Proofpoint CASB
Controles de acceso adaptables

Administre el acceso y los datos para proteger sus aplicaciones cloud

DESAFÍOS

- Compromiso de cuentas cloud
- Acceso no seguro a aplicaciones cloud
- Pérdida de datos e incumplimiento de normativas

FUNCIONES PRINCIPALES

- Impida el acceso no autorizado con controles basados en identidad y en roles.
- Reduzca los riesgos regulatorios con controles de acceso por dispositivo y mediante el control de los datos.
- Proteja los archivos confidenciales con prevención de fuga de datos en tiempo real.
- Despliegue rápido en cloud.

PRODUCTOS

- Proofpoint CASB
- Proofpoint SaaS Isolation

POR QUÉ PROOFPOINT

- Controles de seguridad centrados en las personas (Very Attacked People™, usuarios con privilegios y usuarios más vulnerables a ciberataques)
- Políticas granulares basadas en el riesgo, el contexto y el rol del usuario
- Inteligencia sobre amenazas (reputación de IP, inicios de sesión sospechosos de alto riesgo)
- Solución sin agente y robusta que se despliega en cuestión de horas

Las plantillas modernas trabajan en entornos cloud, están distribuidas de forma remota y se han convertido en objetivo principal de los ciberataques actuales. De igual manera que las oficinas tradicionales y las jornadas laborales de 9 a 5 han cambiado a rutinas más flexibles, las amenazas han abandonado el perímetro de red antiguo y han desplazado su interés hacia las personas y los datos, sistemas y recursos a los que acceden.

En este entorno cambiante, es absolutamente fundamental proteger el acceso a las aplicaciones cloud, impedir la pérdida de datos y garantizar el cumplimiento de normativas.

Cuando trabajan desde casa o desde cualquier otra ubicación remota, los usuarios carecen de la protección de la red corporativa. A menudo trabajan con dispositivos no gestionados, y puede que descarguen archivos con datos confidenciales en sus dispositivos personales. Esta combinación deja a las organizaciones vulnerables frente a ciberamenazas, como el compromiso de credenciales, que a su vez provoca el compromiso de cuentas, las pérdidas de datos y todo tipo de ataques basados en phishing, como las estafas Business email compromise (BEC).

Estos riesgos son reales, y muy graves. Afortunadamente, Proofpoint CASB puede ayudarle a mitigarlos. Nuestra solución es fácil de desplegar y protege rápidamente aplicaciones como Microsoft 365 (Office 365), G Suite, Zoom, Box, Salesforce, Workday, etc.

Los controles de acceso adaptables de la solución CASB permiten la aplicación de medidas de seguridad en tiempo real basadas en el riesgo, el contexto y rol. La solución bloquea automáticamente el acceso a ubicaciones y redes peligrosas, así como a ciberdelincuentes conocidos. Y aplica controles a usuarios de alto riesgo y con privilegios elevados, incluida una autenticación más estricta, políticas de dispositivos gestionados y la imposición del uso de VPN.

A diferencia de los controles de seguridad y cumplimiento estáticos que se aplicaban por igual a todos los usuarios, los controles de acceso mediante CASB son adaptables. Le permiten aplicar justo la cantidad adecuada de controles de seguridad y regulatorios sin perturbar indebidamente el trabajo de los usuarios de menor riesgo.

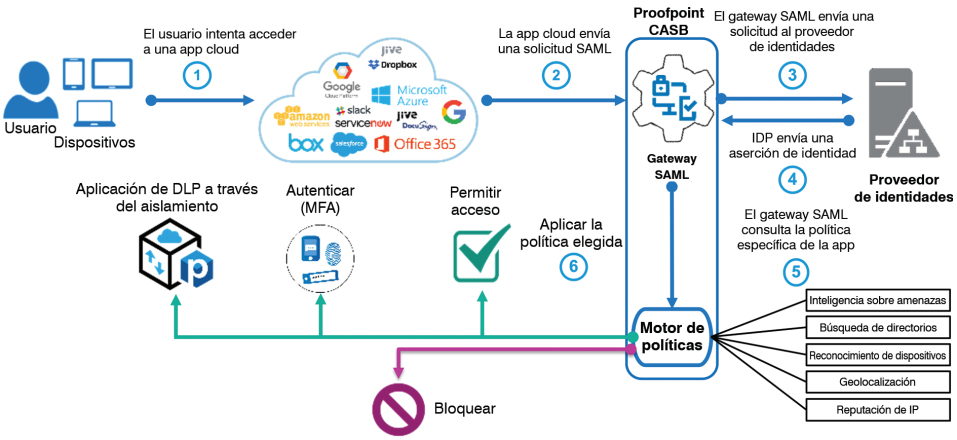

Figura 1: Arquitectura de controles de acceso adaptable.

