WithSecure™ Elements Exposure Management

Pitch Deck
GA version

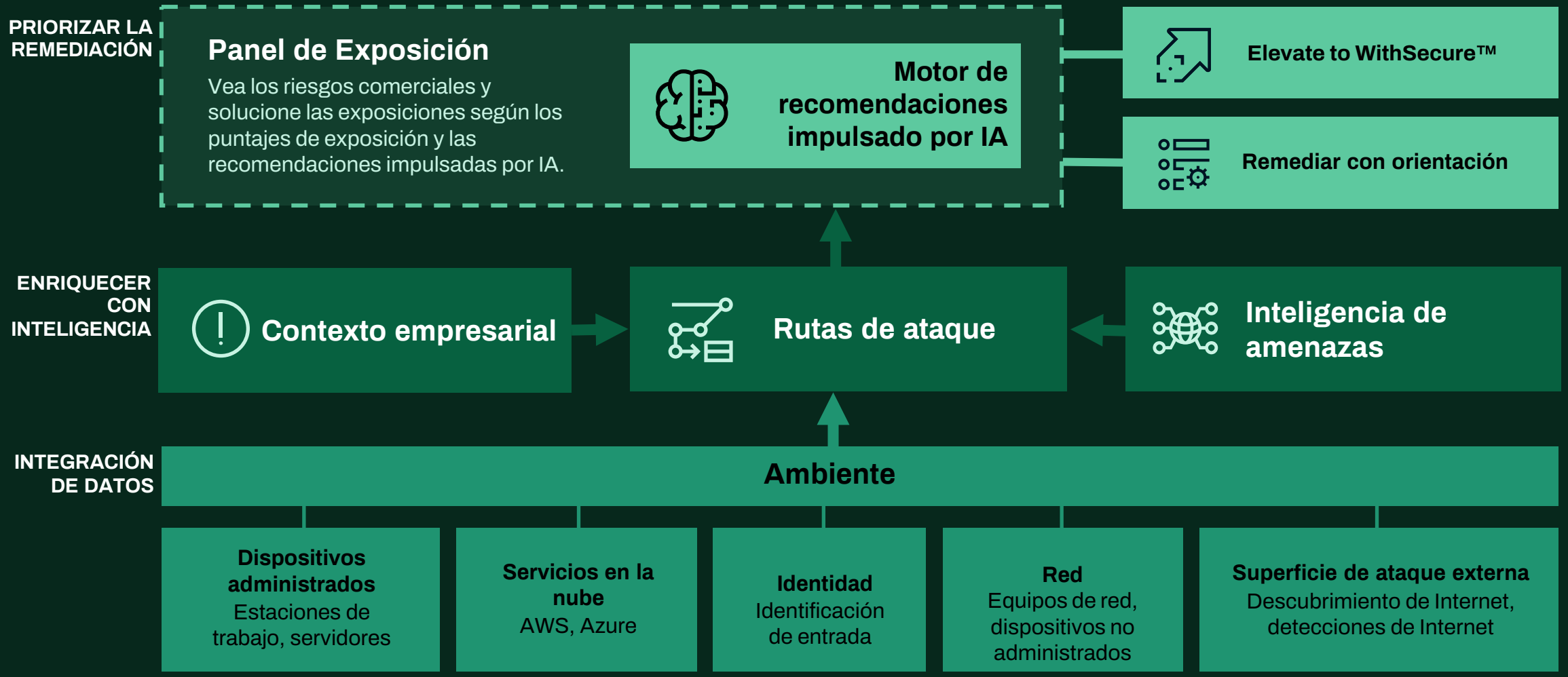
WITH secure

WithSecure™ Elements Exposure Management (XM)

Una solución proactiva continua para predecir y prevenir violaciones a los activos y operaciones comerciales de su empresa.

WithSecure™ Elements Exposure Management

Evaluación continua de la exposición a amenazas, utilizando la visión que tiene el atacante de su entorno.



