Descripción general de la solución

WithSecure™ Elements Endpoint Protection

WithSecure™ Elements – Reduzca el riesgo cibernético, la complejidad y la ineficiencia.

Contenido

Resumen ejecutivo 3
Flexibilidad para construir una ciberseguridad resiliente con WithSecure™ elements 3
1.Descripción general de la solución..... 5
1.1 Paquetes de soluciones..... 6
1.2 Componentes de la solución..... 8
1.3 Implementación de soluciones..... 8
2.Centro de seguridad de elementos..... 9
3.Protección informática..... 11
3.1 Combinando toda la pila de protección de endpoints requerida en una sola 11
3.2 Análisis de amenazas heurísticas y conductuales..... 11
3.3 Inteligencia de amenazas en tiempo real..... 12
3.4 Diseñado específicamente para Mac..... 12
3.5 Protección para puntos finales de Linux..... 13
3.6 Gestión integrada de parches..... 13
3.7 Antimalware multimotor..... 13
3.8 Perfiles basados en la ubicación..... 13
3.9 Flexibilidad al asignar tareas automatizadas..... 13
3.10 Protección web amplia y proactiva..... 14
4.Protección móvil..... 16
4.1 VPN móvil..... 16
4.2 Nube de seguridad..... 16
4.3 Protección de aplicaciones..... 17
4.4 Protección de navegación..... 17
4.5 Navegación más rápida y menor uso de datos..... 17
4.6 TImplementación de mdm de terceros..... 17
5.Protección de servidores..... 18
5.1 Análisis heurístico y conductual de amenazas..... 19
5.2 Inteligencia de amenazas en tiempo real..... 19
5.3 Gestión integrada de parches..... 19
5.4 Antimalware multimotor..... 19
5.5 Protección web proactiva..... 20
5.6 Protección de recursos compartidos del servidor..... 20
5.7 Citrix y servidores de terminales..... 20
5.8 Linux..... 20
5.9 Antimalware multimotor..... 20
5.10 Control de integridad 20
6.Integración con siem/rmm..... 21
7.Servicios profesional. 22
8.Seguridad de datos..... 23

Enero 2023

Resumen ejecutivo

WithSecure™ Elements Endpoint Protection ayuda a las empresas a detener amenazas como el ransomware y a evitar de forma proactiva las filtraciones de datos en sus estaciones de trabajo, portátiles, móviles y servidores. La solución tiene todo lo que las empresas necesitan para la protección de endpoints, incluidas capacidades de administración de parches totalmente integradas para prevenir de manera efectiva ataques que aprovechan las vulnerabilidades del software instalado. Elements Endpoint Protection supera a los productos de la competencia y obtiene constantemente las mejores calificaciones por brindar la mejor protección de la industria.

Flexibilidad para crear ciberseguridad resiliente con WithSecure™ Elements

En el ágil entorno empresarial actual, la única constante es el cambio. WithSecure™ Elements ofrece a las empresas seguridad todo en uno que se adapta a los cambios tanto en el negocio como en el panorama de amenazas, creciendo junto con la organización. Ofrece flexibilidad en los modelos de licencia y en sus tecnologías de seguridad seleccionables. WithSecure™ Elements integra una gama completa de componentes de seguridad cibernética, incluida la gestión de vulnerabilidades, la gestión de parches, la protección de terminales y la detección y respuesta, en un único paquete de software liviano que se administra en una consola de administración unificada basada en la nube. Utilizando la misma consola, las empresas pueden gestionar la seguridad de sus servicios de colaboración de Microsoft 365.

La solución está disponible como un servicio de suscripción totalmente administrado a través de nuestros socios certificados o como una solución en la nube autoadministrada. Los clientes pueden pasar fácilmente de un servicio autogestionado a un servicio totalmente gestionado, de modo que las empresas que luchan por encontrar empleados con habilidades en ciberseguridad puedan mantenerse protegidas en medio del panorama de ataques en constante desarrollo.

WithSecure™ Elements consta de cuatro soluciones que se administran con la misma consola, WithSecure™ Elements Security Center.

WithSecure™ Elements Endpoint Protection: la protección de endpoints impulsada por IA, nativa de la nube, ganadora en múltiples ocasiones de AV-TEST Best Protection de WithSe-cure, se puede implementar de manera fácil y flexible, y administrar la seguridad de todos sus endpoints, manteniendo a su organización cerca de ataques. WithSe-cure™ Elements Endpoint Protection cubre móviles, equipos de escritorio, portátiles y servidores.

WithSecure™ Elements Detección y respuesta de endpoints: obtenga visibilidad total de amenazas avanzadas con nuestra detección y respuesta de endpoints. Con nuestra exclusiva Detección Amplia de Contexto, puede minimizar el ruido de las alertas y concentrarse en los incidentes, y con la respuesta automatizada puede detener eficazmente las infracciones las 24 horas del día. WithSecure™ Elements EndpointDetection and Response cubre computadoras de escritorio, portátiles y servidores.

WithSecure™ Elements Vulnerability Management: descubra y administre vulnerabilidades críticas en su red y activos. Al exponer, priorizar y parchear las vulnerabilidades, puede reducir la superficie de ataque y minimizar los puntos de entrada de los atacantes.

WithSecure™ Elements Collaboration Protection: complemente las capacidades nativas de seguridad del correo electrónico de Microsoft 365 proporcionando seguridad avanzada para evitar ataques a través de correo electrónico y URL. La integración de nube a nube hace que la solución sea fácil de implementar y administrar.

WithSecure™ Elements Endpoint Protection, EndpointDetection and Response y Vulnerability Management están empaquetados en un único paquete de software actualizado automáticamente, lo que le ahorra tiempo y dinero en la implementación y administración de software.

Beneficios de las soluciones integradas

La solución modular WithSecure™ Elements se adapta a las necesidades cambiantes de su empresa. La seguridad cibernética unificada significa licencias más sencillas, menos tareas de gestión de seguridad y más productividad sin sacrificar la postura de seguridad cibernética de su empresa. La consola basada en la nube, WithSecure™ Elements Security Center, proporciona visibilidad, información y administración centralizadas en todos los puntos finales y servicios en la nube. Está completamente administrado por uno de nuestros proveedores de servicios administrados certificados o autoadministrado con soporte bajo demanda de WithSecure™ para casos difíciles. El Centro de seguridad proporciona una vista única del estado de seguridad que combina Endpoint Protection, Endpoint Protection and Response, Vulnerability Management y Microsoft 365.

