# WithSecure™ Elements Vulnerability Management

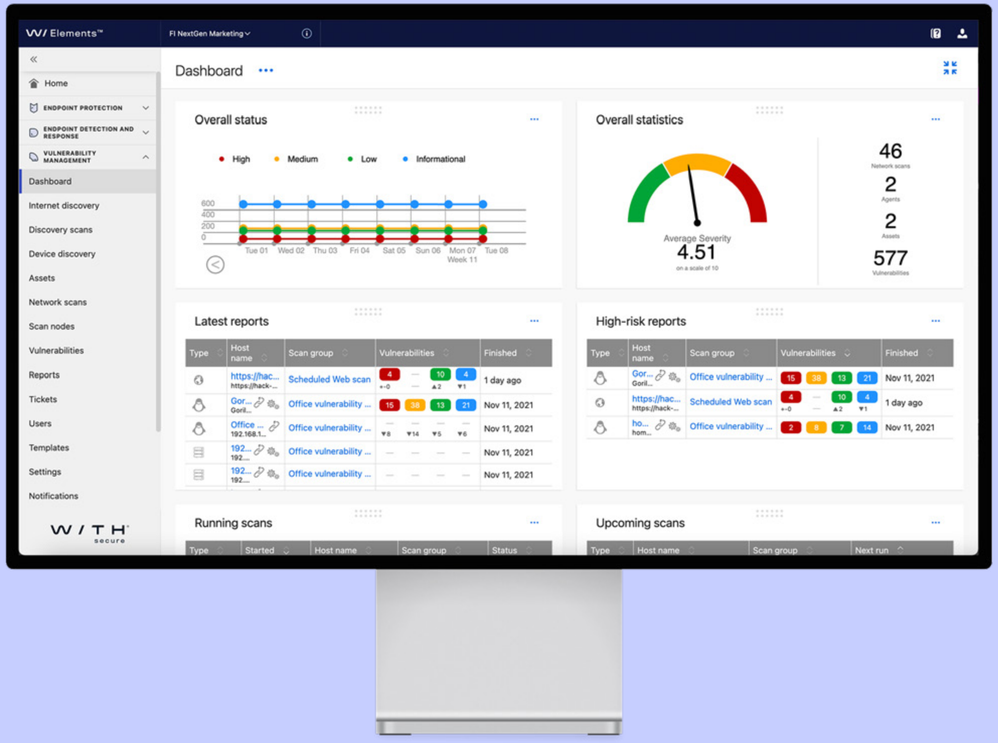
**Conozca su superficie de ataque para reducir el riesgo. Corrija vulnerabilidades con una solución integral diseñada para entornos de TI dinámicos.**

W / T H secure

Los entornos de TI en expansión son más difíciles de proteger y necesitan más énfasis en medidas predictivas de seguridad cibernética. Con el escaneo automatizado y la corrección continua de vulnerabilidades, puede minimizar los riesgos y abordar las amenazas antes de que ocurran. Con una priorización basada en riesgos, sus esfuerzos tendrán el mayor impacto y su productividad se disparará.

Por muy evidentes que sean los beneficios empresariales, las nuevas soluciones conllevan inconvenientes de seguridad. Los entornos de TI dinámicos y complejos generan amplias superficies de ataque con más desafíos y vulnerabilidades de seguridad. Los atacantes buscan constantemente oportunidades para explotar sistemas defectuosos y sin parches para obtener acceso no autorizado a datos valiosos. Buscan vulnerabilidades por una sencilla razón: funciona. Cuantos más dispositivos, sistemas y aplicaciones del entorno queden vulnerables, más oportunidades habrá para el atacante. Una laguna jurídica es suficiente.

