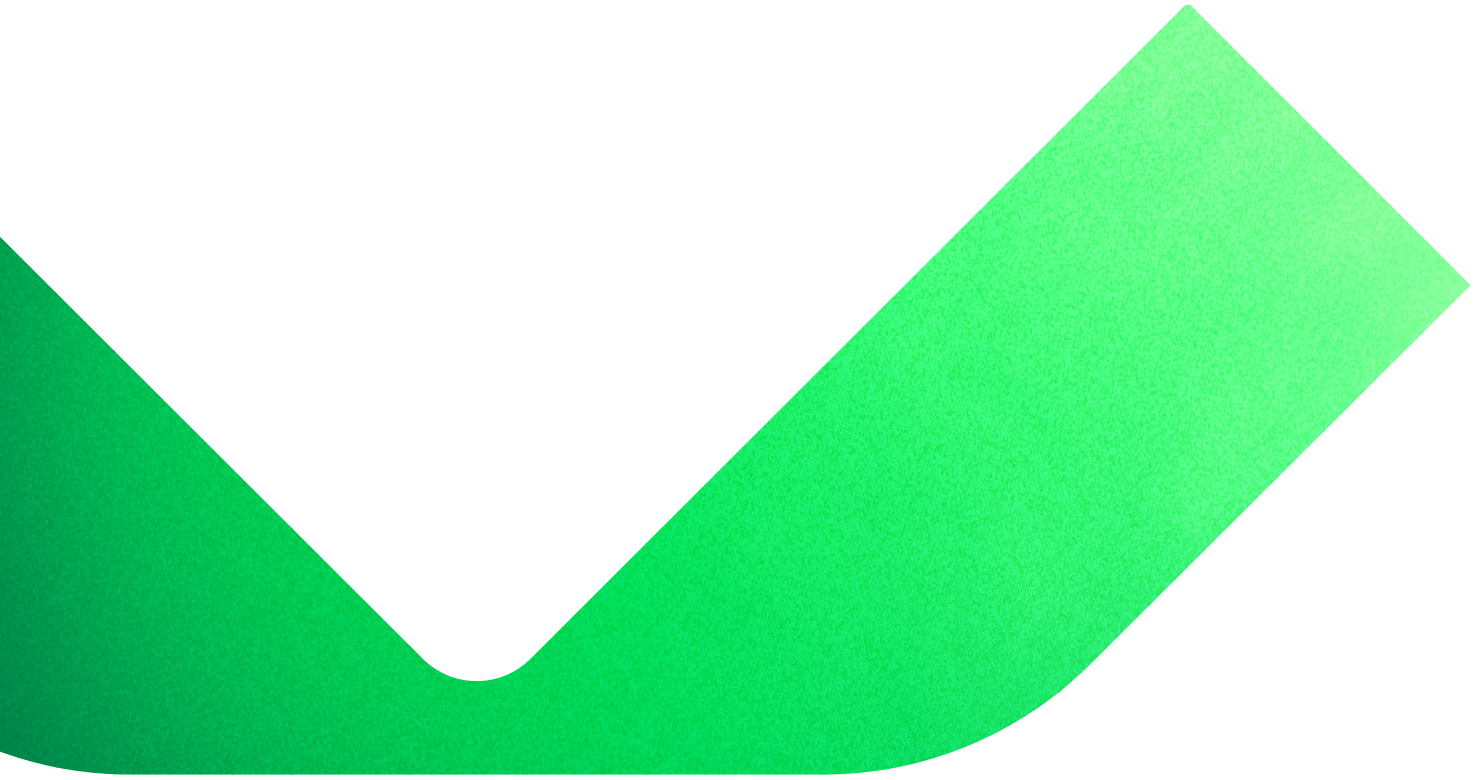
零信任
数据弹性

安全的数据备份
和恢复模型



内容

要点概述

如今，企业在保护数据和网络免受恶意攻击者侵害方面，特别是抵御勒索软件和数据泄露攻击方面，面临着持续的重大挑战。为了解决这些问题，一种名为“零信任”的策略在信息安全行业获得了极大的关注，并被全球企业广泛采用。

然而，即使是应用最广泛的零信任模式，在某些重要领域，尤其是数据备份和恢复领域，也缺乏全面的指导原则。我们认识到填补这一空白并将零信任原则应用到这一领域的重要性，因此引入了零信任数据弹性的概念。这包括一组要求、架构和对现有零信任成熟度模型的扩展。