Todas las soluciones de endpoint (Elements Endpoint Protection, EndpointDetection and Response y Vulnerability Management) utilizan un único agente de software que debe implementarse solo una vez. Las soluciones complementarias se pueden activar posteriormente sin tener que implementar soluciones adicionales. WithSecure™ Elements Collaboration Protection es una solución basada en la nube que no requiere instalaciones en los puntos finales de la empresa.

Además de los beneficios de implementación y administración, las soluciones WithSecure™ Elements están diseñadas para trabajar juntas maximizando los beneficios de seguridad para la empresa.

Al combinar alertas y eventos de seguridad, las capacidades XDR de WithSecure™ Elements pueden proporcionar seguridad integral rompiendo los silos de soluciones desconectadas.

WithSecure™ Elements Endpoint Protection es la opción preferida por las empresas que desean:

- Cobertura de servicios y terminales más amplia que la que pueden ofrecer las soluciones comunes en el mercado, a un costo total de propiedad (TCO) mucho más atractivo.
- Logre un excelente nivel de protección con requisitos mínimos de recursos con la opción de subcontratar completamente la gestión de la solución a un proveedor de servicios certificado.
- Una forma sencilla y escalable de proporcionar visibilidad y protección para múltiples sitios geográficamente dispersos desde una sola ubicación
- Evitar invertir tiempo y recursos en el mantenimiento de entornos de servidores locales.

Al fusionar la protección de varios endpoints y herramientas de seguridad de valor agregado en una solución unificada, Elements Endpoint Protection ofrece:

• Cobertura y capacidades de seguridad más amplias que la mayoría de las soluciones de seguridad para endpoints
• Gestión unificada y optimizada basada en la nube que ahorra tiempo y recursos de gestión y mantenimiento de la seguridad, reduciendo aún más el TCO.

La solución está diseñada para entregarse como un servicio basado en la nube; ya sea como un servicio autoadministrado, servicio administrado por un proveedor de servicios certificado, con opción de integrarlo con sistemas de terceros. Nuestra capacidad para brindar una protección mejor y más consistente que nuestros competidores se demuestra año tras año mediante pruebas realizadas por expertos y analistas independientes de la industria.

WithSecure™ ha demostrado su consistencia en pruebas independientes al ser el único proveedor con prestigiosos premios anuales AV-TEST a la 'Mejor protección' para productos comerciales en 6 años desde su creación. AV-Test realiza pruebas comparativas continuamente durante todo el año, por lo que para alcanzar este preciado premio es necesario mostrar consistentemente buenos resultados en las pruebas de protección.

Para cumplir con estos estándares exigentes, la solución utiliza un enfoque de seguridad de múltiples capas y aprovecha varias tecnologías modernas, como análisis de amenazas heurístico y de comportamiento, e inteligencia de amenazas en tiempo real proporcionada a través de WithSecure™ Security Cloud.

Esto garantiza que esté a la vanguardia de la seguridad.

1. Descripción general de la solución

Las empresas enfrentan desafíos para minimizar el riesgo comercial provocado por amenazas cibernéticas como el ransomware. WithSecure™ Elements Endpoint Protection está diseñado desde cero para resolver las desafiantes necesidades de seguridad empresarial con una mínima sobrecarga de mantenimiento y gestión. Ofrece la mejor protección galardonada para computadoras Windows y Mac, dispositivos iOS y Android y una variedad de plataformas de servidores. Con administración de parches integrada, protección en capas y análisis heurístico y de comportamiento avanzado, Elements Endpoint Protection detiene las ciberamenazas del mañana, hoy.

WithSecure™ Elements Endpoint Protection ofrece:

- **La mejor protección del sector** mejora la continuidad del negocio y ahorra tiempo en la recuperación de incidentes.
- **Minimiza proactivamente el riesgo empresarial** de infracciones cibernéticas con una gestión de parches totalmente integrada
- **La solución nativa de la nube** ahorra tiempo en la implementación, administración y monitoreo de la seguridad

La solución WithSecure™ Elements Endpoint Protection también está disponible como un servicio totalmente administrado. Los proveedores de servicios certificados de WithSecure™ pueden utilizar la versión SaaS o administrada por socios de la solución para aprovechar muchas características únicas del proveedor de servicios, como el panel de control de varias empresas, la generación de informes y la gestión de suscripciones. La versión SaaS de la solución permite a los proveedores de servicios utilizar modelos comerciales flexibles, p. Facturación basada en el uso para todos los productos WithSecure™ Elements.

1.1 Paquetes de soluciones

La protección de servidores y computadoras de la solución Elements Endpoint Protection para Windows y Mac está disponible como paquetes estándar y premium. Las características estándar incluyen antimalware avanzado, administración de parches y muchas otras capacidades de seguridad para terminales. Las funciones premium añaden una mejor protección contra ransomware y control de aplicaciones. Ambos paquetes de endpoints se pueden complementar con las soluciones Elements EndpointDetection and Response y Elements Vulnerability Management. Las funciones de detección y respuesta brindan visibilidad, detección y respuesta automatizadas mejoradas ante amenazas e infracciones avanzadas. La gestión de vulnerabilidades ayuda a descubrir y gestionar vulnerabilidades críticas en los puntos finales. Además, WithSecure™ Elements Collaboration Protection se puede implementar mediante la integración de nube a nube sin necesidad de instalar middleware o software en los puntos finales.

WithSecure™ Elements

	Endpoint Protection standard	Endpoint Protection premium	Detection and Response	Vulnerability Management	Collaboration Protection
Gestión avanzada de parches y antimalware	✓	✓			
Protección anti-ransomware adicional con DataGuard y control de aplicaciones		✓			
Protección avanzada contra amenazas			✓		
Gestión y priorización de vulnerabilidades.				✓	
Seguridad avanzada de colaboración y correo electrónico basada en la nube para Microsoft 365					✓

Los diferentes paquetes de funciones de protección se pueden activar sin tener que reinstalar el software del cliente. Más información sobre WithSecure™ Elements.

Actualizador de software
Gestión automatizada de parches para actualizar Microsoft y Mac y más de 2500 aplicaciones de software de terceros.

DeepGuard
Un motor antimalware heurístico inteligente que ofrece capacidad de detección de día 0. Lea el documento técnico de WithSecure™ DeepGuard.

Control de contenido web
Mejore la seguridad y la productividad con acceso controlado a sitios web. Evite el acceso a sitios web según categorías y haga cumplir su política corporativa.

Control de conexión
Active seguridad adicional para transacciones sensibles como la banca en línea.

Protección en tiempo real
WithSecure™ Security Cloud protege contra nuevo malware, ya que utiliza detalles de amenazas vistos por otras máquinas protegidas, lo que hace que las respuestas sean mucho más eficientes.

Antimalware multimotor
Proporcione una protección inigualable con antimalware multimotor altamente avanzado.