Fuera de la vista, fuera de la mente no es la mejor opción cuando se trata de ciberseguridad. Quiere saber qué es lo que está protegiendo y cómo hacerlo más seguro. Su superficie de ataque es un organismo vivo donde cada día surgen nuevas vulnerabilidades. Buscar vulnerabilidades de vez en cuando es mejor que nada, pero no es suficiente. Al tomar medidas programáticas predictivas y preventivas, puede mejorar considerablemente sus probabilidades de resistir las amenazas cibernéticas.



# Dile adiós a volar a ciegas y reduce tu superficie de ataque.

## Fortalecer su ciberseguridad comienza con conocer sus activos y dónde son vulnerables

La gestión de vulnerabilidades significa cerrar de forma proactiva las brechas de seguridad antes de que los atacantes las exploten. Es un proceso continuo de descubrimiento y seguimiento de sus activos. Incluye identificar, categorizar, priorizar y remediar vulnerabilidades en sus sistemas operativos, así como software y aplicaciones en su entorno de TI. Es un elemento vital en la estrategia de seguridad cibernética de cualquier organización y para garantizar una postura de seguridad saludable al reducir las probabilidades de que los ciberdelincuentes accedan a sus sistemas.

La gestión eficaz de la vulnerabilidad evoluciona con los entornos cambiantes sin dejar de ser sistemática. Se prioriza en función de su nivel de riesgo y sus objetivos comerciales. El escaneo regular de redes y vulnerabilidades garantiza que aprovechará al máximo sus esfuerzos. La gestión continua y cíclica de vulnerabilidades le ayuda a obtener y mantener una comprensión profunda de su entorno, sus nuevos dispositivos, servicios y tendencias, y si se han actuado adecuadamente frente a las vulnerabilidades.

## Obtenga conocimiento de la situación y obtenga actualizaciones periódicas sobre su estado de seguridad

WithSecure Elements Vulnerability Management identifica los activos de su organización, señala exactamente dónde son vulnerables y determina dónde están las vulnerabilidades más críticas. En lugar de conducir a ciegas puedes:

- Identifique todos los hosts en su rango de red
- Escanee sus activos en busca de puertos abiertos
- Detectar versiones actuales de software y sistema operativo
- Encuentre versiones de software vulnerables comparando sus versiones instaladas con una base de datos de vulnerabilidades conocidas
- Identificar fallas de configuración
- Escanee y verifique minuciosamente los activos de destino
- Aproveche los escaneos automatizados
- Responda rápidamente a sus mayores amenazas con una priorización basada en riesgos.

## ¿Por qué elegir la gestión de vulnerabilidades de WithSecure Elements?

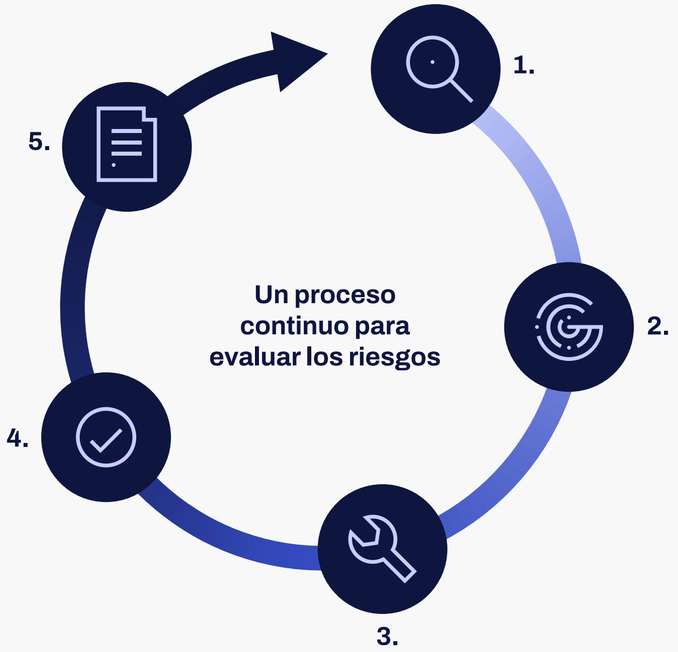
**Sepa lo que está protegiendo**
Una buena seguridad requiere que usted sepa qué es exactamente lo que está protegiendo.

