# 基于人工智能的网络韧性创新功能

## 消除混乱干扰，轻松恢复常态化运行，无惧网络威胁攻击

### 引言

过去两年，全球超过 65%[1] 的企业遭遇过网络中断事件，给企业造成严重影响。它是全球企业共同面对的严峻威胁，必须竭力避免。网络威胁、停机及其造成的损失，乃至政府部门不断出台的新政策法规，使得企业对**更简捷、更智能、更快速**的网络韧性解决方案需求巨大。

### 网络恢复现状

网络恢复流程通常比较复杂、低效且充满不确定性。整个流程要求各部门之间配合协作，通常由 IT 部门主导，但 IT 员工经常任务繁重，技能培训也有不足。企业平均恢复时间已上涨至 19 天，高于 2022 年的 15.7 天和 2021 年的 6.7 天[2]。2023 年，只有 35% 的企业表示他们可以在一个月内恢复，与 2022 年的 52% 相比出现大幅下降[2]。有些企业的恢复时间甚至长达三个月。

恢复能力不足对企业的财务和声誉影响深远。网络中断事件令企业遭受的平均损失高达 273 万美元[2]，这个数字在过去两年中几乎翻了一番。不仅如此，网络事件还会伤及品牌信誉和公众信任，造成额外损失。例如，米高梅度假村最近的网络中断耗时 10 天才得以恢复，损失估计近 1 亿美元。西雅图机场勒索软件攻击引发航班中断和客户滞留等一系列公众事件，对企业及社会造成重大影响。这些都凸显了网络安全和恢复的重要性。

### 高效网络韧性需求

要在复杂环境中守护数据安全，企业可尝试利用 AI 赋能的解决方案提升安全性，推进恢复流程，这在员工任务繁重和培训不足的情况下，尤为可行。而且，迅速可靠的恢复也是减少停机时间，维护企业声誉的重要保障。行之有效的网络韧性解决方案应做到充分的智能化、透明化且用户友好，使企业更简捷、智能、快速的实现恢复，同时满足严格的政策法规要求。

### 网络恢复面临的主要挑战：

- **缺乏自动化恢复方案：**许多企业缺少可整合各层级应用程序的自动化恢复蓝图，而这样的蓝图有助于消除网络恢复过程中的各种干扰和无序。
- **多团队协调：**卓有成效的恢复要求 IT、数据管理、安全团队和其他团队之间密切协作。
- **威胁和恶意软件管理：**确保恢复的数据不含有恶意软件或漏洞。
- **备份平台还原：**一旦备份平台遭到攻击，务必快速还原。
- **数据点识别：**要从 90,000 多个潜在数据点中找到最佳恢复点，工作量庞大。
- **干净的恢复环境：**将数据恢复到“干净”的环境，防止再次引入威胁。
- **技能短缺：**专业 IT 人才短缺加剧了恢复难度，45% 的 IT 领导者表示员工缺乏数据安全技能，29% 的 IT 领导者表示员工的数据保护专业知识欠缺。