PROTECCIÓN FRENTE A AMENAZAS EN CLOUD

Las credenciales de las cuentas de los usuarios son las llaves de acceso a su empresa.
Cuando los ciberdelincuentes comprometen estas credenciales de sus cuentas cloud, tienen libertad para lanzar ataques desde dentro y fuera de la empresa.

Los controles de acceso adaptables utilizan inteligencia sobre ciberdelincuentes conocidos para bloquear inicios de sesión sospechosos e impedir la apropiación de cuentas. CASB también utiliza datos contextuales para confirmar la identidad de un usuario e impedir el acceso de riesgo. Los datos de contexto incluyen:

- Ubicación del usuario
- Dispositivo
- Red
- Hora de conexión

Puede utilizar estos indicadores de riesgo para definir las políticas de control de acceso que impidan que los atacantes accedan a las aplicaciones corporativas.

Políticas comunes

Estas son las políticas CASB más comunes que se utilizan para detener las amenazas basadas en cloud.

Bloqueo de inicios de sesión sospechosos de alto riesgo

Cuando Proofpoint ya conoce la firma de un atacante, usted puede impedir esos inicios de sesión peligrosos mediante el uso de los controles de acceso adaptables de la solución CASB. Proofpoint realiza un seguimiento de los inicios de sesión sospechosos en decenas de millones de cuentas y tiene un excelente conocimiento de las amenazas cloud. Por ejemplo, puede bloquear el acceso a sus cuentas de usuario más atacadas cuando CASB detecta una conexión sospechosa.

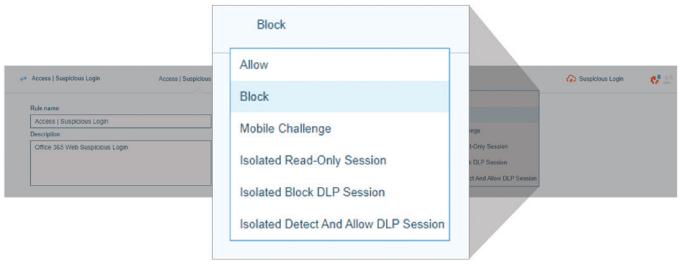

Figura 2: Ejemplo de regla CASB para bloqueo de inicios de sesión sospechosos.

Bloqueo de acceso desde países y redes peligrosas

Puede crear una lista de bloqueo de países en los que su organización no tiene presencia, pero que son origen de ataques. O en función de la reputación de IP proporcionada por Proofpoint, puede bloquear o solicitar autenticación multifactor (MFA) para el acceso desde redes peligrosas como Tors, proxies y redes privadas virtuales (VPN) utilizadas por los atacantes para garantizar su anonimato.

ACCESO CENTRADO EN LAS PERSONAS

Para satisfacer los requisitos de seguridad y regulatorios, las empresas deben proteger el acceso a las aplicaciones aprobadas y a los datos corporativos para todos los usuarios. Esto incluye empleados que podrían trabajar en la oficina o de forma remota, así como contratistas, partners y proveedores. Pero solo porque la cloud permite el acceso universal no quiere decir que usted deba permitirlo. Las empresas necesitan poder crear conjuntos de políticas específicas según la función y privilegios del usuario, y la confidencialidad de la app y los datos que contiene. Las personas son el nuevo perímetro y protegerlas requiere atención a la experiencia del usuario. Proofpoint le ayuda a aplicar controles de acceso adaptables para usuarios/grupos que se encuentran entre las personas más atacadas o Very Attacked People™ (VAP), o que tienen privilegios de acceso a datos, sistemas y recursos de alto valor.

¿Qué es un VAP?

Cada persona es diferente, por lo que el valor de cada uno para los ciberdelincuentes, así como el riesgo para los empresarios, es único.

