WithSecure™ Elements Exposure Management

Exposure remediation through the attacker's lens

October 2024

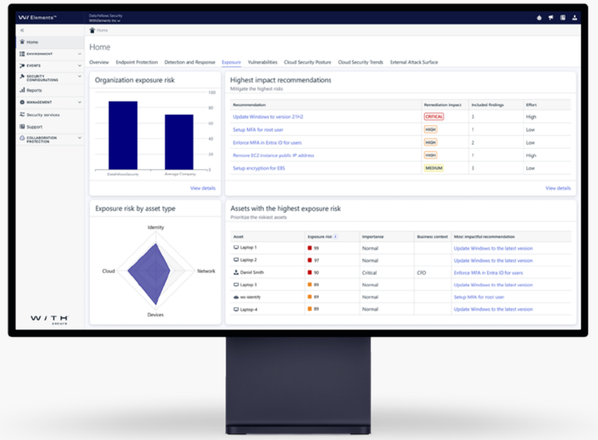
Introducción

WithSecure™ Elements Exposure Management (XM) es una solución continua y proactiva que predice y previene brechas de seguridad contra los activos y las operaciones de su empresa. Elements XM proporciona visibilidad de su superficie de ataque y sus recomendaciones permiten la remediación eficiente de sus exposiciones de mayor impacto desde una perspectiva unificada. Obtenga una solución integral para la gestión de la exposición digital y la visibilidad de su superficie de ataque externa y su estrategia de seguridad interna, para prevenir ciberataques de forma proactiva.

La transición de la ciberseguridad reactiva a la proactiva ha sido una prioridad para los profesionales de la seguridad desde hace tiempo, pero las soluciones satisfactorias han sido escasas. En la era digital actual, las empresas se enfrentan a un panorama de amenazas en constante evolución, con nuevas vulnerabilidades que surgen constantemente, especialmente con el desarrollo de la Inteligencia Artificial (IA), que permite nuevos tipos de ciberataques. Las organizaciones tienen entornos cada vez más híbridos con límites difusos. El reto no solo reside en proteger los sistemas y datos dentro de estos límites, sino también en salvaguardar la continuidad del negocio frente a amenazas externas, como los riesgos en la cadena de suministro digital.

El innovador sistema WithSecure™ Elements Exposure Management (XM), basado en IA, aborda estos desafíos ofreciendo capacidades integrales de gestión de la exposición.WithSecure™ es el proveedor líder en gestión de la exposición para pymes europeas y proveedores de servicios gestionados, así como para organizaciones que buscan una ciberseguridad a la europea. Elements XM proporciona herramientas y procesos que evalúan la accesibilidad y exposición de los activos digitales de una organización, así como la facilidad para explotarlos. La solución ofrece recomendaciones continuas mediante la simulación de rutas de ataque, la identificación de vulnerabilidades críticas y la generación de resultados centrados en el riesgo para reforzar las defensas de forma proactiva.

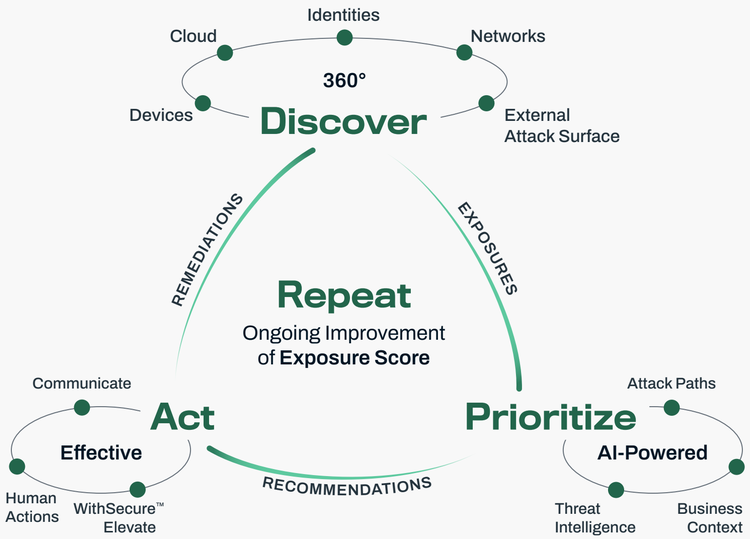
Por lo general, las organizaciones aíslan actividades de exposición, como pruebas de penetración, gestión de inteligencia de amenazas y análisis de vulnerabilidades. Estas vistas aisladas ofrecen poca o ninguna información sobre la situación general de los riesgos reales que enfrenta la organización. Sin embargo, Elements XM combina datos de la superficie de ataque externa, los sistemas de gestión de identidades (Entra ID), los dispositivos, la red y los servicios en la nube (Azure, AWS). La solución enriquece estos datos con inteligencia de amenazas en tiempo real y el contexto empresarial para un enfoque de seguridad integral. Las recomendaciones basadas en IA incluyen orientación para los equipos técnicos sobre cómo tomar las medidas más eficaces para mejorar rápidamente la seguridad. Las rutas de ataque visuales facilitan la comprensión de los riesgos de seguridad para los responsables de la toma de decisiones empresariales.



