Proofpoint Shadow

Acabe con los escalamientos de privilegios y desplazamientos laterales en tiempo real

Ventajas principales

- Detección temprana de ataques e investigación exhaustiva de las amenazas.
- Reducción de los falsos positivos en el SOC, con alertas de alta fiabilidad.
- Tecnología sin agentes que se despliega fácilmente con poca intervención del equipo de TI.
- Protección continua que se ajusta dinámicamente según los cambios en el entorno de TI.
- Capacidad de ampliación demostrada en redes de más de un millón de endpoints.
- Solución que cubre el vacío que deja la detección de amenazas basada en firmas y anomalías.

Más del 90 % de los ciberataques implican el uso de identidades poco seguras. Los ciberdelincuentes han adaptado sus estrategias y dirigen sus ataques a identidades con privilegios, en lugar de intentar acceder directamente a los sistemas. Este cambio ha provocado un incremento de los ataques de ransomware y fugas de datos que logran su objetivo. Al centrarse en las identidades vulnerables, los atacantes consiguen acortar el tiempo de ataque de meses a días, o incluso horas.

Pero Proofpoint puede ayudarle. Nuestra potente solución Shadow transforma sus endpoints en una red de trampas que impide que los atacantes puedan desplazarse lateralmente por su entorno sin ser detectados. Proofpoint Shadow, que forma parte de la plataforma Proofpoint Identity Threat Defense, captura indefectiblemente a los ciberdelincuentes basándose en sus interacciones con las que en apariencia son vías legítimas en los endpoints, pero que en realidad son nuestras trampas.

A diferencia de otras herramientas, Shadow no depende de análisis basados en firmas ni de comportamientos. Tampoco utiliza agentes ni honeypots que los atacantes puedan aprovechar. En la arquitectura sin agentes de Shadow, los engaños actúan con discreción, pasando inadvertidos para los ciberdelincuentes. Shadow ha garantizado la protección en más de 160 ejercicios de equipo rojo para algunas de las principales organizaciones de seguridad del mundo, incluidas Microsoft, Mandiant, el Departamento de Defensa de Estados Unidos y Cisco.

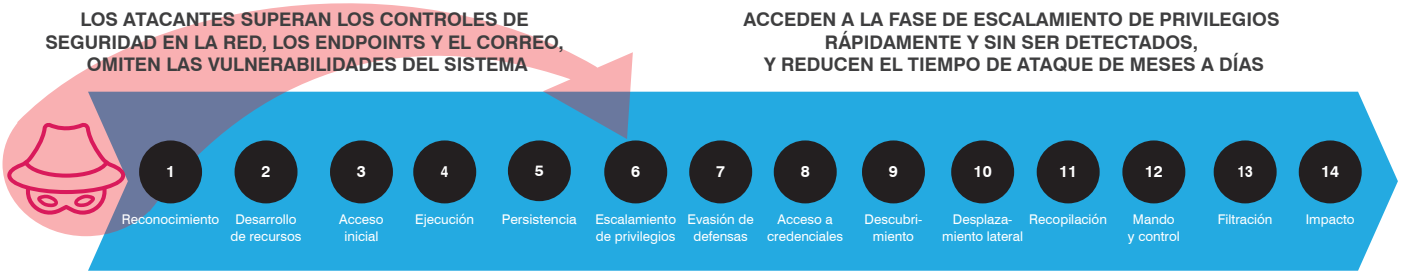

Figura 1. Actualmente los atacantes se centran en las identidades vulnerables como vía de acceso clave por la cadena de ataque.

