

通过零损失策略精准化解风险

了解勒索病毒并加以防御和恢复

实施零损失策略，为抵御勒索病毒做好准备并从勒索病毒中恢复

随着网络攻击数量逐年增加，企业面临着日益动荡的数据环境。预计到 2025 年，全球网络犯罪造成的损失每年将达到 10.5 万亿美元。¹ 工作环境的不断变化、远程就业模式的普及和勒索病毒威胁的蔓延，给 IT、网络和基础架构团队带来了更大的压力。平均而言，企业的技术预算将增加 48%，以投资于新人才和技能，从而应对所有这些变化。²

降低勒索病毒风险绝非易事，如若能引入一种策略来提供数据可见性和快速恢复能力，便有可能从根本上恢复正常业务运营。40% 到 60% 的小企业主在遭遇数据丢失问题后难以为继，对于企业来说，停机的平均成本超过每分钟 11,600 美元。³ 支持零信任原则并遵循 NIST 多层安全框架的数据环境是一个良好的开端。但如果发生网络攻击，您的企业是否做好了充分准备？您需要制定计划来持久抵御勒索病毒。



零损失策略

除了坚持零信任原则然后听天由命之外，您还可以通过最终的解决方案管理并大幅降低勒索病毒攻击的影响。该解决方案可以通过使用一个集中式管理平台来降低企业的成本，因此安全团队不需要登录和退出多个单点产品。它可以通过单一环境提高数据的可见性，尽可能为团队降低复杂性。最后，它可以通过统一的方法提供最广泛的工作负载覆盖范围和快速恢复的功能，从而保护最重要的数据。要实现所有这些目标，解决方案必须采用零损失策略。



端到端的数据可见性：

提前发现威胁，防患于未然

您必须能够查看您的数据，知道数据所在位置并保护数据。提前发现威胁，避免其影响您的业务，并通过一个可视化环境查看数据、工作负载和基础架构，无需使用不同的工具来实现数据可见性。

- 通过 [Commvault Command Center™](#) 进行集中管理，在统一的环境中查看备份和恢复状态
- 您可以通过我们的安全健康评估仪表盘查看实时和备份环境的数据指标，从而轻松检测可疑活动
- 实时监控，以便及早检测到备份和实时数据环境中的异常活动
- 通过内置了机器学习、异常检测和蜜罐技术的威胁监控框架提早收到预警

1 Cybercrime Magazine, Steve Morgan, 2021 年至 2025 年 6 大网络安全预测和统计数据, 2021 年 12 月

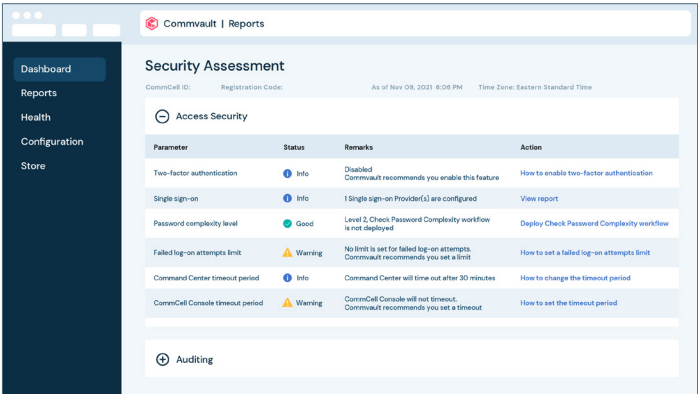
2 2022 年首席信息官状况

3 Web Tribunal, Branko K, 2022 年要记住的超过 15 项令人恐慌的数据丢失统计, 2022 年 4 月

Commvault 安全健康评估仪表盘

您可以将此视为完整的风险管理工具，为您的数据环境提供所需的端到端可见性。Commvault 云指标报告和 Commvault Command Center 中均提供安全健康评估仪表盘。该仪表盘将快速提供有关制定行动计划的见解和建议。

