ivanti

2020
零信任进度报告

Cybersecurity Insiders

概览

不断增加的数据泄露事件表明，没有任何企业可确保不受网络攻击。其中一个原因是，移动工作和云计算将大部分的工作移出了企业网络和传统的周界防御的保护之外。作为降低网络风险的关键举措之一，企业正在越来越多地采纳零信任安全模式。零信任的原则是，对用户、设备和基础架构进行验证，然后授予基于有条件访问的最低权限。因此，零信任策略有希望显著增强可用性、数据保护和管理。这份《2020零信任进展报告》显示了企业在内部实施零信任安全的现状及相关的重要驱动因素、采纳情况、技术、投资和效益。

《2020零信任进度报告》访问了400多位从技术主管到IT安全从业人员的网络安全决策者，均衡代表了多个行业中不同规模的企业横截面。虽然72%的企业有计划在2020年在某种程度上评估或实施零信任策略，以降低日益增长的网络风险，但仍有近一半（47%）的网络安全专业人士对将零信任模式应用于安全访问架构缺乏信心。

主要发现包括：

- •对于把零信任模式应用于安全访问架构，有信心和缺乏信心的人数几乎相等（53%有信心，47%没有信心）。
- 53%的受访者计划将零信任访问功能转移到混合IT模式中。
- 超过60%的受访者认为零信任的原则，包括持续认证和授权、通过实体验证获得信任以及数据保护，对其企的吸引力最大。
- 超过40%的受访者表示，权限管理、不安全的合作伙伴访问、网络攻击、影子IT风险以及易受攻击的移动和高风险设备资源访问是安全访问应用程序和资源的最大挑战。
- 45%的企业担心公共云应用的访问安全，43%的企业担心自带设备的风险。
- 70%的企业有计划提高身份和访问管理能力。
- 30%的企业正在寻求简化安全访问交付，包括改善用户体验、优化管理和配置。
- 41%的企业有意重新评估安全访问基础设施，并正在考虑采用软件定义边界（SDP），其中大多数需要采用混式IT部署，而四分之一将采用SaaS策略。

非常感谢Ivanti对这一重要研究项目的支持。

我们希望这份报告能为您提供有用信息和帮助，协助您不懈地保护您的IT环境。

谢谢！
Holger Schulze

零信任原则

哪些零信任模式原则对企业最有吸引力？持续认证/授权以67%的比例高居榜首，这也是零信任价值主张的核心组成部分。通过实体验证（用户、设备和基础架构组件等）获取信任（65%）和数据保护（如安全连接）（63%）紧随其后。

哪些零信任原则对您和您的企业最有吸引力？[1]