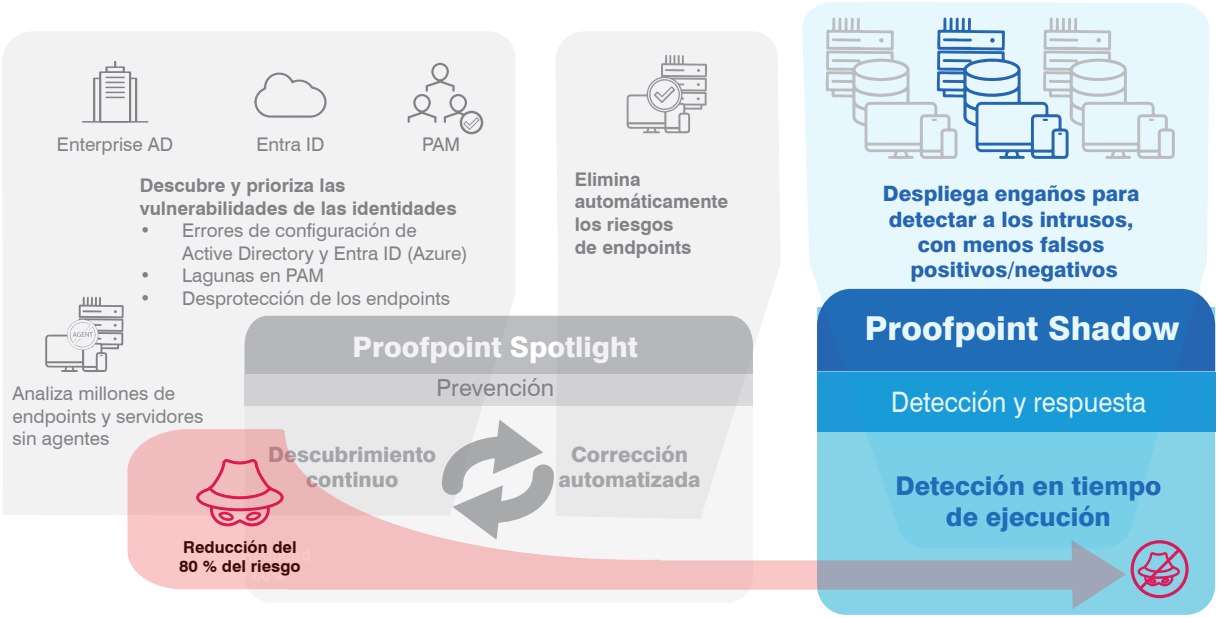

Figura 2. Shadow, que forma parte de la plataforma Proofpoint Identity Threat Defense, crea una red de engaños que detectan y alertan sobre el desplazamiento lateral del atacante en sus redes.

Del enfoque probabilista a la detección determinista

Las amenazas se pueden detectar de muchas formas y la respuesta también puede ser distinta. Se pueden buscar patrones específicos, por ejemplo, firmas, o bien se puede analizar cómo se comporta un atacante potencial. Las herramientas convencionales no suelen detectar ataques graves, como cuando los atacantes escalan los privilegios o se desplazan lateralmente por la red sin ser descubiertos. Y estos fallos de detección pueden ser el inicio de la usurpación de cuentas, la propagación de ransomware o el robo de datos. Los equipos de seguridad necesitan un enfoque más avanzado y fiable para adelantarse a este tipo de ataques.

Shadow ofrece un enfoque determinista que usa engaños distribuidos para conseguir que los atacantes interactúen con ellos en la cadena de ataque y así poder seguir el rastro de sus actividades. Estas trampas están escondidas en lo más profundo de los endpoints. Presentan el aspecto y el funcionamiento de los recursos reales (archivos, sesiones RDP, conexiones de base de datos, mensajes de correo electrónico, scripts y demás) que los ciberdelincuentes intentan encontrar. Cuando un atacante interacciona con un engaño, Shadow envía al equipo de seguridad una alerta en tiempo real con datos forenses. El equipo puede entonces utilizar esta información para tomar decisiones inteligentes encaminadas a detener el ataque y proteger a la empresa para evitar que sufra daños.

Detección y protección sin agente

El exclusivo enfoque de Shadow sin agentes y sin archivos binarios ayuda tanto a los administradores de TI como a los equipos de seguridad. La automatización inteligente y la reducida huella en las operaciones minimizan el impacto en TI. Además, a diferencia de lo que ocurre con las herramientas de seguridad que dependen de agentes de software, los atacantes no pueden inhabilitar ni evitar Shadow.

Más de 75 técnicas de engaño

Shadow emplea más de 75 técnicas activas de engaño. Crea recursos falsos, como archivos y recursos de archivos compartidos, conexiones de base de datos, conexiones FTP y RDP/SSH, historiales y URL del navegador, credenciales de Windows, sesiones de red, mensajes de correo electrónico, scripts e incluso chats de Teams, que parecen atractivos para los ciberdelincuentes, pero que son trampas ocultas. Estas técnicas de engaño funcionan juntas para capturar al atacante en el acto, tanto si el compromiso se inicia dentro como fuera del entorno.

