

Sophos ITDR

Identity Threat Detection and Response

Sophos Identity Threat Detection and Response (ITDR) identifiziert Bedrohungen, die traditionelle Identität-Sicherheitskontrollen umgehen, und reagiert auf sie. Sophos ITDR ist vollständig in Sophos Extended Detection and Response (XDR) und Sophos Managed Detection and Response (MDR) integriert und hilft Ihnen, Ihren Sicherheitsstatus zu verbessern. Sophos ITDR überwacht Ihre Umgebung kontinuierlich auf Identitäts-Fehlkonfigurationen und -Risiken und liefert Darkweb-Informationen zu kompromittierten Zugangsdaten.

Anwendungsfälle

1 | SCHUTZ VOR IDENTITÄTSBEDROHUNGEN

Gewünschtes Ergebnis: Beseitigen identitätsbasierter Angriffe, bevor sie Ihr Unternehmen beeinträchtigen können

Lösung: 90 % der Organisationen verzeichneten im vergangenen Jahr einen identitätsbasierten Sicherheitsvorfall.¹ Sophos ITDR ermöglicht Ihnen, komplexe Bedrohungen proaktiv zu identifizieren und gegen 100 % der MITRE ATT&CK Credential Access-Techniken² früh in der Angriffskette zu schützen sowie schnell und präzise zu reagieren. Unsere Sophos MDR-Experten können risikoreiche Aktivitäten analysieren und sofortige Maßnahmen für Sie ergreifen, u. a. Benutzer blockieren, Passwortzurücksetzung erzwingen, Accounts sperren und Sitzungen beenden.



Gartner® Peer Insights™
„Customers' Choice“ für Extended
Detection and Response 2025

2 | REDUZIEREN DER IDENTITÄTS-ANGRIFFSFLÄCHE

Gewünschtes Ergebnis: Erkennen und Beheben von Fehlkonfigurationen und identitätsbezogenen Sicherheitslücken

Lösung: 95 % der Microsoft Entra ID-Umgebungen haben eine kritische Fehlkonfiguration.³ Werden solche Schwachstellen nicht behoben, können sie von Cyberkriminellen ausgenutzt werden, um Berechtigungen auszuweiten und identitätsbasierte Angriffe zu starten. Sophos ITDR scannt Ihre Entra ID-Umgebung kontinuierlich, um Fehlkonfigurationen und Sicherheitslücken schnell zu erkennen und Empfehlungen zur Behebung zu geben.



Ein Leader in den G2 Overall
Grid® Reports für MDR und XDR
(Kundenbewertung)

3 | ERKENNEN GELEAKTER ODER GESTOHLENER ZUGANGSDATEN

Gewünschtes Ergebnis: Risikominimierung, dass exponierte Zugangsdaten für Angriffe missbraucht werden

Lösung: Identität bleibt einer der wichtigsten Zugriffsvektoren für Ransomware und laut Beobachtungen von Sophos hat sich die Anzahl der gestohlenen Zugangsdaten, die auf einem der größten Marktplätze im Darkweb zum Kauf angeboten werden, im vergangenen Jahr mehr als verdoppelt.⁴ Sophos ITDR überwacht das Darkweb und Datenbanken zu Sicherheitsvorfällen und informiert Sie, wenn Zugangsdaten exponiert wurden, um die Gefahr eines Missbrauchs bei einem zukünftigen Angriff zu minimieren.

MITRE | ATT&CK®
Evaluations

Ein „Strong Performer“ bei
den MITRE ATT&CK® Evaluations
für Enterprise-Produkte und
Managed Services

4 | ERKENNEN VON RISKANTEM BENUTZERVERHALTEN

Gewünschtes Ergebnis: Ermitteln und Bekämpfen von riskantem Benutzerverhalten, um Ihr Unternehmen zu schützen

Lösung: Durch die Überwachung ungewöhnlicher Anmelde- und Benutzeraktivitäten können Sie Ihr Cyber-Risiko erheblich reduzieren und wertvolle Assets schützen. Sophos ITDR identifiziert risikobehaftete Verhaltensweisen, die Cyberkriminelle ausnutzen könnten – oder die darauf hindeuten, dass die Zugangsdaten eines Benutzers kompromittiert wurden – und liefert Detailinformationen zu Benutzern in Ihrer Organisation, die an aktuellen Sophos Security Alerts beteiligt waren.

Weitere Infos unter
www.sophos.de/ITDR

¹ Studie der Identity Defined Security Alliance (IDSA) 2024. | ² Basierend auf den Erkennungsfähigkeiten von Sophos, die nach dem MITRE ATT&CK Framework eingeordnet sind.

³ Von Sophos im Rahmen von Tausenden Incident-Response-Einsätzen erhobene Daten. | ⁴ Daten der Sophos X-Ops Counter Threat Unit (CTU), Juni 2024–Juni 2025.

Gartner, Gartner Peer Insights „Voice of the Customer“: Extended Detection and Response, Peer Contributors, 23. Mai 2025. Gartner Peer Insights geben die subjektiven Meinungen einzelner Enduser wieder, die auf deren eigenen Erfahrungen basieren. Sie sind in keinem Fall als Tatsachenfeststellung zu werten und repräsentieren nicht die Ansichten von Gartner oder seinen verbundenen Unternehmen. Gartner befürwortet in dieser Publikation keine bestimmten Hersteller, Produkte oder Dienstleistungen und übernimmt keinerlei Gewähr für die vorliegenden Forschungsergebnisse und schließt jegliche Mängelgewährleistung oder Zusicherung der erforderlichen Gebrauchstauglichkeit aus. GARTNER ist eine eingetragene Marke und Dienstleistungsmarke von Gartner, Inc. und/oder seiner verbundenen Unternehmen in den USA und international; PEER INSIGHTS ist eine eingetragene Marke von Gartner, Inc. und/oder seiner verbundenen Unternehmen und werden hier mit Genehmigung verwendet. Alle Rechte vorbehalten.

© Copyright 2025. Sophos Ltd. Alle Rechte vorbehalten. Eingetragen in England und Wales, Nr. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, GB. Sophos ist die eingetragene Marke von Sophos Ltd. Alle anderen genannten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken ihres jeweiligen Inhabers.