Todos tenemos hábitos digitales distintos y nuestros propios puntos débiles. Los agresores atacan de diversas formas y con distinto nivel de intensidad. Además, tenemos diferentes contactos profesionales y acceso con distintos niveles de privilegios a los datos, sistemas y recursos.

Estos tres factores (vulnerabilidad, ataques y privilegios) determinan el riesgo global de las personas VAP.

V: Vulnerabilidad. Es posible que utilicen dispositivos no gestionados o redes no fiables sin VPN ni controles ZTNA (acceso zero-trust a redes). Podrían tener tendencia a abrir mensajes de phishing o a hacer clic en enlaces no seguros.

A: Ataques. Son objetivo importante de ciberataques. Esto puede implicar que reciben un gran volumen de intentos de ataque, o bien ataques únicos o de particular eficacia o que proceden de ciberdelincuentes de reconocido éxito.

P: Privilegios. Además, tienen acceso con distintos niveles de privilegios a los datos, sistemas y recursos. En ocasiones, los privilegios pueden no ser obvios. Es posible que un asistente no tenga acceso a datos valiosos de la empresa. Sin embargo, ese usuario tiene acceso al correo electrónico, los contactos y el calendario de algún ejecutivo, algo que resulta muy útil en los ataques tipo BEC.

Un VAP es alguien que constituye un riesgo elevado debido a cualquier combinación de estos factores.

No todo el mundo es VIP. Pero cualquiera puede ser VAP.

Políticas comunes

A continuación se incluyen políticas CASB comunes para administrar el acceso en función de la vulnerabilidad individual, el perfil de ataque y los privilegios de los usuarios.

Aplique autenticación multifactor a VAP

Puede elevar la seguridad para los usuarios que están en peligro. Por ejemplo, si hay determinados usuarios identificados como VAP por la inteligencia sobre amenazas basada en las personas de Proofpoint, puede bloquear o dificultar su acceso a apps sensibles.

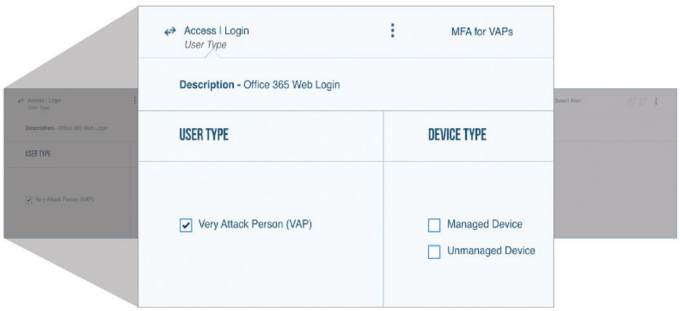

Figura 3: Ejemplo de regla de política CASB para controlar qué dispositivos pueden utilizar los VAP para acceder a Microsoft 365 en la web.

Aplique el acceso a través de una red privada virtual (VPN) para los usuarios con privilegios a apps sensibles

Puede bloquear el acceso a apps sensibles por parte de usuarios con privilegios a menos que utilicen una VPN o acceso a redes zero-trust (ZTNA) o de confianza cero, como Proofpoint Meta. Puede definir rangos IP para su red corporativa y VPN.

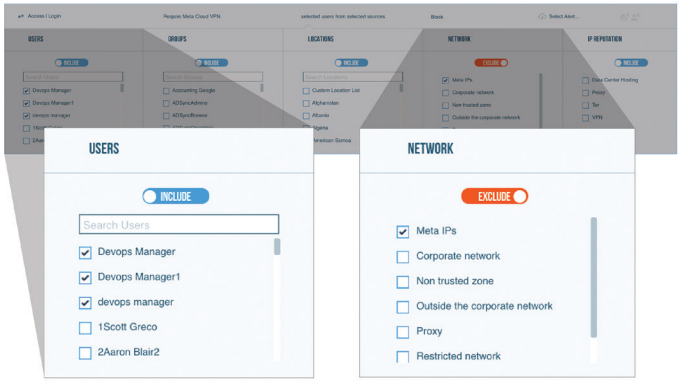

Figura 4: Ejemplo de reglas CASB para exigir VPN o ZTNA a administradores u otros usuarios con privilegios para el acceso remoto.

