# 构建强大的网络弹性数据恢复策略

# 目录

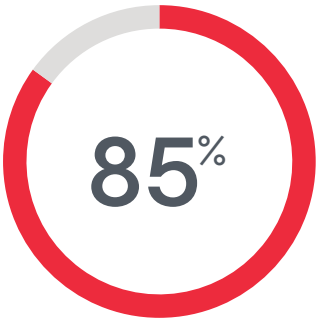


© 2023 Veeam Software。机密信息。保留所有权利。所有商标均归其各自拥有者所有。

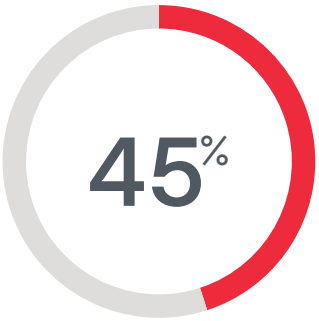
# 引言

所有组织都应该将数据安全作为一项首要的策略，因为网络攻击威胁（主要是勒索软件）迫在眉睫。遗憾的是，85% 的组织在 2022 年遭遇过至少一次勒索软件攻击（2023 年 Veeam 数据保护趋势报告）。更令人担忧的是，如今的勒索软件不仅会锁定组织的数据，还会泄露、窃取数据，进行兜售，甚至会将数据用于发动进一步攻击或策划勒索活动。

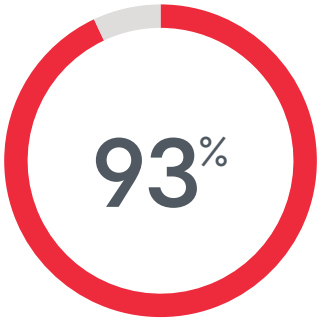
防止恶意访问这些数据应是网络安全计划的首要目标。然而，任何组织的防御都不可能坚不可摧。因此，构建数据恢复能力以守好最后一道防线同样重要。在受勒索软件影响的组织中，生产数据丢失率平均为 15%（2023 年 Veeam 勒索软件趋势报告），这凸显了精心设计可靠数据恢复计划的重要性。




的组织在 2023年
遭到勒索软件攻击*




的生产数据受到了
网络攻击的影响*




的勒索软件攻击
锁定了备份*

资料来源：2023 年 Veeam 勒索软件 趋势报告

# 可靠的数据恢复基础

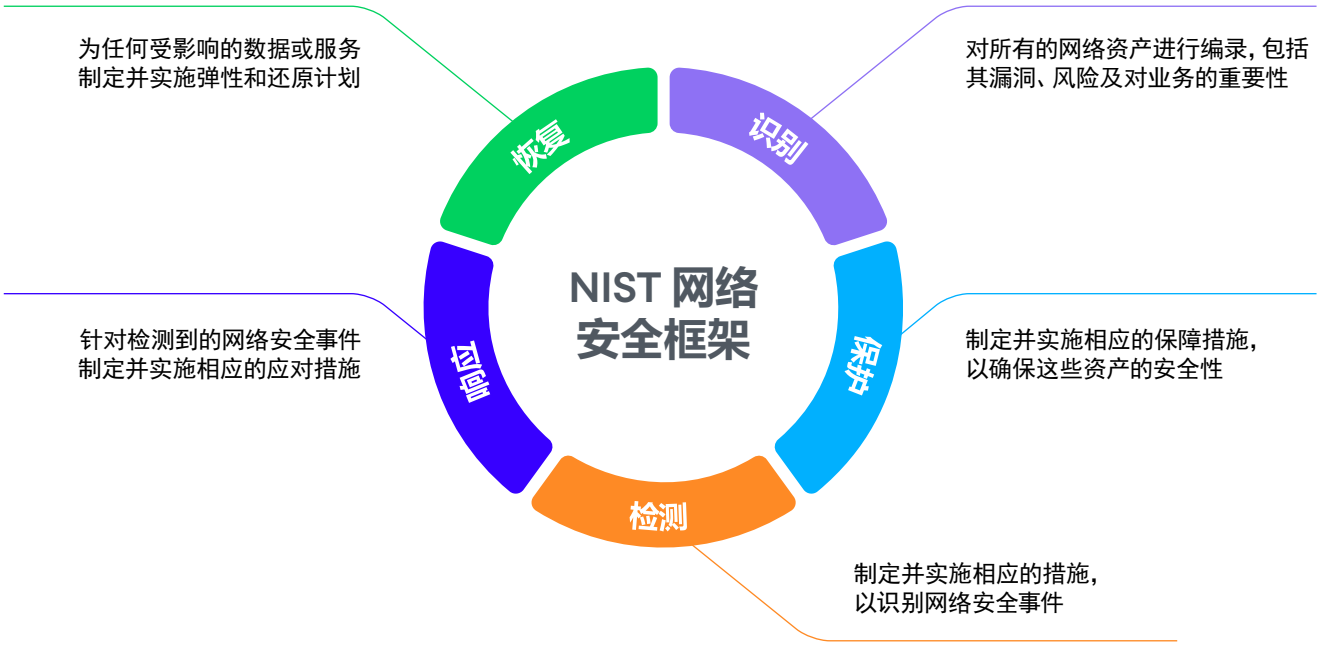
作为数据可用性策略的一部分，数据恢复通常是网络安全计划的最后保障，因此需要充分考虑和细致规划。组织不仅要利用 3-2-1-1-0 数据保护策略等措施，而且还需使用一套可备份整个基础架构的数据并支持在网络事件后随时随地将其还原到健康状态的可靠工具，以便在任何情况下都能快速恢复数据。

