FOLLETO DE LA SOLUCIÓN

Sophos ITDR

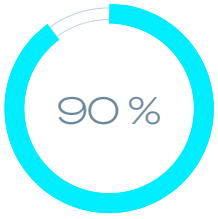
Neutralice las amenazas basadas en la identidad antes de que puedan afectar a su negocio

Sophos Identity Threat Detection and Response (ITDR) detiene los ataques basados en la identidad mediante la supervisión continua de su entorno en busca de riesgos de identidad y errores de configuración, al tiempo que proporciona información procedente de la Web Oscura sobre credenciales vulneradas.

Amenazas a la identidad: un problema de seguridad que va en aumento

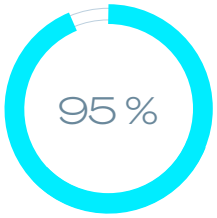
Los controles y el acceso basados en el usuario son clave en el panorama actual de TI y ciberseguridad, y el cambio a la nube y al teletrabajo ha aumentado la complejidad de supervisar y proteger la superficie de ataque relacionada con la identidad. Los adversarios utilizan identidades vulneradas, deficiencias en la infraestructura y errores de configuración para obtener acceso no autorizado a datos y sistemas confidenciales. Como resultado, la detección del uso indebido de identidades y el bloqueo de los ataques basados en la identidad son cada vez más importantes para garantizar la eficacia de las operaciones de seguridad.

Las cifras hablan por sí solas

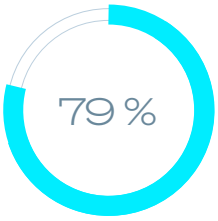


de las organizaciones sufrieron al menos una filtración relacionada con la identidad en el último año.[1]

Coste medio de una filtración de datos.[2]



de los entornos de Microsoft Entra ID tienen errores de configuración críticos.[3]



de las filtraciones de datos están relacionadas con la identidad.[4]

Ventajas

- **Mejore la visibilidad** con una vista centralizada de las identidades en todos sus sistemas.
- **Identifique rápidamente** los riesgos basados en la identidad y los errores de configuración, con recomendaciones prácticas.
- **Monitorice continuamente** los cambios en la postura de identidad.
- **Escanee la Web Oscura** en busca de credenciales filtradas.
- **Detecte actividades potencialmente maliciosas** de amenazas internas y direcciones IP y ubicaciones desconocidas.
- **Responda a las amenazas a la identidad** con rapidez y precisión.
- **Se integra con Sophos MDR** para ofrecer una investigación y respuesta expertas a las amenazas basadas en la identidad.

Solución Sophos ITDR

Sophos ITDR previene los ataques basados en la identidad: supervisa continuamente su entorno en busca de riesgos de identidad y errores de configuración, un problema que afecta al 95 % de las organizaciones, al tiempo que proporciona información procedente de la Web Oscura sobre credenciales vulneradas. Identifique sus riesgos de identidad en cuestión de minutos (en vez de días con las soluciones tradicionales) y evalúe su superficie de ataque relacionada con la identidad a lo largo del tiempo.

Reduzca la superficie de ataque relacionada con la identidad

Sophos ITDR escanea continuamente su entorno de Microsoft Entra ID para identificar rápidamente errores de configuración y lagunas de seguridad basadas en la identidad y priorizar los problemas que requieren atención inmediata. Los ciberdelincuentes aprovechan esas vulnerabilidades para causar daños, aumentando sus privilegios y llevando a cabo ataques. Aborde rápidamente los riesgos, incluyendo las deficiencias en las políticas de acceso condicional, las cuentas huérfanas, las cuentas con demasiados privilegios y las aplicaciones poco seguras.

Minimice el riesgo de filtración o robo de credenciales

Según la información recopilada por la Counter Threat Unit (CTU) de Sophos X-Ops, el número de credenciales robadas puestas a la venta en uno de los mayores mercados de la Web oscura se ha duplicado con creces en el último año. Sophos ITDR detecta y responde a las amenazas de identidad que eluden los controles tradicionales de seguridad de la identidad; de hecho, protege contra el 100 % de las técnicas de acceso a credenciales de MITRE ATT&CK.[5] La solución identifica comportamientos de usuario de riesgo, como patrones de inicio de sesión inusuales, y avisa del uso de credenciales robadas o vulneradas para obtener acceso a sus sistemas.

Qué ofrece Sophos ITDR

Catálogo de identidades
Mejore la visibilidad con una vista centralizada de las identidades en todos sus sistemas.

Escaneado continuo de la postura de identidad
Monitorice constantemente su entorno de Microsoft Entra ID para identificar errores de configuración y lagunas de seguridad.

Supervisión de credenciales vulneradas en la Web Oscura
Busque credenciales filtradas en la Web Oscura y en bases de datos de filtraciones de seguridad.

Análisis del comportamiento de los usuarios
Busque actividades anómalas relacionadas con credenciales robadas o amenazas internas.

