevenire l'uso delle identità nei percorsi di attacco. Fai la tua parte nella prevenzione delle violazioni della supply chain e migliora le pratiche di sicurezza dei dipendenti e l'igiene della sicurezza.

WithSecure™ Elevate

Gli utenti di Elements possono richiedere l'invio di una segnalazione specifica a WithSecure per l'analisi e per ottenere una consulenza da parte di WithSecure sulla validità e la priorità dell'elemento segnalato. Ottieni assistenza dai nostri esperti di sicurezza per compiere i passi successivi e comprendere perché determinati risultati sono importanti.

Il nostro team di esperti nella ricerca delle minacce e di consulenti di sicurezza prenderà in carico la richiesta Elevate, analizzerà i risultati, le raccomandazioni o il percorso di attacco segnalati e aggiornerà il cliente in modo appropriato.

Luminen GenAI per Elements XM

Potenzia la tua soluzione Elements XM con le raccomandazioni di Luminen GenAI, comprese le istruzioni per la correzione delle esposizioni fornite nelle lingue locali. Luminen è automaticamente incluso nella licenza Elements XM.

L'assistente aggrega i risultati, gli asset e le istruzioni di correzione in un riepilogo sinergico. Luminen può anche fornirti consigli personalizzati che utilizzano i nomi dei tuoi asset. Il Security Awareness Assistant di Luminen ora riunisce anche i più importanti eventi di sicurezza XDR e XM in un unico riepilogo, comprese le raccomandazioni di Elements XM.

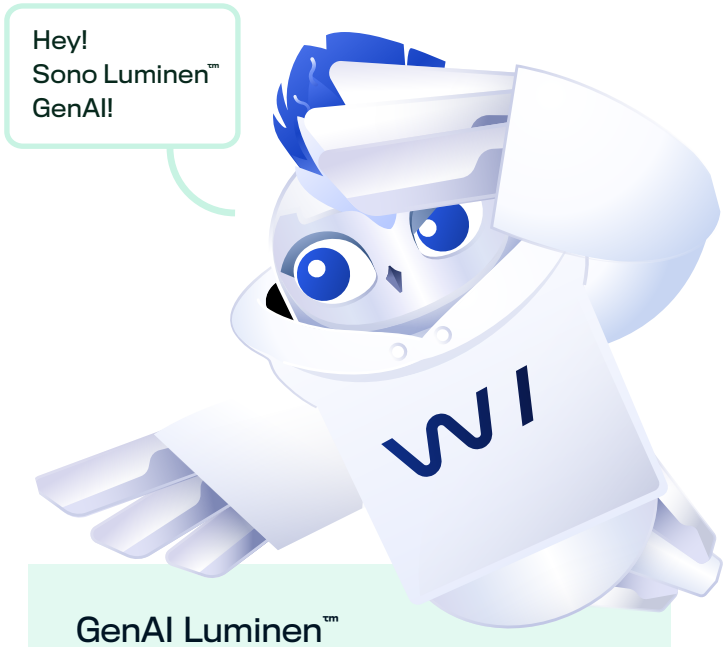
Protezione ibrida dalle minacce

Elements XM comprende le minacce ibride, come i percorsi di attacco ibridi dagli asset locali a quelli cloud o dalle credenziali utente divulgate alle risorse cloud. Ciò garantisce un'ampia protezione contro i percorsi di attacco che coinvolgono minacce alle identità e sul cloud:

- **Identità utente con privilegi potenzialmente eccessivi:** Elements XM indica quali identità dispongono di privilegi estesi, poiché gli utenti con privilegi elevati sono obiettivi interessanti per gli autori delle minacce a causa dei loro ampi diritti di accesso. La trasparenza negli account con diritti estesi consente agli amministratori della sicurezza di ridurre al minimo i potenziali danni derivanti da violazioni dei dati e minacce interne.

- **Attacchi ibridi basati sule identità:** per modellare il movimento laterale tra diversi ambienti, ad esempio dall'identità ai dispositivi e poi al cloud, il nostro reasoning engine AI-powered riconosce quale utente ha effettuato o potrebbe effettuare l'accesso e a quale dispositivo. A tal fine, utilizza un database di identità utente locali e basate su cloud (Entra ID), collegando le identità ai dispositivi utilizzati più di frequente. In questo modo, il nostro motore può anche simulare e visualizzare una violazione dei dati che potrebbe verificarsi utilizzando identità rubate.

