Proofpoint Cloud App Security Broker IaaS Protection

Identificación de los servicios cloud con problemas de configuración y protección de los datos confidenciales en el almacenamiento IaaS

PROBLEMAS

- Configuraciones incorrectas
- Recursos y cuentas IaaS desconocidos
- Pérdida de datos e incumplimiento de normativas
- Usurpación de cuentas cloud

CARACTERÍSTICAS PRINCIPALES

- Simplificación de la seguridad multicloud y el cumplimiento de normativas con una administración centralizada de todos los recursos IaaS de los distintos proveedores, cuentas y regiones
- Identificación de ajustes de seguridad mal configurados que no se ajustan a las bases de referencia publicadas
- Supervisión y análisis del comportamiento de los usuarios para detectar y detener los inicios de sesión y la actividad administrativa no autorizados
- Protección de los datos confidenciales en almacenamiento IaaS
- Descubrimiento y administración de cuentas IaaS no autorizadas
- Despliegue rápido en la nube

PRODUCTOS

- Proofpoint Cloud App Security Broker (CASB)
- Proofpoint CASB IaaS Protection

La adopción de la nube se acelera. Al igual que las empresas y los equipos de TI, los equipos de DevOps despliegan aplicaciones SaaS para mejorar la agilidad, la elasticidad y la escalabilidad. Han optado por desarrollar nuevas aplicaciones y servicios en la infraestructura cloud.

Su empresa puede tener decenas o cientos de cuentas IaaS con cargas de trabajo desplegadas en uno o varios servicios cloud. Debido a las normativas de privacidad de los datos, es posible que deba almacenar sus datos en repositorios cloud ubicados en distintas regiones del mundo. La carencia de visibilidad de las brechas de su seguridad cloud puede complicar la seguridad de IaaS y el cumplimiento de las normativas. Además, las amenazas cloud, como el compromiso de cuentas, y la falta de personal convenientemente formado, pueden agravar la situación.

La incorrecta configuración y gestión de los clientes, así como otros errores pueden provocar violaciones de seguridad a gran escala. Como resultado, pueden producirse ataques a servicios cloud, como Amazon Web Services (AWS), Microsoft Azure o Google Cloud (GCP). Los responsables de la seguridad y la gestión de riesgos deben identificar y mitigar estos riesgos. Es preciso proteger las cuentas IaaS, los recursos y los datos confidenciales guardados en almacenamiento cloud, como los registros de clientes o las historias clínicas de pacientes.

Para proteger sus entornos IaaS y garantizar el cumplimiento de las normativas, Proofpoint CASB IaaS Protection (IaaS Protection) ofrece:

- Descubrimiento de IaaS
- Administración del estado de seguridad cloud (CSPM)
- Seguridad de los datos
- Protección frente a amenazas
- Controles de acceso adaptables

IaaS Protection es un complemento de Proofpoint CASB.

Identificación de configuraciones incorrectas en entornos IaaS

IaaS Protection le ayuda a gestionar su estado de seguridad en un entorno multicloud. Esta función de Proofpoint CASB descubre las configuraciones y ajustes que se desvían de las bases de referencia publicadas en los servicios IaaS. Por ejemplo, cuando la cuenta de usuario "root" no implementa autenticación multifactor. IaaS Protection evalúa los ajustes de máquinas virtuales, almacenamiento, red y controles de acceso, y los compara con estos cuatro estándares de seguridad:

- CIS Foundations
- PCI DSS
- ISO 27001
- SOC TSP

Si identifica errores de configuración que presenten un riesgo de seguridad, recomienda mejores prácticas para solucionarlos.

