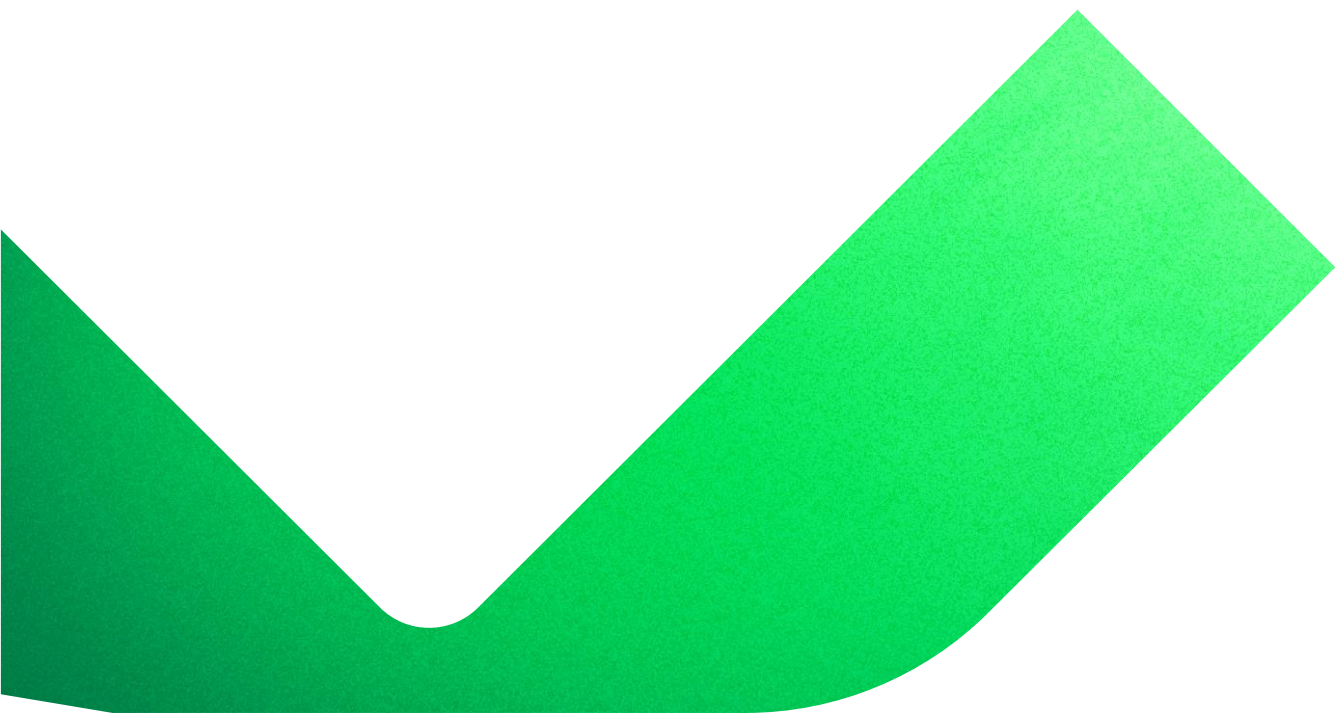
零信任数据弹性（ZTDR）

安全的数据备份和恢复架构

实施零信任的实用方法



概述

各行各业各种规模的企业都明白零信任在确保数据和业务安全方面的重要性。然而，当前的零信任模型尚未实质性地应用于数据备份和恢复。将零信任原则扩展到数据备份和恢复的概念符合网络安全的整体性，并且保护敏感信息不仅仅涉及边界安全。

为了应对这一挑战，Veeam 与 Numberline Security 的零信任专家 Jason Garbis 合作开发了零信任数据弹性框架，该框架旨在最大限度降低风险，加强数据保护，并彻底改变组织的安全态势。该框架基于网络安全和基础设施安全局（CISA）零信任成熟度模型（ZTMM）构建，并将 ZTMM 的主要原则扩展到了备份和恢复场景。零信任数据弹性框架意味着从不假定信任，并且在整个数据生命周期（包括备份和恢复过程）中一致地应用安全措施；这是一个实用的模型，可以帮助 IT 和安全团队显著降低风险、增强数据保护并大幅改善任何组织的安全态势。

