Descripción general de la solución

# WithSecure™ Elements **Collaboration Protection**

**WithSecure™ Elements: reduzca el riesgo cibernético, la complejidad y la ineficiencia**

# Contenido





November 2022

# Resumen ejecutivo

WithSecure™ Elements Collaboration Protection ayuda a las organizaciones a mitigar los riesgos del correo electrónico empresarial al proporcionar una protección eficaz contra amenazas para Microsoft 365 contra ataques de phishing cada vez más sofisticados y contenido malicioso. La perfecta integración de nube a nube elimina la necesidad de middleware o costosos trabajos de TI, lo que convierte a Elements Collaboration Protection en una solución rentable y fácil de administrar.

## Flexibilidad para crear ciberseguridad resiliente con WithSecure™ Elements

En el entorno empresarial ágil de hoy, 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 sus tecnologías de seguridad de elegir y elegir. WithSecure™ Elements integra una gama completa de componentes de ciberseguridad, incluida la gestión de vulnerabilidades, la gestión de parches, la protección de terminales y la detección y respuesta, en un único paquete de software ligero que se gestiona en una consola de gestión unificada basada en la nube. La solución está disponible como un servicio de suscripción totalmente administrado a través de nuestros socios certificados o como una solución en la nube autogestionada. Los clientes pueden cambiar fácilmente de un servicio autogestionado a un servicio totalmente gestionado, por lo que las empresas que luchan por encontrar empleados con habilidades en seguridad cibernética pueden permanecer protegidas en medio del panorama de ataques en constante desarrollo.

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

**WithSecure™ Elements Endpoint Protection:** Con el ganador múltiple de AV-TEST Best Protection de Secure, la protección de terminales basada en IA y nativa de la nube se puede implementar instantáneamente desde su navegador y administrar la seguridad de todos sus terminales, manteniendo a su organización protegida contra ataques. WithSecure™ Elements Endpoint Protection cubre móviles, computadoras 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. Con elementos Secure™. 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 parchar automáticamente las vulnerabilidades, puede reducir la superficie de ataque y minimizar los puntos de entrada de los atacantes.

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

WithSecure™ Elements Endpoint Protectio, Endpoint Detection and Response and Vulnerability Management se incluyen 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 al estado de seguridad que combina Endpoint Protection, Endpoint Detection and Response, Vulnerabillity Managemente y Collaboration Protection.

Todas las soluciones para endpoints (Elements Endpoint Protection, Endpoint Detection and Response, Vulnerabillity Managemente y Collaboration Protection) utilizan un único componente de software que se requiere implementar solo una vez. Las soluciones complementarias pueden activarse luego con solo agregar una clave de licencia en el Centro de seguridad sin tener que implementar soluciones independientes. WithSecure™ Elements Collaboration Protection es una solución basada en la nube que no requiere instalaciones para puntos finales de la empresa.

Además de los beneficios de implementación y gestión, WithSecure™ Elements está diseñado para trabajar juntos maximizando los beneficios de seguridad para la empresa. Un ejemplo es las acciones de respuesta automatizadas: cuando Elements Endpoint Detection and Response detecta un incidente de seguridad en algún dispositivo de punto final en particular, puede iniciar automáticamente Endpoint Protection para ejecutar un análisis completo del sistema en el dispositivo o aislar el dispositivo asignando reglas de firewall especiales con la protección de terminales.

# WithSecure™ Elements

| | Endpoint Protection standard | Endpoint Protection premium | Detection and Response | Vulnerability Management | Collaboration Protection |
|---|---|---|---|---|---|
| Gestión avanzada de parches y antimalware | ✓ | ✓ | | | |
| Anti-ransomware con dataguard y control de aplicaciones | | ✓ | | | |
| Protección avanzada contra amenazas | | | ✓ | | |
| Gestión y priorización de vulnerabilidades. | | | | ✓ | |
| Seguridad avanzada de aplicaciones de correo electrónico y colaboración en la nube | | | | | |

*Nota: las funciones disponibles pueden variar según la plataforma operativa

WithSecure™ Elements Collaboration Protection se ve favorecida por empresas que quieran:

- Minimizar la interrupción del negocio mitigando los riesgos de correo electrónico y colaboración derivados del contenido dañino no detectado por la protección estándar de Microsoft 365.
- Una solución rentable para proteger Microsoft 365 contra phishing, ransomware, archivos maliciosos, riesgos de correo electrónico internos y externos, archivos adjuntos maliciosos y URL
- Integración de nube a nube con implementación sencilla y administración perfecta para garantizar una protección eficiente e ininterrumpida contra amenazas de correo electrónico.

