CSO Microsoft Security

推广内容

零信任安全：**早期采用者的经验教训**

CSO Microsoft Security

目录

引言

过去两年发生的颠覆性变化改变了传统 IT 和安全模型。这使得零信任安全迅速从一个有趣的概念发展成为现代企业安全的基础。

Foundry 进行的新研究发现，52% 的组织正在试用或已经部署零信任体系结构，另外有 15% 的组织正在研究零信任模型。这些采用者表示，他们通过部署获得了许多好处，包括改善了客户数据保护状况、降低了复杂性并提供了对企业资源安全、可靠的访问。

本电子书将探讨 Foundry 调查的结果，该调查强调了零信任策略在帮助首席信息安全官保护组织免遭众多攻击途径带来的诸多风险方面的重要性。此外，还为刚刚开始其旅程的组织提供了有关如何实施零信任的指导。

关于本调查

在 2022 年 2 月和 3 月，Foundry 调查了多家美国企业来了解零信任采用的现状。受访者需要在拥有超过 500 名员工的公司担任 IT 经理 或更高级别的职位，并承担网络安全产品和服务采购方面的角色。

本调查包含 23 个问题，总共有 250 名受访者给出了回答。

CSO Microsoft Security

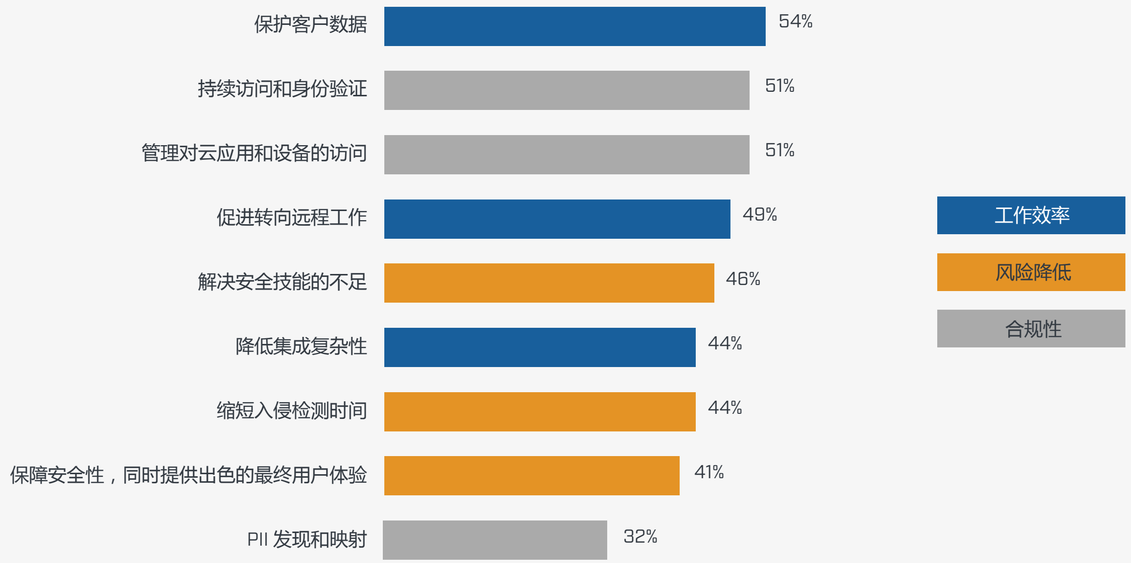
零信任已被广泛接受并持续提供价值

从调查结果以及与 IT 和安全高管的深入访谈中可以明显看出，大多数组织将零信任放在首位，而那些部署了各种零信任组件的组织已经从中受益。

大多数已实施零信任的受访者（87%）表示，该体系结构实现甚至超越了他们最初的实施、采用和集成目标。

一家跨国零售商的 IT 总监表示：“[零信任] 已成为我们的标准操作程序。我无法想象重新采用以前的工作方式。”（本调查允许受访者匿名参加，以便他们自由讨论安全计划。）

自实施零信任以来获得的好处



12% 的受访者表示，他们获得了*所有* 这些好处

资料来源：Zero Trust Adoption Survey，2022 年 3 月，Foundry。受访人数：250

CSO Microsoft Security

大约 44% 的受访者还表示，零信任降低了实施集成式安全体系结构本身具有的复杂性。一家拥有 3,500 名员工的呼叫中心公司的首席信息安全官表示 ：“你要处理和使用的是一个框架，这确实能降低工作的复杂性。”