67%

持续认证/授权

65%

通过实体验证
（如用户、设备、基础架构）

63%

数据保护
（如安全连接）

端到端的访问可视性
和审计

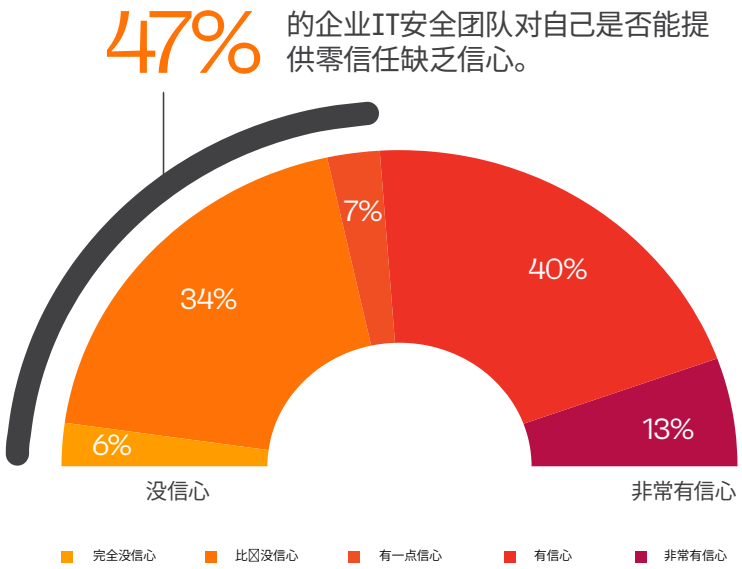
推行最低权限访问

集中化、
精细化的访问策略

零信任信心

53%的企业有信心能够在安全访问架构中实施零信任策略，但也超过40%的企业IT安全团队对自己是否能提供零信任缺乏信心。

您是否有信心在您的安全访问架构中应用零信任模式/原则？



零信任的驱动因素

企业启动或建立零信任计划的动力是什么？首先是数据安全（85%），其次是防止泄漏（70%）和减少对端点的威胁（56%）。除了行业、监管和内部的合规性要求外，近三分之一的企业的目的是解决混合型IT的安全问题。

您的公司启动/增强身份访问/零信任管理计划的主要驱动因素有哪些？[2]

85%

安全/数据保护

70%

防止泄漏

56%

补救终端和物联网安全威胁

减少内部威胁

行业/监管规定
（例如HIPAA、GDRP、PCI DSS等）

内部规定

安全访问的挑战

企业在确保访问安全时面临的主要挑战有哪些？员工过度授权（62%）、合作伙伴访问敏感资源（55%）以及易受攻击的移动和高风险设备访问资源（49%）是受访者提及最多的企业挑战。

在确保应用程序和资源的访问安全方面，您的企业面临的主要挑战有哪些？[3]

62%

员工访问时过度授权

55%

合作伙伴以不安全的方式访问应用程序和资源

49%

易受攻击的移动和高风险设备访问资源
（未知、未批准、不合规、丢失的端点）

网络攻击
（例如拒绝服务、跨站脚本、中间人、网络钓鱼）

影子IT

安全重点

根据我们的调查显示，71%企业把改进身份和访问管理视为首要任务。其次是预防数据丢失（59%）和安全访问云服务提供商托管的云应用程序（45%）。

您的企业目前有哪些网络安全方面的优先事项？[4]

