Commvault

用户指南

让勒索软件防护及恢复计划与关键功能保持一致

企业日新月异，勒索软件“层出不穷”

由于混合就业和远程就业增加、数据蔓延增多以及复杂网络威胁上升等多种因素，企业面临日益动荡的数据环境，预计到 2025 年，由网络犯罪造成的损失将达每年 10.5 万亿美元。[1] 公司需要超越传统型备份和恢复的专用解决方案，从而在混合世界中实现真正的网络韧性。这些专用解决方案不仅能让企业保护好数据，还能主动预测潜在风险，最大限度减少损失，遇到困境时实现迅速恢复。这反过来又可以帮助企业降低总体风险并有效管理成本。

显而易见，旧手段不再奏效。企业正在转向基于多层框架的新一代数据安全，这些框架提供主动防御和自动化，为防范勒索软件攻击并从中恢复提供了最佳蓝图。

美元 10.5 万亿

每年到 2025 年。[1]

本指南宗旨

使用本指南对照您当前的勒索软件防护和恢复功能，确定如何在混合式、云或 SaaS 工作负载环境中对您的准备计划做最佳优化。

1 Cybersecurity Ventures，Steven C. Morgan，《2023 年网络犯罪每年将给世界造成 8 万亿美元损失》，2022 年 10 月

国家标准与技术研究院(NIST)网络安全框架

01 **识别：**形成组织层面的理解，从而管理系统、人员、资产、数据和能力的网络安全风险。

02 **保护：**通过开发及实施适当的保障措施，确保关键服务提供到位。

03 **监督：**建立持续的程序来识别网络安全事件的发生。

04 **回应：**实施恰当举措，防御已知的网络安全事件。

05 **恢复：**制定并实施恰当措施，以维持复原能力计划，恢复因网络安全事件而受损的功能或服务。

为帮助增强数据基础设施复原能力，目前的 NIST 网络安全框架(CSF)V1.1 推荐了成功且全面的网络安全计划五大重要方面。

为了在不断发展的网络安全环境中有效管理网络安全风险，NIST 起草了新版框架：CSF 2.0。此更新版本定于 2024 年初发布，该版本推出了第六个方面——治理，对现有五大方面中的治理部分进行了重新定位，强调网络安全是企业风险的主要来源。

在本指南各个部分中，我们都会阐述为什么每个安全层都至关重要，同时对要纳入勒索软件防护及恢复解决方案的关键功能进行回顾。

01 识别

在混合世界中，要准确了解关键数据的使用地点和方式的确面临不小的挑战。有效的数据安全工具应当能看到整个数据环境，从而更好地识别风险区域，消除盲点。这些工具通过零信任架构对数据和备份进行保护，其中包括内置安全协议以保护数据、防止非法访问、以及在面对不断变化的网络威胁时遵从合规性。如果攻击成功，端到端可观察性能帮助组织机构在网络攻击的之前、期间和之后做出更好的数据决策。

识别 主要部分	勒索软件防范要求	COMMVAULT 功能
数据保护见解	自动分析和识别问题，并提供操作建议以解决安全问题。	Commvault® Cloud 中由人工智能驱动的实时警报、摘要和建议。
自动安全评估	使用交互式工具集快速评估安全状况以及采纳建议提高安全性。	通过深入了解数据安全各方面的全方位仪表板，在攻击造成损害或传播之前主动采取行动。
自动备份运行状况评估	验证备份是否正常。	云端指标和本地指标提供定期运行状况报告。
数据管理报告和仪表板	快速查看备份及恢复就绪状态。 针对特定意向项目的定制报告和仪表板。	统一的仪表板和可扩展的报告供您了解恢复就绪情况，附带详细的 KPI 数据。
审计	跟踪数据更改，包括访问者和更改时间。	审核与特定用户和 IP 地址相关的登录信息。在详细的审计跟踪中监督所有的配置更改以及备份与恢复事件。
威胁诱捕	在攻击触及目标之前将其拦截。	Threatwise™ 提供差异化工具来检测生产环境中的零日威胁和未知威胁，帮助客户在数据泄露之前发现高级网络威胁。
风险分析	识别并调查敏感数据和有风险的数据，从而最大限度减少数据暴露与泄露。	• 对敏感信息（例如个人数据和财务数据）进行识别、归类和分类，从而排定安全措施的优先次序并减少泄露发生时的数据外流。 • 采取主动措施确保遵守法规，对过时（ROT）数据进行归档以节省存储成本。 • 安全搜索及共享利用人工智能快速识别大型数据集中的敏感数据和关系，确保只与恰当人员共享恰当信息。
威胁扫描	识别并调查文件异常，确保对正常数据进行恢复并避免再次感染恶意软件。	• 识别恶意软件威胁以避免在恢复期间再次感染。 • 威胁扫描对备份数据进行分析，查找其中的加密文件或损坏的文件，确保用户能快速恢复可信的数据版本。 • 威胁扫描预测添加了实时人工智能预测技术，能发现人工智能驱动的勒索软件威胁。