一家拥有 17,000 名员工的金融服务公司的副总裁兼首席信息安全官表示，作为零信任策略的一部分，其公司实施了多重身份验证，这受到了员工们的热烈追捧。他说 :“这切实提高了员工满意度，因为他们现在不必登录公司提供的计算机并使用 VPN 客户端 ；他们可以随时随地获取资源。”

这位首席信息安全官指出，最小特权访问的概念同样奏效。他表示 :“得益于实施该特权访问系统，我们的系统管理员所犯的灾难性错误减少了。他们会在特定时间段内获得进行特定事项所需的特权，这意味着他们犯错的几率会有所下降。”

考虑到网络钓鱼和其他网络攻击的不断增加，一家零售公司的 IT 总监这样总结了零信任的好处 :“如果我们没有这些类型的工具，我们的处境可能会很糟糕，而且现在可能正要向某个人支付比特币。”

CSO Microsoft Security

零信任部署的驱动因素

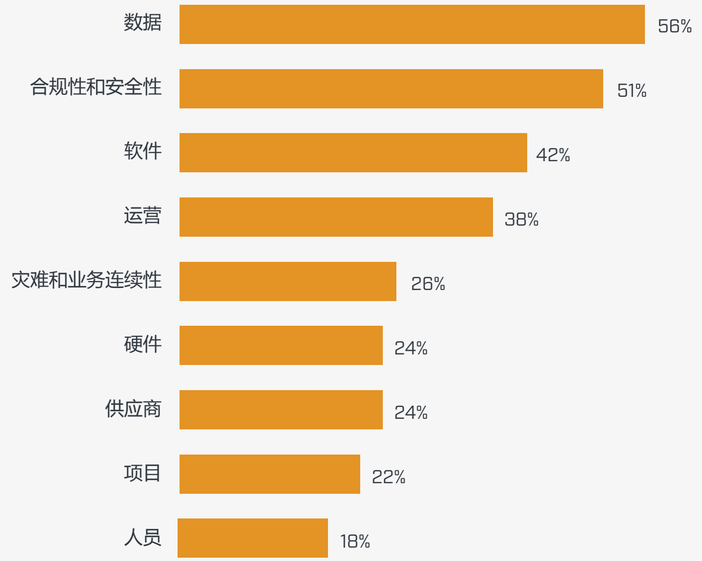
一系列事件促使众多公司至少开始将零信任体系结构纳入考虑，而首要任务则是需要控制大量资源面临的风险，使其免受诸多威胁。调查受访者将一年的安全事件归结为第三方个人或组织的安全漏洞引发的多个原因。其他原因包括 ：

- 意外业务风险
- 错误配置服务或系统
- 蓄意的恶意内部攻击
- 非恶意用户错误，包括网络钓鱼受害者
- 身份遭到泄露
- 软件未修补
- 凭据被盗

这些事件带来了数据主导的各种风险。

对于许多组织来说，伴随着基于边界的传统安全模型的过时，因疫情导致的向远程工作模式的骤然转变加速了他们对零信任策略的采用。随着更多应用程序和 IT 基础结构迁移到云，许多组织已朝着这个方向迈进，但疫情提供了额外的推动力。

最易面临网络安全威胁风险的类别



资料来源 ：Zero Trust Adoption Survey，2022 年 3 月，Foundry。受访人数 ：250

CSO Microsoft Security

例如，一家拥有 1,700 名员工的医疗技术公司的首席信息安全官表示，云和疫情推动了其对零信任的采用，如今，无论他们打算采用何种工作场所模式，零信任都能在安全性方面为之奠定坚实的基础。

他说 :“事实上，我们是一家基于云的公司并且需要能够保护我们的环境，这正是其中的业务驱动因素。在疫情期间，我们还需要提供一支有能力的远程员工队伍。[零信任] 使我们能够大幅减少房地产的体量，未来，我们公司可能仍会有至少 60% 的工作通过虚拟远程方式开展。”

威胁层出不穷

合规性需求也为采用更稳健的安全模型提供了动力。一家拥有 290,000 名员工的金融服务公司的全球信息安全高级副总裁表示：“监管机构一直在监督我们，他们希望我们能够继续改进我们的安全框架”。