**Visibilidad continua**
Mapeo de seguridad efectivo a través del descubrimiento y mapeo precisos de todos los activos, sistemas y aplicaciones en la red y más allá.

**Encuentre lagunas**
Minimice su superficie de ataque solucionando las vulnerabilidades antes de que sean explotadas

**Predecir el riesgo**
Sepa dónde están sus activos de alto riesgo y priorícelos.

## Encuentre sus puntos débiles internos y externos antes que nadie con operaciones consistentes y sistemáticas.




*La gestión eficaz de la vulnerabilidad es un proceso continuo*

Existe una creencia generalizada, pero falsa, de que la gestión de vulnerabilidades es engorrosa y requiere muchos recursos. Requiere un cierto nivel de compromiso y esfuerzo constante cuando se hace bien, pero es más fácil de lo que piensas.

Hemos dividido el proceso de gestión de vulnerabilidades en cinco pasos sencillos. Con este marco, puede mantenerse informado de manera efectiva sobre su entorno de TI, comprender sus activos y vulnerabilidades, corregir las vulnerabilidades encontradas, realizar un seguimiento de su progreso y documentar todo.

1. **Descubra** todos los activos de la red
2. **Escane** activos y aplicaciones en busca de vulnerabilidades
3. **Remedie** eficazmente a través de un proceso gestionado
4. **Valide** que se completaron las acciones correctivas.
5. **Documente** todas las acciones correctivas tomadas para la auditoría.

## Beneficios

- **Minimizar el riesgo**
  Prediga y prevenga amenazas derivadas de su arquitectura de seguridad.

- **Priorizar la productividad**
  Céntrese en las vulnerabilidades de alto riesgo en lugar de luchar constantemente contra incendios.

- **Optimice los flujos de trabajo**
  Construir procesos de gestión eficientes. Automatiza y reduce los puntos de contacto manuales.

- **Rentable sin compromisos**
  Obtenga visibilidad continua con escaneos de vulnerabilidades y nodos de escaneo ilimitados. El costo de las medidas predictivas es extremadamente bajo en comparación con los costos de remediación o el costo de una infracción.

- **Cumplir con las regulaciones**
  Siga cumpliendo con las regulaciones actuales y futuras realizando evaluaciones periódicas de vulnerabilidad.

## 1. Descubra los activos de la red

Recopile información sobre sus sistemas conectados a Internet y mapee sus dispositivos internos.

Al principio, empiezas conociendo tu entorno. En la práctica, asigna sus activos conectados a Internet con Internet Discovery Scan y sus activos internos con Discovery Scan. Al hacer esto, puede mantenerse al día con un entorno de TI moderno y en constante cambio y descubrir activos desconocidos u olvidados (TI en la sombra) con parches de seguridad potencialmente faltantes que representan un riesgo para su postura de seguridad. Este primer paso es bastante simple, pero importante para el flujo de trabajo, ya que lo ayudará a corregir fallas en su verdadera superficie de ataque en etapas posteriores del proceso.

## 2. Escanear activos y aplicaciones en busca de vulnerabilidades.

Una vez que haya mapeado todos los activos en la red, puede escanearlos en busca de vulnerabilidades.

Puede escanear computadoras con Windows con escaneo basado en agentes para obtener información detallada sobre vulnerabilidades, que incluye:

- Lista de software instalado
- Versiones de software vulnerables
- Y versiones de SO vulnerables

Para un escaneo más amplio, puede usar System Scan para escanear todos los sistemas con una dirección IP en su red para:

- Puertos abiertos
- Vulnerabilidades conocidas
- Contraseñas predeterminadas
- Y malas configuraciones.

Para una investigación en profundidad, tiene un escaneo autenticado que le permite iniciar sesión de forma remota en los sistemas para recopilar datos de vulnerabilidad más detallados y precisos.

