CISCO
SECURE

思科零信任成熟度指南

如何快速致胜

cisco SECURE

目录

I. 执行摘要

“零信任” 已然从一个时髦术语变成了国际准则。美国、英国和澳大利亚等国政府都发布了相关要求，与 “绝不妄加信任，始终坚持验证” 的立场保持一致。

采用零信任方法的业务主管积极为其组织构筑安全弹性，取得了切实进展。事实上，一部分思科客户因数据泄露引发的风险和损失降低了近一半，而其余的客户则通过推行混合办公和优化安全团队的绩效实现了 191% 的投资回报率 (ROI)。

通过提高效率，零信任可以加快安全运营中心 (SOC) 团队的响应速度。我们已经能够让客户的 SOC 效率提高 90%。显然，零信任可以提供价值。

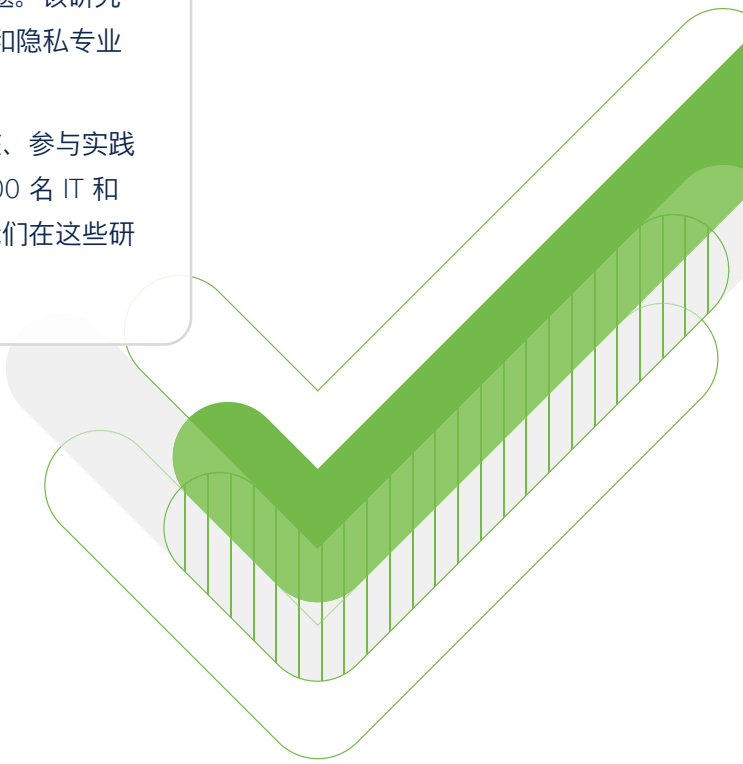
尽管如此，业界对于如何实现零信任原则，以获得商业回报，仍存困惑。然而，思科等许多企业在采用零信任安全方面已经取得显著进展，对此还有切实的回报作为证明。

那么，这些企业有何不同之处？他们成功的秘诀是什么？

关于本指南中使用的数据

我们使用了《思科安全成果研究》（第二卷）的调查结果，这是一份经过独立验证的报告，旨在回答 “为什么” 某些安全实践如此成功的问题。该研究对来自 27 个国家/地区、各行各业的 5,000 多名在职 IT、安全和隐私专业人士进行了访谈，以探索有助于提升安全能力和成果的措施。

思科还定期组织零信任研讨会，帮助参与者了解零信任采用之旅、参与实践活动、执行差距分析并制定行动计划。到目前为止，已有约 3000 名 IT 和安全主管以及从业人员报名参加了这些研讨会。本指南列出了我们在这些研讨会中收到的调查回复。



我们研究了编制《思科安全成果研究》（第二卷）的团队收集和分析的现场数据，以及思科去年组织的众多零信任研讨会参与者的反馈。

图 1：受访者在采用零信任方面取得的进展

结果可为寻求实施零信任的团队提供以下洞察：

- **无论组织规模如何，也无论 IT 基础设施的复杂程度如何，都可以在实现零信任方面取得进展。**纵观各种从简单到复杂的 IT 环境，我们发现，无论组织规模如何，都可以在实现零信任安全方面取得显著进展。
- 零信任实施成熟的组织实现**业务弹性的可能性** (63.6%) 是只有限实施零信任组织的两倍以上。
- 零信任实施成熟的组织**在**以下五个安全实践方面表现出色的可能性是其他组织的**两倍**：
  - 准确检测威胁
  - 及时响应事件
  - 积极更新技术
  - 充分集成各项技术
  - 迅速从灾难中恢复
- 零信任实施成熟的组织出色地实现预期成果的可能性是其他组织的 **2 倍**，其中此类成果包括**增强高管信心** (47%)、**获得同事支持** (45%)、**紧跟业务发展步伐** (46%) 以及**打造安全文化**。
- 拥有**现代 IT 基础设施**的组织零信任实施成熟的可能性是其他组织的**两倍以上**。
- **通过集成提升零信任成熟度**。即使在选择集成的组织中，也有 **51%** 的零信任实施成熟的组织优先考虑**从首选供应商处采购集成技术**这一平台方法，而考虑采用开箱即用集成方法的组织仅占 **28.8%**。
- 零信任实施成熟的组织会充分利用**自动化** (64.4%)，来改善零信任安全模式可以执行的操作。

本零信任成熟度指南旨在帮助您确定您目前在零信任方面所处的状态、如何快速致胜、获得动力并继续在零信任安全方面取得进展。

II. 简介

零信任将成为常态，但为什么实现零信任会这么具有挑战性？团队如何才能获得动力，来完成这项艰巨的任务？

我们认为，组织可以向零信任实施更成熟的团队学习。他们成功的秘诀是什么？他们的哪些做法值得全球其他组织借鉴？

具体包括:

1. 成功的团队实现了哪些安全成果？成功率如何？
2. 在选择零信任供应商和提供商时，他们会优先考虑什么因素？
3. 他们在部署零信任时，采用了哪些集成和自动化策略？
4. 他们遵循哪些零信任标准？
5. 他们的安全流程自动化达到了什么水平？

