WithSecure™ Elements Identity Security

Obtenga visibilidad sobre los ataques basados en la identidad

May 2025

Introducción

WithSecure™ Elements Identity Security es una solución de Detección y Respuesta a Amenazas de Identidad (ITDR). Protege a las organizaciones contra ataques basados en la identidad al detectar identidades de Microsoft Entra ID potencialmente comprometidas y permite a los analistas responder r pidamente a las amenazas para minimizar el impacto en su negocio. Como parte de la familia de productos Elements XDR, Identity Security previene el robo de credenciales y los ataques contra la infraestructura de gestión de identidades y acceso.

Los objetivos de los atacantes no han cambiado; siguen intentando causar interrupciones y robar información. Sin embargo, los ataques se centran cada vez menos en desplegar cargas útiles en los endpoints y más en abusar de las identidades (de usuario y de entidad) y sus privilegios. El equipo de respuesta a incidentes de WithSecure observa una tendencia creciente en los ataques centrados en la identidad. Un informe reciente* reveló que las credenciales robadas se han convertido en el punto de entrada más común para las brechas de seguridad, y las brechas iniciadas con credenciales robadas o comprometidas fueron las que tardaron más en identificarse y contenerse.

Entre 2023 y 2024, se observ un aumento del 71 % en los ataues basados en credenciales de usuario robadas o comprometidas. as filtraciones de datos iniciadas con credenciales robadas o comprometidas fueron las ue tardaron ms en resolverse entre los diversos vectores de ataue casi 10 meses.***

A medida que los entornos de TI modernos se expanden más allá de las instalaciones locales, se necesita más que una higiene de seguridad básica para mantenerse protegido. Si bien siguen siendo útiles para proteger los endpoints, las herramientas tradicionales de Detección y Respuesta de Endpoints (EDR) no pueden proporcionar visibilidad de las identidades y los servicios en la nube accesibles desde cualquier lugar. El uso de identidades Entra ID basadas en la nube por parte de trabajadores remotos y la autenticación con herramientas de terceros aumentan la superficie de ataque, y a menudo no hay ningún dispositivo endpoint que atacar o defender como parte de estos procesos.

Las identidades se han convertido en un nuevo y lucrativo vector de ataque, especialmente en el caso de Microsoft Entra ID, el servicio de gestin de identidades y acceso (IAM) basado en la nube ms utilizado. Entra ID desempea un papel fundamental en Microsoft 365, ya que tambin incluye autenticacin multifactor y acceso condicional. Lo utilizan la mayora de las organizaciones que utilizan servicios de Microsoft 365 basados en la nube.

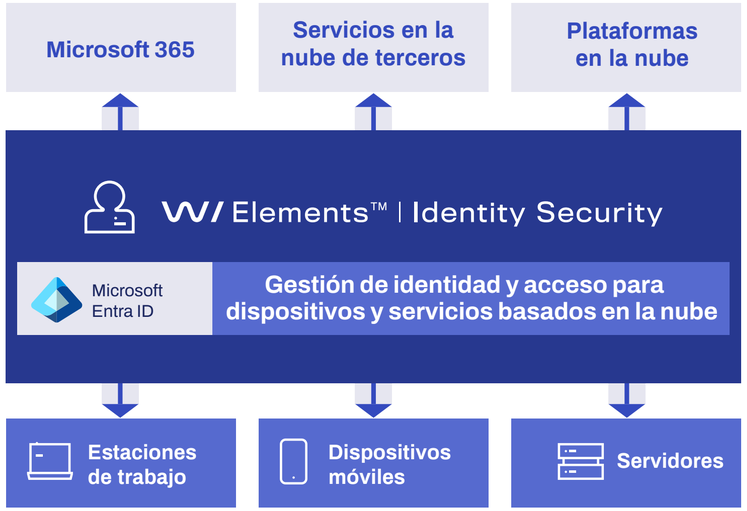
* IBM Cost of a Data Breach Report 2024
** IBM X-Force Threat Intelligence Index 2024

Con Elements Identity Security de WithSecure™, detecta y responde a ataques basados en la identidad, destacando las credenciales de usuario potencialmente comprometidas, para que los analistas puedan tomar medidas para proteger su organizacin. Los atacantes suelen recopilar credenciales mediante campaas de phishing por correo electrnico o incitando a los administradores a aceptar flujos de autenticacin no estndar en su organizacin. Elements Identity Security ampla sus capacidades de deteccin a ataques basados en la identidad ms all de los endpoints para proteger sus credenciales de usuario.