Firewall
Reglas adicionales y funcionalidad de administración integradas con Windows Firewall.

Protección de navegación
Evita de forma proactiva que los empleados accedan a sitios dañinos que contengan enlaces o contenido maliciosos.

Control del dispositivo
Device Control evita que las amenazas entren en su sistema a través de dispositivos de hardware como memorias USB, unidades de CD-ROM y cámaras web. Esto también evita la fuga de datos, permitiendo, por ejemplo, el acceso de sólo lectura.

DataGuard
Proporciona protección adicional contra ransomware y evita la destrucción y manipulación de datos.

Control de aplicaciones
Bloquea la ejecución de aplicaciones y scripts de acuerdo con las reglas creadas por nuestros evaluadores de penetración o según lo definido por el administrador. Además, el Control de aplicaciones se puede utilizar para bloquear la carga de DLL u otros archivos para mayor seguridad.

XFENCE
Capacidad de seguridad única para proteger Mac contra malware, troyanos, puertas traseras, aplicaciones que se comportan mal y otras amenazas al evitar que las aplicaciones accedan a archivos y recursos del sistema sin permisos explícitos.

Cifrado de terminales
Supervise y administre el estado del cifrado de discos de sus computadoras con Windows. Puede activar y desactivar el cifrado Bitlocker y obtener claves de recuperación directamente desde WithSecure™ Elements Security Center.

Control de brotes
Outbreak Control brinda la capacidad de cambiar automáticamente los perfiles de EPP para que sean más restringidos, si tienen detecciones de EDR abiertas de gravedad media, alta o crítica. Una vez que se resuelve el incidente, el endpoint vuelve a su perfil original.

1.2 Componentes de la solución

La solución se compone de cuatro componentes principales, cada uno de los cuales se describe en este documento:

1. **Elements Security Center** como portal de gestión basado en la nube
2. **Computer Protection** como clientes de seguridad dedicados para estaciones de trabajo (Windows, Mac, Linux*)
3. **Protección Móvil** para dispositivos móviles (iOS, Android)
4. **Protección de servidores** para una variedad de plataformas de servidores (Windows, Citrix, Linux)

1.3 Implementación de la solución

Los clientes de seguridad de endpoints se pueden implementar por correo electrónico, instalación local, secuencias de comandos por lotes, sistemas de administración empresarial (SolarWinds, Kaseya, Datto) o con un paquete MSI a través de herramientas de instalación remota basadas en dominio. De manera similar, los clientes Mac se implementan como paquetes mediante el instalador de macOS o las herramientas de administración de dispositivos móviles y se pueden configurar con pasos de implementación adicionales en paquetes firmados personalizados.

Para implementaciones normales, todas las implementaciones de clientes de seguridad de endpoints se pueden iniciar desde el portal a través de un flujo de correo electrónico.

La clave de suscripción se incluye automáticamente en el enlace o instalador, de modo que el usuario final solo necesita hacer clic en el enlace para que el proceso de instalación comience automáticamente.

** Las condiciones se aplican. Por favor contacte a su representante de ventas.*

Para entornos más grandes, puede crear un paquete MSI que se puede implementar con sus propias herramientas de instalación remota o con las nuestras. El cliente de Windows también contiene indicadores de programa integrados, que se pueden utilizar para automatizar la implementación del cliente mediante secuencias de comandos por lotes.

Siempre que el cliente Windows se implementa en sistemas con una solución de seguridad conflictiva, nuestra función de actualización lateral lo detecta y lo desinstala automáticamente antes de continuar con la instalación del software WithSecure™. Esto garantiza una transición mucho más fluida y rápida de un proveedor a otro.

Cuando se agrega una nueva computadora a Elements Endpoint Protection, se puede asignar automáticamente una configuración predeterminada (perfil) en función de su ubicación en una jerarquía de Active Directory. Esto agiliza el proceso de implementación y reduce los riesgos de una mala configuración.

Las funciones de protección móvil se implementan comúnmente mediante el uso de una administración de dispositivos móviles (MDM) de terceros disponible con una suscripción que admite el uso de soluciones MDM externas.

Las capacidades de administración de parches están completamente integradas en los clientes de estaciones de trabajo y servidores de Windows y se pueden controlar a través del portal de administración. Como solución alojada, no es necesario instalar agentes, servidores o consolas de administración independientes, a diferencia de las soluciones tradicionales de administración de parches.

WithSecure™ Elements Connector es proporcionado por WithSecure™ para minimizar el uso de ancho de banda al descargar actualizaciones a los clientes de Computer Protection. Este proxy almacena en caché las actualizaciones de la base de datos de firmas de malware, así como las actualizaciones de software del propio cliente Computer Protection y las actualizaciones del software de administración de parches, y además puede usarse como interfaz entre WithSecure™ Elements y sus sistemas SIEM.

El software cliente de Endpoint Protection actualiza las bases de datos de firmas de malware y el propio software cliente automáticamente sin que el administrador tenga que preocuparse por las actualizaciones o mejoras manualmente.

Los socios de WithSecure™ pueden personalizar tanto el software cliente de protección de endpoints como Elements Security Center con su logotipo y enlace de soporte.

2. Centro de seguridad de elementos

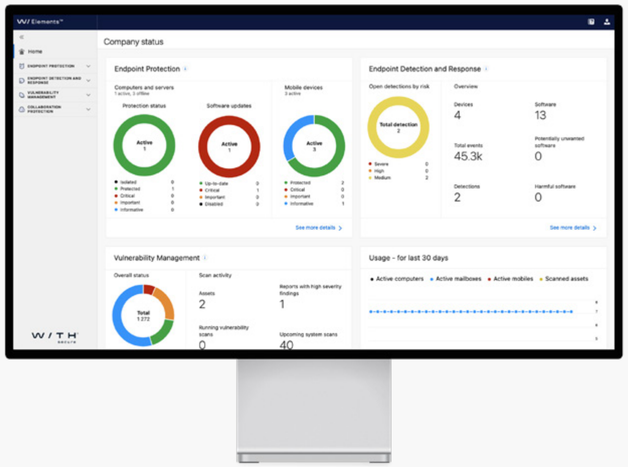
WithSecure™ Elements Endpoint Protection facilita la implementación, administración y monitoreo de la seguridad de sus terminales desde una consola única e intuitiva. Le brinda una excelente visibilidad de todos sus dispositivos.