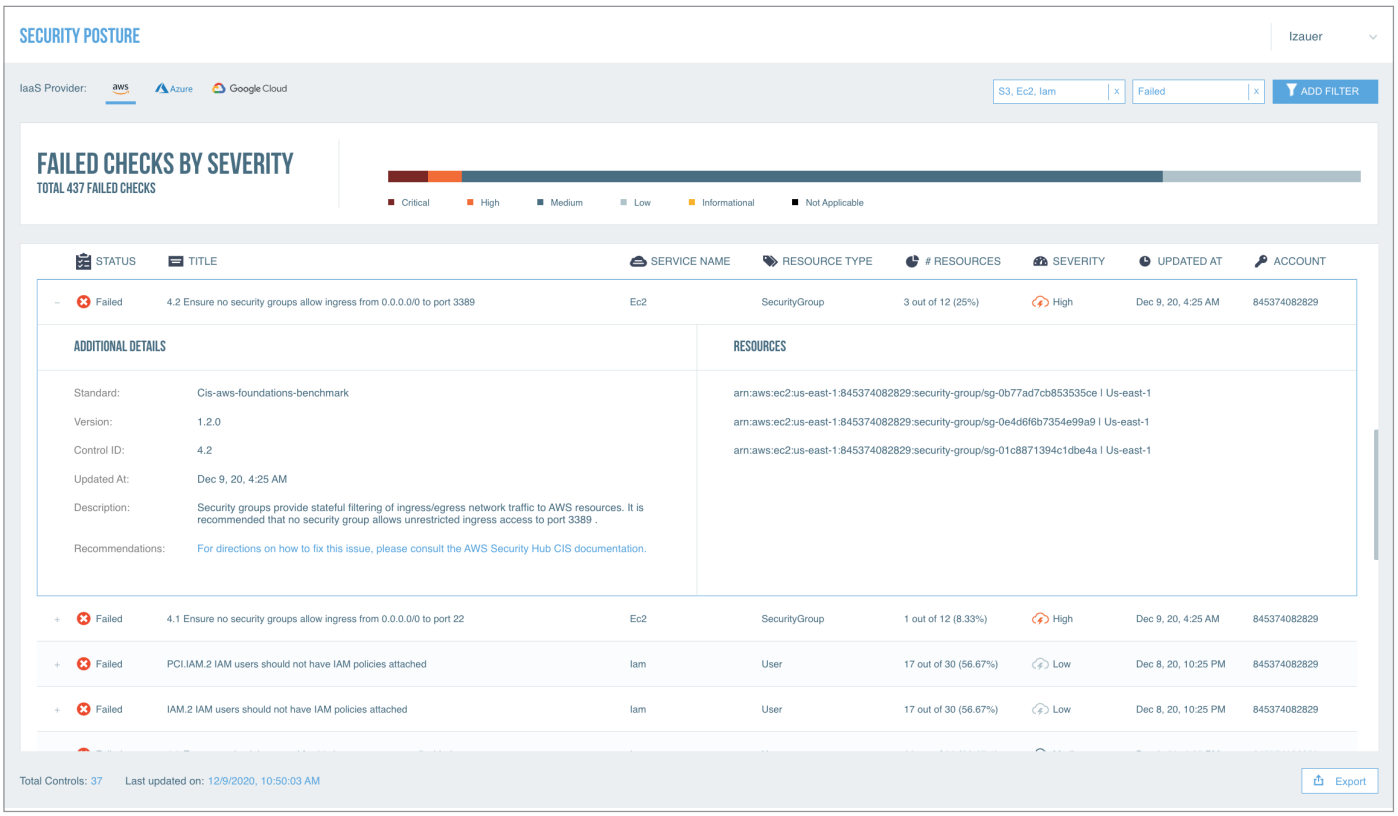

Figura 1: Panel de estado de seguridad que muestra errores de configuración, las instrucciones para ajustarse a la base de referencia de seguridad y una lista de recursos que incumplen el estándar.

Supervisión y control de la actividad de los usuarios con privilegios

A diferencia de las aplicaciones SaaS, la mayoría de los usuarios de IaaS, como los ingenieros de DevOps o los desarrolladores de software, tienen privilegios. Por lo tanto, pueden desplegar, eliminar y configurar recursos de IaaS, como máquinas virtuales y almacenamiento cloud. También pueden asignar privilegios de administrador. Es fundamental supervisar las actividades de estos usuarios con privilegios.