III. 零信任是什么？

零信任是一种安全**策略方法**，其核心理念是在组织环境中**杜绝一切隐式信任**。

这种信任既不是非此即彼的，也不是永久性的。我们再也不能想当然地认为：内部实体值得信任，直接管理便能降低安全风险，或者只需检查一次，即可一劳永逸。

零信任安全模式要求在每次**出现访问尝试时都应进行信任验证**，无论访问尝试来自哪里都不例外。

根据零信任方法，对于每种公司资源的每个连接请求，都应部署“绝不妄加信任，始终坚持验证，并应用最低权限访问”的策略。在授予对应用、设备和网络的访问权限之前，始终验证信任，确保只有那些应该有权访问信息的人才能进行访问。

策略决策点 (PDP) 和策略实施点 (PEP) 负责决定什么人拥有访问权限，并执行此决定。事实上，可以说 PDP/PEP 是其中最关键的架构功能。这些组件实施零信任原则，并根据在连接期间观察到的情况扩展或撤销信任边界。

零信任:

- 不是一种产品或技术，而是一个安全框架
- 不是可以“买”或“卖”的东西，而是一种在框架内定位解决方案的机会
- 不是一个一次性项目，而是为了提高安全性所需要持续执行的工作

一个简单的事实是，业务发展太快，安全措施已无法跟上其步伐。尽管实施了安全创新，但风险的影响从未如此之大。很多时候，一次网络安全事件就可能威胁到组织未来的生死存亡。

在思科，我们认为零信任安全策略的优势应该是，以一种能够阻止攻击者而不妨碍用户的方式来保护访问。

A. 为什么现在是实施零信任的绝佳时机？

零信任并不是一个新概念。然而，如今零信任正在获得日益广泛的采用，这反映出一个快速变化的现实：曾经用于保护对企业数据的访问的安全边界如今已不复存在。现在，企业与其供应商、合作伙伴和客户之间形成了集成式生态系统。这些连接扩大了企业受攻击面，增加了风险和复杂性，并加大了从攻击中恢复的难度。

鉴于网络攻击对企业盈利的影响，业务主管纷纷准备遵循零信任访问原则，以全新方式实施端到端安全，但前提是这些变革不会影响工作效率或企业运营。

风险如此之高，各种严重影响具有如此巨大的潜在破坏性，导致大刀阔斧的变革势在必行。因此，零信任安全原则得到了广泛采纳。

无论 IT 基础设施的复杂程度如何，都可以在实现零信任方面取得进展。无论 IT 环境复杂程度如何，组织都可以在实现零信任方面取得进展，同时改善各项成果。

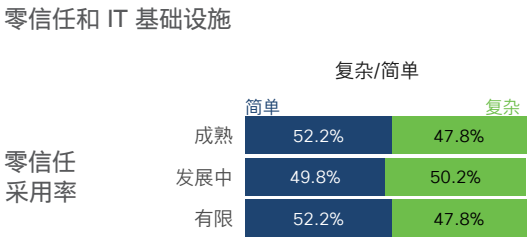


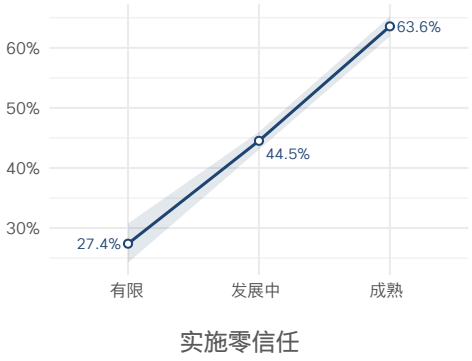
图 2：具有简单基础设施和复杂基础设施的组织的零信任采用率

零信任可以提高业务弹性。虽然零信任似乎又是一个营销流行词，但事实是，改用零信任架构可以保护整个组织、提升业务绩效并加快威胁响应速度。

我们发现，零信任实施成熟的组织实现业务弹性的可能性是有限实施零信任的组织的两倍以上。

我们使用与弹性特别相关的 12 项安全成果中的以下 4 项创建了“弹性得分”：

- 紧跟业务发展步伐 (安全应该起到推进作用，而不是阻碍作用)
- 避免重大事故 (以及随之而来的业务影响)
- 保持业务连续性 (即使在灾难来袭时也能正常运行)
- 留住人才 (如果留不下顶尖员工，就无法保持领先优势)



弹性得分越高，意味着这些成果的成功率越高。

挑战在于，组织担心影响工作效率或危及业务灵活性和运营弹性，不知道如何 “实施零信任” 或从哪里开始 “实施零信任”。

然而，关键是要从某个方面开始，专注于把某些事情做好。我们发现，零信任实施成熟度的高低与《思科安全成果研究》（第二卷）中提到的五个安全实践之间存在明显关联，这些实践被称为安全计划成功的 “五强” 驱动因素：

