加强数字化工作空间安全的综合性方案

vmware®

目录

一些企业允许员工使用他们喜欢而且需要的应用，并使这些应用随时随地都可以从任何设备上立即访问到，以此增强了员工的能力；这些企业取得的优势，是在个人和组织层面切实提升了决策能力、生产力和效率。[1]

简介

通过最新的量化分析发现的业务优势表明使用数字化工作空间的员工更高产，而且他们的公司在业绩上胜过那些使用传统工作空间的公司，这让更多的企业希望了解如何实现类似的优势，同时安全地将应用交付到任何设备。企业都希望获得 Forbes Insights 在其 Impact of the Digital Workforce 研究中发现的优势，但谁也不想牺牲安全性来实现这些优势 — 即使传统的工作边界正在消失。

工作边界的消失将企业暴露在风险之中

世界各地的 IT 团队在继续与数量和严重性都在增加的安全威胁作斗争。对于许多企业，恶意软件侵入已造成了代价高昂的运营中断。例如，WannaCry 网络攻击就利用了 Microsoft Windows 中的一个漏洞同时锁住 150 个国家/地区的数百万台计算机，以勒索“赎金”。在美国，2017 年追踪记录的数据泄露事件数量达到了创纪录的新高。[2]

当今不断扩大的组织和工作边界，为网络犯罪提供了更好的机会。新式零日威胁和中间人攻击 (MITM) 就是很好的例子，前者以发起攻击的时间命名，是在开发者发现漏洞的第一（或第零）天之前或当天发起攻击；后者则是一种窃听形式，攻击者通过拦截公钥消息交换主动进行侦听，并重新发送消息，同时用自己的密钥替换请求的密钥，实际上就是在两个用户不知情的情况下接管、监视和修改他们之间的通信。[3] 利用社会工程和编程专业知识、机器人和勒索软件威胁的高级网络钓鱼技术也是更多地攻击企业，甚至那些努力保持领先一步的企业也不能幸免。

战胜威胁并保护企业数据

需要使用一种的更好方案，通过一个智能驱动型平台来防范、检测和修复威胁，以保护不断发展中的数字化工作空间。有了此方案，企业就可以更有效地保护敏感数据。因为，随着其数字化工作空间战略的扩展和改进，动态网络威胁也会升级并调整，将目标瞄准传统边界之外的新漏洞。

本白皮书介绍了一种全新的综合性、预测式安全方案，可在现代化的无边界运营环境中提供安全保护。本白皮书强调了加强不断发展中的数字化工作空间安全的重要性，并指出企业需要在其生态系统中的各组件之间建立一个信任框架。文中还介绍了防范、检测和修复方面的八项核心能力，为确保 IT 组织可以从收集的数据中获得洞察信息并使用它们作出关于防止威胁和阻止攻击蔓延的正确决策，这八项能力是必须具备的。

1 Forbes Insights。“The High-Performance Digital Culture: Empowerment, Trust, and the New Equilibrium Between the Employee and IT”，2017 年 10 月。

2 Identity Theft Resource Center。“2017 Annual Data Breach Year-End Review”。

3 Technopedia。“Zero-Day Threat”，2018 年。

“安全性是 2018 年移动技术和数字化工作空间投资的首要考虑事项。”

– CCS INSIGHTS

安全性是实施现代数字化工作空间战略的最大障碍

如今，随处都可以开展工作。员工们正在从办公室、从家中、在咖啡馆，甚至在 1 万英尺的高空访问信息和应用；而且，为进行访问，他们使用了多种个人和公司端点设备，跨越多种不同的网络。IT 团队认识到，员工希望能够更自由地选择工作时间、工作地点以及工作所用的设备，于是他们纷纷行动起来，希望能够做到在满足员工偏好的同时保护宝贵的企业数据。

然而，现有安全解决方案不能提供足够的保护。IT 团队仍在尝试使用复杂而且往往是拼凑起来的传统安全技术来满足快速变化中的终端用户需求；其中部署的一些技术是要保护一些它们并不能够保护的东西。IT 团队随着时间推移购买了许多不同的解决方案，其结果是，许多技术彼此间无法很好地通信，从而为各种攻击提供了众多潜在的途径。虽说员工满意度对其企业的成功至关重要，但 IT 领导者报告说，在他们 2018 年的移动技术和数字化工作空间的投资中，安全性依然是首要考虑事项。[4]