Una vez que Elements Identity Security detecta un ataque, facilita sus siguientes pasos para responder. Toda la actividad detectada de un usuario potencialmente comprometido se integra en un sistema de Detección de Contexto Amplio™ (BCD), lo que facilita la investigación en un lugar central dentro de la plataforma WithSecure Elements Cloud. Con Elements Identity Security, puede responder a las amenazas de identidad de forma rápida y sencilla para minimizar las interrupciones, por ejemplo, eliminando el acceso, restableciendo contraseñas o cerrando sesiones para detener a los atacantes.

La cobertura de detección de Entra ID abarca una variedad de los escenarios de ataque más recientes, incluyendo la vulneración del correo electrónico empresarial, donde un atacante obtiene acceso no autorizado al correo electrónico de la empresa, que puede utilizarse para robar datos u obtener fondos fraudulentamente. Además de una amplia gama de técnicas, se cubren las fases de ataque MITRE: acceso inicial, persistencia, escalada de privilegios, evasión de defensa y acceso a credenciales.

El servicio también combina las alertas nativas de Microsoft Entra ID Protection* con la actividad capturada por Elements Identity Security de WithSecure y agrega estos datos. Esto permite a los clientes tener una visión completa de las acciones recientes realizadas por cuentas sospechosas o comprometidas desde un único panel.



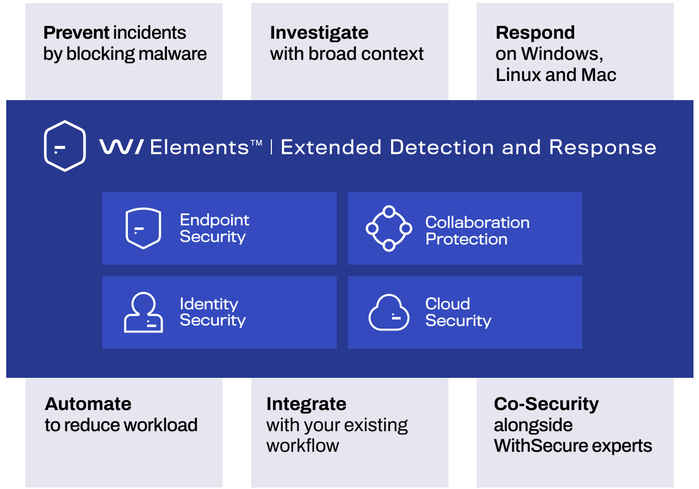
*Requires also a separate license for Microsoft Entra ID Protection that is a product that alerts for risky sign-ins (part of Microsoft bundle licenses like Entra ID P1 and above).

Part of WithSecure™ Elements XDR

WithSecure™ Elements Identity Security es un módulo de WithSecure™ Elements Extended Detection and Response (XDR) y está diseñado para entornos de TI modernos. Elements XDR no solo permite a las organizaciones comprender y responder a amenazas avanzadas en endpoints, identidades, correos electrónicos y herramientas de colaboración, sino que sus controles preventivos avanzados y automatizados controlan el volumen de incidentes y los ataques de bajo nivel.

Elements XDR le permite reconocer toda la cadena de ataque que representa una amenaza para su negocio, extendiéndose más allá de los endpoints a diferentes partes del ataque en plataformas de nube, identidades y correo electrónico. Reconocer los ataques a tiempo no solo le da ventaja para reaccionar, sino que también ahorra costos al reducir las repercusiones derivadas de las vulnerabilidades.

Elements XDR forma parte de nuestra plataforma Elements Cloud, que incluye una amplia gama de herramientas y capacidades disponibles desde la nube para ofrecer gestión de exposición, gestión automatizada de parches, inteligencia dinámica de amenazas y análisis continuo del comportamiento. Los usuarios de Elements Cloud pueden acceder fácilmente a la experiencia de WithSecure con nuestros flexibles Servicios de Co-Security, que ofrecen ayuda para trabajar con detecciones complejas o incidentes graves generalizados, por ejemplo..