CONTROLES BASADOS EN DISPOSITIVOS PARA LA PREVENCIÓN DE LA FUGA DE DATOS EN TIEMPO REAL

Una seguridad de datos deficiente supone uno de los mayores riesgos de los dispositivos no gestionados. Cuando un empleado accede a datos de la empresa a través de una red no segura con un dispositivo no gestionado, el riesgo de fugas o pérdida se dispara. A menos que haya desplegado controles en las aplicaciones utilizadas para acceder, compartir y guardar los datos, es fácil acceder a la información o compartirla con personas ajenas a la organización.

Gracias a los controles de acceso adaptables basados en CASB, puede permitir a los empleados acceder a aplicaciones cloud de forma segura desde cualquier lugar y dispositivo. CASB:

- Detecta certificados de dispositivos.
- Ayuda a crear políticas de seguridad de los datos para los dispositivos.
- Aplica controles en tiempo real a través de la integración con Proofpoint SaaS Isolation.

Puede permitir a los usuarios navegar en una aplicación dentro de un navegador aislado seguro en modo de solo lectura. O puede impedir la carga o descarga de archivos que infrinjan las reglas de DLP.

Los empleados de la mayoría de las empresas comparten habitualmente contenido de alto valor en la nube. Eso incluye desde registros de empleados o clientes a código fuente y fórmulas. La detección y prevención de fugas de datos y de infracciones de cumplimiento son fundamentales. En primer lugar, necesita seguridad de datos con reconocimiento de riesgo capaz de llevar a cabo análisis de prevención de la pérdida de datos (DLP) en tiempo real. A continuación necesita poder impedir que se suba a la nube contenido sensible o que se descargue a dispositivos personales.

Políticas comunes

Estas son las políticas CASB más comunes que se utilizan para proteger los dispositivos.

Acceso de solo lectura para dispositivos no gestionados en redes no fiables

Los empleados acceden desde sus dispositivos personales a los datos corporativos en aplicaciones autorizadas, como Microsoft 365, Salesforce, Atlassian, etc. Esa actividad crea nuevos riesgos para sus datos corporativos.

Cuando se descargan datos o se sincroniza un dispositivo personal, la información viaja más allá de su entorno protegido. Un dispositivo robado supone la inmediata pérdida de los datos.

Esa es la razón por la que una empresa podría permitir a los usuarios acceder a herramientas de colaboración desde cualquier dispositivo, pero limitar las descargas de datos exclusivamente a los dispositivos gestionados. Con CASB, puede crear fácilmente una política que dirija los dispositivos no gestionados a una sesión de navegación aislada segura, que no permita ni descargas ni subidas de archivos.

Bloquear las infracciones de la política de DLP para los dispositivos no gestionados, incluso en la red corporativa o equivalente

Más de la mitad de las fugas de datos vienen provocadas por ataques maliciosos o delictivos. Cuando un usuario está en una red corporativa o VPN, el riesgo de ciberataque externo es menor. En este caso, tal vez desee permitir la descarga de archivos no confidenciales a dispositivos no gestionados, mientras bloquea la transferencia de archivos confidenciales.

Con CASB, puede crear una política que dirija a los usuarios a una sesión aislada que aplique las políticas de DLP de la empresa en todas las transferencias de archivos. Si se detecta una infracción, se bloquea la transferencia

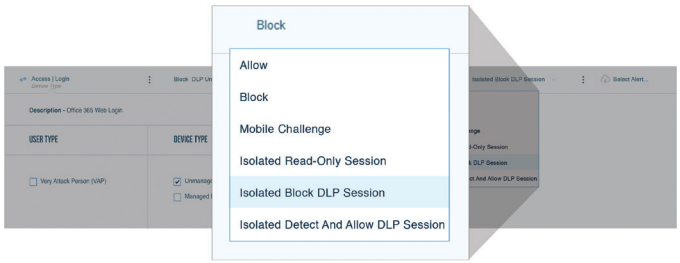

Figura 5: Ejemplo de regla CASB para bloquear la descarga de contenido sensible en dispositivos no gestionados.

DESPLIEGUE RÁPIDO EN CLOUD

Los controles de acceso adaptables de CASB redirigen a un gateway SAML los inicios de sesión a aplicaciones cloud . Este gateway negocia la autenticación federada entre cada proveedor de servicios y el proveedor de identidades. Se despliega en línea con el proveedor de identidades.