一些组织主动采取措施来采用零信任，以免备受瞩目的入侵事件让他们因错误的原因而成为人们关注的焦点。一家拥有 3,500 名员工的高等教育机构的首席信息官表示：“这在于主动采取措施，并设法避免登上新闻报道。在一些真实的可怕案例中，本地其他一些与我们规模相当的机构停工了很长时间。”

其他组织经历的严重网络安全事件促使他们快速重新审视其安全策略。一家拥有 6,000 名员工的保险公司遭受了勒索软件攻击，导致其公司网络停止运行了两周，之后，首席执行官直接要求采用零信任策略。这家公司的 IT 部署副总裁说：“我们加快了实施速度。这在一开始无疑就是最佳实践，而在我们遭受勒索软件攻击后，实施速度大幅加快了。”

基于云的推动因素

一家大型金融服务公司的副总裁兼首席信息安全官表示，多年前，随着其团队开始采用更多基于云的资源以及用户越来越多地采用移动设备，他们认识到需要采用新的安全体系结构。

他说：“我们意识到，我们过去依赖的传统‘城堡与护城河’安全体系结构无法保护我们未来免受攻击。”

2020 年初，这一现实情况变得显而易见，当时这家公司发现在上一年的某个时间，在未经检测的情况下，攻击者侵入了其外围并在环境内横向移动。“我们需要采用新的体系结构，以便在用户使用驻留在任何位置的资源时提供保护并进行身份验证，而零信任体系结构便可做到这一点。”

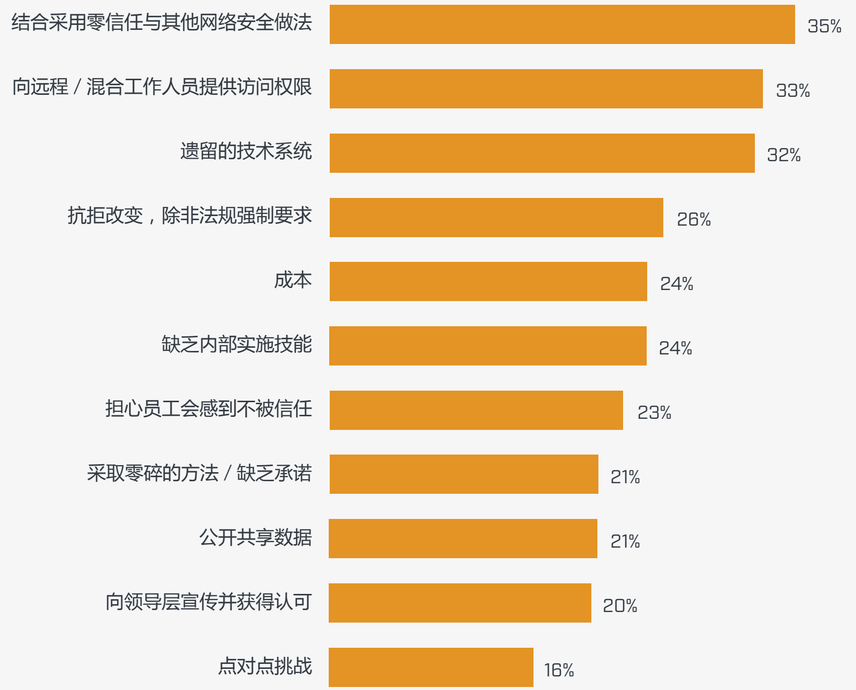
CSO Microsoft Security

零信任采用所面临的障碍

对于许多组织来说，零信任代表了安全结构、流程和思维发生的根本性转变，这诠释了他们在采用零信任之前必须克服的一些障碍。

呼叫中心首席信息安全官指出 ：“我们在组织内开始碰到许多不同的孤岛。” 他解释道 ,每个服务器、网络和数据库团队都有自己的一系列 Web 服务器和工具。“这使我们陷入了困境，因为对于从哪里以及如何执行操作，每个人都有不同的想法。”

零信任采用的障碍因素有哪些？



资料来源 ：Zero Trust Adoption Survey，2022 年 3 月，Foundry。受访人数 ：250

CSO Microsoft Security

Microsoft 零信任高级产品营销经理 Anthony Mocny 表示，挖掘此类问题实际上可能是零信任带来的积极的副作用。他说：“作为一种体系结构，零信任旨在打破技术支柱中存在的安全团队孤岛，并帮助团队协同工作。这可能也意味着会发生文化变革，具体体现则是团队合作方式的变化。”