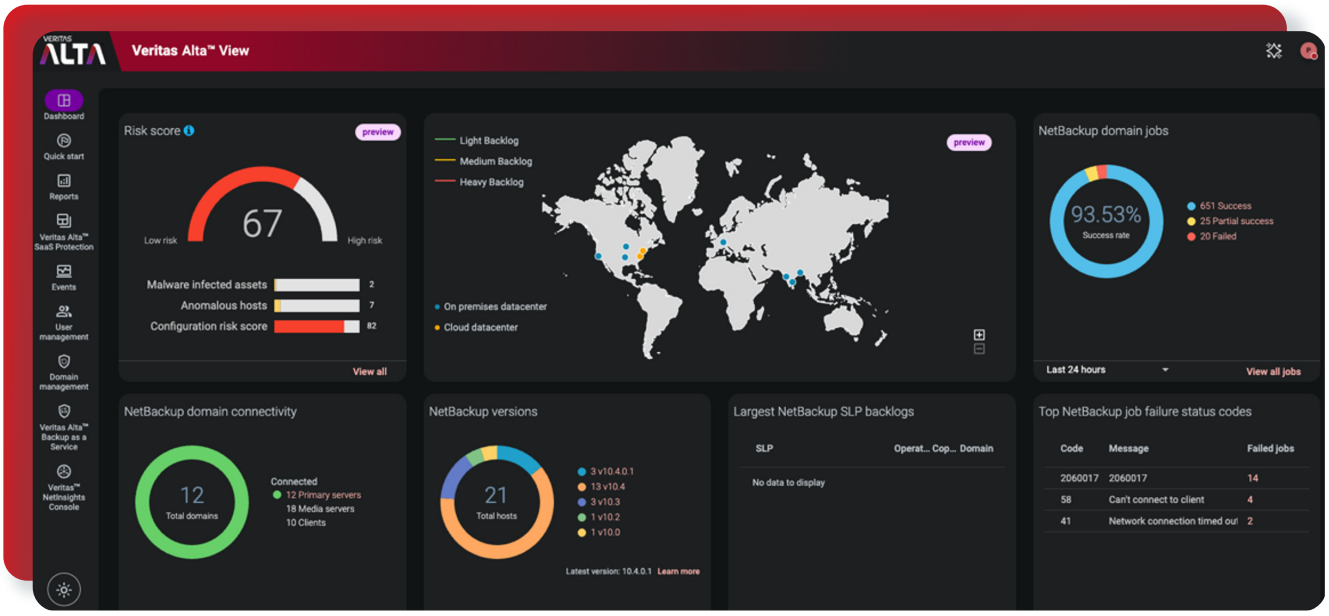
## Veritas 增强型网络韧性解决方案

Veritas Technologies 一直以来都是网络安全领域的领导者，其网络韧性解决方案采用美国国家标准与技术研究院 (NIST) 框架构建并可按需扩展。该框架的五大核心原则是：识别、保护、检测、响应和恢复。Veritas 基于这些原则推出强大、可扩展的解决方案，帮助大型企业解决痛点问题。Veritas 遵守这些基本原则，在技术上不断创新，不仅可以安全守护数据资产，还能够确保企业在遭到攻击后可迅速恢复正常运营，从而在同类企业中脱颖而出。

Veritas 作为行业领导者，近期的创新目标是不断提升网络韧性功能，让网络恢复更简捷、更智能、更快速。新功能的开发将侧重于提高自动化水平，优化威胁智能检测以及简化数据管理实践，提高数据保护策略的主动性和可预测性。例如，Veritas Alta™ Copilot 引入智能自动化，显著减少了恢复时间和人工操作。Veritas 产品的持续演进不只是为了适应复杂多变的威胁形势，也是为了在恢复的简便性和快捷性上树立行业新标杆。这一系列改进体现出 Veritas 的战略转变，即着力打造集成度更高、用户体验更好的解决方案。这些解决方案尽可能地化解了操作复杂性，最大限度提高了运营效率和掌控度，从而确保 Veritas 始终稳立数据保护行业的领先地位。