¿Cuál es la diferencia entre EDR y XDR?

Las soluciones EDR se centran en detectar y responder a las amenazas para los endpoints, mientras que WithSecure Elements XDR es una solucin ms completa y unificada para proteger los activos de TI modernos. Minimiza el impacto de los ataques mediante controles preventivos avanzados y automatizados que controlan el volumen de incidentes y los ataques de bajo nivel. Las herramientas basadas en IA permiten una rpida deteccin, investigacin y respuesta a las amenazas en un contexto ms amplio en endpoints, identidades, correos electrnicos y otros servicios de colaboracin en la nube. WithSecure Elements Identity Security es una solucin ITDR que protege a las organizaciones contra ataques basados en la identidad, como parte de Elements XDR. WithSecure Elements Endpoint Detection and Response (EDR) tambin forma parte de nuestra oferta Elements XDR, como parte de nuestra solucin de seguridad para endpoints, que combina Elements EDR y Elements EPP (Endpoint Protection).

¿Cómo funciona el precio de Elements Identity Security?

El precio se basa en el número de cuentas de usuario de Entra ID, por lo que se deben agregar todos los usuarios de cada* inquilino. Puede obtener XDR con protección para identidades sin necesidad de invertir en las suscripciones más caras de Microsoft Entra ID, como P1 y P2, gracias a Elements Identity Security. Ofrecemos un precio combinado para Elements Identity Security junto con Elements Endpoint Security (EPP + EDR).

¿Por qué aún necesitas EPP y EDR (Elements Endpoint Security)?

Los atacantes buscan constantemente nuevas formas de evadir la deteccin. Es un juego perpetuo del gato y el ratn entre atacantes y defensores. La creciente explotacin de los ID de Entra indica una falta de cobertura efectiva contra ataques basados en la identidad. Es probable que esta tendencia contine hasta que se adopten ampliamente las herramientas ITDR, lo que dificulta tanto los ataques que los atacantes se ven obligados a buscar nuevos mtodos. El aumento de los ataques relacionados con la identidad no disminuye la importancia de protegerse contra las amenazas a los endpoints. El ransomware sigue siendo una amenaza significativa para muchas organizaciones. Para obtener informacin ms detallada, consulte nuestros ltimos Informes de Inteligencia de Amenazas

* The solution is compatible with multiple tenants.

¿Por qué WithSecure™ Elements Identity Security?

Proteja sus activos más vulnerables: sus usuarios. La identidad es la capa que une sus endpoints, los servicios en la nube y las plataformas que utiliza su organización. Las capacidades de protección, detección y respuesta de endpoints protegen sus dispositivos, pero necesita Elements Identity Security como la siguiente extensión para proteger su entorno de TI moderno.

Basado en ataques reales de nuestro equipo de Respuesta a Incidentes

Proteja la fuerza laboral remota de su organización utilizando lógica de detección creada a partir de ataques reales dirigidos a identidades.

Actúe rápidamente para minimizar el impacto

Utilice nuestras capacidades de respuesta de Entra ID para finalizar sesiones y deshabilitar el acceso de los usuarios.

Prevenir el uso de credenciales robadas

Detecte credenciales comprometidas y ataques basados en identidad obteniendo visibilidad ms all del punto final.

Investigar en un contexto amplio

Toda la actividad detectada de un usuario potencialmente comprometido se agrega para que la investigación de la actividad sospechosa se pueda realizar desde un lugar central.

Detectar correo electrónico empresarial comprometido

Detección probada de las técnicas que resultan más costosas para las organizaciones.

Servicios flexibles

Haga más con recursos limitados administrando fácilmente Elements XDR y accediendo a servicios flexibles siempre que sea necesario para ampliar su propio equipo.