Proofpoint CASB con IaaS Protection le permite definir políticas centradas en las personas (Figura 2). Estas políticas emplean un amplio contexto y alertas cuando se detectan actividades de usuarios con privilegios que no están autorizadas. El contexto incluye el riesgo del usuario, la ubicación, el dispositivo y la red, así como cualquier aplicación cloud a la que el usuario intenta acceder. Por ejemplo, puede impedir actividades de administración, como la modificación de permisos de cubos para países incluidos en la lista de bloqueados.

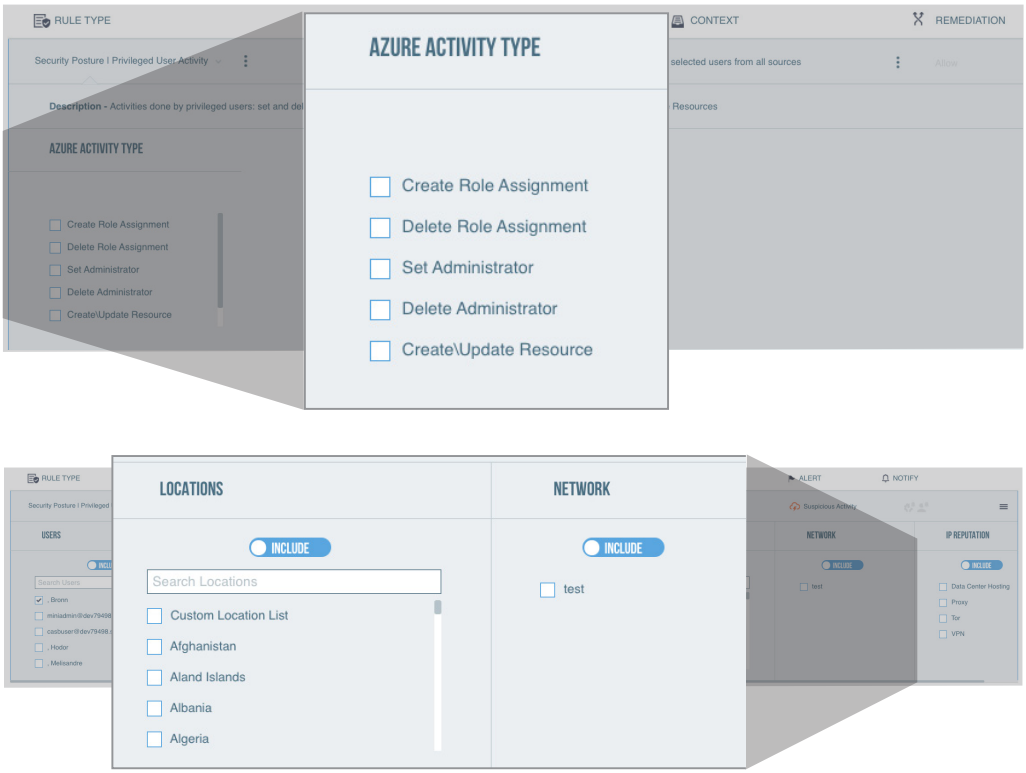

Figura 2: Plantilla de reglas para las actividades de usuarios con privilegios.

Descubrimiento de todos los recursos de IaaS

Con Proofpoint CASB, puede simplificar la seguridad de IaaS y el cumplimiento de normativas para varias nubes y regiones, gracias a la administración centralizada. Además, tiene visibilidad de todas sus apps SaaS y recursos IaaS de distintos proveedores, cuentas y regiones (Figura 3).

Puede mostrar las tendencias de creación de recursos y localizar anomalías, como un exceso de recursos creados o eliminados. También puede analizar en detalle los recursos descubiertos por tipo y región, y asegurarse de que se aprovisionen las cuentas de acuerdo con las normativas y las mejores prácticas; por ejemplo, las empresas multinacionales o europeas pueden controlar los cubos que se despliegan fuera de la UE a fin de evitar que se incumpla el RGPD.

