proofpoint®

Proofpoint Information Protection

Arquitectura de soluciones

Proteger a las personas. Defender los datos.

Componentes de la solución Proofpoint Information Protection

Proofpoint Information Protection se basa en Proofpoint Nexus, una suite de tecnologías impulsadas por IA. Estas tecnologías se han diseñado para identificar datos confidenciales, prevenir pérdidas de datos y contener amenazas internas en varios canales. Nexus utiliza modelos de lenguaje avanzados y análisis de comportamiento para detectar posibles intercambios de datos confidenciales por parte de los usuarios, ya sean accidentales o deliberados. Además, puede identificar comportamientos anómalos, como cuando usuarios no autorizados acceden a datos o los desplazan.

La solución ofrece también un control granular mediante políticas automatizadas para bloquear o corregir actividades de riesgo en tiempo real. Al correlacionar el acceso a los datos y su desplazamiento con el comportamiento de los usuarios, Nexus ayuda a proteger datos confidenciales, como datos personales, datos de tarjetas de pago y otros contenidos clasificados, en el correo electrónico, los endpoints y las aplicaciones cloud.

Además, Nexus mejora las funciones de Proofpoint Data Loss Prevention (DLP), unificando la gestión y análisis mediante IA avanzada. Esto permite a los equipos de seguridad supervisar el acceso a los datos y su desplazamiento, garantizando al mismo tiempo el cumplimiento de normativas sobre privacidad, como el RGPD y la HIPAA. Las empresas pueden así adaptar sus estrategias a sus necesidades, lo que les garantiza una protección específica sin interrumpir las operaciones comerciales legítimas.

Proofpoint Information Protection incluye varios productos. La mayoría de los siguientes productos pueden integrarse en esta solución.

Proofpoint Insider Threat Management (ITM) et Proofpoint Endpoint DLP previene la pérdida de datos y los daños a la reputación causados usuarios internos negligentes, malintencionados o inconscientes. Proofpoint correlaciona las actividades de los usuarios y los desplazamientos de datos, permitiéndole identificar los riesgos relacionados con los usuarios, detectar los compromisos de datos provocados por usuarios internos y acelerar la respuesta a incidentes. También le ayuda a evitar la filtración de datos a través de llaves USB, carpetas de sincronización en la nube, impresiones, etc. Su exclusivo agente ligero para endpoints le ofrece la flexibilidad necesaria para supervisar a los usuarios habituales y a los empleados de alto riesgo.

Proofpoint Cloud DLP combina la seguridad de los datos centrada en las personas (incluida la DLP en línea) y las capacidades de gobierno de las aplicaciones cloud. Protege los datos sensibles y rige las aplicaciones Oauth, y le ayuda a cumplir la normativa sobre confidencialidad y seguridad de los datos. Esta solución CASB multimodal admite modelos de despliegue basados en API y proxy, incluida la DLP para BYOD (uso de dispositivos propios).

Proofpoint Email DLP ayuda a evitar pérdidas de datos sensibles por correo electrónico. También ayuda a cumplir requisitos normativos, como PCI, RGPD, SOX, HIPAA y diversas leyes de privacidad, con estrategias listas para usar que se ajustan a estas normas. Asimismo, puede crear diccionarios personalizados, incluida la clasificación basada en IA, para identificar y proteger los datos específicos de su empresa. Proofpoint Email DLP es fácil de desplegar. Puede configurarla como parte de un sistema de seguridad de correo electrónico existente, o integrarla en un programa DLP para toda la empresa.

Proofpoint Adaptive Email DLP utiliza IA basada en el comportamiento para identificar el comportamiento habitual de sus empleados en el envío de mensajes de correo electrónico, sus relaciones de confianza y la forma en que comunican datos sensibles. A continuación, analiza cada mensaje de correo electrónico en busca de comportamientos anómalos e informa a los administradores de posibles pérdidas de datos. Alerta a los usuarios en tiempo real y evita la pérdida de datos sensibles por correo electrónico. Actualmente, Proofpoint Adaptive Email DLP no pueden integrarse en nuestra plataforma, y no se tratará en este documento.

Proofpoint Information Protection se aloja íntegramente en modo SaaS. Su aplicación backend Analytics ofrece funciones unificadas de gestión y elaboración de informes, incluidas visualizaciones, detección de anomalías, consultas de Big Data, revisiones automáticas y gestión de casos. También ofrece paneles de control para que pueda supervisar su nivel de seguridad, las tendencias de seguridad y los riesgos de cumplimiento en tiempo real. La solución permite generar informes que incluyen indicadores para la gestión.

Arquitectura lógica de Proofpoint Enterprise DLP

La solución Proofpoint Enterprise DLP proporciona a los administradores de seguridad herramientas para proteger los datos confidenciales e investigar eficazmente los incidentes en los entornos, lo que reduce considerablemente los riesgos de puesta en peligro de los datos a los que se expone la empresa.

En cuanto a la gestión de incidentes, el principal objetivo de la solución DLP es ofrecer una consola única para reducir el tiempo dedicado a analizar los registros de investigación forense, acelerar la investigación y corrección de incidentes y, de forma más general, aumentar la eficacia del equipo.

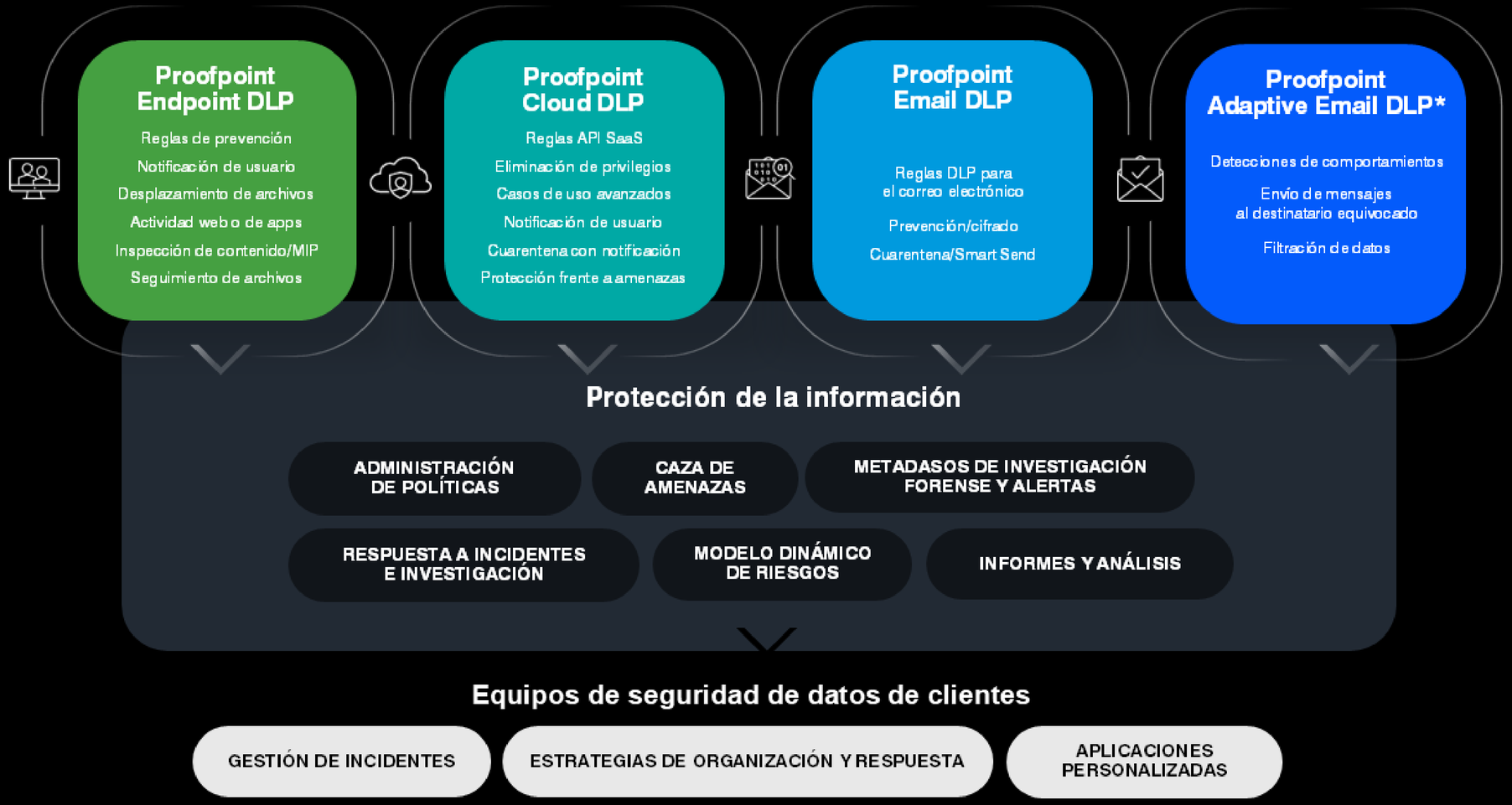
Varios componentes de detección independientes trabajan juntos en una solución integrada. Una arquitectura de soluciones describe la configuración, las normas y las estrategias de aplicación del producto. Define claramente los riesgos para la empresa y los objetivos empresariales del programa de DLP.

