DETENGA
ATAQUES DIRIGIDOS

WithSecure™Elements Endpoint Detection and Response

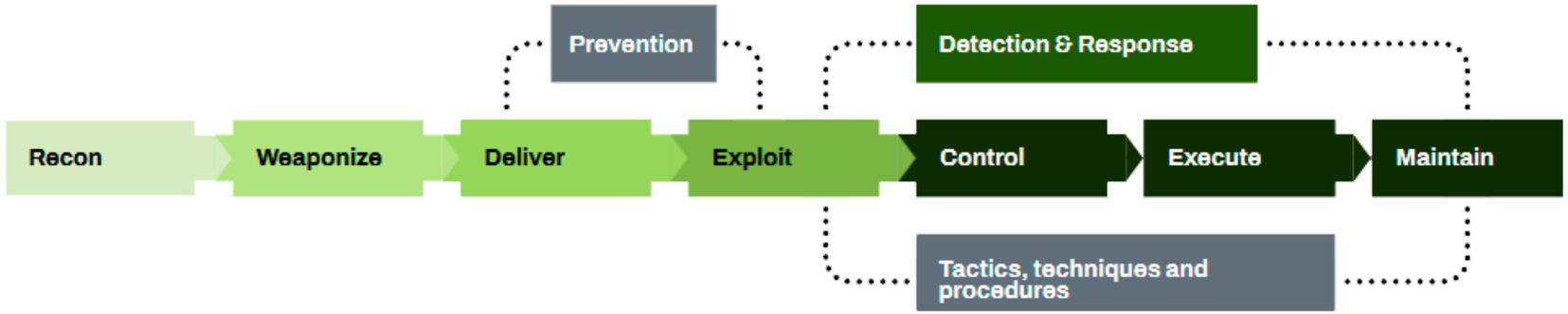
PROTEGE TU NEGOCIO Y SUS DATOS CONTRA LOS CIBER ATAQUES AVANZADOS

La prevención eficaz de amenazas antes del 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 ataques dirigidos.

El panorama de amenazas en constante evolución, junto con las demandas regulatorias como GDPR, requieren que las empresas estén preparadas para la detección de infracciones posteriores al compromiso. Eso significa garantizar que una empresa sea capaz de responder rápidamente a ataques avanzados.

La solución WithSecure™ Elements Endpoint Detection and Response, está respaldada por un equipo experimentado en la búsqueda de amenazas, permitiendo que su propio equipo de TI o un proveedor de servicios certificado proteja su organización contra amenazas avanzadas.

Con el respaldo de los expertos en ciberseguridad de clase mundial de WithSecure™, sus propios especialistas en TI podrán responder a los incidentes de manera rápida y eficaz. 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 cuando sea atacado.