Para cada aplicación, el gateway SAML aparece como el proveedor de identidades. Para el proveedor de identidad acreditado (que mantiene el directorio de usuarios y gestiona sus ciclos de vida), el SAML figura como el proveedor de identidades.

La solución de administración de identidades y acceso mantiene el aprovisionamiento de usuarios y otras funciones de administración del flujo de trabajo de identidades. En función de la evaluación del motor de reglas, el gateway SAML permite distintas acciones de control de acceso, como autenticación multifactor, protección de sesiones y protección de fuga de datos (DLP) en tiempo real.

En comparación con los enfoques basados en proxy y proxy inverso, nuestro gateway SAML ofrece varias ventajas en término de arquitectura para el control de cuentas y DLP en tiempo real. Enumeramos algunas:

- **Funciona con cualquier dispositivo:** puede proteger el acceso a apps de cualquier usuario dentro y fuera de la red, tanto con dispositivos personales como gestionados por la empresa.
- **Funciona con cualquier app aprobada por TI:** el gateway SAML puede admitir cualquier app cloud aprobada por TI que admita SAML 2.0 y esté federada a través de un proveedor de identidades.
- **No requiere un agente en el endpoint:** puesto que el gateway SAML actúa como un proveedor de identidades e inspecciona la transacción de inicio de sesión, no requiere un agente en el endpoint para enrutar el tráfico. No tener que gestionar el ciclo de vida del dispositivo de un usuario se traduce en una rentabilización más rápida.
- **Basado en políticas:** los controles de acceso adaptables ofrecen flujos personalizables para amenazas, DLP y controles de aplicaciones. Estas opciones le permiten equilibrar riesgo y confianza.
- **Robusto y escalable:** el gateway SAML no depende de técnicas como reescrituras de URL o terminación de SSL para inspeccionar el tráfico de red. La inspección solo de la transacción de inicio de sesión significa baja latencia. Por lo tanto, no hay riesgo de "ruptura" de la app cloud y no hay pérdida de cobertura.
- **Ofrece privacidad de usuarios:** a diferencia de las soluciones en línea, el gateway SAML no inspecciona todos los datos ni tiene visibilidad de las credenciales de usuario. Si se redirige al usuario a un navegador aislado para prevenir la fuga de datos, solo se inspeccionan las transferencias de usuarios. No se almacenan datos a menos que se produzca una infracción de la política. Esto preserva la privacidad de los datos de los usuarios y de la organización.

Proofpoint CASB es una solución sin agente basada en cloud, por lo que la implementación puede realizarse rápidamente y sin necesidad de instalar hardware adicional. Con la ayuda de los servicios profesionales de Proofpoint, la mayoría de las organizaciones pueden implementar controles de datos y acceso cloud en cuestión de horas.

PRODUCTOS

Proofpoint Cloud App Security Broker (CASB)

Con Proofpoint CASB puede proteger aplicaciones cloud como Microsoft 365, Google G Suite o Box, entre otras. Le protegemos para evitar el compromiso de cuentas cloud, el exceso de datos confidenciales compartidos y el riesgo regulatorio en cloud. Nuestra solución le ofrece controles adaptables para proteger el acceso a sus apps cloud. Con CASB obtiene:

- Visibilidad de amenazas centrada en las personas
- Funciones de respuesta automatizada
- Seguridad integral de los datos con DLP
- Administración de apps cloud y de terceros

Nuestra arquitectura sin agente ofrece un retorno de inversión imbatible y aplica políticas en tiempo real. Nuestro avanzado sistema de análisis le ayuda a conceder a los usuarios y a los "add on" de terceros los niveles de acceso adecuados en función de factores de riesgo relevantes.

Proofpoint SaaS Isolation

SaaS Isolation es un complemento opcional de Proofpoint CASB que protege el acceso de los usuarios a los datos y apps cloud mediante el aislamiento de las sesiones del navegador en un contenedor seguro. Esta solución exclusiva protege las descargas y subidas de archivos de usuarios y comportamientos peligrosos. Aplica políticas DLP en cloud para transferencias de archivos en tiempo real, lo que impide el robo o la pérdida de datos sensibles. Ayuda a afrontar las consecuencias de seguridad, productividad y privacidad que conlleva un uso de alto riesgo de la cloud. SaaS Isolation admite todas las aplicaciones aprobadas por TI a través de nuestra arquitectura sin agente. Es sencilla de desplegar, administrar y mantener.