Beneficios

Proteja a su fuerza laboral remota

Las soluciones tradicionales de EDR no protegen todos los activos a los que accede su personal remoto. Los servicios en la nube son cada vez más comunes en los entornos de TI modernos y suelen depender de Entra ID gracias al uso de funciones como el inicio de sesión único (SSO). Con Elements Identity Security, puede ampliar las capacidades de detección más allá de los endpoints para cubrir las identidades y responder rápidamente a las amenazas basadas en la identidad.

Investigar con Detección™ de contexto amplio

Las Detecciones de Contexto Amplio™ (BCD) reducen la fatiga de alertas al agregar automáticamente eventos relevantes, evaluar la gravedad general y permitir investigaciones desde una vista consolidada. La actividad sospechosa de los usuarios se puede investigar mediante una vista completa de las acciones recientes realizadas por las cuentas presuntamente comprometidas. Con las BCD, puede analizar los ataques en una línea de tiempo para encontrar patrones, visualizar eventos relevantes y actuar con rapidez, con nuestras recomendaciones. El análisis de comportamiento, reputación y big data en tiempo real se utiliza junto con el aprendizaje automático para contextualizar las detecciones, considerando los niveles de riesgo y la importancia de cada host afectado.

Nuestros diversos mecanismos de detección generan alertas de alta fidelidad. Utilizamos una combinación de señales en la puntuación de riesgo y en otras detecciones para identificar acciones que un atacante podría realizar tras obtener el acceso inicial. Estas señales incluyen acciones como la creación de registros de aplicaciones, la adición de credenciales a principios de servicio y la adición de principios de servicio con nombres similares a Microsoft para ocultar acciones. La combinación de estos tipos de señales reduce los falsos positivos, ya que podemos estar más seguros de que el BCD es malicioso si contiene múltiples detecciones sospechosas.

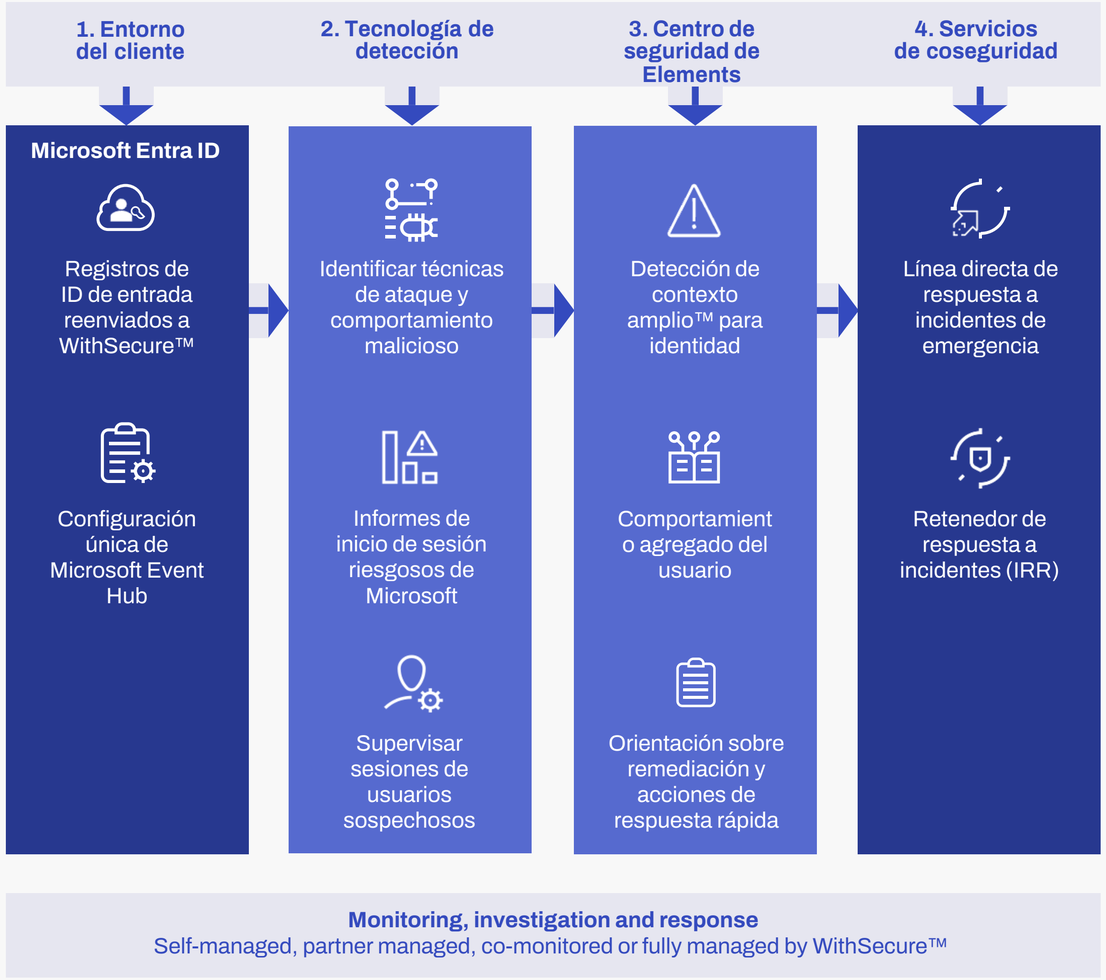
Detectar y responder a ataues basados en la identidad