02 保护

了解数据环境后，您可以开始减少攻击面，从而限制潜在威胁，防止系统性传播。通过零信任架构防止来自内部和外部的数据更改，从而防止非法访问。您可以在数据泄露、加密和外流之前，对网络进行隔离和分段，采用气隙技术对备份副本进行隔离及保护，并结合网络欺骗技术对威胁进行拦截。凭据遭到泄露或用户凭据具备其本不应有的系统特权访问时，可能会发生勒索软件攻击。确保采用行业标准的安全协议对数据进行加密和保护，以减轻勒索软件攻击的影响。

保护 主要部分	勒索软件防范要求	COMMVAULT 功能
不可变性	确保备份数据安全，防止未经授权的更改。	• 针对 Windows 和 Linux 系统的反勒索软件保护。 • 对本地部署和云部署采用存储锁 – 进行定制从而满足业务需求。 • 启用 WORM（一次写入，多次读取）防止未经授权的更改，并启用云气隙技术进一步防范勒索软件威胁。
基础设施强化	减少备份基础设施面临的威胁。	Commvault® 软件经过测试及确认，能进行互联网安全中心（CIS）1 级强化。 符合 CIS 1 级安全控制的要求，可作为预强化版 CIS VM（通过 OVA 部署）或作为按 HyperScale X™ 交付的硬件设备。包括 CommServe、媒介代理和访问节点在内的所有子组件也可以强化至 CIS 1 级。
认证与授权	控制有权访问的人员及其访问权限级别，同时添加多层授权以确保额外的安全性。	• 基于角色的访问控制对未经授权的使用进行限制，同时安全断言标记语言（SAML）和 OATH IdP 也提供多一层的安全性。 • 与 Active Directory 和 LDAP 集成。 • 对保留锁和命令授权实行多重身份验证和多人身份验证控制措施，以保护数据免受意外影响，防止破坏性操作。 • 与特权访问管理以及增强型身份与访问管理工具（例如 CyberArk、Yubikey 和生物识别技术）集成，进一步增加用户身份验证和保证（AAL3）。 • 与 CyberArk 实时集成，最大限度降低已存储凭证的风险。 • 端到端数据加密，同时允许外部密钥管理平台对密钥进行管理和控制，还有证书身份验证 - 防止恶意数据访问。 • 软件 WORM（保留锁） • 多租户

02 保护

保护 主要部分	勒索软件防范要求	COMMVAULT 功能
加密	实施符合行业准则的加密标准。	用于有效管理 Commvault 中备份和恢复所用加密密钥的标准和工具:: • 联邦信息处理标准加密模块 • 内置密钥管理 • 与第三方密钥管理集成 • 密码密钥管理系统
备份目录保护	确保多个区域的保护不变，无论是本地副本还是在云端。	• 针对本地副本的强大的勒索软件防护。 • 备份到 Air Gap Protect 或第三方云。
隔离/气隙	将数据分段并与外部网络隔离，确保在攻击发生时能快速恢复。	• Air Gap Protect 使用气隙对敏感数据进行隔离和保护。 • HyperScale X 设备具有集成气隙控制功能。 • 网络拓扑：使用单向拓扑或代理拓扑。
Active Directory 保护	创建保护及恢复 Active Directory、对对象属性进行备份以及执行完整备份、差异备份、增量备份和合成备份的功能。	Commvault Cloud 平台提供本地和云端的气隙式 Active Directory 保护。
3-2-1 备份策略	创建能确保数据始终可用的有效备份策略。 至少拥有三份数据副本，其中两份位于本地但在不同地点，一份异地副本。	• 在本地或多个云端点配置数量无限的数据副本。 • Air Gap Protect 提供启用气隙式云存储的功能。
威胁诱捕	在数据泄露、加密、外流或损坏之前尽早发现勒索软件攻击。	• 批量部署威胁传感器（假诱饵）以覆盖您的表面区域。 • 使用预配置的传感器模拟关键资产。 • 模仿您所在环境特有的高度专业化的资产。
按需安全控制	遵守及管理不影响备份保护的密码轮换策略。	借助零信任控制对安全状况进行改善，消除受损凭证。CyberArk 集成允许及时检索凭证，包括在 CyberArk 内的安全凭证存储和管理。

