Datasheet

Detener Ataques Dirigidos

WithSecure Elements Endpoint Detection and Response

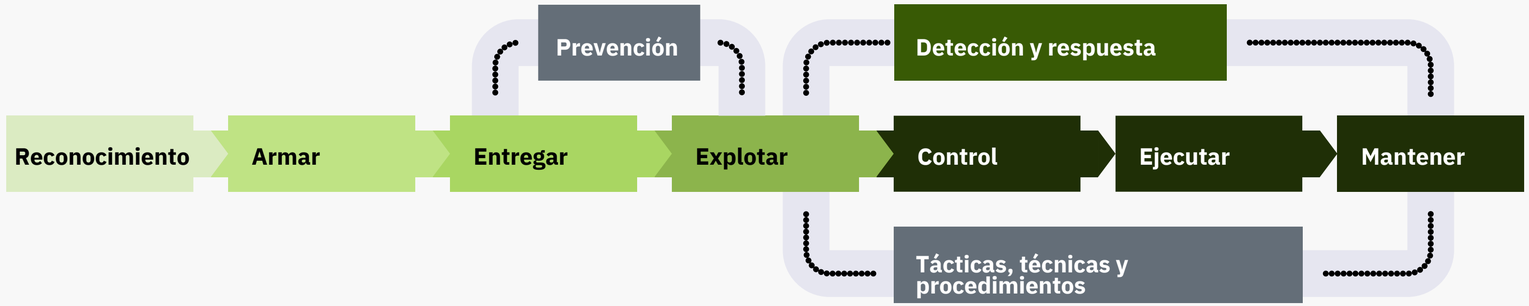
Proteja su negocio y sus datos contra ataques cibernéticos avanzados

La prevención efectiva de amenazas previas al compromiso es la piedra angular de la seguridad cibernética, pero no puede confiar solo en las medidas preventivas para mantener su negocio y sus datos a salvo de las tácticas, técnicas y procedimientos que utilizan los adversarios en los ataques dirigidos.

El panorama de amenazas en continua evolución, junto con las exigencias normativas como el RGPD, exigen que las empresas esten preparadas para la detección de brechas posteriores al compromiso. Eso significa garantizar que una empresa sea capaz de responder rápidamente a los ataques avanzados.

WithSecure™ Elements Endpoint Detection and Response, es mantenida por un equipo experimentado en detección de amenazas, y permite que su propio equipo de TI o un proveedor de servicios certificado proteja a su organización contra amenazas avanzadas.

Con el respaldo de los expertos en seguridad cibernética de clase mundial de WithSecure, sus propios especialistas de TI podrán responder a los incidentes de manera rápida y efectiva. O al permitir que un proveedor de servicios administre las operaciones de detección y respuesta de su organización, puede concentrarse en su negocio principal y confiar en la orientación de expertos siempre que esté bajo ataque.