De este modo, se pueden crear reglas específicas de la empresa para proporcionar visibilidad y control sobre las actividades designadas que implican información corporativa. Se pueden crear reglas de DLP para alertar a un analista de incidentes de seguridad u organizar la corrección automática intracanal. Las reglas granulares permiten implementar funciones de respuesta flexibles para evitar el bloqueo de actividades empresariales legítimas.

Además, los incidentes importantes y las actividades de alto riesgo pueden identificarse, recopilarse, exportarse y compartirse fácilmente con los equipos responsables. Esto reduce la carga de trabajo y los costes asociados a la gestión de incidentes, y permite a los equipos proteger mejor la empresa y a sus usuarios contra las consecuencias negativas de la pérdida de datos.

Arquitectura de referencia de Proofpoint Enterprise DLP

El flujo de actividad y comunicación entre los componentes de la solución de DLP es el siguiente:



*Integración futura

Análisis unificado para Proofpoint Information Protection

Arquitectura de análisis unificado para Proofpoint Information Protection para endpoints, la nube y el correo electrónico.

Análisis unificado para la gestión de alertas, investigación y respuesta

El administrador de alertas unificado proporciona análisis de datos e informes para todos los eventos recogidos por la solución. También permite gestionar los flujos de trabajo de alertas. Esta función de análisis de datos admite muchos casos de uso avanzado, como exploraciones de caza de amenazas, detección de anomalías y clasificación automática de alertas.

Puede crear reglas de detección específicas en la aplicación Analytics. Estas reglas generan a su vez alertas que un analista de incidentes de seguridad puede clasificar. En caso de infracción, se envía un mensaje de correo electrónico o un evento webhook saliente con los detalles de la alerta a una aplicación receptora externa, como una solución SIEM/SOAR o un sistema de mensajería instantánea.

Las herramientas SIEM de Splunk y otros proveedores pueden integrarse con Proofpoint Information Protection para ofrecer una visión unificada de las amenazas internas, los desplazamientos laterales y la filtración de datos. Esto permite identificar rápidamente a los usuarios implicados y correlacionar la información con otras fuentes de eventos.

Nuestra plataforma también puede informar a ServiceNow de cualquier filtración de datos o incumplimiento de normativas a través de integraciones. ServiceNow puede entonces notificar a sus clientes y crear otras incidencias o flujos de trabajo basados en las alertas. La integración con ServiceNow DLP acelera las investigaciones y la respuesta.

Acceso a la plataforma y controles de privacidad

Los empleados de Proofpoint nunca tienen acceso a sus datos, a menos que su equipo los comparta con ellos. Si les concede acceso, el personal de Proofpoint o los miembros de su equipo pueden utilizar Proofpoint User Center para iniciar sesión en el sistema. También se les puede dar acceso mediante un perfil, es decir, un usuario temporal.

Las alertas deben configurarse en torno al uso de una cuenta de administrador con privilegios elevados. Para asegurar la cuenta, debe cambiarse la contraseña asociada. También puede depositarse en custodia o dividirse entre las partes responsables.

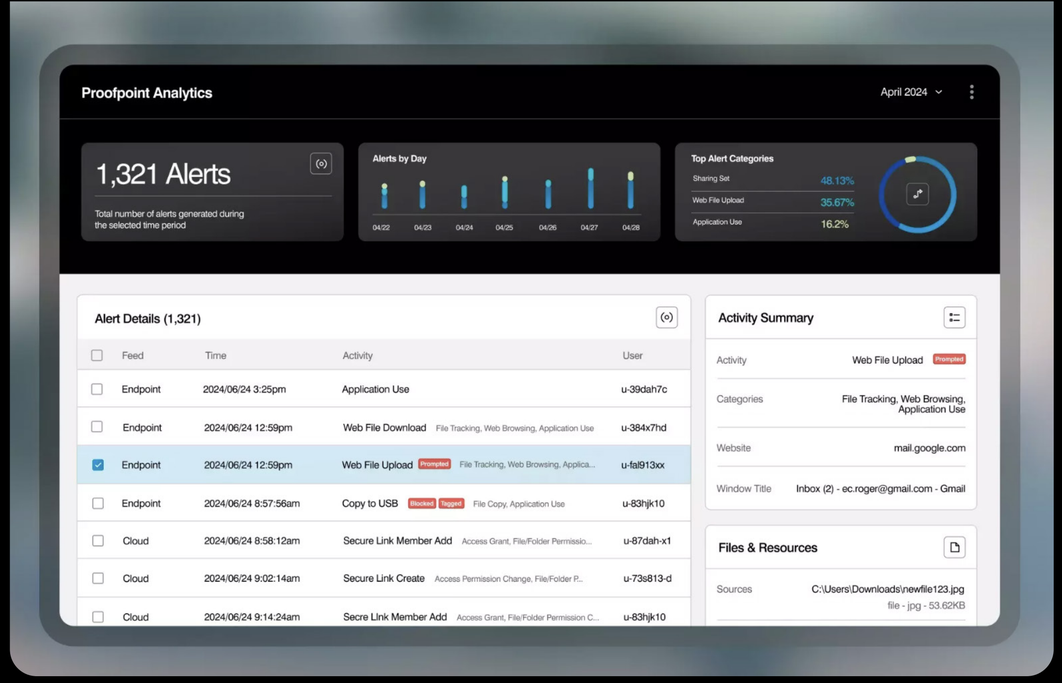
Recomendamos encarecidamente utilizar el protocolo SAML u OAuth 2.0 para integrar métodos de autenticación en la nube, como el inicio de sesión único (SSO) y la autenticación multifactor (MFA). También puede conectar varios proveedores de identidad.