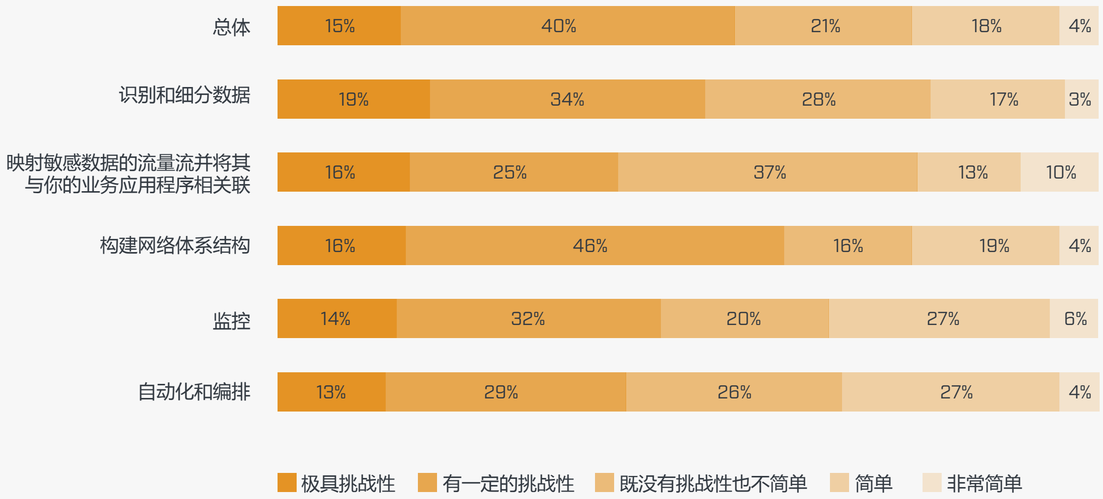
对于这位金融服务副总裁 / 首席信息安全官来说，遗留的应用程序是实施零信任所需要克服的一个障碍。他表示：“应该利用现代身份验证技术对这些应用程序进行改造。不过根据它们存在的时长，这可能不是一件容易的事情。”

CSO Microsoft Security

部署挑战

一旦公司开始零信任之旅，各种实施挑战就会浮出水面。超过一半的受访者（56%）承认实施零信任具有挑战性或极具挑战性。具体情况为 ：

零信任实施的挑战性有多大？



资料来源 ：Zero Trust Adoption Survey，2022 年 3 月，Foundry。受访人数 ：168

在深度访谈中，受访者频繁提及有关分段和微分段的挑战。

前文提到的金融服务副总裁 / 首席信息安全官表示 :“目前的做法是以单台主机为基础对网络进行分段，这就像是在内部网络上的每台主机之间设置了一个小型防火墙，这样就可以看到所有的流量并控制其向每台计算机的流动。这具有巨大的安全优势，但实施起来非常困难，因为现在你必须管理数以万计的防火墙。”

映射流量可能是另一个需要数月时间的过程。拥有 5,000 名员工的出版和媒体公司的首席技术官表示，在明确了公司需要保护的关键数据、应用程序和网络服务后，“我们沿着网络映射了事务流，并试图将它们理解为一组信息。[然后我们] 将这些信息细分为多个部分，并对信息在网络中传播的方式进行细分，有时甚至会将其细分为单个信息包。” 此时，该公司对每种类型的流量都应用了零信任策略。“我们还构建了监控和维护网络的新功能。”

尽管存在这些挑战，许多受访者仍认为零信任最终将简化日常运营。采用传统技术，“需要几天时间才能做出改变 ;你必须在所有硬件和软件组件上部署这些技术，我们为此耗费了大量资源，” 前文提到的负责全球信息安全的金融服务高级副总裁表示。“我们认为，从长远来看，零信任确实最大限度地降低了架构复杂性，并减少了从事同类工作所需的员工数量。”