在 CCS Insights 最近进行的一项调查中，将近一半 (47%) 的 IT 购买者表示，在未来 12 个月内的数字化工作空间投资中，网络安全是最优先的投资方面，然后依次是设备安全性 (42%)、应用安全性 (27%)。在工作负载移动时，这些投资可能能够更好地保护数据和应用；然而，安全解决方案孤井只会增加复杂性，并且仍存在出错的可能。例如，企业可能会利用网络防火墙防止一种入侵渗透某一系统，但然后却发现该入侵正在影响跨一系列系统流动的东西向流量，这是因为该入侵已潜行数月未被检测到 — 这会给企业带来严重损害。采用一种基于一个信任框架将各个安全解决方案孤井连接起来的方案，IT 将不需要对防范、检测和修复威胁这些工作进行优先级排序 — 因为该方案会持续执行这三项工作。

企业可以使用一种现代化的数字化工作空间安全保护方案，来更有效地战胜针对系统和数据的不断变化的网络威胁；在此方案中，安全保护将随员工的数字化工作空间而行。该模型应该在保护终端用户计算生态环境 — 员工、应用、端点和网络 — 的各个组件之间建立信任，并基于验证而只允许获得授权的访问。一个全面而且集成的信任框架可帮助确保数据得到保护，而且可以通过洞察力和自动化信息处理能力用于日常检测和修复，以最大限度地降低风险。

4 CCS Insights 调查，“IT Buyer Survey”，2017 年 9 月。

新的安全要求

- 为保护企业，需要引入防范、检测和修复方面的八项核心能力。
- 为获得一个聚合视图，企业需要使用一个框架，来建立用于确保生态系统安全性的各个组件之间的信任。
- 为了不断降低风险，企业需要洞悉其环境中的一切，从而为保护其数字化工作空间作出预测性、自动化的决策。

在不断发展中的数字化工作空间实施全面安全保护的三个步骤

IT 组织需要一种全面的安全保护方案，来保护其终端用户环境。该模型通过将各个安全技术孤井连为一体，而涵盖了端点、应用、员工和网络的安全保护。为实现最佳效果，IT 必须考虑执行这些步骤，从战略高度保护其不断发展的数字化工作空间。

第 1 步：防范、检测和修复威胁

网络威胁已发生变化。一些最初可能是恶作剧的黑客活动，例如，学生通过进入并立即离开非经授权的系统而向朋友炫耀其 IT 本领的情形，现在几乎都演变成了有恶劣意图的黑客行为。防范网络犯罪要求一种全面的响应措施，既要实施好做法，又要摒弃坏习惯，以便：

防范

企业 — 尤其是金融服务和医疗保健等受监管的企业 — 在竭尽全力满足存放有高度敏感且宝贵数据的后端存储方面的合规性要求。然而，如今的客户经理可能会在会见客户期间访问移动设备上的敏感数据，然后意外将平板电脑丢在出租车上，导致敏感数据可能被盗取。此丢失而且被盗用的客户信息，将几乎肯定会给企业品牌和财务造成负面影响。

让员工能够以消费级的简便性无缝访问数据，不应以给企业带来巨大风险为代价。正因如此，企业安全功能都从保护员工的数字化工作空间开始。IT 应该能够通过教育员工不点击可疑链接，并部署旨在防止数据丢失的策略，来防止恶意软件进入环境。当企业从员工到应用、从设备到网络对其所有资产有了全面了解之后，就能进一步发现漏洞，并针对内部和外部威胁为其环境提供保护了。只有当他们能够全面实施一系列保护 — 包括发布策略（如访问控制策略）、执行敏感数据分类，实施设备使用限制，以及定期修补应用 — 时，他们才能够安下心来，准备开始检测阶段的工作。毕竟，防范方案若离开了同样有效的检测方法，将使 IT 部门即使在处理最严重的问题时，也不了解其所做工作的重要性。

检测

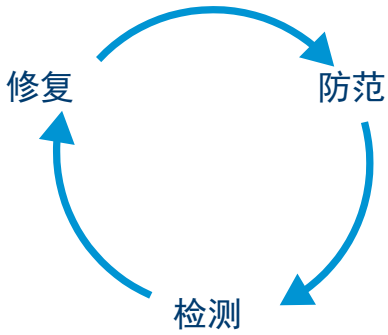
正在消失的边界、内部威胁以及创造性越来越高的网络犯罪，已经将关于安全的对话从“是否”会发生攻击变成攻击将在“何时”发生。这就要求企业不能只着眼于保护资产，还要更进一步，考虑如何检测发生入侵的情形 — 从凭证被破解，到未打补丁的漏洞利用等等。IT 团队必须能够识别并瓦解活跃的威胁，使其没有机会给企业造成更大的损害。检测机制的实施还不能造成警报疲劳。