- **Attacchi ibridi basati sul cloud:** analogamente agli attacchi ibridi basati sulle identità, Elements XM simula attacchi che utilizzano il movimento laterale da ambienti cloud verso dispositivi on-premise o macchine degli sviluppatori. I percorsi di attacco in cloud di Elements XM comprendono gli obiettivi comuni degli attaccanti e le attuali tendenze di sfruttamento negli ambienti cloud, identificate nella ricerca di threat intelligence di WithSecure (come cryptojacking, furto di dati e ransomware).



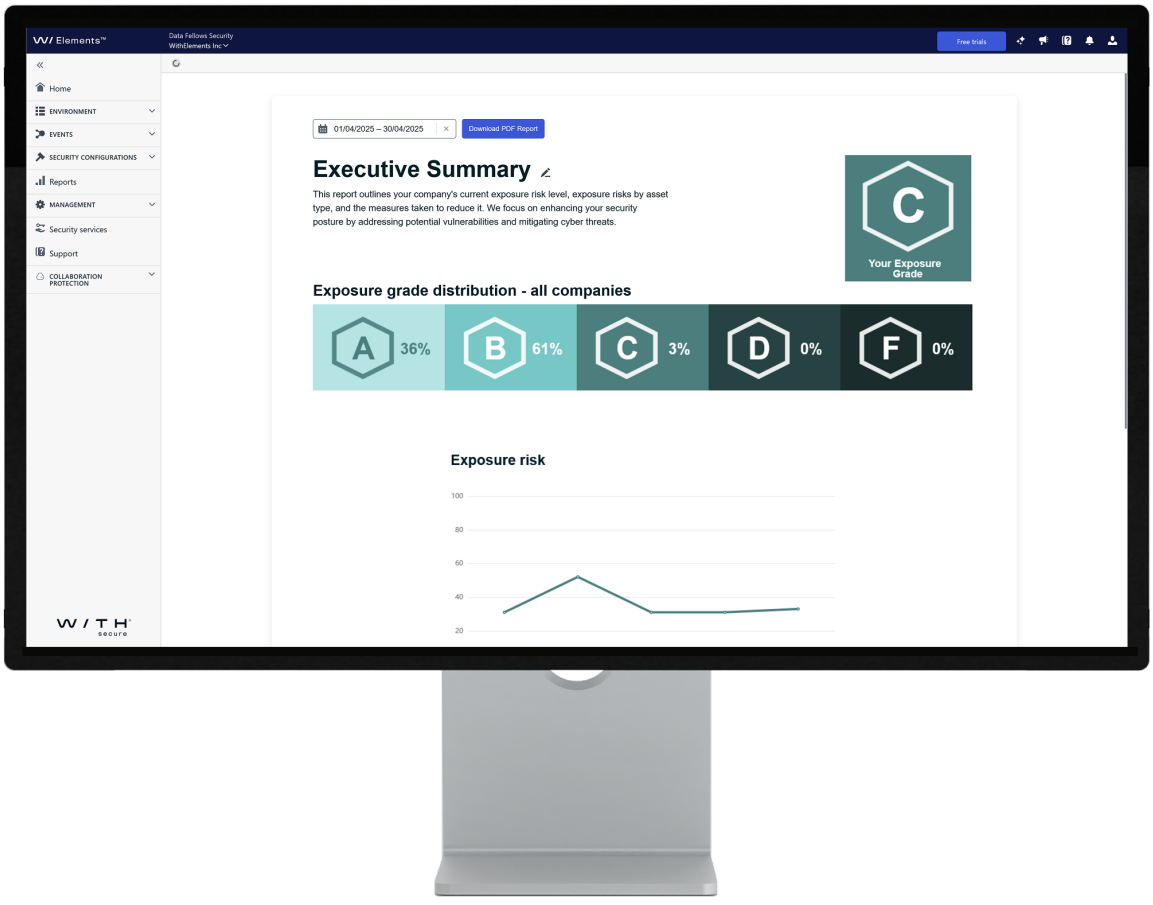
GenAI Luminen™

Utilizza il nostro utile assistente di sicurezza GenAI, Luminen, per ottenere il massimo dalla soluzione Elements XM migliorando l'efficacia delle attività di correzione delle esposizioni svolte dai tuoi analisti della sicurezza.

