

数据保护、恢复及任务

数据管理和保护软件必须与您需要成熟的技术、时刻的警惕、及时的更新、相应的指导的任务相匹配。

勒索病毒等网络威胁已经转变为何时发生而不是会不会发生的问题。为了确保您能在不支付赎金的情况下就恢复数据，您要相信，您的数据保护供应商与您保持着同样的警惕。有效的解决方案需要最好的技术、合适的人选及正确的流程。

在 Commvault，我们就像首席信息安全官一样，始终保持警惕性。我们以对客户高度负责的态度提供产品和服务。Commvault 因其专注性与可信度而享有盛誉，同时拥有广泛的客户资源，正是这些客户证明了在勒索病毒攻击的高强压力与深层影响下，我们所拥有的责任心、创新力和快速执行力。

Commvault 以数据安全为战略目标，我们利用多层保护、高级检测，以及在面临安全威胁（包括勒索病毒和数据泄露）时快速恢复来解决问题。

企业需要一些工具来不断衡量他们的恢复就绪状态，以发现并修复问题，通过自动测试验证其数据与业务应用程序的可恢复性，并不断强化自身环境来提高安全性，减少风险的发生。

在考虑对备份数据本身的威胁时，常用的一种方法就是创建具有一定隔离级别的数据副本，例如安全隔离网闸（Air Gap）和不可变副本。Commvault 认可这种方法，我们在为写入本地和云存储的目标提供不可变保护、地理分离，以及安全隔离网闸方面经验丰富，您可以选择使用我们的设备，也可以使用您自己的存储设备。

要保证数据安全，同时又要对软件进行有效管理，这对许多人来说可能是个挑战。而 Commvault 数据保护方案是这个领域的开拓者，保护数据的同时还为隐私、盗窃、损坏、删除等问题作保，而不论它们是由内部还是外部威胁引起的，抑或是恶意还是误导造成的。

用于身份验证、授权和审计的 AAA 安全框架可谓是评估任何软件解决方案的一种有效途径，在安全社区中广为人知。Commvault 利用此框架来评估、改善和展示自身能力以及对行业法规和最佳实践的遵守情况。Commvault 恪守 [NIST SP 800-207](#) 中所述的零信任原则，为客户提供分割 / 隔离数据、建立用户身份所需的一系列服务，以最低权限要求提供访问权限，避免受到用户错误的影响，并拥有粒度完备的日志记录和审计功能。这些控件可通过所有类型的接口进行工作，包括 UI、命令行或 API。

威胁并不总是来自外部，也可能是由凭证泄露或问题管理员的蓄意行为造成的。为了对抗内部威胁，Commvault 采用一种控制机制，来确保可能威胁数据的管理任务得到选定权限组中至少两名管理员的批准，将四眼原则应用于数据安全。

恢复解决方案只有在各种故障模式下都表现出弹性时才是可行的。例如，有一种情况是数据恢复事件需要恢复到损坏之前的实例。同时，还有一种情况可能需要将业务应用程序完全恢复到一个新的位置。设计跨环境可恢复性，并提供简便的自动化流程来测试和验证每种情况，即可帮助建立恢复就绪状态。知道任务关键数据和应用程序已经通过自动化流程进行恢复验证后，即实现了所需的安全性、合规性和舒适度。

Commvault 开发了一些方法，通过提供数据保护架构的关键方面，为安全软件提供了监控和检测功能。机器学习（ML）算法可检测文件活动中的异常情况，蜜罐文件的实施可发出有关潜在勒索病毒攻击的早期警告。在不增加成本或管理工作的条件下，这些工具还提供额外的早期警告功能。