De la gestión de vulnerabilidades a la gestión de exposiciones

Elements Exposure Management (XM) Presentación para clientes de Elements Exposure Management

WITH secure

3 desafíos clave en la gestión de vulnerabilidades

1. **NO HAY SUFICIENTE VISIBILIDAD:** No integra datos de todo su patrimonio digital ni descubre dependencias entre activos.
   - Por ejemplo, identidades faltantes, la nube y la superficie de ataque externa.
2. **MÁS TRABAJO:** Puede provocar fatiga de alerta y requiere un procesamiento regular de las vulnerabilidades.:
   1. Revisar todas las alertas y hallazgos
   2. Realizar investigaciones sobre el contexto empresarial y las dependencias de cada hallazgo importante
   3. Acordar qué es lo más importante que hay que arreglar
   4. Empezar a remediar los problemas
3. **RIESGO LIMITADO:** No incluye muchos factores de riesgo relevantes.
   - **Por ejemplo:** Inteligencia de amenazas, gestión de la superficie de ataque, exposiciones de red, TI en la sombra y activos desconocidos o no administrados

WITH secure

VM – Método antiguo

X Vulnerabilidades individuales que no están conectadas y que cubren una parte de su superficie de ataque

X Centrarse en la identificación: ¿Cuáles son los activos más críticos para los cuales es necesario reparar las vulnerabilidades en mi entorno derivadas de todas estas alertas?

X Priorización manual: Reserve tiempo para priorizar las vulnerabilidades antes de remediarlas

XM – Método nuevo

✓ Modelado de ruta de ataque que cubre las vulnerabilidades, configuraciones incorrectas y otras exposiciones entre los activos en toda su superficie de ataque

✓ **Centrarse en la remediación:** Las recomendaciones continuas impulsadas por IA ya realizan la priorización de riesgos, cubriendo dimensiones de riesgo sofisticadas:

- Probabilidad de exposición, contexto empresarial, explotabilidad como parte de las rutas de ataque e inteligencia de amenazas

✓ **Priorización automática:** Remediar rápidamente las exposiciones que se muestran como puntos críticos de estrangulamiento como parte de las rutas de ataque

WITH secure

De la identificación a la remediación:
Elements Exposure Management (XM)

- **Concéntrese en minimizar el riesgo empresarial** con una solución continua y proactiva para predecir y prevenir infracciones contra los activos y las operaciones comerciales de su empresa.
  - Utilice rutas de ataque, información del contexto empresarial e inteligencia de amenazas para solucionar lo que más importa.
- **Obtenga funcionalidad adicional** además de las excelentes funciones existentes de Elements VM:
  - Conecte sus identidades de Entra ID para identificar violaciones de credenciales o configuraciones riesgosas
  - Conecte sus cuentas de nube de Azure y AWS
  - EASM (Mapeo de la superficie de ataque externa)™
  - Aumente la funcionalidad consultando a los expertos de WithSecure sobre las recomendaciones de Withsecure Elements XM

WITH secure

Mira cómo podrías ser atacado

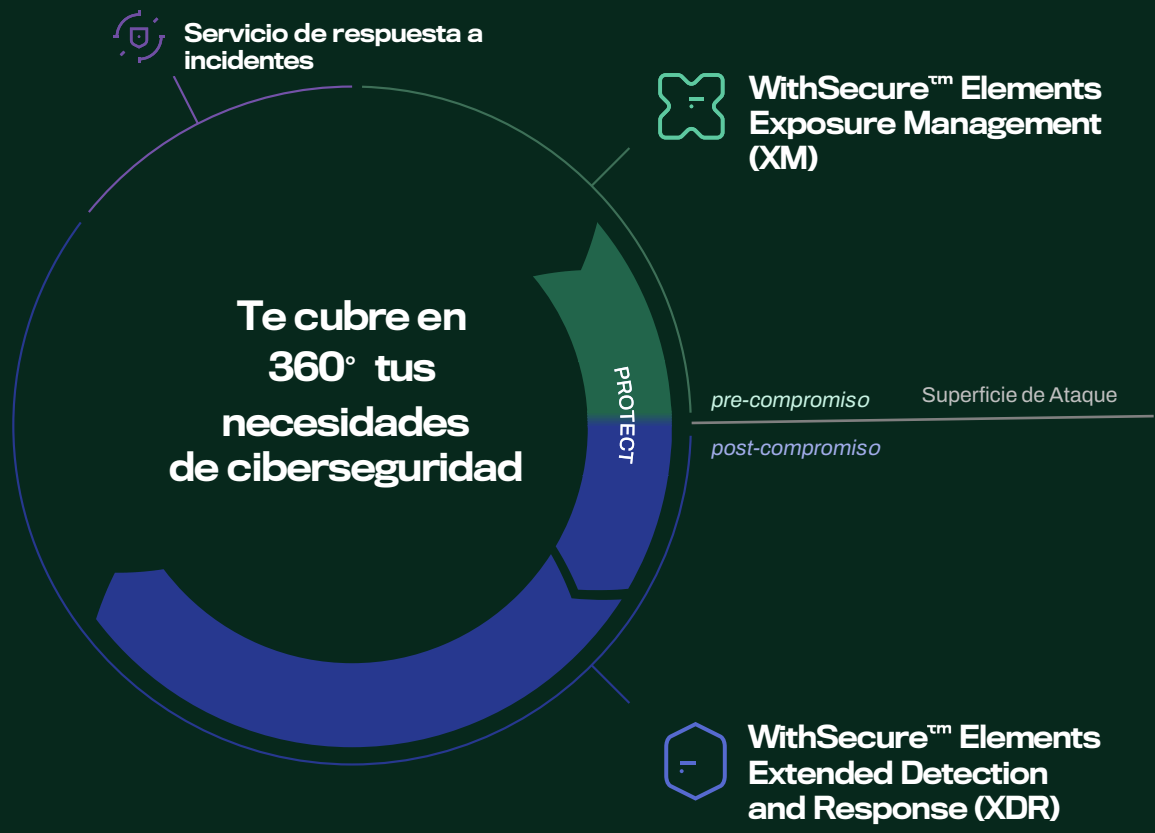
Elements Exposure Management (XM) Presentación para clientes de Elements Exposure Management