Deberá acceder a Administration > Account Settings (Administración > Configuración de cuentas) de la plataforma Proofpoint Information Protection para configurar un proveedor de identidad según sus parámetros requeridos. También tendrá que configurar su proveedor de identidades para que se conecte a la aplicación Proofpoint Information Protection.

La cuenta de administrador tiene acceso total y anónimo a todos los parámetros y datos de la plataforma. Por lo tanto, las credenciales deben protegerse y considerarse altamente confidenciales. Se pueden crear cuentas de administrador locales adicionales durante la prueba del producto en Administration > User Management (Administración > Gestión de usuarios). A cada cuenta se le pueden asignar sus propias estrategias de acceso, según sea necesario. Sin embargo, en la mayoría de los casos, añadir administradores significará limitar su control y acceso de administrador.

Proofpoint Information Protection se basa en principios de confidencialidad desde la fase de diseño. Solo quienes realmente lo necesitan pueden acceder a los datos sensibles y a la información de identificación de los usuarios. Proofpoint utiliza data centers regionales en Estados Unidos, Europa, Australia, Canadá (a finales de 2024) y Japón (solo datos de endpoints). Esto permite separar los datos desde un punto de vista geográfico. Por ejemplo, un grupo de Estados Unidos puede gestionar datos estadounidenses, que se envían al data center estadounidense. Las políticas de acceso granular permiten a su administrador asignar el acceso de modo que un analista de seguridad con sede en EE. UU. solo pueda ver datos de EE. UU.

Con Proofpoint Information Protection, los administradores del sistema también pueden configurar los datos forenses digitales (datos de identificación personal, información sanitaria protegida, datos de la industria de tarjetas de pago) que desean ocultar en la consola y ocultar la identidad de un usuario para eliminar la parcialidad de los analistas. Puede anonimizar el nombre de usuario, el nombre de host, la dirección IP, la información de ubicación y los nombres de archivo. Cuando se necesite conocer la identidad de un usuario más adelante durante las investigaciones, el analista de seguridad puede solicitar que se desanonimicen los datos, lo que puede ser conceder un administrador.



Acceso a la consola web

Los administradores y analistas pueden conectarse a la plataforma utilizando un navegador compatible. Pueden gestionar políticas y reglas, revisar alertas, corregir incidentes directamente, analizar conjuntos de datos recopilados y ver informes basados en la actividad capturada de los usuarios.

Para gestionar subentidades separadas, muchas empresas pueden acceder a varios subinquilinos en la plataforma de Proofpoint.

Notificaciones de la plataforma

Las alertas se pueden supervisar y procesar en la plataforma de Proofpoint. Estas operaciones también pueden realizarse externamente de acuerdo con sus procedimientos internos de gestión de incidentes. Deberá identificar las direcciones de correo electrónico que recibirán las alertas generadas por la plataforma Proofpoint Information Protection. Los sistemas externos (SIEM, SOAR, ITSM) también pueden configurarse para recibir alertas.

Aplicaciones externas

Las aplicaciones externas pueden acceder a la plataforma de Proofpoint a través de API REST.

Arquitectura de referencia de Proofpoint Endpoint DLP/ITM

El agente único para DLP y gestión de amenazas internas (ITM) recopila y carga datos en la plataforma al tiempo que aplica políticas de DLP.

CONFIGURACIÓN del agente para endpoints DLP/ITM

El agente de Proofpoint Endpoint DLP se instalará en los endpoints del cliente que ejecuten versiones compatibles de Windows o macOS. Para instalar el agente en producción, debe utilizar métodos desatendidos y sus herramientas estándar de instalación remota de software.

En cuanto se despliega, el agente registra metadatos que describen las actividades de los usuarios. No requiere normas explícitas. La plataforma Proofpoint Information Protection carga y procesa los metadatos de forma segura. Para gestionar y configurar el agente, utilice la aplicación Administration > Endpoints (Administración > Endpoints) de la plataforma.

Los agentes de Proofpoint pueden desplegarse en modo silencioso. Cada uno se ejecuta en la memoria del usuario con un consumo mínimo de recursos y puede actualizarse automáticamente. Tras la instalación o actualización, no es necesario reiniciar el sistema. Los agentes no entrarán en conflicto con los sistemas de seguridad de endpoints existentes y no interrumpirán el funcionamiento o el rendimiento de otras aplicaciones.

Los agentes instalados y el servidor ITM se comunican de forma asíncrona a través del protocolo HTTP. Los agentes DLP utilizan el cifrado TLS para comunicarse con los servicios de nube de Proofpoint. Los requisitos del firewall para la conectividad figuran en nuestro portal de documentación en línea.

Los agentes que necesiten conectarse a través de un proxy dinámico utilizarán la configuración de proxy definida a nivel de sistema operativo. El sistema operativo debe estar configurado para utilizar un proxy dinámico para las aplicaciones que se ejecutan bajo la cuenta del sistema (y no la cuenta de usuario). También es posible utilizar un proxy estático. Este parámetro se configura cuando se instalan los agentes.

Algunos programas antivirus y EDR se ejecutan bajo demanda. Escanearán archivos ejecutables y procesos de almacenamiento o bloquearán comunicaciones por defecto. Para garantizar un funcionamiento fiable, debe excluir nuestros procesos de la inspección por parte de otras herramientas de seguridad. No deberías necesitar poner aplicaciones específicas en la lista de blanca de nuestra propia herramienta, ya que es poco probable que nuestro enfoque ligero interfiera con las acciones de un agente para endpoints en modo kernel.

Componentes del agente para endpoints de Windows para listas seguras

Para incluir nuestros archivos en una lista segura, de modo que queden excluidos de la inspección de los sistemas EDR y antivirus, consulte **esta guía**.

NOTA: para mostrar notificaciones o recopilar capturas de pantalla en macOS, también debe asegurarse de que se concede la configuración de privacidad a nuestros procesos desplegando el archivo de configuración móvil. Este proceso se detalla en nuestra documentación online.

El agente para endpoints de Proofpoint admite dos tipos de proxies. Para un proxy dinámico, utilice un archivo de configuración automática de proxy (PAC) en el sistema operativo. Para un proxy estático, introduzca el nombre de host y el puerto en el momento de la instalación. Para definir las credenciales de inicio de sesión predeterminadas que utilizará el agente, introduzca la información necesaria en los campos Dominio, Nombre de usuario y/o Contraseña durante la instalación.

Actualizaciones del agente

Como plataforma SaaS, Proofpoint puede desplegar rápidamente nuevas funciones en el agente. Proofpoint también ofrece una versión LTS (Long Term Support) con soporte a largo plazo del agente para los clientes que no pueden seguir el ritmo de nuestro calendario de lanzamientos. No obstante, en general recomendamos instalar la última versión del agente compatible.

Recomendamos utilizar el servicio de actualización automática para mantener los agentes al día según una estrategia de actualización preconfigurada. Cuando un administrador decide actualizar el agente, todo lo que tiene que hacer es modificar o crear una política que defina la versión de destino y las condiciones para aplicar la actualización. El actualizador de agentes se ejecuta en los endpoints y, a continuación, se asegura de que se descarguen e instalen automáticamente las versiones correctas.

Certificado raíz

Los endpoints instalados deben tener un certificado raíz. Proofpoint firma el agente con un certificado raíz válido para garantizar que el cliente sabe que procede de Proofpoint. Este certificado depende de un certificado raíz válido y tiene una fecha de caducidad anual.