WithSecure™ Elements Collaboration Protection proporciona funciones de seguridad que mitigan los riesgos que plantean los archivos y URL compartidos mediante Microsoft 365. Cada vez que un usuario final recibe o crea un elemento de Microsoft Outlook, como un correo electrónico, una cita, una tarea, un contacto o una nota en su buzón , la solución analiza todos los archivos adjuntos y enlaces incluidos en busca de contenido dañino, como malware, troyanos, ransomware o phishing. De manera similar, cada vez que un usuario final almacena o modifica de otro modo un archivo almacenado en un sitio de SharePoint, los datos se analizan en busca de contenido dañino. La solución también proporciona informes completos, análisis de seguridad avanzados y eventos del sistema para garantizar una respuesta más rápida a las amenazas potenciales identificadas. WithSecure™ Elements Collaboration Protection comprende un portal de gestión para la administración diaria y un servicio backend que utiliza WithSecure's Security Cloud para analizar los elementos de Microsoft 365 en busca de archivos y URL maliciosos. Además, la solución emite una alarma si detecta que las cuentas de correo electrónico de la empresa se han visto comprometidas, lo que brinda a los administradores de TI un tiempo precioso para reaccionar antes de que las credenciales robadas estén disponibles para una audiencia criminal más amplia.

No necesita instalar ningún software adicional ni realizar ningún cambio en la configuración de su red para comenzar a utilizar la solución. WithSecure™ ha demostrado su coherencia en pruebas independientes al ser el único proveedor con 7 prestigiosos premios anuales AV-TEST a la "Mejor protección" 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 Security Cloud de WithSecure.

Esto garantiza que esté a la vanguardia de la seguridad.

La solución WithSecure™ Elements Collaboration Protection también está disponible como un servicio totalmente administrado. Los proveedores de servicios certificados 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 multiempresa, 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. Modelo de responsabilidad compartida

Algunas empresas creen que cuando compran un servicio en la nube, el proveedor de la nube también es responsable de la seguridad. En parte tienen razón, pero con los servicios en la nube existe un modelo llamado modelo de responsabilidad compartida, que establece que los proveedores de la nube son responsables de la seguridad DE la nube y los clientes que la utilizan son responsables de la seguridad EN la nube. En la práctica, esto significa que el proveedor de la nube se encarga de la seguridad física de los centros de datos para que nadie pueda irrumpir físicamente en sus instalaciones y socavar la seguridad de la plataforma subyacente. Los proveedores de la nube también se encargan de la autenticación, la identificación y los controles de usuario y administrador. En términos del RGPD, los proveedores de la nube son Procesadores de Datos.

Los clientes que utilizan los servicios en la nube son responsables de la seguridad de los datos almacenados en la nube. Esto incluye cuidar de que no haya contenido malicioso o ataques dirigidos, riesgos de seguridad de datos internos, engaños o ingeniería social ofreciendo capacitación sobre comportamientos de seguridad a sus empleados. Esto significa que los clientes que utilizan los servicios en la nube son responsables de la seguridad de su correo electrónico. Son los dueños de los datos.