所有建议的控制和设置都可以在此仪表板中找到，并使用交互式操作快速实施。有关更多信息，请阅读使用 [Commvault 安全健康评估仪表盘改进风险管理](#)。



Commvault® File Storage Optimization

通过识别业务关键数据并确保文件通过单一环境即可得到适当备份和保护，减少勒索病毒攻击的攻击面。

- 识别存在风险的业务关键数据，并按数据类型和位置对其分类
- 使用主动补救措施备份、归档数据或将数据移至安全位置
- 使用备份副本确保数据可用性

Commvault® Data Governance

通过一个集中式管理控制平台，定义、查找、管理和保护整个混合云实时和备份数据孤岛中包含敏感数据的文件。

- 快速识别和保护敏感数据，包括个人身份信息 (PII)
- 通过协作决策管理风险补救
- 从备份中删除敏感数据，以确保不会意外恢复以前删除的数据



**最广泛的工作负载保护：
保护最重要的数据**

随着企业的发展，数据也会随之增长。Commvault 可以轻松帮助您实现扩展，因为我们涵盖了从本地、云到 SaaS 应用程序的最广泛的工作负载保护，并为原生云集成提供支持，从而将复杂性降至最低。

- 通过灵活且持续的服务水平保护您的所有工作负载
- 为传统应用、大型主机、现代应用和容器提供支持
- 与云、应用和数据库进行原生集成
- 跨整个环境的数据安全和保护的单一管理控制台视图
- 能够将任何工作负载恢复到任何目标位置、云或本地

Commvault 为您的数据保驾护航

无论您的数据位于何处，Commvault 都能对其进行保护。[Commvault Complete™ Data Protection](#)是一款功能强大的数据保护以及备份和恢复软件解决方案。它为您的所有工作负载提供简单、可扩展且全面的备份、复制和灾难恢复编排：

- **多云**：为您带来创建混合云环境的灵活性，在混合云环境中，您可以将数据备份（和恢复）到云、云内甚至在云之间进行备份和恢复。
- **虚拟机**：无论数据存在哪里，都可以跨环境备份、恢复和管理虚拟机。
- **应用程序和数据库**：只需使用一个解决方案，即可将工作负载迁移到云，高效地备份数据库，并加快对数据的访问。
- **终端**：可以在台式机、笔记本电脑和移动设备上轻松安装终端保护，支持用户自行恢复文件

简化原生云集成的数据管理

如今，企业纷纷选择多个云备份位置，而 Commvault 能够保护、迁移数据并轻松将数据移动到其他云提供商甚至移回本地。

通过云原生工具保护工作负载可能既复杂又有诸多限制。为了保护云工作负载和数据，企业经常需要自行创建脚本，以便编排出不同的云服务中可用的快照和数据复制方法。所以企业在享受公有云带来的云的灵活性与弹性的同时，会发现难于维护、审计和拓展这些脚本。此外，如果您的企业机构必须根据定期要求或业务流程需求而在其他云服务提供商或本地数据中心内创建二级备份副本，那么会进一步大幅增加其复杂性。虽然云服务提供商擅长保持数据和工作负载的高可用性，但您有责任确保动态和静态数据的安全性。借助 Commvault，您可以获得用于保护云数据的自动化和安全功能，以及旨在满足云数据保护 SLA 的自动化且经过验证的云迁移工具。

为了保护最重要的内容，您需要一种有效的方法来保护应用程序、数据库、虚拟机和大型数据集的迁移，并随着企业云利用率的提高而扩展。[了解更多](#)有关 Commvault 支持技术的信息。

Commvault HyperScale™ X

通过利用整个 Commvault 软件产品组合，您可以访问所有特性和功能，并以行业领先的技术集成各类应用程序、数据库、公有云环境、虚拟化平台管理程序、操作系统、NAS 系统和存储阵列。Commvault HyperScale™ X 提供以下两种规格，可为您提供上述所有功能，并可根据您的特定需求和偏好灵活地选择实施方案：