Supervisión de la integridad de los agentes

La información sobre la integridad del agente, como los errores y la marca de tiempo de las últimas horas de registro pueden verse en Administration > Endpoints > Endpoint Catalog (Administración > Endpoints > Catálogo de endpoints). El agente de Windows tiene capacidades de autorreparación e incluye un servicio de supervisión en la nube que reinicia el agente en caso de apagado. El proceso de registro del agente Mac se inicia de forma similar mediante un programa que reinicia el agente si se detiene.

Refuerzo del agente

La configuración del agente y los archivos de registro en los endpoints pueden estar totalmente cifrados. Durante la instalación, también se pueden aplicar refuerzos adicionales, como utilizar una clave de seguridad para impedir que el agente se desinstale o cambiar el nombre de sus procesos.

Configuración de la agrupación de endpoints

Las agrupaciones de agentes separan a los agentes según la ubicación regional de almacenamiento y los periodos de conservación de datos.

Las reglas de prevención a nivel de endpoint se despliegan mediante políticas de agentes diferenciadas. Realizan acciones como mostrar advertencias o bloquear al usuario. Al mismo tiempo, el agente registra señales de metadatos sobre las actividades de los usuarios relacionadas con las aplicaciones. Estos registros se envían al motor de análisis de Proofpoint para su procesamiento. Las capturas de pantalla son opcionales.

Los datos procesados se almacenan en el data center regional de AWS elegido (EE. UU., Europa, Asia-Pacífico, Japón y Canadá en este momento) en función de la configuración de agrupación de agentes seleccionada.

Configuración de la política del agente

Configuración de la política del agente de Proofpoint. Se asignan a grupos de agentes. Por tanto, puede configurar parámetros y aplicarlos simultáneamente a endpoints de varios grupos.

Puede asignar varias políticas de agente a un grupo de agentes. En este caso, puede colocarlos en el orden que prefiera para definir con mayor precisión los parámetros aplicados a los distintos agentes. Este orden determina qué parámetros se activarán en función de la política del agente.

Prevención de endpoints y notificaciones a los usuarios

Cambiar el comportamiento de los usuarios para reducir el riesgo de fugas de datos es un componente esencial de cualquier programa eficaz de DLP o de gestión de riesgos internos. Cuando las reglas DLP se despliegan en endpoints gestionados, pueden utilizarse para bloquear infracciones o advertir a los usuarios. Esto influye en su comportamiento y reduce el riesgo de que los datos se vean comprometidos.

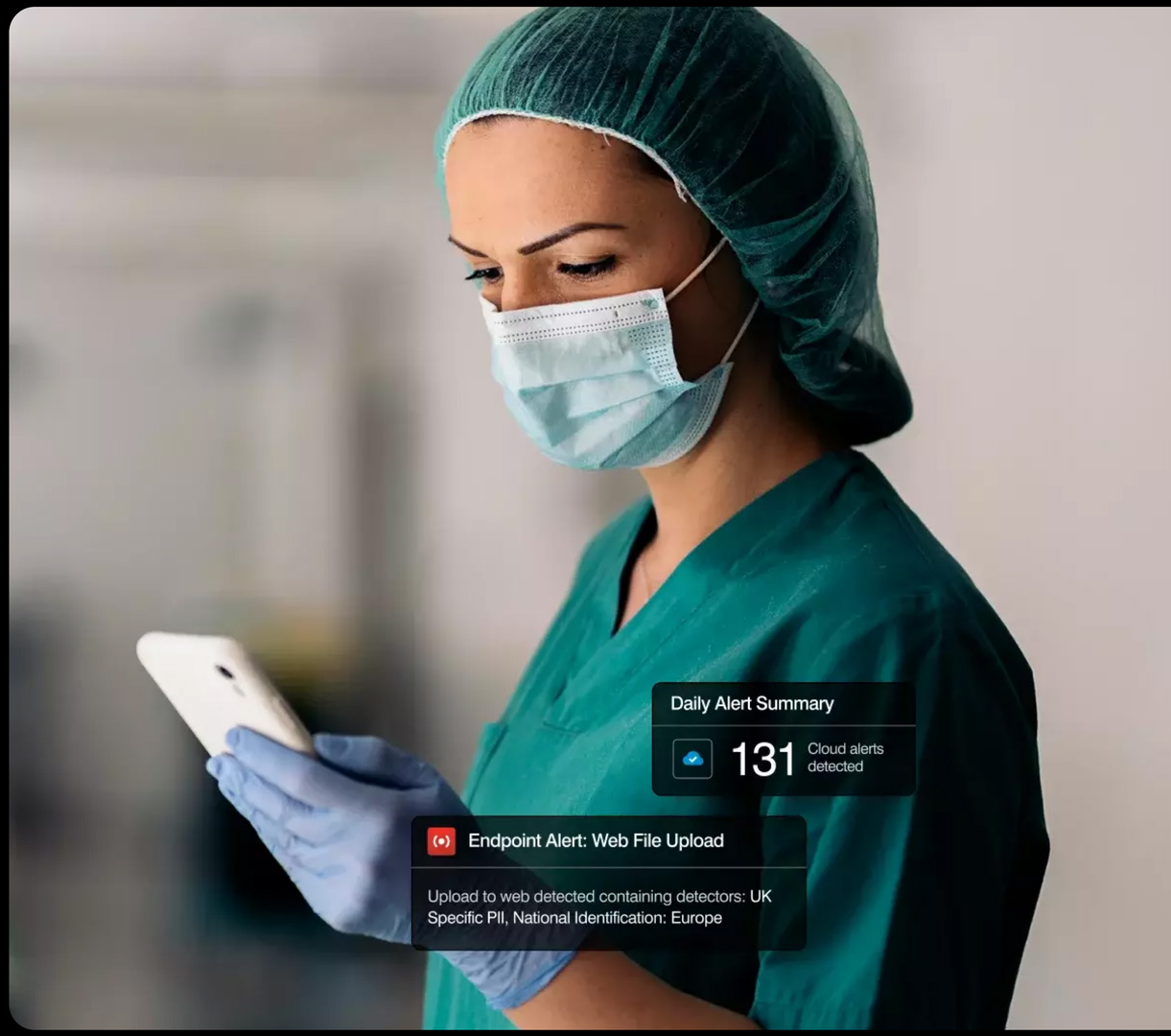
Las reglas DLP están diseñadas para modificar el comportamiento de los usuarios cuando se filtra información confidencial de la empresa. Inicialmente, un enfoque común consiste en supervisar lo que hacen los usuarios a través de los metadatos de actividad en alertas y exploraciones. Cuando los equipos examinan las alertas, pueden utilizarlas para ajustar las reglas de modo que estén en consonancia con las prioridades y procesos de detección de incidentes de la empresa.

Una vez que este proceso está maduro, pueden desplegarse las reglas. En esta fase, cuando los usuarios no respeten las políticas, se les impedirá realizar una acción y se les notificará mediante un mensaje de bloqueo. Para continuar su actividad, se les invitará a seleccionar una justificación predefinida o personalizada.

Las notificaciones a los usuarios suelen personalizarse con un mensaje en el que se describe la política que ha incumplido el usuario También incluyen el logotipo oficial de la empresa y un enlace a una página web en la que se detallan sus políticas de seguridad. El tamaño de la imagen importada para el logotipo de la empresa debe ser inferior a 56 KB (tipo MIME image/*).