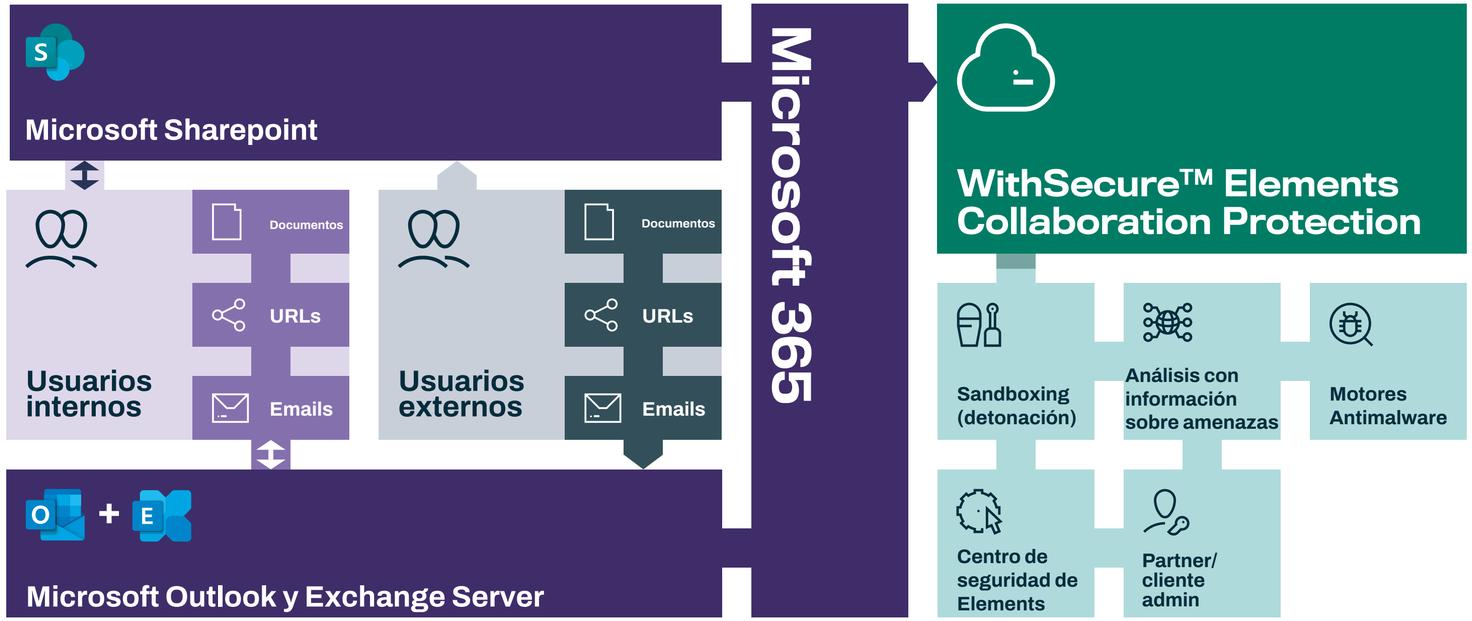
**WithSecure™ Elements Collaboration Protection ofrece:**

- **Una solución rentable** para proteger Microsoft 365 contra phishing, ransomware, archivos maliciosos, riesgos de correo electrónico interno, archivos adjuntos maliciosos y URL
- Combinada con la galardonada protección de terminales de WithSecure, así como con capacidades de detección y respuesta, la solución proporciona una **protección más completa** para su empresa que cualquier solución de seguridad de correo electrónico por sí sola.
- **Integración de nube a nube** con implementación sencilla y administración perfecta para garantizar una protección eficiente e ininterrumpida contra amenazas de correo electrónico

# 2. Descripción general de la solución

WithSecure™ Elements Collaboration Protection es un servicio de seguridad basado en la nube que está diseñado para mitigar los riesgos de colaboración y correo electrónico empresarial en las organizaciones proporcionando una protección eficaz contra amenazas para Exchange Online, OneDrive y SharePoint contra phishing, ransomware, archivos maliciosos, riesgos de correo electrónico interno, archivos adjuntos maliciosos y URL. Además de los mensajes de correo electrónico, se inspeccionan otros elementos de Exchange, como tareas, citas del calendario, contactos y notas adhesivas, en busca de URL y contenido malicioso.

El siguiente diagrama le brinda una descripción general de alto nivel de cómo la solución proporciona seguridad para Microsoft 365.



**Archivos, URL o correos electrónicos**

WithSecure™ Elements Collaboration Protection processes data from Microsoft 365 user mailboxes, OneDrive and SharePoint to inspect and block malicious content. The analyzes cover file attachments and web links included in the body and headers of Exchange items such as email, calendar appoinments, tasks, contacts, and sticky notes in inbound, outbound, and internal traffic. In SharePoint and OneDrive environments, the analysis covers data stored on selected OneDrive spaces and SharePoint sites.

**WithSecure™ Security Cloud (zona de pruebas, inteligencia sobre amenazas a la reputación, motores antimalware)**

WithSecure™ Security Cloud emplea un análisis de contenido de varias etapas en un proceso escalonado desencadenado por el perfil de riesgo del contenido. Además, los archivos de alto riesgo se someten a un análisis más profundo con nuestra tecnología de espacio aislado en la nube, que está diseñada para prevenir ataques de malware de día cero y otras amenazas avanzadas.