Veeam 客户可通过 Veeam Data Platform 以安全可靠、精心编排和详细记录的方式实现上述目标。借助一整套工具，包括 Veeam Backup & Replication、Veeam ONE 和 Veeam Recovery Orchestrator，客户不仅能够执行数据备份和恢复，而且还可根据 NIST 网络安全框架的所有阶段要求实现数据安全目标。

© 2023 Veeam Software。机密信息。保留所有权利。所有商标均归其各自拥有者所有。

# 网络安全计划的通用框架

NIST 网络安全框架是一个业经验证的框架，能帮助组织改进网络安全计划。该框架由一组可重复的阶段和功能组成，可应用于多项不同 IT 和业务实践，旨在指导组织专注于管理网络安全风险。




尽管数据可用性软件是 NIST 网络安全框架恢复阶段的关键组成部分，但大多数人并不认为它适用于网络安全计划的其他阶段。多年来，Veeam 一直致力于利用其作为企业数据保护平台的优势，更好地为客户提供数据保护所需的信息。

本文大量引用了 NIST 网络安全框架中的信息，为 IT 组织、安全团队及负责任的决策者提供洞察和知识，以利用 Veeam Data Platform 提供其他的丰富信息源和功能，从而协助识别关键数据、检测恶意软件、保护数据、快速响应主动威胁和迅速恢复干净数据，还重点介绍了实现上述目标所用的关键功能。

© 2023 Veeam Software。机密信息。保留所有权利。所有商标均归其各自拥有者所有。

# 识别关键数据

与防御企业可能遭遇的任何灾难一样，制定计划是首要任务。事实上，网络安全与传统灾难恢复有一个共同的核心问题：您无法保护您不了解的内容。较之主动防御和应对网络安全威胁，对需要保护的资产进行编录和分类似乎无关紧要，但了解面临风险的内容和相对优先级是应对网络威胁的第一步。Veeam 解决方案具有以下可靠功能，可成为识别关键数据的多层策略的重要组成部分。

## 对关键系统和数据进行编录

为了制定可靠的恢复计划，IT 和安全团队需要与业务团队展开密切配合，以掌握整个组织中的所有工作负载和数据，并对其进行编录和优先级排序。建议先从 Veeam ONE 中提供的报告和 Veeam Backup & Replication 备份的系统目录开始。所有关键数据均应进行备份，Veeam 解决方案可明确指出是否存在未受保护的虚拟机或数据。

同样，安全团队使用的网络和安全工具将能够创建环境中的系统列表。比较这些不同的系统通常可突显每个工具的数据保护缺口，从而尽量完善保护和恢复计划。

## 通过标记和分类来识别数据并对其进行优先级排序

借助 Veeam Backup & Replication 中的标记和数据分类功能，客户可先获得现有工作负载（其备份）目录，并开始应用标记来识别系统元数据，例如位置、所有者及恢复优先级。这种做法有时会突出显示缺失的数据，指出数据保护方面的差距，并识别正确制定数据恢复计划所需的关键元数据。