Nuestro servicio adicional WithSecure™ Elevate permite enviarnos una recomendación específica para un análisis más detallado. Esta consulta con nuestros expertos garantiza la validez y la prioridad del elemento elevado, brindándonos mayor orientación.

Maximice su resiliencia cibernética con el mínimo esfuerzo

Descubra y actúe ante sus exposiciones digitales antes de que lo hagan los ciberdelincuentes. Elements XM ofrece recomendaciones continuas para mejorar la seguridad, basadas en puntuaciones de exposición de activos que utilizan el contexto empresarial, el modelado de rutas de ataque y la inteligencia dinámica de amenazas como datos clave.



1. Discubre
Descubra su perímetro digital e identifique los activos e identidades más críticos. Vea una visión general de su superficie de ataque desde una única interfaz de usuario, incluyendo activos como dispositivos, la nube (AWS, Azure) y redes, así como su superficie de ataque externa e identidades (Entra ID). Obtenga una visión integral de los ciberriesgos de su organización para identificar sus exposiciones peligrosas sin brechas de visibilidad.

2. Priorizar
Nuestras conclusiones sobre qué exposiciones priorizar en la remediación se basan en la simulación de la ruta de ataque, que integra datos de inteligencia de amenazas de WithSecure y el contexto de su negocio. Puede estar tranquilo ante nuevos ataques al contar con los datos de inteligencia de amenazas más recientes como parte integral de la gestión de la exposición, y saber que la solución se adapta a las necesidades específicas de su negocio gracias a la información del contexto empresarial. Asegúrese de que sus activos más críticos estén protegidos mediante la gestión continua de la exposición, donde nuestro motor de recomendaciones basado en IA combina los hallazgos relacionados y ofrece recomendaciones prácticas sobre qué remediar a continuación según el impacto.

3. Actuar
Implemente acciones de remediación priorizadas para reducir su superficie de ataque y disminuir el nivel de riesgo empresarial con nuestra guía práctica. Empiece a proteger su superficie de ataque con recomendaciones basadas en IA para priorizar las exposiciones más dañinas o, si tiene poco tiempo, implemente soluciones rápidas a las exposiciones de mayor impacto con el mínimo esfuerzo. Utilice el Actualizador de Software de WithSecure para aplicar los parches faltantes al instante*. Comuníquese sobre el proceso de remediación dentro del portal para una colaboración fluida con su equipo de seguridad. El servicio adicional WithSecure™ Elevate permite enviarnos una recomendación específica para su posterior análisis y validación. Repita el proceso de detección, priorización y actuación sobre sus exposiciones para mejorar continuamente la seguridad de su organización.

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

¿Qué es una superficie de ataque?

“El conjunto de puntos en el límite de un sistema, un elemento del sistema o un entorno donde un atacante puede intentar entrar, causar un efecto o extraer datos de ese sistema, elemento del sistema o entorno”*.

¿Qué es una identidad?

La identidad es una presencia digital que puede ser un usuario, un grupo de usuarios o una organización completa. Una persona también puede tener múltiples identidades digitales. Las identidades pueden representar humanos o máquinas y operar en entornos locales, híbridos, convencionales o privilegiados.

En el contexto de las soluciones WithSecure Elements, una identidad consiste en un conjunto de datos asociados a la entidad, protegidos por la solución Elements. Estos datos pueden incluir información de identificación personal (PII), derechos y privilegios de acceso, roles y grupos a los que pertenece la entidad, activos asociados a la identidad, comportamiento y actividad en línea, contactos, etc. Nuestra implementación actual de identidades en Elements XM utiliza Entra ID como base.

¿Qué son las rutas de ataque?

Una ruta de ataque simula las posibles rutas y acciones que un atacante podría tomar dentro del entorno de una organización, con el objetivo de acceder a los activos más críticos para el negocio. El motor de razonamiento de Elements XM está diseñado para priorizar las acciones más accesibles y probables de los atacantes, centrándose en las rutas de ataque principales, para garantizar una evaluación de riesgos y actividades de respuesta eficaces.

* NIST (National Institute of Standards and Technology). “attack surface” definition (Sources: NIST SP 800-172 from GAO-19-128). https://csrc.nist.gov/glossary/term/attack_surface (Accessed 22.8.2024)

Por qué WithSecure™ Elements Exposure Management?

European Exposure Management

Gestión de exposición europea líder con inteligencia de amenazas locales, cumplimiento y privacidad, además de nuestros más de 30 años de experiencia en ataques en el mundo real.

Modelado de ruta de ataque visualizada

Modelado de rutas de ataque impulsado por IA, donde nuestro motor de razonamiento y nuestras rutas de ataque se basan en una puntuación heurística a través de la lente del atacante.