下表对一些关键问题以及如何借助 Commvault 解决这些问题进行了总结。

威胁	策略
备份数据卷是勒索病毒的破坏目标	保护备份卷，让任何管理员帐户都不能对其进行更改。只能由经过验证的 Commvault 进程进行修改。通过在 Commvault 二进制文件上进行数字签名并要求 Commvault 组件之间进行证书认证来提高安全性。
攻击者以密码、策略和数据为目标	通过选择多重控制，并对其范围内的功能和系统进行基于角色的细粒度访问锁定，来保护身份验证。对数据进行加密并给予外部密钥管理支持。四眼原则工作流可预防潜在的破坏性管理任务。
恶意管理员访问备份数据	除了四眼原则和基于角色的细粒度锁定的限制之外，每一次访问和更改都将被记录下来，任何关键的更改都会向选择的系统发出警报。隐私锁定选项通过确保管理员无法看到或恢复敏感数据和私人数据来对其实行保护。
管理员意外删除	阻止攻击者和问题管理员的所有控件也适用于管理员误操作的情况，并且会杜绝误操作的可能。
遵守日志文件管理的安全含义和规定	企业必须制定政策确保符合相关法律法规要求，通常日志要长期保存。服务器、终端和网络设备上的日志文件可以独立于常规备份保留政策进行保存。

本座谈指南集合了全球客户群采用的关键安全最佳实践。这些实践已通过不断改进和创新进行了调整，从而在数据量不断增加、数据格局从开放存储系统扩展到云的形势下，实现数据安全及恢复就绪。

数据安全建议

数据安全可帮助企业保护数据并从数据泄露和勒索病毒等安全威胁中恢复，同时控制对关键数据的访问。Commvault 的智能数据服务包括高级威胁和异常检测功能，它是多层保护功能的一部分，有助于减轻威胁对数据的影响。勒索病毒攻击已成为新闻焦点，在 Commvault 的帮助下，您可以降低勒索病毒发生的风险，并在勒索病毒进行攻击时，帮助加快恢复工作。

安全运行状况评估仪表盘

Access Security			
Parameter	Status	Remarks	Action
Two-factor authentication	Info	Disabled Commvault recommends you enable this feature.	How to enable two fac
Single sign-on	Info	No Single sign-on Providers are configured.	
Password complexity level	Good	Level 2. Check Password Complexity workflow is not deployed.	Deploy Check Passwor
Failed log-on attempts limit	Good	The account will lock after 5 failed log-on attempts.	How to set a failed log
Account lock duration	Info	The account will be locked for 5 seconds.	How to set the account
Command Center timeout period	Info	Command Center will timeout after 30 minutes.	How to change the tim
Commcell Console timeout period	Warning	Commcell Console will not timeout. Commvault recommends you set a timeout.	How to set the timeout
Auditing			
Platform Security			
Parameter	Status	Remarks	Action
Storage pools without encryption	Info	9 storage pools without encryption.	View report
Ransomware protection	Good	All mount paths are secured against ransomware.	
File Activity Anomaly alert	Critical	Deleted Commvault recommends you enable this alert.	How to enable an alert • The alert is triggered • The alert should not
Disaster recovery backup to cloud	Good	DR backup to cloud is configured.	
Key Management Server for Password Encryption	Info	passphrase (Passphrase) key management service is used.	How to configure a key
Company and Owners Security			
Capabilities			

首先要正确确定并评估风险与差距。Commvault Cloud Metrics Reporting 和 Commvault Command Center™ 中都提供了安全运行状况评估仪表盘。安全运行状况评估仪表盘可快速提供见解和建议，帮您制定行动计划。所有推荐的控制与设置都可在此仪表板中找到，并可通过交互式操作快速实施。有关更多信息，请参阅使用 [Commvault 安全运行状况评估仪表盘改善风险管理](#)。

制定多层策略的计划

Commvault 明白拥有多层安全策略对数据安全至关重要，恢复就绪也同样不可或缺。确保您的关键任务数据可以抵御蓄意破坏数据主副本和备份副本的有针对性的攻击，并通过尽可能自动化和协调的恢复流程使管理不再复杂。

您制定的任何计划都必须足够广泛和深入，以覆盖任何有价值的数据所处的位置。您的计划应该扩展到中央服务器和整个组织的应用程序之外，以覆盖笔记本电脑、各种媒体格式的文件，以及功能特定的应用程序。

备份目标不变性

确保备份副本不可变且无法被勒索病毒更改或加密至关重要。此功能对您环境中的所有数据都具有成本效益，您可以为所选存储开启此功能；无论是在本地，在云，还是在 Commvault HyperScale™ 解决方案中都适用。选择此法很明智，比只用安全隔离网闸的解决方案更有优势，而且没有增加复杂性和成本。

备份存储不变性功能采用有效方法限制写入和删除操作，从而防止不良行为或恶意软件修改受保护路径中的文件。Commvault 最近运用 RIPlace 规避技术测试了此功能的可靠性和有效性，这种技术可以侵入