Protjase del riesgo de ataques basados en la identidad al tener visibilidad de las credenciales de usuario comprometidas. Las credenciales suelen ser robadas mediante campaas de correo electrnico de phishing que recopilan credenciales de sitios web falsos para incitar a los administradores a aceptar flujos de autenticacin no estndar en su organizacin. Utilice alertas centradas en el usuario para investigar toda actividad sospechosa detectada de un usuario potencialmente comprometido. Al recibir alertas, puede responder rpidamente cuando se produce actividad sospechosa, lo que le permite minimizar el impacto de los ataques antes de que se roben datos crticos para la empresa. Cada Broad Context Detection™ incluye gua de remediacin y acciones de respuesta rpida, lo que facilita una accin rápida.

GenAI Luminen™

Utilice nuestro til asistente de IA de la plataforma Elements Cloud para comprender los ataques basados en identidad y los conceptos clave. Luminen™ GenAI analiza y proporciona explicaciones en lenguaje natural de las Detecciones de Contexto Amplio™ de WithSecure Elements XDR, enriquecidas con datos relevantes de inteligencia de amenazas externas. Facilita a los equipos de TI la asistencia inmediata a usuarios de cualquier nivel de experiencia para comprender mejor el contexto y el impacto de las detecciones, permitindoles centrarse en lo ms importante.

Cómo funciona



1. Existe una configuración única de Microsoft Event Hub para capturar los registros de Entra ID del entorno del cliente*. La integración se configura en tres pasos: primero, crear el inquilino en Elements Security Center; luego, implementar la infraestructura en el inquilino de Microsoft; y, finalmente, volver a agregar la cadena de conexión a Elements Security Center para que pueda comenzar la recopilación de datos.

2. Los registros de Microsoft Entra ID se envían a WithSecure a través de un centro de eventos de Microsoft alojado por el cliente. La tecnología de detección de WithSecure identifica técnicas de ataque y comportamiento malicioso mediante los informes de inicio de sesión de riesgo de Microsoft y la monitorización de sesiones de usuarios sospechosas.
   - Los registros recopilados son registros de inicio de sesión y auditoría, registros de inicio de sesión de usuarios no interactivos, registros de inicio de sesión de entidades de servicio, registros de inicio de sesión de identidad administrada, alertas de riesgo de Microsoft y eventos de usuarios y entidades de servicio**.

3. En el Centro de Seguridad de Elements, las detecciones relacionadas con la identidad se agrupan en posibles incidentes. Broad Context Detection™ for Identity se utilizará como método para comprender el comportamiento agregado de los usuarios. Cada Broad Context Detection™ incluye guías de remediación y acciones de respuesta rápida.

4. A menudo, el siguiente paso en una investigación es confirmar que la actividad es esperada y legítima. Por lo tanto, el socio suele contactar al usuario final para validar la actividad en el contexto de la organización. Sin embargo, la monitorización, la investigación y la respuesta pueden ser autogestionadas o gestionadas por el socio. De ser necesario, WithSecure también ofrece servicios adicionales de Co-Security para la respuesta a incidentes, como nuestro servicio garantizado de Retención de Respuesta a Incidentes (IRR). También ofrecemos una línea directa de soporte de emergencia para la respuesta a incidentes 24/7/365.

