将零信任扩展到数据备份和恢复

面向 IT 和安全专业人员的实用指南

内容

要点概述

零信任是一种高效的现代化策略，可更好地保护我们的企业 IT 基础架构免受勒索软件和其他威胁。数据备份和恢复系统对于我们的企业至关重要，必须纳入任何零信任计划。

然而，零信任的架构和实施可能非常复杂，直到目前，人们还没有就如何将其最好地应用于数据备份和恢复系统达成共识。

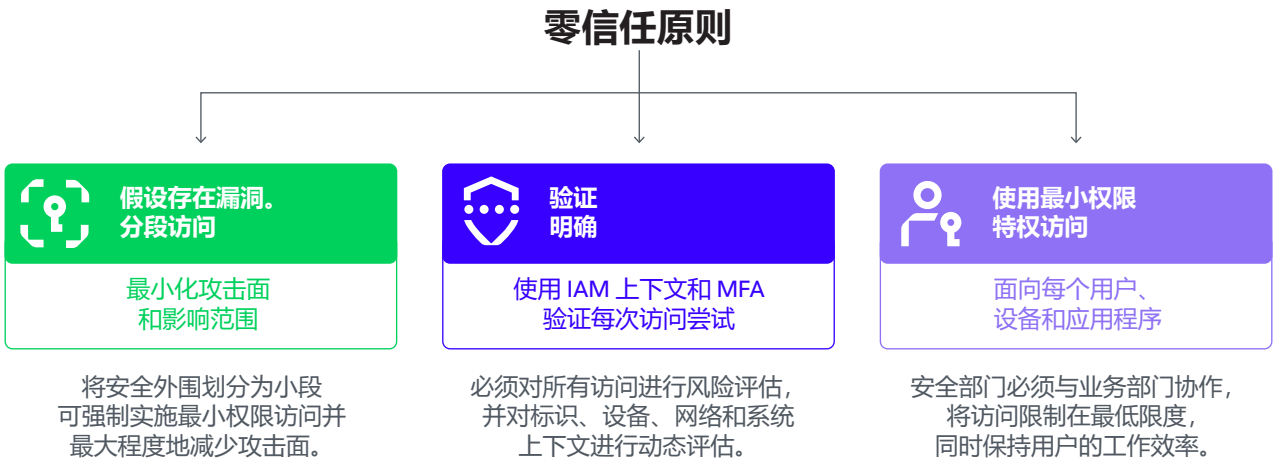
零信任数据弹性 (ZTDR) 是 Veeam 和 Numberline Security 推出的一种新模型，它基于网络安全和基础架构安全局 (CISA) 零信任成熟度模型而构建。ZTDR 将零信任原则扩展到备份和恢复，确保企业能够降低风险并实现其安全和弹性目标。

通过遵循本指南中介绍的零信任数据弹性方法，您将了解数据备份和恢复平台和架构中的关键特性，并能够在您的环境中快速有效地开始使用。

零信任：简介

零信任是一种现代安全策略，其理念是不应隐式信任任何用户、设备或网络数据包。为确保数据安全，应对关键数据资产的访问进行分段，并且必须对所有通信进行身份验证、评估和授权，然后才能授予任何访问权限。这必须应用于每个段及其数据、应用程序、资产或服务。

与传统信息安全架构相比，这是一个重大转变，传统信息安全架构基于静态的、基于网络的边界，显然无法保护我们的企业免受勒索软件和恶意攻击者的侵害。



介绍零信任数据弹性（ZTDR）

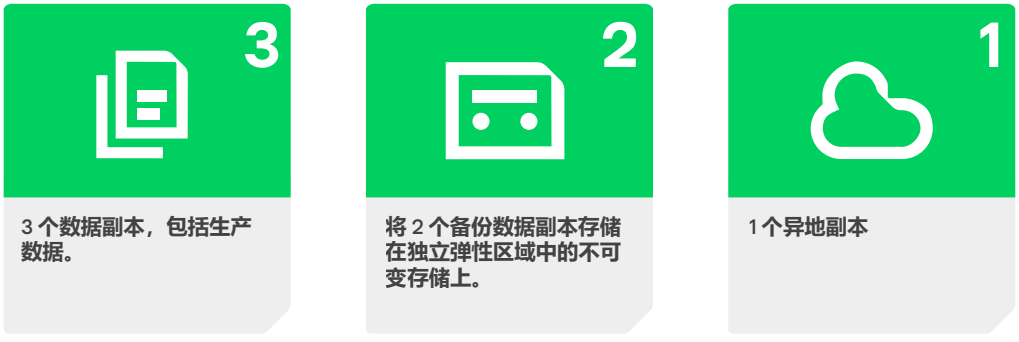
数据备份和恢复系统是企业 IT 的关键要素，但经常成为攻击目标。它们必须得到适当和全面的保护。

