Proofpoint Cloud Account Defense

Proofpoint Cloud Account Defense (CAD) protege a los usuarios de Microsoft 365 y Google Workspace para evitar poner en compromiso las cuentas cloud. Con CAD, puede detectar, investigar y defenderse de los ciberdelincuentes que intentan acceder a sus datos sensibles y a sus cuentas de confianza. Nuestros eficaces controles de análisis forense, basados en políticas, permiten efectuar la supervisión según los factores de riesgo más relevantes y aplicar las reparaciones oportunas de las amenazas.

VENTAJAS PRINCIPALES

- Identificación de los usuarios que presentan mayor riesgo y control de los incidentes en los paneles interactivos.
- Personalización y priorización de las alertas según los factores de riesgo relevantes para su caso concreto.
- Correlación de las amenazas del correo electrónico y la nube, para detectar con precisión las cuentas comprometidas.
- Investigación de los incidentes de seguridad a través de análisis forenses detallados e informes personalizables.
- Prevención del acceso no autorizado a servicios y apps cloud con controles de acceso adaptables.
- Automatización de la respuesta de seguridad con controles de políticas flexibles.
- Despliegue rápido en cloud.
- La confianza de un soporte al cliente galardonado.

Las credenciales de cuentas de los usuarios son la llave que abre la puerta de su organización. Cuando los ciberdelincuentes comprometen estas credenciales de sus cuentas de Microsoft 365 y Google Workspace, pueden lanzar ataques desde el interior y el exterior de la empresa. De esta forma, consiguen convencer a los usuarios para que transfieran cierta cantidad de dinero o para que revelen información sensible. Además, pueden acceder a sus datos críticos, como la propiedad intelectual o la información de clientes. Esto puede dañar su reputación y sus finanzas. Y, una vez que los atacantes consiguen introducirse en su organización, a menudo instalan puertas traseras para facilitar el acceso a futuros ataques. Las cuentas suelen comprometerse a través del phishing, sin embargo, también puede ocurrir mediante:

- Ataques de fuerza bruta que automatizan el descubrimiento de credenciales.
- Reciclado de credenciales, o *stuffing*, que emplea combinaciones de nombres de usuario y contraseñas procedentes de robos anteriores.
- Malware, como registradores de pulsaciones y ladrones de credenciales.

Puede defenderse frente al compromiso de cuentas cloud con nuestro enfoque integrado, centrado en las personas, que correlaciona la actividad de las amenazas de la nube y del correo electrónico. Nosotros combinamos los análisis basados en el acceso a cloud y el comportamiento de los usuarios, con nuestra inteligencia sobre amenazas del correo electrónico. De esta forma, puede identificar a los usuarios que corren riesgos y detectar las cuentas comprometidas.

Además, evitamos el acceso no autorizado con nuestros controles de acceso adaptables para las apps y servicios cloud aprobados por TI. Nuestras políticas centradas en las personas le alertan en tiempo real si se producen problemas y aplican controles basados en riesgos, como la implementación de VPN o la autenticación multifactor, cuando es necesario.

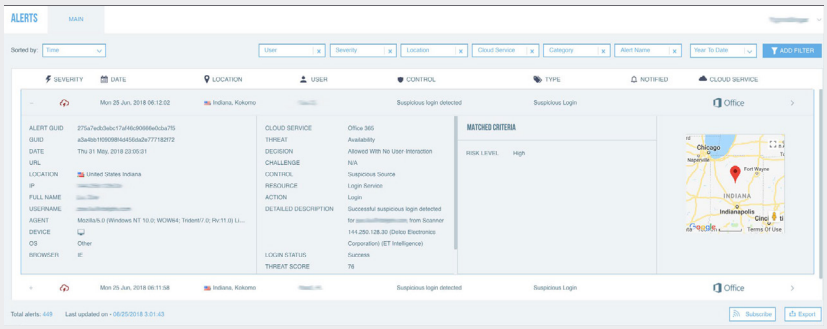
Detección de cuentas comprometidas

CAD ofrece visibilidad centrada en las personas de las amenazas cloud y del correo electrónico. Nosotros le ayudamos a:

- Identificar en su empresa a las personas más atacadas, Very Attacked People™ (VAP), y proteger sus cuentas cloud.
- Detectar ataques de compromiso de cuentas usando datos de contexto del usuario, como su ubicación, dispositivo, red y hora de inicio de sesión.
- Establecer comportamientos de referencia seguros mediante la aplicación de análisis.
- Descubrir anomalías mediante la supervisión con huellas digitales, umbrales y aprendizaje automático avanzado, y buscar actividades sospechosas, como un número excesivo o inusual de intentos de inicio de sesión, un comportamiento de fuerza bruta o inicios de sesión muy próximos en el tiempo pero desde lugares demasiado alejados geográficamente.

