VERITAS

运用气隙隔离技术加强数据恢复

维护数据的安全副本，降低网络攻击影响。

白皮书 | 2023 年 5 月

为什么要创建数据保管库

网络安全一直是企业领导者眼中的第一要务。网络威胁日渐复杂，犯罪分子越来越狡猾，同时还在不断研究新的攻击手段，目的是对受害者造成最大程度的损害。Gartner 预测，到 2025 年，40% 的董事会将设立专门的网络安全委员会，就网络安全策略、执行和恢复方面进行报告并制定战略预期[1]。网络犯罪呈指数级增长，给各大企业造成了数百万美元和数小时的停机损失，企业正在竭力减少攻击的影响，尽快恢复运行。在 2022 年里，每 15 秒就发生一次网络攻击[2]，这已成为一场争分夺秒的生死之战。因此，您的当务之急就是确保自己做好应对准备，部署战略，全力降低风险、消除不确定性并维系对环境的掌控。

韧性和恢复计划能否成功，关键在于实施可靠的网络安全框架，选择正确的技术和流程。您是否部署了网络安全事件响应计划？能否信心十足地向经理和高层管理人员汇报？Gartner[3] 指出，到 2025 年，70% 的首席执行官会在企业内建立防范网络犯罪，确保运营安全的企业文化。当前，您的首要任务是了解网络安全趋势，以及确保恢复成功的关键要素。您需要提前将勒索软件攻击扼杀在摇篮中，以便向董事会证明您实施了正确的恢复方案。

什么是气隙隔离及其重要性

网络攻击越来越狡猾难辨，黑客不仅垂涎您的主数据存储，还盯上了您的备份数据。因此，您务必在灾难恢复战略中对此做出妥善的规划。在大多数情况下，黑客会蛰伏在系统中，等待时机访问和破坏您的主数据和备份数据。一旦获取访问权限，他们就会立即摧毁数据。

依据美国国家标准和技术研究院 (NIST) 的定义，气隙是两个系统之间的接口：(a) 这两个系统之间没有物理连接，(b) 任何逻辑连接都不是自动的（即数据只能在人工控制下通过接口进行手动传输）[4]。过去，气隙是保护恒温器或家用电器等技术操作的黄金标准。现在，几乎所有设备都通过无线或有线网络连接，因此需要落实更严格的气隙隔离流程来保护用于恢复的数据副本。

在联网环境下，黑客几乎可以利用一切入口点潜入系统，即使系统中禁用了所有无线和有线信号。在保存高度机密数据的大多数封闭系统中，一些 IT 部门禁用了所有 USB 端口，并使用法拉第笼来阻止所有无线传输并防止电磁泄漏。

借助 Veritas 的自动映像复制 (AIR) 技术，您可在相同或不同站点（包括公有云）的备份域之间复制备份数据。AIR 还支持离线的气隙隔离备份副本，进一步杜绝从未知来源访问数据。企业数据不仅存储在自有数据中心，还广泛分布在各大公有云中，若您要运用气隙隔离结构来维护关键数据的最新干净副本，部署备份和恢复解决方案就显得必不可少。

云端数据和气隙隔离

云优先趋势如火如荼：85% 的企业称，到 2025 年，他们将实现云优先战略，其中 94% 的企业正在实施多云战略[5]。我们已经看到，加速推进云战略的企业越来越多，最终的局面可能会是云服务提供商的工具五花八门，决策和管理没有章法。如果您部署了多种公有云选项来扩充和优化主数据存储，务必运用最佳解决方案来备份数据，以优化数据恢复。

我们建议将隔离恢复环境 (IRE) 作为您的最佳选择。IRE 中的气隙隔离解决方案可创建关键数据的安全副本，管理员可按需启用干净的备份文件，以降低多云环境中勒索软件攻击造成的影响。

隔离恢复环境 (IRE)

