LÖSUNGSBROSCHÜRE

Sophos ITDR

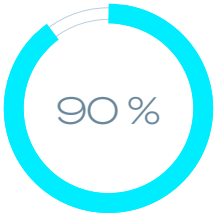
Beseitigen Sie identitätsbasierte Bedrohungen, bevor sie Ihr Unternehmen gefährden

Sophos Identity Threat Detection and Response (ITDR) stoppt identitätsbasierte Angriffe, indem es Ihre Umgebung kontinuierlich auf Identitätsrisiken und Fehlkonfigurationen überwacht und gleichzeitig Darknet-Informationen zu kompromittierten Zugangsdaten bereitstellt.

Die wachsende Gefahr durch Identitätsbedrohungen

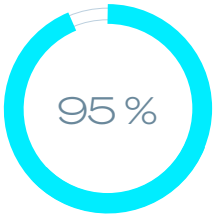
Benutzerbasierter Zugriff und entsprechende Kontrollen spielen in der heutigen IT- und Cybersecurity-Welt eine immer größere Rolle. Durch die Umstellung auf Cloud-Infrastrukturen und Remote-Arbeit wird es jedoch immer schwieriger, die Identitäts-Angriffsfläche adäquat zu überwachen und zu schützen. Angreifer machen sich diesen Umstand zunutze und verschaffen sich über kompromittierte Identitäten, Infrastrukturschwächen und Fehlkonfigurationen unbefugten Zugriff auf sensible Daten und Systeme. Daher gewinnen die Erkennung von Identitätsmissbrauch und die Blockierung identitätsbasierter Angriffe für einen effektiven Sicherheitsbetrieb zunehmend an Bedeutung.

Die Fakten in den Zahlen

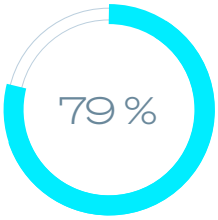


der Unternehmen/Organisationen hatten im letzten Jahr mindestens einen identitätsbezogenen Vorfall.[1]

Durchschnittliche Kosten einer Datenschutzverletzung.[2]



aller Microsoft Entra ID-Umgebungen weisen eine kritische Fehlkonfiguration auf.[3]



aller Datenschutzverletzungen sind identitätsbezogen.[4]

Vorteile auf einen Blick

- **Verschafft Einblick** mit einer zentralen Übersicht über die Identitäten auf Ihren Systemen.
- **Erkennt schnell** identitätsbasierte Risiken und Fehlkonfigurationen auf und gibt konkrete Handlungsempfehlungen.
- **Scannt kontinuierlich** nach Änderungen Ihres Identitäts-Sicherheitsstatus.
- **Scannt das Darknet** nach geleakten Zugangsdaten.
- **Erkennt potenziell schädliche Aktivitäten** von Insidern, unbekannten IPs und Standorten.
- **Reagiert schnell und präzise** auf Identitätsbedrohungen.
- **Lässt sich in Sophos MDR einbinden**, damit Experten Analyse- und Reaktionsmaßnahmen zum Bekämpfen identitätsbasierter Bedrohungen für Sie ergreifen.

Sophos ITDR-Lösung

Sophos ITDR verhindert identitätsbasierte Angriffe durch eine kontinuierliche Überwachung Ihrer Umgebung auf Identitätsrisiken und Fehlkonfigurationen – 95 % der Unternehmen/Organisationen haben solche Schwachstellen – und stellt gleichzeitig Darknet-Informationen zu kompromittierten Zugangsdaten bereit. Decken Sie Ihre Identitätsrisiken in Minuten auf – im Vergleich zu Tagen mit herkömmlichen Lösungen – und bewerten Sie Ihre Identitäts-Angriffsfläche im Zeitverlauf.

Reduzieren Sie Ihre Identitäts-Angriffsfläche

Sophos ITDR scannt Ihre Microsoft Entra ID-Umgebung kontinuierlich, um Fehlkonfigurationen und identitätsbasierte Sicherheitslücken schnell zu erkennen und Probleme zu priorisieren, die sofortige Aufmerksamkeit erfordern. Cyberkriminelle nutzen diese Schwachstellen, um Schaden zu verursachen, indem sie Berechtigungen eskalieren und Angriffe durchführen. Gehen Sie Risiken schnell an, einschließlich Lücken in Richtlinien für bedingten Zugriff, verwaiste Accounts, überprivilegierte Accounts und riskante Anwendungen.

Minimieren Sie Risiken durch geleakte oder gestohlene Zugangsdaten

Beobachtungen der Sophos X-Ops Counter Threat Unit (CTU) zufolge hat sich die Anzahl der gestohlenen Zugangsdaten, die auf einem der größten Marktplätze im Darknet zum Kauf angeboten werden, im vergangenen Jahr mehr als verdoppelt. Sophos ITDR erkennt und reagiert auf Identitätsbedrohungen, die traditionelle Identitätssicherheitskontrollen umgehen, und schützt zu 100 % vor MITRE ATT&CK-Credential Access-Techniken. Die Lösung identifiziert riskantes Benutzerverhalten wie ungewöhnliche Anmeldemuster und informiert Sie, wenn gestohlene oder kompromittierte Zugangsdaten verwendet werden, um Zugriff auf Ihre Systeme zu erlangen.

Leistungen von Sophos ITDR

Identitätskatalog
Verschaffen Sie sich Einblick – mit einer zentralen Ansicht aller Identitäten auf Ihren Systemen.

Kontinuierliche Sicherheits-Assessments der Identitäts-Infrastruktur
Scannen Sie Ihre Microsoft Entra ID-Umgebung kontinuierlich, um Fehlkonfigurationen und Sicherheitslücken zu identifizieren.