**WithSecure™ Elements Security Center**

WithSecure™ Elements Security Center es el portal de administración para que los administradores administren el servicio para proteger el contenido de Microsoft 365. El portal de gestión consta de funciones avanzadas de análisis y eventos del sistema para ayudar a los administradores a priorizar las amenazas en función de la información proporcionada en el portal y mitigar los riesgos de seguridad relacionados a tiempo. El portal también proporciona tableros y capacidades de generación de informes para verificar e informar sobre el estado del sistema en todo momento. Los informes se pueden descargar para compartirlos fácilmente entre las partes interesadas.

**Socio / administrador de clientes**

El servicio WithSecure™ Elements Collaboration Protection confía en que los administradores de socios/clientes trabajen en las detecciones de seguridad y notificaciones por correo electrónico como resultado del contenido malicioso encontrado al analizar los buzones de correo de los usuarios de Microsoft 365 y los archivos almacenados en SharePoint y para tomar medidas según la gravedad de la categoría de alerta y amenaza del contenido.

**Roles de gestión**

Al administrador de WithSecure™ Elements Collaboration Protection se le puede asignar una función según las necesidades de gestión del portal. El servicio permite funciones de administrador, administrador de cuarentena y de solo lectura. Cada rol define permisos que hacen que la funcionalidad de administración del portal sea accesible para el usuario. Un usuario con la función de administrador puede agregar o eliminar usuarios de diferentes funciones mediante el portal web WithSecure™ Business para la gestión de usuarios. La misma cuenta de usuario se puede utilizar para acceder a otros productos y portales de administración de WithSecure™ agregando acceso a la solución respectiva mediante el portal WithSecure™ Business.

**Usuarios**

Los usuarios internos y/o externos son las entidades que utilizan el servicio WithSecure™ Elements Collaboration Protection mientras intercambian elementos como correos electrónicos, citas del calendario, tareas, contactos, notas adhesivas, etc. en sus buzones de correo.

El buzón del usuario interno se analiza en busca de contenidos dañinos en elementos de Exchange en el tráfico entrante, saliente e interno.

## 2.1. Protección de archivos

WithSecure™ Elements Collaboration Protection analiza contenidos dañinos en archivos adjuntos que se encuentran en elementos de Exchange, archivos de OneDrive y SharePoint para proteger contra virus, troyanos, ransomware y otro malware avanzado. Ofrece una protección muy superior en comparación con las tecnologías tradicionales al aprovechar la inteligencia sobre amenazas en tiempo real recopilada de decenas de millones de clientes de seguridad, brindando una protección mejor y más rápida contra amenazas nuevas y emergentes.

### 2.1.1. Analisis inicial

Se realiza una llamada al backend de WithSecure™ con la suma de verificación (SHA1) de los archivos adjuntos que se encuentran en los elementos de Microsoft 365 Exchange (correo electrónico, calendario, citas, notas adhesivas, etc.) y archivos de SharePoint. La suma de comprobación se compara con las guardadas en la caché de detección de amenazas existente en el backend para ver si el archivo se ha analizado antes. Si los resultados del análisis están disponibles en la memoria caché, se utilizan automáticamente y no se realizan más análisis. Los resultados de detección de amenazas existentes se actualizan periódicamente y los resultados caducados se borran automáticamente para garantizar una protección actualizada.

### 2.1.2. Verificación de inteligencia de amenazas

Si no se encuentran resultados en el caché, se realiza una verificación de inteligencia de amenazas a través de Security Cloud de WithSecure utilizando la suma de verificación SHA-256. El servicio devuelve la reputación de seguridad del archivo, su prevalencia y las posibles amenazas detectadas. Dependiendo de la configuración de la política, el sistema elimina el archivo adjunto del elemento de Exchange, pone en cuarentena todo el elemento, lo elimina por completo y/o envía una notificación al usuario y al administrador. En SharePoint y OneDrive, los archivos se colocan en cuarentena según el veredicto de Security Cloud.

### 2.1.3. Antimalware multimotor

Si se desconoce la reputación del archivo, el contenido del archivo se envía a Security Cloud de WithSecure para realizar más análisis de amenazas. El archivo se somete a un análisis más profundo por parte de múltiples motores antimalware complementarios para encontrar malware, exploits de día cero y patrones de amenazas avanzadas. En esta etapa, el proceso de análisis utiliza toda la extensión de los datos y capacidades de inteligencia de amenazas recopilados por WithSecure™ Labs.