71%

改善身份和访问管理（IAM）

59%

预防数据丢失（DLP）

45%

确保安全访问云服务提供商托管的应用程序
（如微软、亚马逊、谷歌等）

启用端点移动管理（EMM）/自带设备（BYOD）
（如：用户、设备）

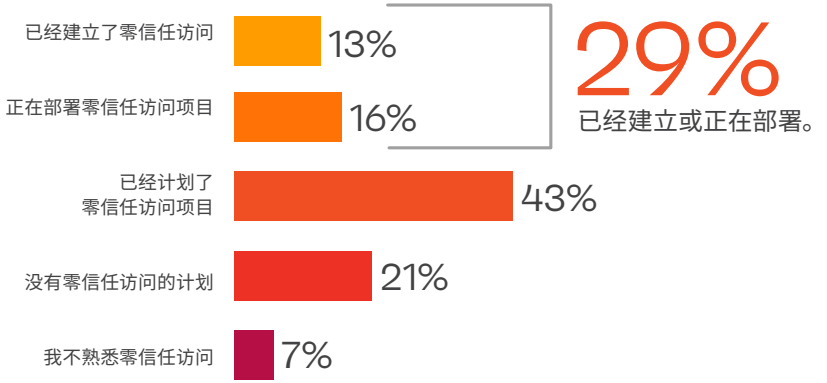
进行深度SSL检查
（例如：安全解密恶意软件扫描
会话数据/电子邮件过滤）

简化安全访问交付
（如用户体验、管理）

采纳零信任

在采用零信任访问的规划方面，29%的受访者已经建立了模式或正在部署项目，而43%的人尚处于计划阶段。令人惊讶的是，近三分之一的受访者并未计划或不熟悉零信任模式。

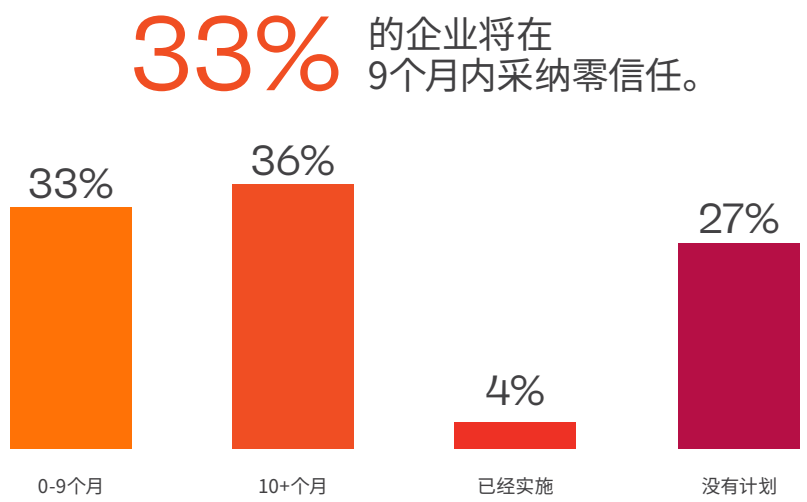
您的公司有什么样的零信任访问模式采用计划？



采纳速度

对零信任的关注正在转向初步部署。事实上，33%的企业将在9个月内采纳零信任。但近三分之一的企业没有相关计划，这表明企业在零信任的价值或所需工作方面还存在困惑。

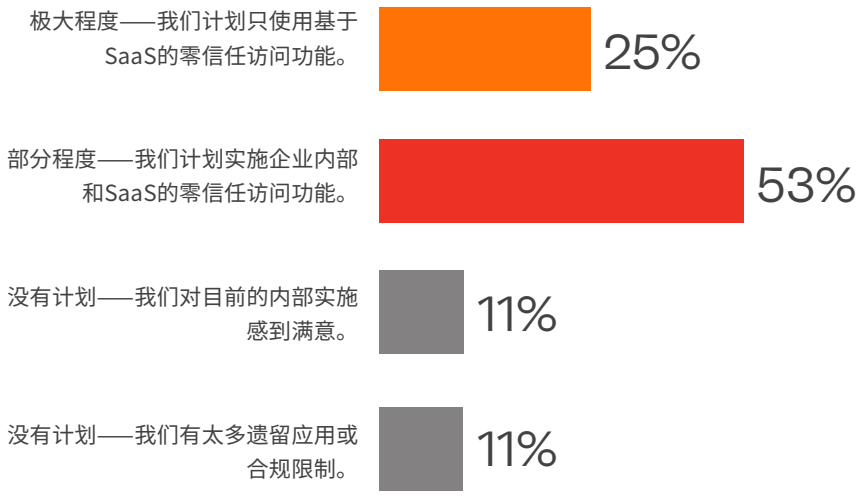
您最有可能在什么时候采用零信任安全？



零信任SaaS

超过一半的企业计划把零信任访问能力转移到混合型IT（企业内/SaaS）部署。四分之一的企业计划完全转为基于SaaS的零信任解决方案。22%的企业没有基于SaaS的零信任部署计划，原因包括遗留应用、合规性限制或对目前实施的访问保护感到满意。

在未来18个月中，您和您的企业计划在多大程度上把零信任访问功能转为SaaS？[5]



零信任访问投资重点

对零信任访问技术的大部分投资用于多因素认证(59%)、身份管理和治理(48%)以及单点登录(44%)。此外还有网络访问控制和网络应用防火墙(43%),特权访问管理和微分段(41%),以及虚拟专用网络(35%)。

在未来12个月内,您的企业会重点投资以下哪些身份访问/零信任控制技术?[6]

59%

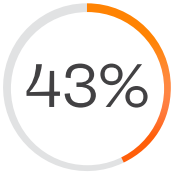
多因素验证(MFA)

48%

身份管理和治理

44%

单点登录 (SSO)



网络访问控制(NAC)、网络应用防火墙(WAF)