传统网络隔离解决方案从物理或逻辑层面断开安全位置之间的连接，切断通信的传入或传出途径。在这种情况下，数据无法传输到隔离环境，也就无法满足企业的三份备份副本需求，进而威胁到恢复时间目标 (RTO) 和恢复点目标 (RPO)。它通常是将复制数据从来源推送到目标，来源域独立处理并提交复制作业到目标域。这种传统方法在连接中断或受阻时无法将关键数据复制到安全环境，会极大延迟恢复时间。

比较而言，拉取复制模式会从目标发起复制请求。Veritas 推出 NetBackup IRE 解决方案，通过拉取复制模式来优化数据移动。在这种模式下，发送数据的请求来自 IRE 的介质服务器数据去重池 (MSDP)，这种反向连接可以更好地控制数据流，进一步从逻辑和物理层面保护环境安全。用户可完全掌控在 IRE 内以及 IRE 间复制数据的请求，还可支持 IRE 气隙隔离时间表中定义的特定窗口期。

NetBackup IRE 采用多层安全防御措施，包括入侵防御机制、传输中和存储中数据加密，因此在数据传输过程中攻击无法渗透到系统中。在整个数据生命周期内，无论数据位于何处，都始终安全无虞且存储不会遭到感染，恶意或未经授权的用户读取或修改数据的风险为零。Veritas NetBackup Recovery Vault 带来本地和云端数据隔离功能。这是一项无缝的云存储即服务，采用气隙隔离备份抵御勒索软件攻击，而且经过优化可轻松扩展，确保数据可移植，成本可预测。

Veritas 秉持简化运行的理念，支持您将本地或云端部署的 NetBackup 转移到 IRE 框架，以三大原则为基础构建勒索软件应对韧性：

- **保护**：遵循 Veritas 零信任安全原则，轻松整合隔离恢复功能，支持多重身份验证 (MFA) 和基于角色的访问控制 (RBAC)。
- **检测**：NetBackup IT Analytics 的异常检测可实时检测勒索软件。集成的 NetBackup 恶意软件扫描功能可在恢复之前进行恶意软件扫描，根据异常评分确定风险严重性。
- **恢复**：在隔离环境、云端或本地统筹协调整个数据集的恢复，能够满足多种 RPO 和 RTO 要求。