WITH secure

Más vale prevenir que curar.

3 razones para agregar XM a su suite Elements:

1. Solucione sus brechas de seguridad antes de realizar **investigaciones costosas**.
   - Elements XM le ayuda a identificar y solucionar sus exposiciones antes de que necesite invertir mucho tiempo, dinero y esfuerzo en investigar incidentes.
2. Ayuda a **evitar daños a la reputación de su marca y la pérdida de datos de clientes** debido a incidentes.
   - La confianza del público y de los clientes suele requerir mucho tiempo y muchos recursos para reconstruirse.
3. Visibilidad de los **riesgos de su negocio** desde el mismo Elements Security Center.



Note: Figure adapted from NIST cyber security framework. We offer additional Incident Response services to cover the "Recover" area of NIST.

WITH secure

Un caso de prevención: Cambiar la atención médica

Qué: Cambia Healthcare extorted por el grupo Blackcat en un ataque de ransomware

Razón: Probablemente causado por credenciales robadas (ataque basado en identidad) debido a la falta de MFA

Exposición: Potencialmente, la información de salud protegida de hasta 1 de cada 3 estadounidenses

Costos Directos:

- Se pagaron $22 Millones de dólares (USD) como rescate
- Datos filtrados y rescatados nuevamente por el grupo RansomHub (¿rescate repagado?
- Casi $2 Mil millones de dólares en costos de respuesta directa

Costos indirectos:

- Al menos ~$300 millones perdidos debido a la interrupción del negocio
- Costos legales y costos de notificación a más de 110 millones de personas
- Daño a la confianza del cliente, la reputación de la marca y la valoración del mercado de valores

1 en 3

Hasta cada tercer ciudadano estadounidense afectado

Total: Se prevé que los costos del ataque sean de al menos 2.300 millones de dólares en 2024 (más de 100 veces la suma del rescate)

Source: Change Healthcare Reports Ransomware Data Breach to HHS (hipaajournal.com) (Accessed 12.9.2024) **Note:** MFA means Multi-Factor Authentication.

WITH secure

Elements XM mejora tu experiencia con Elements

- Remediar vulnerabilidades:
  - Active rápidamente el **análisis basado en agentes** para sus dispositivos e identifique vulnerabilidades y obtenga recomendaciones priorizadas al instante sobre qué problemas solucionar primero y qué dispositivos están expuestos a rutas de ataque. Además, obtenga la puntuación de exposición de cada dispositivo.
  - Escanee nodos para escanear todos los activos de su **red**
  - Mapee su **superficie de ataque externa**
- Aborde las configuraciones incorrectas de la nube con el escaneo de cuentas en la nube de **Azure y AWS**
- Gestione los riesgos de identidad escaneando las identidades de **Entra ID para identificar violaciones de credenciales** o configuraciones riesgosas
- Obtenga un **inventario de activos**, incluido el software instalado y las versiones:
  - Implemente actualizaciones de software instantáneamente desde Elements XM a través del **Actualizador de software***
  - Mejore sus prácticas de gestión de parches centrándose en las recomendaciones de mayor impacto de Elements XM

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

WITH secure

Escanee su patrimonio digital

Dispositivos y redes administrados		Superficie de ataque externa, identidad y servicios en la nube		
Nodo de escaneo local/en la nube	**Elements Agent**	**Superficie de ataque externa**	**Integraciones de identidad**	**Integraciones en la nube**
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	**Identificación de entrada** 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* 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.

