Proofpoint Spotlight

Descubre, prioriza y corrige automáticamente las vulnerabilidades de las identidades antes de que los atacantes puedan aprovecharlas

Ventajas principales

- Descubrimiento del riesgo relacionado con las identidades en varias etapas de la cadena de ataque.
- Visibilidad de las identidades que incluye: Active Directory, Entra ID (antes Azure AD), PAM, endpoints, LAPS.
- Una lista automática de las vulnerabilidades de las identidades en los endpoints, organizadas por prioridades.
- Corrección manual o automática de las vulnerabilidades, incluidas las de administradores en la sombra.
- Visibilidad de los riesgos en filiales y entidades de nueva adquisición, con un mapa de los dominios y relaciones de confianza de las empresas.
- Informes inteligentes sobre las tendencias de los riesgos a lo largo del tiempo para mejorar la seguridad de sus identidades.

El robo y abuso de credenciales es una preocupación muy presente y cada vez mayor. Los atacantes que antes se centraban en amenazas basadas en los sistemas ahora hacen uso de las identidades. Para llevar a cabo estos ataques bastan horas o incluso minutos. Además, no dejan rastro de compromisos ni malware.

Incluso cuando emplean soluciones de gestión de cuentas con privilegios (PAM) y autenticación multifactor (MFA), 1 de cada 6 endpoints empresariales sigue teniendo identidades vulnerables. Estos endpoints son objetivos de preferencia para los ciberdelincuentes. El ransomware y otras amenazas dirigidas utilizan las identidades con privilegios como medio para conseguir un fin.

Proofpoint Spotlight ayuda a reducir el riesgo de que sus identidades se utilicen en su contra. Esta solución, que forma parte de la plataforma Proofpoint Identity Threat Defense, proporciona descubrimiento continuo y exhaustivo de vulnerabilidades en las identidades y neutraliza automáticamente estas amenazas. Spotlight aborda las amenazas para las identidades antes de que se conviertan en un ataque a gran escala.

Los ingenieros de defensa nacional han desarrollado Spotlight para ayudar a los equipos a priorizar las tareas de neutralización automática de las amenazas. El objetivo de las alertas es prevenir el impacto en el negocio. Sin embargo, el aumento del número de alertas ha generado una sobrecarga que los equipos de seguridad deben filtrar.

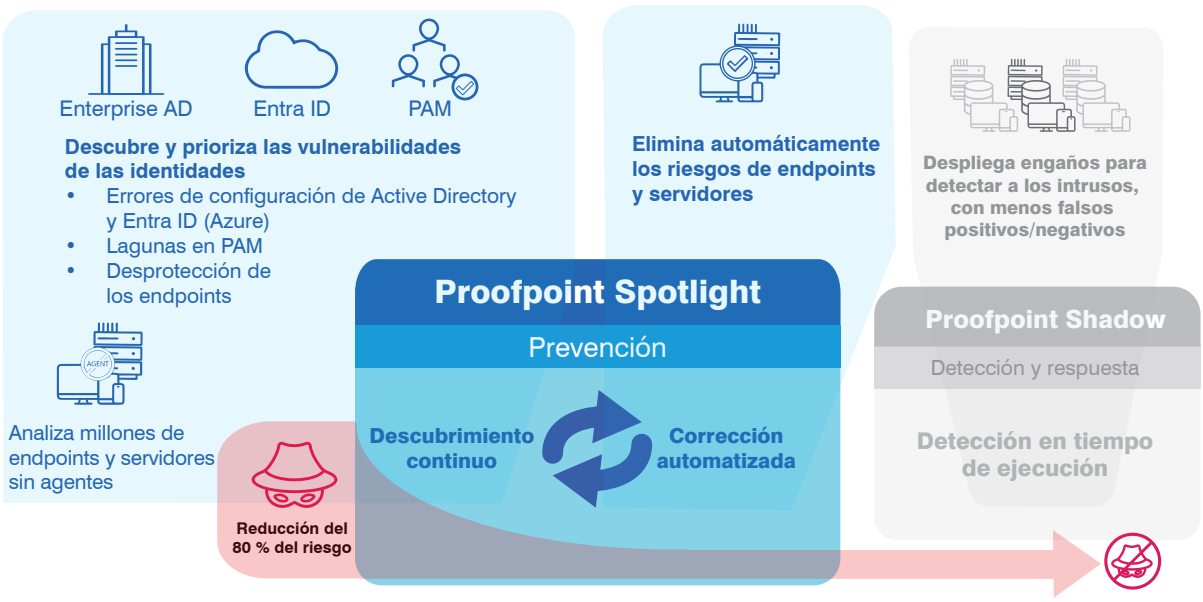

Figura 1. Proofpoint Spotlight, que forma parte de Proofpoint Identity Threat Defense, ofrece descubrimiento continuo y corrección de las vulnerabilidades de identidades con privilegios y las infracciones de políticas.

Cómo abusan los ciberdelincuentes de las identidades con privilegios

Cuando los atacantes aterrizan inicialmente en un host, muy rara vez se trata de su objetivo final. En la mayoría de los ataques, intentan escalar los privilegios. A continuación, se desplazan lateralmente por el entorno para alcanzar su objetivo sin ser detectados. Para ello, emplean herramientas como Bloodhound, Cobalt Strike, Mimikatz y ADFind con el fin de sacar partido rápidamente de las credenciales con privilegios y ocultar su presencia.

Según nuestras investigaciones, más del 90 % de las organizaciones sufrieron un ataque relacionado con la identidad el año pasado. Y los ataques de ransomware alcanzan niveles de récord. Este incremento se debe a múltiples motivos. Uno de ellos es que desplegar los sistemas de administración de acceso e identidades es muy complejo. Las identidades cambian continuamente y las organizaciones carecen de visibilidad total de las brechas de su entorno.