- 准确检测威胁
- 积极更新技术
- 迅速从灾难中恢复
- 及时响应事件
- 充分集成各项技术

零信任实施成熟的组织在这五个安全实践方面表现出色的可能性是其他组织的两倍。

拥有良好实践的受访者百分比

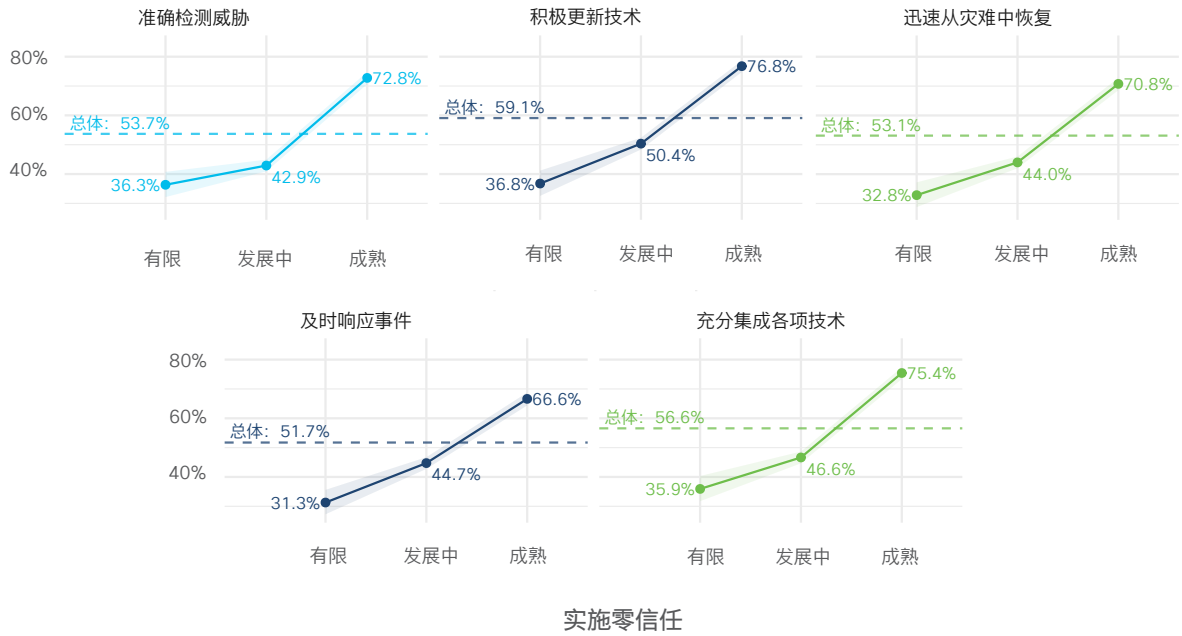


图 3：零信任采用程度和安全实践

温馨提示：零信任目前已占据 200 亿美元的市场份额（并且还在不断攀升）[1]，因此您要选择的合作伙伴必须能够满足您的独特需求，能够整合零信任的各个支柱，并且自己就用得很好。

[1]Grandview Research 研究报告显示，2020 年全球零信任安全市场规模达到 198 亿美元，预计 2021 年到 2028 年的复合年均增长率 (CAGR) 将达到 15.2%。https://www.grandviewresearch.com/industry-analysis/zero-trust-security-market-report

IV. 成功的秘诀

A. 从文化入手

成功实施零信任的主要因素包括：能够获得高层的认可，赢得同事的支持，以及建立安全文化。如果安全团队缺乏认可和预算，安全计划违背企业文化，安全团队就会举步维艰。

没有什么比文化抵制更能阻止一项计划了。

从我们自己的思科案例研究中可以看出，这些因素都存在于自上而下的领导层和整个组织中。《安全成果研究》也反映了这一点，零信任实施成熟的组织报告在**增强高管信心 (47%)** 和**获得同事支持** (45%) 方面表现更为出色。在**紧跟业务发展步伐** (46%) 和**打造安全文化** (48%) 方面，我们也发现了相应趋势。事实上，**零信任实施成熟的组织在这些方面表现出色的可能性要比其他组织高出 2 倍。**

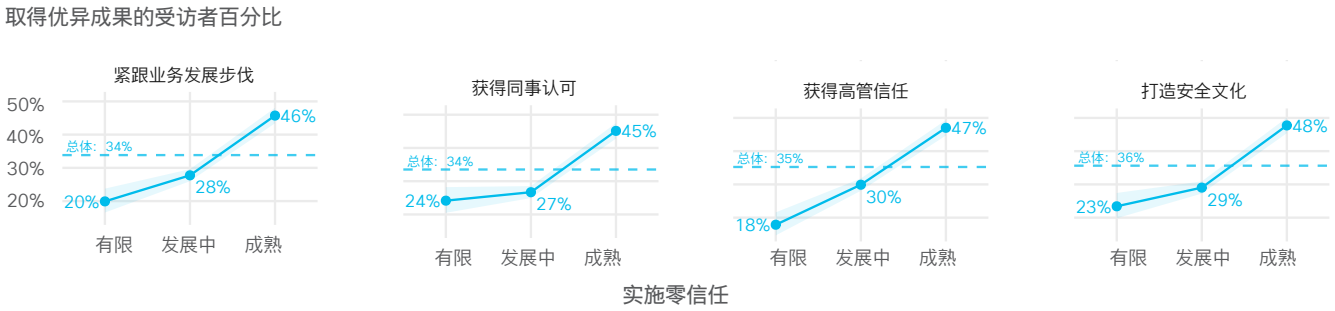


图 3：预期成果背景下的零信任采用程度

关系推动组织变革。在拿起白板笔草拟计划之前，以及打开控制台并配置策略之前，首先应加强安全团队与高管之间的关系。这包括 IT、网络、架构、项目管理和审计领域的同事。这些关系使我们的零信任计划能够更快地成熟，从而实现更大的成功，这是转型变革的关键因素。

变革始于高层。当我们得到充分的支持时，前进道路就会更加清晰。当首席执行官呼吁实施零信任计划时，或者当我们的客户要求将零信任作为其供应链管理的一部分时，您就需要将零信任计划与业务联系起来。如果上述情况正在发生，请充分抓住机会，并利用这种势头推动计划向前发展。

建立信任文化。在讨论技术之前，以及在确定零信任业务项目之前，安全主管首先需要努力建立同事的信任和信心，并获得高管的支持。以符合组织文化的方式构建对话框架。

寻求加强关系。在构建和实施零信任时，请确定可以加强这些关系的方法。制定工作流程、部署策略引擎、围绕零信任对组织的意义展开对话、重点发展业务并防御威胁：所有这些措施都可以加强关系。

案例研究和数据明确显示，这些都是成功实施零信任的关键因素。

B. 开发令人信服的业务案例

在思科零信任研讨会和更广泛的市场中，我们都看到了零信任计划的明显趋势。

早期的零信任项目都是试点项目。安全主管听说了零信任这一说法，就想尝试看看哪些方法行之有效，哪些方法无效。这些早期的试点项目让人们了解了零信任在组织中的可能形态。从 2018 年到 2020 年，许多组织因高管要求、客户要求或现代化需求，实施了许多零信任计划。