具体来说，企业必须使用一种数据备份和恢复系统，该系统可提供不可变数据存储和配置，同时对生产中的源数据和备份数据实施上下文和强认证访问。该系统还必须无缝支持当今企业中常见的混合架构，并灵活处理不同环境的恢复问题。

通过实施满足这些要求的零信任架构，企业将更好地保护其数据、网络和应用程序免受恶意攻击者的侵害。与传统方法相比，零信任提供了明显更好的安全性，组织有义务采用它。本白皮书提出的新数据弹性要求增强并扩展了零信任，应被视为企业安全战略的强制性要求。

介绍

零信任是一种安全策略，其适用范围必然很广。但是，广泛使用的零信任模型和框架并未涵盖所有内容[1]. 这可能会导致企业安全架构中出现相应的漏洞或遗漏。具体来说，数据备份和恢复系统没有纳入常用的零信任框架。这是一个令人遗憾的空白，因为在勒索软件和数据泄露攻击中，企业数据往往是恶意行为者的主要目标。

数据备份和恢复系统是企业 IT 的关键要素，必须如此对待。它们可以读取所有重要数据，以便进行备份。他们还需要能够将数据写入生产环境，以执行数据还原功能。它们还包含企业最重要数据的完整副本。综上所述，所有这些属性都强调了数据备份和恢复系统的重要性，并突出了它们作为恶意行为者攻击目标的价值。

当然，几十年来，数据备份和恢复系统一直是 IT 职责的一部分，但往往不在安全团队的职责范围内。然而，考虑到企业目前面临的安全威胁的程度和复杂性，仅从网络和 IT 基础架构的角度来看数据备份和恢复已经不够了。在实践中，我们遇到过一些企业，他们的系统配置不当且未受到监控，因此造成了重大风险。

现代有效的安全保护基于零信任原则，因此是时候从这个视角重新审视数据备份和恢复系统了。本白皮书提出了“零信任数据弹性”的新概念，从而实现了这一目标。通过采用这种方法，企业将有一条清晰而具体的途径来获得更强大的防御、更高效的运营和更快的恢复。

[1] CISA ZTMM 文件指出：“虽然 ZTMM 涵盖了对联邦企业至关重要的网络安全的许多方面，但它并未涉及网络安全的其他方面，例如 …… 恢复”。

方法

信息安全的经典基本要素 — CIA 三要素：保密性、完整性和可用性 — 都适用于数据备份和恢复。企业需要避免数据泄露（保密性），阻止勒索软件加密数据(完整性)，并确保系统既能抵御攻击，又能在攻击后快速恢复（可用性）。

核心零信任原则当然与此领域相关，应应用于用户和企业 IT 系统访问以及数据备份和恢复系统。这些原则包括消除隐式信任和非分段式网络，通过策略执行点 (PEP) 以动态和上下文策略控制所有访问，要求对所有主体进行适当的强认证，假定存在漏洞，并确保和验证系统和数据的完整性。在本白皮书中，我们将看到这些原则是如何贯穿到零信任数据弹性架构的一系列新要求中的。

零信任成熟度的实际标准框架是图 1 中描述的 CISA 零信任成熟度模型[2]，它定义了五个核心支柱：身份、设备、网络、应用程序和工作负载以及数据。它还定义了三个跨领域功能：可见性与分析、自动化与协调以及治理。