### 2.1.4. Análisis avanzado de amenazas (sandbox)

Según los resultados del análisis de amenazas, el sistema utiliza técnicas de aprendizaje automático optimizadas para decidir si se envía el archivo al entorno limitado de la nube para un análisis más profundo. Si tiene indicadores de riesgo sospechosos, se envía un archivo al sandbox, donde se ejecuta en varios entornos virtuales para analizar el comportamiento. Al centrar el análisis en el comportamiento malicioso en lugar de en identificadores estáticos, el entorno de pruebas en la nube puede identificar y bloquear incluso los exploits y el malware de día cero más sofisticados.

### 2.1.5. Resultados de analisis

Según el veredicto final, el archivo adjunto se clasifica como dañino o limpio. Dependiendo de la configuración especificada, el archivo se elimina del elemento Exchange, OneDrive o SharePoint si es dañino o sospechoso y/o se notifica al usuario y a los administradores sobre el incidente. Si no se encuentran amenazas a la seguridad, se puede acceder al archivo en su ubicación original Elemento de Exchange. El veredicto final, la reputación del archivo y otros detalles del análisis de amenazas se almacenan en la caché de detección de amenazas para su uso futuro en el backend del servicio.

## 2.2. Protección de URL

La protección de URL es una función de seguridad clave que evita de forma proactiva que los usuarios de Microsoft 365 accedan a contenido malicioso o no deseado a través de vínculos web agregados a elementos de Exchange, como correos electrónicos, citas del calendario, tareas, contactos y notas adhesivas. Esto lo convierte en un servicio de seguridad particularmente eficaz, ya que la intervención temprana reduce en gran medida la exposición general a contenido malicioso y, por tanto, a ataques. Por ejemplo, evitará que se engañe a los usuarios para que accedan a sitios de phishing aparentemente legítimos y a sitios maliciosos.

La protección de URL se creó para abordar de manera eficiente los miles de millones de sitios disponibles en Internet y su estado de seguridad en constante fluctuación. Se basa en consultas de búsqueda en tiempo real en Security Cloud de WithSecure. Todas las consultas pasan por varias capas de anonimización para garantizar la máxima confidencialidad empresarial.

La consulta obtiene la reputación más reciente de los sitios web y sus archivos, en función de varios puntos de datos, incluidas direcciones IP, palabras clave de URL, patrones de sitio, metadatos de sitios web extraídos como iframes y tipos de archivos, y comportamiento del sitio web como intentos de explotación, redireccionamientos maliciosos o scripts.

### 2.2.1. Comprobación de seguridad de URL

La solución escanea el cuerpo de los elementos de Exchange y consulta la reputación de las URL incluidas desde Security Cloud de WithSecure. Si el enlace se considera malicioso según la información recibida de la consulta, el acceso a la URL se bloquea o se permite, según la configuración de la política. El administrador puede configurar la política para permitir el acceso a la URL alertando al usuario en el asunto del elemento de Exchange sobre la reputación de la URL. El administrador también puede configurar la política para bloquear el acceso poniendo en cuarentena el elemento o eliminándolo si se determina que la URL es maliciosa o sospechosa.

## 2.3. Detección de cuenta comprometida

El correo electrónico es uno de los mayores vectores de amenazas para empresas de todos los tamaños. El acceso a las cuentas de correo electrónico de los usuarios a menudo otorga acceso a una amplia gama de otros servicios de la empresa y brinda a los atacantes la oportunidad de robar datos de la empresa y de los clientes. Una cuenta vulnerada es una manera fácil para que el atacante ingrese a una organización. Los ataques realizados utilizando una cuenta vulnerada, como campañas de phishing o suplantación de identidad son difíciles de detectar porque utilizan una cuenta de usuario legítima de la empresa. La función de detección de cuentas comprometidas detecta cuentas comprometidas tan pronto como la información sobre la infracción esté disponible. Informa a los usuarios y administradores que tomen medidas para remediar las cuentas cambiando la contraseña o tomando otras medidas de seguridad, como activar la autenticación multifactor para evitar una mayor explotación de los datos violados.

## 2.4. Escaneo de reglas de la bandeja de entrada

Las reglas de la bandeja de entrada en Outlook funcionan como un activador para realizar acciones específicas en los correos electrónicos entrantes automáticamente. Después de obtener acceso a un buzón, un atacante crea reglas de bandeja de entrada para llevar a cabo diferentes tipos de ataques, como el reenvío y la eliminación automática de correos electrónicos. La función de escaneo analiza todas las reglas de la bandeja de entrada en un buzón. Este análisis ayuda a detectar reglas sospechosas que puedan indicar un compromiso de la cuenta. También notifica al propietario del buzón y a los administradores que tomen medidas.