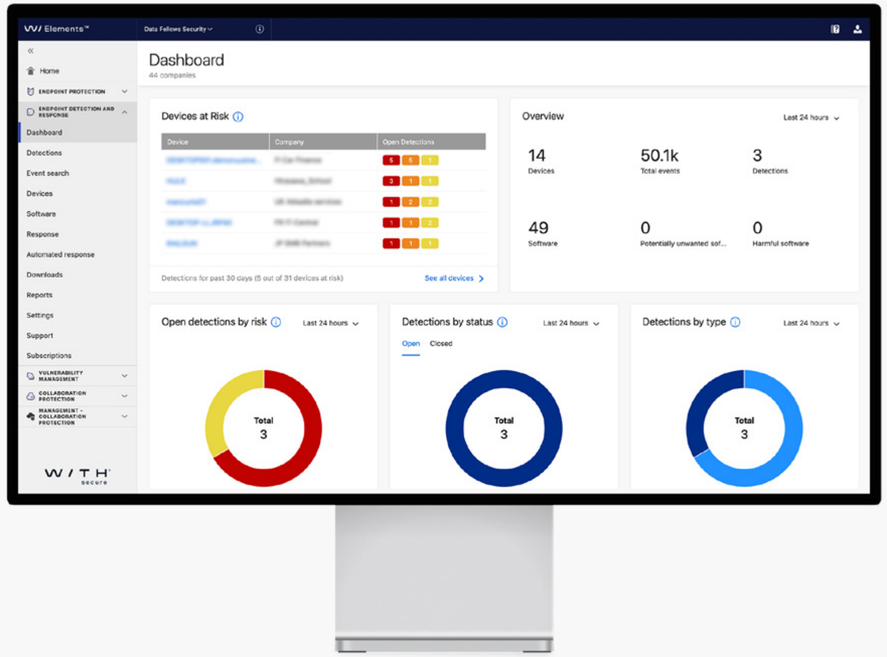
Descripción

Detenga los ataques dirigidos rápidamente con orientación y automatización

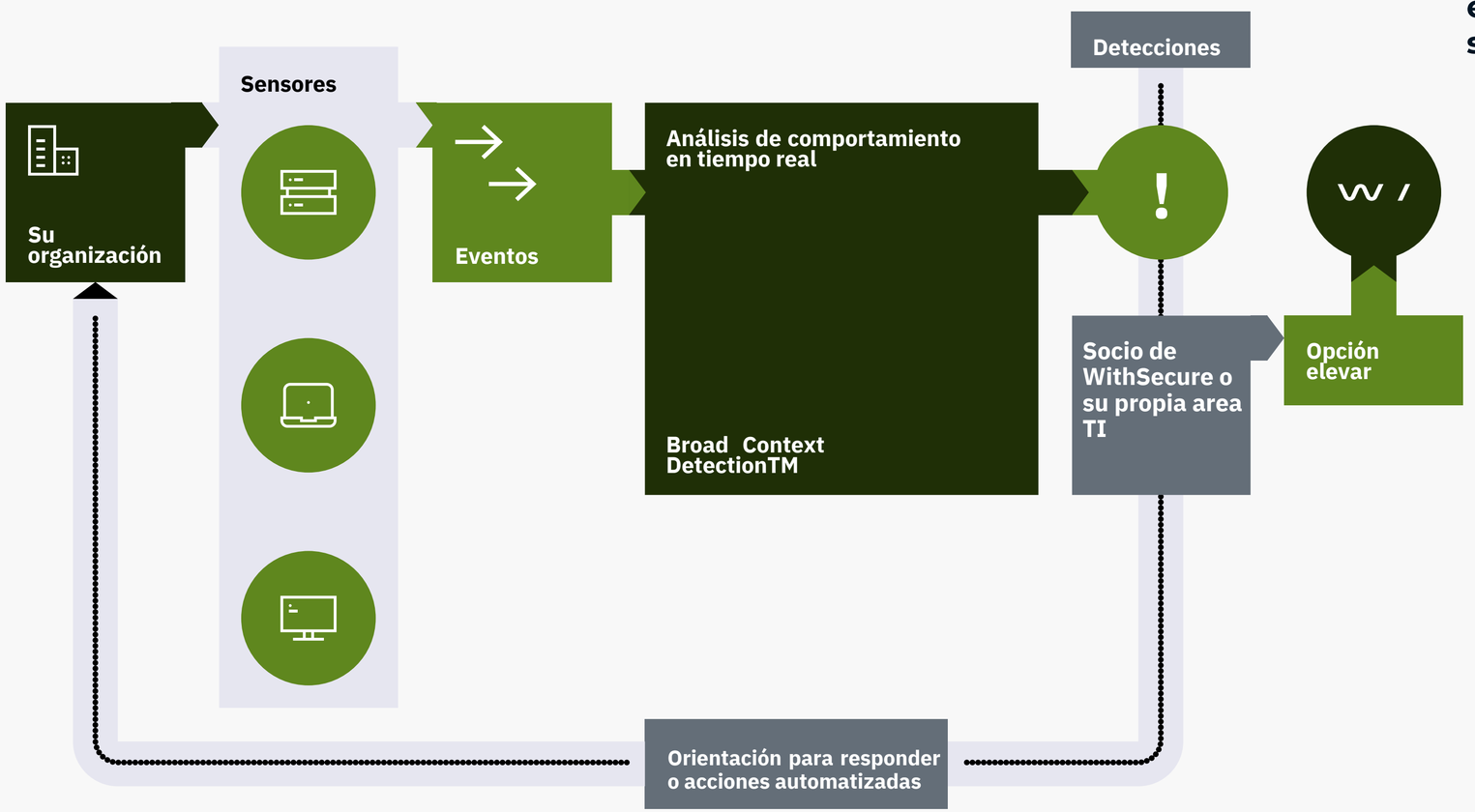
¿Cómo se detecta un ataque sofisticado? Usted hace uso de las tecnologías de análisis y aprendizaje automático más avanzadas para proteger a su organización contra amenazas e infracciones cibernéticas avanzadas