Los usuarios pueden saber qué hacer si se bloquea una actividad o cómo presentar una queja por la interrupción. También es buena idea incluir un enlace a la página de la intranet de seguridad corporativa que explique la necesidad de dicho programa DLP.

Las reglas de detección generan alertas en nuestra aplicación Analytics, donde pueden ser gestionadas por un especialista en respuesta a incidentes. Revisan los metadatos recopilados, generados por determinadas actividades de los usuarios en los endpoints. El agente registra los metadatos de acuerdo con la configuración de la política del agente, como la frecuencia y la resolución de las capturas de pantalla. Se gestionan en la consola de administración.



Configuración de Proofpoint Cloud DLP

Proofpoint Cloud DLP admite una arquitectura sin agentes. Utiliza las API de la nube para proteger las principales aplicaciones en la nube. También ofrece DLP en línea para dispositivos BYOD que utilizan el aislamiento del navegador después de que un usuario se autentique para acceder a una aplicación cloud.

Proofpoint Cloud DLP se conecta a los principales servicios en nube de una empresa y a las aplicaciones SaaS/IaaS aprobadas a través de las API correspondientes. Se beneficiará de una funcionalidad bidireccional, incluida la corrección casi en tiempo real de incidentes de seguridad en la nube.

Proofpoint Cloud DLP es extremadamente potente. Proporciona corrección con la misma pila de detectores DLP que Proofpoint Endpoint DLP.

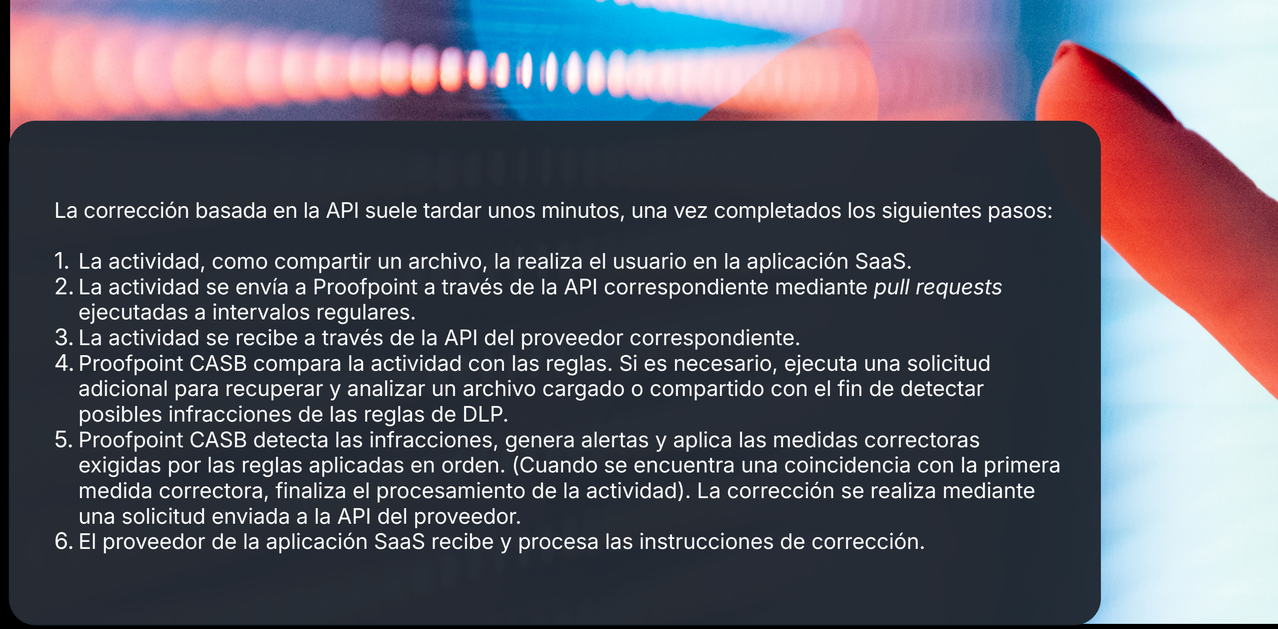
Proofpoint CASB Adaptive Access Controls amplía el poder de Proofpoint Cloud DLP a una gran variedad de casos de uso avanzados en tiempo real. Ejemplos: reconocimiento y bloqueo de endpoints no gestionados, y acceso desde ubicaciones de alto riesgo a través de nuestra integración SAML/OIDC con proveedores de identidad en la nube.

Puede beneficiarse de un control DLP aún más granular sobre las cargas y descargas de archivos a través de un navegador, gracias a la integración con Proofpoint SaaS Isolation, y sin un agente. Por tanto, la solución es adecuada para DLP en dispositivos BYOD. Tenga en cuenta que los conectores API de Okta para Proofpoint simplifican las integraciones SAML. Podemos aplicar automáticamente controles adaptables para aplicaciones federadas por Okta.

Como paso adicional, los servicios IaaS como Azure y AWS pueden configurarse para la supervisión de DLP. Proofpoint factura estas API por separado.

Inicialmente, las API de proveedores para algunas de sus aplicaciones cloud empresariales estarán conectadas a Proofpoint Cloud DLP con fines de supervisión de seguridad.

Puede crear reglas específicas en Proofpoint Cloud DLP para identificar y corregir las infracciones de las políticas de DLP de la empresa en los servicios en la nube. También puede aplicar reglas de gobierno automatizadas a aplicaciones OAuth de terceros, que mantienen el acceso al sistema y a los datos de sus servicios SaaS y empresariales clave, como Microsoft 365 y Google Workspace.



La corrección basada en la API suele tardar unos minutos, una vez completados los siguientes pasos:

1. La actividad, como compartir un archivo, la realiza el usuario en la aplicación SaaS.
2. La actividad se envía a Proofpoint a través de la API correspondiente mediante *pull requests* ejecutadas a intervalos regulares.
3. La actividad se recibe a través de la API del proveedor correspondiente.
4. Proofpoint CASB compara la actividad con las reglas. Si es necesario, ejecuta una solicitud adicional para recuperar y analizar un archivo cargado o compartido con el fin de detectar posibles infracciones de las reglas de DLP.
5. Proofpoint CASB detecta las infracciones, genera alertas y aplica las medidas correctoras exigidas por las reglas aplicadas en orden. (Cuando se encuentra una coincidencia con la primera medida correctora, finaliza el procesamiento de la actividad). La corrección se realiza mediante una solicitud enviada a la API del proveedor.
6. El proveedor de la aplicación SaaS recibe y procesa las instrucciones de corrección.

