解决方案手册

Sophos ITDR

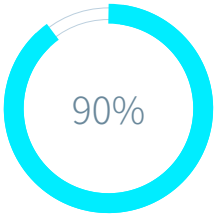
在身份识别威胁影响您的业务之前加以消除。

Sophos Identity Threat Detection and Response (ITDR) 身份识别威胁侦测与响应通过持续监控您的环境中的身份风险和配置错误，并提供关于被入侵凭证的暗网情报，以阻止基于身份的攻击。

身份识别威胁：日益严峻的安全问题

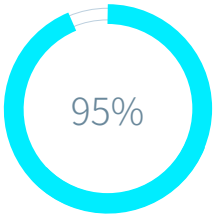
基于用户的访问与控制是当今 IT 和网络安全领域的前沿，随着转向云端和远程工作，监控和保护身份识别攻击面变得更加复杂。攻击敌手利用被入侵的身份识别信息、基础设施漏洞和配置错误，未经授权访问敏感数据和系统。因此，侦测身份滥用并阻止基于身份的攻击，对于有效的安全运营变得越来越重要。

数据就是最佳证明

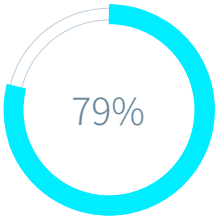


的组织在过去一年中经历了至少一次与身份识别相关的入侵事件。[1]

数据泄露的平均成本。[2]



Microsoft Entra ID 环境存在严重配置错误。[3]



的数据泄露与身份识别相关。[4]

产品优势

- 透过跨系统的身分识别集中化视图，全面掌握状况。
- **快速发现**身份识别的风险和配置错误，并提供可付诸行动的建议。
- **持续扫描**身份状态的变化。
- **扫描暗网**，查找泄露的凭证。
- **侦测潜在恶意活动**内部人员、不熟悉的 IP 地址和位置。
- 响应身份识别威胁**迅速且精准有效。**
- **与 Sophos MDR 集成**，获得专家级调查和响应基于身份识别的威胁。

Sophos ITDR 解决方案

Sophos ITDR 通过持续监控您的环境中的身份识别风险和配置错误（95% 的组织受此影响），来防止基于身份识别的攻击，同时也提供关于被入侵凭证的暗网情报。与传统解决方案需耗费数天相比，您可几分钟内即找出身份识别风险，并且可以随时间持续对身份识别攻击面进行基准对比。

减少您的身份识别攻击面

Sophos ITDR 持续扫描您的 Microsoft Entra ID 环境，以快速识别配置错误和基于身份识别的安全缺口，并优先排序需要立即关注的问题。网络犯罪分子利用这些曝露，来提升权限和发动攻击来造成损害。快速解决风险，包括条件访问 (Conditional Access) 政策的漏洞、孤儿账户、权限过大的账户和高风险应用。

降低泄露或被盗凭证的风险

根据 Sophos X-Ops 对抗威胁小组 (CTU) 的情报，过去一年，在暗网最大市场之一上出售的被盗凭证数量翻了一番。Sophos ITDR 能够侦测并响应绕过传统身份安全控制的威胁，有效防护 100% 的 MITRE ATT&CK 凭证访问技术。[5] 该解决方案能够识别高风险用户行为，例如异常登录模式，并突出显示使用被盗或遭入侵凭证来访问系统的情况。

Sophos ITDR 提供的服务

身份识别目录
透过跨系统的身分识别集中化视图，全面掌握状况。

持续身份状态评估
持续扫描您的 Microsoft Entra ID 环境，识别配置错误和安全漏洞。

暗网遭入侵凭证的监控
在暗网和泄露数据库中搜索泄露的凭证。

用户行为分析
监控与被盗凭证或内部威胁相关的异常活动。

高级身份识别威胁侦测
在攻击链的早期阶段找出显示特定攻击敌手技术的可疑活动。

威胁响应措施
快速且精准地响应：强制重置密码、锁上表现出可疑行为的账户等。

“Sophos ITDR 显著提升了我们对身份识别风险的可见性。通过在 XDR 平台内的统一视图，使我们能够将 Sophos ITDR 所揭示的身份识别和配置风险纳入所有安全项目中，从而提升整体组织的网络安全状态，并降低风险。”

——金融服务公司信息安全总监

“Sophos ITDR 揭露了我过去一直担心的 Azure 与 Microsoft 生态系统风险，例如条件式访问政策的漏洞，以及不安全或过度授权的应用。”

—— 高级信息安全官

与 Sophos MDR 集成

Sophos ITDR 完全集成了全球最受信任的托管式侦测与响应服务 Sophos MDR。这个强大的组合使 Sophos 安全专家能够代表您监控、调查并响应基于身份识别的威胁：

- Sophos ITDR 会自动为身份识别威胁侦测和高风险发现创建 MDR 个案。
- Sophos MDR 安全分析师将调查个案并执行响应措施，消除威胁。

示例：暗网上的泄露凭证

- Sophos ITDR 发现到某用户的凭证在一个主流的暗网市场上出售。
- Sophos MDR 分析师可以锁上该用户账户并强制重置密码。

示例：被盗凭证正在被使用

- Sophos ITDR 发现到来自之前未见过的国家、设备和 IP 地址的可疑登录。
- Sophos MDR 分析师可以锁上受入侵用户账户并终止所有作用中的会话。

完美结合：Sophos ITDR + Microsoft Entra ID

Microsoft Entra ID 是一个身份与访问管理 (IAM) 工具，提供身份和组管理、RBAC 控制、特权访问管理和条件访问政策。Sophos ITDR 通过统一控制台来侦测并消除身份识别威胁和风险，并超越核心 IAM 功能，额外提供身份识别保健检查、状态评估、暗网监控、先进的威胁侦测等功能。**Entra ID 与 Sophos ITDR 的结合，为您的企业提供全面的身份识别安全保护。**

简单授权许可模式

Sophos ITDR 易于部署、使用和采购。基于您组织中用户和服务器数量的简单订阅授权许可，更能预测成本。您可以根据需要选择将 Sophos ITDR 添加到 Sophos XDR 解决方案或 Sophos MDR 服务中。

- **附加到 Sophos 托管式侦测与响应 (MDR) 服务中：**Sophos 安全专家来代表您监控、调查并响应基于身份识别的威胁：
- **附加到 Sophos 扩展式侦测与响应 (XDR) 产品中：**您的内部团队可以通过 Sophos ITDR，运用 Sophos 强大的 AI 侦测、调查和响应工具。

Gartner

在 2025 Gartner® Peer Insights™ 中，获评为托管式侦测与响应 (XDR) 服务的“客户之选”

在 G2 Overall Grid® 报告中，获评为扩展式侦测与响应 (XDR) 和托管式侦测与响应 (MDR) 领域的领导者。

MITRE | ATT&CK® Evaluations

在 MITRE ATT&CK® Evaluations 托管服务和企业产品的中表现强劲。

FROST & SULLIVAN

在 Frost & Sullivan 的 2025 年 Frost Radar™ 中，获评为托管式侦测与响应领域的领导者。

想要了解更多信息，请访问：
sophos.com/ITDR

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 - 基于 MITRE ATT&CK Framework 映射的可用侦测器。

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

2025-09-15 BR-ZHCN (MP)

SOPHOS