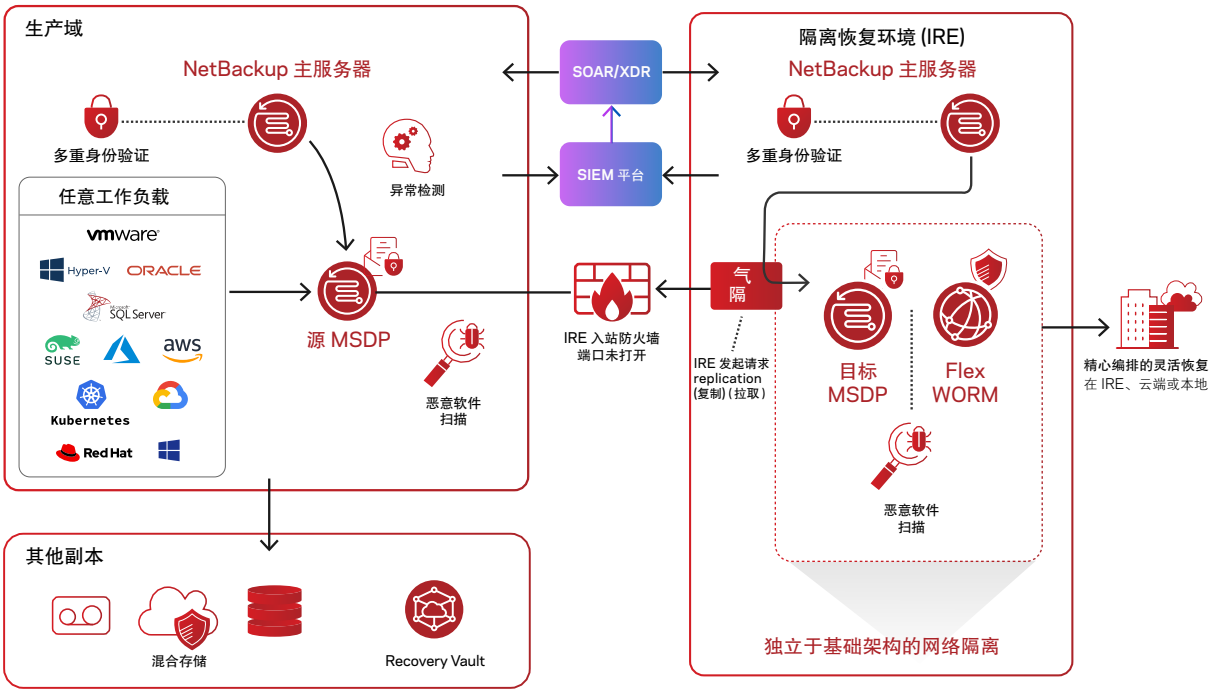

图 1：NetBackup 隔离恢复环境

隔离环境为企业增加多一重韧性保护，有效对抗勒索软件和恶意软件攻击。

运用零信任原则增强保护

采用零信任原则，进一步提升保护级别。事实证明，在全公司内贯彻零信任理念可以降低遭受毁灭性攻击的风险。

Veritas IRE 是在 Flex 一体机上构建、基于容器的多租户 WORM（一次写入、多次读取）存储。它采用零信任架构和强化的操作系统，运用多重身份验证和基于角色的访问控制 (RBAC) 强化用户、工具及设备的身份和访问管理 (IAM)，限制对高度敏感数据和备份的访问。仅需要访问数据的用户才有权限。密码保护也是关键措施之一。

您可在零信任原则基础上构建强大的 IAM 控制、权限控制、系统强化和安全硬件，以阻止他人擅自访问。即使发生攻击，也可通过多层安全防护措施缩小攻击面或攻击范围，最大限度减少影响。一旦恶意软件入侵您的系统，网络犯罪分子就会在环境中悄悄移动，搜索关键业务数据、机密信息和系统备份。

异常检测和恶意软件扫描

凭借全面可见性、智能异常检测和恶意软件扫描，您可从容掌握数据的所有存储位置，降低运行复杂性，优化成本管理。Veritas 基于人工智能的异常检测引擎可识别整个环境中的异常数据和用户活动，近乎实时地提醒您注意可疑活动。此功能可确保您的数据始终可恢复，有助于您在遭遇勒索软件攻击时立即采取行动，将备份与恶意软件隔离开来，并限制恶意软件对备份数据的影响。您可以恢复经过扫描并验证为安全的完整图像，也可以恢复单个文件。如果标记为要还原的文件受到感染，则可以从未受感染的备份中恢复该文件。这样您可安全地恢复数据，不会有感染目标计算机的风险。

