SOPHOS

SOPHOS IDENTITY THREAT DETECTION AND RESPONSE

Detect and neutralize identity threats, faster.

Attacks start with identity. So does the defense.

Find, prioritize, and respond to threats that bypass traditional identity security controls. Sophos ITDR continuously monitors Microsoft Entra ID and on-premises Active Directory environments, uncovers identity risks and credential exposure, applies AI-driven risk scoring, and enables rapid response before attackers can escalate privileges or move laterally.

95%
of organizations have a Microsoft Entra ID misconfiguration[1]

71%
of organizations experienced an identity breach in the past year[2]

1.3 Billion
AI agents projected to be in use by 2028, expanding the attack surface[3]

Attackers don't break in. They log in.

Identity is now one of the most targeted attack surfaces in cybersecurity. Cloud adoption, remote work, AI agents, and other non-human identities have dramatically expanded the opportunities attackers can exploit , while stolen credentials remain one of the fastest paths to compromise.

Identity and Access Management (IAM) solutions are essential for managing users, access, and authentication, but they weren't designed to surface identity risks, discover exposed credentials, investigate suspicious behavior, nor drive security response. Sophos ITDR closes that gap, connecting identity visibility with threat detection, investigation, and response to stop attacks before they spread.

FROM IDENTITY CHALLENGES		TO OUTCOMES THAT MATTER
Identity misconfigurations and weak policies	→	**Reduce identity exposure with continuous monitoring and 160+ posture checks**
Low visibility into active identity threats	→	**Full visibility to identity catalogue of users, devices, apps, and groups**
Stolen / breached credentials	→	**Prevent attacks with dark web credential intelligence**
Risky users and non-human identities	→	**Understand who's risky and why, with AI-driven identity risk scores**
Fragmented investigations	→	**Accelerate investigations and response within contextualized cases**

Secure identity from risk to response.

SOPHOS FUSION

Sophos ITDR is part of Sophos Fusion, the industry's most complete AI-native cybersecurity defense system. It continuously monitors identity posture, exposed credentials, risky behaviors, and identity threats, then turns findings into contextualized investigations and coordinated responses.

What Sophos ITDR delivers

See every identity

- Gain a complete, **searchable view of identities** across your Microsoft Entra ID and Active Directory environments, including users, groups, devices, applications, service accounts, and AI identities.
- Sophos ITDR continuously monitors your environment with more than **160 identity posture checks**, rapidly identifying misconfigurations, excessive privileges, insecure authentication methods, and other identity-based security gaps.
- Findings are prioritized by risk and accompanied by **actionable recommendations,** helping security teams reduce the identity attack surface and improve security posture over time.

Catch credential compromise

- Stolen credentials remain one of the fastest paths to a successful breach. Sophos ITDR continuously monitors **dark web marketplaces** and breach sources for exposed credentials, linking compromised passwords directly to identities in your environment.
- Designate **VIP accounts** to monitor high-value attributes like personal emails, phone numbers, and more.
- Quickly identify affected users, assess the level of risk, and **take immediate action** through built-in response actions. Reset passwords and revoke sessions before attackers can abuse exposed credentials.

Understand identity risk

- Not all identities present the same level of risk. Sophos ITDR applies AI-driven **identity risk scores** to human and non-human identities, helping security teams quickly identify those most likely to be targeted or abused.
- By analyzing login patterns, privilege use, security findings, and behavioral anomalies, Sophos ITDR provides **clear explanations** of what is risky and why.
- Uncover compromised accounts, insider threats, risky service accounts, and suspicious activity associated with AI identities, enabling teams to **focus on the identities** that matter most.

Respond as one

- Identity threat visibility is only valuable if it leads to action. Sophos ITDR automatically groups related findings into **contextualized cases** that provide analysts with the identities, detections, evidence, and risk factors needed to investigate and respond to threats quickly.
- Centralized investigation workflows and built-in response actions accelerate remediation, while native integration with **Sophos XDR** and **Sophos MDR** extends identity intelligence across the broader cyber defense system, enabling coordinated response.

Sophos + Microsoft: Better together

Microsoft Entra ID and Active Directory + Sophos ITDR = Comprehensive identity security

Sophos secures more than 625,000 customer environments through Sophos Fusion, bringing deep Microsoft expertise, integrations, and security operations experience to identity defense. Sophos ITDR extends Microsoft identity environments with continuous posture assessment, credential monitoring, AI-driven risk scoring, and threat detection, helping teams accelerate investigation and response.

UPGRADE TO SOPHOS MDR

Run a world-class SOC without building one

Sophos ITDR is integrated with Sophos MDR for fully managed, 24/7 expert-led detection, investigation, and response. Sophos MDR is the world's largest Agentic SOC — AI investigates identity threats in seconds; analysts own the outcomes.

52%

of MDR cases are solved end-to-end by AI

89 sec

average time from alert to automated response

WHY SOPHOS ITDR

Why customers choose Sophos ITDR

Close the gaps attackers find first

160+ continuous posture checks and 100% coverage of MITRE ATT&CK Credential Access techniques

Explainable identity risk

AI-driven, behavior-based identity risk scores show who's risky and why

Dark web intelligence built-in

Transform credential exposures into immediate action

Human and non-human identity coverage

Protect users, service accounts, AI identities, and more

Part of Sophos Fusion

Identity insights fuel coordinated action across the world's most complete cyber defense system.

INDUSTRY RECOGNITION

Validated by the analysts and organizations that matter most

GARTNER

A Gartner® Peer Insights™ "Customers' Choice" for MDR and XDR.

G2

A Leader in G2 Overall Grid® Reports for MDR and XDR.

MITRE ATT&CK EVALUATIONS

A strong performer in MITRE ATT&CK® Evaluations for enterprise solutions.

KUPPINGERCOLE

An overall leader in the 2026 KuppingerCole Analyst Leadership Compass for Managed Detection and Response.

SPEAK WITH AN EXPERT

Sophos ITDR

See your first identity findings in minutes. Start your free trial:

sophos.com/ITDR →

[1] Sophos Incident Response team.
[2] Sophos Identity Security Report, 2026.
[3] IDC Info Snapshot, 2025.

2026-08-21 BR (MC)

SOPHOS