Con Shadow, los equipos de seguridad pueden automatizar la creación de cientos de archivos falsos de Word y Excel que tienen el aspecto de verdaderos; incluso pueden incluir el logotipo y el membrete de su empresa. Los datos falsos de estos documentos disparan las alarmas de los administradores de seguridad si un atacante intenta utilizarlos para conseguir acceso a otros recursos.

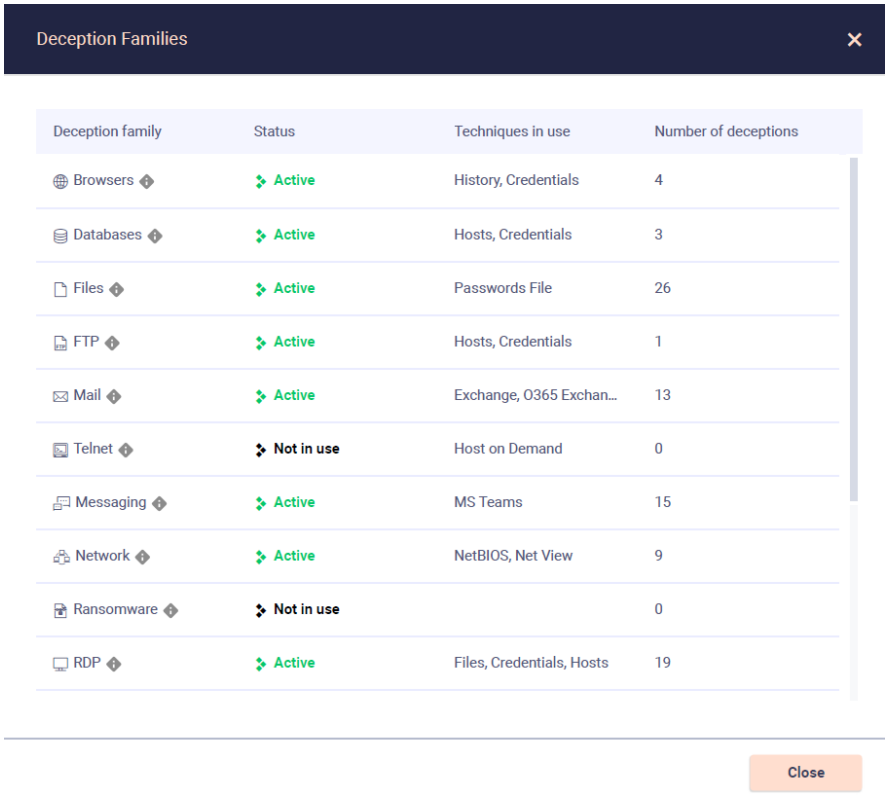

Figura 3. La interfaz de usuario de Proofpoint Shadow

Engaños automatizados personalizados para cada endpoint

El sistema de automatización inteligente de Shadow crea trampas realistas y creíbles para los ciberdelincuentes, y se puede adaptar y ampliar fácilmente, sin cargar de trabajo al equipo de seguridad. Shadow analiza el estado del endpoint, diseña engaños adaptados a cada máquina y permite desplegarlos con solo un clic. Además, la solución se encarga del proceso continuo de ajuste y gestión de los engaños.

Una visión desde la perspectiva del atacante

La consola de administración de Shadow proporciona gran cantidad de información forense sobre la actividad de los atacantes. Ofrece a los equipos de seguridad datos importantes para determinar lo cerca que están los ciberdelincuentes de sus recursos esenciales. Además, puede mostrar una cronología completa de lo que estaban haciendo cuando cayeron en las trampas y los analistas de seguridad pueden observar cómo se ven los engaños desde el punto de vista de los atacantes.

MÁS INFORMACIÓN

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

ACERCA DE PROOFPOINT

Proofpoint, Inc. es una compañía líder en ciberseguridad y cumplimiento de normativas que protege el activo más importante y de mayor riesgo para las organizaciones: las personas. Gracias a una suite integrada de soluciones basadas en cloud, Proofpoint ayuda a empresas de todo el mundo a detener las amenazas dirigidas, a salvaguardar sus datos y a hacer a los usuarios más resilientes frente a ciberataques. Compañías líderes de todos los tamaños, entre las que se encuentra el 75 % del Fortune 100, confían en las soluciones de Proofpoint para su seguridad centrada en personas y su cumplimiento regulatorio, mitigando los riesgos más críticos en sus sistemas de correo electrónico, cloud, redes sociales y web. Encontrará más información en **www.proofpoint.com/es**.