## 2.5. Portal de gestión

El servicio WithSecure™ Elements Collaboration Protection proporciona un portal de administración para que los administradores administren los entornos Microsoft 365 Exchange, OneDrive y SharePoint.

Gracias a los informes enriquecidos, las alertas flexibles, los análisis de seguridad avanzados y los eventos del sistema, responder a las amenazas es fácil para los administradores del sistema, y la visibilidad completa de 360 grados garantiza que conozca sus patrones de uso de Microsoft 365. Esto es útil al responder a un ataque que se produce a través de MS 365, al investigar un ataque proveniente de una fuente desconocida o al verificar si MS 365 fue parte de un incidente.

### 2.5.1. Despliegue

WithSecure™ Elements Collaboration Protection admite la integración de nube a nube sin necesidad de instalar software adicional ni realizar cambios en el servidor o los clientes. La protección es totalmente independiente de la plataforma y capaz de detectar amenazas independientemente del dispositivo o aplicación que se utilice para acceder al buzón de Exchange, a los elementos de OneDrive y SharePoint. Los administradores pueden configurar el servicio para escanear Microsoft 365 y brindar protección integral en solo unos minutos.

### 2.5.2. Dashboard

El portal de administración WithSecure™ Elements Collaboration Protection proporciona un panel fácil de usar para acceder rápidamente a las detecciones de seguridad más recientes de contenido malicioso encontrado en los entornos administrados, los buzones de correo más afectados con el mayor número de detecciones de seguridad y actualizaciones constantes. -Datos actualizados sobre los elementos escaneados y el tipo de acción tomada para proteger contra contenido malicioso.

El panel también muestra la cobertura del entorno en términos de número de buzones de correo y sitios de SharePoint protegidos y que no están protegidos por el servicio de seguridad. Esto te permite saber en todo momento si existen huecos de seguridad en el entorno debido a buzones de correo y sitios de SharePoint desprotegidos.

### 2.5.3. Security detections

El widget de detecciones de seguridad proporciona acceso rápido y sencillo a las detecciones de seguridad más recientes de una organización, ordenadas por la gravedad de la alerta. La lista ordenada ayuda al administrador a priorizar inmediatamente las alertas de alto riesgo con información detallada sobre el contenido malicioso encontrado.

### 2.5.4. Estado del buzón

The mailbox status widget on the dashboard provides a count of protected vs unprotected mailboxes in Microsoft 365 tenants for the organization. This helps the administrator to understand at all times if there are any security gaps present due to those unprotected mailboxes.

### 2.5.5. Buzones de correo más específicos

El widget de buzones de correo más específicos en el panel enumera los 5 buzones de correo de usuarios principales con la mayor cantidad de detecciones de seguridad en una organización. El widget ayuda al administrador a comprobar si hay un aumento repentino en el número de detecciones de seguridad para determinados buzones de correo, lo que podría estar relacionado con un posible incidente de seguridad en la organización.

### 2.5.6. Estatus de Protección

El widget de estado de protección muestra la cantidad total de elementos escaneados y no seguros. El widget también muestra el tipo de acciones tomadas para proteger contra contenido malicioso, como poner en cuarentena o eliminar.

La pestaña de tipos de elementos en el widget proporciona información más detallada sobre el contenido malicioso encontrado por tipo de elemento (correos electrónicos, citas del calendario, tareas, notas adhesivas, contactos, grupos y otros) en el buzón del usuario.

### 2.5.7. Tendencia de protección

El widget de tendencia de protección muestra el porcentaje de contenido inseguro durante el período actual en comparación con el promedio de la organización y el período anterior. La información de tendencias ayuda a los administradores a saber en todo momento si el estado de seguridad de la organización está en el mismo nivel o si hay un aumento repentino de contenido inseguro, lo que podría estar relacionado con un posible incidente de seguridad en la organización.

### 2.5.8. Analítica

WithSecure™ Elements Collaboration Protection brinda visibilidad completa de 360 grados del uso de Microsoft 365. Todas las detecciones de seguridad de contenido malicioso o sospechoso que se encuentran en los buzones de correo de los usuarios son accesibles en el portal en una cómoda vista de tabla. La tabla se puede buscar y ordenar fácilmente según diferentes columnas y criterios.

Muchos departamentos de TI no saben qué tipo de contenido envían o reciben sus usuarios a través de elementos de Microsoft 365 Exchange. Ese conocimiento suele ser útil, ya que los administradores de TI pueden, por ejemplo, encontrar archivos maliciosos o URL que no deberían compartirse a través de Microsoft 365.