Con Web Scan puede encontrar vulnerabilidades en aplicaciones web personalizadas. Lo mismo se aplica a los módulos personalizados en plataformas comunes como WordPress.

## 3. Priorizar las vulnerabilidades encontradas por nivel de riesgo y remediarlas

Las puntuaciones de las soluciones encontraron vulnerabilidades basadas en el riesgo y la criticidad. Esto permite flujos de trabajo priorizados con énfasis en las vulnerabilidades con mayor impacto comercial y le permite a usted y a su equipo dedicar su tiempo a las más críticas. Puede asignar y gestionar vulnerabilidades con un sistema de tickets integrado.

## 4. Validar acciones correctivas

Puede verificar si las vulnerabilidades se han solucionado con el sistema de tickets integrado. Volver a escanear un objetivo indicará automáticamente en la emisión de tickets si se realizó la corrección.

La solución documenta automáticamente cualquier acción correctiva tomada para la auditoría.

## 5. Documentar acciones correctivas con informes estándar y personalizados.

Con nuestra herramienta de informes integrada, puede crear informes personalizados que se adapten a las necesidades de su gerente, administrador del sistema o proveedor de servicios externo. Puede informar fácilmente el cumplimiento de las regulaciones y justificar su valor en la gestión de riesgos.

Los informes se pueden personalizar con etiquetado, escaneo de objetivos y de muchas otras maneras.

Siguiente paso: repetir. La evaluación continua de su red y sus activos en busca de posibles vulnerabilidades lo mantiene al tanto de su superficie de ataque y minimiza las lagunas para los atacantes.

## Impulsa un proceso eficiente de gestión de vulnerabilidades con:

**Evaluación y priorización basada en riesgos**
Dar prioridad a la corrección de vulnerabilidades puede resultar difícil basándose únicamente en métricas tradicionales, como la puntuación CVSS.

Al combinar información contextual sobre el activo y su importancia, como cómo se utiliza, con información amplia sobre la vulnerabilidad, se puede comprender el riesgo real detrás de las vulnerabilidades identificadas. Esto le ayuda a crear listas priorizadas de los problemas de seguridad más urgentes. Puede tomar decisiones informadas, optimizar el tiempo empleado y mantener niveles de riesgo generales saludables y una higiene de seguridad constante.

**Paneles intuitivos**
Obtenga una visión general de un vistazo a partir de visualizaciones completas. Cree y edite fácilmente widgets para satisfacer sus necesidades de información.

**Sistema de emisión de billetes integrado**
Integre su sistema de tickets de TI existente para reducir los puntos de contacto manuales.

**Borrar informes**
Comunique los riesgos, el estado actual y lo que se ha hecho a las partes interesadas adecuadas con informes personalizados y listos para usar.

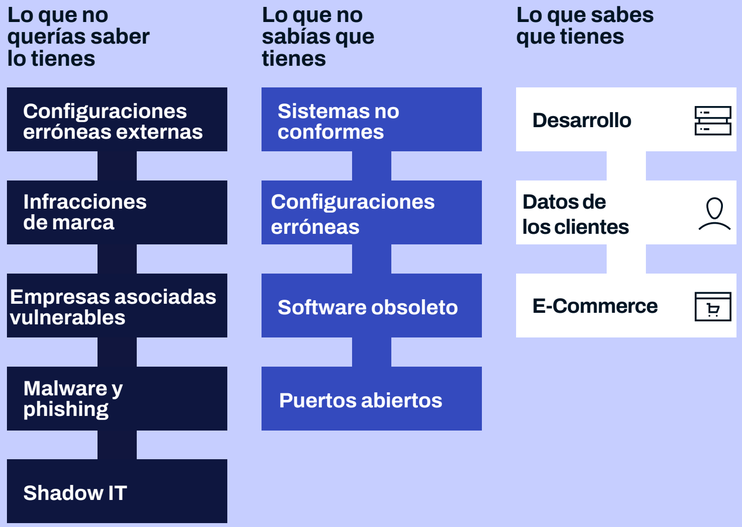
**Escaneos automatizados**
Manténgase actualizado escaneando continuamente su entorno con escaneos automatizados ilimitados.

