VERITAS

直面网络韧性威胁

借助 Veritas 360 度的网络韧性蓝图全方位应对当今网络威胁

面对手段狡猾的勒索软件攻击，唯有着眼于综合防御，方能缓解数据泄露影响。Veritas 360 度的网络韧性蓝图将传统独立的数据保护、数据安全和数据治理架构融合一体，打造全面统一的管理平台，确保数据始终安全、可快速恢复且合规。

73 天

从发现漏洞到遏制影响所需的平均用时。[1]

如今，网络威胁日嚣尘上，各职能团队亟需通力协作，共同对抗网络威胁，努力减轻攻击对运营、收入和品牌声誉的负面影响。过去各职能部门各自为政，采用五花八门的工具（通常还涉及自定义代码）来检测和缓解攻击风险，导致恢复进程缓慢。这种“DIY”式方法会引入漏洞，让发起威胁的不法分子有机可乘。

Veritas 360 度的网络韧性蓝图将 Veritas 产品组合中的核心功能与网络安全合作伙伴生态系统中的预集成解决方案相结合，旨在：

- 巩固您的安防城墙
- 化解单重和双重勒索软件攻击的影响
- 从容快速恢复运行，提高业务韧性

Veritas 360 度的网络韧性蓝图是业界首个可扩展的体系架构，整合数据保护、数据治理和数据安全功能。它还推出了一系列广泛多元的网络韧性功能，经认证可与我们生态系统中顶流网络安全供应商的产品功能相集成，充分体现我们的差异化竞争优势。Veritas 秉承“主动筑起安全屏障、安全为本”的设计理念，在 Veritas REDLab 实验室中严格测试了 Veritas 360 度的网络韧性蓝图功能，证明它可以抵御现实世界的多种勒索软件攻击（REDLab 详情见下文）。

八大功能体现差异化竞争优势

Veritas 360 度的网络韧性蓝图

防止数据损坏

1. 异构资产盘点

全面可见性功能确保所有数据保护到位，帮助用户从容精准地恢复。运用生成式人工智能和大语言模型驱动的解决方案，简化企业数据管理，赋能 IT 团队洞察整个 IT 系统，包括服务器、存储、网络、管理程序、云基础架构、混合云和传统基础架构。Veritas 提供深度备份报告功能，甚至可跨其他供应商进行综合报告。您还可以生成成本分摊报告、SLA 报告，以及生成提醒和工单流程。

2. 整体数据安全态势管理

发现、分类和监控非结构化数据，可防止数据被盗和未经授权的访问。监测元数据和活动，可检测和分析用户行为、权限问题以及异常和恶意行为，从而及时拦截内部威胁。Veritas 的差异化优势在于其广泛的数据覆盖范围、全面分类以及跨内容源（包括语音和图像）的关联能力。部署 Veritas 解决方案，即可对自身拥有的数据以及数据存储位置了如指掌。万一发生攻击事件，用户就能迅速查明攻击者是否访问了敏感数据。我们将即时通知利益相关方，报告是否发生了数据泄露、潜在的内部风险以及事件的严重程度。

3. 多项数据分类

Veritas 采用预置的数据隐私策略和特定于垂直行业的策略，对内容进行分类。分类不仅限于 REGEX 和关键词，还包括模板匹配、文档相似性和情感分析。快速扫描和定向扫描能够帮助您快速了解大型数据资产。这有助于企业快速评估大量数据源，探明风险最大的资产。

4. 多层防篡改保护

Veritas 的端到端数据防篡改保护广泛支持各种存储平台。这种多层保护从网络、用户和系统出发，充分保护备份目录、存储 API 和访问权限的安全性。该解决方案可在云中运行，支持对云端和本地备份实行防篡改保护。它也可将通信信息保存到防篡改存储中，除了保护通信记录，还帮助企业及时查找通信，确保满足行业法规。Veritas 一体机内置安全的存储合规时钟和控制功能，可防止未经授权的数据访问，即使是拥有完整权限的管理员也不例外。Cohasset Associates 对 Veritas 一体机进行了严格评估，证明其符合美国证券交易委员会、美国金融业监管局和美国商品期货交易委员会的各项规定。

增强网络防御

5. 异常行为检测

根据活动和角色对用户进行分析，识别有问题的数据、应用程序和资源活动，包括拥有完整权限的 IT 管理员执行的活动。您可基于用户风险分数来评估潜在威胁，优先处理高风险数据，防止数据被盗和损坏。早期预警提示可显示背景信息，扩充数据外泄警报范围，方便您及时调查，以免造成实质损害。自适应的自防御算法可从您对用户操作的批准或拒绝结果中学习经验，然后将其应用到下次异常提示的推理中。

6. 最终用户情绪分析

从 120 多个内容源采集数据并进行分类，以检测违反公司政策和行业法规的行为。情绪分析会使用自然语言处理技术，从原始材料中识别和提炼主观信息。根据转录的音频或书面内容识别态度、情感或情绪，以深入了解内部人员风险，并标记相应内容供人工审核。

值得信赖的可编排恢复

7. 基于 Pull 的恢复环境

基于 Pull 的复制技术可防止攻击者将受感染数据推送到隔离恢复环境。它会创建虚拟气隙隔离，仅允许隔离环境请求的授权数据进入环境。这项实施并不需要配备第三方工具或高薪聘请顾问。

8. 可扩展的编排恢复

可执行复杂的应用程序编排恢复，支持“一键式”依赖关系映射和自定义操作。它还支持用户在生产环境中进行零中断演练，从备份和复制系统中恢复数据。即便真的发生网络事件，也可以快速稳妥地恢复。

VERITAS REDLab

在 Veritas REDLab 中的威胁实测

在 REDLab 中，Veritas 围绕勒索软件和恶意软件攻击展开第一手研究。在这个完全隔离的实验室中，我们定期模拟威胁演练，对产品发起真实的勒索软件和恶意软件攻击。REDLab 团队将评估产品各项功能表现，例如是否可快速检测网络攻击、保护备份存储库和基础架构并确保成功恢复。事实证明，REDLab 为解决方案的可靠性和未来路线图的规划提供了极具价值的评估数据。此外，合作伙伴的集成产品也在真实攻击场景中得到可信验证。

了解更多关于 Veritas 360 度的网络韧性蓝图

数据保护、数据安全和数据治理解决方案与我们网络安全合作伙伴生态系统中的产品功能相结合，打造全面统一的管理视图，解决企业对数据安全、快速恢复和合规运营的迫切需求。了解 Veritas 360 度的网络韧性蓝图及其如何全面应对当今网络韧性威胁。

1. IBM 2023 年《数据泄露的成本》报告

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/

Copyright © 2024 Veritas Technologies LLC. © 2024 年 Veritas Technologies LLC 版权所有。All rights reserved. 保留所有权利。Veritas、Veritas 标识和 NetBackup 是 Veritas Technologies LLC 或其附属机构在美国和其他国家/地区的商标或注册商标。其他名称可能是其各自所有者的商标。

V2014 04/24