Además, una mejor comprensión de las necesidades y los casos de uso de los clientes internos ayuda a los administradores a prestar servicios a su organización de forma más eficaz. Con una potente funcionalidad de búsqueda, los administradores de soluciones y los departamentos de seguridad de TI pueden investigar ataques basados en contenido muy rápidamente.

### 2.5.9. Administración de políticas

WithSecure™ Elements Collaboration Protection proporciona políticas para definir la configuración de seguridad para los contenidos analizados en elementos de Microsoft 365. Una política es el conjunto de configuraciones y reglas que definen cómo el servicio protege los buzones de correo de los usuarios y qué acciones se toman cuando se detecta una amenaza a la seguridad.

Los administradores pueden usar la política predeterminada de WithSecure™ para brindar la máxima protección desde el principio al configurar los inquilinos, o pueden copiar la política predeterminada para modificar la configuración de seguridad de acuerdo con los requisitos de seguridad de la organización y convertirla en la política predeterminada, que luego se convierte en la política predeterminada. asignado de forma predeterminada cada vez que un inquilino está configurado para protección.

### 2.5.10. Gestión de cuarentena

WithSecure™ Elements Collaboration Protection permite a los administradores poner en cuarentena elementos de Exchange, OneDrive y Share-Point en función de la nocividad de los archivos o URL que se encuentran en el elemento. La vista de cuarentena en el portal de administración permite a los administradores ver, liberar o eliminar elementos en cuarentena según sea necesario. El administrador también puede utilizar varios criterios de clasificación y búsqueda para ajustar la vista mientras maneja la lista de elementos en cuarentena para los entornos administrados.

### 2.5.11. Gestión de Detecciones

Cualquier sistema de generación de alertas sólo se puede utilizar si proporciona un buen flujo de trabajo para los administradores que gestionan las alertas. Con WithSecure ™ Elements Collaboration Protection, los administradores pueden gestionar las detecciones filtrando, cambiando el estado del ciclo de vida de las alertas y añadiendo comentarios. La gestión de detecciones es especialmente útil cuando se trabaja en una organización con múltiples administradores donde es necesario distribuir y realizar un seguimiento del trabajo.

### 2.5.12. Reporting

WithSecure™ Elements Collaboration Protection proporciona capacidades de generación de informes enriquecidas para que los administradores informen sobre el estado de seguridad del entorno protegido en cualquier momento en un formato que se puede compartir fácilmente. El administrador puede definir el contenido y programar los informes (diarios, semanales, mensuales) que se generarán automáticamente y tener los informes disponibles en el portal para descargarlos. Además, los administradores pueden agregar un resumen del estado de seguridad del entorno como un mensaje que se agrega al comienzo del informe generado.

# 3. WithSecure™ Security Cloud

Security Cloud de WithSecure es un sistema de análisis de amenazas digitales basado en la nube operado por WithSecure™. Consiste en una base de conocimientos en constante crecimiento y evolución sobre amenazas digitales alimentada por datos del sistema del cliente y servicios automatizados de análisis de amenazas. La infraestructura de Security Cloud está alojada en servidores en múltiples centros de datos de Amazon Web Services en todo el mundo. Security Cloud es un sistema de gran volumen que recibe más de 8 mil millones de consultas todos los días.

Recopilamos solo la cantidad mínima de datos del cliente necesaria para proporcionar nuestros servicios. Cada bit transferido debe ser justificable desde una perspectiva de prevención de amenazas, y los datos nunca se recopilan para supuestas necesidades futuras. Con la configuración predeterminada, Security Cloud no recopila direcciones IP, archivos u otra información privada. Los clientes pueden otorgar permiso a WithSecure™ para almacenar archivos ejecutables sospechosos y/o archivos no ejecutables sospechosos.

Al evaluar los metadatos combinados con información extraída de bases de datos internas y otras fuentes, los sistemas de análisis automatizados proporcionan una evaluación de riesgos completamente informada y actualizada para la amenaza, bloqueando inmediatamente aquellas que han sido vistas previamente por cualquier otro servicio. o dispositivo conectado a Security Cloud.

Security Cloud también permite a los analistas de WithSecure™ Labs proporcionar inteligencia y juicio humanos críticos para complementar los sistemas automatizados y la tecnología de escaneo en el host. Además de crear y mantener las reglas que sustentan las bases de datos y los sistemas de análisis automatizados, los analistas monitorean activamente las amenazas más recientes y estudian las características del malware y los patrones de comportamiento para encontrar las formas más efectivas de identificar programas maliciosos.