当威胁进入数字化工作空间时，有所准备的企业将能够通过持续的自适应监控检测到它们，从而使其 IT 运维和安全团队能够发现移动和桌面端点及应用上的威胁。通过自动、持续监控谁在访问哪些信息、是从哪里以何种方式访问的、通过了什么网络，并在必要时发出警报信息，IT 将始终保持控制能力。然后，使用最后已知良好状态、登录信息以及分析形式的情报信息，IT 就掌握了必要的工具，可以识别异常，并根据洞悉的情况作出关于下一步行动的更好决策。

修复

数字化业务的节奏极快，这使多数任务都要求手动修复的传统安全解决方案变得过时。如今的企业在应对恶意入侵以及意外停机时，都要求快速响应。等待响应会导致恶意软件渗透到更大的范围。VMware 内部的一项研究指出，1/10 的企业客户需要一年或更长时间才能完成影响到其多数或全部端点的 Windows 修补。这就为网络犯罪分子发明侵入方法留出了时间。

IT 团队必须能够利用来自其环境的洞察信息，自信地基于问题根源预先制定策略，以便快速自动进行响应和恢复，实现最佳效果。通过自动化，IT 可以选择隔离、暂停或阻止对一项应用和云服务的访问。在检测到威胁后，准备最充分的企业将有一个有效的解决方案，他们可通过一个能够检测到行为异常并启动一个自动化策略以阻止对敏感数据访问的引擎，来自动完成修复。



那些选择使用一个战略框架以在其生态系统中的组件与保护这些组件的解决方案之间建立信任的企业将处于最有利的地位，能够全面保护重要的企业资产，并加快检测和修复速度。

第 2 步：防范、检测和修复能力

这八项重要能力将推动企业朝着现代化、综合性数字化工作空间安全保护的方向前进：

单一开放平台方案	单一开放平台使 IT 能够简化合规性的强制实施 — 例如设备和应用的合规性 — 并降低风险。企业应采用一个单一、开放的平台，它将访问、设备和应用管理功能与分析和信息处理能力结合起来，从而以独特方式将复杂而且成本高昂的现有安全解决方案孤井连为一体。一个具有 Intelligence 服务的平台确保了工作空间数据聚合、关联和建议，以实现整体洞察力和自动化。 使用此方案的企业应获得可显示其员工、应用、端点和网络的一个聚合视图。此平台方案应基于一个 API 通信框架而构建，该框架有助于在企业生态系统中的各组件之间建立信任。这非常关键，因为跨整个数字化工作空间建立信任后，就会实现一个最低权限的互联系统，使安全保护可以随员工而行，让他们能力大增。
数据丢失防护 (DLP) 策略	DLP 策略可帮助企业保护数据 — 无论数据在哪里，无论是在数据中心之内还是之外。在一件设备丢失或被盗后，IT 团队应该能够远程锁定或擦除设备，并获取实时设备信息，如操作系统 (OS) 版本、上次更新时间、位置等。利用虚拟桌面基础架构 (VDI) 将桌面和应用集中化，可帮助减少设备丢失或被盗造成的数据丢失。 企业还应该能够跨其所有端点使用由原生操作系统提供的 DLP 控制，以应用为单位强制实施并管理安全策略，并通过电子邮件附件控制、剪切/复制/粘贴限制、动态水印等功能防止在内容方面出现数据丢失。控制并限制用户使用软件开发工具包 (SDK) 从企业删除内容的能力是一项必须满足的要求。 策略和合规性引擎可帮助自动实现对高级 DLP 的遵守。高级安全策略包括针对被 root 或越狱的设备的设置保护、白名单和黑名单应用、“打开方式”应用限制、地理围栏、网络配置、阻止导出和快照，以及将公司信息备份或保存到外部 SD 卡或远程云备份解决方案。
上下文策略	通过使用上下文策略设置并强制实施终端用户条件访问，将有助于确保只有获授权的用户可以访问敏感信息和资源。企业必须能够建立条件访问 — 按角色、部门、许可级别等授予访问权 — 以便只有获得授权的用户可以访问某些信息和资源。 通过将策略强制实施与访问和设备管理结合起来，IT 将能够限制用户对数据、应用或设备的权限。同样的技术也可以用于将条件访问功能应用到移动应用，并确保只有合规应用才能访问内部系统。

