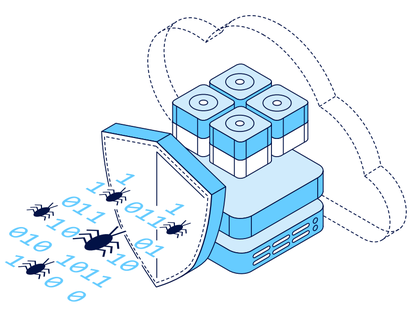
亚太及日本地区版本

2022年

勒索软件趋势报告

2022 年 1 月，一家独立研究公司针对 **1,000** 名无偏见 IT 领导者展开了一项调研，以了解勒索软件对组织环境的影响及其补救方法和面向未来的策略。受访者包括首席信息安全官、安全专业人员、备份管理员和 IT 操作人员。他们来自亚太及日本地区与欧洲、中东和非洲地区及美洲地区的 16 个不同国家（地区），其中 **200** 人来自亚太及日本地区，他们的组织规模有大有小。

勒索软件的泛滥程度



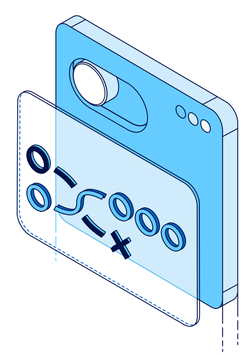
97%

的勒索软件攻击企图感染备份存储库，其中 **73%** 的攻击得逞

52%

的生产数据被加密，– 而且其中仅 **68%** 的数据得以恢复

赎金 ≠ 补救



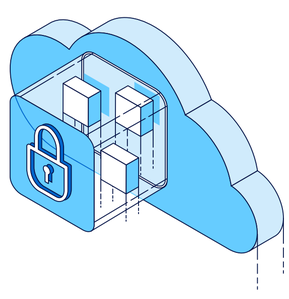
18%

的组织没有支付赎金就恢复了数据

36%

支付赎金的组织仍无法恢复其数据

防御技术



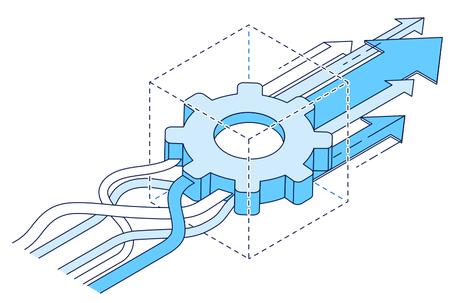
84%

的组织依赖备份日志或介质可读性来确保可恢复性，这意味着仅有 **16%** 的组织通过还原和测试功能进行例行测试

41%

的组织在遭遇勒索软件攻击后先还原到隔离沙盒，然后恢复数据

组织协调



55%

的组织认为备份和网络安全需要进行重大或彻底的改革

29%

的网络团队的勒索软件防护手册包括验证或保证不被感染的要求

安全备份是您的最后一道防线

勒索软件会带来灾难，每起事件将给企业造成近 200 万美元的损失。Veeam® 认为安全备份是抵御勒索软件侵害的最后一道防线。我们的软件采用安全设计，消除了专有硬件的限制，可在内部和云端支持现有架构，可靠的备份有助于防范停机和数据丢失并避免支付高昂赎金。

更多信息请访问：www.veeam.com/cn

点击此处，下载完整研究报告