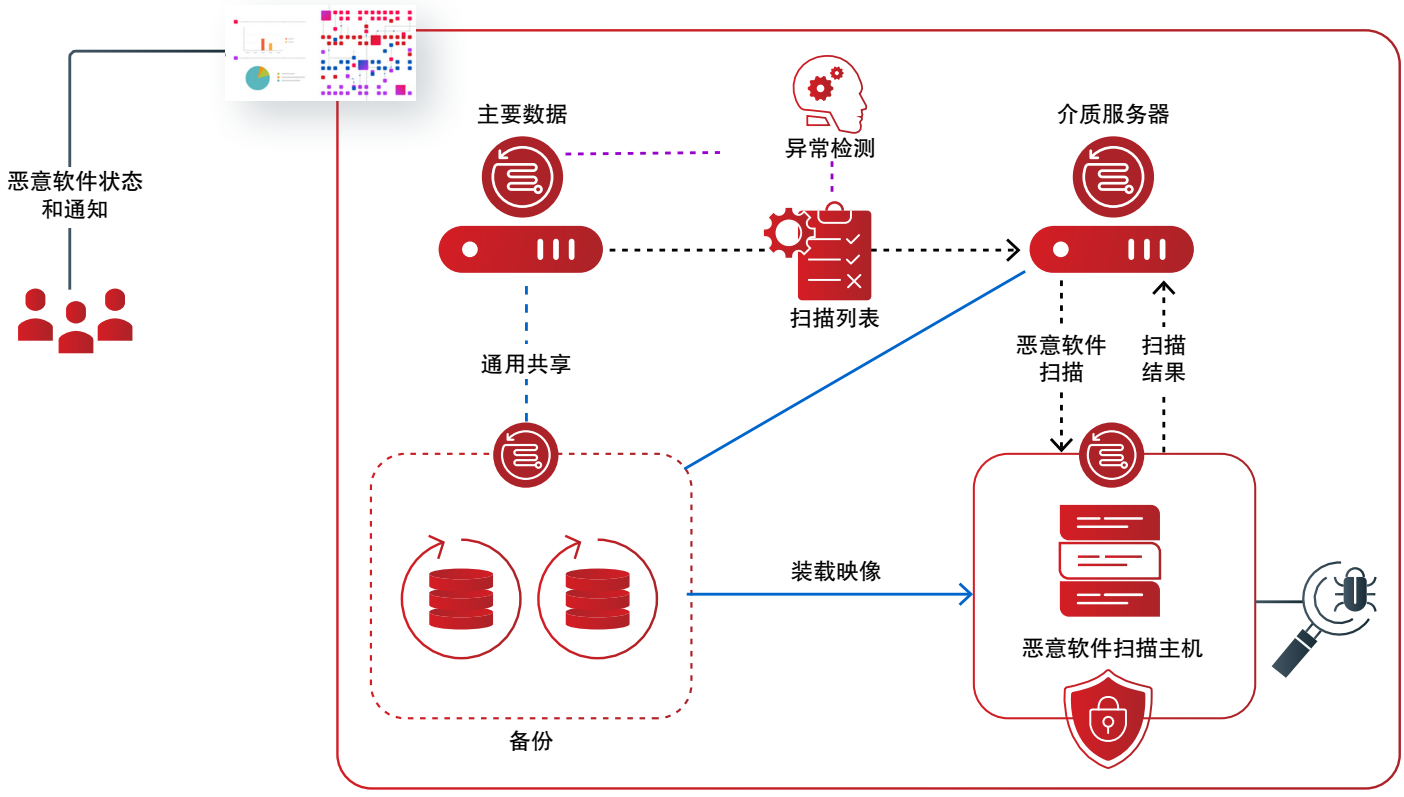

图 2：NetBackup 集成式恶意软件扫描

采用防篡改且不可擦除存储，保证数据及时恢复

防篡改且不可擦除的存储可确保在确定期限内（或数据的整个生命周期内），任何人或任何攻击都无法更改、加密或删除数据。它还能阻止数据被篡改和未经授权的访问。在 IRE 策略中，NetBackup Recovery Vault 提供云端防篡改且不可擦除的存储解决方案，您可以根据需要向上或向下扩展。

运用 IRE 从容恢复

运用 NetBackup 隔离恢复环境降低风险、消除不确定性并维系掌控权。访问 Veritas.com 或联系我们的团队，详细了解我们的解决方案如何保证多云环境中的勒索软件应对韧性。

弥补企业韧性战略的短板。了解详细信息 >

1. www.gartner.com/en/newsroom/press-releases/2021-01-28
2. www.sonicwall.com/resources/white-papers/2023-sonicwall-cyber-threat-report/
3. www.gartner.com/en/articles/the-top-8-cybersecurity-predictions-for-2021-2022
4. csrc.nist.gov/glossary/term/air_gap
5. www.gartner.com/en/newsroom/press-releases/2021-11-10

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）。

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

V1626 05/22