SOLUTION BROCHURE

Sophos ITDR

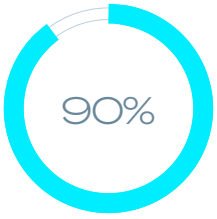
Neutralize identity-based threats before they can impact your business

Sophos Identity Threat Detection and Response (ITDR) stops identity-based attacks by continuously monitoring your environment for identity risks and misconfigurations while providing dark web intelligence on compromised credentials.

Identity threats: An expanding security problem

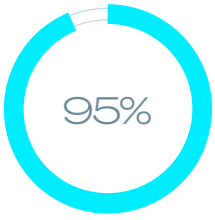
User-based access and controls are at the frontline of today's IT and cybersecurity world, and the shift to cloud and remote work has increased the complexity of monitoring and securing the identity attack surface. Adversaries use compromised identities, infrastructure weaknesses, and misconfigurations, to gain unauthorized access to sensitive data and systems. As a result, detecting identity abuse and blocking identity-based attacks are increasingly important for effective security operations.

The proof is in the numbers

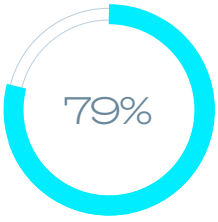


of organizations experienced at least one identity-related breach in the past year.[1]

Average cost of a data breach.[2]



of Microsoft Entra ID environments have a critical misconfiguration.[3]



of data breaches are identity related.[4]

Sophos ITDR solution

Sophos ITDR prevents identity-based attacks, continuously monitoring your environment for identity risks and misconfigurations — an issue affecting 95% of organizations — while also providing dark web intelligence on compromised credentials. Uncover your identity risks in minutes, compared to days with legacy solutions, and benchmark your identity attack surface over time.

Benefits

- **Gain visibility** with a centralized view of identities across your systems.
- **Quickly uncover** identity-based risks and misconfigurations, with actionable recommendations.
- **Continuously scan** for changes in identity posture.
- **Scan the dark web** for leaked credentials.
- **Detect potentially malicious activities** from insiders, unfamiliar IPs, and locations.
- **Respond to identity threats** with speed and precision.
- **Integrates with Sophos MDR** for expert investigation and response to identity-based threats.

Reduce your identity attack surface

Sophos ITDR continuously scans your Microsoft Entra ID environment to rapidly identify misconfigurations and identity-based security gaps, and prioritize issues requiring immediate attention. Cybercriminals use these exposures to inflict damage by escalating privileges and conducting attacks. Address risks fast, including Conditional Access policy gaps, orphan accounts, over-privileged accounts, and risky applications.

Minimize risk of leaked or stolen credentials

The number of stolen credentials offered for sale on one of the dark web's largest marketplaces more than doubled in the past year, based on Sophos X-Ops Counter Threat Unit (CTU) intelligence. Sophos ITDR detects and responds to identity threats that bypass traditional identity security controls, protecting against 100% of MITRE ATT&CK Credential Access techniques.[5] The solution identifies risky user behaviors such as unusual login patterns and highlights the use of stolen or compromised credentials to gain access to your systems.

What Sophos ITDR delivers

Identity catalog
Gain visibility with a centralized view of identities across your systems.

Continuous identity posture assessments
Constantly scan your Microsoft Entra ID environment to identify misconfigurations and security gaps.

Dark web compromised credential monitoring
Search the dark web and breach databases for leaked credentials.

User behavior analytics
Monitor for abnormal activity associated with stolen credentials or insider threats.

Advanced identity threat detection
Identify suspicious activities indicative of specific adversary techniques early in the attack chain.

Threat response actions
Respond with speed and precision: Force password resets, lock down accounts that exhibit suspicious behavior, and more.

"Sophos ITDR has significantly improved visibility into our identity risks. Having a centralized view within our XDR platform enables us to feed the identity and misconfiguration risks Sophos ITDR has spotlighted into all our security programs, therefore improving our overall organizational cyber posture and reducing risk."

– Information Security Director, Financial Services

"Sophos ITDR is uncovering risks in areas that I used to worry about within Azure and the Microsoft ecosystem, like conditional access policy gaps and insecure or over-privileged applications."

– Senior Information Security Officer

Integrated with Sophos MDR

Sophos ITDR is fully integrated with Sophos MDR, the world's most trusted managed detection and response service. This powerful combination enables Sophos security experts to monitor, investigate, and respond to identity-based threats on your behalf:

- Sophos ITDR automatically creates MDR cases for identity threat detections and high-risk findings.
- Sophos MDR security analysts investigate cases and execute response actions to neutralize threats.

Example: Credentials leaked on the dark web

- Sophos ITDR identifies a user's credentials for sale on a popular dark web marketplace.
- Sophos MDR analysts can lock the user's account and force a password reset.

Example: Stolen credentials in use

- Sophos ITDR identifies suspicious logons from previously unseen countries, devices, and IP addresses.
- Sophos MDR analysts can lock the compromised user's account and terminate all active sessions.

Better together: Sophos ITDR + Microsoft Entra ID

Microsoft Entra ID is fundamentally an Identity and Access Management (IAM) tool, providing identity and group management, RBAC controls, privileged access management, and conditional access policies. Delivered in a unified console to detect and neutralize identity threats and risks, Sophos ITDR extends beyond core IAM capabilities with identity hygiene, posture assessment, dark web monitoring, advanced threat detection, and more. **The combination of Entra ID and Sophos ITDR provides the most comprehensive identity security coverage for your business.**

Simple licensing

Sophos ITDR is easy to deploy, easy to use, and easy to procure. Simple subscription licensing based on the number of users and servers in your organization makes pricing predictable. Choose to add Sophos ITDR to the Sophos XDR solution or the Sophos MDR service, to suit your needs.

- **Add-on to the Sophos Managed Detection and Response (MDR) service:** Sophos security experts monitor, investigate, and respond to identity-based threats on your behalf.
- **Add-on to the Sophos Extended Detection and Response (XDR) product:** Your in-house team can take advantage of Sophos' AI-powered detection, investigation, and response tools with Sophos ITDR.

Gartner

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

A Leader in G2 Overall Grid® Reports for Extended Detection and Response (XDR) and Managed Detection and Response (MDR).

MITRE | ATT&CK® Evaluations

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

FROST & SULLIVAN

A Leader in Frost & Sullivan's 2025 Frost Radar™ for Managed Detection and Response.

1 - 2024 Identity Defined Security Alliance (IDSA) study.
2 - IBM, Cost of a Data Breach 2024.
3 - Sophos Incident Response team research.
4 - Identity Defined Security Alliance.
5 - Based on available detectors mapped to the MITRE ATT&CK Framework.

To learn more, visit
sophos.com/ITDR

United Kingdom and Worldwide Sales
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Asia Sales
Tel: +65 62244168
Email: salesasia@sophos.com

2025-09-15 BR-EN (MP)

SOPHOS