WITH secure

Actualizadora de software
(parte de Elements EPP)

✓ Solo informa sobre problemas de software que puede solucionar

✓ Centrarse en todos los parches disponibles para software, sistemas operativos y aplicaciones, ya sean relacionados con la seguridad o no.

- Actualizaciones de seguridad de Microsoft
- Actualizaciones de software de terceros

✓ Las capacidades automatizadas para aplicar parches de software se pueden aplicar fácilmente desde las vistas de Elements XM

Elements XM

✓ Utiliza fuentes de datos integrales para identificar el software expuesto, como parte de la protección de toda su superficie de ataque.

✓ Centrarse en las vulnerabilidades y las configuraciones incorrectas, así como en los informes de exposiciones, ya sea que el parche exista o no.

- Centrarse en todos los dispositivos, sistemas, hardware, etc.

✓ Capacidades integrales para respaldar los procesos de gestión de exposición y remediación

WITH secure

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

Elements Exposure Management Presentación para nuevos clientes

WITH secure

Puntos críticos de la superficie de ataque actual

Entorno híbrido con fronteras poco claras

Falta de visibilidad en entornos locales y en la nube

Las identidades como eslabón débil

Potentes puntos de aceleración de ataques, fácilmente robados y estafados

Panorama dinámico de amenazas

Cambios constantes en el panorama de amenazas y ciberataques impulsados por IA

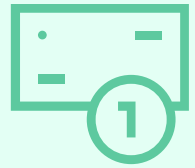
WITH secure

Resultados clave:

Benefíciese de la remediación de la exposición a través de la perspectiva del atacante:

Tranquilidad de espíritu
Conozca su nivel de riesgo y cómo reducirlo

Aumentar la productividad
Concéntrese en lo que importa en lugar de ahogarse en alertas



Utilizar habilidades existentes
Gestionar la exposición con los recursos de TI existentes

Asegure su parte de la cadena de suministro
como una superficie de ataque digital compleja

Muchas exposiciones, una solución
Aborde vulnerabilidades, exploits y configuraciones incorrectas sin silos

Motor de recomendaciones impulsado por IA
Para una priorización automatizada con orientación práctica

WITH secure

Elements XM ayuda a los tomadores de decisiones a tomar decisiones informadas sobre el riesgo de su negocio.

WITH secure

Optimice su inversión en pruebas de penetración

Elements Exposure Management

Presentando argumentos para clientes importantes

WITH secure

Obtenga la perspectiva de un atacante en su organización

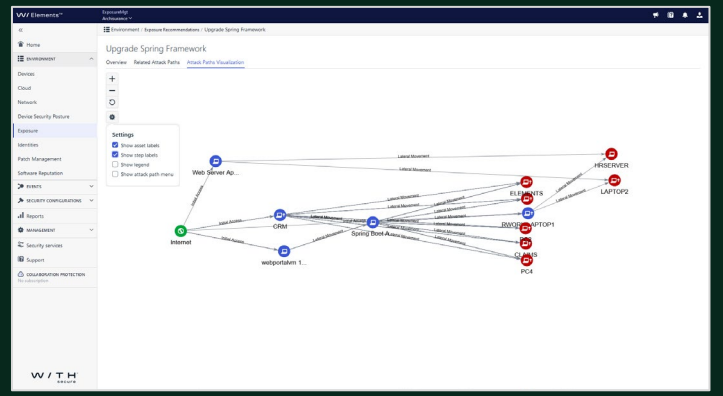
?

¿Está seguro de saber cómo se ve su entorno de TI desde el punto de vista de un externo?

WITH secure

Mapeo de rutas de ataque

Comprenda los activos en su entorno, los riesgos activos y la relación entre los activos.



External Attack Surface

Collaboration Tool

CRM System

HR Platform

Messenger

W/TH secure

Estás en el asiento del conductor

Estar a la vanguardia: Comprenda cómo se pueden explotar los riesgos en el entorno de su organización antes de que lo haga un atacante y luego redúzcalos.