La solución líder en la industria de detección y respuesta para endpoint (EDR) de WithSecure le brinda visibilidad contextual de las amenazas avanzadas, lo que le permite detectar y responder a ataques dirigidos con automatización y orientación.

Cuando se produce una infracción, necesita algo más que una alerta. Para planificar la mejor respuesta posible, debe comprender los detalles del ataque. Nuestros mecanismos de detección de contexto amplio (**Broad Context Detection**™), junto con los proveedores de servicios certificados y la automatización integrada, detendrán rápidamente el ataque y brindarán consejos procesables para futuras acciones de remediación.



¿Como funciona?



La tecnología líder en la industria y los expertos en ciberseguridad de WithSecure a su servicio

- Los sensores ligeros implementados en los endpoints monitorean los eventos de comportamiento generados por los usuarios y los transmiten al análisis de datos de comportamiento en tiempo real y mecanismos de detección de contexto amplio, para distinguir los patrones de comportamiento malicioso, del comportamiento normal del usuario.

- Las alertas con puntuaciones de riesgo y el contexto amplio visualizado en todos los hosts afectados facilitan la confirmación de una detección, ya sea por parte del socio de WithSecure™ o de su propio equipo de TI, con la opción de elevar las investigaciones difíciles a WithSecure™ o de automatizar las acciones de respuesta.

- Después de una detección confirmada, la solución brinda consejos y acciones de respuesta recomendadas para guiarlo a través de los pasos necesarios para contener y remediar rápidamente el ataque.

¿Como funciona?

Buscando una aguja en un pajar - un ejemplo del mundo real

Detectar amenazas avanzadas detectando los pequeños eventos individuales que desencadenan los atacantes es como tratar de encontrar una aguja en un pajar.

En una instalación de cliente de 325 nodos, nuestros sensores recolectaron alrededor de 500 millones de eventos durante un período de un mes. El análisis de datos sin procesar en nuestros sistemas back-end filtró ese número a 225,000 eventos.

Los eventos sospechosos se analizaron más a fondo mediante nuestros mecanismos Broad Context Detection™ para reducir el número de detecciones a solo 24. Finalmente, esas 24 detecciones se revisaron en detalle y solo 7 se confirmaron como amenazas reales.

Permitir que los equipos de TI y seguridad se concentren en menos detecciones y más precisas da como resultado acciones de respuesta más rápidas y efectivas siempre que se encuentren bajo un ataque cibernético real.

500 millones
eventos de datos / mes recopilados por 325 sensores de endpoint

225 000
eventos de datos / mes después del análisis de comportamiento en tiempo real de los eventos

24
detecciones después de agregar un contexto más amplio a los eventos sospechosos

7
amenazas reales después de confirmar las detecciones como amenazas reales

Beneficios

Visibilidad

Obtenga visibilidad inmediata de su entorno de TI y estado de seguridad

- Mejora la visibilidad del entorno de TI y el estado de seguridad a través del inventario de aplicaciones y terminales.
- Identifica actividades sospechosas recopilando y correlacionando eventos de comportamiento más allá del malware comercial.
- Proporciona alertas con información de contexto amplia y criticidad de activos, lo que facilita la respuesta a incidentes

Detección

Proteja su empresa y sus datos confidenciales detectando infracciones rápidamente