转向业务成果。最近，一个明显的转变是，从仅仅为了实现零信任而确定项目，转向为了在应用零信任原则的同时满足业务需求而确定项目。例如，远程优先的员工、数字化优先的客户群、数字化转型、云迁移和 IT 现代化。成功的零信任计划会寻找机会来改进组织，同时提高安全性。

优先考虑用户体验。现在，在商业案例中，零信任的主要焦点之一是用户体验。这是零信任的信任要素。成熟的计划可以改善用户体验，使得员工在执行常规日常业务活动时，随时随地获得安全保护。仅当存在实际风险时，例如当连接不受信任或可能存在攻击行为时，安全控制功能才应中断相应连接。

提高安全效率。商业案例的另一个考虑因素是可管理性。**安全成果研究发现，零信任实施成熟的组织获得了运营成本效益 (47%)，同时最大限度地减少了计划外工作 (43%)。**思科零信任研讨会的参与者普遍将工具整合列为其目标，仅次于提高可视性。成功的组织可以减少安全维护工作负载，同时增强保护组织的能力。

简而言之，零信任商业案例的驱动因素是防范攻击者，而不妨碍用户。

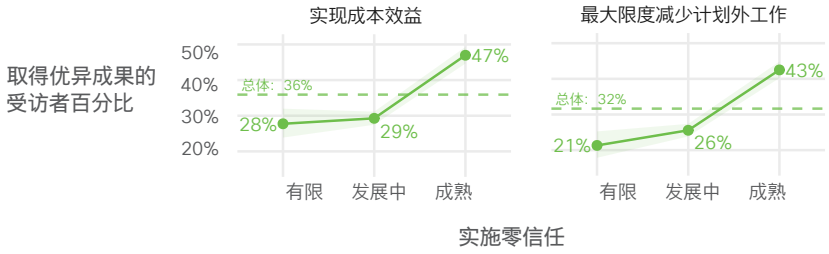


图 6：零信任安全的成本效益

缩小受攻击面。这是零信任中 “零” 的意义所在：减少过度信任和隐式信任，从而降低安全风险。大多数组织会想到减少网络钓鱼和勒索软件等威胁，但更广泛而言，他们可以使用零信任框架来缩小受攻击面。

充分利用审核。由于合规性要求，组织对零信任的需求不断增加，尤其是在美国联邦部门。我们预计，随着组织采用零信任并将其作为供应链风险管理的一部分，合规性因素只会有增无减。

基本结论：商业案例必须首先满足业务需求，然后通过满足这种需求，应用零信任原则来提高安全性。

C. 保护 IT 堆栈

零信任是指创建动态边界：这种边界存在的时间较短，有严格的范围限制，通过策略来实施，并充分利用信任信号和遥测信息，是主体（通常是使用设备的用户）与资源（通常是用户正在访问的应用）之间的信任边界。

IT 堆栈需要支持在每个会话和每个连接的基础上建立这些信任边界。

成熟的零信任实施更可能采用现代化基础设施而不是过时的基础设施（68% 比 31.3%），更可能采用云优先部署而不是本地部署（46% 比 23.6%）。这些现代化云优先堆栈有助于更充分地满足为每个会话和每个连接建立信任边界的策略需求。

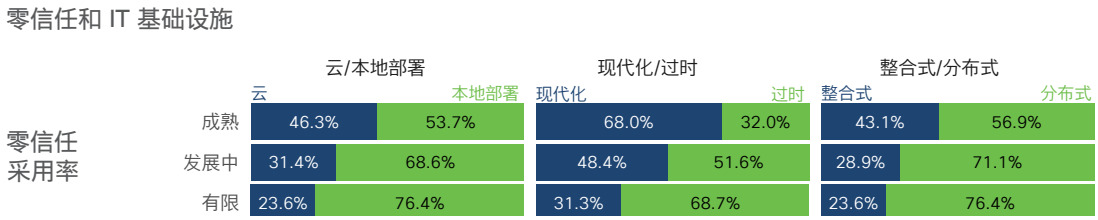


图 7：IT 基础设施属性背景下的零信任采用率

纵览全局。零信任的控制点包括人员、设备、网络、应用工作负载和数据。这些控制点彼此分散，可能会形成孤岛，需要重复执行工作和协调。因此，**毫无疑问，成熟的实施方法倾向于采用整合式基础设施而非分布式基础设施（43.1% 比 23.6%）。**这就是机制经济原则在数据中的体现。

推送补丁。使环境保持最新状态是实现成功的一个因素。零信任在不断发展，使得架构模式、标准、身份验证和授权协议以及共享信任信号协议也在不断发展。

零信任实施更成熟的组织更依赖供应商驱动的升级策略，而不是主动升级（45.8% 比 30.9%）。传统更新策略以多年为一个周期，通常会等待有计划的更新，让技术多年处于停滞状态；而 SaaS 应用可以自动更新，似乎可以为组织提供更大程度的灵活性，而且云端 SaaS 应用可以进行策略控制。

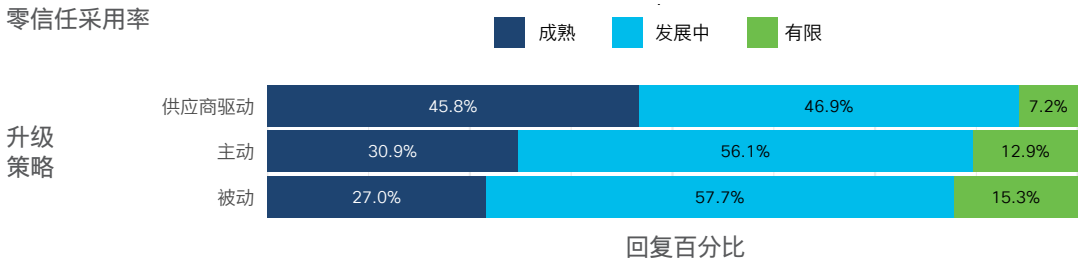


图 8：升级策略背景下的零信任采用程度

集中管理身份。在现代技术栈中采用联合身份的组织将更容易达到成熟状态。然而，正在部署现代技术栈的组织具有得天独厚的优势，可以在此过程的早期阶段应用零信任原则和架构模式。