El Security Center fue diseñado desde cero para simplificar y acelerar la gestión de la seguridad en entornos exigentes, de múltiples dispositivos y de múltiples sitios. A continuación se muestran algunos ejemplos de cómo la solución reduce considerablemente la cantidad de tiempo y recursos necesarios para el mantenimiento y la gestión de la seguridad:

- Los clientes finales reciben automáticamente actualizaciones de clientes, de seguridad y de bases de datos, minimizando el tiempo necesario para las actualizaciones y el mantenimiento.
- Al consolidar la gestión de seguridad de varios puntos finales y herramientas en un solo portal, la gestión general se optimiza considerablemente, ahorrando tiempo.
- La gestión de parches se puede configurar para implementar automáticamente los parches de seguridad faltantes tan pronto como estén disponibles, ahorrando tiempo en las actualizaciones manuales de software.
- Como servicio alojado, no es necesario instalar ni mantener hardware ni software de servidor; todo lo que necesita es un navegador.
- El portal ha sido diseñado por un equipo dedicado a la experiencia del usuario para utilizar los recorridos de usuario más óptimos, lo que aumenta considerablemente la eficiencia del usuario.

La comunicación consola-endpoint funciona en tiempo real. Esto permite a los administradores de TI gestionar y monitorear la seguridad del entorno sin interrupciones ni retrasos causados por los intervalos de sondeo.

En esencia, permite a los administradores de TI configurar, implementar y validar cambios de una sola vez. Y si hay un incidente de seguridad que debe resolverse "ahora mismo", puede remediarlo e implementar una solución de inmediato.



Puede crear y personalizar políticas de seguridad individuales. (perfiles) y asignarlos individualmente o en grupos a computadoras y servidores mediante etiquetas. Todas las configuraciones y políticas se pueden aplicar hasta el nivel individual si es necesario para que los usuarios finales no puedan cambiarlas. Se pueden crear políticas, p. por grupo de Active Directory y asignar las políticas automáticamente a los dispositivos conectados al grupo.

El portal de administración le brinda una descripción completa del estado de seguridad de todo su entorno. Esto incluye posibles vulnerabilidades de software, actualizaciones de seguridad faltantes y el estado de las funciones de seguridad, como el escaneo en tiempo real y el firewall. Al utilizar Security Events, los administradores de TI pueden ver fácilmente todas las alertas en una ubicación central.

Por ejemplo, puede realizar un seguimiento del número de infecciones bloqueadas y prestar más atención a los dispositivos que son más atacados. Puede configurar alertas automáticas por correo electrónico para que los parámetros de infección específicos llamen su atención primero. Si necesita más información sobre alguna infección en particular, puede obtenerla directamente de nuestra base de datos de seguridad.

El portal de gestión ofrece una amplia gama de informes gráficos en un formato intuitivo, lo que hace que los datos sean más fáciles y rápidos de digerir y comprender, y que su lectura sea más atractiva para las partes interesadas. Los detalles de seguridad del dispositivo también se pueden exportar como archivos CSV si es necesario.

3. Protección informática

La protección de terminales para computadoras constituye la piedra angular de cualquier entorno seguro. Y en el panorama de seguridad actual, es vital garantizar que la protección vaya mucho más allá del antimalware tradicional. Con WithSecure™ Elements Endpoint Protection, es sencillo ofrecer seguridad potente y amigable con los recursos para computadoras Windows, Mac y Linux.

3.1 Combinar toda la pila de protección de endpoints requerida en una

Las modernas suites de protección de endpoints emplean un enfoque de múltiples capas para brindar seguridad. Tecnologías como el filtrado y escaneo de redes, el análisis de comportamiento y el filtrado de URL aumentan los componentes tradicionales de escaneo de archivos. Estas diferentes funciones de protección están integradas en WithSecure™ Ultralight en un diseño de varias capas, de modo que si una amenaza escapa de una capa, todavía hay otra capa que puede atraparla. Y a medida que cambia el panorama de amenazas, es posible que se eliminen algunas capas o se agreguen otras nuevas tanto en los puntos finales como en la nube.

Ultralight combina todas las tecnologías presentes en la pila completa de protección de terminales de WithSe-cure en un solo paquete. Consta de una serie de controladores, motores y servicios del sistema que proporcionan mecanismos para proteger tanto un dispositivo como a sus usuarios.

Ultralight proporciona funciones antivirus tradicionales, como escaneo de archivos en tiempo real y escaneo de red. Además, incluye tecnologías de protección proactivas y modernas cuyo objetivo es detener los exploits de día cero y adelantarse a nuevos ataques. Security Cloud de WithSecure proporciona a los componentes Ultralight información en tiempo real a medida que cambia el panorama de amenazas.

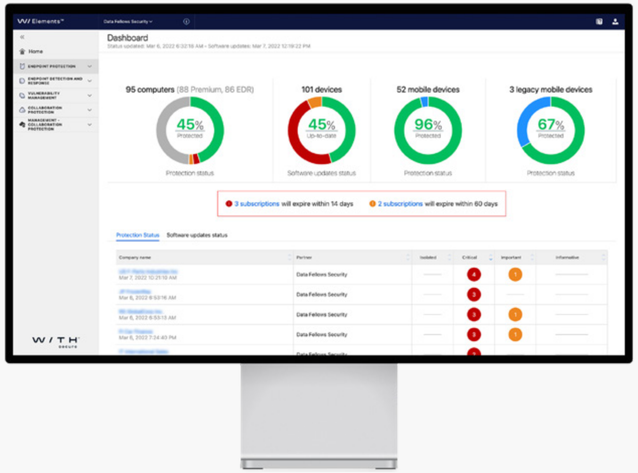
Para obtener más información sobre las tecnologías de protección integrada realizadas por Ultralight, consulte el documento técnico.

3.2 Análisis de amenazas heurísticas y conductuales

El análisis de amenazas heurístico y de comportamiento, realizado por DeepGuard, es fundamental para identificar y bloquear el malware más sofisticado que prevalece en la actualidad. DeepGuard proporciona protección inmediata y proactiva en el host contra amenazas nuevas y emergentes al centrarse en el comportamiento de las aplicaciones maliciosas en lugar de mediante la identificación estática de amenazas específicas y conocidas.

Este cambio de enfoque le permite identificar y bloquear malware nunca antes visto basándose únicamente en su comportamiento, brindando protección de manera clara hasta que los investigadores de seguridad puedan analizar y emitir una detección para esa amenaza específica.

Al comunicarse con Security Cloud de WithSecure, Deep-Guard también puede utilizar la información más reciente sobre reputación y prevalencia disponible para cualquier objeto encontrado previamente para ajustar sus evaluaciones de seguridad,



reduciendo el riesgo de falsos positivos o análisis redundantes que pueden interferir con el usuario. experiencia.