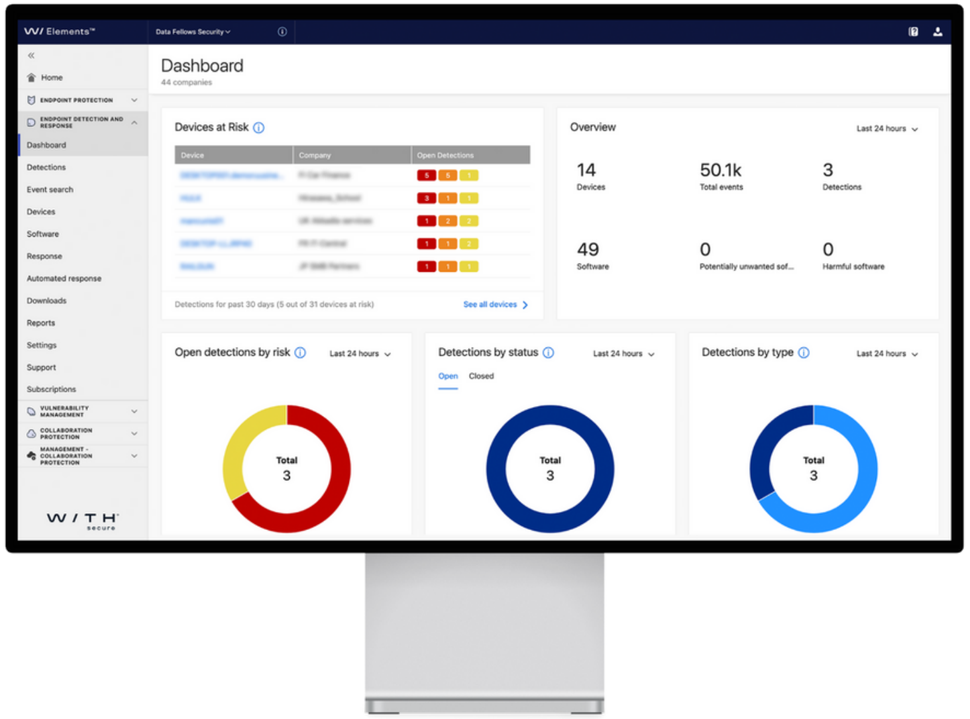
Resumen

DETENGA ATAQUES DIRIGIDOS RÁPIDAMENTE CON ORIENTACIÓN Y AUTOMATIZACIÓN

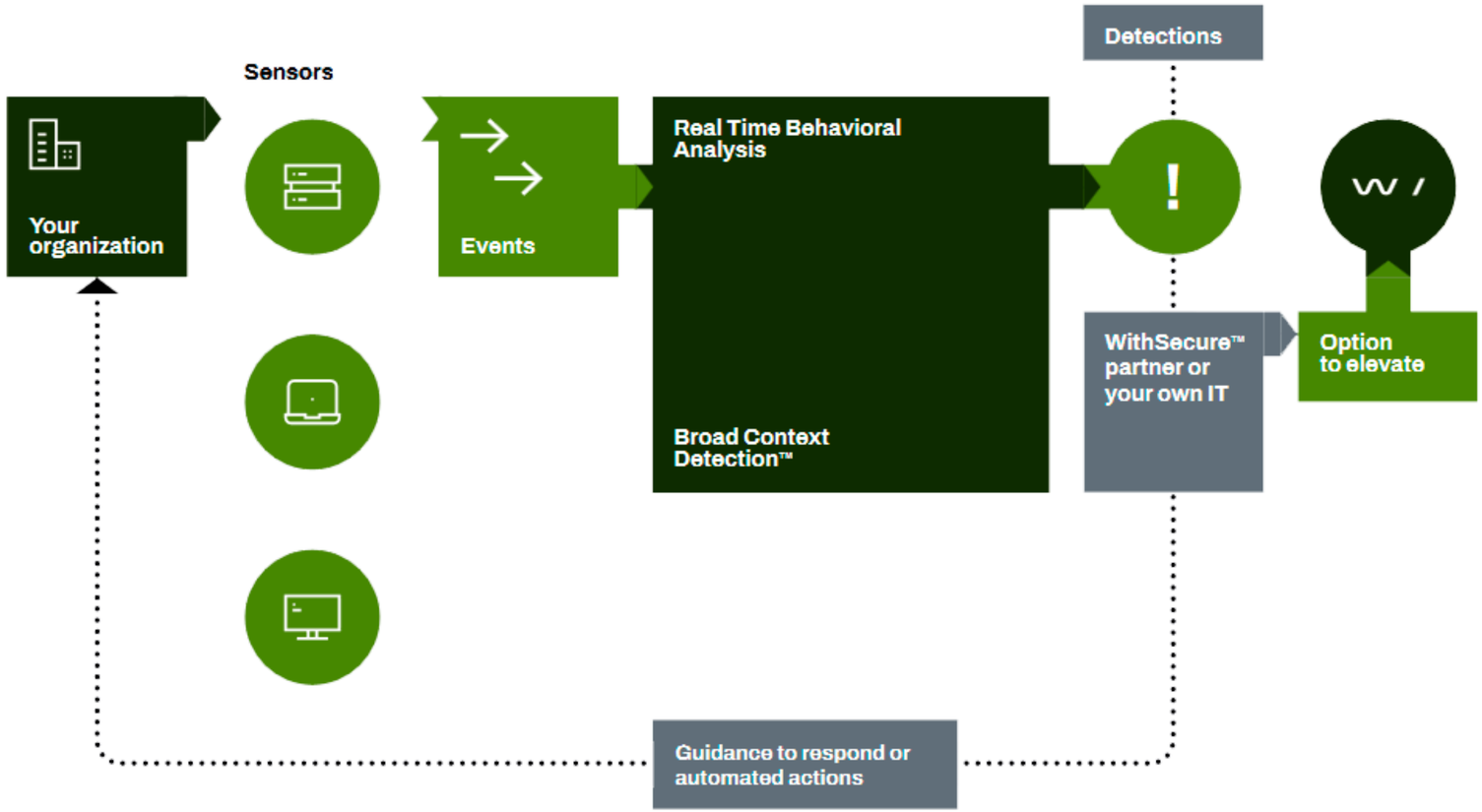
Cómo detecta un ataque sofisticado? Utilice las tecnologías de análisis y aprendizaje automático más avanzadas para proteger a su organización contra ciberamenazas e infracciones avanzadas.