03 监督

受到安全威胁影响的组织机构甚至可能没有意识到自己受到了攻击，直到为时已晚，漏洞蔓延超出其控制范围。因此，要想在勒索软件攻击对更大范围的基础设施造成影响之前将其遏制，就必须确保有适当的工具来迅速洞察网络安全事件。通过结合下一代预警和深入监控，您可以发现并消除零日威胁和内部威胁，从而保护您的数据。对恶意活动更快地进行检测、转移和标记，以减少数据恢复工作量。

监督 主要部分	勒索软件防范要求	COMMVAULT 功能
人工智能安全监控	使用 AI 对支持虚拟机备份和 SaaS 应用程序的异常框架进行监控，通过使用审计跟踪查明潜在的安全事件，提供异常文件活动的详细信息。	利用人工智能的潜力： • 通过 AI/ML 实现干净、快速、安全的恢复，同时减少误报。 • 监督备份并对事件和行为进行成功、待处理或失败状态分析。 • 通过备份趋势分析来预测未来 SLA 合规性。
系统监控	监控关键工作负载和基础设施。	• 识别因实时数据和备份数据的损坏、加密或恶意文件而导致文件特征发生变化的异常情况。 • 发现新的零日威胁和人工智能驱动的勒索软件威胁。
日志监控	搜索特定日志事件来监督环境中的日志活动。在仪表板上编排好的所有日志事件中搜索特定事件。搜索与特定客户端、日志文件、模板或监控策略相关联的日志事件。	Commvault Cloud 平台可让您详细监控日志文件状况以及 Syslog 和 Windows 事件。
威胁意识	主动即时洞察主动威胁和潜在威胁	• 仅将传感器暴露给不良行为者；对合法用户和系统不可见。 • 获得活动及策略的关键情报。 • 消除误报和警报疲劳。 • 引诱不良行为者使用虚假资源。
蜜罐和实时文件活动	监控面临勒索软件风险的资产并确定干净的恢复点。	监控实时可疑文件，检测威胁并保护备份，以确保实现干净的文件恢复并避免文件重新感染。

03 监督

监督 主要部分	勒索软件防范要求	COMMVAULT 功能
威胁意识	主动即时洞察主动威胁和潜在威胁。	• 仅将传感器暴露给不良行为者；对合法用户和系统不可见。 • 获得活动及策略的关键情报。 • 消除误报和警报疲劳。 • 引诱不良行为者使用虚假资源。
人工智能安全监控	使用人工智能对支持虚拟机备份和其他工作负载（例如 SaaS 应用程序）的异常框架进行监控。	• 深入了解备份何时发生异常变化，从而推动干净、快速的安全恢复。 • 查找干净的数据版本，推动干净、快速、安全的恢复。 • 通过 AI/ML 减少误报。
蜜罐和实时文件活动	监控面临勒索软件风险的资产并确定干净的恢复点。	监控实时可疑文件，检测威胁并保护备份，以确保实现干净的文件恢复并避免文件重新感染。

04 响应

一旦检测到勒索软件，必须立即做出响应。通过安全工具和主动警报进行深入了解，这使得您的企业能对数据进行保护。有据可查的策略和事件响应计划有助于确定后续步骤。必须既有技术响应也有业务响应，各领域的每一位利益相关者都必须了解自身角色和将要采取的行动。各团队之间的协调与沟通至关重要。关键在于安全团队要尽可能遏制并阻止传播，同时采用适当工具避免任何潜在的再次感染。