通过遵循 ZTDR 原则，根据 ZTDR 指南选择备份和存储厂商，您的企业将获得更强大的防御、更高效的运营以及更快、更可靠的恢复。

ZTDR 扩展了核心零信任原则

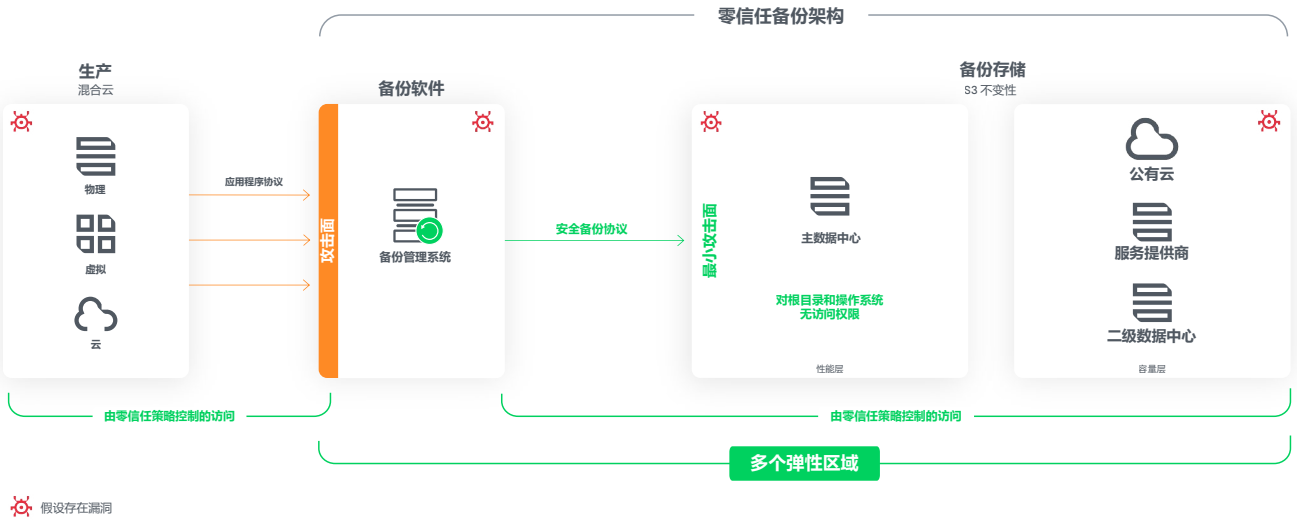
	分离备份软件和备份存储	多家弹性区域	不可变备份存储
	最小化攻击面和影响范围	3-2-1 备份规则	保护备份数据不被修改或删除
解决方案要求	数据备份和恢复解决方案在架构上应将备份软件和存储分开，最好能防止 root 或操作系统访问备份存储。 这些功能将允许您通过零信任策略严格实施访问控制。	数据备份和恢复解决方案应支持多个弹性区域，这意味着贵组织可以在任何单一备份系统或存储环境丢失或受损的情况下仍能继续运行。 这有助于您轻松满足 3-2-1 备份准则。	寻找能够轻松、高效地支持强大、可靠的不可变备份存储的数据备份和恢复解决方案。 这样，您就可以完全放心，即使面临恶意行为者的威胁，备份的数据也不会被删除或修改。

备份最佳实践的 3-2-1 原则：



ZTDR 参考架构

此 ZTDR 参考架构向您展示了如何将零信任平台与备份管理和存储系统一起部署。



ZTDR 入门

虽然零信任是一种过程，但您可以立即采取一些有效措施来提高数据备份和恢复基础架构的安全弹性。

本周：

了解您的备份和恢复系统在多大程度上满足 ZTDR 要求。

任务	要提出的问题
与您的网络和 IT 基础架构团队讨论您的网络分段	• 我们的网络是如何划分的？ • 备份软件和备份存储是否划分为单独的安全区域？ • 如何控制对备份基础架构各部分的访问和退出？
评估您的备份数据存储是否划分为多个弹性区域	• 我们是否遵循有关 3-2-1 的行业指南？ • 如果我们的一个备份区域不可用，那么我们的备份和恢复流程会怎样？ • 如果我们的两个备份区域不可用，那么我们的备份和恢复流程会怎样？
确定备份存储系统是否具有不可变性	• 您的存储厂商如何记录和保证不可变性？ • 恶意管理员能否使用根或操作系统对存储的访问来更改不可变性或保留设置？ • 如果系统时间被恶意提前，会发生什么情况？
验证您的恢复流程	• 我们的灾难恢复响应计划是什么？我们上次测试它是什么时候？ • IT 或存储团队中有多少人可以按照记录的步骤成功恢复系统？ • 如果（重要人员 X）在事件期间没空，会发生什么情况？

