VERITAS

未雨绸缪
防范未然

持续引领新未来

数据保护和恢复并不是一场游戏，而是一项长期艰苦的任务。

数据威胁呈现出从量变到质变的趋势，不法分子不断研究新的手段来攻击和破坏企业的生命线——数据。

数据保护也从一个项目发展成企业文化的一部分，而且其重要性还在不断加强。工作负载的种类和位置、每个应用程序及数据的重要程度是评估保护级别和恢复方式的关键要素。

高可用性、治理、合规等也是关键因素，它们会影响到恢复时间目标 (RTO) 和恢复点目标 (RPO)。

影子 IT 和技术负债已经迅速蔓延开来。企业各部门不仅创建了海量数据，还错误地将关键任务数据置于易受攻击的位置。因缺乏对数据的全局可见性，企业很难确定数据的优先级，更别提缓解数据风险。

您需要秉持前瞻性思维，加之以持续的努力，才能站在趋势前沿，从容应对未来的一切潜在挑战。

了解您的数据

看不到的数据，如何充分保护到位？

企业会采用大量应用程序和平台希望提高工作效率，为员工提供更有价值的数据。不过，员工通常都是独立地使用各种不同工具，同时将客户信息和公司数据存储到云平台。结果如何？公司数据无序蔓延，多云覆盖的挑战也接踵而至。

这给不法分子带来可乘之机，因为公司并没有妥善保护这类数据。无人察觉数据上发生的可疑行为，IT 团队可能根本没意识到应该关注这部分数据，甚至不知道它们的存在。一旦灾难来袭，您才突然发现关键信息没有妥善备份，数据无从恢复。

问题在于，灾难发生后我们才意识到这部分信息很重要，但由于没有妥善备份，如今再也无法恢复。

数据无序蔓延是企业要直面的一大治理挑战。为此，企业不但要提高基础架构可见性，还需要搭建额外的环境和进行员工培训。

要获得理想的治理成效，企业最好将数据置于环境背景中进行流程的评估，再据此决定如何执行边缘、核心和云中的备份与恢复。

关键问题：

- 您拥有哪些数据，它们位于何处？
- 如何提高数据的可见性？

Veritas 解决方案

Veritas 数据保护解决方案可提供大规模数据保护。基于人工智能的异常检测引擎有助于监测海量数据，建立潜在攻击预警机制，自动监控并报告，并提供可操作的洞察。

Veritas Analytics 解决方案可在备份供应商之间交叉引用服务器和存储中的数据，确保数据无一遗漏，也没有安全漏洞。它可以扫描和监控所有系统，包括第三方产品，帮助消除系统盲点。

Veritas Data Insight 提供丰富的报告功能，可检测潜在受感染的数据，限制对敏感数据的访问，支持数据所有者协同工作，以做出更明智的决策并始终遵守合规标准。它不仅可发现风险、揭示暗数据并记录大量用户活动，还可透过用户行为模式，识别和检测异常。

将不法分子拒之门外

犯罪分子深谙人是网络攻击中最易攻克的薄弱所在。

大部分网络攻击和数据泄露都是源于人际互动和警惕性降低。这也是网络钓鱼骗局屡屡得逞的原因。

如何防止攻击？身份和访问管理以及加密等都是必不可少的措施。同时，您可以实施多重身份验证和基于角色的访问控制，以有效降低攻击的成功率。传输中和存储中的数据加密可增加数据访问难度，有助于防止数据泄露。智能卡身份验证、单一登录和特权访问管理等措施强化了基于零信任的“最低权限”原则。

分层防御和保护策略是指在不同层面实施不同的解决方案。您可以（并且应该）为设备颁发数字证书，实施进一步的身份验证，即在访问备份时，要增加一层验证，实施双重身份验证。

访问权限和数据保护的管理更是重中之重，以避免出现配置错误。无论是在本地还是云环境中，限制以及强制实施某些权限的前提是要识别和了解环境中的资源、操作和身份。跟踪和监控更改数据的行为和进度，有助于您掌握安全状态，实时调整应对措施。

关键问题：

- 目前您采取了哪些措施来防止网络钓鱼和恶意软件的入侵？
- 当前的保护措施还能进一步改进吗？

Veritas 解决方案

Veritas 数据保护解决方案基于零信任基础构建，不受供应商限制。它运用 AES 256 位加密技术对传输中和存储中的数据进行加密，满足 FIPS 140-2 认证要求，限制用户访问权限，启用基于角色的访问控制和多重身份验证，可全面保护您的网络。