**Nodos de escaneo ilimitados**
Pague solo por la cantidad de direcciones IP que cubra. Escanea tantos entornos como quieras.

**Implementación flexible**
Implemente rápidamente como una solución entregada en la nube o en el sitio, incluso en entornos cerrados fuera de línea.

**Seguridad consolidada**
Con la plataforma de ciberseguridad unificada nativa de la nube WithSecure™ Elements, puede estar al tanto de su estado de seguridad y proteger sus puntos finales y su colaboración en la nube, mientras administra su superficie de ataque con administración de vulnerabilidades basada en red. Al administrar su seguridad a través de un único panel, puede reducir el riesgo, la carga de trabajo y el tiempo de respuesta cuando surgen amenazas.

## ¿Cuál es la superficie de ataque?




## ¿Qué es una vulnerabilidad?

En seguridad cibernética, una vulnerabilidad es cualquier medio por el cual un atacante puede obtener acceso no autorizado o control de una aplicación, servicio, punto final o servidor.

## Potente arsenal de escaneo para cubrir su superficie de ataque

WithSecure Elements Vulnerability Management le brinda una amplia gama de opciones de escaneo. Obtenga visibilidad total combinando escaneos de red basados en nodos, escaneos de la nube, escaneos de nodos para amenazas externas y escaneos basados en agentes para un escaneo remoto ágil. Inicie sesión en los sistemas para obtener una vista detallada.

**Escaneo de descubrimiento**
Discovery Scan descubre y mapea todos los activos, sistemas y dispositivos de su red. El escaneo le permite crear grupos de escaneo para una gestión eficiente de las vulnerabilidades.

**Escaneo basado en agentes**
El escaneo basado en agente aprovecha el agente único de la plataforma WithSecure Elements y le permite escanear computadoras Windows distribuidas de forma remota fuera de su red. Esto es especialmente útil en la era del trabajo remoto y significa que se requieren menos puertas abiertas para sus dispositivos más valiosos al realizar análisis de vulnerabilidad. El análisis basado en agentes recopila listas de hardware y software e identifica puertos abiertos y vulnerabilidades relacionadas con el software y los sistemas operativos instalados. El escaneo basado en agentes es un procedimiento liviano, fácil de realizar con frecuencia para mantener una vista actualizada de sus activos.

**Escaneo de descubrimiento de Internet**
Internet Discovery Scan identifica todos los sistemas/servicios conectados a Internet. Internet Discovery Scan le ofrece una potente función de búsqueda mediante el uso de nombres DNS para identificar activos dentro del dominio. Le ayuda a conocer qué servicios residen realmente dentro de los dominios bajo su control. Con un Internet Discovery Scan puede encontrar TI oculta y posibles infracciones/violaciones de marca (por ejemplo, un nombre de dominio engañoso).

**Exploración del sistema**
System Scan es un escáner de vulnerabilidades basado en red que puede escanear cualquier sistema con una IP en busca de vulnerabilidades comunes. Primero identifica el sistema y su número de versión, y luego lo verifica en busca de puertos abiertos, vulnerabilidades conocidas (es decir, parches faltantes), contraseñas predeterminadas y configuraciones incorrectas. No causa ninguna interrupción, por lo que no hay temor a que se le niegue el servicio.

**Authenticated Scan** permite que System Scan inicie sesión en los sistemas (mejora la precisión y disminuye los falsos positivos y negativos) para encontrar versiones vulnerables del sistema, parches faltantes y configuraciones erróneas.