响应 主要部分	勒索软件防范要求	COMMVAULT 功能
与安全信息和事件管理（SIEM）和安全编排、自动化和响应（SOAR）集成	与您现有的 SIEM 和 SOAR 平台无缝集成，可从中心位置对操作和事件进行监控、管理及编排。导出审计跟踪和事件并将其安全地记录到您的 SIEM 和 SOAR 平台上，进行保存和事件编排。通过实时监控，您可以对检测到的威胁做出快速响应，并通过适当操作保护您的备份资产。	Commvault 的集成可实现与各种编排平台的互操作性，例如 Microsoft Sentinel、Palo Alto Networks XSOAR、Splunk 和 ServiceNow。我们的集成提供： • 实时了解安全事件和事故。 • 增强版自动化及编排功能。 • 减少事件响应时间和人工干预。 • 改善内部协作及整体安全状况。
警报	提供关于操作的自动通知，例如失败的任务。 在“触发的警报”页面上显示警报，指定用户会收到电子邮件通知。	获取各种形式的可操作警报：电子邮件、系统中心运营管理器（SCOM）、SNMP 和 webhooks 等。
仪表板	显示对组织机构中所有 CommServe 计算机收集的最关键信息的预览，例如 SLA 百分比、容量使用情况和备份失效。	Commvault Cloud 平台提供了一体化的方式，对跨本地和 SaaS 的网络复原能力进行查看和管理。它可在全球范围内提供安全性、容量和使用情况仪表板，通过安全运行状况评估和异常文件活动仪表板进一步深入了解情况。
编排工具	创建精心编排的工作流程对勒索软件事件做出快速响应。甚至能与第三方供应商整合。	• 轻松创建备份前/备份后命令的工作流程。 • 工作流程通过命令行界面、REST API、PowerShell 模块和 Python SDK 进行。 • 与 Splunk、ServiceNow、Ansible 或 Terraform 集成。
主动威胁响应	在攻击者开始攻击时发出警报，积极保护数据的可恢复性。	• 在有价值的资产（例如文件服务器、数据库、虚拟机等）周围部署威胁传感器，从而在您的环境中创建诱饵。 • 通过调查备份环境中的工作负载，对诱饵放置提出智能建议。 • 在攻击开始时立即获得极其准确的警报。

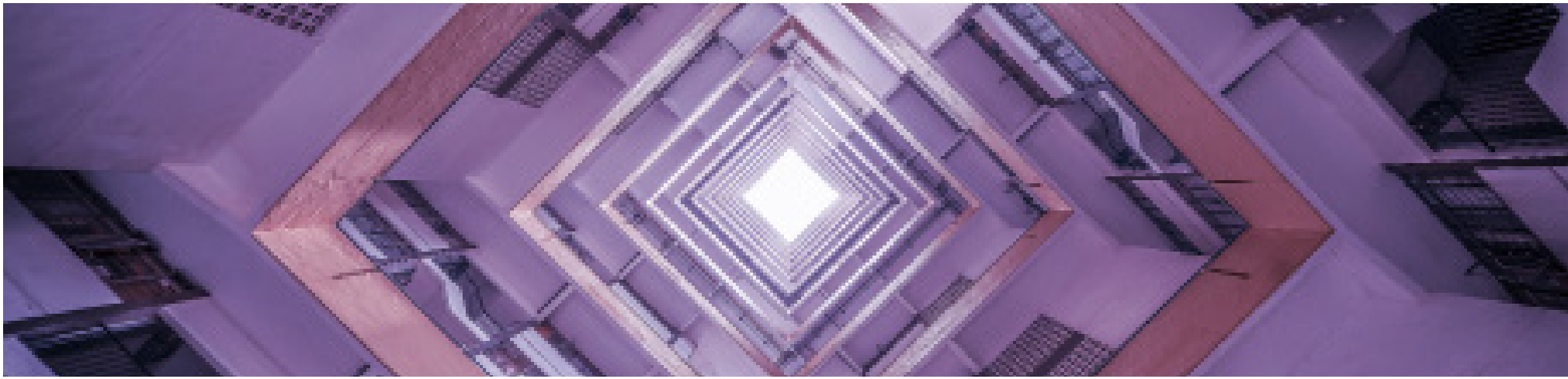
05 恢复

一旦识别出威胁，并且有适当的事件响应对恶意软件进行隔离并删除，恢复过程就宣告开始。确保所有受影响的数据从网络安全事件发生前的时间点恢复至正常运行条件，这一点至关重要。事实证明，覆盖最广泛工作负载的主动、可靠的恢复工具及选项能缩短停机时间、防止数据丢失并加快响应时间，从而实现无与伦比的业务连续性。
在确定根本原因且文件得到恢复后，恢复计划就开始进行了，目的是通过恰当的安全工具减轻未来可能产生的影响。在恢复阶段，必须只恢复所有受影响的技术中的干净文件。