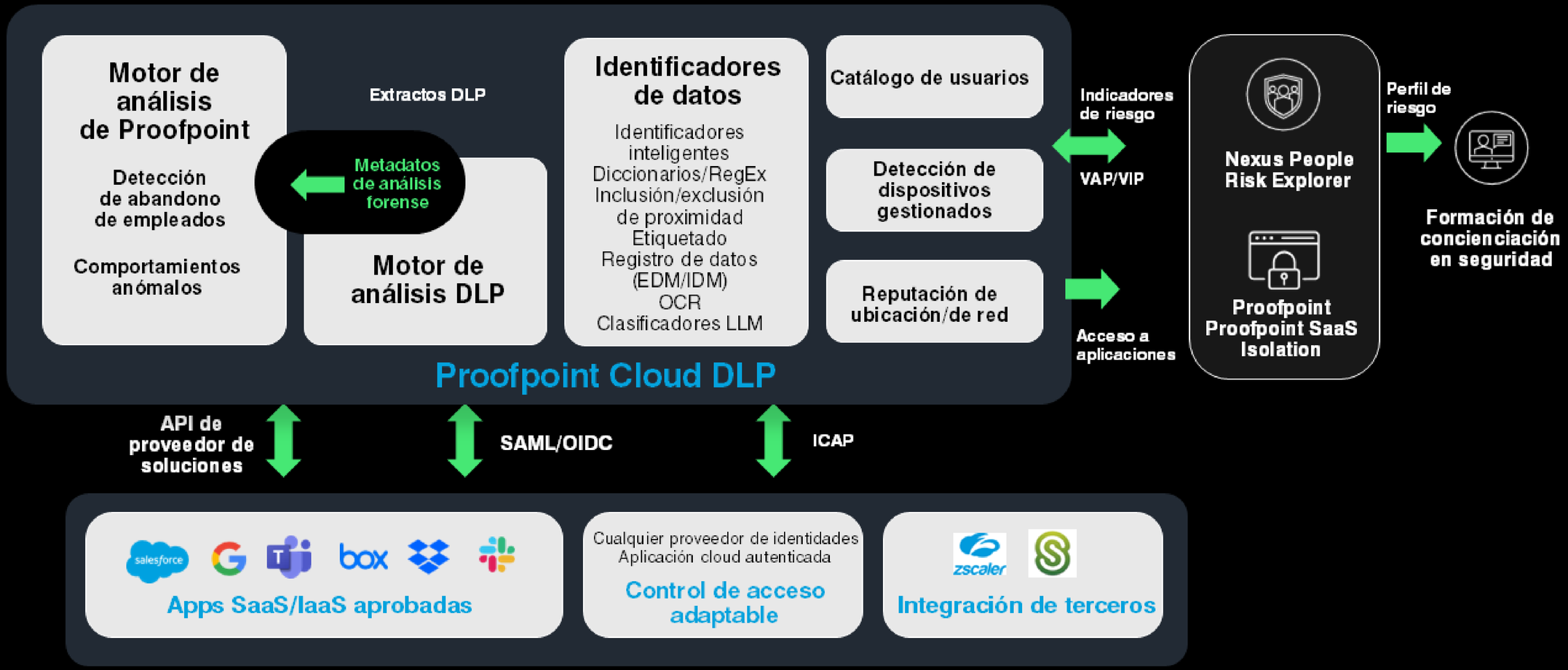
Proofpoint CASB Adaptive Access Controls permite el control en línea de las aplicaciones compatibles, sin necesidad de un agente. Mediante la integración de SAML 2.0 u OIDC con su proveedor de identidades, podemos aplicar protección adicional a cualquier aplicación autenticada mediante de Proofpoint Cloud DLP.

Para configurar Proofpoint CASB Adaptive Access Controls, las solicitudes de conexión de los usuarios deben redirigirse a través de Proofpoint antes de ser autenticado por el proveedor de identidad. A continuación, podemos aplicar una regla que permita el acceso a las aplicaciones cloud de la empresa aprobadas, pero solo en determinadas condiciones.

Las políticas pueden basarse en parámetros tales como si un usuario accede o no a la aplicación SaaS desde un endpoint no gestionado, fuera del alcance de salida de la red de origen de una oficina, desde una ubicación de alto riesgo u otros factores de alto riesgo. Puede obtener un control aún más granular sobre el acceso a las aplicaciones cloud a través de un navegador, gracias a la integración adicional con Proofpoint SaaS Isolation. La integración con nuestra pila DLP tendrá lugar entonces en tiempo real, sin necesidad de un agente.

Para unificar aún más la DLP y proporcionar visibilidad de la pérdida de datos multicanal, Proofpoint también admite la integración ICAP con Zscaler y Citrix ShareFile. Para ello, configure el cliente ICAP de su aplicación de terceros para que redirija su tráfico a nuestro servicio de DLP después de configurar su conjunto de detectores de DLP para ese canal en nuestra plataforma.

Arquitectura de referencia de Proofpoint Cloud DLP



Configuración de Proofpoint Email DLP

Proofpoint Email DLP utiliza un gateway de correo electrónico en línea de Proofpoint para procesar el correo electrónico saliente. Este gateway se integra en su arquitectura de correo saliente.

Proofpoint le asesorará sobre cómo configurar su infraestructura y sistemas para adaptarlos a su arquitectura de mensajería actual, tanto si está probando el gateway de correo saliente de Proofpoint Email DLP como si la va a poner en producción.

Si ya utiliza Proofpoint para su gateway de correo saliente, Proofpoint Email DLP simplemente se activará directamente en su gateway de correo electrónico de Proofpoint existente adquiriendo una licencia para el módulo de cumplimiento de normativas. No se realizará ningún cambio en su flujo de correo electrónico. No hay consecuencias para las normas SPF y DMARC, ni para el calentamiento de direcciones IP ("IP Warmup").

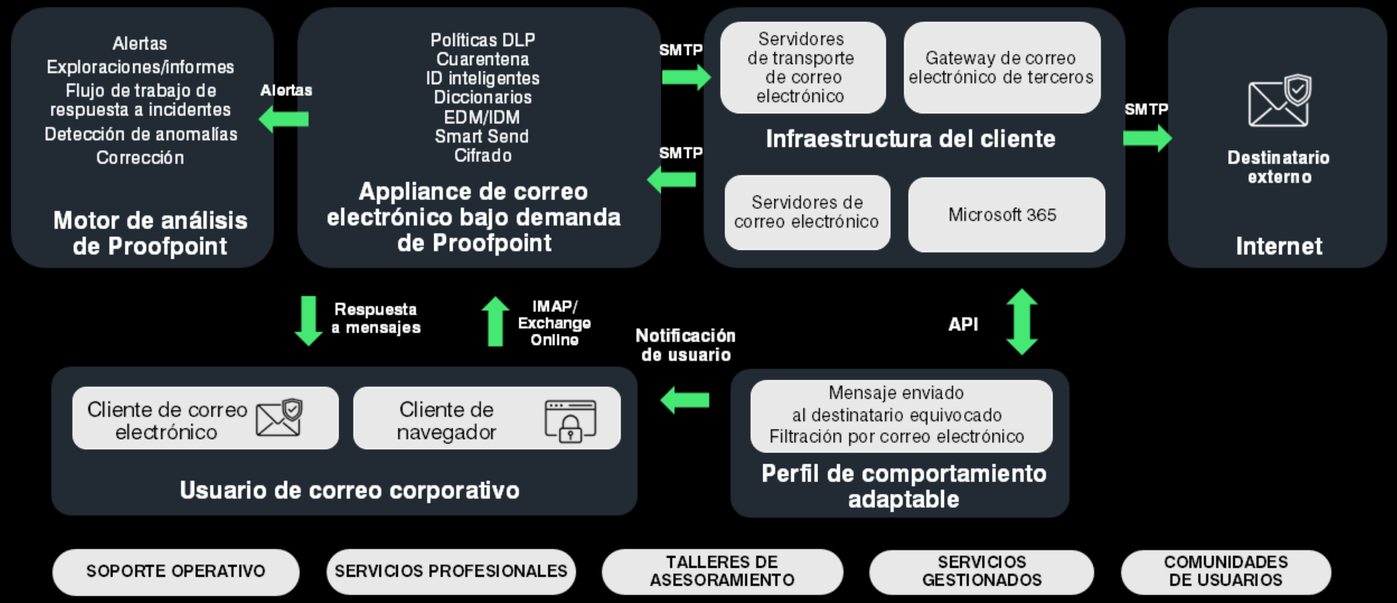
Una vez que Proofpoint Email DLP está activada, puede evaluar toda la gama de funciones de DLP, incluidos los informes, la aplicación, las notificaciones a los usuarios y las interacciones.