**Escaneo Web**
El escaneo web, generalmente utilizado como escaneo complementario, le permite escanear y probar aplicaciones web personalizadas. Puede utilizar análisis web durante el desarrollo de nuevas aplicaciones como parte del ciclo de vida de desarrollo, lo que le permite detectar vulnerabilidades en las primeras etapas del proceso y ahorrar recursos considerables a largo plazo.



**Servidores web, servidores de correo electrónico, subredes DMZ (Cloud Scan Node)**

**Servidores Windows, escritorios Windows (Endpoint Agent)**





**Servidores, Computadoras, Dispositivos de red, Otros dispositivos (nodo de escaneo local)**

# Unificar la gestión de vulnerabilidades con medidas de seguridad cibernética preventivas y receptivas para una verdadera conciencia situacional

La buena ciberseguridad no puede vivir aislada. En primer lugar, cuando se utiliza una pila de herramientas de ciberseguridad fragmentada, hay que saltar constantemente de un portal a otro. La fatiga por alertas es real y la gestión de múltiples flujos de trabajo separados es compleja, lo que dificulta la priorización.

En segundo lugar, la gestión no es la única ineficiencia. Las soluciones en una configuración como ésta no cooperan y pueden ignorarse por completo unas de otras. Esto significa silos, detecciones fallidas, respuestas lentas y, en última instancia, una postura de seguridad más débil.

Para superar los desafíos de un mundo aislado, WithSecure™ Elements unifica las capacidades centrales de seguridad cibernética en una plataforma inteligente. Más elementos significan más resultados, pero usted puede crear su propia suite de seguridad cibernética basada en la nube con módulos de tecnología seleccionables. Puede introducir fácilmente nuevas capacidades y aumentar o disminuir el uso a medida que pasa el tiempo y cambian sus necesidades.

Cuando potencia su pila de ciberseguridad con una combinación unificada de gestión de vulnerabilidades, protección de endpoints, detección y respuesta de endpoints y protección de aplicaciones en la nube, puede defenderse de un espectro completo de amenazas cibernéticas. Las tecnologías unificadas funcionan juntas como una sola, desde el back-end hasta el front-end, y son fáciles y eficientes de administrar desde un único portal.

Lo que hace que el conjunto unificado de gestión de vulnerabilidades y detección y respuesta de endpoints sea tan poderoso es el conocimiento de la situación que se obtiene. Obtendrá visibilidad basada en el riesgo de las amenazas que enfrenta desde múltiples frentes. Puede ver dónde están las fallas en su arquitectura de seguridad, cuáles son los puntos débiles que el atacante puede aprovechar para ingresar y qué está sucediendo en su entorno de TI.

Cuando incorpora WithSecure™ Elements Collaboration Protection, podrá detectar contenido y actividad maliciosos en sus aplicaciones de colaboración de Microsoft 365 críticas para el negocio. Además de las vulnerabilidades, el correo electrónico sigue siendo uno de los vectores de ataque más explotados por los ciberdelincuentes para acceder a los sistemas de destino. En la era del trabajo híbrido, otras aplicaciones de colaboración como SharePoint también están ganando terreno.

En lugar de soluciones de puntero aisladas, WithSecure™ Elements le brinda los medios para proteger su patrimonio de TI de una manera unificada y eficiente. Las tecnologías inteligentes están impulsadas por IA avanzada y automatización, lo que aligera la carga para usted y su equipo. También puede transferir su gestión de seguridad diaria a nuestros socios certificados y liberar tiempo para centrarse en actividades más estratégicas.

