借助 Workspace ONE 实现零信任安全

问： 什么是零信任？

答： 零信任是一种条件访问控制模型，需要持续进行信任验证，然后才允许对应用和数据进行最低权限访问。零信任背后的策略可以归结为抛弃传统的安全方法（即认为网络边界范围内的所有资源都是值得信任的），改为采用“永不信任，始终验证”的方法。与传统的安全方法相比，零信任存在动态决策点，用于验证信任并影响对企业应用和数据的访问级别。

问： 零信任是一种理念、功能还是一种产品？

答： 零信任是内含一套准则的安全模型，即使 IT 部门采用了移动技术和云技术等新技术，该安全模型也能为企业提供端到端安全性。它依赖于这样一种概念：在授予对企业应用和数据的最低必要权限之前对设备合规性和用户身份进行持续验证。

问： 为什么需要零信任？

答： 传统的安全方法是在网络边界范围内的环境中开发的，假设对组织网络内的任何人都绝对信任。这种方法类似于“城堡和护城河”，往往侧重于通过 VPN 和网络访问控制等技术构建“护城河”上。然而如今，随着移动技术和云技术等技术的出现，我们所知道的网络边界已经消失了。我们需要一种全新的安全方法，这种方法依赖于对合规性的持续验证，并且无论人们从任何位置以及任何设备访问应用和数据，这种方法都能保护相关应用和数据。零信任恰恰做到了这一点。

问： 为什么零信任如今很重要？

答： 零信任是 Forrester 公司的 John Kindervag 在 2010 年提出的，它是一种基于“永不信任，始终验证”概念的安全方法。该方法侧重于信任概念，以及恶意行为者是如何通过看似可信但实际上已被入侵（例如网络钓鱼攻击、恶意软件等）的设备潜入的。随着组织采用数字化工作空间，设备选择（移动设备、台式机、物联网）、灵活的工作方式（网络内与网络外）和应用异构性（SaaS、Web、原生、虚拟）等概念变成了现实并开始共存共生。在这种用户可以从任何设备访问任何应用的动态环境中，我们需要一种同样具有动态特点的安全方法，在允许访问敏感信息之前持续进行信任验证。安全漏洞正在增加，而最近大多数安全漏洞都是因公司采用过时的安全策略而造成的。目前零信任方法比以往任何时候都更加重要。

问： 零信任的主要原则是什么？

答： 虽然不同公司和组织定义了多种零信任访问模型（Google 的 BeyondCorp、Forrester 的 Zero Trust eXtended、Gartner 的 CARTA 等），但 VMware 的零信任体系架构规定了五项主要原则：

- 设备管理和合规性 - 确保设备的合规性状态
- 条件访问 - 旨在通过逐级身份验证方面的功能确认用户的身份
- 应用隧道和代理 - 保护数据中心路径和虚拟桌面，并部署相关技术以减少攻击面
- 风险分析 - 通过提升可见性和行为分析功能来提高安全性
- 修复和编排 - 通过自动修复和编排提升安全性和体验

问： 客户是否必须遵循所有原则才能拥有零信任 IT 环境？

答： 通过遵循“零信任之旅”的所有原则，企业能够在不断发展的 IT 环境中得到端到端安全访问控制机制的保护，包括保护对云应用或本地应用的访问。然而，对于大多数组织而言，采用零信任方法将会是一个历经多年的过程，与此同时，公司会重新思考并投资能够为其带来完全零信任环境的技术。此外，每个组织都有自己的零信任方法采用历程，具体取决于他们想要保护哪些应用以及如何实现数字化转型。

问： 我的客户已经有了其他安全解决方案。零信任方法将会如何影响这些投资？

答： VMware 针对数字化工作空间的零信任方法不依赖于供应商。该方法围绕如何为企业提供最佳安全性规定了一些主要原则，同时与“永不信任，始终验证”的零信任原则保持一致。Workspace ONE 可提供灵活且支持所有应用的跨平台端到端零信任安全性。Workspace ONE 灵活且可扩展，还可轻松集成其他第三方解决方案来防范威胁或实现编排，从而使客户既能利用现有投资，又能实现零信任目标。

问： 客户可以将零信任解决方案作为一项产品来购买吗？

答： 不可以。客户必须确定自己的需求，并将这些需求与适当的 Workspace ONE SKU 对应起来。可在此处获取有关 Workspace ONE SKU 的更多信息。

问： VMware 收购 Carbon Black 对 VMware 的零信任产品/服务定位有何影响？

答： 作为端点和工作负载安全方面的行业领导者，Carbon Black 为 VMware 的零信任安全产品/服务带来了巨大的价值。借助全新的 Workspace Security Bundle，Workspace ONE Advanced 客户可以利用 Workspace ONE Intelligence 和现有的 Trust Network 集成，摄取 Carbon Black Next-Gen Antivirus (NGAV) 和 Endpoint Detection and Response (EDR) 产品 CB Defense 所检测到的威胁实时数据，从而计算风险得分并评估合规性状态。这有助于持续验证信任，并强化 VMware 面向数字化工作空间的零信任产品/服务。

问： 在哪里可以查看有关零信任的更多信息？

答： 如需详细了解 VMware 对应用于数字化工作空间的零信任产品/服务的定位，请访问数字化工作空间的安全网站。您也可以访问我们的技术专区网站获取深入的技术信息。

问： 是否可以提供专业服务来帮助客户执行零信任计划？

答： 可以。现在，我们可以提供各种专业服务来帮助您开启零信任之旅。如需了解入门方面的详细信息，请与您的客户主管联系。

问： 客户如何开启零信任之旅？

答： 刚开始时，客户可以访问 TechZone 以获取详细的技术文档和基于应用场景的实施指南。如需详细了解可帮助您开启零信任之旅的各种 Workspace ONE 解决方案，请联系您的客户主管。VMware Solution Exchange (https://marketplace.vmware.com/vsx/) 提供了有关合作伙伴解决方案的更多信息。

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
威睿信息技术（中国）有限公司
中国北京办公室 北京市朝阳区新源南路 8 号启皓北京东塔 8 层 801 邮编：100027 电话：+86-10-5976-6300
中国上海办公室 上海市淮海中路 333 号瑞安大厦 805B-809 室 邮编：200021 电话：+86-21-8024-9200
中国广州办公室 广州市天河路 385 号太古汇一座 3502 室 邮编：510610 电话：+86-20-87146110
中国香港公司 香港港岛东太古城太古湾道 12 号太古城中心 4 期 4 楼 电话：852-3696 6100 传真：852-3696 6101
www.vmware.com/cn

项目号：vmw-faq-temp-word 2/19

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
威睿信息技术（中国）有限公司
中国北京办公室 北京市朝阳区新源南路 8 号启皓北京东塔 8 层 801 邮编：100027 电话：+86-10-5976-6300
中国上海办公室 上海市淮海中路 333 号瑞安大厦 805B-809 室 邮编：200021 电话：+86-21-8024-9200
中国广州办公室 广州市天河路 385 号太古汇一座 3502 室 邮编：510610 电话：+86-20-87146110
中国香港公司 香港港岛东太古城太古湾道 12 号太古城中心 4 期 4 楼 电话：852-3696 6100 传真：852-3696 6101
www.vmware.com/cn

项目号：vmw-faq-temp-word 2/19