proofpoint.

Plataforma Proofpoint Identity Threat Defense

Impida el escalamiento de privilegios y el desplazamiento lateral

Productos

- Proofpoint Shadow
- Proofpoint Spotlight

Ventajas principales

- Identifique, priorice y corrija las vulnerabilidades relacionadas con la identidad.
- Conozca los riesgos asociados a las identidades con privilegios y las vías de ataque disponibles en su entorno.
- Consiga visibilidad de las vulnerabilidades asociadas a las identidades, con cobertura para Active Directory, Entra ID, AWS Identity Center, Okta, PAM, endpoints y LAPS.
- Corrija automáticamente las vulnerabilidades de las identidades expuestas en los endpoints.
- Garantice la detección temprana de ataques y acelere la investigación de amenazas.
- Utilice tecnología sin agentes imposible de eludir para los ciberdelincuentes.
- Corrija los fallos que generan la detección de amenazas basada en firmas y en el comportamiento.
- Aproveche la integración con Proofpoint TAP, TAP ATO y NPRE.
- Disponible para despliegue SaaS.

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

Los ataques son mucho más sofisticados y dirigidos que nunca. Y las soluciones destinadas a proteger frente a ellos no están a la altura de la amenazas[1]. Las tendencias sugieren que los ciberdelincuentes están estandarizando sus tácticas, técnicas y procedimientos para centrarse en las identidades. Sin embargo, las organizaciones todavía no son capaces de romper la cadena de ataque de manera fiable. Las identidades son una parte fundamental de la superficie de ataque, y hay que prestarles más atención.

La plataforma Proofpoint Identity Threat Defense proporciona protección integral contra las amenazas a la identidad. Incluye los componentes Proofpoint Shadow y Proofpoint Spotlight, e incluye funciones de identificación y corrección de vulnerabilidades de las identidades, así como la detección basada en engaños y sin agente y la recopilación de datos forenses. La plataforma le permite descubrir, priorizar y corregir las identidades vulnerables. También le ayuda a detectar y responder a las amenazas activas.

Crisis de identidad

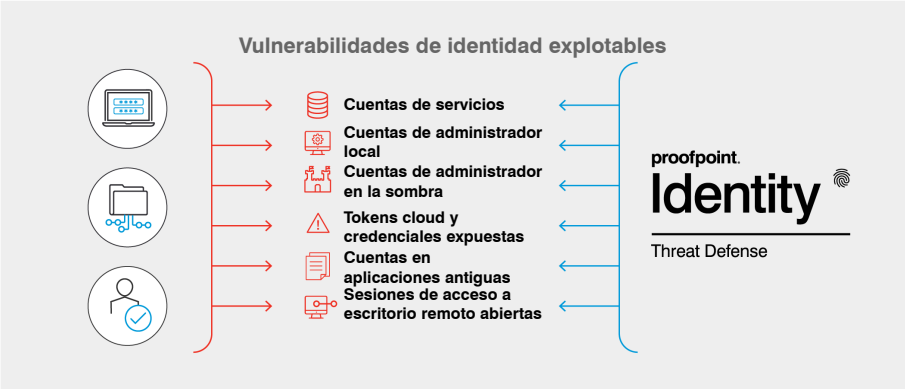

Figura 1: Proofpoint Identity Threat Defense y las vulnerabilidades de identidad explotables.

1 Algunas de estas soluciones incluyen la gestión de identidades y acceso (IAM), la autenticación multifactor (MFA), la detección y respuesta para endpoints (EDR), los sistemas de administración de información y eventos de seguridad (SIEM) y la detección y respuesta ampliadas (XDR).

La mayoría de las organizaciones despliegan Active Directory. Desafortunadamente, el 79 % ha sufrido un incidente relacionado con la identidad en los últimos dos años. Según el informe DBIR de Verizon, el 94 % de los ataques que consigue su objetivo utilizaron Active Directory e identidades con privilegios para escalar sus privilegios. Los atacantes utilizan un amplia variedad de herramientas. Bloodhound, Cobalt Strike, Mimikatz y ADFind son solo algunas de ellas. Estas herramientas les ayudan a aprovechar las identidades con privilegios rápidamente, y complican enormemente la detección de sus ataques.