想要详细了解零信任数据弹性？
下载白皮书

Veeam 的零信任方法：零信任数据弹性 (ZTDR)

零信任是组织安全战略的基础，在保护备份环境方面，关键原则（例如对最关键数据资产进行细分、最小特权访问以及使用 Identity and Access Management (IAM) 最佳实践进行持续身份验证和授权）尤为重要。通过整合零信任数据弹性功能，企业可以化解数据保护解决方案带来的独特挑战，并为企业制定全面的安全策略，无论他们身处内部、云端还是混合环境中。

零信任的一个关键概念是无论给定环境的安全性如何，始终假设存在安全漏洞。在 ZTDR 方法中，应对这种风险的一项关键技术是将备份管理软件和备份存储分成单独的弹性区域或安全域，将备份数据与备份管理软件的任何威胁隔离开来，无论这些威胁来自内部还是外部。Veeam 支持多种技术，以创建具有高度安全性、不可变存储的弹性区域（参见图 1）。

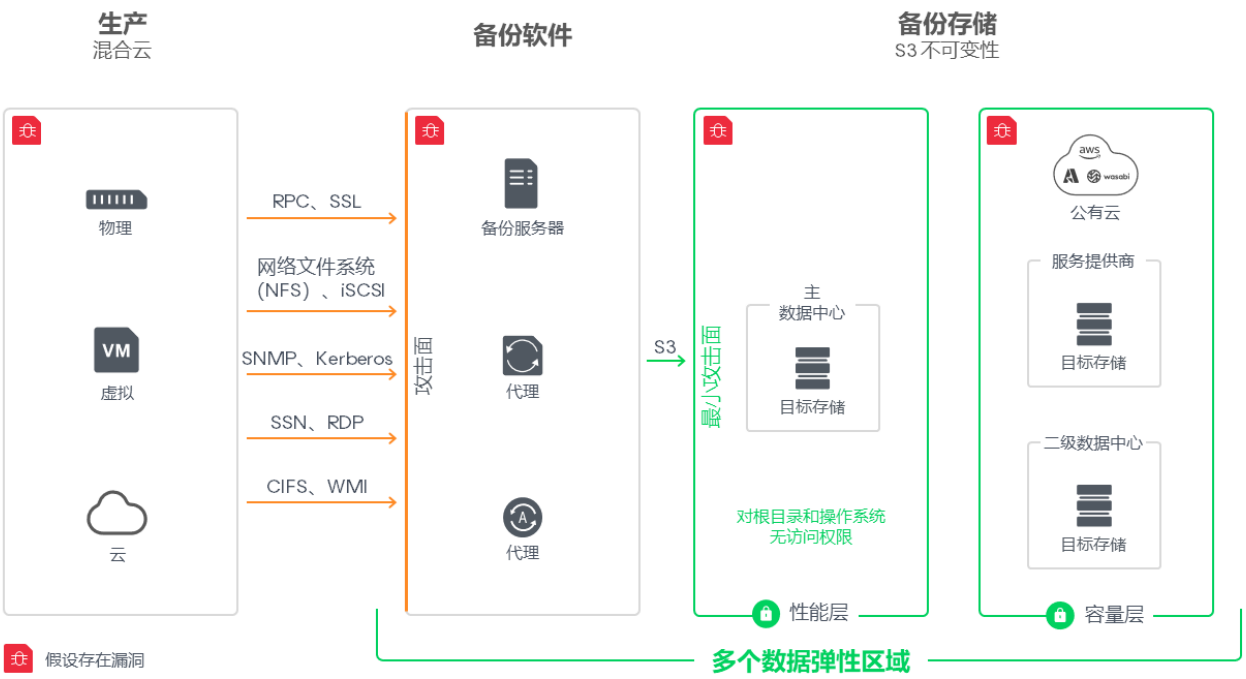


图 1

由于数据保护解决方案对整个组织的生产数据（通常是最关键的数据）具有最高级别的读写访问权限，因此必须遵循零信任最佳实践来确保组织的备份环境安全无虞。

零信任数据弹性原则

在 CISA 零信任成熟度模型（见图 2）的基础上，组织应针对数据支柱特别考虑一些其他事项。

CISO 零信任成熟度模型

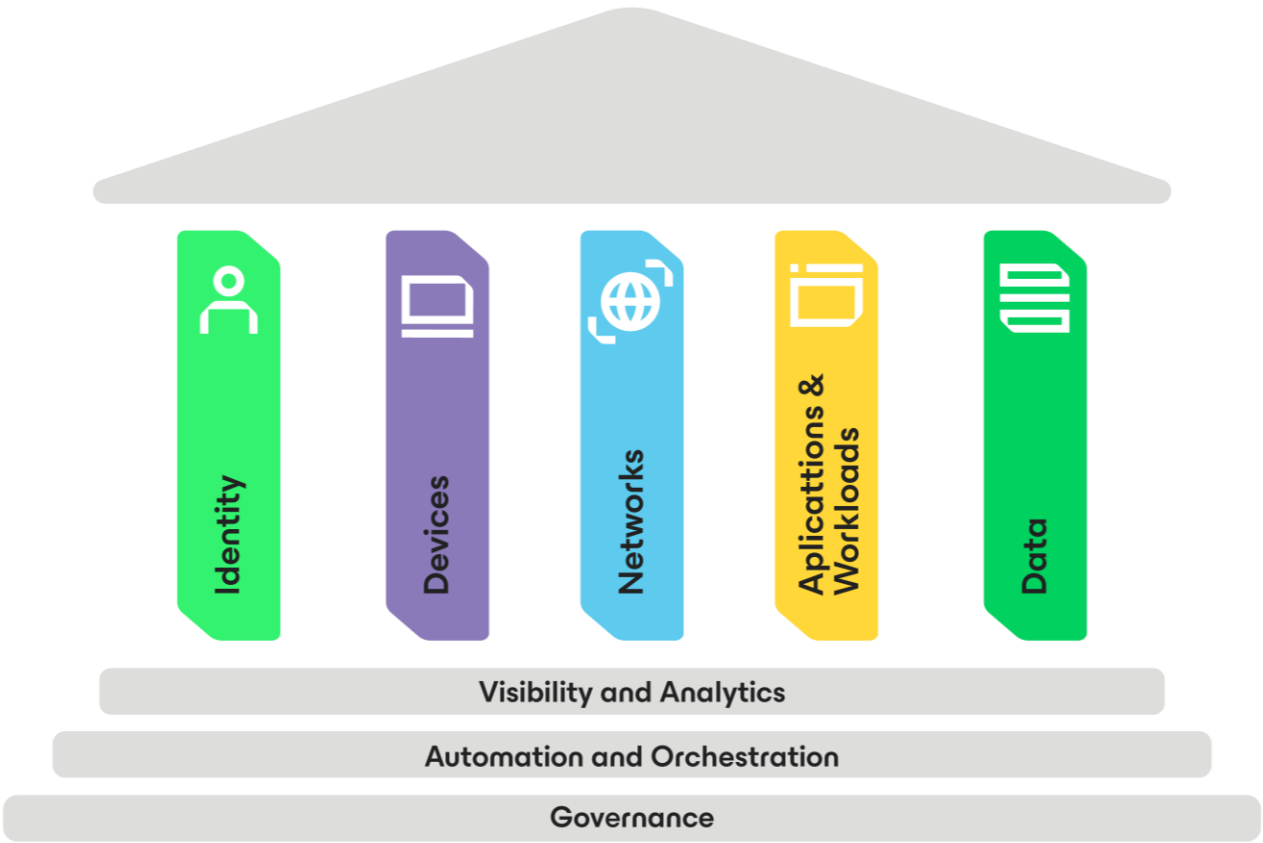


图 2

零信任数据弹性研究报告重点介绍了零信任数据弹性 (ZTDR) 的 5 个核心原则，以帮助组织实施整体网络弹性策略，并确保在面对不断变化的网络威胁时保护关键数据资产。