实施零信任的最佳实践

随着越来越多的公司实施零信任体系结构，他们正在开发路线图和最佳实践，以便其他人效仿遵循。以下是规划部署时的五个注意事项。

不要一开始就进行大规模投入

如果仅从必须跨网络、数据、应用程序、身份、终结点和基础结构修改策略和保护方法的大背景来看，制定零信任策略可能会令人生畏。“一开始，我们只是在仰望这座高不可攀的山峰，质疑自己是否真的要这么做，”前文提到的高等教育机构首席信息官表示。“你只需要循序渐进。”

这位首席信息官和所在团队最终采用了一种“跟钱走”的方法，将在一个单独网络上对财务和薪资应用程序进行细分作为优先事项。

Mocny 表示，确定需要保护的关键资产是一个可靠的方法。他说：“首先，要明确你实施零信任的原因”。

如果不确定从何处着手，建议先实施多重身份验证

在确定安全堆栈的优先级时，许多首席信息安全官和安全供应商都建议首先关注身份验证和其他基于身份的保护。Mocny 表示：“如果你不知道从哪入手，那么多重身份验证是一个不错的选择。” Microsoft 估计，多重身份验证可阻止超过 90% 的基于身份的攻击。

这位金融服务副总裁 / 首席信息安全官对此表示同意，他说道：“身份验证是实施零信任体系结构的一个基本要素。如果不能验证最终用户的身份，其他组件都将无法工作，所以我们从身份验证入手。”

接下来，这位金融服务副总裁 / 首席信息安全官对网络连接组件进行了处理，这在为远程工作者提供支持方面带来了立竿见影的好处。该团队将微分段留到了零信任之旅的后期完成，因为其带来的影响短期之内不会在整个企业内部显现。他表示：“完成微分段后，企业的安全性会显著提高，但人们并不能察觉到其中的不同。”

CSO Microsoft Security

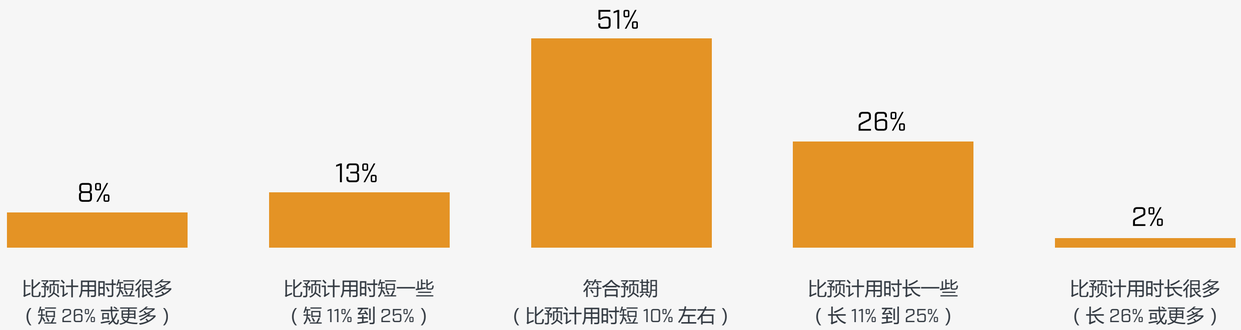
制定切合实际的时间表

首席信息安全官应对零信任部署设定合理的预期，这点非常重要。这位金融服务副总裁 / 首席信息安全官表示 :“实施零信任体系结构是一项计划，而不是一个项目。此举带来了巨大的变化。如果能够圆满完成，众多项目也将从中受益，这种好处可能会持续数年 ;实施零信任基础结构没有捷径可走。”

一位同为金融高级副总裁的同事对此表示同意。他说 :“我认为这个旅程永远不会结束，因为新的技术、新的恶意软件、新的威胁层出不穷。”

