解决方案概要

Sophos ITDR

身份威胁侦测与响应

Sophos Identity Threat Detection and Response (ITDR) 身份识别威胁侦测与响应能够识别并响应绕过传统身份安全控制的威胁。Sophos ITDR 完全集成于 Sophos Extended Detection and Response (XDR) 扩展式侦测与响应，和 Sophos Managed Detection and Response (MDR) 托管式侦测与响应中，帮助您提高组织的安全防护能力，持续监控您环境中的身份配置错误和风险，并提供关于被入侵凭证的暗网情报。

使用案例

1 | 防范身份识别威胁

期望结果：在基于身份识别的攻击影响您的业务之前加以消除。

解决方案：90% 的组织在过去一年中遭遇过身份识别入侵事件。[1] Sophos ITDR 帮助您主动辨识复杂威胁，并在攻击链的早期阶段就防止 100% 的 MITRE ATT&CK 凭证访问技术 [2]，同时迅速、精准地做出响应。我们的经验丰富的 Sophos MDR 分析师可以调查高风险活动，并为您采取及时行动，包括禁用用户、强制重置密码、锁上
账户、撤销会话等。

2 | 减少身份识别攻击面

期望结果：辨识并修复身份安全配置错误和基于身份识别的安全漏洞。

解决方案：95% 的 Microsoft Entra ID 环境存在严重配置错误。[3] 如果不加以修复，网络犯罪分子可能利用这些曝露来升级权限并发动基于身份识别的攻击。Sophos ITDR 持续扫描您的 Entra ID 环境，快速辨识配置错误和安全漏洞，并提供修复建议。

3 | 发现泄露或被盗凭证

期望结果：尽量减少泄露凭证被用于攻击的风险。

解决方案：身份仍然是勒索软件攻击的主要访问途径，Sophos 观察到，仅仅在过去一年里，暗网上最大的市场之一上出售的被盗凭证数量已翻倍。[4] Sophos ITDR 会监控暗网和泄露数据库，并在凭证泄露时及时提醒您，以减少它们在未来攻击中被利用的风险。

4 | 辨识高风险用户行为

期望结果：了解并处理高风险的用户行为，保护您的企业。

解决方案：通过监控不寻常的登录模式和异常的用户活动，您可以显著降低网络安全风险，保护关键资产。Sophos ITDR 能辨识出可能遭恶意行为者利用的高风险行为，或可能表明用户凭证已被泄露的迹象，并提供有关您组织中最近牵涉 Sophos 安全警报的用户详细信息。

Gartner Peer Insights Customers' Choice 2025

2025 Gartner® Peer Insights ™ 扩展式侦测与响应服务的 ” 客户之选”。

在 G2 Overall Grid ® MDR 和 XDR 报告中获客户评选为的领导者。

MITRE | ATT&CK® Evaluations

在 MITRE ATT&CK® Evaluations 企业产品和托管服务领域中表现强劲。

欲了解更多信息，请访问：
sophos.com/ITDR

[1] 2024 年Identity Defined Security Alliance (IDSA) 研究。| [2] 基于映射 MITRE ATT&CK Framework 的 Sophos 侦测能力。

[3] 数据来源于 Sophos 执行的数千次事件响应案例。| [4] Sophos X-Ops Counter Threat Unit (CTU) 数据，2024 年 6 月至 2025 年 6 月。

Gartner，Gartner Peer Insights ‘客户之声’：扩展式侦测与响应，由业界人士提供，2025 年 5 月 23 日。Gartner Peer Insights 内容包含个人终端用户基于自身经验的意见，不应被解释为事实陈述，也不代表 Gartner 或其附属公司的观点。Gartner 不认可本内容中描述的任何厂商、产品或服务，也不对本内容的准确性或完整性做出任何明示或暗示的保证，包括对适销性或特定用途的适用性做出任何保证。GARTNER 是 Gartner, Inc. 和/或其附属公司在美国及国际上的注册商标和服务标志，PEER INSIGHTS 是 Gartner, Inc. 和/或其附属公司的注册商标，本文件已获许可使用。保留所有权利。

2025-09-16 SB-ZHCN (MP)