报道功能相似的多个安全端点解决方案。不论如何，事实证明 Commvault 可以不受 RIPlace 规避方法的影响提供安全保护。

在采用多层策略的建议下，一些客户选择实施额外的策略以获得更强大的保护。对于特定的数据，企业可能只写入一次，在内部或云中读取多个 (WORM) 副本，并实施安全隔离网闸隔离策略。在 Commvault 中，通过策略（包括网络分段、加密网络拓扑、网关和防火墙）很容易实现这些操作。同时，还支持自动化编排网络和服务器断开操作。

基础架构强化

所有软件环境都需要基础强化原则。Commvault 解决方案的核心组件依赖于底层操作系统、数据库、应用程序和网络服务器技术。因此，需要关闭底层技术中的所有安全漏洞，以免成为网络威胁的切入点。

- 应用强化建议 – 根据美国国家标准与技术研究院 (NIST) 标准自动启用强化建议
- 二进制签名 (包含第三方) – 一个用于二进制数字签名, 同时确保恶意行为者不会对这些二进制签名进行修改的 Commvault 框架。
任何第三方库都会定期更新并对报告的漏洞做出响应
- CIS 1 级强化 – Commvault 软件已经过测试，并确认能够进行互联网安全中心 (CIS) 1 级强化

通过身份验证、授权和审计来强化应用程序

认证、授权和审计 (AAA) 是一种安全框架，可智能管控对计算机资源的访问，完善策略、审计使用情况。这些互相交叉的流程对于实现高效网络管理和安全必不可少。Commvault 在上述三方面推出了一系列安全、稳妥的功能。

用于控制访问的 AAA 安全框架

身份验证	授权	审计
证明和授予访问权限	控制所需的访问级别	跟踪和审计访问和功能

身份验证

认证过程按照每个用户的不同，设立不同的访问权获取标准。Commvault 采取多重身份验证方式 (MFA)，让模拟有效用户帐户成为不可能完成的任务。

- 安全轻量级目录访问协议 (LDAP) – 支持 Active Directory 和通用类 LDAP 认证服务器
- 外部识别供应商 – 使用开放授权 (OAuth) 和安全声明标记语言 (SAML) 等安全协议提供支持
- 多重认证 – 使用认证器应用程序、智能卡和硬件认证密钥进行登录
- 证书认证 – 面向 Commvault 基础架构，抵御欺诈
- 多租户 – 提供管理细分和访问划分
- 使用 CyberArk 的权限访问管理 (PAM) – 在不暴露密码的情况下，集中存储、组织、保护和管理 Commvault 凭据、服务帐户凭据和管理登录会话。

授权

认证后，必须向用户授权，方能开展特定任务。Commvault 平台提供丰富而全面的功能：

- 基于角色安全 – 依照分配给用户和组的角色管理操作，包括支持多租户环境，限制可访问和管理的服务器、应用程序和数据集的功能和范围
- 授权认证工作流程 – 支持管理任务四眼原则，例如删除数据集、客户端、资源、目标、作业和策略
- 密钥和隐私锁 – 管理员可管理数据，但不得查看或恢复无所有权的数据。一同使用时，只有个人、部门或企业层级的数据集所有者才能使用所需密钥恢复数据
- 数据加密 – 联邦信息处理标准 (FIPS) 认证的加密，包括 AES 256 在内的 6 位以上密码，数据加密是从第一次接触一直贯穿整个数据管理的生命周期
- 加密密钥管理 – 内置密钥管理系统 (KMS) 或使用外部系统，包括密钥管理互操作协议 (KMIP)，涉及 AWS KMS、Azure Key Vault 和密码 KMS 支持
- 网络加密 – HTTPS 封装、TLS 1.2、代理 / 网关支持
- 第三方端口映射 (TPPM) – 将第三方通讯纳入到 Commvault 网络端口，大幅降低安全环境中执行的复杂性
- WORM 副本支持 – WORM 策略在应用于数据副本时，会强制移除和删除权限，强制保留固定数据
- 云 WORM 服务支持 – 支持桶和对象级存储的 WORM 配置