应用元数据后，客户便可使用 Veeam Recovery Orchestrator 中的向导驱动型恢复计划功能来创建恢复计划，从而缩短制定计划所需的时间。然后，客户可与业务团队一同单独审查该计划，以根据业务需求确保其准确性和完整性。

## 通过自动恢复测试凸显不足和变更

确定备份或计划是否尚不可用于紧急情况的最佳方式是对二者进行测试。Veeam Recovery Orchestrator 的自动化测试功能有助于确保部分或全部基础架构的全面可恢复性。除了可在测试执行过程中显著减少工作量外，自动执行测试恢复流程的优势还包括增加测试频次，从而更快地发现缺陷。

系统未备份或未列入计划是频繁测试可以发现的问题之一。定期查看相关测试结果并快速修复任何缺陷有助于进一步明确需要保护的对象。

© 2023 Veeam Software。机密信息。保留所有权利。所有商标均归其各自拥有者所有。

# 保护备份基础架构和数据

备份基础架构在任何 IT 环境中都有着特殊的意义，不仅为数据安全提供了最后的安全屏障，而且还包含所有数据的多个副本（越重要，副本越多），包括生产环境中可能被删除的数据。因此，它成为了犯罪分子突破安全屏障、窃取数据和提高其赎金勒索计划成功率的理想切入点。鉴于此，保护备份基础架构本身至关重要。

## 零信任备份基础架构

保护备份的第一步是防止未经授权访问备份管理系统本身。应实施零信任原则 — 明确验证、假设违规和最小权限访问，以尽可能加大横向移动到备份基础架构的难度。

利用多重身份验证，并部署单独的专用数据保护身份和访问管理 (IAM) 系统来控制用户策略，可确保用户身份得到妥善验证并加大破坏难度。实施最小权限访问，例如拥有单独的管理和操作帐户，以防止意外错误，并最大限度地减少权限升级。最后，所有的配置均应假设基础架构的其余部分遭到破坏，具体方法是将备份组件隔离到隔离的网络上，并限制通过 VPN 或远程连接访问 Veeam Backup & Replication 控制台本身。

备份基础架构的每个级别均应采用上述方法，但每个级别看起来可能略有不同。操作系统、文件共享、带外管理及用于管理它们的其他任何应用程序均应遵循类似的原则。

## 分析备份基础架构合规性

为了帮助客户正确实施零信任原则，Veeam Backup & Replication 控制台采用了名为“安全与合规分析器”（原“最佳实践分析器”）的内置实用程序，用于分析 Veeam 基础架构并报告尚未根据 Veeam 建议实施的配置项目。该分析应定期运行，并应更正或暂停每个不合规项目。暂停的项目将注明用户以及暂停日期/时间。修复完成后，应再次运行分析，并记录结果。

© 2023 Veeam Software。机密信息。保留所有权利。所有商标均归其各自拥有者所有。

## 确保在需要时备份始终可用

现在，删除备份以使数据无法恢复是勒索软件的一个共性。因此，确保备份无法被篡改或删除至关重要。

不可变性是计算机科学领域中很早提出的一个概念，最近已经成为备份的关键特性，特别是对于需要保持无变更或错误以满足保留需求的备份。借助强化存储库、对象存储、第三方去重设备或磁带，Veeam 备份能够以管理员也无法修改或删除数据的状态进行存储。与任何安全系统一样，通常都有变通方案，因此必须考虑整个堆栈乃至数据中心，以确保消除或严格控制这些变通方案。

网络安全领域流传着一个经典笑话：最安全的系统是关闭电源、断开网络连接并存放在无人可踏足的房间中的系统。这则笑话虽然正确，但很荒唐，因为这样的系统没有存在的意义。但在考虑备份的安全性时，这句老话恰如其分。如果只能在必要时可供访问，离线存储的备份就最不可能被篡改。Veeam 提供了多个选项来创建这种用于存储备份的物理隔离方案，包括需要不同身份验证的在线系统和卓越的离线存储介质 — 磁带。