* There is also a one-time onboarding for the response capability, which grants consent from the customer tenant to a WithSecure Elements Azure Response Application. This connection will be used by the Elements Platform to issue response jobs in the customer tenant.

** More information about what data is collected and its purpose can be found in the Elements Privacy Policy.

Evite un gran impacto por robo de credenciales con nuestra tecnología

Amplia cobertura de detección

La cobertura de detección de ataques relacionados con la identidad para Microsoft Entra ID abarca diversas fases de MITRE ATT&CK. Estas incluyen acceso inicial, persistencia, escalada de privilegios, evasión de defensa y acceso a credenciales. La cobertura de detección abarca diversos escenarios de ataque recientes, como por ejemplo, la vulneración del correo electrónico empresarial, donde un atacante obtiene acceso no autorizado al correo electrónico de la empresa para robar datos u obtener fondos fraudulentamente. Elements Identity Security también puede detectar escenarios como cuentas sospechosas comprometidas, el uso de credenciales robadas, actividades sospechosas de identidad y acceso, o viajes atípicos.

Las cookies y tokens de sesión pueden ser robados por un sitio web malicioso AitM (Adversario en el Medio) para reutilizarlos en un ataque de toma de control de sesión. Las circunstancias en las que se reutilizan estas cookies y tokens, como la ubicación y el dispositivo, pueden ser propiedades rastreables de la actividad de la sesión. Esto puede utilizarse para detectar actividad sospechosa. Nuestra solución rastrea los metadatos del dispositivo y la ubicación de la actividad de la sesión, entre otros tipos de datos, lo que nos permite evaluar la probabilidad de una sesión maliciosa.

Factores de riesgo para determinar la protección del inicio de sesión

WithSecure utiliza numerosos factores para determinar los riesgos de un evento de inicio de sesión:

- **Geolocalización:** cubrimos una variedad de anomalías de viaje imposibles, desde inicios de sesión exitosos hasta fallidos.
- **Fuerza bruta:** Puede haber cientos de inicios de sesión fallidos en casos de viajes imposibles. Para reducir el ruido, estos se agrupan y se utilizan para determinar el riesgo final del inicio de sesión, en lugar de alertar al usuario sobre intentos individuales de fuerza bruta.
- **Anomalías del protocolo OAuth:** identificamos anomalías en los eventos de inicio de sesión de OAuth, que podrían ser nuevos recursos, aplicaciones o clientes.
- **Metadatos del dispositivo:** las diferencias en los dispositivos y sus metadatos pueden indicar una sesión comprometida y, por lo tanto, aumentarán el riesgo de inicio de sesión.
- **MFA (Autenticación multifactor):** utilizamos metadatos de MFA para evaluar qué tan sospechoso es un evento de inicio de sesión.
- **MFA (Autenticación multifactor):** utilizamos metadatos de MFA para evaluar qué tan sospechoso es un evento de inicio de sesión.

Extensive Visibility via Entra ID Integration

WithSecure Elements Identity Security integrates with Microsoft Entra ID (previously known as Azure AD) as the most widely used cloud-based Identity and Access Management (IAM) service. Entra ID is mandatory for cloud-based Microsoft 365 services, and it can be used for authentication across third-party cloud services. Elements Identity Security captures relevant identity-based Entra ID events, including sign-in and audit logs, and combines them with native alerts from Microsoft Entra ID Protection (if this Microsoft product is in use). With the combination of these two types of identity-based events, you have extensive visibility into identity-based attacks.

Viajes imposibles

La solución detecta viajes imposibles o atípicos. Esto funciona detectando casos en los que no es posible realizar viajes físicos de larga distancia en un periodo de tiempo determinado entre inicios de sesión.

Compromiso del correo electrónico empresarial

El Compromiso de Correo Electrónico Empresarial (BEC) es un tipo de ataque de identidad en el que los perpetradores se hacen pasar por un usuario interno robando sus credenciales. Esto les permite enviar un correo electrónico para engañar a otras personas de la misma organización y que envíen dinero o divulguen información confidencial. WithSecure ha desarrollado detecciones basadas en casos reales de respuesta a incidentes de Compromiso de Correo Electrónico Empresarial donde se utilizaron datos de clientes de Microsoft Outlook.