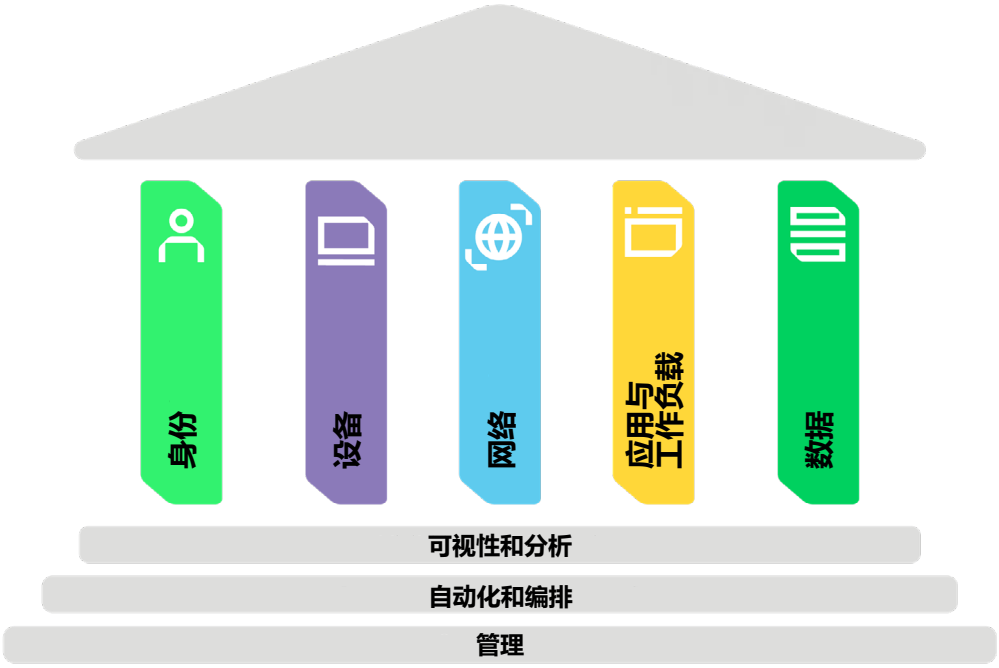


图 1：CISA 零信任成熟度模型

[2] https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model

在数据支柱中，CISA 模型确定了五项详细功能，以及每个成熟度级别的预期能力和属性。

但是，在这些功能中，数据备份完整性和恢复的主题很少，CISA 向读者介绍了与零信任无关的 2020 年 NIST 文档。总之，CISA 零信任模型对数据备份和恢复系统的要求和成熟度级别只字未提。因为这个领域对于企业机密性、完整性和可用性非常重要，所以我们认为这一差距需要得到解决。

为此，我们引入了零信任数据弹性的概念，其中包括零信任成熟度模型的原则、参考架构和一组新的功能。综合来看，这些都是对零信任的扩展和加强，并将带来更强的企业安全立场。

这些功能是：

- 数据清单管理
- 数据分类
- 数据可用性
- 数据访问
- 数据加密

零信任数据弹性：原则

零信任数据弹性（ZTDR）的核心原则包括：

最小权限访问 **不可变性** **系统弹性** **主动验证** **操作简易性**

让我们依次讨论其中的每一个。

最小权限访问

这一原则是零信任的核心，也是任何零信任架构的必要组成部分。但是，值得研究一下它对 ZTDR 细节的适用性，因为它适用于多个级别。从网络角度来看，备份管理系统本身必须在网络上隔离，以确保任何未经身份验证或未经授权的用户或设备都无法访问它。同样，备份存储系统也必须隔离。这可以防止恶意行为者通过网络侦察或利用漏洞发现任一系统。

对备份系统的合法授权访问只能通过零信任政策执行点 (PEP)，并进行适当的强身份验证和设备状态检查。零信任 PEP 还必须通过适当的身份验证和某种级别的设备或系统验证来控制对源数据（即正在备份的数据）的访问，以确保备份管理系统读取生产数据，而不是恶意系统或进程。

从备份管理系统到备份存储的访问也必须由 PEP 控制，并通过适当的强身份验证与网络其他部分隔离。请注意，我们将在下面的架构图中再次讨论这一要求，因为它非常重要 — 备份存储系统必须与备份管理系统隔离。

不可变性

近年来，随着勒索软件的流行和复杂程度不断提高，不可变备份数据的概念和要求得到了广泛采用。不可变备份的定义是，利用存储机制备份的数据一旦写入就不能更改。前提是，即使恶意攻击者存在于网络上并能够控制备份系统并访问备份存储，他们也无法删除或修改（加密）备份数据。有些不可更改性来自于存储介质的物理特性，如“一次写入多次读取”的光盘，而较新的技术则使用在硬件、固件或软件层具有不可更改性的介质。最近，主要云服务提供商纷纷添加不可变存储功能，以满足企业合规性和归档要求。

注意

对不可变性的要求不仅限于存储的数据，还必须包括数据保留期。有些不可变数据可以配置为无限期存储，而其他数据则可能有规定的保留期，如一年或五年。超过保留期的数据会被删除，因此数据存储系统也必须使数据的保留期不可变。这消除了恶意缩短保留期限的问题。

系统弹性

我们对系统弹性的看法相当宽泛，认为它不仅适用于备份基础架构本身，还适用于与数据备份和恢复相关的工具、技术和流程的整个生态系统。具体来说，备份基础架构必须能够抵御故障和攻击，如组件或网络不可用，或网络时间服务器 (NTP) 被操纵以恶意过期备份数据。此外，用户还必须能够轻松配置分布式和异构备份数据存储的使用，例如跨地理位置或跨基础架构类型进行配置。通过将备份数据与备份管理系统分离，还可提高弹性，这样，备份系统受到损害时，数据存储也不会受到损害。实际上，您需要一款备份管理系统，在发生攻击或故障时，可以快速重组，同时不会影响您访问和还原备份数据的能力。