Otros de los motivos son:

- Una insuficiente o inadecuada configuración de PAM y una deficiente administración de las credenciales de: servicio o cuentas, acceso local o de administrador y con privilegios o para dominios.
- La creación no intencionada de cuentas de administrador en la sombra.
- La finalización incorrecta de sesiones de RDP.
- Aplicaciones de los usuarios, como navegadores, SSH, FTP, PuTTY y bases de datos, que guardan las credenciales y los tokens de acceso a la nube en la caché de los endpoints.

Ejemplo real: ataque a una empresa de seguros

Un ciberdelincuente utilizó la técnica de relleno de credenciales (o *credential stuffing*) para acceder a una red a través de un protocolo RDP. El atacante aprovechó credenciales robadas para el acceso inicial.

A partir de ahí, escaló sus privilegios hasta administrador de dominio; se cifraron datos esenciales y una parte de ellos se filtraron. La organización pagó un rescate de 40 millones de dólares para recuperarse del ataque.

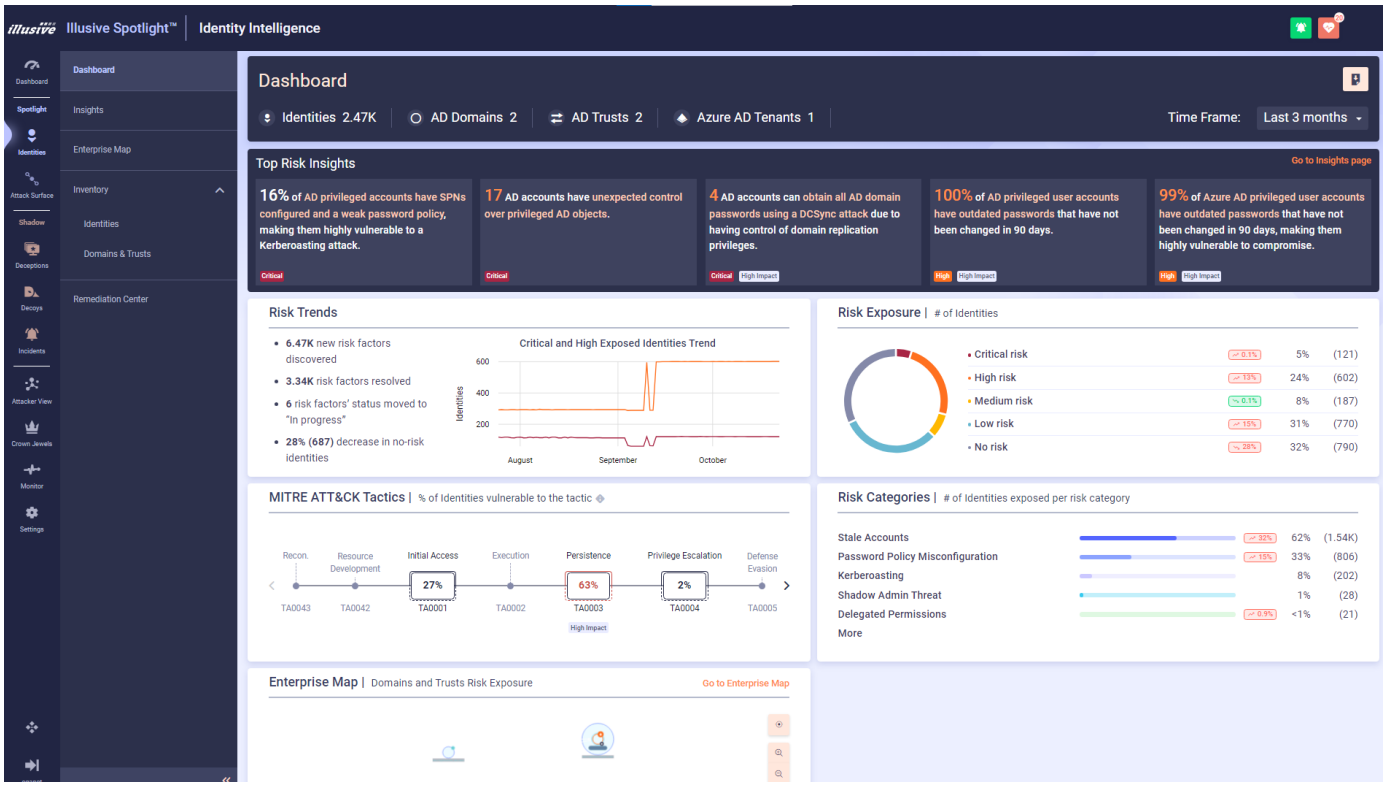

Figura 2. El panel de riesgos para las identidades de Proofpoint Spotlight.

Localice, priorice y corrija las identidades vulnerables

Spotlight identifica las brechas existentes entre las políticas de seguridad de las identidades y los entornos reales. La solución analiza los siguientes sistemas para proporcionar visibilidad total y priorización de las vulnerabilidades actuales de las identidades:

- **Estructuras de directorio.** Active Directory y Entra ID (antes Azure AD).
- **Soluciones PAM.** CyberArk y Delinea Centrify.
- **Endpoints.** Clientes y servidores.
- **Tareas.**

Proofpoint Spotlight ayuda a prevenir ataques eliminando las vulnerabilidades de las identidades que sirven a los ciberdelincuentes para cometer delitos que pueden llegar a convertirse en ataques de graves consecuencias.

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**.