下周：

验证您的流程和工具，然后针对备份和恢复基础架构及流程的短期和中期变更进行规划并达成共识。

任务	要提出的问题
通过定期（每周 / 每月）进行测试，评估您对恢复流程的信心以及其可重复性	• 我们多久进行一次恢复测试？ • 我们从文档或流程差距中学到了什么？ • 何时可以补救这些问题？

任务	要提出的问题
开始规划网络配置、分段或防火墙规则更改	• 我可以与 IT 或安全团队中的哪些人员协作，以确定潜在更改的范围？ • 安全团队中的哪些人员正在领导我们的零信任计划，我该如何支持该计划？ • 我们正在进行哪些网络分段或基础架构变更？
制定存储配置变更或新厂商评估计划，以弥合任何不可变性差距	• 我们评估和采购额外备份存储的流程是什么？ • 我们需要做出什么样的财务、效率或风险论证？ • 我应该如何获得批准以启动供应商评估流程？
为任何流程和文档改进指派负责人	• 谁将参与批准和实施（流程 X）的更改？ • 我们如何才能为实施设定一个双方都同意的最后期限？

下个月：

开始实施短期更改，并开始识别任何需要的长期更改。

任务	要提出的问题
部署改进的灾难恢复流程，并再次测试	• 我们的灾难恢复流程改进了多少？ • 我们是否解决了所有流程和文档方面的差距？
对网络分段进行验证和迭代	• 网络的哪些区域仍然允许我们的备份系统进行广泛的网络访问？ • 我们如何加强防范以增强弹性来抵御勒索软件攻击？
执行存储容量、位置和不可变性改进	• 我们对备份存储容量的满意程度如何？ • 我们对备份存储系统不可变性有多大信心？ • 我们遵循 3-2-1 最佳实践指南的情况如何？ • 我们如何利用多个弹性区域？

您还应该寻找什么?

主动灾难恢复验证

需要恢复备份数据的事件可能会在意外时间发生，而且很可能是在高压环境下发生的。您的组织必须拥有充分理解、详细记录并经过充分演练的灾难恢复计划和流程。此外，请确保您对备份数据的完整性和有效性具有高度的信心。

操作简单

确保选择的系统足够简单，便于组织轻松、自信地运行，同时仍提供足够的功能、可扩展性和复杂性，以完全满足企业的需求。努力清楚地了解员工的能力和技能，这样运营就不会依赖于任何一个人或“超级英雄”。

常见问题解答

零信任是您可以从供应商处购买的东西吗?

否 — 零信任需要您**实施** — 它是一种安全策略，可更改和改进 IT、安全和业务成果。

零信任是否只是限制访问并降低用户工作效率?

否 — 零信任意味着消除所有**不必要的**访问，同时保持用户高效工作。许多企业实际上通过零信任**提高了**用户生产力和用户体验。

为何零信任至关重要?

零信任是保护企业免受勒索软件、恶意攻击者和其他风险的最有效方法。鉴于当前的威胁形势，我们有责任利用零信任。

您能否将当前的安全基础架构用于零信任?

是的，很有可能！如果使用得当，现代防火墙、身份认证和基础架构系统可以在您开始零信任之旅时为您提供支持。实现零信任成熟度的最佳水平可能需要额外的投入，这可以通过 ZTDR 参考架构等工具来进行指导。

其他资源

想要了解有关零信任和 ZTDR 的更多信息?

- 访问 Veeam 网站，阅读 ZTDR 的完整研究报告，了解 Veeam 实现数据安全和网络弹性的方法。
- 要阅读完整的 ZTDR 研究白皮书并了解 Numberline Security 对此的看法，请访问 Numberline 网站。

关于 Veeam Software

Veeam 是数据弹性领域的 #1 全球市场领导者，它认为企业应随时随地控制所有数据。Veeam 通过数据备份、数据恢复、数据自由、数据安全和数据智能提供数据弹性。Veeam 总部位于西雅图，为全球超过 550,000 家客户提供保护，他们信赖 Veeam 来确保其业务正常运行。请访问 veeam.com/cn 了解更多信息或关注 Veeam 的 @veeam-software 和 X @veeam。

了解更多信息：veeam.com