Si no utiliza Proofpoint como último eslabón de su flujo de proceso de correo electrónico, el gateway de correo electrónico de basado en la nube de Proofpoint se integrará en su infraestructura de mensajería saliente como un eslabón SMTP adicional. Lo ideal es insertarlo antes de un gateway de correo electrónico existente para evitar cambios adicionales en la infraestructura.

Una vez integrado el servicio de correo electrónico saliente, puede utilizar toda la gama de funciones de DLP, incluidos los informes, la aplicación, las notificaciones a los usuarios y las interacciones.

Arquitectura de referencia de Proofpoint Email DLP

Interacción de los componentes de Proofpoint Email DLP entre sí y comunicación con un usuario de correo electrónico corporativo.



Recuperación ante desastres

Proofpoint gestiona la recuperación en caso de desastre exclusivamente dentro de su plataforma. En caso de interrupción de uno de nuestros servicios, Proofpoint aplicará su plan de recuperación ante desastres, que incluye la presentación de informes periódicos sobre la situación. Estos informes incluyen una breve descripción del suceso, el impacto en los clientes y una estimación de cuándo se volverá a la normalidad. El programa documentado de continuidad de la actividad de Proofpoint describe cómo se restablecen los procesos empresariales. El plan se revisa al menos una vez al año y todos los años se organiza un simulacro. Los detalles pueden solicitarse como parte de una revisión SOC 2 Tipo 1 a través de Proofpoint.

Si los servicios cloud de Proofpoint se volvieran inaccesibles en la red, la aplicación de las reglas DLP existentes no se vería afectada. Todas las reglas de DLP se aplican directamente al agente mediante políticas de máquina. La aplicación de estas reglas no requiere ninguna comunicación con un servidor.

Si el administrador modifica las reglas de prevención durante este período, las máquinas solo recibirán los cambios cuando hayan establecido un enlace con los servicios de Proofpoint. Esta actividad se produce cada 10 minutos.

En cuanto a la detección, una pérdida de conectividad hace que el agente almacene los eventos seleccionados definidos en el conjunto de agentes y la configuración de la política de agentes, que se gestionan en la consola de administración. Una vez que el terminal haya restablecido la comunicación con la aplicación, se cargarán los metadatos de los eventos seleccionados.

Nivel de confidencialidad de los datos

Puede aplicar controles de seguridad de forma coherente y global creando reglas de DLP basadas en identificadores de datos sensibles.

El nivel de confidencialidad de los datos se define por el alcance de las consecuencias negativas que tendría para una empresa la divulgación de un grupo de datos. Estas consecuencias incluyen la erosión de la confianza de clientes y accionistas, pérdidas financieras directas y multas impuestas por un regulador.

Detectores DLP para Proofpoint Cloud DLP y Proofpoint Endpoint DLP
Los detectores DLP de Proofpoint identificados aquí solo se aplican a las normas de Proofpoint Cloud DLP y Proofpoint Endpoint DLP. Si desea utilizar el análisis de contenidos para Proofpoint Endpoint DLP, debe seguir estos pasos:

- El componente de análisis de contenido debe activarse durante la instalación del agente para endpoints Si no es así, debe actualizarse.
- El análisis del contenido de los endpoints debe activarse a nivel de grupo de agentes para estas actividades: cargar archivos web, sincronizar archivos web, copiar en una llave USB, descargar archivos web, abrir documentos, imprimir, pegar texto desde el portapapeles y copiar en una unidad de red.
- Si desea utilizar conjuntos de detectores DLP para el análisis de contenido, los detectores deben añadirse a la configuración del grupo de agentes y desplegarse en los agentes para endpoints.

Una vez desplegados, los detectores pueden utilizarse con fines de detección o prevención.
La lógica de las reglas de prevención desplegadas en el agente incluye la aplicación de endpoints (justificación o bloqueo), así como la detección de datos sensibles.

Para aplicaciones cloud conectadas a Proofpoint Cloud DLP, el motor de políticas podrá utilizar los detectores de DLP poco después de haberlos configurado en la aplicación de DLP. Las reglas de Proofpoint Cloud DLP están configuradas para generar alertas dentro de la plataforma. Sin embargo, en el modo de escritura, pueden aplicar medidas correctoras en función del tipo de conexión para aplicaciones SaaS (API o en línea) mediante reglas en la aplicación Proofpoint Cloud DLP. Las reglas de Proofpoint Cloud DLP pueden incorporar infracciones de las normas de DLP en su lógica. Esta propiedad de la regla se sincroniza automáticamente con los detectores de la aplicación de DLP. Todas las actividades en la nube de las aplicaciones SaaS empresariales integradas alimentan la aplicación Analytics. Las alertas de Proofpoint Cloud DLP configuradas aparecerán en la consola. Todas las medidas correctoras pueden gestionarse y visualizarse directamente desde las alertas.

Proofpoint DLP reconoce los datos sensibles en movimiento y en uso mediante estos tres métodos:

1. **Archivos con etiqueta visual de confidencialidad (Microsoft Information Protection)**

   Si tiene un programa de clasificación de datos que se basa en etiquetas de Microsoft, podemos identificar las etiquetas y los identificadores de inquilinos de Microsoft (MIP). A continuación, pueden utilizarse en las reglas.

2. **Archivos con coincidencias de contenido definidas por los detectores DLP de Proofpoint**

   Los detectores DLP de Proofpoint identifican contenidos sensibles mediante identificadores inteligentes predefinidos, palabras clave de diccionario listas para usar o personalizadas, clasificadores, etc.

3. **Archivos con marcadores contextuales como metadatos (nombre de archivo, ruta, extensión de archivo, tipo de archivo real, propiedades del documento) o archivos de URL supervisadas.**

   En Proofpoint Endpoint DLP, un archivo descargado en el endpoint mediante un navegador compatible se supervisa automáticamente. Se controlan todas las actividades relacionadas con el archivo en el dispositivo (copiar, mover, borrar, cambiar de nombre, etc.). Una vez que el archivo sale de la máquina a través de un canal de salida específico, ya no se supervisa. Toda la actividad relacionada con los archivos supervisados es capturada por el agente, y se puede ver un historial en la vista cronológica de los archivos.

   Por lo tanto, los archivos controlados siempre proceden de URL utilizadas por un navegador para localizar archivos. Esto permite que el agente del endpoint garantice que las reglas de detección y prevención supervisen y controlen las actividades relacionadas con archivos procedentes de servicios web sensibles.

Detectores DLP para Proofpoint Email DLP

Las reglas DLP para Proofpoint Email DLP deben configurarse en la solución Proofpoint Email Security (PPS/PoD). Sin embargo, este proceso queda fuera del ámbito de este documento.

El módulo de cumplimiento normativo de nuestra solución Proofpoint Email Security está configurado para realizar el análisis necesario, registrar la alerta requerida según una regla de Proofpoint Email DLP y, a continuación, llevar a cabo acciones de proceso intracanal. La corrección puede consistir en mover el mensaje a una carpeta local de cuarentena para su procesamiento, cifrar el mensaje, responder al usuario por correo electrónico y abandonar el mensaje, o enviar al usuario una respuesta inteligente invitándole a examinar su propio mensaje antes de aprobarlo.