Überwachung kompromittierter Zugangsdaten im Darknet
Durchsuchen Sie das Darknet und Datenbanken mit Sicherheitsverletzungen nach geleakten Zugangsdaten.

Analysen des Benutzerverhaltens
Überwachen Sie ungewöhnliche Aktivitäten im Zusammenhang mit gestohlenen Zugangsdaten und internen Bedrohungen.

Modernste Erkennung von Identitätsbedrohungen
Identifizieren Sie verdächtige Aktivitäten, die früh in der Angriffskette auf spezifische Techniken von Angreifern hinweisen.

Maßnahmen zur Bedrohungsreaktion
Reagieren Sie schnell und präzise: Erzwingen Sie das Zurücksetzen von Passwörtern, sperren Sie Accounts mit verdächtigem Verhalten und mehr.

„Sophos ITDR hat die Transparenz über unsere Identitätsrisiken deutlich verbessert. Durch die zentrale Ansicht innerhalb unserer XDR-Plattform können wir Informationen zu von Sophos ITDR ermittelten Identitäts- und Fehlkonfigurationsrisiken an alle unsere Sicherheitsprogramme übertragen und so unsere allgemeine Cyberabwehr optimieren und Risiken reduzieren.“

– Direktor für Informationssicherheit, Finanzdienstleistungen

„Sophos ITDR deckt Risiken in Bereichen auf, über die ich mir früher innerhalb von Azure und dem Microsoft-Ökosystem Sorgen gemacht habe, wie Lücken in Richtlinien für bedingten Zugriff und unsichere oder überprivilegierte Anwendungen.“

– Senior Information Security Officer

Integration mit Sophos MDR

Sophos ITDR lässt sich vollständig in Sophos MDR einbinden, unseren Managed Detection and Response Service, dem weltweit die meisten Kunden vertrauen. Diese leistungsstarke Kombination ermöglicht den Sophos-Sicherheitsexperten, identitätsbasierte Bedrohungen für Sie zu überwachen, zu analysieren und darauf zu reagieren.

- Sophos ITDR erstellt automatisch MDR-Fälle für Erkennungen von Identitätsbedrohungen und Hochrisikobefunde.
- Die Sicherheitsanalysten von Sophos MDR untersuchen Fälle und ergreifen Reaktionsmaßnahmen zum Beseitigen von Bedrohungen.

Beispiel: Im Darknet geleakte Zugangsdaten

- Sophos ITDR identifiziert die Zugangsdaten eines Benutzers, die auf einem beliebten Darknet-Marktplatz zum Kauf angeboten werden.
- Die Analysten von Sophos MDR können den Account des Benutzers sperren und ein Zurücksetzen des Passworts erzwingen.

Beispiel: Verwendung gestohlener Zugangsdaten

- Sophos ITDR erkennt verdächtige Anmeldungen aus unbekannten Ländern und über ungewohnte Geräte und IP-Adressen.
- Die Analysten von Sophos MDR können den Account des kompromittierten Benutzers sperren und alle aktiven Sitzungen beenden.

Gemeinsam besser: Sophos ITDR + Microsoft Entra ID

Microsoft Entra ID ist im Wesentlichen ein Identity and Access Management (IAM)-Tool, das Identitäts- und Gruppenverwaltung, RBAC-Kontrollen, privilegiertes Zugriffsmanagement und Richtlinien für bedingten Zugriff bietet. Sophos ITDR wird in einer zentralen Konsole bereitgestellt, um Identitätsbedrohungen und -risiken zu erkennen und zu beseitigen. Der Funktionsumfang geht über IAM-Kernfunktionen hinaus und umfasst u. a. Identity Hygiene, Posture Assessment, Darkweb Monitoring und Advanced Threat Detection. Die Kombination aus Entra ID und Sophos ITDR bietet umfassenden Identitätsschutz für Ihr Unternehmen.

Einfache Lizenzierung

Sophos ITDR lässt sich einfach bereitstellen, bedienen und lizenzieren. Durch die einfache Subscription-Lizenzierung basierend auf der Anzahl der Benutzer und Server sind die Preise vorhersehbar. Fügen Sie Sophos ITDR je nach Bedarf zur Sophos XDR-Lösung oder zum Sophos MDR-Service hinzu.

- **Add-on zum Sophos Managed Detection and Response (MDR) Service:** Sophos-Sicherheitsexperten überwachen, analysieren und reagieren für Sie auf identitätsbasierte Bedrohungen.
- **Add-on zum Produkt Sophos Extended Detection and Response (XDR):** Ihr internes Team kann die KI-gestützten Erkennungs-, Analyse- und Reaktionstools von Sophos mit Sophos ITDR nutzen.

Gartner

Gartner® Peer Insights™ „Customers' Choice" for Extended Detection and Response (XDR) 2025.

Ein Leader in den G2 Overall Grid® Reports für Extended Detection and Response (XDR) und Managed Detection and Response (MDR).

MITRE | ATT&CK® Evaluations

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

FROST & SULLIVAN

Leader im Frost Radar™ Report für Managed Detection and Response 2025 von Frost & Sullivan.

Weitere Infos unter
sophos.de/ITDR

1 - Studie der Identity Defined Security Alliance (IDSA) 2024.
2 - IBM, Kosten einer Datenpanne 2024.
3 - Forschungsdaten des Sophos Incident Response-Teams.
4 - Identity Defined Security Alliance.
5 – Basierend auf verfügbaren Erkennungen, die dem MITRE ATT&CK Framework zugeordnet sind.

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0
E-Mail: sales@sophos.de

2025-09-15 BR-DE (MP)

SOPHOS