Veritas Data Insight 提供生产数据近乎实时的可见性，可基于用户异常行为和已知的勒索软件扩展名识别勒索软件。它还能发现过度暴露的数据，限制和减少攻击面。

Veritas Analytics 解决方案在统一控制板上显示运行信息和洞察，帮助识别勒索软件、未受保护的系统以及备份异常，有助于您优化存储、降低成本，并始终遵守合规和监管要求。

Veritas Alta™ Classification 为您扫清数据安全和合规道路上的障碍。通过收集元数据属性和用户行为取证，生成可操作的洞察，确定数据所有权、使用情况以及访问权限，降低数据隐私和安全风险。

发现重要但保护不到位的数据

您的数据并非静止不动，因此您的策略和解决方案也不能一成不变。

请确保采用可扩展、可适时调整的产品和服务。因为企业要在跨多云且多重集成的压力下满足高性能需求，就必须保持灵活。

一家企业一次性购买单一供应商的全部解决方案，这并不现实。因此，业务开发通常步履维艰：企业基础架构既包含旧式传统软件和技术，又部署了新一代尖端解决方案，各种技术混杂在一起。

您需要对数据进行优先级排序，明确合规级别以及要遵守的法规要求。制定备份管理方案，备份大小和最终的处理方式会直接影响恢复时间。了解您的带宽会对备份和恢复产生何种影响，据此制定备份和恢复策略以及关键工作流程。

关键问题：

- 哪些数据是维持业务正常运行的重要资源？
- 如何确定数据备份的优先级？

Veritas 解决方案

Veritas 数据保护解决方案不受供应商限制，提供可靠的数据保留和保护工作流程，既经济实惠，又易于部署和管理。我们将解决方案便捷地整合到统一平台，可跨多云和混合云环境运行。

Veritas Alta™ Shared Storage 可支持关键业务应用程序，为企业级共享存储提供卓越性能和韧性，同时节省成本。它赋能应用程序和基础架构管理员保护敏感数据，并提供加密、“一次写入、多次读取”(WORM) 存储、一致性快照和数据库加速等功能。

Veritas Alta™ SaaS Protection 支持您在员工离职后继续访问他们在 Microsoft 365 帐户中存储的数据，无需维护和支付额外的许可证费用。多层粒度恢复功能支持您轻松还原文件夹、邮箱或站点，而且可还原到任意位置（无论云端还是本地）。备份存储扩展到 PB 量级，可包含数十亿个对象，最大限度优化性能和灵活性。同时，它可提高增量备份的频率，最大限度缩短 RPO 和 RTO，并对站点实施持续数据保护。

实现数据和备份的高可用性和高效性

您已备份了数据，但为何灾难来临时，还原数据仍如此困难？

迁移海量数据（如移动到辅助存储）要消耗大量时间和计算资源。关键是这并非一次性操作。如果您采用的是 3-2-1 备份原则，则必须要迁移三次，分别迁移到两种不同存储介质，还要迁移到异地以增加额外一重保护。

在迁移过程中，可能会出现很多状况导致完全备份失败。因此，高可用性和故障转移就非常重要。这好比将水壶里的水倒入玻璃杯中；当一个杯子溢出时，第二个杯子就可以存放多余的水。负载均衡会评估哪个系统可处理您的请求，然后合理分发工作负载。您可将多台服务器划分为一组，在出现问题时及时启动故障转移，以确保服务的高可用性。一旦一台服务器失败，另一台服务器可取而代之，确保不会丢失待备份的数据。

关键问题：

- 我们需要从何处入手，提高备份效率？
- 如何得知我们的备份是干净、未被感染且未损坏的？

Veritas 解决方案

Veritas 数据保护解决方案可轻松实施 3-2-1+1 备份策略，同时内置入侵防御系统，可运用气隙隔离环境保护不可擦除存储和内置的隔离防篡改数据保管库，以进一步提高安全性。

Veritas InfoScale 借助数据快照和映射将生产数据与 I/O 隔离开来，保护生产数据免遭攻击。它还可以优化数据恢复以实现低 RTO 和 RPO 目标。您可以对隔离的数据卷运行恶意软件扫描，确保系统没有被感染。

Veritas NetBackup Flex 和 Flex Scale 通过消除硬件中的故障点，增加额外的安全保护。它们采用群集组件，确保设备始终可用。

Veritas Analytics 解决方案可根据以往的成功备份创建一系列基准，作为未来备份的参照，帮助您及时发现异常。您还可以按应用程序对备份进行分类，从单个控制板查看所有应用程序的可恢复性。

运用气隙隔离和防篡改数据保管库保护数据

如何确保备份数据不被篡改?