Descubrimiento de cuentas IaaS no aprovisionadas

Proofpoint CASB ofrece visibilidad de las shadow IT en toda su organización. Esto incluye las cuentas IaaS que no han sido aprobadas o documentadas por TI (Figura 4). Nosotros le ayudamos a auditar los registros de tráfico de red. Puede descubrir las apps cloud y las cuentas IaaS a las que se accede en su red. Entre ellas, puede haber cuentas aprobadas por TI, no documentadas y posiblemente cuentas IaaS privadas. Cuando audite las cuentas no aprobadas, puede registrar su estado en la consola de CASB. Por ejemplo, tras descubrir cuentas no documentadas adquiridas durante una fusión, puede aprovisionarlas de acuerdo con los estándares de seguridad para garantizar así que se cumplen las normativas.

Figura 3: Panel de descubrimiento de IaaS que muestra las tendencias, ubicaciones y tipos de recursos.

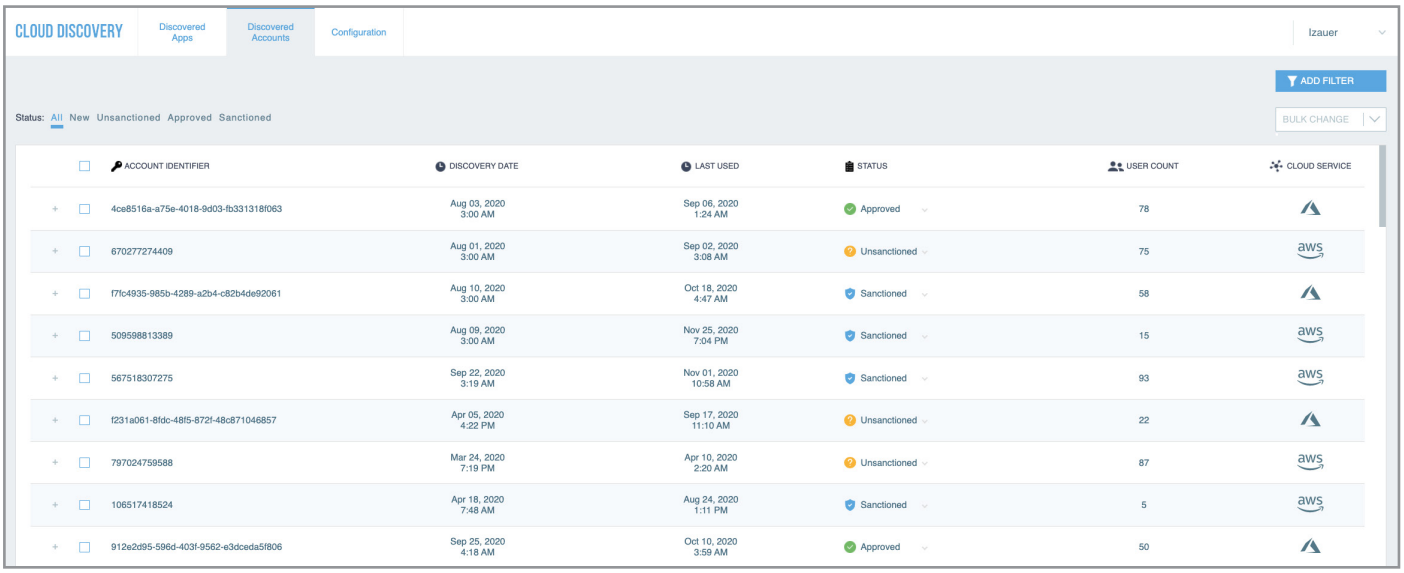

Figura 4: Panel que muestra el estado de las cuentas IaaS descubiertas en la red de la empresa.