系统还需要能够应对企业环境中的预期和意外变化。预期的变化包括计划内添加或删除基础架构组件，包括采用混合或基于云的应用程序和数据。也就是说，备份系统必须能够高效地捕获和存储企业数据，无论其源位置或技术如何。意外变化通常发生在事件响应或灾难恢复 (DR) 期间，最常见的分类是支持恢复到不同的环境。当组织恢复数据时，恢复环境完全有可能在不同的位置或基础架构类型中运行。例如，内部数据中心被水淹后，可能需要恢复到基于云的环境中，并在该环境中长时间持续运行。因此，备份系统必须既支持恢复到这种不同环境中，也支持从这种生产环境中进行新备份。

备份数据存储系统本身除了提供不可变的数据存储外，还应易于强化。这可能会采取预强化设备或可由管理员配置的系统的形式，并提供明确的强化建议，这将更适合成熟的企业。

主动验证

要确保系统正常运行，就必须对系统进行监控，并对所有功能方面和流程进行验证。这有两个方面。首先，应监控备份系统的网络、性能和安全性。也就是说，这个系统应该像对待任何其他高价值生产系统一样对待。

其次，也是最重要的一点，备份数据的有效性以及恢复流程的可靠性和有效性必须得到定期验证。顾名思义，备份数据的恢复会在意想不到的时候发生，而且很可能是在高压力环境下。重要的是，企业要有一个理解透彻、记录完备、演练有序的流程。还需要有多个人能够执行此操作，以解决员工休假、不可用和人员流动的问题。

请记住，虽然这需要投入时间和精力，但这表明了运营的成熟度，也是灾难发生时的“保险政策”。还要注意的是，“灾难”不一定是指字面意义上的灾难，也不一定是指数据中心洪水泛滥等重大事件。例如，我们合作的一家企业由于编程错误导致了自动化工作流程失控，导致其财务管理系统中的大量生产数据被删除。这并不是一场字面意义上的灾难，而是通过使用他们的（经过验证的）数据恢复流程，避免了一场形象化的灾难。

此外，备份管理系统还应能够直接或间接地跨恶意软件感染时间线组织备份。也就是说，它应该能够检测（或获知）恶意软件感染，并根据捕获备份的时间将备份分为干净备份、可疑备份或受损备份。

注意

数据验证和恢复流程还必须尊重任何数据隐私和数据驻留要求。这可能会增加复杂性和风险，因此必须深思熟虑，同时了解数据内容以及组织的法律和合规义务。

操作简易性

我们的最后一项原则是操作简易性，我们将其定义为：系统既能让您的企业放心地操作，又能提供足够的功能、可扩展性和先进性，以完全满足企业的需求。也就是说，一个适合贵组织的系统。

这一点很重要 — 我们已经看到企业难以利用和运行对于组织规模、团队、技能和需求而言过于复杂的系统。这将导致效益有限、挫败感以及无法实现安全成熟度或业务价值。备份厂商需要注意的一组属性是他们在编排和自动化方面的相对优势。平台功能强大的供应商将更快、更容易投入使用。

在本节的最后，我们将这些原则一一融入本文后面讨论的新成熟度模型扩展中，这些原则也将在我们接下来讨论的参考架构中得到体现。

零信任数据弹性：参考架构

考虑到网络、应用和数据基础架构的巨大差异等因素，不同企业的数据备份架构必然会有所不同。即便如此，由于采用了共同的零信任原则，任何零信任数据弹性架构都必须具备一些共同的架构元素。

我们的参考架构如图 2 所示，说明了此类系统的关键要求。请注意，这是从备份管理系统的角度描述环境。用户和系统对生产系统的常规、日常访问也受零信任 PEP 的控制，但为清晰起见，图中省略了这一点。

图 2：零信任数据弹性：参考架构

首先，请注意任何零信任架构的核心部分 — 集中式策略决策点 (PDP)，它将身份验证委托给企业 Identity and Access Management (IAM) 系统。PDP 依靠其策略存储来对经过身份验证的身份（包括人类和非人员（系统）身份）做出访问决策。在此架构中，PDP 负责制定备份管理系统的访问决策。这些决策通过控制平面（如虚线所示）与策略执行点 (PEP) 进行通信，策略执行点在逻辑上位于备份管理系统与要备份的数据源和目标备份位置之间。