大多数受访者 [72%] 表示，他们的部署计划要么正稳步进行，要么进度超前，而剩下的受访者表示实施时间比预期要长。

零信任实施是否符合你的时间预期？



资料来源 :Zero Trust Adoption Survey，2022 年 3 月，Foundry。受访人数 :168

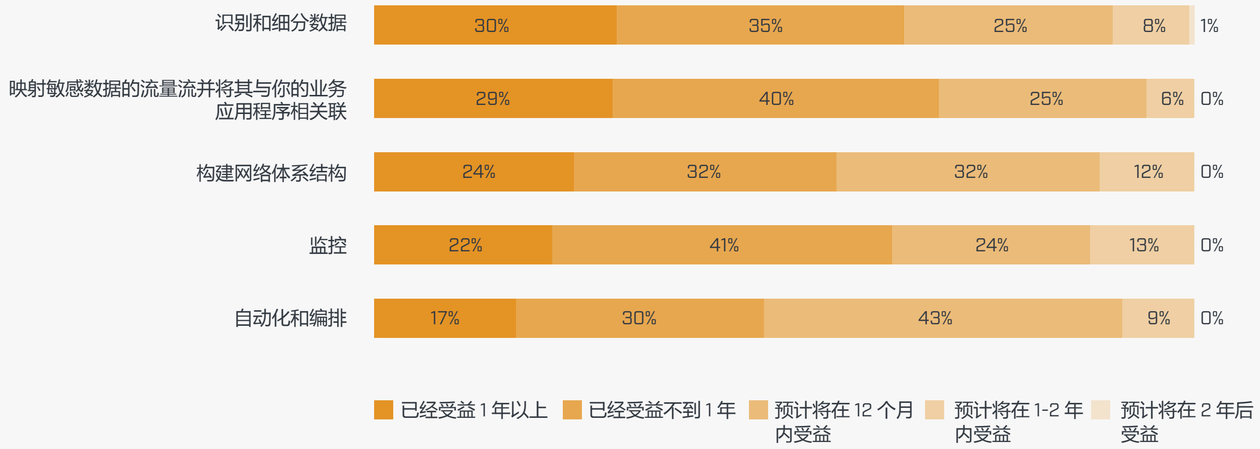
CSO Microsoft Security

在部署过程中衡量进展

在零信任的部署过程中，首席信息安全官可以并且应该创建里程碑来衡量进展。大约三分之二的受访者表示，他们在一年内从其项目的大多数方面获得了好处，还有大约四分之一或更多的受访者预计将在 12 个月内从各项关键活动中获得好处，包括识别和细分数据、映射流量流以及构建网络体系结构 - 这是一个很好的迹象。

Mocny 表示 ：“零信任之所以是一个旅程，是因为你需要持续进行评估，以抵御性质不断变化的攻击。应时刻关注可改进的领域。”

从零信任中受益的时间



资料来源 ：Zero Trust Adoption Survey，2022 年 3 月，Foundry。受访人数 ：103

关注技术的同时也应关注人

零信任安全模式的广泛普及影响到了每一个员工，包括负责零信任部署的 IT 和安全团队。正因如此，与所有大型技术项目一样，必须确保部署遵循新流程和变更管理实践，从而确保成功顺利的推广。

Mocny 表示：“除了技术变革外，与之而来的还有文化变革。如果你有多个解决安全问题的团队，包括网络架构师团队或身份专家团队，那么你还需要更改这些团队协同工作的方式。你需要打破孤岛，确保各项技术都能协同工作。”

要消除孤岛，需要让各个专业领域的团队成员紧密地参与到试点和概念验证 (POC) 项目中。一家拥有约 2,000 名员工的电信公司的 IT 系统主管就学到了这个教训 - 在部署期间他遇到了几个单点故障，包括部分服务无法进行身份验证并突然变得“不受信任”，这导致这些服务和一些系统无法使用。

他表示：“部署一项服务可能会产生多米诺骨牌效应，对其他服务带来影响。”他还表示，未来，“我们将更加谨慎 - 在部署之前，进行更长时间的概念证明、更多的审查，与主题专家进行更多的体系结构审查。”

零信任 ROI

一项 2021 年进行的 **Forrester Consulting Total Economic Impact™ 委托研究**对 Microsoft 零信任解决方案的成本节省和业务优势进行了量化。基于 Forrester 采访的五家企业，一家复合型组织通过实施 Microsoft 的零信任体系结构实现了 92% 的三年投资回报率。

这家复合型组织还实现了平均每月每员工 20 美元的成本节省，因为部署零信任后，安全管理工具变得多余，包括终结点管理、防病毒和反恶意软件解决方案。

CSO Microsoft Security

你处在零信任之旅的哪个阶段？

调查表明，零信任安全模型的优势明显，能够出色地解决首席信息安全官及其安全团队所面临的一些部署挑战。通过制定深思熟虑的实施计划来应对这些挑战，可帮助贵组织快速改进保护措施、降低风险并开始提供业务价值。

要评估贵组织的零信任成熟度并了解更多实用的部署资源，请参与 Microsoft **零信任成熟度模型评估**。