CAD también combina nuestra abundante inteligencia sobre amenazas que llegan a través de distintos vectores, procedente del gráfico de amenazas Nexus de Proofpoint, con indicadores de riesgo específicos para los usuarios. De esta forma puede detectar inicios de sesión desde orígenes sospechosos.

Con nuestra inteligencia global sobre amenazas, realizamos verificaciones de la reputación de IP. Además, correlacionamos la actividad de amenazas del correo electrónico y el entorno cloud. Y nuestra inteligencia sobre amenazas basada en el correo electrónico ayuda a descubrir la relación entre los ataques de phishing de credenciales por correo electrónico y los inicios de sesión sospechosos. Los ciberdelincuentes pueden utilizar una cuenta comprometida para lanzar un ataque de phishing contra otros usuarios de su organización. Para identificar otras cuentas comprometidas, estudiamos la huella digital del atacante, buscando un agente de usuario y actividades inusuales, como por ejemplo, el reenvío de mensajes de correo electrónico.



Investigación de incidentes con análisis forense granular

Cuando se producen los incidentes, nuestros intuitivos paneles le permiten investigar la actividad anterior y las alertas. En ellos puede revisar los datos forenses específicos sobre las transacciones, como el usuario, la fecha y hora, la dirección IP, el dispositivo, el navegador, el agente de usuario, la ubicación, la amenaza y su puntuación, entre otros. Además, puede ver y analizar estos datos con gráficos interactivos e informes de registro. Y puede ordenar o filtrar los registros de actividad y de alertas, así como personalizar los informes de investigación. También es posible suscribirse para recibir sus informes una vez al día, a la semana o al mes. Si desea profundizar en el análisis, los datos forenses se pueden exportar de forma manual o a través de la integración con SIEM, que se ofrece a través de API REST.

Defensa de las cuentas de Microsoft 365 y Google Workspace con políticas flexibles

Con la información que obtiene de nuestros detallados análisis forenses, puede crear políticas de reparación flexibles basadas en distintos parámetros, como el usuario, ubicación, red, dispositivo o actividad sospechosa, entre otros. Por ejemplo, puede generar alertas de inicio de sesión para países incluidos en una lista negra o dispositivos que no cumplen las normativas de su empresa. Además, cuando se supervisa un servicio muy utilizado, como Microsoft 365 o Google Workspace, debe clasificar las alertas por prioridad con el fin de evitar la saturación. Con CAD, puede generar notificaciones de alerta según su gravedad. Es posible personalizar cada notificación o utilizar la plantilla predeterminada. Puede también vigilar más de cerca a los usuarios que están en riesgo o suspenderlos si se lleva a cabo un inicio de sesión sospechoso.

Los controles de acceso adaptables de CAD permiten aplicar en tiempo real medidas de seguridad centradas en las personas en función del riesgo, el contexto y la función del usuario. Puede bloquear automáticamente el acceso desde ubicaciones y redes de riesgo, así como por ciberdelincuentes conocidos. Además, puede aplicar controles basados en riesgo a los VAP y usuarios con muchos privilegios, como una autenticación más estricta y la implementación de VPN.

Despliegue rápido en cloud

Las plataformas cloud necesitan protección basada en la nube. Nuestra protección y nuestra arquitectura cloud a través de las API de Microsoft 365 y Google Workspace permiten realizar el despliegue con rapidez y disfrutar de las ventajas inmediatamente.

Al implementar controles de acceso adaptables, puede redirigir los inicios de sesión para apps cloud a nuestro gateway SAML. Este gateway negocia la autenticación federada entre cada proveedor de servicios y el proveedor de identidades. CAD admite cualquier servicio cloud aprobado por TI compatible con federación de SAML 2.0. Y para reforzar la autenticación, puede integrar su solución de autenticación multifactor o utilizar nuestra app de autenticación móvil, Proofpoint Mobile Access incluida con la solución CAD. Puede proteger a cientos de miles de usuarios en cuestión de días, no en semanas o meses.

Como líder del sector de protección frente a amenazas, utilizamos el entorno cloud para actualizar nuestro software a diario y adelantarnos a los ciberdelincuentes. Nuestro despliegue basado en cloud le ofrece además flexibilidad para proteger a los usuarios en cualquier red o dispositivo.

MÁS INFORMACIÓN

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