## La siguiente tabla documenta nuestros principios de privacidad con todo detalle:

| | |
|---|---|
| **Minimizar el flujo de datos técnicos** | Security Cloud de WithSecure emplea análisis de contenido de varias etapas. Los datos de archivos no se envían a Security Cloud a menos que sean esenciales para brindar protección y el cliente lo haya permitido. |
| **No envíe datos personales ascendentes** | No se envía información a Security Cloud de WithSecure sobre quién publica o accede a los archivos o URL analizados, ni desde dónde. |
| **No confíes en la red** | Todos los metadatos, archivos y otro contenido se transfieren a Security Cloud de forma segura a través de HTTPS o se cifran y firman por separado a través de HTTP. |

Obtenga más información sobre Security Cloud de WithSecure en nuestro documento técnico de Security Cloud y en la Política de privacidad de protección de colaboración de WithSecure™ Elements.

## Principios de la nube de seguridad:

| | |
|---|---|
| **Seguro por diseño** | Un sistema nunca es seguro a menos que haya sido diseñado para serlo. La seguridad no se puede agregar como una ocurrencia tardía del proyecto. Esto es algo que se puso en práctica al desarrollar Security Cloud y sus sistemas relacionados. |
| **Tráfico de red cifrado** | Los datos nunca se transfieren en texto plano a través de Internet. Además, el cifrado se utiliza para garantizar la integridad de varios objetos. WithSecure™ utiliza una combinación de bibliotecas y protocolos criptográficos generalmente disponibles y código criptográfico personalizado. |
| **Entorno de malware separado** | Contamos con más de 20 años de experiencia en enfrentar los desafíos de almacenar y probar software malicioso. Todo el manejo de malware se realiza en redes aisladas de Internet y otras redes WithSecure™. Las redes de almacenamiento y prueba están aisladas entre sí y los archivos se transfieren mediante métodos estrictamente controlados. |
| **Seguimiento profesional** | Todos los sistemas críticos de Security Cloud son monitoreados por personal de WithSecure™. Todos los sistemas que almacenan o prueban malware están alojados en WithSecure™ Corporation. |
| **Acceso controlado** | Solo un número limitado de empleados de WithSecure™ tiene acceso a los sistemas críticos de Security Cloud. Dicho acceso se otorga, revoca y documenta según un proceso documentado y controlado. |
| **Acceso controlado** | El principio más fundamental en todo trabajo de seguridad es tener una actitud abierta y humilde. Hemos puesto mucho esfuerzo en proteger Security Cloud, pero el trabajo nunca termina. Un sistema seguro sólo puede mantenerse promoviendo una actitud abierta, en la que los problemas del sistema se informen, analicen y solucionen rápidamente. Esta actitud incluye la apertura pública, en caso de que nos encontremos con incidentes que pongan en peligro la seguridad del cliente. |

## 3.1. Servicio de inteligencia de amenazas

Al aprovechar la inteligencia sobre amenazas en tiempo real recopilada a partir de decenas de millones de sensores, podemos identificar amenazas nuevas y emergentes a los pocos minutos de su inicio, garantizando una seguridad excepcional contra el panorama de amenazas en constante evolución. Nuestro servicio de inteligencia de amenazas permite que WithSecure™ Elements Collaboration Protection consulte la reputación de objetos como archivos y URL. Los archivos se verifican calculando el hash criptográfico SHA-1 del objeto y enviándolo al servicio de reputación.

## 3.2. Antivirus multimotor

El antivirus multimotor utiliza múltiples capas de seguridad para detectar exploits y malware desconocido utilizados en ataques dirigidos. El sistema combina análisis de comportamiento y capacidades de detección de aprendizaje automático y heurístico, que le permiten identificar malware específico, familias de malware con características similares y una amplia gama de características y patrones físicos maliciosos. Los resultados de este análisis pueden hacer que el archivo se marque como sospechoso y se envíe al entorno limitado de la nube para su posterior procesamiento.

## 3.3. Sandbox en la nube

El entorno de pruebas en la nube ejecuta los archivos detectados en varios entornos virtuales y analiza el comportamiento del archivo. Si se determina que el comportamiento del archivo es sospechoso, la información se envía al servicio de inteligencia de amenazas y antivirus multimotor, donde la siguiente consulta de detección de amenazas bloqueará la amenaza.

# 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.