保护应用	通过在应用级别强制实施 DLP 策略，企业朝着更精细的访问策略又迈出了一大步，从而可以更好地保护数据。数字化工作空间应包括在应用级别提供同样功能的 DLP 策略（详见前面第二项能力中的介绍）。 对于自带 (BYO) 设备和公司设备，移动应用管理都方便了应用的调配和控制访问，这实际上就是用按身份定义的策略来打包应用。类似地，云数据丢失防护，以及对受认可和非受认可云服务中的访问和活动进行监管，可更好地保护数据并防范威胁。 因为可支持完整设备 VPN、应用级 VPN 和跨所有主要操作系统（包括 iOS、Android、macOS 和 Windows 10）的基于 SDK 的代理网关通信，所以 IT 获得了灵活性，可以选择正确的解决方案来保护应用连接。 另外，生产力工具（例如电子邮件、文档管理等）必须提供 DLP 和权限管理服务 (RMS) 功能，包括： • 受信息权限管理 (IRM) 保护的电子邮件 • 使用 PKI 的 S/MIME • 电子邮件分类 • 敏感信息或个人身份信息 (PII) 策略 • 对附件进行加密 • 针对打印、查看和漫游的访问策略 • 文档过期 • 水印
访问权限管理	企业通过用多种因素验证用户身份，或者一次性为许多应用完成用户身份验证，而增强了数据保护。为数量不断增加的应用、设备和云服务分别设置策略是一项越来越复杂的任务，为消除此类任务，企业应该能够使用终端用户的身份来建立安全参数。 一触式单点登录 (SSO) 允许用户访问桌面、移动和云应用 — 避免了多次登录需要的时间和麻烦。通过 SSO，用户的身份可以一次性向多个应用进行验证，实际上就是为单个数字化工作空间提供单一密钥，以便从应用目录打开对所选端点上的一系列 Web、移动、SaaS 和传统应用的访问。 通过多因素身份验证 (MFA)，用户和系统组件的身份可以使用多种因素（不只是简单的密码）进行验证，并且与针对各个应用所请求的访问权限或功能的风险相称。
加密	通过加密，数据在被发送出去并接收到时，非预期接收者将不能看到此数据，这样企业就可以确信其敏感数据得到了保护。针对关键业务流程的最佳实践，包括所有数据在存储或传输时都应加密。即使发生数据泄露，窃取关键文件也只能得到无法读取的数据。此外，对传输中的数据和静态数据使用高级加密标准（如 AES 256 位加密）进行加密是非常重要的。 作为设备平台和企业系统之间的中继，IT 可以使用安全加密链路或应用级 VPN，利用唯一证书来对从合规设备上的各个应用到它们试图访问的后端系统的流量执行身份验证和加密。

微分段	利用跨其所有网络的微分段，企业可以以更大的力度战胜威胁、降低风险，并改善他们的安全状况。微分段提供了多种能力的组合，包括： • 通过分布式有状态防火墙（控制精细度以工作负载为单位）和 ALG（应用层网关）减小数据中心边界内的攻击面。 • 支持使用安全组实现针对虚拟机（包虚拟桌面和虚拟应用主机）的基于对象的策略应用，从而创建精细的应用级控制 • 基于逻辑网络叠加的隔离和分段，可跨越机架和数据中心而不考虑底层网络硬件，从而实现多数据中心安全策略的集中管理 整个 IT 环境被划分成更小的部分后将更易于管理，从而可以在其中一部分受到攻击时保护环境或控制损害范围。通过隔离从应用流向数据中心中特定工作负载的东西向流量，可显著减少意在给公司造成巨大损害的恶意软件/病毒的攻击途径。
分析	利用来自应用部署和使用情况的具有行动指导意义的洞察信息，企业改善了他们的安全状况。聚合在一起的应用部署、使用情况、设备安全性以及终端用户体验方面的详细信息，让 IT 可以更好地了解其数字化工作空间环境的性能和安全性。内置的带有自动化操作的 Intelligence 服务可加快规划、增强安全性，并改善终端用户体验。它还在如今无边界的运营环境中提供了日常的安全风险监控和快速的风险减轻响应。与决策引擎一起，Intelligence 服务可帮助关联信息，以便基于访问策略检测威胁并自动执行修复。