Minimizar el ruido

Debido a la naturaleza probabilística de los eventos de inicio de sesión, siempre existe un delicado equilibrio entre las alertas excesivas y las detecciones no detectadas. Durante el desarrollo del producto, hemos perfeccionado cuidadosamente nuestras detecciones e incorporado mecanismos de supresión de ruido como parte del motor. Estos mecanismos incluyen aspectos como:

- Supresión de alertas sobre principales repetidos en un período de tiempo corto (histogramas)
- Agregar actividades para determinar un puntaje de riesgo basado en la actividad del usuario, en lugar de eventos de inicio de sesión único
- LAnalizar el comportamiento en toda la organización para reducir anomalías con viajes imposibles (si bien el uso de VPN organizacional puede ser un problema aquí, mitigamos este problema utilizando estadísticas de metadatos de inicio de sesión comunes de la empresa).

Respuesta de identidad

La respuesta es fundamental para prevenir el impacto de ataques graves y, por lo tanto, un componente crucial de Elements Identity Security. Las acciones de respuesta rápida disponibles funcionan mediante una integración directa entre Elements Cloud y su instancia de Entra ID. Estas acciones incluyen:

1. Cerarar sesión
2. Restablecer contraseña
3. Bloquear acceso de usuario

¿Qué es un Event Hub?

Un centro de eventos es un mecanismo de recopilación y reenvío de registros que recopila registros y los reenvía a WithSecure.

¿Cuánto costará un Event Hub?

Hay un pequeño costo asociado con el uso de Event Hubs, generalmente 15 euros al mes; revise los Costos asociados de Microsoft para obtener más detalles.

¿Cuál es el enfoque de retención de datos en WithSecure?

Los datos relacionados con las Detecciones de Contexto Amplio (BCD) se almacenan durante la vida útil del servicio. Para más información, consulte nuestra política de privacidad.

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 Identity Security 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 gestión de la seguridad para usted y su equipo. También puede delegar la gestión diaria de la seguridad a nuestros socios certificados y dedicar tiempo a actividades más estratégicas.

WithSecure™ Elements – consolide su cyber security

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

Integrar fácilmente
Conecte fácilmente los datos de seguridad con sus sistemas de terceros SIEM, SOAR, gestión de seguridad, monitoreo o informes

Adaptarse a los cambios
Sin condiciones, con opciones de suscripción flexibles que van desde las basadas en el uso hasta las anuales.

Requisitos técnicos

Sistemas compatibles
Dado que Elements Identity Security está diseñado para proteger Microsoft Entra ID como parte de nuestra solución Elements XDR, necesita tener derechos administrativos en los inquilinos de Entra ID correspondientes para configurar su protección. Tras la configuración inicial, solo necesita un navegador web moderno y acceso a internet para administrar Elements Identity Security como parte de Elements XDR.

Idiomas admitidos
English, Finnish, French, German, Italian, Japanese, Polish, Portuguese (Brazil), Spanish (Latin America), Swedish and Traditional Chinese (Taiwan).

Instalación
Debe poder iniciar sesión como administrador global en la cuenta de Azure para ejecutar el script en Azure Cloud Shell y tener su identificador de inquilino, su identificador de suscripción y la ubicación de implementación listos y disponibles antes de iniciar la implementación. La suscripción debe estar asignada a un grupo de administración de Azure.

Requisitos de licencia de Elements
Elements Identity Security requiere una suscripción a WithSecure Elements Endpoint Security, que incluye capacidades de Endpoint Protection (EPP) y Endpoint Detection and Response (EDR).

Requisitos de licencia de Microsoft
No se requieren licencias de Microsoft para Identity Security. Si el cliente tiene una licencia P2 para Entra ID, ofrecemos una lógica de detección para utilizar los informes de riesgo de Microsoft Entra ID Protection y deshabilitar el acceso condicional (una función que requiere una licencia P2).