Report personalizzati e C-level

Aiuta i tuoi responsabili delle decisioni ad effettuare scelte informate sui rischi aziendali con i C-level Reports per Elements XM. Il reporting C-level mostra il valore delle attività di gestione delle esposizioni sotto forma di sintesi esecutiva.

Gli approfondimenti di Elements XM fanno anche parte di My Reports, che consente di creare report personalizzabili per l'intera suite Elements in uso. Utilizzando My Reports, puoi facilmente dimostrare il valore della gestione continua dell'esposizione pianificando report PDF di facile comprensione da inviare su base continuativa. I report mostrano lo stato complessivo e le tendenze delle esposizioni aziendali e l'impatto delle azioni di gestione delle esposizioni.



6. Scansiona il tuo ambiente

WithSecure™ Elements Exposure Management abbina diversi metodi di scansione disponibili per garantire la copertura completa della superficie di attacco. Inoltre, la tecnologia di simulazione del percorso di attacco, che integra diversi tipi di metodologie di scansione, costituisce di per sé un metodo di scansione sinergico.

Dispositivi gestiti e rete

Nodo locale	Agente Elements
Discovery Scan Identifica e mappa tutti gli asset all'interno della tua rete	**Scansione basata su agenti** Esegui la scansione automatica delle workstation e dei server Windows
System Scan Esegui la scansione di tutti i sistemi IP (Internet Protocol) alla ricerca di vulnerabilità e configurazioni errate.	**Dati di servizio del dispositivo** Configurazione del sistema e informazioni di accesso
Scansione autenticata* Accedi ai sistemi per ottenere dati più dettagliati sulle vulnerabilità, come versioni vulnerabili dei sistemi, patch mancanti e configurazioni errate.	**Gestione delle patch** Stato delle patch di terze parti e di sistema e aggiornamenti automatici tramite Software Updater**

* Non disponibile utilizzando un nodo di scansione cloud.

** Richiede una licenza per WithSecure™ Elements Endpoint Protection (parte di WithSecure™ Elements Endpoint Security).

Superficie di attacco esterna, identità e servizi cloud

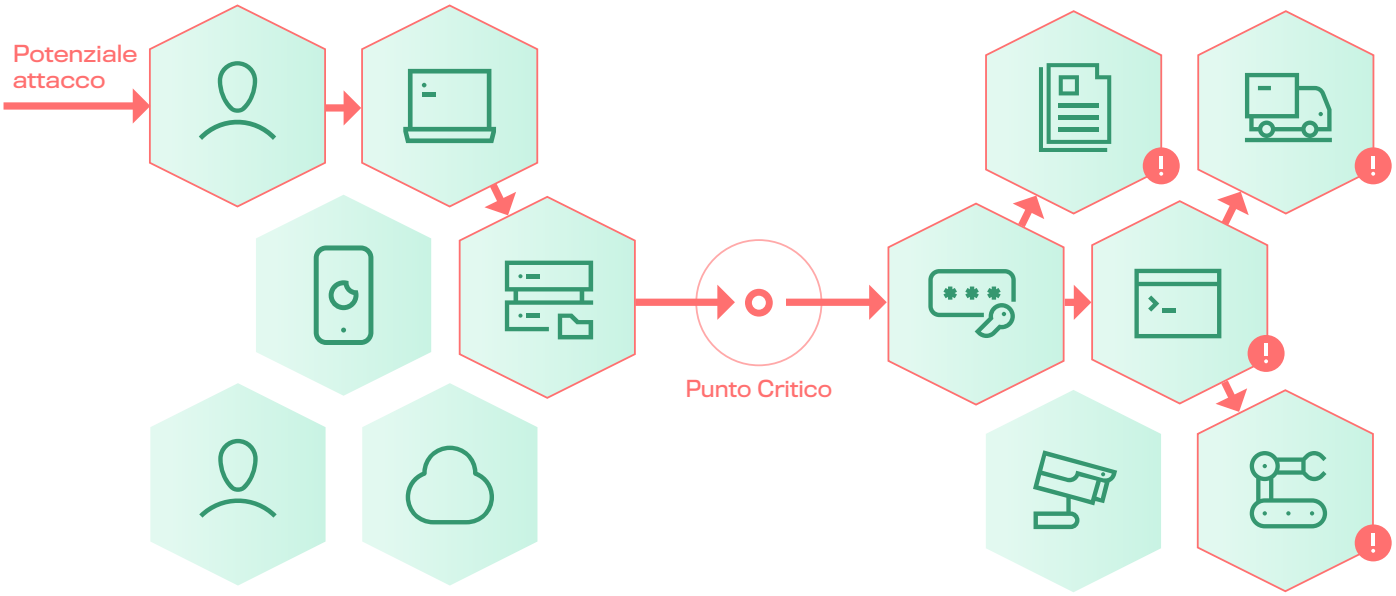
Superficie di attacco esterna e nodo di scansione cloud	Integrazioni Identità	Integrazioni cloud
Internet Discovery Identifica i sistemi della tua organizzazione esposti su Internet	**Entra ID** Individua le potenziali minacce associate a tutte le identità in Entra ID	**Azure** Valuta il profilo di sicurezza e conformità dei tuoi account
Scansione del sistema (nodo di scansione cloud) Esegui la scansione di tutti i sistemi IP (Internet Protocol) accessibili dall'esterno per individuare vulnerabilità e configurazioni errate.	**Violazione degli account** Informazioni relative agli 'account violati	AWS Valuta il profilo di sicurezza e conformità dei tuoi account
Asset esterni Valuta il profilo di sicurezza dei tuoi asset esposti all'esterno		
Scansione Web Esegui la scansione e verifica la presenza di vulnerabilità nelle applicazioni web personalizzate		