### 更简捷

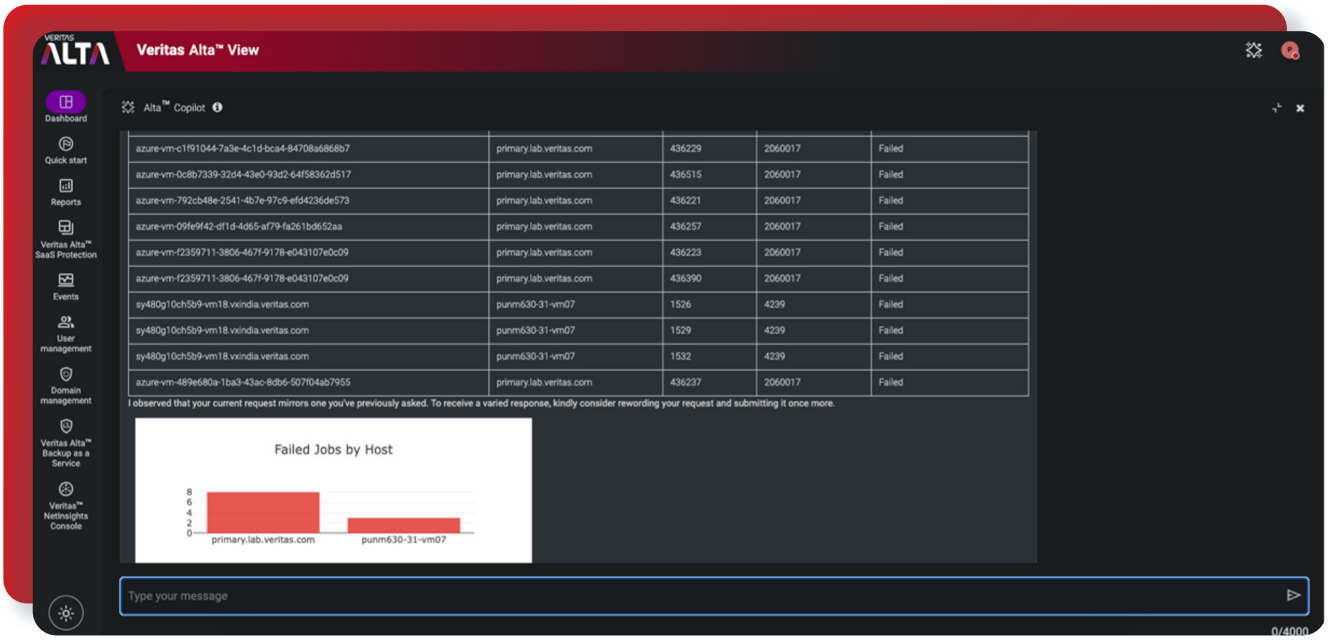
- **提升用户体验：**现代、直观的 Veritas Alta 全新用户界面，导航功能更加精简，有效简化数据管理。




- **自动创建保护策略：**运用人工智能提供数据保护策略的优化建议并自动实施，从而简化安全策略的制定和实施。
- **审查和保护未检测资产：**增强发现和保护前期未检测到的数据资产的能力，全面保护资产安全。

## 更智能

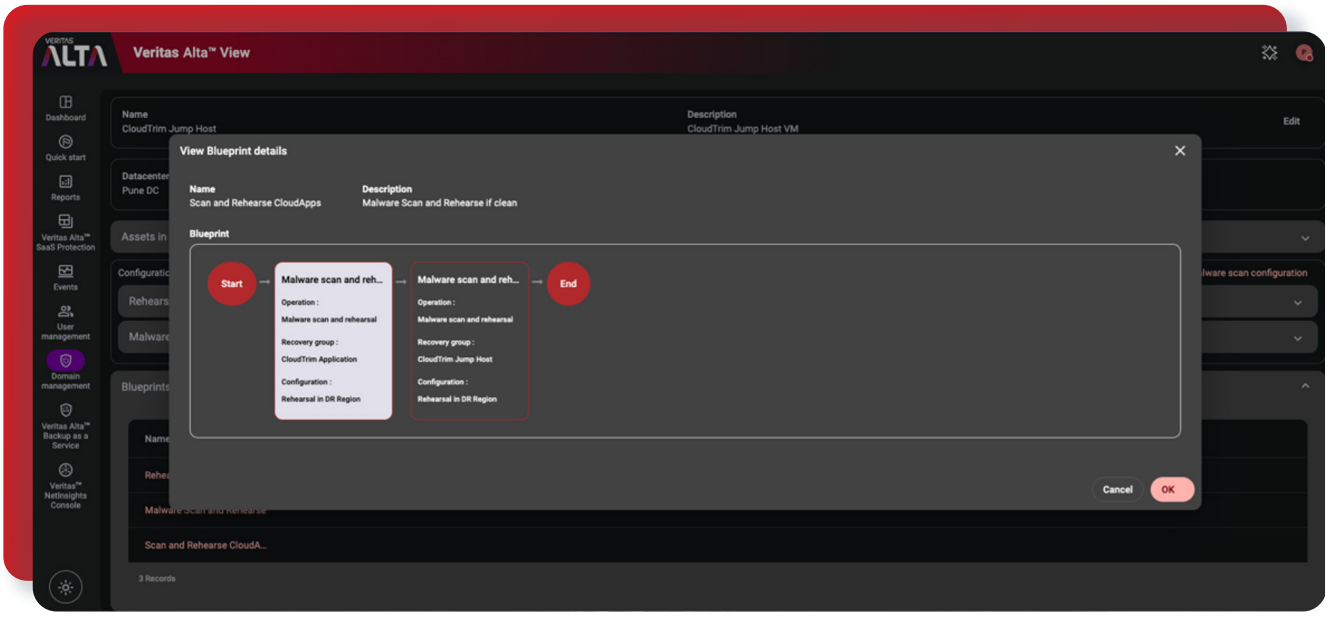
- **智能分析备份作业失败原因：**借助人工智能洞察环境，发现并解决备份失败的根本原因，确保数据保护的一致性。