Detección avanzada de amenazas a la identidad
Identifique actividades sospechosas que sean indicativas de técnicas adversarias específicas en las primeras fases de la cadena de ataque.

Acciones de respuesta a amenazas
Responda con rapidez y precisión: fuerce el restablecimiento de contraseñas, bloquee las cuentas que presentan comportamientos sospechosos y mucho más.

"Sophos ITDR ha mejorado mucho la visibilidad de nuestros riesgos de identidad. Tener una vista centralizada dentro de nuestra plataforma XDR nos permite integrar en todos nuestros programas de seguridad los riesgos relacionados con la identidad y con errores de configuración que Sophos ITDR ha detectado, lo que mejora la postura general de ciberseguridad de la organización y reduce el riesgo".

– Responsable de seguridad de la información, servicios financieros

"Sophos ITDR identifica riesgos en áreas que solían preocuparme en Azure y en el ecosistema de Microsoft, como las lagunas en las políticas de acceso condicional y las aplicaciones poco seguras o con demasiados privilegios".

– Responsable sénior de seguridad de la información

Integración con Sophos MDR

Sophos ITDR se integra completamente con Sophos MDR, el servicio de detección y respuesta gestionadas que goza de mayor confianza en todo el mundo. Esta potente combinación permite a los expertos en seguridad de Sophos supervisar, investigar y responder a las amenazas basadas en la identidad en su nombre:

- Sophos ITDR crea automáticamente casos MDR para las detecciones de amenazas a la identidad y los elementos de alto riesgo.
- Los analistas de seguridad de Sophos MDR investigan los casos y ejecutan acciones de respuesta para neutralizar las amenazas.

Ejemplo: credenciales filtradas en la Web Oscura

- Sophos ITDR identifica las credenciales de un usuario a la venta en un conocido mercado de la Web Oscura.
- Los analistas de Sophos MDR pueden bloquear la cuenta del usuario y forzar un restablecimiento de contraseña.

Ejemplo: uso de credenciales robadas

- Sophos ITDR identifica inicios de sesión sospechosos desde países, dispositivos y direcciones IP no vistos anteriormente.
- Los analistas de Sophos MDR pueden bloquear la cuenta del usuario afectado y finalizar todas las sesiones activas.

Sophos ITDR + Microsoft Entra ID: la combinación perfecta

Microsoft Entra ID es una herramienta de gestión de identidad y acceso (IAM) que proporciona gestión de identidades y grupos, controles RBAC, gestión del acceso con privilegios y políticas de acceso condicional. Sophos ITDR, que se incorpora en una consola unificada para detectar y neutralizar amenazas y riesgos relacionados con la identidad, va más allá de las capacidades básicas de IAM: ofrece higiene de la identidad, evaluación de la postura, monitorización de la Web Oscura, detección de amenazas avanzadas y mucho más. **La combinación de Entra ID y Sophos ITDR proporciona la cobertura de seguridad de la identidad más completa para su empresa.**

Licencias sencillas

Sophos ITDR es fácil de desplegar, usar y adquirir. El sencillo sistema de licencias de suscripción, basado en el número de usuarios y servidores de su organización, ofrece precios predecibles. Añada Sophos ITDR a la solución Sophos XDR o al servicio Sophos MDR, según le convenga.

- **Complemento del servicio Sophos Managed Detection and Response (MDR):** los expertos en seguridad de Sophos supervisan, investigan y responden a las amenazas basadas en la identidad en su nombre.
- **Complemento del producto Sophos Extended Detection and Response (XDR):** con Sophos ITDR, su equipo interno puede sacar partido de las herramientas de detección, investigación y respuesta basadas en IA de Sophos.

Gartner

Distinción Gartner® Peer Insights™ Customers' Choice 2025 para la detección y respuesta ampliadas (XDR).

Líder en el informe general G2 Grid® para detección y respuesta ampliadas (XDR) y detección y respuesta gestionadas (MDR).

MITRE | ATT&CK® Evaluations

Sólidos resultados en las evaluaciones de MITRE ATT&CK® para productos empresariales y servicios gestionados.

FROST & SULLIVAN

Líder en el informe Frost Radar™ 2025 de Frost & Sullivan para la detección y respuesta gestionadas.

Para obtener más información, visite

es.sophos.com/ITDR

1 - Estudio de la Identity Defined Security Alliance (IDSA), 2024.
2 - IBM, Cost of a Data Breach, 2024.
3 - Investigación del equipo de respuesta a incidentes de Sophos.
4 - Identity Defined Security Alliance.
5 - Basado en los detectores disponibles asignados al marco MITRE ATT&CK.

Ventas en España
Teléfono: (+34) 913 756 756
Correo electrónico: comercialES@sophos.com

Ventas en América Latina
Correo electrónico: Latamsales@sophos.com

2025-09-15 BR-ES (MP)

SOPHOS