Abordar los riesgos basados en la identidad

Considera las identidades como activos que se pueden suplantar y robar fácilmente. Pueden utilizarse como puntos de estrangulamiento para interrumpir las rutas de ataque.

Diseñado para empresas medianas

Optimizado para una seguridad mínima efectiva y diseñado para ofrecer seguridad cibernética democratizada para organizaciones de tamaño mediano, proporcionando facilidad de uso con recursos limitados.

Recomendaciones impulsadas por IA

Crea recomendaciones prácticas sobre qué remediar en función de los puntajes de riesgo de exposición que utilizan nuestro enfoque único de modelado de ruta de ataque como su componente clave.

Experiencia de usuario de seguridad unificada

Parte de WithSecure™ Elements Cloud que ofrece una experiencia de usuario unificada desde un único panel de vidrio, complementada con servicios de co-seguridad como WithSecure™ Elevate.

Beneficios

Descubra su superficie de ataque

Conozca la superficie de ataque de su empresa obteniendo una visión general de su entorno, incluyendo activos, superficie de ataque externa e identidades, desde una única interfaz de usuario. Integre datos en sus dispositivos administrados (estaciones de trabajo, servidores), servicios en la nube (AWS, Azure), identidad (Entra ID), red (equipos de red, dispositivos no administrados) y superficie de ataque externa (descubrimiento y detección de Internet). Visualice su entorno desde una única pantalla.

Comprenda sus rutas de ataque

Las rutas de ataque exponen diversos activos internos a ciberataques. Normalmente, un atacante intentaría usar estas rutas para acceder a activos críticos de la empresa, por ejemplo, en un ataque de ransomware. Elements XM integra datos de su entorno organizacional interno y externo que conforman su superficie de ataque. Posteriormente, enriquece estos datos con inteligencia sobre su contexto empresarial y la información de amenazas más reciente para modelar posibles rutas de ataque en su organización. Dado que la información de inteligencia de amenazas más reciente forma parte integral de la gestión de la exposición, puede tener la tranquilidad de saber que está protegido contra los ataques más recientes. El uso de la información del contexto empresarial permite adaptar nuestro modelado de rutas de ataque y nuestras recomendaciones a las necesidades específicas de su negocio.

*Requires a license for WithSecure Elements Endpoint Protection (part of WithSecure Elements Endpoint Security) that includes the Software Updater functionality.

Elements Exposure Management detecta rutas de ataque perjudiciales que afectan a activos cruciales antes de que los atacantes puedan explotarlas. Al identificar los puntos críticos que pueden detener los ataques, Elements XM le permite mejorar significativamente la protección de los activos y datos de su empresa, minimizando al mismo tiempo el esfuerzo de remediación necesario. En otras palabras, Elements Exposure Management se centra en desmantelar la mayoría de las rutas de ataque peligrosas en su organización.

Remediar de manera priorizada

Asegúrese de que sus activos más críticos no sean explotados y manténgalos seguros mediante la gestión continua de exposiciones con IA. Elements Exposure Management proporciona a su personal las herramientas y los medios adecuados para remediar con éxito. Empiece a trabajar en la protección de su superficie de ataque con recomendaciones basadas en IA para priorizar las exposiciones más dañinas o, si tiene poco tiempo, implemente soluciones rápidas para las exposiciones de mayor impacto con el mínimo esfuerzo. También puede usar el Actualizador de Software de WithSecure para aplicar los parches de software que faltan al instante, con solo pulsar un botón y sin tener que cambiar de solución*.