不抛弃传统技术。零信任面临的一个持续挑战是将这些原则应用于传统环境和边缘案例。我们看到，在各种不同的安全控制措施中，领先安全技术往往针对的是领先 IT 技术，这可能会使许多环境被置之不顾。

基本结论：就像上云一样，向零信任迁移也需要采用一种混合使用传统安全模式和新型安全模式的方法。

D. 从用户、应用和设备着手

零信任是一项针对特定使用案例的安全计划。观察成功的组织，可以发现许多这样的使用案例。其中包括:

- 保护员工队伍
- 应用现代化
- 保护物联网 (IoT)、IT 和运营技术 (OT) 系统

...并结合情景来提供上述所有保护，以便所有系统都受到保护并通过策略引擎运行。

此外，还需要考虑其他几个符合零信任原则的补充安全计划。我们从以下基本运营领域入手:

- 身份和访问管理 – 谁是授权用户？我怎么知道？他们需要访问哪些资源 (例如应用) ？
- 资产管理 – 我的物联网、IT 和 OT 环境包含哪些设备？我如何知道这些设备是否已进行安全配置？

要找到这些问题的答案绝非易事。

例如，参加思科零信任研讨会的人员经常表示，**在身份管理计划方面遇到重大困难。74% 的与会者表示，他们的组织的身份策略未定义、不清楚或不太清楚。**当我们认为身份是新的边界时，缺乏身份控制就会出现问题。

零信任仍面临挑战的另一个领域是资产管理计划。**55% 的与会者表示，他们对设备没有可视性、可视性较低或只有部分可视性。**信任边界建立于使用设备的用户与其应用之间。如果我们缺乏可视性或良好的配置管理数据库，怎么才能实现零信任呢？

一个可能的答案是，不将身份和设备管理视为一种在固定时点的活动，而是将其视为一种随时、按需发生的活动。换言之，就是在人们进行身份验证时或者在设备访问资源时，执行身份和设备管理。

相比之下，一些与零信任相关并支持零信任的安全计划则取得了巨大成功。**成熟的零信任组织表示，他们的风险管理计划取得了更好的成果 (49%)**。他们保持通信和协作，通过策略确保零信任执行通过风险管理计划确定的正确风险评估和风险决策。

我们还发现，**零信任实施成熟的组织，其事件响应 (43%) 和业务连续性 (41%) 计划也取得了更好的成果。**

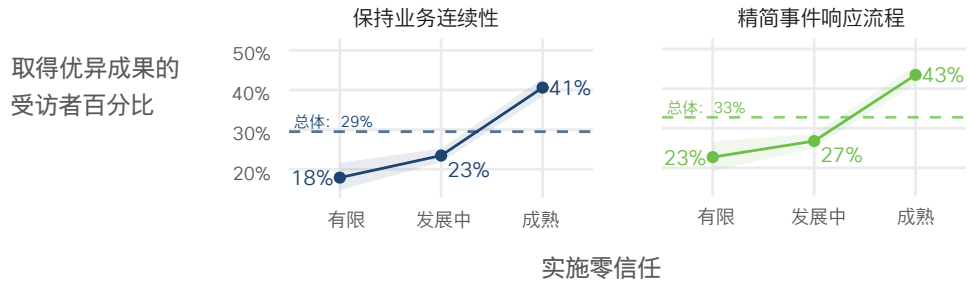


图 9：零信任采用程度与业务连续性和事件响应

新兴做法是，将零信任计划与其他正在进行的安全计划相结合，以取得更好的成果。安全团队正在摆脱传统的手动流程，无论是资产管理、身份管理还是检测和响应活动，都存在这种趋势。如果我们发现不符合策略的事物，且情景和条件表明我们不应该信任这些事物，我们必须自动采取行动。

基本结论：成功的零信任实施通过协作和技术集成，充分利用其他计划的优势。

E. 专注于零信任功能

在构建商业案例、制定计划并将其应用于现代技术栈时，零信任应该能带来多项功能。

树立远大目标：分析、集成和自动化。可视性、集成以及自动化和协调的工作流程是零信任功能，属于成熟度模型和参考架构的“最佳”范围。这些都是需要追寻并逐渐达到的里程碑。

成熟的组织专注于集成。数据反映了行业中持续存在的争论：是购买开箱即用的技术来集成到现有基础设施中更好 (28.8%)，还是从单一供应商处采购解决方案来建立零信任以便这些解决方案本身可以充分集成或成为更大平台的一部分更好 (51%)？**这两种方法都有组织表示取得了成功，这可能表明产品市场正在不断发展。**

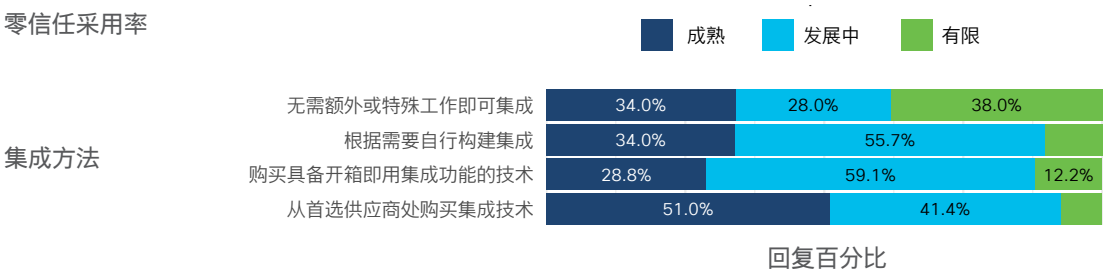


图 10：集成策略背景下的零信任采用率

一些共同信号有助于制定明智的策略。实现零信任成熟度的一种方法是与其他信任信号进行更大程度的集成，以**检测**威胁、**识别**漏洞、**保护**资产、**应对**事件并**快速恢复**运营。换言之，从策略实施的角度来看，我们在做出基于信任的决策时需要使用什么信号？我们扩展信任边界时，需要使用哪些信号？回答这些问题需要充分集成的技术，而成熟的组织报告的技术集成水平要高得多。