- **AI 增强型恶意软件检测：**运用更先进的人工智能技术检测并缓解所有数据资产可能面临的威胁。
- **加速威胁搜寻和爆炸半径分析：**运用哈希算法的恶意软件检测和有效的文件索引来加速威胁检测，遏制潜在危害的发生。

## 更快速

- **智能恢复点建议：**运用高级分析获得最佳恢复点建议，实现恢复速度和数据完整性的最优平衡。
- **可编排定制的恢复蓝图：**推出客户定义的自动恢复工作流程，整个流程可根据客户特定的恢复目标和合规要求进行定制。



- **灵活的跨云恢复：**推进跨多个云环境的数据恢复，确保在特定云平台中断或被攻击期间，保持业务的连续性。
- **安全评估和全局风险评分：**通过备份频率和潜在漏洞等多方面评估，全面掌握安全态势。

## 总结

Veritas 在网络韧性领域继续保持着领先地位，为企业倾力打造更简捷、更智能、更快速的恢复解决方案。这些解决方案可有效简化数据管理操作，缩短了恢复时间，并保证企业满足各项政策法规要求。Veritas 的创新工具可帮助企业从容应对当下及未来的网络威胁，化解恢复的复杂性，确保业务的连续性，避免企业声誉受损。采用 Veritas 解决方案的企业可以全面保护其数据，快速从网络事件中恢复正常运行，维持运营效率，彰显其强大的网络韧性，进而提升客户的信任度。

如需了解有关 Veritas 如何增强企业网络韧性的更多信息，请访问 veritas.com/zh/cn/alta/view 或立即联系我们。

1. Veritas https://www.veritas.com/content/dam/www/zh/documents/analyst-report/AR_veritas_data_risk_management_report_2023.pdf
2. Statista: https://www.statista.com/statistics/1422159/us-healthcare-ransomware-attacks-downtime-average-by-days/

## 关于 Veritas

Veritas Technologies 是安全多云数据管理领域的领导者。超过八万家企业级客户，包括 91% 的全球财富 100 强企业，均依靠 Veritas 确保其数据的安全性、可恢复性和合规性。Veritas 在规模化的可靠性方面享有 盛誉，可为企业提供抵御勒索软件攻击等网络威胁所需的韧性。我们支持 800 多个数据源、100 多个操作系统以及 1400 多个存储目标，这样的执行能力在业界尚无出其右者。凭借云级备份技术支持，Veritas 正在实现其自治数据管理的战略愿景，帮助您减少运营开销，为您带来更高价值。如需了解更多详细信息，请访问 www.veritas.com/zh/cn/ 或关注 Veritas 官方微信平台：VERITAS_CHINA（VERITAS 中文社区）。

VERITAS

北京市海淀区中关村科学院南路 2 号
融科资讯中心 C 座北楼 16 层
100190
咨询服务热线：400-120-4816
www.veritas.com/zh/cn

关于全球联系信息，请访问：
www.veritas.com/zh/cn/company/contact/



V2128 09/24