WITH secure

Optimice su inversión en pruebas de penetración y equipos rojos

¿Invertir en pruebas de penetración y en equipos rojos?

Enfoque su inversión en aspectos de seguridad complejos más allá de los básicos que se pueden solucionar fácilmente con Elements XM.

Pruebas de penetración

Equipo rojo

W/ Elements™ | Exposure Management

W/TH secure

Prueba del trabajo de seguridad proactivo del CISO – para tiempos de paz y crisis

Con Elements XM, los CISO pueden demostrar e informar sobre el impacto de las mejoras de seguridad proactivas y granulares de su equipo en el riesgo de seguridad general de la organización.

WITH secure

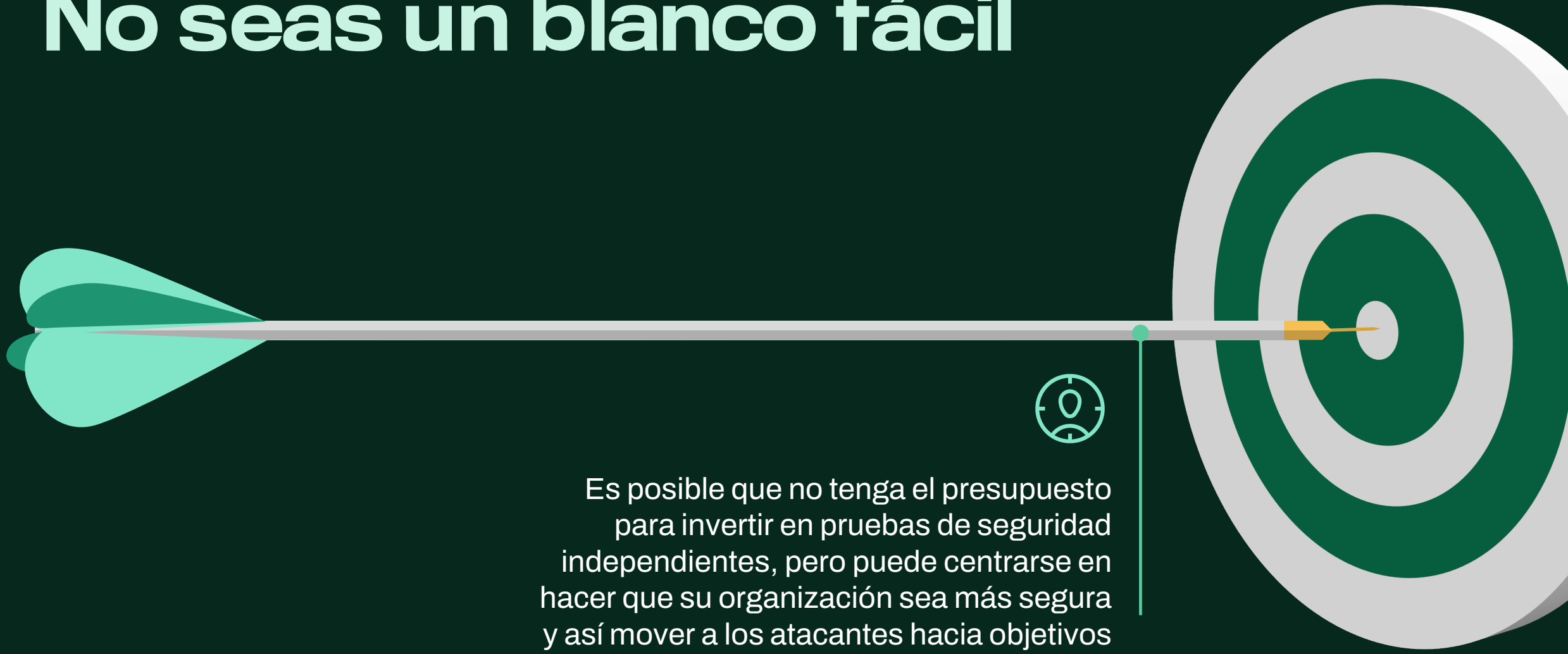
No seas un blanco fácil

Elements Exposure Management

Lanzando argumentos para pequeñas clientes finales

WITH secure

No seas un blanco fácil



Es posible que no tenga el presupuesto para invertir en pruebas de seguridad independientes, pero puede centrarse en hacer que su organización sea más segura y así mover a los atacantes hacia objetivos más fáciles.