该体系结构还包括一个建议的备份数据结构。除了数据不变性要求外，企业还应在主位置至少保留一份副本，该位置应与预定的恢复站点有低延迟网络连接。这有助于快速创建备份快照，提高恢复点的频率和恢复速度。当然，主位置通常与生产系统位于同一地点，因此我们的参考架构也说明了在辅助位置至少保留 2 份数据副本的目标[3]。这些数据中心必须在地理位置上与主要地点隔离，以实现抵御区域性灾难的弹性。可能的代价是网络连接速度较慢，这可能导致恢复点频率降低和恢复时间延长。

注意

备份管理系统特意与其存储层分开。这有助于备份系统将备份数据无缝分布在多个不可变且地理位置分散的存储库中。它还支持企业选择性能、价格和操作简单性最佳组合的备份存储库，以满足其独特要求。它还通过 PEP 控制通信，提供了额外的安全层。

[3] 关于不同位置的备份数量，有各种不同的说法，通常采用 3-2-1 或 3-2-1-1-0 等记忆法。

零信任数据弹性：扩展成熟度模型

虽然我们提出的零信任数据弹性原则和参考架构普遍适用，但它们无法立即完全应用于大多数企业。对于零信任的大多数方面，必须对其进行规划并逐步采用。标准的建模和交流方式是通过成熟度模型。正如我们在导言中提到的，我们遵循事实上的标准 CISA 零信任成熟度模型框架，并用四个新功能对其进行扩展，这四个新功能包含了我们的原则和要求。

这些新功能包括：

访问企业数据和系统

访问备份存储和数据

系统弹性

系统监控和验证

ZTDR 对成熟度模型的这些扩展如图 3 至图 6 所示，其中显示了四项新功能在标准成熟度层级中的推进方式：传统、初始、高级和优化。

对于每个功能，我们确定了每个成熟度级别的预期属性。因此，该模型描述了组织为了提高每个职能的成熟度而需要进行的改进和更改。接下来，我们将依次查看每个功能在成熟度层级中的进展情况。