- Detecte y detenga ataques dirigidos rápidamente para minimizar las interrupciones comerciales y el impacto negativo en la marca
- Tenga la solución configurada en cuestión de horas, lo que le permite estar listo para las infracciones de inmediato
- Cumplir con los requisitos reglamentarios de PCI, HIPAA y GDPR que exigen que se notifiquen las infracciones en un plazo de 72 horas

Respuesta

Responda rápidamente con orientación y automatización siempre que sea atacado

- La automatización y la inteligencia integradas ayudan a su equipo a concentrarse solo en ataques reales
- Las alertas incluyen una guía de respuesta adecuada, con una opción para automatizar las acciones de respuesta durante todo el día.
- Refuerce sus habilidades o recursos respondiendo a los ataques con un proveedor de servicios certificado respaldado por WithSecure™

Características

Sensores endpoint

Herramientas de monitoreo ligeras y discretas diseñadas para funcionar con otras soluciones de protección endpoint

- Los sensores se implementan en todas las computadoras relevantes dentro de su organización
- Un solo Agente e Infraestructura de administración con las soluciones de seguridad endpoint de WithSecure
- Los sensores recopilan datos de comportamiento de dispositivos Windows, Mac y Linux sin comprometer la privacidad de los usuarios.

Broad Context Detection™

La tecnología de detección patentada de WithSecure facilita la comprensión del alcance de un ataque dirigido.

- Análisis de comportamiento, reputación y big data en tiempo real con aprendizaje automático
- Coloca automáticamente las detecciones en un contexto visualizado en una línea de tiempo
- Incluye los niveles de riesgo, la criticidad del host afectado y el panorama de amenazas predominante.

Visibilidad de la aplicación

Obtener visibilidad de su entorno de TI y el estado de seguridad nunca ha sido tan fácil

- Identifica todas las aplicaciones dañinas o no deseadas y destinos foraneos de diferentes servicios en la nube
- Aprovecha los datos de reputación de WithSecure para identificar aplicaciones potencialmente dañinas
- Restringe las aplicaciones y los servicios en la nube potencialmente dañinos incluso antes de que se produzcan filtraciones de datos

Respuesta guiada

Lo prepara para enfrentar incluso los ataques cibernéticos más avanzados con sus recursos existentes

- Guía de respuesta paso a paso incorporada y acciones remotas para detener los ataques
- Los proveedores de servicios certificados lo guían y lo apoyan a través de las acciones de respuesta
- El exclusivo servicio de análisis de amenazas Elevate to WithSecure™ y orientación experta lo respalda