- **从本地开始并扩展到云**。在这种场景下，Commvault HyperScale™ X 支持您保护本地工作负载并管理自己的基础架构，然后在 [Metallic® Recovery Reserve™](#) 的帮助下扩展到云 – 用于数据的二级和/或气隙副本。
- **从 SaaS 开始**，使用 HyperScale™ X 作为边缘存储。此方法通过 [Metallic™](#) 备份即服务和本地气隙副本为您提供了简便的 SaaS 数据保护，从而加快恢复并降低成本。



更迅捷的业务响应： 确保一致、灵活、周密的恢复

速度和准确性对于快速恢复和快速回归正常业务运营至关重要。通过将数据保护功能整合到单个仪表板上，Commvault Command Center™ 能够尽可能降低复杂性，并最大程度提高效率。

- 通过我们的自动化工作流和健康检查优化恢复时间目标 (RTO)
- 通过删除可疑文件并了解确保健康文件恢复的确切时间点，通过前后一致且经过净化的恢复过程来尽可能减少数据丢失
- 通过 Metallic® Recovery Reserve™ 来采用气隙云存储，这支持您将备份副本存储在物理上无法从外部连接访问的基础架构上
- Commvault 专业服务可提供额外的资源和专业知识，帮助您防范勒索病毒，并在发生攻击时提供响应服务

Commvault Complete™ Data Protection 可实现快速恢复

Commvault Complete™ Data Protection 是一款功能强大的备份和恢复软件解决方案，可实现快速、周密的恢复。该统一解决方案可降低复杂性、成本并缩短恢复时间，使您能够平衡数据恢复需求，以满足您的服务水平协议。经过整合的统一恢复环境为您提供：

- 灾难恢复脚本自动化以及一键式故障转移和故障恢复，易于实施，操作简单
- 自动发现停机并进行故障转移，以尽可能减少操作中断
- 快速虚拟机、应用程序和存储快照复制，实现亚分钟级 RPO 和接近零的 RTO
- 通过副本数据管理进行灾难恢复副本验证，确保在需要时可以将其投入生产
- 测试升级程序和补丁
- 自动化合规报告
- 可配置的端到端数据加密，无论是静态还是动态
- 集成的勒索病毒防御，包括异常检测和报告
- 副本保护，通过在灾难恢复站点对副本进行定期安全扫描来实现

Metallic® Recovery Reserve™：使用空气间隙（Air Gap）获得不可变性

Metallic® Recovery Reserve™ 是一种采用空气间隙云存储的简便方式，具有可预测的成本和更低的开销，可保护备份副本不受任何工作负载变化的影响。所有内容都由 Commvault Command Center™ 集中管理，您的 IT 团队可以通过单个统一的管理界面轻松控制整个环境中的数据和工作负载。Metallic® Recovery Reserve™ 可以说是一个“快捷键”，可帮助您在几分钟内采用安全且可扩展的云存储，使您能够满足组织的混合云策略需求，而无需企业另行掌握云专业知识。

Commvault 防勒索病毒服务

Commvault® 专业服务可提供所需的资源和专业知识来增强 Commvault 解决方案以抵御勒索病毒攻击，支持您随时查看环境状态，并在遭到攻击时帮助您恢复业务的正常运营。我们的 Commvault 勒索病毒服务可提供最符合您业务需求的服务水平。这些服务包括：

- 勒索病毒防御设计和规划：根据您的业务需求来检查并审查您所用解决方案的恢复能力，并根据您的恢复目标来调整 Commvault 的技术能力
- 勒索病毒防御审查：验证您的恢复解决方案并帮助验证先前已实施的建议，以及确定是否未发生任何不利变化
- 勒索病毒响应：在遭到攻击时立即联系专门的响应团队，帮助您识别问题并启动快速恢复正常运营的流程。