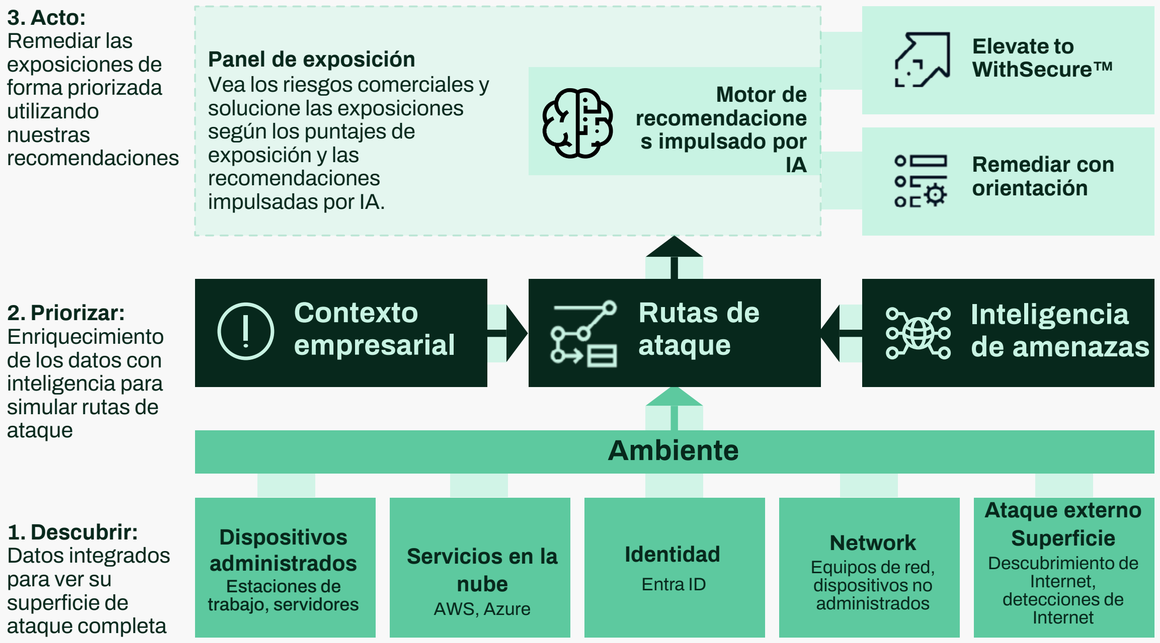
Nuestro motor de recomendaciones funciona como un equipo rojo, un grupo de personas que se hacen pasar por el ciberatacante, buscando posibles rutas de ataque hacia su organización. Mientras que el equipo rojo tradicional es un ejercicio ocasional, Elements Exposure Management permite un "equipo rojo virtual" controlado por IA de forma continua. Elements XM le ayuda a identificar los puntos débiles críticos en su superficie de ataque, como activos o identidades, que pueden funcionar como puntos de aceleración en una ruta de ataque y, a la inversa, desde la perspectiva del defensor, como cuellos de botella para romper las rutas de ataque de forma eficaz. Su administrador de seguridad puede remediar fácilmente los cuellos de botella de las rutas de ataque mediante recomendaciones basadas en IA, minimizando así el riesgo de ciberataques que comprometan los activos críticos de la empresa.

GenAI Luminen™

Utilice nuestro útil asistente de inteligencia artificial de la plataforma Elements Cloud, Luminen, para obtener más valor al usar la solución Elements XM (el asistente estará disponible próximamente también para WithSecure™ Elements Exposure Management).

Cómo funciona

Obtenga una visión integral de los riesgos cibernéticos. Analice toda su superficie de ataque y corrija las vulnerabilidades de mayor impacto, las configuraciones incorrectas y otras exposiciones que representan el mayor riesgo de intrusión para su organización. Proteja las rutas de ataque a sus activos críticos para el negocio.



1. Elements Exposure Management integra datos de sus entornos internos y externos para formar una descripción general holística de su superficie de ataque:
   - Superficie de ataque externa (que abarca el descubrimiento y la detección en Internet)
   - Servicios en la nube (Azure, AWS)
   - Identidades (Entra ID)
   - Dispositivos administrados(estaciones de trabajo y servidores)
   - Network (equipos de red como firewalls y conmutadores, dispositivos no administrados)

2. Elements XM utiliza vulnerabilidades, configuraciones incorrectas y otras exposiciones en su entorno para identificar posibles rutas de ataque. Combina el conocimiento sobre la superficie de ataque externa con información sobre la postura de seguridad interna, como vulnerabilidades de activos y configuraciones incorrectas en la nube. Esto proporciona comprensión sobre exposiciones peligrosas y rutas de ataque que afectan a activos críticos para el negocio. Elements XM enriquece los datos integrados con inteligencia de amenazas actualizada e información del contexto empresarial, simulando rutas de ataque basándose en esta inteligencia. La solución visualiza sus rutas de ataque y las utiliza para ofrecer recomendaciones basadas en IA que le ayudan a priorizar las medidas a tomar.

3. La visión general que ofrece el Panel de Exposición le ayuda a priorizar las acciones de remediación y le ofrece una visión general basada en el riesgo de las debilidades identificadas en su superficie de ataque. El motor de recomendaciones basado en IA le recomienda acciones de remediación basándose en grupos de hallazgos con un alto impacto en su exposición general. Nuestras recomendaciones incluyen una guía práctica sobre cómo tomar medidas de remediación. También ofrecemos la opción rápida de usar el Actualizador de Software de WithSecure para aplicar los parches de software faltantes al instante, con solo pulsar un botón*. Ver las puntuaciones de exposición de su empresa, sus diferentes tipos de activos y activos individuales le ayuda a priorizar la remediación.
   - El servicio adicional WithSecure™ Elevate permite enviarnos una recomendación específica para un análisis más detallado. Esta consulta con nuestros expertos garantiza la validez y prioridad del elemento elevado.

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

Gestione continuamente sus exposiciones digitales con nuestra tecnología

Panel de exposición

Olvídese de la fatiga por alertas. Mantenga la remediación de la exposición simple y efectiva con nuestro panel de Gestión de Exposición Elements, que le muestra dónde enfocar sus esfuerzos de remediación desde una vista única. Comprenda el riesgo de su negocio y recomiende acciones para mejorar la seguridad. Vea la solidez de su superficie de ataque mediante la vista de resumen de exposición, que le ofrece una visión general basada en el riesgo de las debilidades identificadas. Vea los activos críticos para el negocio en riesgo utilizando las Puntuaciones de Exposición para comenzar a priorizar la remediación de los activos que causan el mayor riesgo de explotación. Conozca los próximos pasos para mejorar la exposición obteniendo recomendaciones sobre qué corregir primero para una acción rápida y sencilla, gracias a nuestro motor de recomendaciones basado en IA.