访问企业数据和系统

该功能被定义为备份管理系统（BMS）访问其负责备份的源数据的方式和机制。

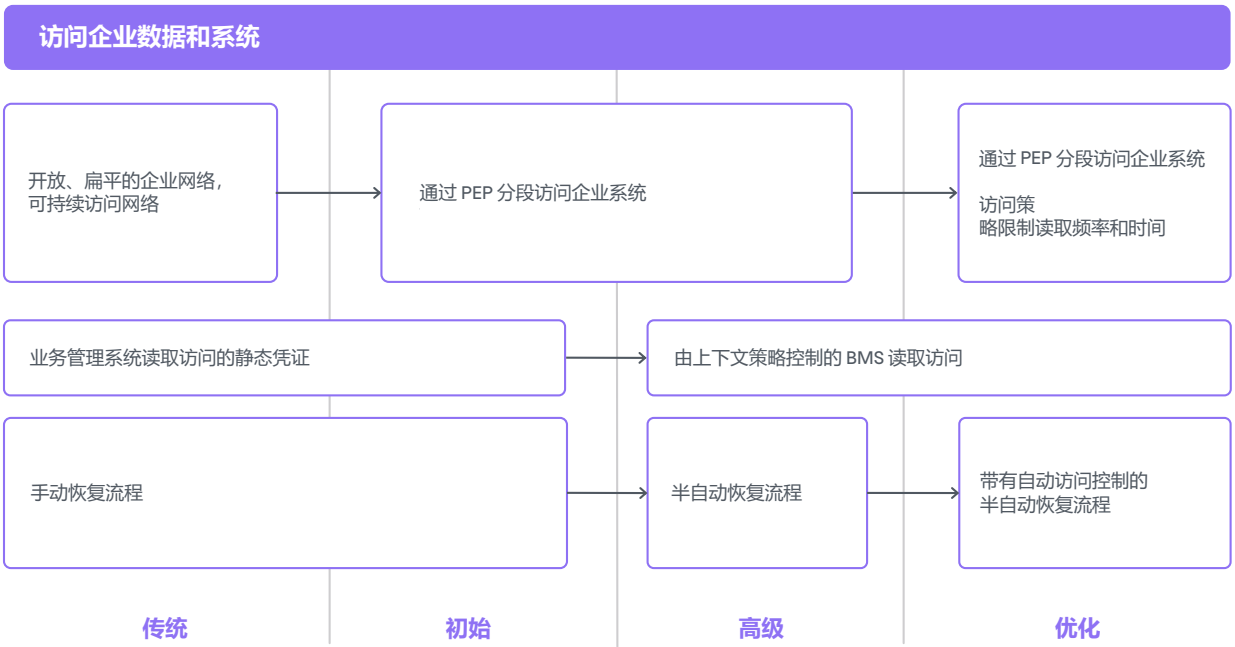


图 3 — 访问企业数据和系统：成熟度模型

在**传统**成熟度级别，企业拥有一个扁平、开放的网络，备份管理系统可以持续、无障碍地通过网络访问源系统。BMS 使用静态凭据(如 API 密钥、存储的用户名 / 密码或证书）来验证和读取源数据。当企业使用 BMS 恢复系统时，他们依赖于手动流程。

为了提升到**初始级别**，企业必须开始执行更好的网络分段，并通过零信任策略执行点限制 BMS 对企业系统的访问，引入最小特权原则。

当企业达到**高级**级别时，他们将为 BMS 访问企业数据和系统引入上下文访问策略，从而更好地利用动态零信任策略执行功能。他们还将开始使用自动恢复流程，并通过一些手动步骤启动和验证流程。

在**优化**级别，企业将加强对访问策略的使用，将 BMS 的访问限制在允许的时间段或活动恢复事件范围内。这进一步强化了最小特权原则。

访问备份存储和数据

该功能被定义为备份管理系统对备份存储和存储数据进行写入和读取访问的手段和机制。

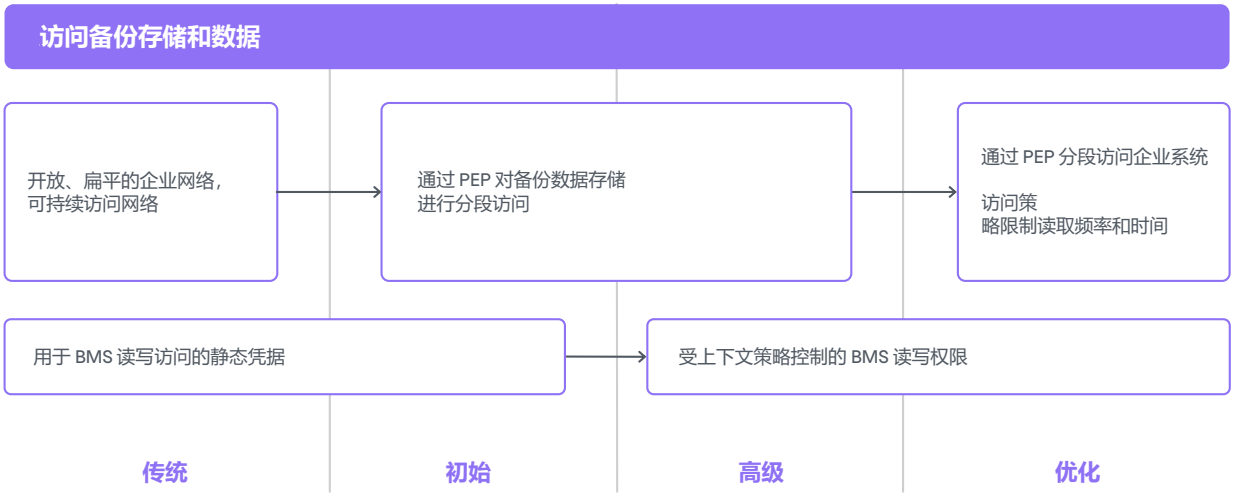


图 4— 访问备份存储和数据：成熟度模型

在**传统**成熟度级别，企业拥有扁平、开放的网络，备份管理系统可持续、无障碍地通过网络访问备份存储系统和存储在其中的备份数据。备份管理系统使用静态凭证（如 API 密钥、存储的用户名 / 密码或证书）来验证和写入存储系统，并读取存储的数据。