# WithSecure™ Elements: Consolida su ciberseguridad

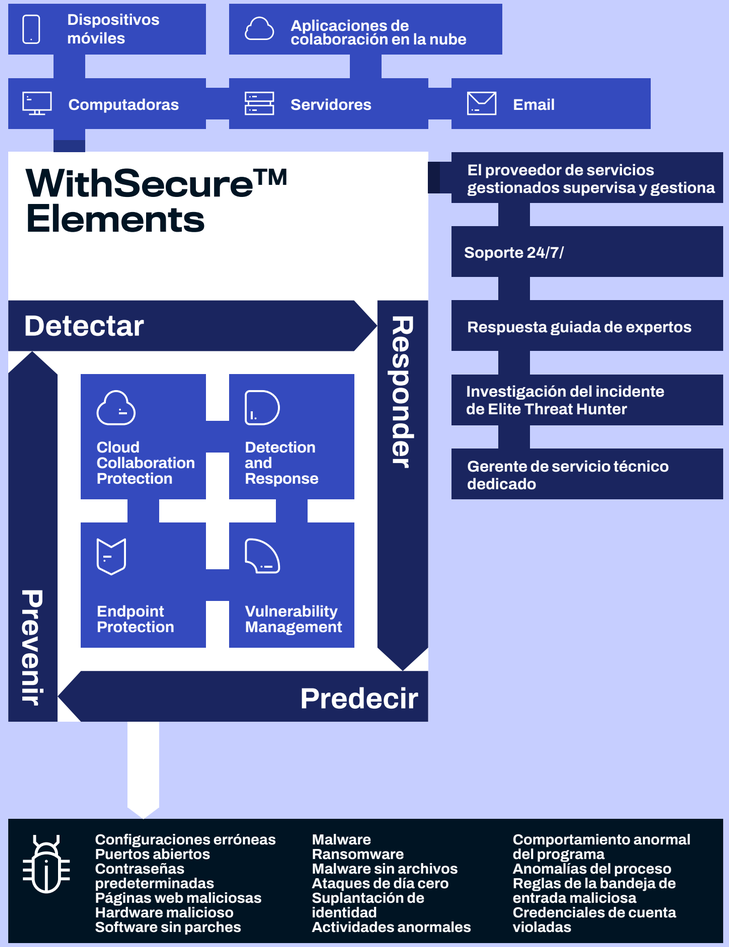
**Unifique sus tecnologías de seguridad**
Los componentes de seguridad funcionan juntos a la perfección sin lagunas utilizando un conjunto de datos compartido y se administran a través de un único centro de seguridad.

**Sea 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 y elección

**Integre fácilmente**
conecte los datos de seguridad fácilmente con sus sistemas SIEM, SOAR, de administración de seguridad, de monitoreo o de informes de terceros

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




---

**Sistemas operativos compatibles:**
Requisitos

**Navegadores compatibles**
Vulnerability Management admite las últimas versiones de los siguientes navegadores:

- Microsoft Internet Explorer
- (fin del soporte el 1 de mayo de 2020)
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari

**Idiomas soportados**
Alemán, español (América Latina), finlandés, francés, inglés, italiano, japonés, polaco, portugués (Brasil) y sueco.

**Instalación en sitio**
Las instalaciones in situ de Vulnerability Management requieren uno de los siguientes sistemas operativos Windows:

- Windows Server 2008 R2 o posterior (instalación completa, no Server Core)

## Reduzca su superficie de ataque encontrando y solucionando vulnerabilidades en su entorno de TI.

Reserva una demostración

# Quiénes somos

WithSecure™, anteriormente F-Secure Business, 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 obtener una seguridad cibernética basada en resultados que proteja y permita sus operaciones. Nuestra protección impulsada por IA protege los puntos finales y la colaboración en la nube, y nuestra detección y respuesta inteligentes están impulsadas por expertos que identifican riesgos comerciales mediante la búsqueda proactiva de amenazas y enfrentando ataques en vivo. Nuestros consultores se asocian con empresas y desafíos tecnológicos para desarrollar resiliencia a través de asesoramiento de seguridad basado en evidencia. Con más de 30 años de experiencia en la creación de tecnología que cumpla con los objetivos comerciales, hemos creado nuestra cartera para crecer con nuestros socios a través de modelos comerciales flexibles.

WithSecure™ Corporation se fundó en 1988 y cotiza en NASDAQ OMX Helsinki Ltd.

WITH secure