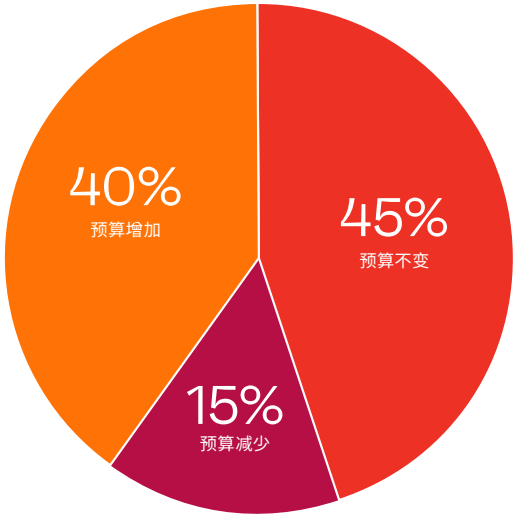
特权访问管理(PAM)、微分段

虚拟专用网络(VPN)

零信任访问预算

40%的企业预计在未来18个月内会增加与访问管理相关的预算。只有15%的企业预计会削减预算。

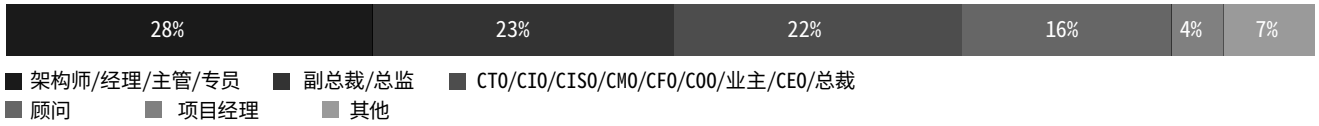
您预计您的企业的访问管理相关预算在未来18个月内会有什么变化?



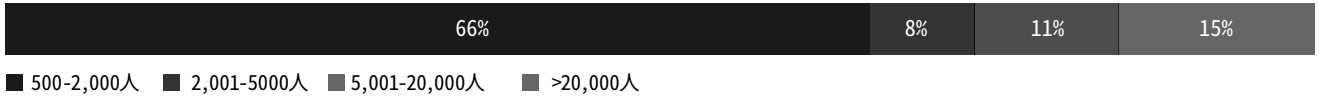
研究方法&人群统计资料

本报告基于一项全面网上问卷调查的结果，该调查于2020年1月在美国进行，共访问了413位IT和网络安全专业人士，目的是研究企业在零信任安全方面的最新采用趋势、挑战、空白和解决方案选择。受访者中有技术主管，也有IT安全从业人员，均衡地代表了多个行业不同规模企业的横截面。

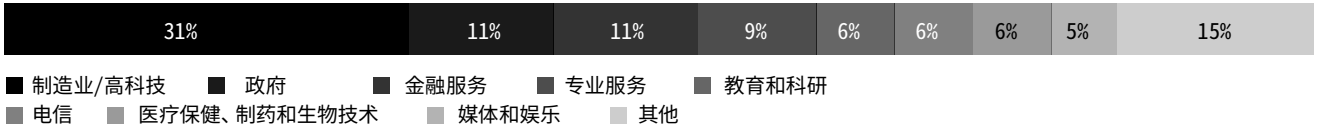
职务级别



公司规模



行业



ivanti.com.cn
+86 (0)10 85412999
ContactChina@ivanti.com

1 资源隔离 44% | 内部和外部网络之间没有信任区分 39% | 其他 2%

2 应对审计或安全事件 37% | 运营效率 33% | 解决混合型IT的安全问题 31% | 其他 4%

3 人工操作流程复杂，影响了快速反应的能力 37% | 其他 2%

4 增强SD-WAN的安全功能 28% | 补充端点检测和响应（EDR） 27% | 增强或取代现有的远程访问工具（如VDI、VPN、RDP） 24% | 其他 5% | 无2%

5 SSL检查 40% | 保护SD-WAN 27% | 简化 26% | 替换现有的远程访问安全技术（如VPN） 25% | EDR 20% | 无 2% | 其他8%

6 云访问安全代理（CASB） 33% | 企业移动管理（MDM） 31% | 软件定义的周界（SDP） 28% | 身份分析 24% | 企业目录服务 17% | 其他2%