Todas las actividades contrarias a una política de Proofpoint Email DLP aparecerán en las alertas. Entre ellas se incluyen los datos de correo electrónico, que pueden ser descargados y revisados directamente por un administrador.

Identificadores, detectores y conjuntos DLP

Nuestras expresiones detectoras están escritas en una sintaxis propia. Incluyen cualquier combinación booleana para cinco tipos de condiciones: identificadores inteligentes, diccionarios, inclusión/exclusión por proximidad y conjuntos de datos EDM e IDM. Su orden de proceso se indica entre paréntesis (). Las URL supervisadas se mostrarán como listas de URL específicas visibles para el agente cuando se descargue un archivo con un navegador desde la ubicación designada.

Los diccionarios personalizados son listas de términos específicos del cliente que utilizan los detectores de DLP para localizar datos potencialmente sensibles en los archivos. Cuando se analiza un archivo, un detector compara todas las palabras y frases del fichero con todos los términos contenidos en los diccionarios activados.

Los identificadores inteligentes personalizados están más integrados en la plataforma y son gestionados por el equipo de ingeniería de Proofpoint. A veces es necesario crearlas para realizar sumas de comprobación de valores, por ejemplo, un número de tarjeta de fidelización específico de un cliente o un algoritmo que utiliza expresiones regulares y código.

Gran parte del despliegue inicial se dedica a perfeccionar y ajustar los marcadores de datos sensibles. Este enfoque garantiza una baja tasa de falsos positivos y una alta tasa de precisión.

Los detectores de análisis de contenido indican las condiciones de coincidencia de los datos sensibles basándose en los diccionarios e identificadores inteligentes incluidos.

Los conjuntos de detectores contienen los detectores DLP utilizados por el agente para endpoints. Deben incluirse en los parámetros de configuración del grupo de agentes y desplegarse.

Otras funciones avanzadas de inspección de contenidos:

- Reconocimiento óptico de caracteres (OCR) para extraer texto de imágenes para análisis DLP.
- Coincidencia exacta de datos para una detección de alta precisión mediante coincidencias de varias columnas de datos tabulares estructurados.
- Coincidencia de datos indexados (huella digital de documentos) para cargar archivos no estructurados y realizar análisis de similitud en archivos transmitidos a través de un canal de salida.

Las funciones avanzadas no están disponibles actualmente en el agente para endpoints debido a limitaciones de recursos. Sin embargo, estas limitaciones desaparecen cuando el proceso de análisis tiene lugar en la nube. Por lo tanto, estas funciones solo están disponibles para Proofpoint Cloud DLP y Proofpoint Email DLP.

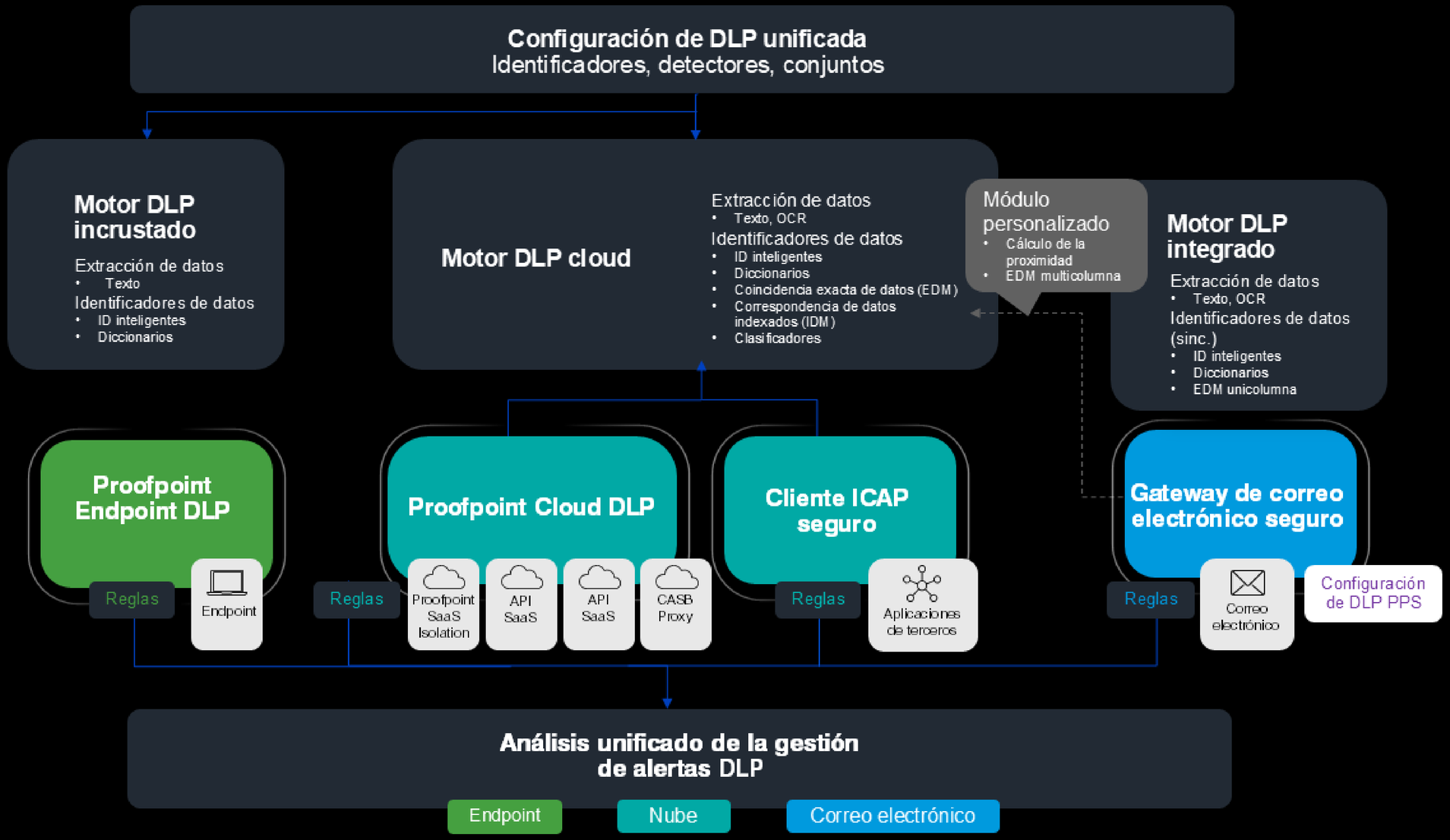
Archivo/exportación de datos fuera de línea

Nuestra funcionalidad de exportación de datos le permite replicar sus datos de forma segura fuera de Proofpoint. Especifique los datos que desea exportar. Se trata de datos de actividad, alertas y eventos. No existe un período de conservación para los datos exportados. Una vez finalizada la exportación, puede manipular los datos para analizarlos y correlacionarlos.

Los datos pueden replicarse en un bucket de AWS S3/Azure perteneciente al cliente, que es independiente de la aplicación de Proofpoint. A continuación, puede integrarlas con otras herramientas de análisis, como soluciones SIEM y lagos de datos.

Los datos exportados son de 15 minutos antes de que se activara la exportación, que funciona cada 15 minutos.

Extracción e identificación de datos por canal DLP



Documento n.º: 1207-005-06-01

proofpoint.

Más información en proofpoint.com/es

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentra el 85 % del Fortune 100, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en www.proofpoint.com/es.