El análisis de comportamiento en el host también se extiende a los ataques de interceptación que intentan explotar vulnerabilidades en programas populares para instalar malware en la máquina. Deep-Guard es capaz de identificar y bloquear rutinas características de un intento de explotación, evitando la explotación y, a su vez, la infección. La interceptación de exploits protege a los usuarios de daños incluso cuando hay programas vulnerables presentes en su máquina.

Para obtener más información sobre el análisis heurístico y de comportamiento de amenazas realizado por DeepGuard, consulte el documento técnico.

3.3 Inteligencia sobre amenazas en tiempo real

El cliente de seguridad utiliza inteligencia sobre amenazas en tiempo real proporcionada por Security Cloud de WithSecure, lo que garantiza que todas las amenazas nuevas o emergentes se identifiquen, analicen y prevengan en cuestión de minutos.

Un servicio de análisis de amenazas basado en la nube ofrece muchos beneficios sobre los enfoques tradicionales. WithSecure™ recopila inteligencia sobre amenazas de decenas de millones de nodos de clientes, generando una imagen en tiempo real de la situación de amenazas global.

Por ejemplo, si el análisis de amenazas heurístico y de comportamiento identifica un ataque de día cero en otro punto final en el otro lado del mundo, la información se comparte con todos los dispositivos protegidos a través de Security Cloud, lo que hace que el ataque avanzado sea inofensivo apenas unos minutos después de la detección inicial. .

Para obtener más información sobre las funciones y beneficios de Security Cloud de WithSe-cure, consulte nuestro documento técnico.

3.4 Diseñado específicamente para macOS

WithSecure™ Computer Protection para macOS incluye XFENCE, una capacidad de seguridad única para Mac. El producto aprovecha las capacidades de seguridad modernas de macOS mejorando la protección contra malware, troyanos, puertas traseras, aplicaciones que se comportan mal y otras amenazas sin sacrificar la usabilidad y el rendimiento. La poderosa protección XFENCE evita que procesos erróneos, ransomware y otro malware accedan a sus archivos y recursos del sistema sin un permiso explícito.

WithSecure™ Computer Protection para macOS aprovecha el análisis avanzado basado en reglas para monitorear aplicaciones que intentan acceder a archivos confidenciales y recursos del sistema, mejorado por la inteligencia de amenazas proporcionada por Security Cloud para minimizar los falsos positivos y la interacción del usuario a través de mensajes de permiso/no permitido. .

Además, WithSecure™ Computer Protection para macOS proporciona un firewall en la capa de aplicación que puede configurar y controlar el acceso a la red a nivel de aplicación. Se puede utilizar para aislar hosts, permitir el acceso a la red solo a aplicaciones registradas confiables y incluir aplicaciones en la lista negra o blanca por ID de paquete.

WithSecure™ Computer Protection para macOS viene con herramientas de administración para facilitar la implementación y administración de los clientes Mac.

3.5 Protección para puntos finales de Linux

WithSecure™ Elements Endpoint Protection incluye protección para Linux en WithSecure™ Server Protection. El producto también se puede utilizar para proteger dispositivos terminales.*

3.6 Gestión integrada de parches

Los puntos finales de Windows y Mac incluyen una función de administración de parches automatizada que está completamente integrada con los clientes. No es necesario instalar agentes, servidores de administración o consolas independientes. Funciona escaneando en busca de actualizaciones faltantes, creando un informe de vulnerabilidad basado en los parches faltantes y luego descargándolos e implementándolos automáticamente. También puede optar por instalar las actualizaciones manualmente si es necesario.

Los parches de seguridad incluyen actualizaciones de Microsoft y Mac y más de 2500 aplicaciones de terceros como Flash, Java, OpenOffice y otras que comúnmente sirven como vectores de ataque debido a su popularidad y mayor número de vulnerabilidades.

Los administradores pueden definir exclusiones detalladas para el modo automático según los nombres del software o los ID de los boletines. Algunas actualizaciones están excluidas por definición, como los Service Packs. Los administradores también pueden definir de manera flexible el día y la hora en que se deben realizar las instalaciones, así como también cómo se fuerzan los reinicios y el tiempo de gracia antes de forzar un reinicio después de la instalación.

> La gestión de parches es un componente de seguridad crítico. Es la primera capa de protección cuando el contenido malicioso llega a los puntos finales y puede prevenir hasta el 80 % de los ataques simplemente instalando actualizaciones de seguridad de software tan pronto como estén disponibles.

3.7 Antimalware multimotor

Nuestro componente informático utiliza una plataforma de seguridad patentada de múltiples motores para detectar y prevenir malware. Ofrece una protección superior en comparación con las tecnologías tradicionales basadas en firmas:

- Detecta una gama más amplia de características, patrones y tendencias maliciosas, lo que permite detecciones más confiables y precisas, incluso para variantes de malware nunca antes vistas.
- Al utilizar búsquedas en tiempo real desde Security Cloud de WithSecure, puede reaccionar más rápido ante amenazas nuevas y emergentes, además de garantizar una huella pequeña.
- La emulación permite la detección de malware que utiliza técnicas de ofuscación y ofrece otra capa de seguridad antes de ejecutar un archivo.

3.8 Perfiles basados en la ubicación

WithSecure™ Elements Endpoint Protection se puede configurar para activar diferentes configuraciones según la ubicación del punto final. Como ejemplo, el administrador puede configurar reglas y ubicaciones de red de modo que cuando un dispositivo esté en casa, la administración de parches y el firewall estén activados, pero cuando esté en la oficina, tanto la administración de parches como el firewall estén desactivados.

3.9 Flexibilidad mediante la asignación de tareas automatizadas

WithSecure™ Elements Endpoint Protection se puede configurar para ejecutar determinadas tareas automatizadas de forma muy granular. Por ejemplo, las actualizaciones de productos se pueden configurar para que se ejecuten en un momento específico, instalar inmediatamente las actualizaciones críticas y de seguridad faltantes, buscar actualizaciones de seguridad faltantes todos los días y ejecutar un análisis completo del sistema en busca de malware todos los días de la semana. Al utilizar las tareas automatizadas, puede configurar la protección de endpoints para que se ajuste a las necesidades de seguridad de su empresa con un impacto mínimo en el rendimiento.

* Las condiciones se aplican. Por favor contacte a su representante de ventas.

3.10 Protección web amplia y proactiva

Además, la solución ofrece una protección web amplia y proactiva, lo que garantiza que el vector de ataque más explotado esté bien defendido.