最小权限访问

此原则强调授予对执行预期功能至关重要的人员、流程、设备或工作负载的访问权限。

备份基础架构的受控访问：

- 通过实施零信任策略来控制对备份基础架构的访问，可确保只有经过验证的用户才能与备份解决方案建立连接。这是防止未经授权的访问和潜在数据泄露的关键步骤。

细粒度自助服务角色和受限备份管理员角色：

- Veeam 提供细粒度自助服务角色和受限备份管理员角色，表明了其对执行最小特权原则的承诺。这可确保用户只能访问其任务所需的特定功能，从而减少无意或故意误用的可能性。

Identity and Access Management (IAM) 最佳实践

- 通过实施 IAM 最佳实践，例如使用多重身份验证 (MFA)，可为备份环境增加一层额外的安全保护。这是防止未经授权访问的关键措施，尤其考虑到与备份解决方案相关的高级别权限。

关键运营决策的“四眼”原则：

- 通过将“四眼”原则纳入关键运营决策，可确保关键行动需要至少两名授权人员的批准或验证。这增加了一层监督，并降低了恶意或错误活动的风险。

不变性

即使拥有安全的网络边界，零信任的一个关键概念仍是假设存在漏洞。备份的不可变性是一种强大的防御机制，可确保内部或外部威胁行为者无法修改或删除关键的备份数据。

用于最小化攻击面和影响范围的分段：

- ZTDR 的关键概念是将备份软件和备份存储划分为单独的弹性区域。通过隔离关键组件，这可以最大限度地降低内部或外部威胁的潜在影响。通过确保备份软件在备份存储上没有操作系统/管理级别的权限，可以增加一层保护。

多个弹性区域和 3-2-1-1 备份规则：

- 多个数据弹性区域或安全域可提供多层安全性。此外，3-2-1-1 备份规则是备份策略的最佳实践，与数据弹性原则非常吻合。在两种不同类型的介质上拥有至少三个数据副本，其中至少一个异地副本和至少一个物理隔离或不可变副本可提供多层安全性，从而降低数据丢失风险。

弹性区域

网络的核心零信任概念是微分割，将安全边界分解为较小的区域，从而减少攻击面、任何受感染区域的影响范围和攻击者的横向移动。对于 ZTDR，可以使用数据弹性区域来应用此概念。弹性区域将备份存储分开，并将存储控制平面与备份软件及其控制平面隔离。这提供了一条关键的分界线，即使在备份软件遭到破坏的情况下，也能确保备份数据的生存能力。发生这种情况的原因有很多，包括内部威胁行为者。备份系统必须确保从全新安装的备份软件中简单、快速地恢复备份数据。

生产
基础架构

Veeam
基础架构

自主
备份数据

不可变　加密　3-2-1-1-0

数据完整性和增强的安全性：

- 配置兼容的备份存储库并为不可变的备份存档设置保留期是确保数据完整性和增强安全性的主动措施。不可变的备份存档可以有效抵御勒索软件攻击和其他形式的数据操作。

系统弹性

整体 IT 安全方法包括整个生态系统（包括平台、工具、技术和流程）的弹性。Veeam 的多种弹性选项表明 Veeam 致力于为组织提供抵御各种类型中断（包括整个系统丢失）的工具。

不可变的备份存档的时移检测：

- 时移检测的实施是一种防止删除不可变的备份存档的主动措施，即使 NTP（网络时间协议）遭到破坏也是如此。该特性可增强备份存储库的安全性和可靠性，确保关键备份数据的完整性。

灵活的恢复选项：

- Veeam 提供灵活的恢复选项，甚至适用于不同的环境，支持物理和虚拟部署及混合环境，以适应企业可能运营的各种 IT 基础架构。这种灵活性使组织能够快速恢复：例如在原始环境不可用的情况下，将内部 VMware 恢复到 AWS 或 Azure，或者将 AWS 恢复到 Azure。

细粒度数据还原选项：

- 将数据以不同粒度还原到不同环境的灵活性可增强整体数据弹性。这种适应性使组织能够根据不同场景的特定需求定制其恢复流程。

主动验证

对功能方面和流程的持续验证是确保数据始终受到保护以及及时检测和处理任何异常情况的关键。

持续监控和验证：

- 对 365/24/7 全天候监控系统的重视反映了对网络安全威胁随时可能出现的认识。通过实时洞察环境状态，管理员可及早发现任何异常情况，并在潜在的网络攻击或数据丢失发生之前进行调查和做出响应。