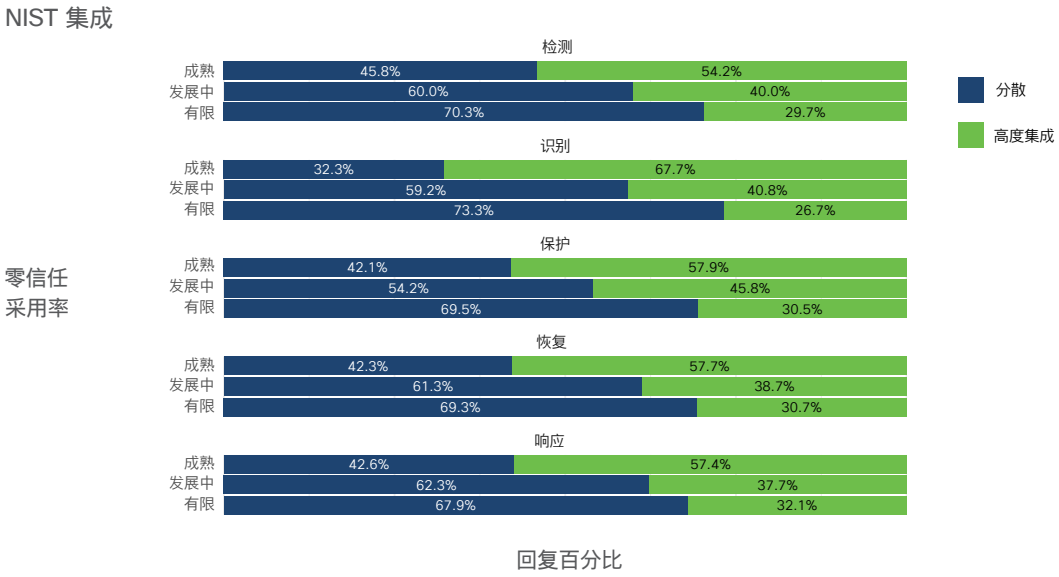
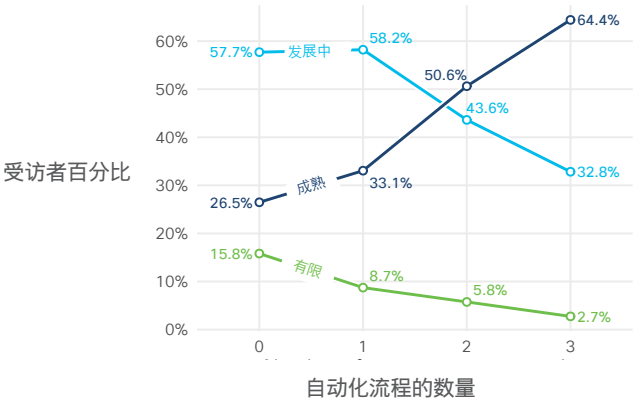


图 10： 集成策略背景下的零信任采用率

自动化和协调使得大规模实施零信任变得切实可行。集成改进了策略决策的制定，自动化和协调改善了零信任可以执行的操作。**零信任实施成熟的组织报告，在威胁监控、事件分析和事件响应方面的自动化程度最高 (64.4%)。**随着策略决策的制定，以及数据可用于对持续性威胁进行追溯检查或主动预防，这些集成日益普及。



自动化程度越高越好。自动化和协调可以应用于许多不同的项目，例如更改信任边界、更改权限级别、调整角色以及调整身份所处的情景，直到信任得到改善。

图 12： 零信任实施成熟的组织对自动化的利用

我们发现，零信任实施成熟的组织报告的自动化流程更多，这反映了全面应用协调和自动化这一总体趋势。

要点总结：对于零信任功能，首先应制定策略，这是基本要求。然后，确保获得对这些策略实施点的可视性。规划策略引擎与不断增长的信任信号之间的集成。最后，提高自动化和协调能力，以便能够在更广泛的环境中采取行动。一步一步拾级而上。

F. 为下一步行动做好准备

然而，将任何安全计划描述为一段旅程的问题是，要在较长时期内维持高管的支持和同事的认可。

这既不是一场马拉松，也不是一次短跑：零信任计划提供了一种将安全性嵌入到我们开展业务的方式中的方法。

与业务价值和优先事项保持一致。成功的零信任计划需要执行一系列措施，将零信任原则与具有商业价值的事项、高管团队和同事关注的事项以及对安全功能重要的事项联系起来。这样可以及时实现成果。

充分利用参考架构和项目管理框架。这是一项转型工作，应该利用企业架构和项目管理。这些功能可以建立一种一致的方法，针对具有不同身份（例如人员、服务和设备）的各种环境实施零信任原则。基本上，建立零信任的早期第一步措施是建立监管。

将您的架构与监管联系起来。如果您的组织拥有强大的企业架构团队，他们首先要着手做的事情是建立零信任参考架构。如果您的组织拥有强大的 GRC（监管、风险与合规性）团队，请着手将零信任原则逐渐应用于指南、标准，并最终将其纳入策略。使用零信任策略决策点 (PDP) 和策略决策引擎 (PDE) 来确定和执行 GRC 策略。

建立和沟通关键绩效指标 (KPI)。我们预计，如果不首先将零信任控制与监管目标联系起来，就难以有效地与审核机构沟通零信任控制。内部审核中的 GRC 功能可以确定如何衡量和报告零信任，并且向第三方和外部审核机构阐述预期结果，从而解决这个问题。这对于具有合规性驱动因素或客户需求的商业案例尤其重要。尽早确定第三方将如何评估和衡量零信任，并与同事和高管进行交流。

从快速致胜中获得动力。每个组织的安全堆栈都会存在不同程度的优势和劣势。如果您拥有非常强大的云访问安全代理 (CASB) 解决方案，则可能能够获取动态应用列表。如果您采用了非常强大的单点登录 (SSO) 或多因素身份验证 (MFA)，则可能能够获取一组动态的设备数据。重要的是要充分发挥您的优势，并利用稳固的基础获得可视性和情景感知。

