SOPHOS

SOPHOS ITDR

Attacks start with identity. So does the defense.

AI-driven identity threat detection and response.

Attackers don't break in. They log in. Sophos ITDR continuously monitors your environment, applies AI-driven risk scoring to surface what matters most, and enables rapid response before threats spread.

95%
of Entra ID environments have a critical misconfiguration[1]

71%
of organizations suffered an identity-based breach in the past year, with an average of 3 attacks per org[2]

67%
of attacks trace back to a compromised identity[3]

1.3B
AI agents projected by 2028, expanding your attack surface[4]

WHAT SOPHOS ITDR DELIVERS

Secure identity from risk to response.

No entry, no escalation.

Identify suspicious identity behaviors early in the attack chain, before attackers can escalate privileges, move laterally, or cause lasting damage.

- 100% coverage of MITRE ATT&CK Credential Access techniques
- AI-driven risk scoring surfaces your highest-risk identities
- Enables rapid response — from alert to action in seconds

Close the gaps attackers find first.

Every AI agent, service account, and over-privileged identity is a potential attack path, leading to 41% of identity breaches last year.[2] Sophos ITDR surfaces hidden risks before attackers can exploit them.

- 100+ continuous posture checks, beyond identity hygiene
- Visibility across human and non-human identities (NHIs), including AI agents

From dark web exposure to immediate action.

Stolen credentials are the fastest path to a serious breach. Sophos ITDR monitors the dark web and breach sources, linking exposed credentials to identities in your environment.

- Stolen credentials for sale on the dark web have doubled in the past year[5]
- Get instant alerts when your credentials are exposed
- Trigger immediate response — revoke sessions, reset passwords

See the risk behind every identity.

Sophos ITDR analyzes login patterns, privilege use, and behavioral anomalies across human and non-human identities to surface those most likely to be abused — with clear reasoning that explains what's risky and why.

- AI-driven risk scoring surfaces your highest-risk identities
- Detect insider threats and compromised accounts
- Identify risky behavior from Microsoft AI agents

SOPHOS ITDR AT A GLANCE

- Continuous monitoring across your entire identity environment
- 100+ identity posture checks for Entra ID
- Dark web monitoring for exposed credentials, with expanded coverage for VIP identity attributes
- AI-driven risk scoring across human and non-human identities, including Microsoft AI agents
- Natively integrated with Sophos MDR for expert response

WHO SOPHOS ITDR IS FOR

- Organizations lacking visibility into their identity attack surface
- Security teams struggling to keep pace with identity sprawl
- Businesses adopting AI agents and non-human identities
- Sophos MDR and XDR seeking integrated identity security
- MSPs and MSSPs adding identity defense to their managed security practice

SOPHOS ITDR + SOPHOS MDR

Identity threats don't wait. Neither do we.

Fully managed threat response.

Sophos ITDR automatically escalates high-confidence identity threats to Sophos MDR, where every threat is investigated, validated, and neutralized before it can spread.

AI speed. Human judgment.

Sophos MDR is the world's largest Agentic SOC — AI investigates identity threats in seconds; analysts own the outcomes.

Smarter with every threat.

Every threat across 600,000+ defended organizations makes the next defense stronger. The system doesn't just scale, it learns — continuously strengthening your identity protection.

INDUSTRY RECOGNITION

Validated by the analysts and organizations that matter most.

GARTNER 2026
A "Customers' Choice" for MDR Services

KUPPINGERCOLE 2026
Leader, Leadership Compass for MDR

G2 SPRING 2026
#1 in Endpoint, EDR, XDR, MDR & Firewall

MITRE ATT&CK EVALS
100% detection coverage

FROST & SULLIVAN 2025
Leader, Frost Radar for MDR

GARTNER PEER INSIGHTS
4.8 / 5.0 rated by MDR customers

START HERE

Speak with an expert or start your free 30-day trial.

sophos.com/ITDR

[1] Sophos Incident Response Team, [2] Sophos Identity Security Report 2026, [3] Sophos Active Adversary Report, 2025, [4] IDC Info Snapshot, 2025, [5] Sophos X-Ops CTU research

SOPHOS