proofpoint.

FICHA TÉCNICA

Proofpoint Account Takeover Protection

Detecte, analice y neutralice los intentos de usurpación de cuentas multifase

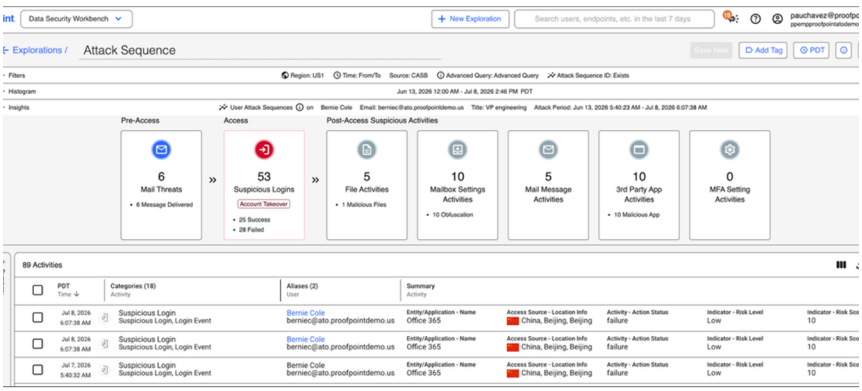
Características principales

- **Detección de alta precisión del compromiso de cuentas multifase.**
- **Investigaciones más ágiles gracias a una visibilidad unificada durante todo el ciclo de vida de los ataques.**
- **Reducción del tiempo de permanencia de los ciberdelincuentes mediante la automatización de la respuesta y la corrección.**
- **Prevención del fraude, la pérdida de datos y las interrupciones de la actividad empresarial derivadas de cuentas comprometidas.**
- **Refuerzo de la defensa en profundidad con Proofpoint Collaboration Security Prime.**

Proofpoint Account Takeover Protection ayuda a las organizaciones a detectar, analizar y contener las cuentas de usuario comprometidas durante todo el ciclo de vida de una toma de control de cuenta (ATO), desde los indicadores previos al acceso y los que confirman que la cuenta se ha visto comprometida hasta las actividades ciberdelictivas posteriores al acceso.

Optimizada por la inteligencia de amenazas de Proofpoint Nexus® AI, Proofpoint Account Takeover Protection permite detectar con una fiabilidad excepcional los casos confirmados de cuentas comprometidas, al tiempo que ofrece una visibilidad completa del comportamiento de los ciberdelincuentes. Los equipos de seguridad pueden evaluar rápidamente el alcance de un incidente, agilizar las investigaciones y contener las amenazas antes de que den lugar a ataques BEC (Business Email Compromise), robos de datos, desplazamientos laterales u otros ataques que afecten a la actividad empresarial.

Como parte de Proofpoint Collaboration Security Prime, Proofpoint Account Takeover Protection se integra con Threat Protection Workbench y Threat Interaction Map para ampliar el alcance de las investigaciones más allá de una única cuenta comprometida. La correlación de las cuentas comprometidas con las amenazas por correo electrónico, las interacciones de los usuarios y la actividad de los ciberdelincuentes ayuda a los equipos de seguridad a comprender mejor la campaña de ataque. Esto permite acelerar las investigaciones, fundamentar mejor las decisiones sobre las medidas a adoptar y reforzar la corrección.



1. Figura 1. Obtenga una visibilidad completa de todo el ciclo de vida de los ataques ATO, desde las actividades previas al acceso hasta las posteriores.

Detección extremadamente fiable de los ataques ATO

Optimizada por Proofpoint Nexus AI, la solución Proofpoint Account Takeover Protection permite una detección extremadamente fiable de los casos confirmados de compromiso de cuentas en Microsoft 365, Google Workspace y Okta.

Mediante el análisis continuo de la actividad de los usuarios durante todo el ciclo de vida de las usurpaciones de cuentas (desde los indicadores previos al acceso hasta el comportamiento de los ciberdelincuentes tras acceder a ellas), Proofpoint Account Takeover Protection detecta con un alto grado de fiabilidad los casos confirmados de cuentas comprometidas y clasifica las detecciones según la gravedad del riesgo: crítico, alto o moderado. Cada detección incluye los indicadores de comportamiento y las pruebas en las que se basa, lo que permite a los analistas comprender rápidamente por qué se considera que una cuenta está comprometida, priorizar la respuesta y actuar con confianza.

Visibilidad completa del ataque

Una vez confirmada la usurpación de la cuenta, la protección contra la usurpación de cuentas ofrece una visibilidad completa de la secuencia del ataque, lo que permite a los equipos de seguridad comprender cómo se desarrolló y qué hizo el atacante tras acceder a ella.

Los análisis forenses exhaustivos revelan las actividades posteriores al acceso, como la manipulación de cuentas de correo electrónico, el uso de reglas maliciosas en la bandeja de entrada, el abuso de OAuth, los cambios de privilegios, el phishing interno, la actividad sospechosa relacionada con el correo electrónico y las técnicas de persistencia. Esto permite a los analistas determinar rápidamente el alcance, la sofisticación y la magnitud del ataque. Al reconstruir la secuencia del ataque e identificar a los usuarios y recursos afectados, Proofpoint Account Takeover Protection agiliza las investigaciones, permite tomar decisiones de respuesta mejor fundamentadas y hace más eficaz la corrección.

Respuesta automatizada frente a amenazas

Proofpoint Account Takeover Protection ayuda a las empresas a contener rápidamente las amenazas activas mediante correcciones automatizadas que bloquean el acceso de los ciberdelincuentes y aceleran la recuperación. Entre las medidas de respuesta figuran exigir el cambio de contraseñas, restablecer las contraseñas de los usuarios, revocar las sesiones activas, eliminar las reglas maliciosas de los buzones de correo electrónico, revocar las aplicaciones OAuth de terceros no autorizadas y aplicar otras medidas correctivas para eliminar la presencia de los ciberdelincuentes y restablecer la integridad de las cuentas.

Al automatizar las medidas críticas de contención, los equipos de seguridad pueden reducir el tiempo de permanencia de los ciberdelincuentes, limitar sus desplazamientos laterales, minimizar las interrupciones de la actividad empresarial y acelerar la recuperación cuando una cuenta se ve comprometida.

Defensa en profundidad con Proofpoint Collaboration Security Prime

Como parte de Proofpoint Collaboration Security Prime, Proofpoint Account Takeover Protection va más allá de la protección frente a las usurpaciones de cuentas y ofrece una defensa coordinada durante todo el ciclo de vida de los ataques dirigidos contra las personas. Mientras que Proofpoint Account Takeover Protection detecta, analiza y contiene las cuentas comprometidas, Proofpoint Prime refuerza la protección bloqueando las amenazas antes de que se produzca el compromiso, correlacionando los ataques en los canales de mensajería y colaboración, mejorando el comportamiento de los usuarios mediante una formación adaptativa y proporcionando investigaciones y respuestas unificadas a través de Threat Protection Workbench y Threat Interaction Map.

En conjunto, estas funcionalidades sustentan una estrategia de defensa en profundidad que ayuda a las organizaciones a prevenir ataques, mitigar las amenazas activas, reforzar la resiliencia de los usuarios y mejorar continuamente su nivel de seguridad mediante una plataforma integrada.

Más información en **proofpoint.com/es**

proofpoint.