可视性至关重要。建立可视性并设置这些资产流程，是早期的快速致胜方法。请记住，这应该包括确保部署多因素身份验证和单点登录，以提高这些控制措施的策略实施可视性。实际上，我们此时要做的是部署策略引擎，并开始获得可视性，同时决定要维持的策略实施级别。然后，确定其他安全计划的协作点。

从 “取得进展” 到 “成熟” 的零信任实施路线图

从取得进展过渡到成熟实施包括三个要点:		
· 首先是**实施的广度**，可以通过扩大控制措施的覆盖范围来实现。例如，让更多的人注册 MFA，管理更多的设备，以及保护更多的应用。	· 其次，**增加策略的深度。**在策略引擎中充分利用遥测、情景和条件，做出更明智的信任决策。然后，将集成扩展到其他安全技术。	· 取得成熟实施进展的第三个方面是**提高自动化和协调能力。**当我们发现某些事物不可信时，我们可以自动化执行哪些额外措施？

基本结论: 零信任最好通过一系列步骤分阶段实施，并且这些单独的步骤应作为单独的安全项目进行管理。

每一个步骤均可提供以下优势:

- 提供更广泛的机会来加强安全关系和安全文化
- 从身份管理到资产管理，从事件响应到灾难恢复，提供早该启动的增强安全性的方法
- 通过具备成本效益、充分集成且自动化的安全技术，提供商业价值

V. 零信任实施要点

A. 使用 CISA 零信任框架

作为一种架构策略，有了行业专业知识的指导才能最好地实现零信任。在零信任架构方面，CISA 设定了标准。CISA，即美国网络安全和基础设施安全局，成立于 2018 年，是一种公私合作伙伴关系，旨在保护美国国土安全部 (DHS) 内部的数字关键基础设施，并 “与合作伙伴共同抵御当今的威胁，携手为未来建设更安全、更有弹性的基础设施。”[2]

> “零信任是实现国家防御现代化和加强国家防御的关键要素。”
> – Jen Easterly，CISA 总监

CISA 零信任成熟度模型为希望追求零信任的组织提供了路线图。此框架概述了零信任的五个关键支柱:

- 身份
- 设备
- 网络 (或环境)
- 应用 (或工作负载)
- 数据

[2] https://www.cisa.gov/about-cisa

每个支柱都包括对可视性和分析、自动化和协调以及监管（或合规性）的要求。此外，对于每个支柱，都有基于控制强度或其部署方式的成熟度级别：传统、高级和最佳。

CISA 零信任成熟度模型反映了这样一个现实，即零信任安全是一种持续追求，而不是一个 “一劳永逸” 的项目。借助此模型，团队可以评估自己所处的阶段、存在的差距以及如何取得进展。

根据 CISA 模型以及我们的调查数据，零信任的最佳实施涉及使用：

- 自动化
- 集成式工作流程
- 持续信任验证
- 数据资产
- 加密
- 微边界

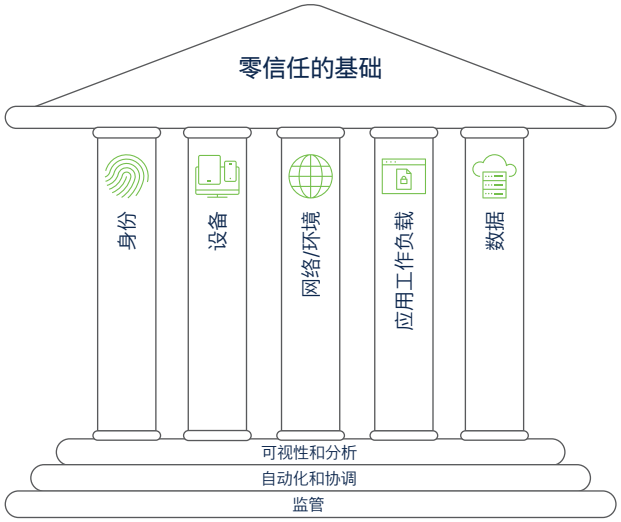


图 13：美国网络安全和基础设施安全局 (CISA) 的零信任支柱

CISA 零信任成熟度模型

	身份	设备	网络/环境	应用工作负载	数据
传统	· 密码或多因素身份验证 (MFA) · 有限风险评估	· 对合规性的有限可视性 · 简单库存	· 大型宏观分段 · 最低限度的内部或外部流量加密	· 基于本地授权的访问 · 与工作流程最低限度的集成 · 部分云可访问性	· 库存不足 · 静态控制 · 未加密
高级	· MFA · 与云和本地系统进行部分身份联合	· 满足合规要求 · 数据访问取决于首次访问时的设备状态	· 按入口/出口微边界定义 · 基本分析	· 基于集中式身份验证的访问 · 基本集成到应用工作流程	· 最低权限控制 · 对存储在云或远程环境中的数据进行静态加密
最佳	· 持续验证 · 实时机器学习分析	· 持续的设备安全监控和验证 · 数据访问取决于实时风险分析	· 完全分布式入口/出口微边界 · 基于机器学习的威胁防护 · 对所有流量进行加密	· 持续授权访问 · 密切集成到应用工作流程	· 动态支持 · 对所有数据进行加密

可视性和分析 | 自动化和协调 | 监管

图 14：美国网络安全和基础设施安全局 (CISA) 零信任成熟度模型

美国政府推动零信任观念

2021 年 5 月，拜登总统签署了他的第一个关于网络安全的行政命令 (EO)，要求联邦政府转向采用零信任架构。2022 年 1 月，美国行政管理和预算局 (OMB) 发布了一份备忘录，对具体要求给出了截止日期，赋予了这份零信任命令更强大的 “效力”。尽管 OMB 备忘录仅适用于民事联邦机构，但许多行业分析师在分析商业零信任市场时仍依赖于 CISA 框架。