Rutas de ataque

Elements XM simula las rutas de ataque que un atacante podría tomar para comprometer el patrimonio de un cliente. En lugar de crear rutas de ataque optimizadas para la ruta más corta desde la superficie de ataque externa hasta los activos críticos para el negocio, nuestro motor de razonamiento y nuestras rutas de ataque se basan en la puntuación heurística desde la perspectiva del atacante. Esto significa que nuestro motor de IA analiza el entorno del cliente desde la perspectiva del atacante, buscando debilidades mediante la ruta de un activo a otro que cause el máximo daño. Nuestra lógica de toma de decisiones se basa en décadas de experiencia en el desmontaje de ataques reales y en nuestra telemetría de detección de Detección y Respuesta Extendidas (XDR).

Esto es lo que significa un verdadero equipo rojo con IA. Nuestro motor de recomendaciones funciona como un equipo rojo (un grupo de personas que se hacen pasar por el ciberatacante) y busca posibles rutas de ataque hacia su organización. Si bien el equipo rojo tradicional es una práctica que, en ocasiones, puede ser una inversión útil para algunas empresas, nuestra Gestión de Exposición de Elementos permite el equipo rojo virtual con IA de forma continua.

Visualización de la ruta de ataque

Elements XM visualiza las rutas de ataque relacionadas con una recomendación, lo que permite profundizar en el razonamiento subyacente. La visualización de rutas de ataque proporciona información ampliada sobre los activos, los pasos y las identidades involucradas en la ruta de ataque, incluyendo las técnicas utilizadas, el acceso obtenido y los recursos relacionados. A continuación, se presentan los principales casos de uso de la visualización de rutas de ataque:

- **Validación**: Las rutas de ataque validan las recomendaciones proporcionadas por nuestro motor de recomendaciones impulsado por IA, lo que le permite tener prioridades de respuesta informadas para una toma de decisiones transparente.
- **Colaboración de las partes interesadas**: Facilita la comunicación de información sobre la ruta de ataque a las partes interesadas, incluidos clientes, tomadores de decisiones comerciales y administradores de TI, gracias a elementos visuales fáciles de entender.
- **Evaluación de riesgos**: Proporciona perspectivas de riesgo alternativas, mejorando sus actividades de evaluación de riesgos.

Motor de recomendaciones impulsado por IA

WithSecure lleva casi una década utilizando múltiples modelos de aprendizaje automático para respaldar las capacidades de detección y respuesta, y nuestro proyecto de investigación multianual sobre IA, "Blackfin", fue reconocido con el premio a la Excelencia en IA por sus técnicas de inteligencia colectiva. Gracias a nuestro motor de recomendaciones basado en IA, que encuentra rutas de ataque entre activos, Elements XM ayuda a reducir su nivel de riesgo de exposición al ofrecer recomendaciones sobre qué exposiciones abordar primero. Nuestras recomendaciones se basan en puntuaciones de exposición que utilizan elementos como nuestra fuente de datos de inteligencia de amenazas, la información de su contexto empresarial individual y nuestro innovador enfoque de modelado de rutas de ataque basado en IA.

Gestión de la Superficie de Ataque Externa (EASM)

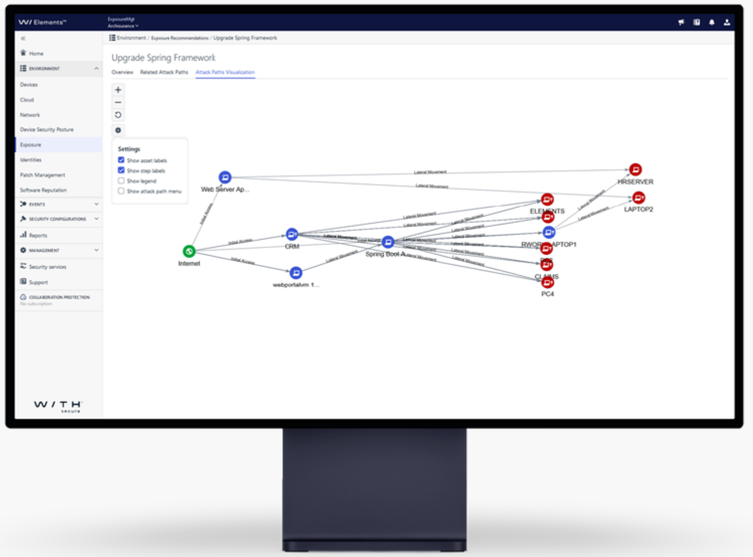
Proteja sus dominios, IP y activos públicos. La Gestión de Exposición utiliza la detección de Internet mediante rastreo y mapeo de puertos para recopilar datos en sistemas públicos. Puede usar los datos según la ubicación, dominio de nivel superior, dominio de pago, palabras clave, nombre de host y dirección IP. Las detecciones de Internet le ayudan a detectar el riesgo de robo de dominios y la divulgación de información de directorios. Además, añadimos continuamente nuevas detecciones de Internet según el panorama actual de amenazas.