Protección de los datos confidenciales en almacenamiento cloud

Proofpoint CASB IaaS Protection le ayuda a identificar y clasificar los datos confidenciales guardados en repositorios cloud, como los cubos AWS S3 y los contenedores de Azure Storage Blob. Además, le permite:

- Supervisar las actividades de archivos para detectar violaciones de DLP.
- Controlar los cubos y contenedores para identificar un exceso de información compartida.
- Crear directivas de seguridad de datos mediante clasificadores de DLP, incluidos identificadores inteligentes integrados, diccionarios, reglas y plantillas que se comparten con otros productos de DLP de Proofpoint.

Los clasificadores listos para utilizar permiten reducir el tiempo necesario para descubrir y proteger los datos regulados guardados en almacenamiento cloud. Además, ayudan a cumplir las normativas. Como parte de Proofpoint Enterprise DLP, nuestra herramienta CASB le permite desplegar políticas de DLP coherentes en sus apps SaaS, cubos IaaS, correo electrónico y endpoints. También permite centralizar en una sola consola la gestión de incidentes de DLP para esos canales. La combinación de telemetría de amenazas, contenido y comportamiento de varios canales ayuda a determinar si la persona que activó la alerta de DLP es víctima de un ataque, o un usuario malicioso o negligente.

Entre las funciones de DLP de Proofpoint CASB se incluyen:

- 240 clasificadores integrados que cubren las normativas PCI, PII y PHI, y el RGPD.
- Búsquedas por proximidad y en diccionarios para mejorar la detección de DLP.
- Correspondencia exacta de datos para automatizar la carga de identificadores o diccionarios personalizados, para detectar información específica de su empresa, como números de cuentas y otros datos estructurados procedentes de bases de datos.
- Huellas digitales de documentos para detectar datos confidenciales en contenido no estructurado, como fórmulas, código fuente, formularios, contratos y otra propiedad intelectual.
- Compatibilidad con 300 tipos de archivos y un identificador de tipos de archivos nuevos, personalizados y propietarios.

Las plantillas de reglas flexibles permiten generar políticas para contenido, comportamientos de usuarios y amenazas (Figura 5). Así puede controlar cómo se comparten, cargan y descargan los datos. Puede restringir automáticamente los permisos para compartir cubos para garantizar el cumplimiento. Por ejemplo, es posible supervisar y suprimir un exceso de uso compartido de cubos cuando se trata de países incluidos en la lista de bloqueados.