B. 思科零信任经验总结

2020 年，思科着手变革基于网络的传统边界和 VPN 模式，转向采用零信任框架。从一开始，其核心目标是为用户提供安全、一致的应用访问体验，无论用户或应用位于何处，都不例外。

我们的团队着手为 10 万多名用户提高安全性并打造更出色的体验，在不到五个月的时间里就完成了这项根本性变革。

那么，思科的零信任是什么样的？根据思科的零信任原则，每一次用户尝试访问应用时，都需要满足四项要求：

1. 使用多因素身份验证对用户进行验证
2. 确认设备处于最新状态且运行正常
3. 确保使用思科管理的设备
4. 无需 VPN 也可访问应用

而我们所说的 “每一次”，不是每天一次，也不是针对单个应用，而是次次如此，毫无例外。

“一般解决方案在增强安全性的同时，很少还能改善用户体验，但是通过这次部署我们做到了。” - Josephina Fernandez，思科 IT 总监

C. 探索快速致胜的秘诀

快速致胜秘诀 #1: 通过简单的信息获得认可。我们发现其他项目中一个常见的问题是，计划过于复杂，难以获得理解和支持。我们的目标是使信息简洁明了、明确，并设定时间期限，以便让其容易记住并方便向他人转述。

快速致胜秘诀 #2: 明确范围并充分传达相关状态。我们清楚地传达了我们的目标：改善用户体验、降低风险并改善监管。我们消除任何将项目扩展到这些目标之外的尝试，同时还确保让所有相关方了解最新部署状态。

快速致胜秘诀 #3: 创造零信任需求。我们从最常用的 10-15 个应用入手，以便改善用户体验，使之产生最广泛、最明显的影响。一旦用户看到访问最重要的应用是多么容易，组织内部从应用所有者到部门主管的需求都会与日俱增。

快速致胜秘诀 #4: 从现有基础入手，充分利用现有基础。正如我们的高级副总裁兼首席安全和信任官 Brad Arkin 所说：“您永远不会从零开始。” 我们的团队决定哪些现有安全控制措施可用于推进零信任目标，以及哪些技术必须淘汰。

点击此处，阅读思科大规模部署零信任解决方案的完整案例。

通过数字看思科的零信任

试点指标	每月指标	每年节省的费用
· 5 个月时间表 – 包括 98 个国家/地区的员工和承包商 · 10-15 个未使用 VPN 保护的专用应用 (现在超过 100 个) · 不到 1% 的用户联系了服务中心 (以前为 7%) · 保护了 17 万台设备	· 576 万次运行状况检查 · 超过 8.6 万台设备进行了自我修复 · VPN 身份验证减少 41 万次	· 通过提高员工的工作效率, 节省 340 万美元 · IT 服务中心支持节省了 50 万美元成本

D. 构筑弹性：Cisco Secure 如何实现零信任

携手思科，组织可以在其多环境 IT 生态系统结构中嵌入零信任，提供安全访问，只防范攻击者，而不妨碍用户。这有助于在面对不可预测的威胁和挑战时保护业务完整性，对于保障安全弹性至关重要。

思科提供关键的零信任功能, 使组织能够实现以下目标:

借助思科的集成方法，组织可以跨网络、设备、应用和云成功实施统一的策略生命周期管理。

最终，携手思科，公司可以通过强大的安全性和卓越的工作效率释放价值并实现其目标，使团队能够实现更出色的安全性、更高的性能和更快的威胁响应。

作为一家在全球运营中实施零信任的公司，思科可以提供值得信赖的专业知识，帮助全球 300,000 多万家客户保护其业务各个方面的完整性，以抵御不可预测的威胁或变化，然后变得更加强大。

我们的解决方案涵盖 CISA 零信任成熟度模型的五个关键支柱, 可提供跨园区、云和本地网络的可视性与可控性。

cisco SECURE

VI. 后续行动

我们在零信任方面合作的许多客户和合作伙伴都在寻求解决一些关键挑战。有些组织将采用零信任机制视为保护其资产免受针对性威胁侵害，或通过保护混合办公环境来提升业务绩效的一种有效方式。有些组织则将零信任与降低供应链风险以及保护云环境联系起来。

不断升级的威胁需要采用全新的安全方法。通过与思科在零信任方面开展合作，您的组织可以更快速地应对威胁，并通过更深入的可视性构筑弹性，减少威胁的影响，从而更快地恢复并重新为客户服务。

准备好迈出零信任的第一步了吗？确保只有正确的用户和安全的设备才能访问应用，并提供无障碍的体验。注册 Cisco Secure Access by Duo 免费试用。

有关如何快速开启零信任之旅的更多信息，请注册思科零信任研讨会

cisco.com/go/zero-trust-workshops

Duo Security 现已并入思科，是领先的多因素身份验证 (MFA) 和安全接入提供商。Duo 构成了 Cisco Secure 零信任产品的一个关键支柱，是一种完善的策略，无论用户使用何种设备访问 IT 应用或环境，都能为其提供可靠保护。Duo 是全球 35,000 多家客户值得信赖的合作伙伴，包括 Bird、Facebook、Lyft、密歇根大学、Yelp、Zillow 等。Duo 成立于密歇根州安阿伯，在德克萨斯州的奥斯汀、加利福尼亚州的旧金山和伦敦都设有办事处。

前往 duo.com 免费试用。

cisco SECURE

思科长期以来一直是网络行业领导者，在此过程中构建了一个开放的集成式网络安全解决方案组合。Cisco Secure 秉持不断优化、简化的安全原则。我们提供以客户为中心的精简安全方法，可确保各产品不仅易于部署、易于管理、易于使用，而且可以协同工作。我们深知，客户及其相关人员是我们产品和服务的核心。Cisco Secure 利用 SecureX 平台为安全行业提供可靠的安全解决方案，确保他们在当下和未来免受威胁困扰。我们提供全球最全面、集成度最高的网络安全平台，帮助财富 100 强公司防御当前和未来的各种威胁。

如需详细了解我们如何简化体验，促进您取得成功并提供面向未来的安全保护，请访问 cisco.com/go/secure。