但任何计划都不应依赖于单一的保护层。Veeam Backup & Replication 可采用 “四眼” 原则实施备份删除。与 “核密钥” 旧方法类似，该配置需要两名管理员授权备份删除，以防止意外或恶意删除备份。

零信任安全模型

“零信任” 概念的目标是消除过去存在于边界安全领域的固有信任，让威胁在环境中寸步难行。秉持 “从不信任，始终验证” 的原则创建一个无边界的安全模型，该模型不假设防火墙会阻止网络威胁。在该模型中，每个系统都会对每次新的交互进行验证，不会信任任何一次交互。

零信任安全模型的三个原则包括：

1. 明确验证
2. 提供最小权限访问
3. 假设存在漏洞

## 加密自己的备份

为了保护数据在泄露后不被滥用，Veeam 可对备份进行加密，以防止任何人在 Veeam 基础架构外部对其进行访问。虽然这不会阻止数据被勒索软件窃取或锁定，但也能够有效防止其被用来实施勒索计划。这种加密既可在 Veeam 内部进行管理，也可以绑定到第三方密钥管理系统 (KMS)，以委托集中管理这些密钥。

© 2023 Veeam Software。机密信息。保留所有权利。所有商标均归其各自拥有者所有。

# 检测网络威胁

确定了系统和数据的整体情况后，组织就需要制定计划和部署系统，以快速检测对相关资产的入侵问题。快速检测能够显著缩短威胁潜藏时间并降低其影响，这些威胁往往意味着经济损失。在这方面，Veeam 软件也可成为网络威胁检测的多层策略中的关键组成部分。

## 注意异常行为

恶意软件的关键策略之一是在升级权限和在环境中横向移动时逃避检测，从而感染尽可能多的系统。为此，它可能一次仅做出一些细小改变，以免引起注意。此外，恶意软件开发者越来越狡猾，为了阻止我们恢复数据和妨碍其索取赎金，他们已经开始删除备份、缩短备份保留时间或禁用备份作业。Veeam 可以通过 Veeam ONE 中的多种警报和报告来识别这些类型的异常行为并发出警报。

## 在备份期间扫描恶意软件

借助内联恶意软件检测，Veeam Backup & Replication 能够分析通过 Veeam 代理节点的数据块，以识别新加密活动的蛛丝马迹，这是活跃恶意软件的关键指标。根据对备份索引的搜索，该解决方案可检测到恶意文件名和特征库，如果发现可疑内容，则备份将被标记为可疑对象。

## 检测备份中的恶意软件

Veeam Backup & Replication 的 SureBackup 功能最初旨在自动执行备份的还原和验证，以验证其可恢复性。鉴于终端保护软件并不完美，这可能会导致恶意软件入侵备份，因此 SureBackup 还提供了一组强大功能，可检查备份中是否存在恶意软件。

作为可还原性测试的一部分，SureBackup 能够使用恶意软件扫描工具来扫描已还原的虚拟机。这支持组织在“信任但验证”的检测方法中利用辅助恶意软件检测工具。另一优势是，SureBackup 扫描对生产工作负载没有任何影响，因此有助于执行更彻底的扫描。SureBackup 还能够将单个磁盘挂载到测试机器上，然后扫描文件中的恶意软件，以便在无需进行全面还原时提高恶意软件扫描的速度和资源利用效率。

如果在这些扫描中发现了问题，那么该特定还原点将被标记为可疑还原点。

© 2023 Veeam Software。机密信息。保留所有权利。所有商标均归其各自拥有者所有。

## 执行定期恢复计划测试以检测威胁入侵

定期测试恢复计划可通过快速发现恶意软件造成的破坏来确保网络安全。全面恢复计划测试（包括应用程序验证）期间出现的故障，有助于快速找到基础架构中密钥文件被加密或配置文件被不当修改的位置。这对于检测在启动序列中执行的恶意软件尤为有用。

## 集中式日志报告和关联

将日志文件发送到外部系统日志服务既提供了二级日志存储库，又提供了便于跨系统进行事件关联的集中化。对于大多数安全团队而言，这是安全事件和事件管理器 (SIEM) 系统的主要功能。通过将 SIEM 系统设置为系统日志目标，Veeam 发现的破坏指标可以直接在安全团队使用的系统中进行标记，从而缩短响应时间，并为安全分析人员提供更可靠的事件视图。