Permisos de Microsoft
Los siguientes roles privilegiados dentro del inquilino de Entra ID son necesarios para la capacidad de respuesta:

- Permiso de la API de gráficos: User.ReadWrite.All
- Rol con privilegios de Azure: Administrador de usuarios. Si bien WithSecure ha implementado medidas para reducir este riesgo, los permisos mencionados anteriormente tienen privilegios elevados que los atacantes podrían aprovechar. Los posibles impactos incluyen:

a) Creación de nuevas cuentas de usuario para mantener el acceso no autorizado al entorno.
b) Ataques de denegación de servicio (DoS) dirigidos a administradores y usuarios de Entra ID.
c) Acceso no autorizado a datos confidenciales, como nombres, direcciones de correo electrónico y cargos.

Limitaciones
Tenga en cuenta que el cliente tiene permitidos 200 millones de eventos en las fuentes de registro de Entra ID cada mes. Si la cantidad de eventos procesados supera este lmite, podra requerirse un ajuste de precio. Durante la implementacin, el cliente ejecutar un script que configura alertas de Azure para cuando Microsoft Event Hubs alcance su capacidad máxia. El cliente es responsable de garantizar que los Event Hubs no alcancen su capacidad mxima, ya que esto afectar la prestacin del servicio.
Dado que WithSecure ya no recibirá todos los eventos del inquilino del cliente, envíe un ticket al servicio de atención al cliente de WithSecure si recibe dichas alertas de Azure.

Costos asociados de Microsoft
La configuración de Microsoft Event Hub implementada utiliza Event Hubs de nivel estándar. El coste mensual se basa en la cantidad de unidades de rendimiento (TU). La cantidad de TU depende de la carga. Los Event Hubs de nivel estándar cuestan aproximadamente 25 € al mes por unidad de rendimiento (TU). Los costes asociados a Event Hubs se describen en la página web de precios de Microsoft Azure Event Hubs. El coste por evento recibido a través de Event Hub es actualmente de 0,026 € por millón de eventos. Según nuestros datos históricos, el volumen mensual de eventos oscila entre 6 y 300 millones de eventos. Para más información sobre este tema, consulte nuestra Guía del usuario de seguridad de identidad.

Elementos WithSecureTM: reduzca el riesgo cibernético, la complejidad y la ineficiencia

WithSecure™ Elements Identity Security está disponible como una capacidad integral en la plataforma de seguridad cibernética modular WithSecure™ Elements.

WithSecure™ Elements ofrece a los clientes protección completa en una plataforma unificada y un centro de seguridad fácil de usar. Esta 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 integrarse en el ecosistema del cliente. Se conecta fácilmente con sus sistemas SIEM, SOAR, de gestión de seguridad, monitorización o generación de informes.

Pruebe Elements hoy

Comuníquese con nuestro equipo de ventas para proteger a la fuerza laboral remota de su organización contra el aumento de ataques dirigidos a las identidades.

Contactar con ventas

Quiénes somos

WithSecure™, anteriormente F-Secure Business, es el socio de ciberseguridad de referencia en Europa. Proveedores de servicios de TI, proveedores de servicios de gestión de datos (MSSP) y empresas de todo el mundo confían en nosotros; ofrecemos soluciones de ciberseguridad basadas en resultados que protegen a las empresas medianas. Comprometidos con el Estilo Europeo de Protección de Datos, WithSecure prioriza la privacidad, la soberanía de los datos y el cumplimiento normativo.

Con más de 35 años de experiencia en el sector, WithSecure™ ha diseñado su portafolio para afrontar el cambio de paradigma de la ciberseguridad reactiva a la proactiva. En consonancia con su compromiso con el crecimiento colaborativo, WithSecure™ ofrece a sus socios modelos comerciales flexibles que garantizan el éxito mutuo en el dinámico panorama de la ciberseguridad.

Elements Cloud es un elemento central de la oferta de vanguardia de WithSecure, que integra a la perfección tecnologías basadas en IA, experiencia humana y servicios de coseguridad. Además, ofrece a los clientes del mercado medio capacidades modulares que abarcan la protección de endpoints y la nube, la detección y respuesta ante amenazas, y la gestión de la exposición.

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

WITH secure