- Previene de forma proactiva el acceso a sitios maliciosos y de phishing incluso antes de acceder a ellos (por ejemplo, en la búsqueda de Google y al hacer clic en un enlace web). Esto es especialmente eficaz, ya que la intervención temprana reduce en gran medida la exposición general a contenidos maliciosos y, por tanto, a ataques.
- Previene la explotación de contenido activo como Java y Flash, que se utilizan en la gran mayoría de los ataques en línea. Estos componentes se bloquean automáticamente en sitios desconocidos y sospechosos en función de sus datos de reputación, con la opción de establecer exclusiones.
- La solución también se puede utilizar para restringir el uso inapropiado de la web, negando o permitiendo de manera granular el acceso a destinos no relacionados con el trabajo, como sitios de redes sociales y sitios para adultos, para maximizar la eficiencia y evitar sitios maliciosos.
- Después de las capas iniciales de protección web, el contenido del tráfico web HTTP también se somete a análisis para proporcionar protección adicional contra el malware, antes de que entre en contacto con el propio punto final.
- Los administradores de TI también pueden designar actividades web críticas para el negocio que utilizan HTTPS (como intranets o servicios sensibles en la nube, por ejemplo CRM) para utilizar una capa de seguridad adicional. Cuando está activo, cierra todas las conexiones de red que no son de confianza, evitando ataques y exfiltración de datos de los servicios durante la sesión.

Las características de seguridad varían según el sistema operativo elegido. A continuación se muestra una descripción general de la comparación de funciones entre Windows, macOS y Linux.

	Windows	macOS	Linux**
Security			
Anti-malware	**Sí**	**Sí**	**Sí**
DeepGuard	**Sí**	No	No
DataGuard	**Sí**	**Sí***	No
Security cloud	**Sí**	**Sí**	**Sí**
Patch management	**Sí**	**Sí**	No
Application control	**Sí**	No	No
Browsing protection	**Sí**	**Sí**	No

	Windows	macOS	Linux**
Security			
Web traffic scanning	**Sí**	No	No
Web content control	**Sí**	**Sí**	No
Content type filtering	**Sí**	No	No
Connection control	**Sí**	**Sí**	No
Firewall	**Sí**	**Sí**	No
Integrity checking	No	No	**Sí**
Endpoint Encryption	**Sí**	No	No

* art of the functionality provided by XFENCE

** Conditions apply. Please contact your sales representative.

4. Protección móvil

Mantener el control sobre los dispositivos móviles es un aspecto fundamental de la ciberseguridad moderna. Con Elements Mobile Protection, los administradores de TI tienen una manera fácil de proteger y controlar los dispositivos móviles, tanto Android como iOS.

El componente entregado por WithSecure™ Elements Mobile Protection incluye todo lo que se necesita para una protección móvil excepcional en un solo paquete: VPN personal, seguridad Wi-Fi y protección web y de aplicaciones proactivas (Android).

El cliente móvil también está diseñado para complementarse y desplegarse a través de soluciones MDM de terceros.

4.1 VPN móvil

La VPN móvil cifra automáticamente el tráfico entre su dispositivo móvil y una red seleccionada

Nodo de servicio WithSecure™, que permite a sus empleados utilizar de forma segura las redes móviles y Wi-Fi públicas.

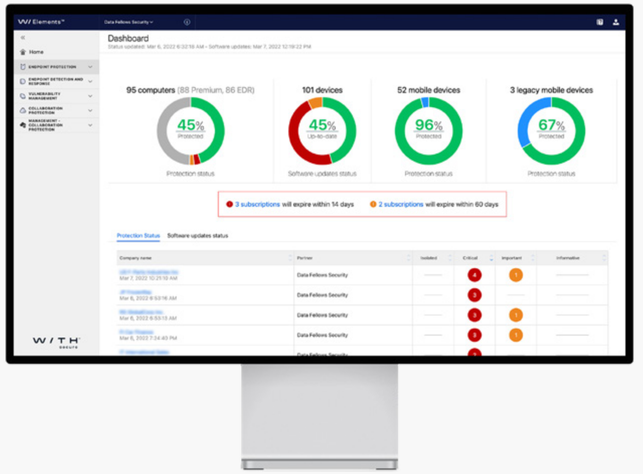
Evita la interceptación de correos electrónicos, sesiones de navegador y uso de servicios en línea, además de proporcionar una capa de seguridad adicional sobre las conexiones HTTPS. También le permite cambiar su ubicación virtual, ocultar su dirección IP y acceder a servicios locales cuando esté en el extranjero.

4.2 Nube de seguridad

El cliente de seguridad utiliza inteligencia sobre amenazas en tiempo real proporcionada por Security Cloud de WithSecure, lo que garantiza que todas las amenazas nuevas o emergentes se identifiquen, analicen y prevengan en cuestión de minutos.

Un servicio de análisis de amenazas basado en la nube ofrece muchos beneficios sobre los enfoques tradicionales. Recopilamos inteligencia sobre amenazas de decenas de millones de nodos de clientes, creando una imagen en tiempo real de la situación de amenazas global. Por ejemplo, cuando se descarga un APK o un archivo, se escanea y, además, se verifica su reputación en Security Cloud. Se evita la ejecución de archivos maliciosos y se cargan archivos o aplicaciones desconocidos para un análisis más profundo. Los resultados del análisis benefician a todos los usuarios, por ejemplo, al minimizar los falsos positivos y hacer que los nuevos ataques sean inofensivos en cuestión de minutos.

Para obtener más información sobre las funciones y beneficios de Security Cloud de WithSecure, consulte nuestro documento técnico.



4.3 Protección de aplicaciones

Cuando la conexión VPN está activa, los dispositivos móviles se protegen automáticamente contra malware y contenido malicioso. Los nodos de servicio WithSecure™ escanean el tráfico a nivel de red, utilizando toda la gama de análisis de seguridad disponibles. Esto nos permite ofrecer una mejor seguridad que las soluciones de seguridad móviles tradicionales:

- La seguridad no se ve obstaculizada por los recursos limitados de los dispositivos móviles
- Los procesos que consumen muchos recursos no afectan el rendimiento del dispositivo ni la duración de la batería.
- El escaneo a nivel de red previene el contacto con contenido malicioso en primer lugar

Para los dispositivos Android, la seguridad se mejora aún más con el escaneo local, incluidas verificaciones de reputación en tiempo real desde WithSecure™ Security Cloud, incluso cuando la VPN no está conectada.

4.4 Protección de navegación

La protección de la navegación es una capa de seguridad clave que evita de forma proactiva que los usuarios finales visiten sitios maliciosos. Esto es particularmente eficaz, ya que la intervención temprana reduce en gran medida la exposición general a contenidos maliciosos y, por tanto, a ataques.

Por ejemplo, la protección de navegación evita que se engañe a los usuarios finales para que accedan a sitios de phishing aparentemente legítimos, accedan a sitios maliciosos a través de un enlace de correo electrónico o se infecten a través de anuncios maliciosos de terceros en sitios que de otro modo serían legítimos.