为了提升到**初始级别**，企业必须开始执行更好的网络分段，并通过零信任策略执行点限制 BMS 对备份存储和存储数据的访问，执行最小权限原则。

当企业达到**高级**级别时，他们将为 BMS 访问备份存储系统和存储数据引入上下文访问策略。这可以更好地利用企业内的动态策略实施功能。

在**优化**级别，企业将加强对访问策略的使用，将 BMS 对存储的访问限制在允许的时间段内，或在活动恢复事件期间。这进一步强化了最小特权原则。

系统弹性

此功能定义为备份系统在抵抗系统故障、组件故障或恶意活动方面的特征。

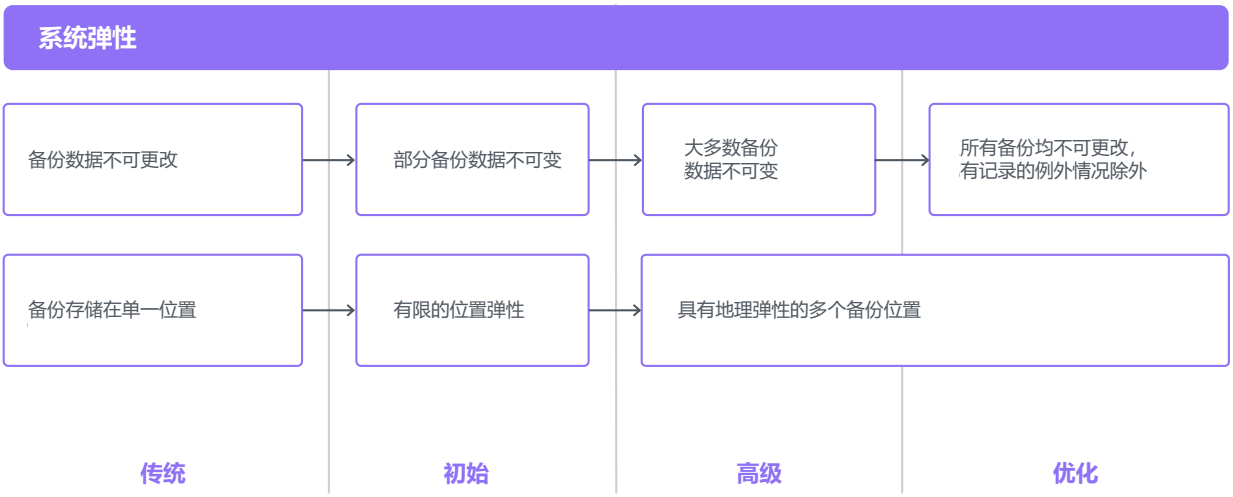


图 5— 系统弹性：成熟度模型

在**传统**成熟度级别，企业使用可变存储来存储备份数据，从而使其完整性和可用性面临风险。此外，它们通常只将备份存储在一个位置，因此在发生区域性灾难时，组织会遭受完全损失。

随着客户升级到**初始**级别，他们必须开始将不可变存储用于某些数据备份，并为这些备份引入一些有限的位置弹性。

在**高级**级别，组织将主要使用不可变备份存储，最好根据数据敏感性和重要性进行优先级排序。他们还将引入并实施跨不同地理位置的多个备份存储位置的使用。

当企业处于**优化**级别时，他们将转向充分利用不可变备份存储，任何例外情况都将记录并获得批准。默认情况下，新的数据源和应用程序将使用不可变备份。该级别可为组织提供最大限度的恢复能力，以抵御地区性灾难和恶意行为者。

