客户案例

旅游和交通

客户挑战

因网络攻击导致恢复时间过长而无法恢复正常业务运营，客户将面临破产风险。因此如果未来发生网络攻击和宕机事件，客户希望能够显著缩减 IT 环境中关键数据的恢复时间。

成果

IBM 承诺提供 7 天期 SLA，在 7 天内恢复客户系统和数据，显著缩短恢复时间（过去超过 30 天），这降低了客户在未来发生网络安全攻击事件时再次遭遇长期业务中断的风险。提议的解决方案包括 7 天期 SLA 管理服务，负责报告、定期更新文档（运行手册等）以及协调所需资源。

客户案例

石油和天然气

客户挑战

客户的整体目标就是让 IBM 提供业务连续性和安全性综合建议，包括推荐一个为期三年的计划来实施选定灾备方案。

成果

IBM 准备了三种灾备方案，说明了相关成本以及每个方案的优点和缺点，以便为客户提供未来三年的方向和规划。该团队还提供了详细的恢复方向、灾备方案的具体规模 / 工作量 / 成本。根据这些信息和安全评估建议，我们共同为客户准备了执行演示报告和三年期路线图。

100%
成功履行承诺，满足客户事件应对要求

您真的准备好应对网络攻击了吗？

企业需要一种统一的网络安全永续的生命周期方法，覆盖信息安全、业务连续性、敏捷网络和组织灾备功能，以便能够缓解新出现的网络风险。

4000 多名
专业人士专门从事业务连续性工作

3500 多项
安全专利

管理 **2,5**
BE 的客户数据

遥遥领先
在企业安全软件和服务领域拔得头筹

IBM 守卫着 **80%**
的财富百强企业

7500 多名
安全专业人士

IBM CYBER RESILIENCY（网络安全永续）全生命周期框架

三大要点

安全

如果客户全球范围内的电子邮件、活动目录、VoIP 和笔记本电脑及桌面基础设施几个小时内被摧毁，那么他们毫无招架之力。

灾备

大多数公司都拥有业务连续性和灾备计划，但这项计划并不适于处理网络攻击。

网络

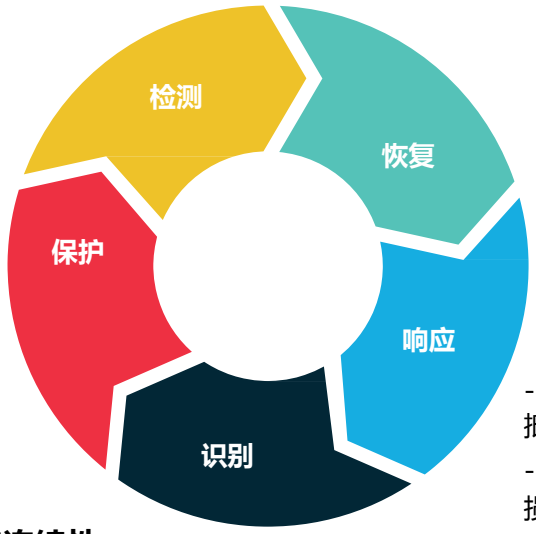
部署时间超过五年的网络往往缺乏连续性和灾备能力。客户将无法分割重要工作负载与其他工作负载。

利用高级分析来检测未知威胁

- 洞悉整个企业中的攻击情况
- 调查隐藏在企业内部的活动威胁
- 检测来自企业外部的攻击

恢复对关键数据和应用的访问

- 重建关键任务型业务应用
- 从备份中恢复数据
- 对网络资源划分优先级，加快恢复速度



防御攻击

- 攻破恶意软件和漏洞利用程序
- 发现漏洞并修补系统
- 自动修复漏洞
- 以“零信任”作为网络策略的指导准则

响应网络攻击事件

- 与网络事件响应人员沟通威胁情报，抵抗攻击者
- 通过恢复系统和关闭漏洞，修复攻击损坏部分
- 利用网络资源抵御外部威胁

确定您的网络连续性计划

- 评估网络连续性准备状态、流程和形势
- 定义一个路线图和行动计划来实施改进。

了解更多信息，请访问：
www-935.ibm.com/services/business-continuity/cyber-resilience