4.5 Navegación más rápida y menor uso de datos

El componente está diseñado para tener un impacto mínimo en el rendimiento del móvil y la duración de la batería. De hecho, al utilizar la compresión del tráfico a través de VPN y evitar el seguimiento y la publicidad en línea con Anti-Tracking, se aumenta la velocidad de navegación.

4.6 Implementación de MDM de terceros

El cliente móvil también está diseñado para complementar e implementar a través de soluciones de administración de dispositivos móviles (MDM) de terceros, como AirWatch, MobileIron, Intune y MaaS360.

Al utilizar un componente de seguridad dedicado además de las capacidades básicas proporcionadas por la solución MDM, los administradores de TI pueden aumentar significativamente la seguridad contra malware, robo de datos e intentos de phishing dirigidos a dispositivos móviles.

5. Protección del servidor

Los servidores son fundamentales para la comunicación, la colaboración y el almacenamiento de datos de una empresa. Elements Endpoint Protection proporciona seguridad a los servidores y les permite funcionar con el máximo rendimiento. La solución proporciona seguridad para servidores Windows, Citrix y Linux.

A continuación se muestra una descripción general de las capacidades principales para diferentes plataformas de servidor:

	Windows	Citrix	Linux
Seguridad central			
Anti-malware	**Sí**	**Sí**	**Sí**
DeepGuard	**Sí**	**Sí**	No
Nube de seguridad	**Sí**	**Sí**	**Yes**
Gestión de parches	**Sí**	**Sí***	No
Protección de navegación	**Sí**	**Sí**	No
Escaneo de tráfico web	**Sí**	**Sí**	No
Firewall	**Sí**	No	No
Control de integridad	No	No	**Sí**
Gestión remota a través del portal			
Gestion de seguridad	**Sí**	**Sí**	**Sí**
Monitoreo de seguridad	**Sí**	**Si**	**Sí**

5.1 Análisis de amenazas heurísticas y conductuales

El análisis de amenazas heurístico y de comportamiento, realizado por DeepGuard, es fundamental para identificar y bloquear el malware más sofisticado que prevalece en la actualidad. DeepGuard proporciona protección inmediata y proactiva en el host contra amenazas nuevas y emergentes al centrarse en el comportamiento de las aplicaciones maliciosas en lugar de mediante la identificación estática de amenazas específicas y conocidas. Este cambio de enfoque le permite identificar y bloquear malware nunca antes visto basándose únicamente en el comportamiento, brindando protección de manera clara hasta que los investigadores de seguridad puedan analizar y emitir una detección para esa amenaza específica.

Al comunicarse con Security Cloud de WithSecure, Deep-Guard también puede utilizar la información más reciente sobre reputación y prevalencia disponible para cualquier objeto encontrado previamente para ajustar sus evaluaciones de seguridad, reduciendo el riesgo de falsos positivos o análisis redundantes que pueden interferir con el usuario. experiencia. El análisis de comportamiento en el host también se extiende a la interceptación de ataques que intentan explotar vulnerabilidades en programas populares para instalar malware en la máquina. DeepGuard es capaz de identificar y bloquear rutinas características de un intento de explotación, evitando la explotación y, a su vez, la infección. La interceptación de exploits protege a los usuarios de daños incluso cuando hay programas vulnerables presentes en su máquina.

Para obtener más información sobre el análisis heurístico y de comportamiento de amenazas realizado por DeepGuard, consulte el documento técnico.

5.2 Inteligencia sobre amenazas en tiempo real

El cliente de seguridad utiliza inteligencia sobre amenazas en tiempo real proporcionada por Security Cloud de WithSecure, lo que garantiza que todas las nuevas
o amenazas emergentes se identifican, analizan y previenen en cuestión de minutos.

Un servicio de análisis de amenazas basado en la nube ofrece muchos beneficios sobre los enfoques tradicionales. WithSecure™ recopila inteligencia sobre amenazas de decenas de millones de nodos de clientes, generando una imagen en tiempo real de la situación de amenazas global. Por ejemplo, si el análisis heurístico y de comportamiento de amenazas identifica un ataque de día cero en otro punto final en el otro lado del mundo, la información se comparte con todos los dispositivos protegidos a través de Security Cloud, lo que hace que el ataque avanzado sea inofensivo apenas unos minutos después del inicio. detección.

Para obtener más información sobre las funciones y beneficios de Security Cloud de WithSe-cure, consulte nuestro documento técnico.

5.3 Gestión integrada de parches

El componente incluye una función de administración automatizada de parches que está completamente integrada con los clientes del servidor Windows. No es necesario instalar agentes, servidores de administración o consolas independientes. Funciona escaneando en busca de actualizaciones faltantes, creando un informe de vulnerabilidad basado en los parches faltantes y luego descargándolos e implementándolos automáticamente.

También puede optar por instalar las actualizaciones manualmente si es necesario. Los parches de seguridad incluyen actualizaciones de Microsoft y más de 2500 aplicaciones de terceros, como Flash, OpenOffice y otras, que comúnmente sirven como vectores de ataque debido a su popularidad y gran cantidad de vulnerabilidades.

5.4 Antimalware multimotor

Nuestro componente informático utiliza una plataforma de seguridad patentada de múltiples motores para detectar y prevenir malware. Ofrece una protección superior a las tecnologías tradicionales basadas en firmas:

- Detecta una gama más amplia de características, patrones y tendencias maliciosas, lo que permite detecciones más confiables y precisas, incluso para variantes de malware nunca antes vistas.
- Al utilizar búsquedas en tiempo real desde WithSecure™ Security Cloud, puede reaccionar más rápido ante amenazas nuevas y emergentes, además de garantizar una huella pequeña.
- La emulación permite la detección de malware que utiliza técnicas de ofuscación y ofrece otra capa de seguridad antes de ejecutar un archivo.

5.5 Protección web proactiva

Además, la solución ofrece una protección web amplia y proactiva para terminales, lo que garantiza que el vector de ataque más explotado esté bien defendido.

- Previene de forma proactiva el acceso a sitios maliciosos y de phishing incluso antes de acceder a ellos. Esto es especialmente eficaz, ya que una intervención temprana reduce en gran medida la exposición general a contenidos maliciosos y, por tanto, a ataques. Después de la capa inicial de protección web, el contenido del tráfico web (HTTP) también se somete a análisis para proporcionar protección adicional contra malware, antes de que entre en contacto con el propio punto final.