恢复 主要部分	勒索软件防范要求	COMMVAULT 功能
混合多云恢复	从任何地点快速恢复数据，无论是在本地还是在云端。	自动化进行并恢复到不同的虚拟机管理程序、超大规模器或其他平台。
高可用性	借助 CommServe LiveSync 功能，让 CommServe 服务器做好灾难恢复准备，并在发生灾难时能快速故障切换到指定备用主机。	Commvault LiveSync 功能支持对目录和其他关键工作负载进行备份。
事件响应恢复	允许事件响应团队以安全方式恢复数据从而进行数据取证。	• 协调异地恢复到隔离的洁净室环境。 • 运行前脚本/后脚本和工作流程对关键数据进行验证和扫描。
恶意软件扫描	验证备份数据可以恢复并且内容中不存在威胁。	• 实时安装使用应用程序验证的虚拟机来安全运行脚本，并扫描虚拟机是否存在恶意软件。 • 通过 AI/ML、异常检测和恶意软件签名扫描，在威胁传播之前对其进行扫描。
精心恢复和消毒	通过删除可疑文件并了解实现健康文件恢复的确切时间点，用连贯一致、经过净化的恢复来减少数据丢失。	通过异常检测将可疑文件删除、分隔和隔离，并通过浏览及删除威胁对备份内容进行清理。
主动恢复	在威胁触及目标之前发现并修复威胁。	借助 Threatwise™ 欺骗行为不端者，将其攻击转向虚假资产，立即了解攻击情况，并在威胁接触到您的数据之前及早补救。

05 恢复

恢复 主要部分	勒索软件防范要求	COMMVAULT 功能
恢复验证	计划、实施、验证及展示可证明的恢复准备就绪的证据。	• 对备份进行持续验证或定期验证，以便在周期早期检测出受损备份。 • 在不中断运营的情况下证明及展示恢复准备情况。 • 通过消除手动步骤，降低恢复测试的复杂性。
恢复取证	在隔离网络中以安全的方式取证，不造成进一步感染。	• 使用文件数据分析对可能被恶意软件加密或损坏的文件进行检测，确保您没有备份受感染的文件。 • 结合威胁分析，在恢复时检测备份数据中的恶意内容，确保在从备份的最后一个良好时间点进行恢复时，生产系统不会面临再次感染的风险。
恢复编排	通过自动合规性报告进行灾难和网络恢复编排。	• 验证并清理恢复点后，一键将跨工作负载的干净副本恢复到生产环境。
基础设施快速恢复	快速恢复云规模，不受恢复地点限制。	• 结合持续测试、基础设施即代码和云扩展，以最低的总拥有成本（TCO），将混合工作负载以快速、可预测且可靠的方式自动从网络恢复到云。 • 具备任意到任意的便携性，可实现任意地点间的恢复。



真正的网络弹性能力，最低的总拥有成本

Commvault Cloud 提供分层防御 - 通过早期预警和网络欺骗最大限度降低网络攻击的影响，同时通过全方位威胁扫描、修复、智能隔离、清洁恢复验证和无与伦比的恢复速度来加速恢复。

使用最佳解决方案快速启动您的网络弹性能力策略，帮助您预测、主动应对网络威胁，并在遭遇网络威胁后加快恢复。

找到满足您需求的最佳解决方案。

COMMVAULT 安全集成

Commvault 提供无缝集成，与领先的安全合作伙伴携手，以 Commvault 现有功能为基础，为集成式混合环境提供多样化的网络弹性能力选择。

了解有关网络弹性能力的更多信息

commvault.com/platform

Commvault®

commvault.com | 888.746.3849 | get-info@commvault.com