要了解更多信息，请访问 www.commvault.com/readiness-solutions。



零信任原则：

信任，但仍需验证，即使是已经在网络外围内的对象

Commvault 支持零信任原则，并建议执行零损失策略以遵循这些原则。我们集成了领先的安全响应工具，如 ServiceNow、Splunk 和 CyberArk。此外，我们还通过多因素身份验证 (MFA) 选项以及对 YubiKey 和 CAC（通用访问卡）的支持来帮助您保持严格的访问控制。我们所有的安全工具都有助于满足 NIST SP 800-207 中所述的零信任原则，以确保您组织的环境安全可靠。

Commvault 安全框架

Commvault 端到端框架遵循 NIST 和零信任原则，为企业提供出色的防御和恢复功能。虽然多层安全框架提供了多种防御措施来弥补您基础架构中的漏洞，更是防范勒索病毒攻击并从攻击中恢复的高效方法，但企业也需要一种策略来保持警惕。零损失策略有助于降低勒索病毒攻击的风险，在发生勒索病毒攻击时减轻其影响，并实现快速恢复。这是一项通过我们的多层安全框架实施的策略。

由于每个环境都混合了不同的基础架构，因此保护备份数据免受未经授权的随机更改似乎非常困难。但就像保护您的房屋一样，您需要识别风险并实施保护和监控功能以满足您的需求。

许多专家建议采用分层的反恶意软件和勒索病毒策略。Commvault 已将这些安全功能内置到我们的数据保护软件和策略中，无需增加管理开销。Commvault 数据保护和管理平台包括五个安全层：



识别



保护



监控



响应



恢复

- 识别并降低备份数据存在的风险，在单个界面中即可完成
- 保护通过应用基于行业领先标准的安全控制来实现
- 监控勒索病毒、内部人员威胁和其他威胁
- 响应威胁并采取措施，同时持续验证备份数据
- 恢复数据，跨多个本地、云和混合环境快速完成

Commvault 多层安全包括功能集、指南和最佳实践，用于管理网络安全风险并确保数据随时可用。它们共同构成了 Commvault 核心平台体验 - [Commvault Complete™ Data Protection](#) 一部分。您不需要支付特殊的许可费和额外费用，也不需要另行安装软硬件。通过与 [Metallic® Recovery Reserve™](#)、[Commvault HyperScale™ X](#)、[Commvault® File Storage Optimization](#) 和 [Commvault® Data Governance](#) 的进一步集成，增强了分层的安全深度。



通过零损失策略为抵御勒索病毒攻击做好准备

一个客观的事实是，美国 31% 的企业因勒索病毒攻击而被迫关闭。⁴ 显然，消除勒索病毒的影响并非易事。制定有效的计划是全面、迅速恢复正常运营的基础，并且该计划应包括以下措施：

- 制定事件响应计划并反复测试
- 确保员工、供应商、流程和技术均已就位
- 遵循 NIST 多层安全框架：识别、保护、监控、响应和恢复，以弥补基础架构中可能存在的安全漏洞
- 遵循零信任原则来验证已在外围的用户真实性
- 使用集中式管理系统，而不是多个单点产品，以便轻松查看数据
- 通过不可变性、空气间隙、蜜罐和隔离的网络分段消除环境中的漏洞

通过 Commvault 对勒索病毒保持警惕

在防范勒索病毒攻击时，方案的综合性比复杂程度更为重要。Commvault 提供功能强大的统一平台和完整的服务，可根据您不断变化的需求轻松扩展，同时提供快速恢复数据资产和恢复正常业务运营的选项。

⁴ AtlasVPN, Edward G., 31% 的美国公司在成为勒索病毒的受害者后倒闭，2021 年 7 月。

了解更多有关 **零损失策略** 与勒索病毒防御和恢复的信息。参加我们的 **免费风险评估** 以了解您针对勒索病毒攻击的准备情况。