Exposición al riesgo de identidad

Utilice datos sobre identidades digitales, ya sean humanas o no, y aborde los riesgos relacionados con la identidad integrando sus datos de Entra ID en Elements XM. Esto proporciona contexto de identidad para cada exposición e incluye datos relacionados con la identidad como insumo para identificar rutas de ataque peligrosas. Cubra los vectores de ataque de identidad que permiten la posible escalada de los derechos de acceso a la identidad. Nuestra funcionalidad de exposición para riesgos de identidad proporciona una evaluación continua de los riesgos relacionados con la identidad en su entorno y ayuda a prevenir el uso de la identidad como parte de rutas de ataque. Cumpla con su parte en la prevención de brechas en la cadena de suministro y mejore las prácticas de seguridad de los empleados y la higiene de la seguridad.

WithSecure™ Elevate

El usuario de Elements puede solicitar que se envíe una recomendación específica a WithSecure para analizar y obtener asesoramiento sobre la validez y prioridad del elemento elevado. Reciba apoyo de nuestros expertos en seguridad para tomar las siguientes medidas y comprender la importancia de ciertos hallazgos. Nuestro equipo de cazadores de amenazas y consultores de seguridad atenderá la solicitud de Elevate, investigará el hallazgo, la recomendación o la ruta de ataque y le informará al cliente según corresponda.



Escanee su entorno

WithSecure™ Elements Exposure Management combina múltiples métodos de escaneo disponibles para garantizar que toda su superficie de ataque esté cubierta:

Dispositivos y redes administrados		Superficie de ataque externa, identidad y servicios en la nube		
Nodo de escaneo local/en la nube	**Elements Agent**	**External Attack Surface**	**Integraciones de identidad**	**Cloud Integrations**
Escaneo de descubrimiento Identifique y mapee todos los activos dentro de su red	**Escaneo basado en agente** Escanee estaciones de trabajo y servidores de Windows automáticamente	**Descubrimiento de Internet** Identifique los sistemas de su organización que dan a Internet	**Entra ID** Descubra las amenazas potenciales asociadas con todas las identidades en Entra ID	**Azure** Evalúe la postura de seguridad y cumplimiento de sus cuentas
Análisis del sistema Escanee todos los sistemas IP (Protocolo de Internet) en busca de vulnerabilidades y configuraciones incorrectas	**Datos de servicio del dispositivo** Configuración del sistema e información de inicio de sesión	**Activos externos** Evalúe la postura de seguridad de sus activos expuestos externamente	**Violación de cuenta** Información de cuenta violada	**AWS** Evalúe la postura de seguridad y cumplimiento de sus cuentas
Escaneo autenticado* Inicie sesión en los sistemas para obtener datos de vulnerabilidad más detallados, como versiones de sistemas vulnerables, parches faltantes y configuraciones incorrectas.	**Gestión de parches** Estado del sistema y de parches de terceros y actualizaciones automáticas a través del Actualizador de software**			
Escaneo web Escanee y pruebe aplicaciones web personalizadas para detectar vulnerabilidades				

* Not available through a cloud scan node.

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

Note: Scans for Cloud Integrations are part of the WithSecure Elements Exposure Management for Cloud license, whereas the other scan types come as part of the WithSecure Elements Exposure Management for Users license.

Medidas de ciberseguridad unificadas para una protección amplia

Hemos estado guiando a nuestros clientes a través de las turbulentas aguas de la ciberseguridad durante más de 30 años y nuestra solución modular de ciberseguridad, WithSecure™ Elements, reúne XDR, gestión de exposición y servicios de co-seguridad en un solo panel.

Una buena ciberseguridad no puede vivir aislada. En primer lugar, al utilizar un conjunto fragmentado de herramientas de ciberseguridad, es necesario cambiar constantemente de un portal a otro. La fatiga por alertas es real, y gestionar múltiples flujos de trabajo separados es complejo, lo que dificulta la priorización. En segundo lugar, la gestión no es la única ineficiencia. Las soluciones en una configuración como esta no cooperan y pueden ser completamente independientes entre sí. Esto se traduce en silos, detecciones fallidas, respuestas lentas y, en última instancia, una estrategia de seguridad más débil. Para superar los desafíos de un mundo aislado, WithSecure™ Elements unifica las principales capacidades de ciberseguridad en una plataforma inteligente.

Más elementos significan mejores resultados, pero puede crear su propia suite de ciberseguridad en la nube con módulos tecnológicos de fácil acceso. Puede incorporar fácilmente nuevas capacidades y aumentar o disminuir su uso según el tiempo y sus necesidades.