即使公司勤于备份数据，也难免不会发生人为错误和设备故障。而且，数据还容易被意外删除或修改。

您的备份方式必须确保数据不会被更改。文件存放在防篡改存储中，就能有效杜绝数据损坏，防范网络攻击。

防篡改备份可为企业带来最高级别的数据保护。数据永久性是防篡改存储提供的基本保障，文件不会被意外或故意篡改。此举可在网络安全和灾难恢复战略中构筑更高效、更可靠的流程，避免因停机等事件给企业造成经济损失。

增加多一层气隙隔离安全保护，可确保您的防篡改备份数据处于隔离状态、无法被访问及损坏，保证您从干净数据恢复。

关键问题：

- 我们目前有何保护备份的措施?
- 合规标准中是否要求您必须对数据实施气隙隔离?

Veritas 解决方案

Veritas 依据 NIST 原则实现数据的防篡改、不可擦除、可见性和快速恢复。它支持运用多种方法保护现场和异地数据，包括基于磁带的备份、基于云的锁定对象存储以及 AWS S3 Object Lock 中的高效数据存储。

Veritas 数据保护解决方案可在操作系统采取行动之前，主动拦截恶意的资源访问行为。

Veritas Flex 自带防篡改数据保管库，同时支持隔离恢复环境 (IRE)，保证 IRE 中的关键备份数据防篡改且始终安全。IRE 架构除了保护您的重要备份之外，还提供隔离安全环境，您可在此编排安全的数据恢复或演练网络韧性恢复计划。Veritas 独立于基础架构的虚拟气隙隔离技术通过增强安全保护和隔离，化解恶意攻击。

制定灾难恢复流程

理想的恢复解决方案应支持每一种工作负载。

您不妨从创建恢复流程入手。该流程不但要能轻松进行集成，还应满足所需的 RPO 和 RTO 目标，支持所有存储，并提供统一的控制板，以管理所有受保护的负载。制定流程时，您应全盘考虑相关因素，例如：

- 编排恢复流程（决定恢复顺序）
- 智能重复数据删除
- 快照集成
- 存储分层
- 自动复制图像、目录和快照到本地和云端存储
- 容器支持
- 数据洞察和分析
- 面向本地和云端的灵活性、安全与合规
- 运用加密技术确保数据和备份系统得到全面保护

您可以运用零信任原则、多层数据安全保护以及智能自动化等技术，确保业务运营具备韧性；运用集成式解决方案，解锁多云智能、升级网络防御，并削减成本；整合面向云端工作负载的备份和恢复、自动迁移工作负载、实施一键式恢复（完全无需额外人工操作）、自定义脚本和恢复演练，以遵守不断变化的法规要求，最大限度降低成本。

关键问题：

- 我要多久才能恢复？
- 恢复的优先级如何？

Veritas 解决方案

如果只有一部分文件损坏，您可以选择裸机恢复或粒度文件恢复。若是虚拟机恢复，还可使用即时回滚功能，在几分钟内并行回滚数百台虚拟机。

Veritas Resiliency Platform 强化的数据韧性功能，支持您分配应用程序的恢复优先级，根据业务重要性按顺序逐层恢复。持续数据保护检查点可保证较低的恢复 RPO。

Veritas NetBackup Flex 和 Flex Scale 采用强化的操作系统、零信任架构以及防篡改且不可擦除的存储。IRE 和防篡改数据保管库提供气隙隔离解决方案，使外部人员无法觊觎存储。恶意软件和异常扫描可保证您的备份数据始终干净，支持您立即恢复数据，无论数据在本地还是云端。