Nota: le scansioni per le integrazioni cloud fanno parte della licenza WithSecure™ Elements Exposure Management for Cloud, mentre gli altri tipi di scansione fanno parte della licenza WithSecure™ Elements Exposure Management for Business.

7. Motore euristico per il percorso di attacco

WithSecure™ Elements Exposure Management utilizza tecnologie di simulazione del percorso di attacco basate su AI e in attesa di brevetto per la ricerca euristica delle esposizioni e la convalida delle esposizioni ostili.

I percorsi di attacco simulano scenari di potenziali compromissioni prima che si verifichino. Il nostro motore euristico, unico nel suo genere, funge da tester di sicurezza virtuale 24 ore su 24, 7 giorni su 7 (pen tester). Individua e convalida i percorsi di attacco per indirizzare i tuoi sforzi di sicurezza nelle aree che offrono i risultati più efficaci. In sostanza, individua il numero minimo di asset da correggere per interrompere il numero massimo di percorsi di attacco.



Elements XM for Cloud identifica in modo proattivo i rischi legati a configurazioni errate

Elements XM for Cloud valuta la configurazione delle risorse distribuite in AWS e Azure, per identificare i punti deboli che potrebbero essere sfruttati da un attaccante. Ciò include decine di diversi tipi di risorse AWS e Azure e circa duecento controlli di configurazione. Il set di regole che utilizziamo si basa sulle ricerche più avanzate e sulle più recenti tecniche di attacco sviluppate dagli esperti di sicurezza cloud di WithSecure, nonché sulle best practice delineate da AWS e Azure.

8. Requisiti tecnici

Sistemi supportati

Poiché il nostro portale di gestione, WithSecure Elements Security Center, è basato su cloud, per accedervi è sufficiente disporre di un browser web moderno e di una connessione Internet. Supportiamo le ultime versioni dei seguenti browser: Microsoft Edge, Mozilla Firefox, Google Chrome e Safari.

Tuttavia, a seconda degli ambienti che desideri integrare in WithSecure Elements Exposure Management, dovrai integrare i tuoi dispositivi (Windows, Linux; consulta i requisiti del sistema operativo a destra), account cloud (AWS, Azure), asset di rete e identità (Entra ID). Per ulteriori informazioni sull'onboarding degli asset, consulta la guida utente di Exposure Management.