Al potenciar su conjunto de ciberseguridad con una combinación unificada de Gestión de la Exposición, Detección y Respuesta Extendidas y Servicios de Co-Security, puede defenderse de un espectro completo de ciberamenazas. Las tecnologías unificadas funcionan como una sola, desde el backend hasta el frontend, y son fáciles y eficientes de gestionar desde un único portal: el Centro de Seguridad de Elementos WithSecure™.

Elements Exposure Management ofrece un diseño coherente con el resto de las soluciones Elements, lo que facilita su uso a los usuarios existentes y facilita su uso a nuevos usuarios con múltiples productos Elements. Nuestro modelo de precios transparente y los modelos de licencias uniformes en todas las soluciones Elements facilitan la gestión del software. Tanto los equipos de seguridad como los socios pueden revisar todos los productos Elements de una sola vez, como parte de su trabajo diario. En lugar de soluciones puntuales aisladas, WithSecure™ Elements le ofrece los medios para proteger su infraestructura de TI de forma unificada y eficiente. Las tecnologías inteligentes se basan en IA avanzada y automatización, lo que facilita la carga para usted y su equipo. También puede delegar la gestión diaria de la seguridad a nuestros socios certificados y liberar tiempo para centrarse en actividades más estratégicas.

Elements XM para servicios en la nube identifica riesgos de configuración incorrecta de forma proactiva.

Elements XM for Cloud evalúa la configuración de los recursos implementados en AWS y Azure para identificar vulnerabilidades que un atacante podría aprovechar. Esto incluye decenas de tipos de recursos de AWS y Azure y alrededor de doscientas comprobaciones de configuración. El conjunto de reglas que utilizamos se basa en investigaciones de vanguardia y las técnicas de ataque más recientes desarrolladas por los expertos en seguridad en la nube de WithSecure, así como en las mejores prácticas de AWS y Azure.

WithSecure™ Elements – consolida tu ciberseguridad

Unifique sus tecnologías de seguridad
Los componentes de seguridad funcionan juntos sin problemas y sin vulnerabilidades mediante un conjunto de datos compartido, y se administran a través de un único portal, el WithSecureTM Elements Security Center.

Ser consciente de la situación
Visibilidad en tiempo real de su entorno, incluida una imagen completa de lo que sucede allí, cuáles son sus riesgos y cómo priorizarlos

Construye tu suite
Personalice su paleta de seguridad con módulos de selección

Adaptarse a los cambios
Sin condiciones, con licencias sencillas

Requisitos técnicos

Sistemas compatibles
Dado que nuestro portal de gestión, WithSecure Elements Security Center, está basado en la nube, solo necesita un navegador web moderno y acceso a internet para acceder. Somos compatibles con las últimas versiones de los siguientes navegadores: Microsoft Edge, Mozilla Firefox, Google Chrome y Safari.
Sin embargo, según los entornos que desee integrar como parte de WithSecure Elements Exposure Management, deberá integrar sus dispositivos (Windows, Linux; consulte los requisitos del sistema operativo a la derecha), cuentas en la nube (AWS, Azure), activos de red e identidades (Entra ID). Para más información sobre la integración de activos, consulte la guía del usuario de Exposure Management.

Proteja los entornos que conforman su superficie de ataque
Nuestro enfoque multientorno cubre los siguientes activos y entornos:
- Superficie de ataque externa
- Servicios en la nube (plataformas Azure y AWS)
- Identidades (Entra ID)
- Dispositivos administrados, incluyendo estaciones de trabajo y servidores
- Red, incluyendo equipos de red

Idiomas admitidos
Inglés, finlandés, francés, alemán, italiano, japonés, polaco, portugués (Brasil), español (Latinoamérica), sueco y chino tradicional (Taiwán).

Instalación en dispositivos
La instalación de Elements Agent requiere uno de los siguientes sistemas operativos Windows:
- Para dispositivos: Microsoft Windows 10 u 11
- Para servidores: Microsoft Windows Server 2016 o posterior (instalación completa, no Server Core)

Para instalar nodos de escaneo, se aplican los siguientes requisitos del sistema operativo:
- Windows Server 2012 R2 o posterior
- Linux (Ubuntu Server y Debian (ambas versiones de 64 bits únicamente); SSH)