演练数据恢复，确保韧性十足

演练并不是为了恢复，而是为了最大限度避免停机。

网络犯罪分子希望您像大多数企业一样，从未优化过恢复流程。他们恨不得攻击造成的破坏力和停机时间达到最严重程度，这样您就不得不支付赎金。做好应对准备并演练恢复流程，您就向前迈进了一大步。要实现快速恢复，您不但要为整个环境制定网络安全响应计划，还要提前并经常测试。定期的恢复演练和测试有助于企业控制停机时间，最大限度减少中断，降低攻击造成的影响。

随着企业对混合云和多云系统需求的不断上涨，您不但要管理多个框架，还要协调多个云和存储系统。IT 团队还要负责服务器和应用程序的管理与扩展。

您可借助自动化管理来应对环境的复杂性，识别潜在威胁，主动安排演练，确保做好周全的准备，最大限度减少停机时间。

关键问题：

- 如何减少停机时间？
- 如何快速补救？

Veritas 解决方案

Veritas NetBackup Flex 和 Flex Scale 采用易于扩展的架构，最大限度发挥数据保护潜力。借助防篡改、自动置备和负载均衡等多层防护措施，助您部署完整的一站式数据保护解决方案。

Veritas InfoScale 和 Veritas Alta™ Application Resiliency 不仅能监控架构运行状态，还能判断运行状态是否良好。这是一款全面的基础架构解决方案，可与关键业务应用程序紧密集成，实现应用程序的高可用性和灾难恢复，并随时启用故障转移，确保业务正常运行。作为一款多功能平台，它可提供如下特色功能并根据行业需求灵活定制保护级别，例如：

- 确保数据完整性和合规
- 自动运行多层应用程序，减少人工操作
- 轻松在平台之间迁移工作负载
- 传统系统和环境无缝集成

优化备份和恢复

直面挑战，在整个企业内实现数据保护管理。

要发现流程中的瓶颈，了解最耗时的流程部分，您可以通过数据编排实现此目标。通过编排，流程将自动执行，如服务器配置、数据库和应用程序管理等，从而节省大量宝贵时间。您还可以编排漏洞扫描、日志搜索，甚至是连接安全工具和系统集成等任务，以避免团队因工作量过多而不堪重负。

选择正确的解决方案可简化数据管理，但管理是一项长期的任务。

分析技术运用得当就能洞察环境中的关键元素。深入了解环境后，您即可发现未充分利用、配置错误或未编制索引的内容，从而帮助 IT 部门解决问题，找出可重复利用的资源以节省成本。

获得可操作的洞察有助于提高资源利用率、系统性能和数据韧性，同时还可预测故障发生位置并主动提供修复建议，以规避不符合服务级别协议 (SLA) 的风险。

智能自动化有助于消除低效的手动流程，解锁无限的可能性。

实施并部署敏捷、安全的备份和恢复解决方案，可全面实现数据保护和优化。

综合性统一控制台视图有助于您监控从边缘、核心再到云环境的整个网络，简化资源管理，降低成本。

Veritas 解决方案

Veritas Data Insight 可分析各种活动，尤其是资源使用情况和协作活动。它可以对用户进行分类，让用户的活动模式更加一目了然；可以识别重复、过期或孤立的数据；还可以运用风险分数来评估潜在威胁，优先保护高风险数据。在 Veritas 合规解决方案的加持下，它可以创建详细的审计跟踪记录，集成文件分析、数据丢失防护和归档等功能。

Veritas Analytics 解决方案可快速识别存在风险的应用程序和服务。通过监控和优化所有环境中的备份，并按位置、环境或应用程序高效定位受影响的主机，加快恢复速度。

关键问题：

- 您的数据是否经过优化，可实现快速恢复？
- 您是否了解自己的 SLA？

弥补网络安全战略的短板。了解详细信息 >

关于 Veritas

Veritas Technologies 是多云数据管理领域的领导者。超过八万家企业级客户，包括 95% 的全球财富 100 强企业，均依靠 Veritas 确保其数据的保护、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等网络攻击威胁所需的弹性。Veritas 通过统一的平台，支持超过 800 种数据源，100 多种操作系统，1400 多种存储设备以及 60 多类云平台。在云级技术的支持下，Veritas 现正在实践其自治数据管理战略，在提供更大价值的同时，降低运营成本。欲了解更多详细信息，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

北京市朝阳区东大桥路 9 号
侨福芳草地大厦 A 座 10 层
04-05 单元 100020
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：
veritas.com/company/contact

V1812 04/23