审计

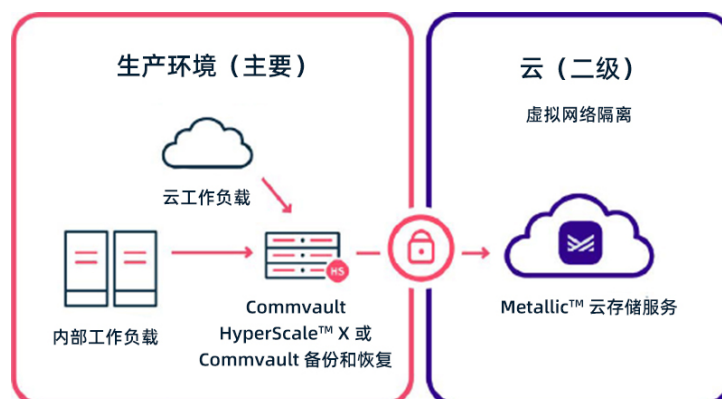
从安全的角度看，审计应聚焦用户访问和操作的完整日志，确保可观察特定报告，并对某些情况发出警报。回答以下基本问题：

- 哪些人员拥有过多访问权？追踪并报告通过 UI、命令行和 API 实现的访问量
- 访问时有哪些操作？提供用户访问和操作的完整审计跟踪
- 可以删除哪些访问权？系统会报告在特定时间段内未访问的用户，以判定是否需要删除
- 哪些数据未加密？通常建议使用的报告会对加密状态进行确认

数据隔离和网络隔离

“网络隔离”控制理念是一种数据保护基础架构，可减少攻击“受力面”，能够将数据恢复至攻击开始前某一时间点。Commvault 可通过以下方法有效缓解加密数据被复制到数据备份基础架构的风险：使备份目标不可变，将 WORM 安全策略定期应用于副本，移除删除功能直到满足保留策略为止。Commvault 改进了为各项解决方案提供的物理访问控件，增强了安全性，简化了流程，降低了成本。

- 网络隔离编排 – 自动化工作流，用于网络编排和服务器断开操作。
- 网络分段 – 使用网络安全控制从逻辑上和物理上阻止对二级存储目标的访问。
- 加密网络拓扑 – 使用 Commvault 网络策略隔离通讯，并创建从隔离的存储目标出站的加密渠道。Commvault 网关可以自动控制持久性连接。



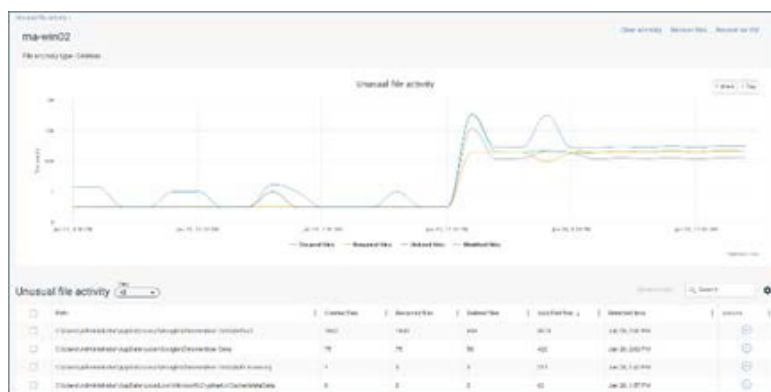
- 轻松采用安全且可扩展的云存储 – Metallic™ 云存储服务 (MCSS) – 仅需短短几分钟即可按可预测的成本为二级副本提供由安全隔离网闸隔离的云存储，无需基础架构。

使用数据隔离和安全隔离技术实现更全面的勒索病毒防护。 [阅读 >](#)

监控和检测

许多专家建议采用分层的反恶意软件和勒索病毒策略。Commvault 已将这些功能构建到现有安全软件和策略中，以获得更显著的优势，而无需增加管理开销。

- 监控文件系统活动 – 利用历史数据和机器学习算法来检测统计变异的文件系统行为
- 监控蜜罐文件 – 将勒索病毒易于攻击的文件隐藏起来，并监控重大变化
- 安全信息和事件管理 (SIEM) 集成 – 使用现有的安全监控平台来集中管理和编排 Commvault 操作及事件。通过 Syslog、插件或 API，将审计跟踪、事件、警报和日志安全地导出到您的 SIEM 和 SOAR 平台，以进行保存和事件编排