WITH secure

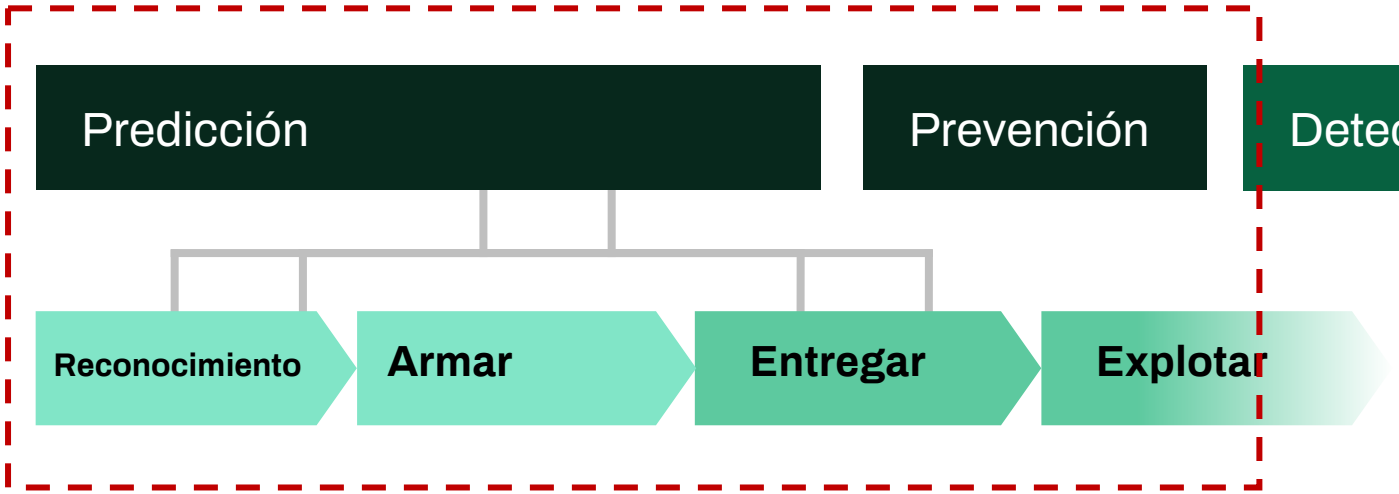
Arregla las cerraduras de tu casa

Su entorno informático es como una mansión donde los atacantes intentan entrar constantemente a través de cientos de puertas y portones, muchos con cerraduras antiguas y fáciles de forzar. En otras palabras, algunas rutas de ataque son más fáciles que otras. Algunas de estas cerraduras conducen a salas donde se almacenan sus activos más valiosos.

Con **Elements XM**, puede ver cómo un atacante puede entrar por una puerta y adentrarse en la mansión, donde se almacenan sus valiosos bienes. Le indicamos qué cerraduras son las más críticas para reparar. Así, su equipo de TI puede centrarse en solucionar los problemas más importantes.

WITH secure

Elimina tus exposiciones – elimina tus problemas de seguridad



MITRE | ATT&CK®

Contramedidas tempranas

La mejor forma de minimizar la superficie de ataque es eliminar las **vulnerabilidades** y **configuraciones** erróneas que podrían explotarse, antes de que puedan surgir problemas de seguridad.

WITH secure

Una alternativa asequible a las pruebas de penetración

Las pruebas de penetración son como contratar a un grupo de expertos que conocen cómo actúan y piensan los ladrones para entrar en tu casa una vez al año. Esto te da una idea de cómo funcionan en tu casa los aspectos de seguridad específicos que el grupo decide explotar. Si bien esto es excelente, tu entorno de seguridad es dinámico, con nuevas debilidades que surgen constantemente y los atacantes desarrollando nuevas técnicas.

Por otro lado, **Elements XM** es como un sistema de seguridad continuo con inteligencia artificial que cubre toda tu casa. Monitorea el entorno y te alerta si algún punto débil podría ser explotado por ladrones. Además, te ofrece recomendaciones inteligentes y priorizadas sobre cómo mitigar posibles ataques corrigiendo las vulnerabilidades de seguridad de tu hogar.

Existimos para construir y mantener la confianza digital

150,000
Clientes

Un líder europeo
Empresa de ciberseguridad

6,000
Fogonadura

70
Nacionalidades

~1,000
Empleados

35
Años de historia

€143m
Ingresos 2023

Listed
En el NASDAQ OMX Helsinki Ltd

WITH secure

secure