La solución líder en la industria de detección y respuesta de endpoints (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 Broad Context Detection TM, junto con los proveedores de servicios certificados y la automatización incorporada, detendrán rápidamente el ataque y brindarán consejos prácticos para futuras acciones de remediación.



Como funciona



La tecnología líder en la industria y los expertos en seguridad cibernética de WithSecure™ a su servicio

1. Los sensores ligeros implementados en los puntos finales monitorean los eventos de comportamiento generados por los usuarios y los transmiten al análisis de datos de comportamiento en tiempo real y a los mecanismos Broad Context Detection TM para distinguir los patrones de comportamiento malicioso del comportamiento normal del usuario.

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

3. Luego 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 con los pequeños eventos individuales que desencadenan los atacantes es como tratar de encontrar una aguja en un pajar.

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

Los eventos sospechosos fueron analizados más a fondo por nuestros mecanismos Broad Context DetectionTM 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.

Permitiendo que los equipos de seguridad y de TI se concentren en menos detecciones más precisas y dando como resultado acciones de respuesta más rápidas y efectivas siempre que estén bajo un ciberataque real.

500 MILLONES

Eventos de datos / mes recolectados por 325 sensores de punto final

225 000

Eventos sospechosos después del análisis del comportamiento en tiempo real de los eventos

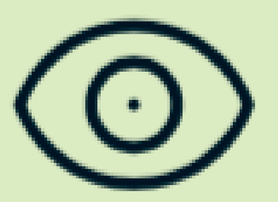
24

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

Obtengavisibilidadinmediatadesu entorno de TI y el estado de seguridad

- Mejora la visibilidad del entorno de TI y el estado de la seguridad a través del inventario de aplicaciones y puntos finales.
- Identifica la actividad sospechosa mediante la recopilación y la correlación de eventos de comportamiento más allá del malware de productos básicos
- Proporciona alertas con información de contexto amplia y criticidad de los activos, lo que facilita la respuesta a incidentes.

Detección

Proteja su negocio y sus datos confidenciales detectando brechas rápidamente

- Detecte y detenga los ataques dirigidos rápidamente para minimizar las interrupciones del negocio y el impacto negativo de la marca.
- Tenga la solución configurada en cuestión de horas, lo que le permitirá estar preparado para las infracciones de inmediato.
- Cumpla con los requisitos reglamentarios de PCI, HIPAA y GDPR que requieren que las infracciones se informen dentro de 72 hrs.

Respuesta

Responda rápidamente con orientación y automatización cuando 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 las 24 horas del día.
- Cubra su falta de habilidades o recursos respondiendo a los ataques con un proveedor de servicios certificado respaldado por WithSecure™

Caracteristicas

Sensores Endpoint

Herramientas de supervisión ligeras y discretas diseñadas para funcionar con cualquier solución de protección de endpoints

- Los sensores ligeros se implementan en todas las computadoras relevantes de su organización.
- Infraestructura de gestión y de cliente único con las soluciones de seguridad para terminales 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 la seguridad nunca ha sido tan fácil

- Identifica todas las aplicaciones dañinas o no deseadas y los destinos externos 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 violaciones de datos.

Respuesta guiada

Lo prepara para enfrentar incluso los ciberataques más avanzados con sus recursos existentes.