系统监控和验证

这一功能是一种工具和流程，企业通过这些工具和流程确保其备份管理系统和备份存储正常运行，以及企业能够在需要时执行恢复流程。

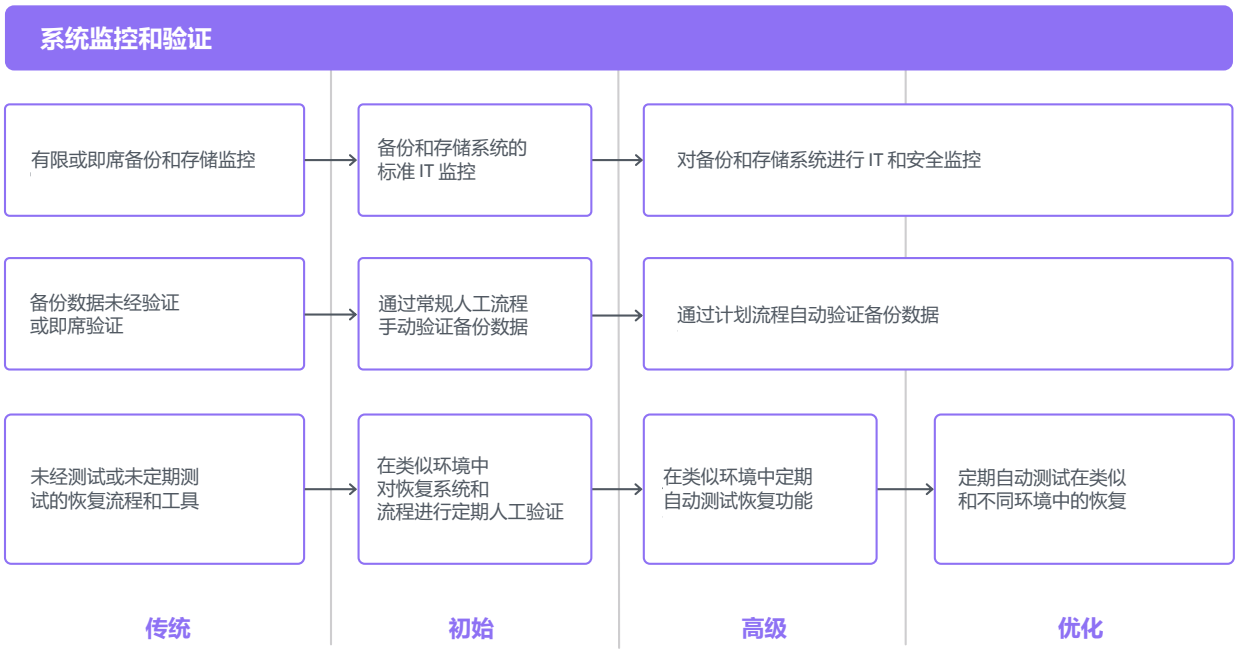


图 6— 系统监控和验证：成熟度模型

在**传统**成熟度级别，企业将仅对备份和存储基础架构实施基础监控，这通常反映出整体 IT 和运营成熟度较低。企业可能不会对备份数据进行验证，或仅执行定期（即手动和不频繁）检查。此外，企业也不会定期测试恢复工具和流程，使其得到很好的理解、记录和重复。

在**初始**级，企业将对备份和存储系统采用标准化的 IT 和操作监控。他们还将通过手动流程对备份数据进行定期验证。他们还将对恢复流程实施定期（手动）验证，以确保机构了解并熟悉这些流程。

在**高级**级别，企业将为备份和存储系统部署 IT 和安全监控工具和流程。而且，它们将通过报告并上报任何异常结果的预定检查自动验证备份数据。这将包括在与生产类似的环境中自动测试恢复工具和流程。

在**优化**级别，企业将提高恢复测试的复杂性，以测试在不同环境中的恢复。

成熟度模型总结

从整体上看，这些新功能定义了一套能力和一套预期能力，并在四个零信任成熟度级别之间进行了映射。对于希望将数据备份和恢复系统纳入零信任计划的企业，它们提供了实用的路线图和指南。

结论

零信任显然是处理信息安全的更好方法，作为安全领导者，我们有义务将这一策略引入我们的企业。当前的零信任架构和成熟度模型是坚实的起点，但还不完整。我们认为，零信任成熟度是一个全新的概念，特别是其中没有数据备份和恢复的要求和方法。

传统上，企业将备份和恢复视为 IT 范畴，但随着勒索软件的泛滥和业务几乎完全数字化，安全领导者需要扩大业务范围，将备份和恢复纳入范畴。

在本白皮书中，我们介绍了零信任数据弹性的概念，包括一组核心原则、一个参考架构以及对零信任成熟度模型的扩展。我们相信，通过采用这种“零信任数据弹性”方法，企业将有一个清晰而具体的途径来实现更强大的防御、更高效的运营和更快的恢复。企业数据非常重要，我们不能不应用安全最佳实践，而零信任是最有效的方法。

关于 Veeam Software

Veeam® 是数据弹性领域首屈一指的全球市场领导者，其坚信每家企业在中断后都应该能够绝地反弹，并且能够在需要时随时随地自信地控制其所有数据。Veeam 称之为极致弹性，我们致力于通过创新方法来帮助我们的客户实现这一目标。Veeam 解决方案专门通过提供数据备份、数据恢复、数据自由、数据安全和数据智能功能增强数据弹性。借助 Veeam，IT 和安全领导者可以高枕无忧，因为他们知道其应用程序和数据受到了保护，并且始终在云、虚拟、物理、SaaS 和 Kubernetes 环境中可用。Veeam 总部位于西雅图，在 30 多个国家和地区设有办事处，保护着全球超过 550,000 家客户，包括 74% 的全球 2000 强公司，他们信赖 Veeam 保证其业务正常运行。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。

→ 了解更多信息：veeam.com/cn