**潜藏时间**

潜藏时间（恶意软件在被发现之前潜伏于环境中的时间）是指恶意软件潜伏在环境中而不发动主要攻击的时间。它可能会利用这段时间破坏其他帐户、升级权限、 深植于操作系统、横向传播到其他系统，并收集可用于当前或未来攻击的情报。

## 用于数据保护的外部集成

事件 API 是一组应用程序编程接口 (API)，网络安全工具可利用这些接口将发现的感染告知备份基础架构，并将备份标记为可疑备份或受感染备份。Veeam Backup & Recovery 可配置为根据此信息向管理员发出警报，以便其通过一系列操作进行快速检查、准确验证和做出响应，例如创建即时备份、执行 SureBackup 操作来检查感染情况和恢复干净文件，并创建备份的不可变副本以供取证。核心安全工具和数据保护平台之间的这种开放式集成点可显著加强沟通，从而缩短恶意软件潜藏时间，并有助于更干净、更快速地恢复。

© 2023 Veeam Software。机密信息。保留所有权利。所有商标均归其各自拥有者所有。

# 应对网络威胁

为了防止保护疏漏，企业需要时刻保持警惕，并尽快删除侵入的恶意软件。与制定从自然灾害中恢复的计划一样，所有决策的一大目标应该是达成恢复时间目标 (RTO)。在网络安全事件中，目标大同小异，即阻止恶意软件并将其从环境中删除，以便系统重新投入使用。若能缩短恶意软件潜藏和泄露数据的时间，便可减少清理工作并加快恢复速度，因此随时快速响应至关重要。

## 使用备份进行网络取证

如前所述，SureBackup 功能不仅能够测试备份的可还原性，而且还可以检测恶意软件。响应阶段的目标之一是确定潜藏时间。Veeam Backup & Replication 控制台会使用恶意软件标志，来显示恶意软件是在还原点检测到的，还是在此时间范围内由第三方工具使用事件 API 发现的，从而简化查找第一个感染点所需的搜寻工作。

安全恢复是 Veeam Backup & Replication 的另一项功能，支持在全面还原之前挂载磁盘和扫描恶意软件。迭代此流程直至发现未受感染的点，这有助于更轻松地找到恶意软件首次现身既定系统的时间点，并可通过恢复处于休眠状态的恶意软件来避免再次感染。

借助 Veeam Recovery Orchestrator，可采用编排的 “洁净室” 方法在整个环境中执行这一安全恢复流程。这不仅为检查干净的还原点提供了一种更快的方法，而且还迅速为网络安全事件的数字取证增添了重要信息。

泄露

如果数据遭到恶意软件访问和篡改，那么它很可能已然失窃。泄露的数据是指从受害者的环境落入网络犯罪分子手中的数据。 网络犯罪分子可能会对外透漏或兜售这些数据，导致公司机密泄露、声誉受损及个人信息被盗，进而引起欺诈或网络攻击。

## 通过 YARA 增强威胁捕获

作为网络安全威胁猎手熟悉的工具，YARA 是一种基于规则的方法，用于快速识别和分类恶意软件。在 SureBackup 或 SecureRestore 操作过程中，用户可确定并执行 YARA 规则，以便对恶意软件执行初始分类，然后在备份中对其进行搜索。

## 使用 ServiceNow 执行事件跟踪

通过直接集成到 ServiceNow 中，Veeam 解决方案能够自动新建用例，并随着情况的变化更新现有用例，以帮助不同团队更高效地沟通，并提供更自动化的事件历史记录文档。

© 2023 Veeam Software。机密信息。保留所有权利。所有商标均归其各自拥有者所有。

# 更快速地恢复安全数据

根据网络安全事件的性质，还原干净的数据对于恢复服务至关重要，尤其是在遭遇勒索软件攻击的情况下。如果潜藏时间很长，那么许多恢复点可能藏有恶意软件，并可能需要进行早期回溯以找到干净的还原点。与传统灾难恢复一样，达成数据丢失最少化相关目标 — 恢复点目标 (RPO) 至关重要。鉴于在响应阶段发现感染苗头很重要，因此其中许多工作将与数据恢复工作并行进行。