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

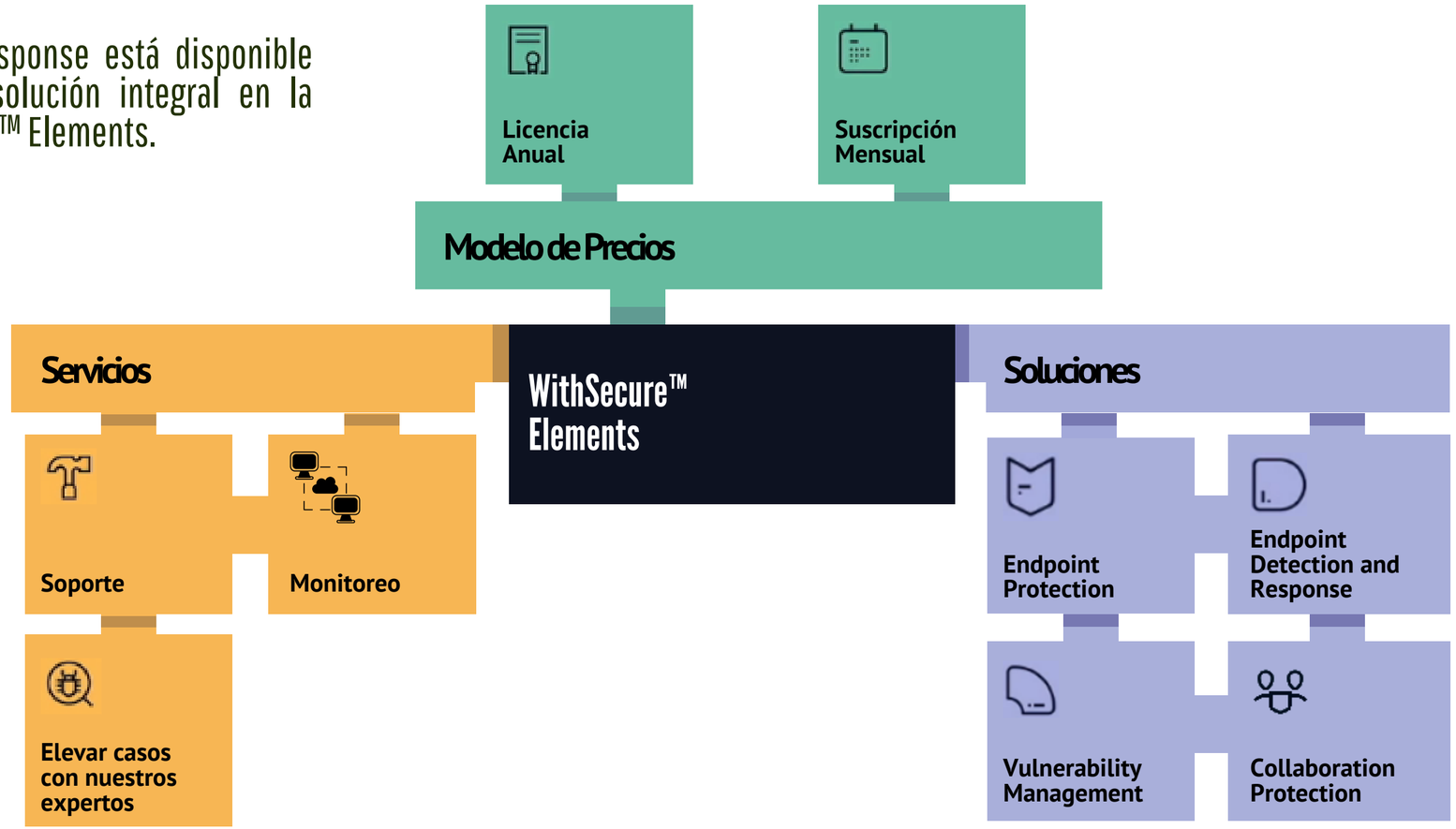
Automated response

Reducir el impacto de los ciberataques dirigidos automatizando las acciones de respuesta durante todo el día.

- Acciones de respuesta automatizadas basadas 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 de oficina.

WithSecure™ Elements
Una plataforma para todas sus necesidades de seguridad

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



Quienes somos

WithSecure es el socio confiable de la seguridad cibernética. 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 protege los endpoints y la colaboración en la nube, y 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 cumpla con los objetivos comerciales, hemos construido nuestra cartera para crecer con nuestros socios a través de modelos comerciales flexibles.

WithSecuretm es parte de F-Secure Corporation, fundada en 1988 y cotiza en NASDAQ OMX Helsinki Ltd.

WITH secure