5.6 Protección de recursos compartidos del servidor

Compartir archivos en servidores de archivos locales expone a las organizaciones a riesgos de ataques de ransomware, especialmente cuando dispositivos fuera del control total de la organización acceden a los recursos compartidos del servidor y terminan cifrando una gran cantidad de archivos importantes como inutilizables.

Puede continuar usando archivos compartidos de Windows de manera segura al tener Server Share Protection como protección adicional contra ransomware diseñada para identificar y revertir inmediatamente cualquier cifrado u otra destrucción involuntaria de archivos y proteger a su organización de la propagación del ransomware.

5.7 Citrix y servidores de terminales

Además de las mismas capacidades de seguridad básicas que los servidores Windows, el componente Citrix proporciona protección adicional para los entornos Citrix al ampliar las capacidades integradas de administración de parches para las aplicaciones publicadas. El cliente cuenta con la certificación Citrix Ready, lo que garantiza que funciona perfectamente en entornos Citrix. De manera similar, Server Protection brinda protección para servidores de terminales de Windows. Tenga en cuenta que los clientes que utilizan Server Protection en entornos de escritorio remoto también necesitan una licencia para WithSecure™ Remote Desktop Protection.

5.8 Linux

Linux Protection proporciona capacidades de seguridad básicas para clientes Linux: escaneo en acceso multimotor, escaneos programados y manuales, y verificación de integridad. Está diseñado para detectar y prevenir ataques basados en Windows y Linux, lo que lo hace particularmente útil en entornos mixtos, donde una máquina Linux desprotegida puede usarse como un vector de ataque fácil.

5.9 Antimalware multimotor

Los clientes utilizan una plataforma de seguridad patentada de múltiples motores para detectar y prevenir malware. Ofrece una protección superior a las tecnologías tradicionales basadas en firmas, con el beneficio adicional de no depender de una sola tecnología.

La plataforma detecta una gama más amplia de características, patrones y tendencias maliciosas, lo que permite detecciones más confiables y precisas, incluso para variantes de malware nunca antes vistas.

5.10 Comprobación de integridad

El componente viene con un verificador de integridad incorporado, que detecta y evita que los atacantes manipulen los kernels, los archivos del sistema o las configuraciones. Es una característica de seguridad vital, ya que protege el sistema contra modificaciones no autorizadas que, de otro modo, podrían pasar desapercibidas.

La verificación de integridad se puede configurar para enviar alertas al administrador de cualquier intento de modificar los archivos monitoreados. Esto hace que los cambios no autorizados sean fáciles de detectar, lo que garantiza que cualquier acción de respuesta a incidentes se pueda tomar sin demora. Si se necesitan cambios en la base, por ejemplo debido al sistema operativo, la seguridad y las actualizaciones de software, los administradores pueden usar una herramienta de instalación protegida para realizar las actualizaciones necesarias sin ningún problema.

6. Integración con SIEM/RMM

WithSecure™ Elements Endpoint Protection se puede integrar completamente con SIEM, RMM o cualquier otra herramienta de auditoría, gestión o generación de informes de terceros con WithSecure™ Elements Connector. Estas incluyen herramientas ofrecidas por Kaseya, Tableau, N-Able, Splunk, entre muchas otras.

La integración ayuda a aprovechar las inversiones existentes de una organización y se beneficia de las herramientas centralizadas, por ejemplo, al optimizar la seguridad del administrador y el trabajo relacionado con la respuesta a incidentes.

Al utilizar las capacidades de los sistemas SIEM/RMM, la integración permite, por ejemplo, la creación de automatización adicional, flujos de trabajo personalizados e informes, lo que reduce aún más la carga de trabajo y optimiza la solución para las necesidades específicas de su organización. El alcance de la integración puede ser tan grande o tan pequeño como sea necesario, ya que se puede acceder a cualquier operación individualmente a través de las llamadas API. Por ejemplo, los administradores de TI pueden optar por enviar solo datos relevantes a un sistema de informes, registro o auditoría, en lugar de integrar también las capacidades de gestión.

La integración se realiza a través de una API REST, llamada WithSecure™ Management API. Proporciona acceso a todas las operaciones y datos disponibles en el Portal de Gestión.

Para obtener más información sobre la API de administración y la integración SIEM/RMM, consulte la descripción de la API de administración en connect.withsecure.com.

7. Servicios profesionales

Los paquetes de soporte adicionales de WithSecure ofrecen una colección de servicios para una experiencia de soporte más flexible e integral. Nuestro soporte está disponible para usted durante el horario comercial o incluso en servicio 24 horas al día, 7 días a la semana. Ofrecemos soporte avanzado o premium con diferentes niveles de servicio para satisfacer sus necesidades.

Avanzado	Premium
Horario comercial local (inglés, finlandés, francés, alemán, japonés y sueco)	24/7 (Inglés)
Acceso prioritario al soporte técnico.	Responder a incidentes críticos en una hora
Herramientas online para emisión de tickets y seguimiento	Escalada de nivel gerencial
Teléfono y devolución de llamada	Consulta de actualización
Chat y remoto	Consejos para eliminar malware

8. Seguridad de los datos

La plataforma WithSecure™ Elements Endpoint Protection utiliza Amazon Web Services (AWS). Esto nos permite garantizar una alta disponibilidad y tolerancia a fallas, además de mejores tiempos de respuesta y capacidad de escalar según sea necesario. Las regiones geográficas actualmente disponibles son Europa, América del Norte y APAC.

AWS afirma que cada uno de sus centros de datos está alineado con las pautas de Nivel 3+. Para obtener más información sobre los centros de datos de AWS, consulte: https://aws. amazon.com/compliance/

WithSecure™ cumple con las regulaciones y leyes de privacidad en todos los países donde opera.

Nos tomamos muy en serio la seguridad de los centros de datos y los mantenemos seguros mediante el uso de docenas de medidas de seguridad, tales como:

- **Seguridad por diseño:** Nuestros sistemas están diseñados desde cero para ser seguros. Incorporamos la privacidad y la seguridad en el desarrollo de nuestras tecnologías y sistemas desde las primeras etapas de conceptualización y diseño hasta la implementación y operación.
- **Controles de acceso rigurosos:** solo un pequeño grupo examinado de empleados de WithSecure™ tiene acceso a los datos del cliente. Los derechos y niveles de acceso se basan en su función y rol laboral, utilizando el concepto de coincidencia de privilegios mínimos con las responsabilidades definidas.
- **Seguridad operativa sólida:** la seguridad operativa es una parte diaria de nuestro trabajo, incluida la gestión de vulnerabilidades, la prevención de malware y procesos sólidos de gestión de incidentes para eventos de seguridad que pueden afectar la confidencialidad, integridad o disponibilidad de sistemas o datos.

¿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.

W / T H®
secure