## 备份只有在可还原（且没有感染恶意软件）的情况下才有用

在检测和响应阶段，通过 SureBackup 和事件 API 等功能标记可疑或受感染的还原点，可轻松地在 Veeam Backup & Replication 控制台中确定是否在每个还原点检测到恶意软件。这是一个良好的起点，但并不能保证早期的还原点是完全干净的。

为了减少还原受感染数据的可能性并最大限度地减少重复工作，恢复工作应与响应阶段执行的网络取证双管齐下。IT、安全和业务团队之间牢密切配合对于还原正确数据并避免再次引入恶意软件至关重要。

当使用最新恶意软件检测工具作为 SureBackup 和安全恢复的一部分时，可在早期还原点中发现以前未检测到的恶意软件，因此切勿仅依赖早期扫描中的恶意软件标志。如果干净的还原点早于定义的 RPO，则可使用文件级还原来还原单项关键数据，同时避免完整备份中的恶意软件。

### 支持网络安全恢复的备份与复制

复制可能是网络安全恢复计划的一部分，但了解复制副本与备份的目的非常重要。复制的重点是尽快移动数据，并回到最新的可靠复制副本。备份不是连续的，因此在确保不被感染和可还原性方面有着明显的优势。网络安全恢复需要基于潜藏时间和还原点的清洁度，因此备份成为了一种更常见的机制。

© 2023 Veeam Software。机密信息。保留所有权利。所有商标均归其各自拥有者所有。

## 尽快还原未受感染的数据

即便是最简单的环境，自动化也是快速恢复的关键，但恢复模式亦会有所不同。借助存储阵列快照和即时恢复，还原的备份几乎立即可供使用。

Veeam Recovery Orchestrator 可规定整个还原流程，让其如同点击按钮一样简单。Veeam 将还原计划与感染标志、安全恢复、存储阵列快照、即时恢复及应用程序验证相结合，能实现非常强大的功能组合，可快速高效地还原数据，同时尽可能确保数据没有感染恶意软件。

## 实现 I/O 异常可视化

有时，没有什么比可视化图表更能凸显趋势了。在 Veeam Backup & Replication 用户界面中，在从复制副本作业中恢复时可查看图表，这有助于确定大规模加密的起始时间，从而减少查找加密前时间点所需的工作量。

© 2023 Veeam Software。机密信息。保留所有权利。所有商标均归其各自拥有者所有。

# 总结

如今，制定网络安全计划并非易事。威胁层出不穷，漏洞对于犯罪分子而言可能有着巨大价值，因此组织需要利用自己掌握的所有工具来创建安全层，以便在 NIST 网络安全框架的每个阶段最大限度地提高其有效性。Veeam 可为 NIST 网络安全框架的所有阶段提供价值，有助于改进组织的整体网络安全计划：

- 创建并定期测试恢复计划可提供宝贵的数据以供在识别阶段使用，从而确保快速识别并有效保护关键数据。
- 实施文档化的最佳实践和原生安全功能可确保在保护阶段轻松解决备份和备份基础架构问题。
- 由于备份涉及整个基础架构中的所有数据，因此它们可用于针对检测阶段中终端观察可能遗漏的恶意软件执行第二次重要检查。
- 快速访问不同的时间点和虚拟的“洁净室”环境对于响应阶段中的信息收集工作至关重要。
- 可按需使用经证明具有可还原性且没有感染恶意软件的备份，并能够尽快还原到干净可用的状态，以支持恢复阶段。

IT 团队不仅是可还原数据的管理者，还应积极参与到网络安全计划中。借助本文档中的指南，IT 团队现在应能够与安全团队高效沟通，从而将基于 Veeam 的数据保护平台融入整体网络安全计划。

如欲详细了解本文档中提到的一系列功能，请查看 Veeam 帮助中心提供的用户指南。其中许多功能均为 Veeam Data Platform 2023 年下半年更新的新功能。

**Veeam Data Platform 2023 年下半年更新**
白金版 30 天免费试用

© 2023 Veeam Software。机密信息。保留所有权利。所有商标均归其各自拥有者所有。