第 3 步：可信赖的合作伙伴在所有位置注入安全防护

安全威胁在发生频率和造成的代价以及在专注度和完善性方面都在不断提升，这就使无缝集成了可信赖安全合作伙伴供应商产品的单一平台成了威胁防范、检测和修复的理想方案。传统的旨在保护宝贵信息的独立安全工具为 IT 提供了有限的可见性，而且往往会导致在整个环境中形成解决方案孤井。其结果是一种无法协调的安全保护方案，它会给企业造成负面影响，并且会因为保护数字化工作空间需要复杂的手动任务而提高成本。

在为保护不断发展变化的数字化工作空间的各个组件之间建立信任，有助于确保全方位的安全保护。理想方案是通过一个信任框架，该框架利用了基于一个经验证的数字化工作空间平台而构建的 API。这是因为 API 使一个丰富的安全解决方案生态系统可以与该平台通信，并最终提供了一个管理员为简化安全性和管理而希望使用并需要的一个聚合视图。

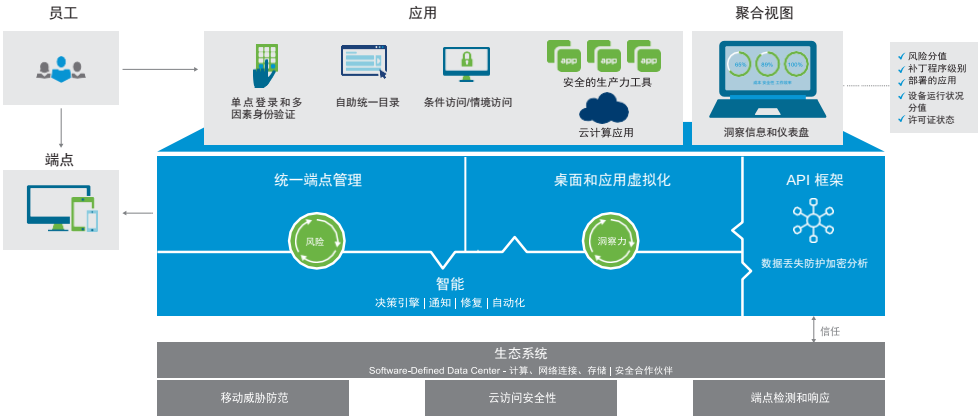
一个稳健的数字化工作空间战略将包括一个开放的、由可信赖的安全解决方案构成的生态系统，这些解决方案专用于在以下几方面挫败攻击和减轻风险：

- 操作系统安全缺陷可见性
- 设备运行状况评估
- 设备发现
- 监管访问和控制
- 策略设置
- 病毒扫描
- 修补
- 灾难恢复
- 合规性监控

VMware 如何帮助转变传统数字化工作空间的安全保护

尽管网络安全工具有了大量创新，但市场上网络安全工具的庞大数量和种类传递并强化了这样一条讯息：IT 领导人应等待一种采用了最佳实践的数字化工作空间安全保护方案的出现。如今，因为 VMware 可以用一个框架来帮助简化安全保护工作，企业可以在不断变化的威胁局面中信心百倍地挫败各种攻击。

VMware® Workspace ONE™ Trust Network™ 为企业提供了一种全面的现代化企业安全保护方案，来加强员工、应用、端点和网络的安全。Workspace ONE Trust Network 提供了一系列功能，可基于一个信任和验证框架跨整个不断发展中的数字化工作空间来防范、检测和抵御威胁。在整个数字化工作空间中建立信任关系后，就会实现一个最低权限的互联系统，使安全保护可以随员工而行，让他们能力大增。为管理与新式网络威胁相关的风险，Workspace ONE Trust Network 将来自智能驱动型 Workspace ONE 数字化工作空间平台的洞察力与可信赖的安全合作伙伴解决方案结合起来，从而为数字化工作空间提供预测式、自动化的安全保护。



防范、检测和修复

VMware 的方案可帮助您的 IT 运维和安全团队通过简化安全保护功能与 Workspace ONE Trust Network 方案所提供的解决方案功能之间的映射（例如使用 NIST 网络安全框架），来管理网络安全风险：

- 安全功能从保护数字化工作空间开始，其中包括使用机器学习识别恶意软件；利用网络微分段以防范高级持续性威胁 (APT)；和防止企业云端应用的数据泄露。
- 当威胁进入数字化工作空间时，VMware 可以通过跨移动和桌面端点的持续、自适应监控检测到它们。
- 然后，此方案使用强大的决策引擎进行自动修复。例如，当检测到木马或中间人攻击时，将启动一个自动化的策略来阻止对企业数据的访问。