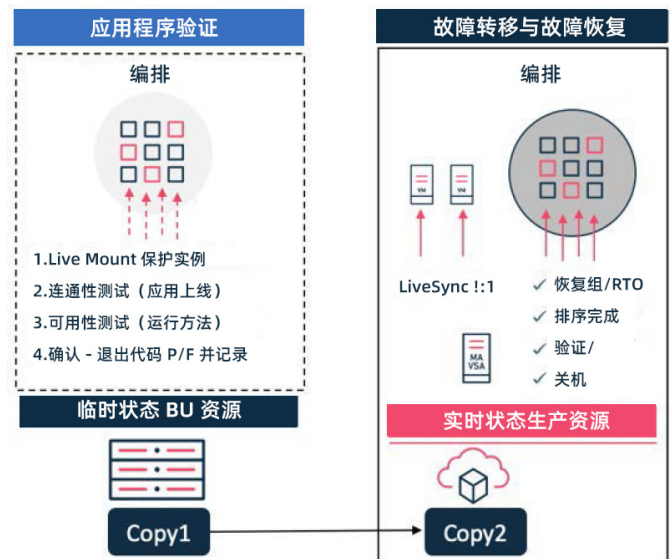


- 证书认证锁定 – 启用证书锁定后，如果没有额外的管理步骤和权限，无法将客户端添加到数据保护基础架构中
- 具有指导意义的警报 – 自动采取行动并发出警报引起管理员注意或将推荐的操作工作流嵌入警报中便于管理员执

简化恢复整备度

真正的安心来自于拥有一个全面、持续的恢复就绪计划。在与高压攻击作斗争时，您最大的弱点就是不知道以什么顺序恢复哪些数据。恢复就绪意味着恢复暂存是文档化的、自动化的和可预测的。Commvault 支持恢复就绪的功能包括：

- **高可用性数据保护基础架构** – Commvault 基础架构可以使用 Live Sync 将数据库复制到一个或多个备用节点来实现保护。数据库可以在任何公有云中进行本地保护，这是 Commvault 提供的一项免费保护服务
- **恢复编排** – Commvault 控制平面管理、操作和保留收集的所有数据记录。完全可以一键恢复，可通过完整编排的测试故障转移进行预先测试，确保在不影响生产的情况下提供恢复验证
- **数据完整性验证** – Commvault 提供多种方法验证数据的完整性。数据签名用于确认传输、接收以及写入存储介质中任何数据的此外，还提供自动定期验证存储数据
- **应用程序恢复验证** – 一项完整编排的应用程序恢复验证任务，可在备份基础架构上直接访问数据保护副本、启动应用程序、连接和运行一种测试方法以验证数据和应用程序的可恢复性
- **轻松识别要恢复的数据** – 可以在任何时间段内进行数据搜索，应用的选项包括显示 / 隐藏最新的、特定的时间点和时间段删除的项目。利用这些选项即可轻松选择要恢复的相应数据



行业认证

Commvault 数据保护解决方案持有（有些标为待定）以下合规性认证：

- **通用标准认证** – 待定
- **FedRAMP** – 联邦风险和授权管理计划 (FedRAMP) Metallic 备份即服务 (BaaS) 和 Metallic 云存储服务 (MCSS) 的“高就绪”状态
- **FIPS 140-2 认证**：密码模块验证程序
- **符合 NIST 800-53 CP9 标准**：NIST 增刊 800-53 (Rev. 4) CP-9
- **符合 NIST 800-53 CP10 标准**：NIST 增刊 800-53 (Rev. 4) CP-10
- **Commvault HyperScale™ 存储池 STIG** (《安全技术实施指南》) 认证
- **STIG 认证** – 扫描结果请访问 <https://documentation.commvault.com>
- **VPAT 2.0** – 符合 WCAG 和 508：VPAT 2.0 声明

抵御勒索病毒攻击产生的风险和回报，对于您的企业和个人发展都至关重要。如果失败，将导致数据丢失、经济受损、身败名裂；如果成功，可快速恢复运营，收获广泛认可。选择权在您的手中，简单明了——时刻准备恢复！

了解有关使用数据保护抵御勒索病毒的详细信息。 commvault.com/ransomware >