Proteggi gli ambienti che costituiscono la tua superficie di attacco

Il nostro approccio multi-ambiente include i seguenti asset e ambienti:

- Superficie di attacco esterna
- Servizi cloud (piattaforme Azure e AWS)
- Identità (Entra ID)
- Dispositivi gestiti, inclusi work station e server
- Networking incluse le apparecchiature di rete

Lingue supportate

Inglese, finlandese, francese, tedesco, italiano, giapponese, polacco, portoghese (Brasile), spagnolo (America Latina), svedese e cinese tradizionale (Taiwan).

Installazione sui dispositivi

L'installazione di Elements Agent richiede uno dei seguenti sistemi operativi Windows:

- Per i dispositivi: Microsoft Windows 10 o 11
- Per i server: Microsoft Windows Server 2016 o versioni successive (installazione completa, non Server Core)

Per l'installazione dei nodi di scansione, sono richiesti i seguenti requisiti di sistema operativo:

- Windows Server 2012 R2 o versioni successive
- Linux (Ubuntu Server e Debian (entrambi solo versioni a 64 bit); SSH)

Prezzi

WithSecure Elements Exposure Management for Business (comprende identità, rete, dispositivi gestiti ed EASM):

- prezzo per utente con workstation
- prezzo per server in uso (Windows, Linux)
- add-on: prezzo per utente senza workstation (operatori in prima linea) tramite WithSecure Elements Exposure Management Frontline Add-On

WithSecure Elements Exposure Management for Cloud (comprende i servizi cloud):

- Commissione legata ai consumi cloud delle risorse analizzate.

9. Panoramica di WithSecure™ Elements Cloud Platform

WithSecure™ Elements Exposure Management è disponibile come funzionalità integrata nella piattaforma modulare di cyber security WithSecure™ Elements.

WithSecure™ Elements offre ai clienti una protezione completa in un'unica piattaforma unificata e un centro di sicurezza facile da usare. La piattaforma centralizzata abbina potenti funzionalità di sicurezza predittiva, preventiva e reattiva in una protezione intelligente contro le minacce, dal ransomware agli attacchi mirati. La nostra semplicità senza pari consente ai clienti di concentrarsi su ciò che è più importante per loro.

I pacchetti di prodotti modulari e i modelli di prezzo flessibili offrono ai clienti la libertà di evolversi. Seleziona i moduli software più adatti per le tue esigenze aziendali e integrale con i nostri servizi Co-Security. WithSecure™ Elements può diventare parte integrante dell'ecosistema del cliente. Può essere facilmente collegato ai loro sistemi SIEM, SOAR, di gestione della sicurezza, monitoraggio o reporting.

Alias
www.alias.it

Gestisci il rischio aziendale.
Supera in astuzia gli attaccanti.
Sei pronto a massimizzare la tua cyber resilienza
con il minimo sforzo utilizzando
WithSecure™ Elements Exposure Management?

Chi siamo

WithSecure™, precedentemente F-Secure Business, è il partner di fiducia in Europa per la cyber security. Scelti da provider di servizi IT, MSSP e aziende di tutto il mondo, forniamo soluzioni di cyber security basate sui risultati per la protezione delle aziende del mid-market.

Impegnata a seguire il modello europeo di protezione dei dati, WithSecure™ dà priorità alla privacy, alla sovranità dei dati e alla conformità normativa.

Con oltre 35 anni di esperienza nel settore, WithSecure™ ha progettato il proprio portafoglio per affrontare il cambiamento paradigmatico dalla cyber security reattiva a quella proattiva. In linea con il suo impegno per una crescita collaborativa, WithSecure™ offre ai partner modelli commerciali flessibili, garantendo il successo reciproco nel panorama dinamico della cyber security.

Il fulcro dell'offerta all'avanguardia di WithSecure è Elements Cloud, che integra perfettamente tecnologie AI-powered, competenze umane, e servizi di co-security. Inoltre, potenzia i clienti del mid-market con funzionalità modulari che vanno dalla protezione degli endpoint e del cloud, al rilevamento e risposta alle minacce, fino alla gestione delle esposizioni.

WithSecure™ Corporation è stata fondata nel 1988 ed è quotata al NASDAQ OMX Helsinki Ltd.

Alias
www.alias.it

WITH secure