Proofpoint Account Takeover Protection

Detección y respuesta a la usurpación de cuentas cloud

Ventajas principales

- Detecte cuentas comprometidas de Microsoft 365, Google Workspace y Okta.
- Proteja frente a ataques de usurpación de cuentas que eluden la MFA.
- Acelere las investigaciones con una vista centralizada de actividades posteriores a la usurpación de cuentas.
- Reduzca el tiempo de permanencia de los atacantes mediante la suspensión de las cuentas y la obligación de cambiar las contraseñas.
- Revierta los cambios maliciosos en las reglas del buzón de correo y la configuración MFA.
- Elimine las aplicaciones externas sospechosas.

Este conjunto de soluciones forma parte de la plataforma Human-Centric Security, que mitiga las cuatro principales áreas de riesgo asociado a las personas.

Proofpoint Account Takeover (ATO Protection) amplía el poder de Proofpoint Targeted Attack Protection (TAP) a la detección de las cuentas cloud comprometidas y la protección de sus entornos de nube.

ATO Protection amplía el poder de Targeted Attack Protection (TAP) a la detección y protección de cuentas cloud comprometidas. ATO Protection utiliza inteligencia artificial (IA), inteligencia de amenazas correlacionada y análisis de comportamiento para detectar actividades sospechosas en toda la cadena de ataque. Detecta los cambios realizados por los atacantes tras el ataque y elimina su acceso. Revierte los cambios maliciosos en las reglas del buzón de correo y la configuración de la autenticación multifactor (MFA). También elimina aplicaciones sospechosas de terceros y pone en cuarentena y elimina archivos sospechosos.

ATO Protection proporciona informes detallados que muestran los inicios de sesión sospechosos, los usuarios atacados y los sistemas y configuraciones afectados. La integración con Proofpoint Identity Threat Defense le muestra el impacto potencial de la usurpación de una cuenta en otras cuentas y hosts con un solo clic. Estos conocimientos le ayudarán a detener los ataques antes de que se conviertan en incidentes graves que perjudiquen a su empresa.

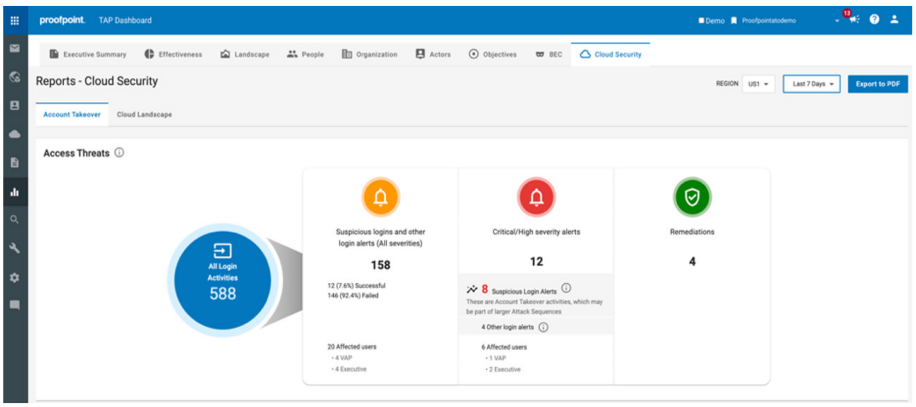

Figura 1: ATO Protection detecta inicios de sesión sospechosos, le ofrece información detallada que le ayuda a investigar las amenazas y revierte los cambios maliciosos.

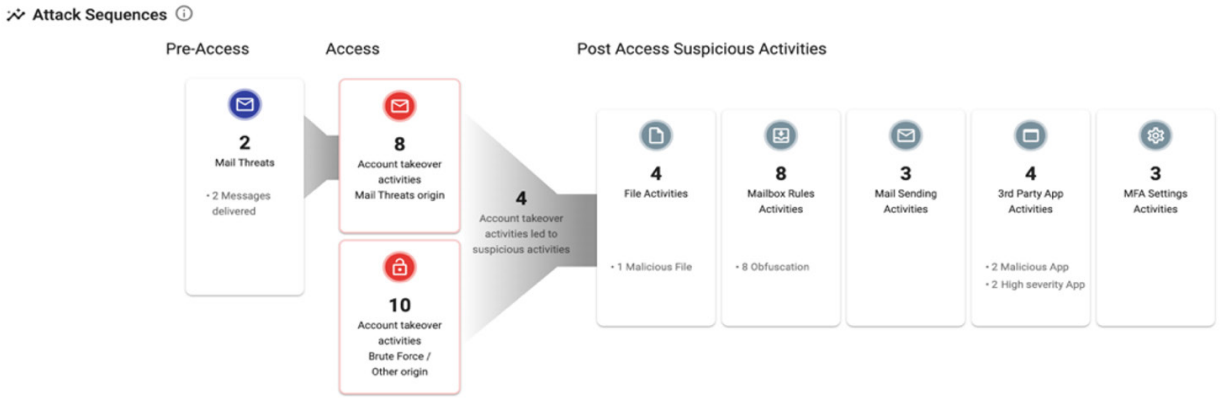

Figura 2: El informe Attack Sequence (Secuencia de ataque) muestra la actividad anterior y posterior al acceso para las cuentas afectadas.

Mejora de la detección y la visibilidad

ATO Protection detecta cuentas comprometidas y correo electrónico y otras actividades sospechosas en sus entornos de nube. Utiliza información sobre amenazas de más de 40 millones de usuarios supervisados en miles de organizaciones. Combina esta información con IA y análisis de comportamiento para detectar actividades inusuales en su entorno. Esta combinación de técnicas reduce las alertas de falsos positivos. Disfrutará de la tranquilidad de la precisión de las detecciones y una visión clara de toda la actividad de sus cuentas atacadas.

Cuando se usurpa una cuenta, ATO Protection añade alertas al panel de TAP. Una cronología del ataque muestra las actividades de adquisición de cuentas, la actividad de archivos y correo electrónico, los cambios en las reglas del buzón de correo y la configuración de la MFA y la incorporación de aplicaciones de terceros.

Aceleración de las investigaciones

ATO Protection muestra a sus analistas de seguridad la causa de una usurpación de cuenta y cómo limitar riesgos adicionales. La información se integra con el sistema y el proceso de investigación de TAP. De este modo, obtendrá información complementaria a la que proporciona TAP.

Una vista cronológica del ataque muestra las cuentas usurpadas. Puede hacer clic e investigar cada evento en la vista cronológica.

Asimismo, puede ver cómo se llevó a cabo el ataque y la ubicación del atacante. Además, puede obtener información sobre usuarios que hayan sufrido amenazas similares. Los análisis avanzados proporcionan cronologías de actividad detalladas por usuarios, direcciones IP, dominios y otros atributos. Esta completa información le ayudará a evaluar otros riesgos para su organización.

Respuesta automatizada

ATO Protection detecta y revierte los cambios maliciosos en las reglas del buzón de correo y la configuración MFA. Los ciberdelincuentes suelen cambiar las reglas del buzón de correo para ocultar su sistema y supervisarlo antes de lanzar ataques de phishing u otras acciones maliciosas. ATO Protection puede eliminar las aplicaciones externas maliciosas. Todas estas acciones limitan los daños a su organización y reducen el tiempo necesario para investigar y responder a las amenazas. Si su investigación muestra otra actividad maliciosa, puede tomar medidas para corregir las cuentas usurpadas. También puede eliminar los archivos que los atacantes han añadido a la cuenta de un usuario.

"Proofpoint Account Takeover Protection" era antes "Proofpoint TAP Account Takover".

MÁS INFORMACIÓN

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