La investigación de Proofpoint muestra que 1 de cada 6 endpoints empresariales, tanto clientes como servidores, contiene vulnerabilidades relacionadas con las identidades. Y esto se produce incluso cuando hay desplegadas soluciones de gestión de identidades y acceso (IAM) tradicionales. Los ciberdelincuentes aprovechan estas vulnerabilidades para conseguir acceso a privilegios de administrador. Cuando se infiltran inicialmente en un host, muy rara vez se trata de su objetivo final. Buscan desplazarse lateralmente dentro de la red para buscar los activos de TI más críticos, o de nivel 0. Una vez lo han conseguido, pueden filtrar datos, o lanzar ataques de ransomware.

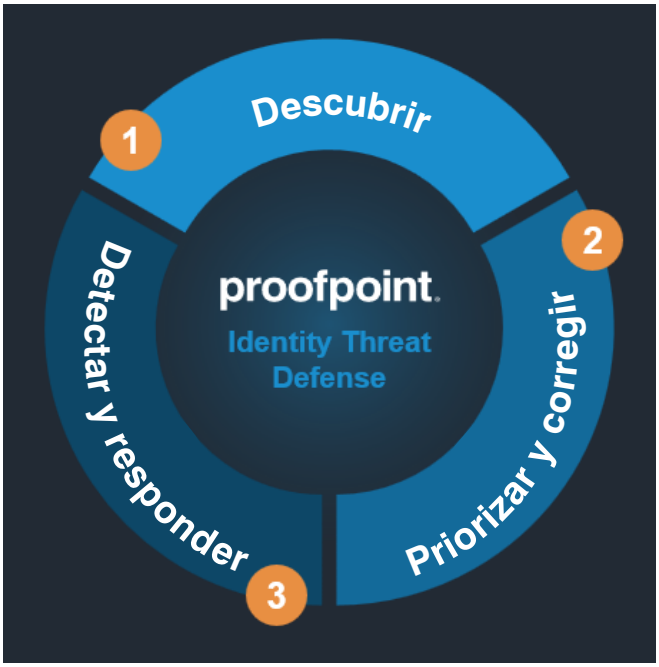

Figura 2: Plataforma Proofpoint Identity Threat Defense.

Muchas riesgos de identidad son el resultado de los procesos operativos y de TI normales de las empresas, por ejemplo:

- **Nombres de usuario y contraseñas.** Las aplicaciones de los usuarios suelen guardar en caché esta información en los endpoints, como los navegadores, SSH, FTP, PuTTY y bases de datos. Las soluciones PAM no protegen estas credenciales.
- **Credenciales de administrador de dominio.** Estas identidades se conservan en la memoria del sistema después de una sesión de asistencia remota, o se almacenan en caché en una cuenta de servicio no protegida.
- **Privilegios en la sombra.** La configuración de objetos y grupos del directorio de identidades en Active Directory puede ser muy compleja. Como resultado, a los usuarios se les pueden asignar involuntariamente privilegios en la sombra excesivos.

Visibilidad integral de la seguridad de las identidades

Los ataques que tienen éxito consiguen explotar los fallos de administración y protección. Nuestra plataforma ayuda a los responsables de seguridad a ver y proteger estas carencias. Les permite:

1. **Descubrir.** Obtenga descubrimiento y visibilidad continuos de las vulnerabilidades relacionadas con las identidades en AD, Entra ID, AWS Identity Center, Okta y en los endpoints.
2. **Priorizar y corregir.** Acceda a una lista de vulnerabilidades ordenadas por las que necesitan mayor atención. Estos riesgos aparecen en un espectro que va de lo no crítico a lo urgente. Permite la corrección automatizada de las vulnerabilidades de las identidades directamente desde la plataforma. Puede definir reglas de excepción que sean conformes con sus políticas de seguridad.
3. **Detectar y responder.** Vea a los atacantes activos en su entorno. Gracias a engaños sin agente, puede detectar distintas actividades, como el Kerberoasting, el volcado de contraseñas, el abuso de cuentas con privilegios, etc. Puede automatizar la recopilación de datos forenses para ayudar a orientar la respuesta de su organización a las amenazas activas.

MÁS INFORMACIÓN

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

0213-003-06-04 6/24