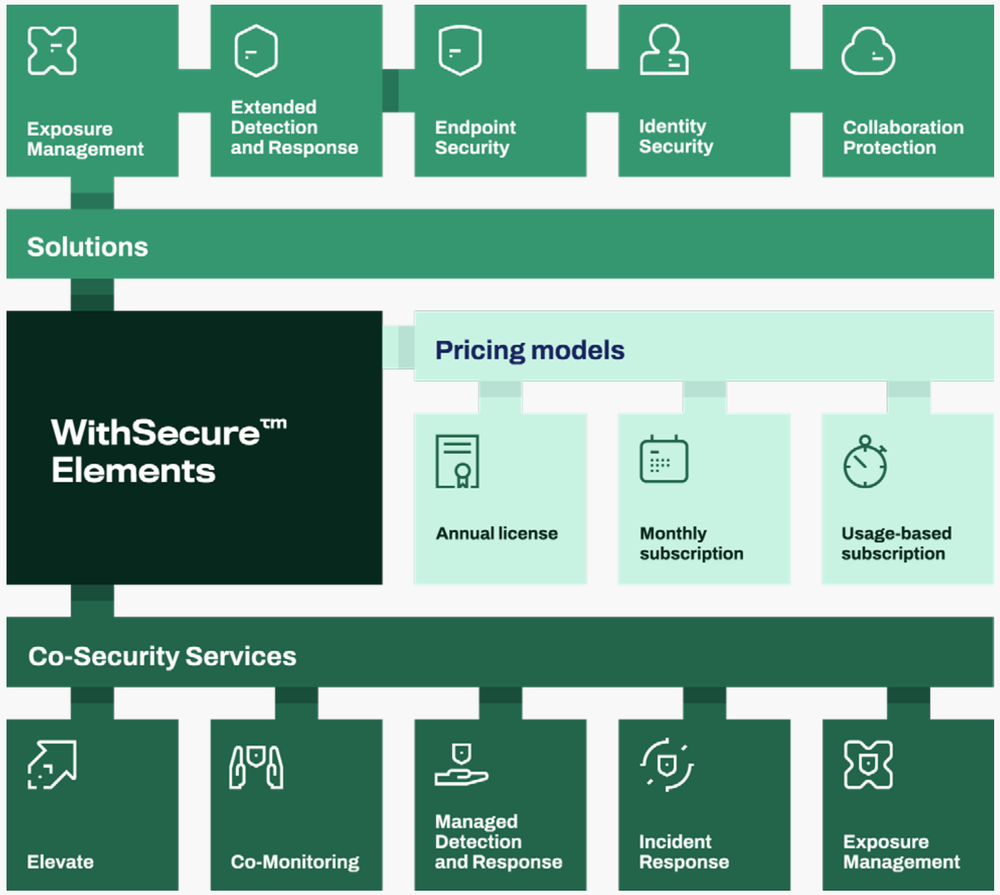
Modelo de precios simple con dos partes
Precios por usuario: Con Secure Elements Exposure Management para usuarios (identidad, red, dispositivos administrados y EASM)

Impuesto sobre la factura de la nube: WithSecure Elements Exposure Management para la nube (Servicios en la nube)

WithSecure™ Elements – Reducir el riesgo cibernético, la complejidad y la ineficiencia

WithSecure™ Elements Exposure Management está disponible como una función integral en la plataforma modular de ciberseguridad WithSecure™ Elements.
WithSecure™ Elements ofrece a los clientes protección completa en una plataforma unificada y un centro de seguridad fácil de usar. La plataforma centralizada combina potentes capacidades de seguridad predictivas, preventivas y reactivas con una protección inteligente contra amenazas que van desde ransomware hasta ataques dirigidos. Nuestra simplicidad inigualable permite a los clientes centrarse en lo que más valoran.
Los paquetes de productos modulares y los modelos de precios flexibles ofrecen a los clientes la libertad de evolucionar. WithSecure™ Elements puede formar parte del ecosistema del cliente. Se conecta fácilmente con sus sistemas SIEM, SOAR, de gestión de seguridad, monitorización o generación de informes.

Pruebe Elements hoy



Controla el riesgo de tu negocio. Sé más astuto que los atacantes.

¿Está listo para maximizar su resiliencia cibernética con el mínimo esfuerzo utilizando WithSecureTM Elements Exposure Management?

Contactar con ventas

Quiénes somos

WithSecureTM, anteriormente F-Secure Business, es el socio de confianza en ciberseguridad. Proveedores de servicios de TI, proveedores de servicios de gestión de servicios (MSSP) y empresas, junto con las mayores instituciones financieras, fabricantes y miles de los proveedores de comunicaciones y tecnología más avanzados del mundo, confían en nosotros para una ciberseguridad basada en resultados que protege y facilita sus operaciones. Nuestra protección basada en IA protege los endpoints y la colaboración en la nube, y nuestra detección y respuesta inteligentes están impulsadas por expertos que identifican los riesgos empresariales mediante la búsqueda proactiva de amenazas y la respuesta a ataques reales. Nuestros consultores colaboran con empresas y empresas tecnológicas para desarrollar resiliencia mediante asesoramiento en seguridad basado en la evidencia. Con más de 30 años de experiencia en el desarrollo de tecnología que cumple los objetivos empresariales, hemos desarrollado nuestra cartera para crecer junto con nuestros socios mediante modelos comerciales flexibles.

WithSecureTM Corporation fue fundada en 1988 y cotiza en NASDAQ OMX Helsinki Ltd.

WITH secure