

Sophos 与 Veeam 集成

阻止针对关键备份数据的威胁



在去年 75% 的勒索软件攻击中，威胁攻击者能够影响备份存储库¹，篡改备份并删除数据以阻止恢复。当备份数据受到威胁时，Sophos 和 Veeam 通过无缝交换安全信息来简化网复原，并扩展可见性以帮助侦测、调查和响应主动攻击。

使用案例

1 | 防御勒索软件

期望结果: 获得针对勒索软件攻击的最强防护。

解决方案: Sophos 提供业界领先的技术，可以在勒索软件影响您的系统之前普遍地侦测和阻止勒索软件，包括新的变种和本地和远程加密攻击。Sophos 先进的侦测和预防能力，结合 Veeam 提供的不可更改备份和版本控制，确保您的备份数据保持安全和可恢复。

2 | 扩大威胁可见性

期望结果: 识别可能影响备份数据的潜在威胁。

解决方案: Sophos 与 Veeam 的集成适用于 Sophos MDR (托管式侦测与响应) 服务和 Sophos XDR (扩展式侦测与响应) 解决方案。它提供了对影响备份的恶意活动的可见性，包括试图删除备份存储库、禁用多因素身份验证、更改加密密码等。

3 | 确保备份的完整性和可用性

期望结果: 备份数据始终可用并受到保护，让您高枕无忧。

解决方案: 我们强大的集成使您能够侦测威胁，调查可疑活动，并最终快速恢复数据，以保持您的业务运行。使用 Sophos 和 Veeam，您可以确保备份的完整性和可用性，降低由于恶意软件、意外删除、内部安全威胁和其他数据丢失场景导致数据丢失的风险。

4 | 缩短威胁响应时间

期望结果: 尽量减少宕机时间并确保业务连续性。

解决方案: Sophos MDR 是一种 24/7 全天候由人工主导的威胁预防、侦测和响应服务，可保护组织防御最先进的攻击。Sophos 专家执行威胁捕猎，以识别试图绕过预防工具的攻击者技术，并执行响应措施，以阻止已确认的威胁，平均响应时间为 38 分钟，比行业基准快 96%。



Gartner“客户之选”的托管式侦测与响应服务



连续第 14 次蝉联，在 2023 年获评 Magic Quadrant 端点防护平台的领导者之一



在 MITRE ATT&CK 托管式安全服务评估中表现顶级的厂商

查阅详情:

www.sophos.com/mdr

www.sophos.com/xdr

¹《Veeam 2023 勒索软件趋势报告》

© 版权所有 2024。Sophos Ltd. 保留所有权利。注册于英格兰和威尔士，注册编号 2096520，地址：The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, 英国。Sophos 是 Sophos Ltd. 的注册商标。所有其他提及的产品和公司名称均为其各自所有者的商标或注册商标。

Gartner Peer Insights 标志是 Gartner, Inc. 和/或其附属公司的商标和服务标志，在此获得许可后使用。保留所有权利。Gartner Peer Insights 的内容由个人最终用户根据自己与平台上所列厂商的合作经验发表的意见组成，不应被视为事实陈述，也不代表 Gartner 或其附属机构的观点。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，包括对适用性或特定用途的适用性做出任何保证。