SOLUTION BRIEF

Sophos ITDR

Identity Threat Detection and Response

Sophos Identity Threat Detection and Response (ITDR) identifies and responds to threats that bypass traditional identity security controls. Fully integrated with Sophos Extended Detection and Response (XDR) and Sophos Managed Detection and Response (MDR), Sophos ITDR helps you improve your organization's security posture, continuously monitors your environment for identity misconfigurations and risks, and provides dark web intelligence on compromised credentials.

Use cases

1 | PROTECT AGAINST IDENTITY THREATS

Desired outcome: Neutralize identity-based attacks before they can impact your business.

Solution: 90% of organizations experienced an identity breach in the past year.[1] Sophos ITDR enables you to proactively identify sophisticated threats and protect against 100% of MITRE ATT&CK Credential Access techniques[2] early in the attack chain and respond with speed and precision. Our experienced Sophos MDR analysts can investigate high-risk activities and take immediate actions on your behalf, including disabling a user, forcing a password reset, locking an account, revoking sessions, and more.

2 | REDUCE YOUR IDENTITY ATTACK SURFACE

Desired outcome: Identify and remediate misconfigurations and identity-based security gaps.

Solution: 95% of Microsoft Entra ID environments have a critical misconfiguration.[3] If left unchecked, cybercriminals can use these exposures to escalate privileges and carry out identity-based attacks. Sophos ITDR continuously scans your Entra ID environment to rapidly identify misconfigurations and security gaps and provide remediation recommendations.

3 | DISCOVER LEAKED OR STOLEN CREDENTIALS

Desired outcome: Minimize the risk of exposed credentials being used to execute an attack.

Solution: Identity remains one of the top access vectors for ransomware, and Sophos has observed that the number of stolen credentials offered for sale on one of the dark web's largest marketplaces has more than doubled in the past year alone.[4] Sophos ITDR monitors the dark web and breach databases, and alerts you when credentials have been exposed to reduce the risk of them being used in a future attack.

4 | IDENTIFY RISKY USER BEHAVIORS

Desired outcome: Understand and address high-risk user behaviors to protect your business.

Solution: By monitoring for unusual login patterns and abnormal user activity, you can significantly reduce your cybersecurity risks and protect valuable assets. Sophos ITDR identifies risky behaviors that malicious actors could exploit — or that may indicate that a user's credentials have been compromised — and provides details of users in your organization that have been involved in recent Sophos security alerts.

Gartner Peer Insights Customers' Choice 2025

A 2025 Gartner® Peer Insights™ "Customers' Choice" for Extended Detection and Response.

A Leader in G2 Overall Grid® Reports for MDR and XDR as rated and reviewed by customers.

MITRE | ATT&CK® Evaluations

A strong performer in MITRE ATT&CK® Evaluations for Enterprise products and Managed Services.

Learn more:
sophos.com/ITDR

[1] 2024 Identity Defined Security Alliance (IDSA) study. | [2] Based on Sophos detection capabilities mapped to the MITRE ATT&CK framework.
[3] Data gathered from thousands of incident response engagements conducted by Sophos. | [4] Sophos X-Ops Counter Threat Unit (CTU) data, June 2024 – June 2025.

2025-09-16 SB-EN (MP)