- 利用 Veeam ONE 等监控工具可主动维护备份和恢复环境的健康与安全。Veeam ONE 能够监控各种参数，包括 CPU 使用率、数据存储写入率、网络传输率和增量备份大小，可为企业提供有关潜在问题的重要洞察信息。

端到端可视性：

- 对整个数据保护基础架构的端到端可视性至关重要。它可确保组织全面了解其备份和恢复系统的健康状况和状态，从而做出明智的决策并在需要时迅速采取行动。
- 作为 Veeam 最新发布的 12.1 的一部分，Veeam 的全新威胁中心汇总了整个平台和基础架构的洞察，并将其整合到单一虚拟管理平台中，可突出显示威胁、识别风险，并为组织提供适用于整个数据保护环境的功能强大的简单安全记分卡。

操作简单

简单操作在发生灾难或网络安全事件时的重要性体现在简单性在有效恢复中发挥的关键作用。停机时间越长，对企业运营和利润的影响就越大。

勒索软件攻击中的平均停机时间：

- Veeam 的《2023 年勒索软件趋势报告》显示，勒索软件攻击造成的平均停机时间为 3 周。这凸显了快速恢复的紧迫性和重要性，尤其在每一刻都至关重要的高压情况下。

平衡工具、人员和流程：

- 在工具、人员和流程之间取得适当的平衡是一项重大挑战，尤其是在组织应对灾难或网络攻击时。操作简单性包括简化工作流程、优化流程以及确保使用正确的工具进行高效恢复。

简化还原功能方面的投资：

- Veeam 等行业领导者通过解决恢复的复杂性问题，积极投资于提供还原功能。Veeam 能够利用 Veeam Recovery Orchestrator 等工具将数据从一个平台还原到另一个平台，这表明他们致力于简化复杂的还原场景，并不断更新、自动化和全面测试故障切换计划，从而确保在高压场景中做好准备。

了解版本 12.1 中的最新安全功能

结论

随着数字格局的不断发展和扩大，网络攻击和威胁行为者的能力也在不断变化。因此，我们迫切需要统一并加强 IT 和安全协作及有效性，以更好地保护和捍卫我们组织的数据、设备和人员。虽然走向成熟的这个过程不是一件一蹴而就的事，但必须尽早开始。第一步是零信任。CISA 的零信任成熟度模型（ZTMM）提供了对保护组织至关重要的核心原则，但并未涵盖所有内容。作为 CISA 零信任成熟度模型（ZTMM）的扩展，引入零信任数据弹性（ZTDR）是一种战略性和前瞻性方法，以应对不断变化的网络威胁环境。

ZTDR 原则（包括最小权限访问、不可变性、系统弹性、主动验证和操作简单性）的整合展现了保护组织数据的全面策略。通过采用 ZTDR，组织将有一条清晰而具体的途径来加强其安全态势。这意味着运营更高效并且 IT 和安全团队之间保持协调，最终将更快、更安全地进行恢复。

关于 Veeam Software

Veeam 是数据保护和勒索软件恢复领域首屈一指的全球市场领导者，其使命是帮助每个组织不仅从数据中断或丢失中恢复过来，而且向前迈进。借助 Veeam，组织可在其混合云环境中实现数据安全、数据恢复及数据自由，实现极致弹性。Veeam Data Platform 为云端、虚拟、物理、SaaS 和 Kubernetes 环境提供统一解决方案，确保其应用和数据受到保护并始终可用，让 IT 和安全领导者高枕无忧。Veeam 总部位于俄亥俄州哥伦布，在 30 多个国家和地区设有办事处，保护着全球超过 450,000 家客户，包括 73% 的全球 2000 强公司，他们信赖 Veeam 能够确保其业务正常运行。极致弹性始于 Veeam。请访问 www.veeam.com/cn 了解更多信息或关注 Veeam 的 LinkedIn @veeam-software 和 X @veeam。