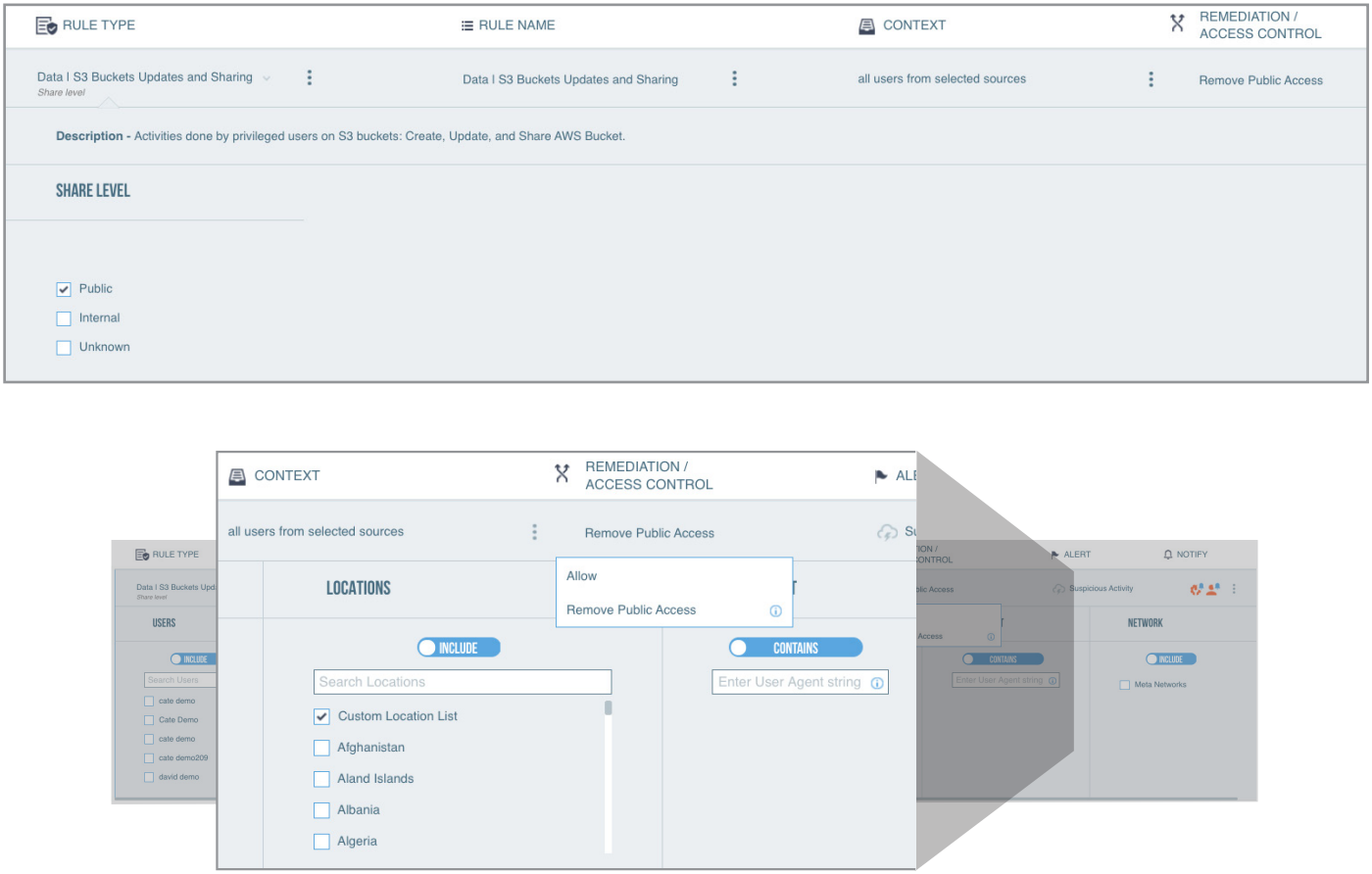

Figura 5: Plantilla de reglas para supervisar los permisos para compartir cubos/contenedores.

La investigación de incidentes de DLP es también más sencilla. Puede correlacionar inicios de sesión sospechosos o cubos con errores de configuración con los incidentes de DLP. También puede filtrar eventos y alertas para generar informes y supervisar estrechamente el cumplimiento mediante la suscripción a alertas.

Controles de acceso adaptables y protección frente a amenazas

La consola de administración de IaaS es una aplicación web para crear y gestionar recursos cloud. Las organizaciones necesitan supervisar y controlar el acceso a esta eficaz herramienta. 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 la función. Además, podrá:

- Proteger su entorno de IaaS configurando automáticamente políticas para bloquear el acceso desde ubicaciones y redes de riesgo, así como por ciberdelincuentes conocidos.
- Aplicar a los usuarios con un riesgo elevado y muchos privilegios controles basados en el riesgo, como una autenticación más estricta, reglas para dispositivos gestionados y la implementación de VPN.

Proofpoint CASB combina nuestra abundante inteligencia sobre amenazas que llegan a través de distintos vectores (la nube, el correo electrónico y otros) procedente del gráfico de amenazas Nexus de Proofpoint, con datos de contexto específicos para los usuarios. Nosotros aplicamos aprendizaje automático a estos datos para analizar el comportamiento de los usuarios y detectar anomalías en los servicios cloud y los suscriptores. Le ayudamos a:

- Detectar el compromiso de cuentas en la nube
- Investigar actividades y alertas, como accesos sospechosos a sus servicios de IaaS federados.

MÁS INFORMACIÓN

Para obtener más información, visite **proofpoint.com/es**.