将访问、设备和应用管理与分析统一起来

Workspace ONE Trust Network 将 Workspace ONE 的数字化工作空间功能（包括访问、设备和应用管理）与 Workspace ONE Intelligence 提供的分析功能结合起来，以独特方式将现有安全解决方案孤井连为一体。Workspace ONE Intelligence 服务提供了工作空间数据聚合、关联和建议，以实现整体洞察力和自动化。通过用 Workspace ONE Intelligence 服务补充 Workspace ONE Trust Network 功能，VMware 确保企业可在当今无边界的运营环境中实现持续的安全风险监控和快速风险缓解响应。

决策引擎可帮助将诸如网外公司设备这样的信息与用户行为关联起来，以检测到威胁并通过访问策略自动进行修复。对威胁数据的整体洞察力和精细的设备合规性状态提供了一种可以轻松地实时识别并减轻安全问题的方法，从而改善了数字化工作空间的安全数据健康状况。借助决策引擎，IT 可以创建规则来自动执行和优化常见任务，例如，使用关键补丁程序修复有漏洞的 Windows 10 端点，和在组级别或个体级别设置对应用和服务的条件访问控制。

利用由可信赖的合作伙伴解决方案构成的生态系统

为了实现整个数字化工作空间的全面安全性，需要在为不断增长和发展的数字化工作空间提供安全保护的各个组件之间建立信任。VMware 凭借 Workspace ONE Trust Network 做到了这一点，后者通过利用构建于 Workspace ONE 平台上的 API 提供了一个信任框架。这些 API 有助于确保生态系统中各式各样的安全解决方案可以与 Workspace ONE 通信，并最终提供了管理员为简化安全性和管理而需要使用的聚合视图。

通过将安全解决方案孤井连为一体，VMware 客户可以利用现有投资大幅改善连续监控和风险分析，从而加快响应速度，基于趋势和模式获得一个可以随部署的增长而扩大规模的预测式安全战略。

VMware 客户可以利用现有投资大幅改善连续监控和风险分析，从而加快响应速度，基于趋势和模式获得一个可以随部署的增长而扩大规模的预测式安全战略。

采用一种新的数字化工作空间安全方案是企业的当务之急，因为工作环境现在已变得没有边界。一个在他们的生态系统内的各个组件之间建立信任的框架可容纳新的员工、新的应用、新的设备和新的网络。它为您的数字化企业继续前进奠定了基础，让您可以在努力加快业务运营的同时减轻风险、保护您的品牌、降低成本、提高敏捷性，并在所有工作设备上提供消费级的方便体验。

防范、检测和修复：8 项必备能力

vmware Workspace ONE™ Trust Network	
能力	为何它很重要
单一开放平台方案	通过跨平台、应用和用户配置文件消除技术孤井，简化合规性的强制实施并降低风险。
数据丢失防护 (DLP) 策略	不管数据在什么位置，都可通过设备擦除、远程锁定和应用级安全策略保护数据。
上下文策略	通过强制实施条件访问策略，确保只有获授权的用户可以访问敏感信息和资源。
保护应用	利用应用级的 DLP 策略，通过控制谁可以访问哪些资源来保护信息安全。
访问权限管理	通过用多种因素验证用户身份，或者使用单点登录一次性为许多应用完成用户身份验证，而增强数据保护。
加密	通过在数据被发送出去并接收到时使非预期接收者无法看到此数据，而对敏感数据提供保护。
微分段	通过隔离工作负载和流量，减少您企业的受攻击面。
分析	利用具有行动指导意义的洞察信息、应用分析和自动化，改善安全状况和合规性。

了解更多

用一个数字化工作空间增强员工的能力，将使工作人员和企业都能受益。不要让 IT 安全问题成为增强生产力和效率优势的障碍。随着你们的数字化工作空间战略的扩展和改进，动态网络威胁也会升级并调整，以瞄准传统边界之外的新漏洞，而 Workspace ONE Trust Network 方案为您的企业提供了必需的能力，确保您实施全面的安全保护，从而可以随着运营环境的发展始终为敏感数据提供保护。通过将访问、设备和应用管理与分析功能结合起来保护您的数字化工作空间，利用一个跨整个生态系统的信任框架，并使用从收集来的数据中获得的洞察信息作出正确的安全决策。

如想了解有关 Workspace ONE Trust Network 的更多信息，请访问：
www.vmware.com/cn/products/workspace-one/security。

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 传真：86-10-5976-6302
中国上海办公室 上海市淮海中路 333 号瑞安大厦 804-809 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

项目编号：VMW-WP-CMPRHENSIVE_APPROACH_SECURITY_WRKPLC-A4_103