VERITAS

提高韧性，从容恢复

做好周密计划，保证恢复流程滴水不漏。

避免停机和数据被盗造成的损失。未雨绸缪，使用我们的网络恢复步骤清单做足韧性准备。

第 1 阶段

第 1 阶段 | 30 天

立足当下，打牢基础。

确认当前有哪些立即可用的措施来保护业务。

- 为所有工作负载创建保护和保留策略。
- 使用防篡改存储。
- 实施 3-2-1 备份措施，即三份副本、两种存储介质、一份异地存储副本，包括虚拟和/或物理气隙隔离存储；SaaS 隔离至关重要。
- 应用安全控制措施（例如 MFA、MPA、网络分段、基于角色的访问控制、加密）。
- 考虑部署专用的强化设备。
- 启用基于人工智能的异常检测。
- 启用恶意软件检测和保留规则。
- 更新软件和安全补丁（持续进行）。

第 2 阶段

第 2 阶段 | 60 天

主动管理，防范风险。

重点关注人员、流程和技术。

- 确定“被忽视的”关键资产。
- 开展暗数据评估。
- 发现并分类敏感数据。
- 识别并监控最终用户的高风险行为。
- 创建隔离恢复环境 (IRE 或干净空间）。
- 制定恢复运行手册，确定操作的优先顺序。
- 集成安全运营功能并制定事件响应实战手册 (例如：集成 SIEM / SOAR / XDR）。

第 3 阶段

第 3 阶段 | 90 天

优化、演练、调整。

- 根据服务级别协议 (SLA) 调整数据保护策略，实现 100% 备份成功率。
- 优化基于人工智能的异常检测（消除误报/漏报）。
- 执行桌面演练，包括零中断恢复。
- 演练恢复并验证效果。

查看完整的网络恢复步骤清单 ›

VERITAS

400-120-4816 ▪ veritas.com/zh/cn/