Respuesta automatizada

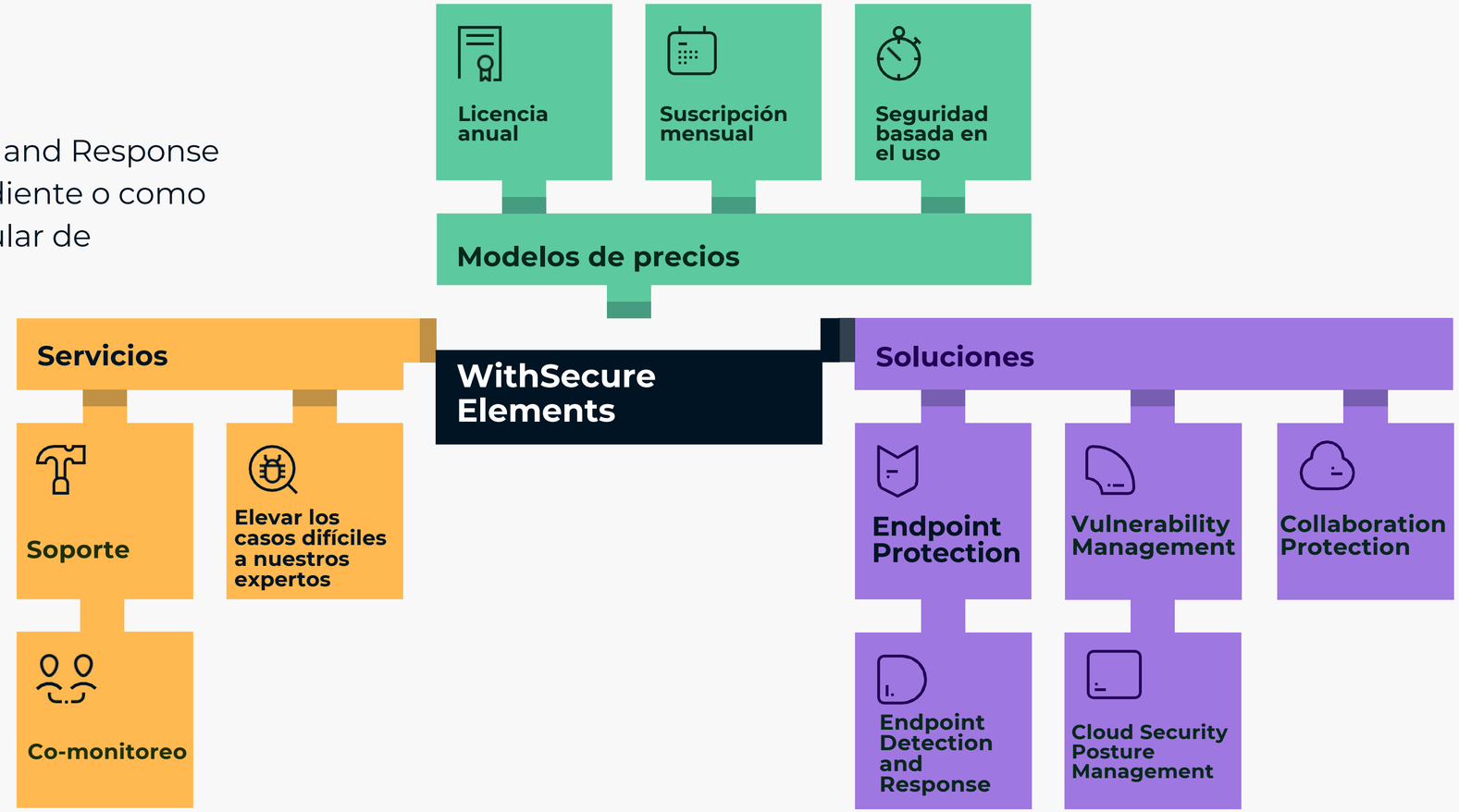
Reduzca el impacto de los ataques cibernéticos dirigidos al automatizar las acciones de respuesta las 24 horas del día.

- Acciones de respuesta automatizadas basadas en criticidad, niveles de riesgo y cronograma predefinido
- Los niveles de criticidad y riesgo proporcionados por la solución permiten priorizar las acciones de respuesta
- Contenga los ataques rápidamente, incluso si su equipo solo está disponible durante el horario comercial

WithSecure Elements – Reduce los ciber-riesgos, la complejidad y la ineficiencia

WithSecure™ Elements Endpoint Detection and Response está disponible como una solución independiente o como un modulo integrado en la plataforma modular de ciberseguridad WithSecure™ Elements.

- Solicite una prueba de concepto y conozca mas a detalle nuestra solucion



Quienes somos

WithSecure anteriormente F-Secure Business, es su socio confiable de ciberseguridad. Los proveedores de servicios de TI, los MSSP y las empresas junto con las instituciones financieras más grandes, los fabricantes y miles de los proveedores de tecnología y comunicaciones más avanzados del mundo confían en nosotros para la seguridad cibernética basada en resultados que protege y habilita sus operaciones. Nuestra protección impulsada por IA asegura los endpoints y su nube de colaboración; nuestra detección y respuesta inteligente está impulsada por expertos que identifican los riesgos comerciales mediante la búsqueda proactiva de amenazas y el enfrentamiento de ataques en vivo. Nuestros consultores se asocian con empresas y desafíos tecnológicos para desarrollar resiliencia a través de consejos de seguridad basados en evidencia. Con más de 30 años de experiencia en la creación de tecnología que cumple con los objetivos comerciales, hemos construido nuestra cartera para crecer con nuestros socios a través de modelos comerciales flexibles. WithSecure Corporation, fundada en 1988, y cotiza en NASDAQ OMX Helsinki Ltd.

W / T H
secure