WORKSPACE ONE TRUST NETWORK

不断发展的数字化工作空间的安全性

概览

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，来加强其员工、应用、端点和网络的安全。凭借针对新式威胁的防范、检测和修复能力，Workspace ONE Trust Network 通过一个丰富的集成式合作伙伴解决方案生态系统补充了智能驱动型 Workspace ONE 平台固有的安全功能，使之能够跨整个数字化工作空间提供持续的风险监控，并快速作出风险缓解响应。

主要优势

Workspace ONE Trust Network 借助一个信任和验证框架简化了安全性和管理。借助 Workspace ONE Trust Network，IT 可以：

- 使用一个可提供聚合视图的基于操作的框架移除安全解决方案孤井，并降低整个数字化工作空间的复杂性
- 以独特方式将访问、设备和应用安全性及管理与洞察力和自动化结合起来，以降低整个终端用户计算生态系统中的风险
- 利用开放和可信赖的合作伙伴生态系统并继续使用现有投资，从而帮助降低成本

安全性 – 实施现代数字化工作空间战略的最大障碍

数字化工作空间可将员工工作效率提高 5 倍[1] 之多，使员工能够以简单而且安全的方式从他们自己选择的设备访问应用和数据。随着企业继续向数字化转型迈进，由员工、应用、端点和网络构成的数字化工作空间生态系统在不断增长和发展，超越了传统的边界；而且，BYOD（自带设备）和 IT 消费化已是大势所趋。随着传统边界的消失，诸如零日攻击、中间人攻击 (MiTM)、网络钓鱼、机器人和勒索软件之类的高级网络威胁开始出现。

安全性是移动和数字化工作空间投资的首要考虑事项[2]，但现有的安全工具只能为 IT 部门提供有限的可见性，让他们只能注意到提供传统功能的安全保护孤井。这样就形成了一种七拼八凑的安全保护方案，这样的保护方案复杂性高，还要求以手动方式确保数字化工作空间的安全，会给企业带来极高的成本。由此带来的后果是，安全性成了实施现代数字化工作空间战略的最大障碍。

无边界企业中全面的预测式安全保护

为在不影响用户体验的情况下满足安全需求，必须满足几项新的要求：

1. 为获得一个聚合视图，企业需要使用一个框架，以在用于确保其生态系统安全性的各个组件之间建立信任。
2. 为了不断降低风险，企业必须能够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。

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，来加强其员工、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，从而为其提供强大助力。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 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。

1 资料来源：https://www.vmware.com/radius/impact-digital-workforce/

2 2017 年 12 月的 CCS Insights Mobile Technology Buyer Survey

防范、检测和修复

企业是否会遇到网络攻击不是重点，重点是攻击何时发生。基于这一认识，IT 运维和安全团队可通过简化安全保护功能与 Workspace ONE Trust Network 所提供的功能之间的映射（例如使用 NIST 网络安全框架这样的框架）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防止恶意软件，防止企业云端应用的数据泄露，以及实施网络微分段以防范高级持续性威胁 (APT)。
- 当威胁进入数字化工作空间时，持续的自适应监控可以检测到它们，这样 IT 运维和安全团队就能够检测到移动和桌面端点及应用上的威胁。
- 在检测到威胁后，Workspace ONE Trust Network 可以利用强大的决策引擎自动执行修复。当基于行为异常检测到一种攻击时，可启动阻止访问企业数据的自动化策略。

将访问、设备、应用安全及管理与分析统一起来

Workspace ONE Trust Network 将智能驱动型 Workspace ONE 平台固有的安全功能（包括访问、设备和应用安全及管理）与分析结合起来，从而以独特方式将不同管理安全解决方案造成的孤井连为一体。Workspace ONE Intelligence 服务驱动 Workspace ONE 平台上的分析功能，并提供工作空间数据聚合、关联和建议，以实现整体洞察力和自动化。通过将 Workspace ONE Trust Network 功能与 Intelligence 服务相结合，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，以及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丰富的生态系统

为了实现整个数字化工作空间的全面安全性，必须在为不断变化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。Workspace ONE Trust Network 利用构建于 Workspace ONE 平台上的 API 提供了一个信任框架。这些 API 允许生态系统中各式各样的安全解决方案与 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。通过将各个安全解决方案孤井连为一体，客户可以利用其现有投资来大幅改善其持续监控和风险分析能力，以缩短响应时间。其结果是形成一种基于趋势和模式，可随部署扩展的预测式安全战略。

了解更多

若要了解有关 VMware Workspace Trust Network 的更多信息，请访问：www.vmware.com/cn/products/workspace-one/security

免费尝试动手练习：https://www.vmware.com/go/workspace-hol

要获取更多信息或购买 VMWARE 产品

敬请致电
010-59934306

或访问
http://www.vmware.com/cn/products，或在线搜索授权代理商。

主要功能特性

企业可以利用 Workspace ONE Trust Network 提供的这些关键安全功能，针对不断发展中的网络威胁形势实施防范、检测和修复措施。

功能	说明
一个连接不同安全解决方案的基础数字化工作空间平台	利用信任框架简化安全性和管理，此框架利用 API 允许一个开放的安全性生态系统与 Workspace ONE 进行通信。
通过访问权限管理简化您的业务运营	充分授权 IT 为所有应用提供应用调配、自服务目录、多因素身份验证和单点登录 (SSO)。
借助上下文策略优化用户体验和安全性	根据设备合规性状态、用户身份验证强度、数据敏感性、用户位置等条件，利用条件访问策略控制身份验证。
数据丢失防护 (DLP) 策略有助于防止数据泄露	启用设备级加密、数据加密和硬件安全策略。配置包括应用黑名单、设备配对、Wi-Fi 安全性和 TLS 实施在内的多种策略。监控恶意软件威胁、恶意应用、内存中攻击或越狱设备，并通过远程锁定、设备擦除、阻止访问或可自定义的设备隔离控制自动进行修复。
加强应用安全而又不牺牲用户体验	利用 VMware 安全的生产力工具中的安全控制机制 - VMware Boxer™、Browser™ 和 Content Locker™。针对所有其他应用和云计算服务检测威胁并自动修复。
静态数据和传输中数据的加密	使用 VMware Tunnel 对从设备上的应用到数据中心的流量进行身份验证和加密。使用 AES 256 位加密，保护静态和传输中的应用数据。
通过微分段跨各个网络实现安全保护自动化	使用 VMware NSX® 的微分段功能，自动确保整个网络的安全性，最大限度减少数据中心的受攻击范围。
整体洞察力和自动化推动预测式安全保护	利用 Workspace ONE Intelligence 提供的针对威胁数据和设备合规性精确状态的整体洞察力，实时发现并缓解安全性问题。

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
版权所有 © 2018 VMware, Inc. 保留所有权利。此产品受美国和国际版权法及知识产权法保护。VMware 及其子公司的产品受 http://www.vmware.com/cn/support/patents 网站中列出的一项或多项专利保护。VMware 及 VMware 徽标是 VMware, Inc. 及其子公司在美国和/或其他司法管辖区的注册商标或商标。此处提到的所有其他标志和名称分别是其各自公司的商标。
项目编号：130019wf-vmw-fy19q1 euc launch-trust network-ds-a4-106 3/18