VMware Workspace ONE

易于使用 — 企业级安全性

概览

VMware Workspace™ ONE™ 是一款简单且安全的企业级平台，可在任何智能手机、平板电脑或笔记本电脑上交付和管理任何应用。通过将身份管理、实时应用交付和企业移动化管理相集成，Workspace ONE 可调动数字化员工的积极性、减少数据泄漏威胁以及革新传统 IT 运维方式以迎接移动云计算时代。

主要优势

- 允许组织安全地采用 SaaS、移动应用，同时支持现有的企业级应用
- 利用使员工随时保持高效的工具吸引和留住顶级人才，同时保持适当的数据安全性和合规性
- 使用跟移动设备相同的现代管理框架来加速 Windows 10 的部署
- 自适应条件访问可根据身份验证强度、数据敏感度、用户位置、设备状况，确保用户处于适当的安全级别

关键市场趋势

新式应用（SaaS 应用、移动应用）的快速采用以及强大且经济实惠的移动设备的激增在工作环境中带来了新的挑战。

为了随时随地高效工作，员工一直在与严格的传统策略相周旋。组织面临关键转折点，要么无视这些趋势承担可能违反安全规定的风险，要么采用利用新管理框架的新工作方式。

什么是 Workspace ONE

VMware Workspace™ ONE™ 是一款简单且安全的企业级平台，可在任何智能手机、平板电脑或笔记本电脑上交付和管理任何应用。首先，该平台可为用户提供对云计算、移动和 Windows 应用的消费级自助式单点登录访问权，并包括为员工提供支持的强大集成式电子邮件、日历、文件和社交协作工具。

同时，员工有权选择自己的设备，评估推动采用 BYOD（自带设备）计划所需的管理工作（包括结合使用 VMware Identity Manager 和 AirWatch 企业移动化管理）的重要性，以便实施精确控制且基于风险的条件访问策略。

最后，Workspace ONE 能够完全自动完成传统的注册、笔记本电脑和移动设备配置，并通过提供实时应用生命周期管理，将旧版企业级客户端 - 服务器应用带入移动 - 云计算时代。

主要功能特性

可对云计算、移动、Windows 应用进行消费级自助访问

注册新应用和新员工非常简单。一旦通过 VMware Workspace ONE 应用的身份验证，员工便可以即时访问他们的个性化企业级应用目录，并能在其中订购几乎任何移动、云计算或 Windows 应用。借助内置的 VMware Identity Manager，由于设备中已经设定了业界领先的一触式移动设备单点登录机制，用户只需轻轻一触即可访问应用。

功能特性	说明
交付任何应用，包括最新的移动云计算应用和旧版企业级应用	通过企业级应用目录向任何设备提供适当的应用，包括： • 通过安全的浏览器和无缝 VPN 安全加密链路提供内部 Web 应用 • 通过基于 SAML 的 SSO 和调配框架提供 SaaS 应用 • 通过公共应用商店代理提供本机公共移动应用 • 通过 Windows 业务应用商店提供新式 Windows 应用 • 通过 MSI 软件包提供旧版 Windows 应用 • 通过 Horizon Air 将应用托管在数据中心内或由云服务提供商进行托管，可确保所记录的敏感应用所在的系统受到 HTML5 代理的保护 • 通过 Horizon Air 在云中或在本地部署的数据中心内交付完整的虚拟化代管桌面 • 支持 Citrix XenApp 托管应用
自助应用目录，改变了员工的入职方式	只需在 Windows、iOS 或 Android 上下载 Workspace ONE 应用即可为员工提供可轻松为您的公司定制和品牌化的完整的自助企业级应用目录。
单点登录，可将即便最复杂的本地部署 Active Directory 拓扑联合在一起登录	通过在用户、设备和企业之间建立一触式身份验证信任，免除了复杂的登录过程。 对较敏感的应用使用无缝的生物识别技术或其他多因素身份验证方法。 Workspace ONE（含 Identity Manager）包括一个企业级身份提供程序，适用于支持 SAML 和 WS-Fed（Web Service 联合身份验证）的应用，并且还可以链接到已在使用的任何现有第三方身份提供程序。
业界领先的一触式移动 SSO 利用设备信任和 PIN/ 生物识别超时设置进行身份验证	让员工通过本地 PIN 或生物识别服务解锁已知、特定且注册的设备，进而轻松保护许多应用。解锁后，员工只需触摸即可打开应用，打开的时间长度为所设置的身份验证时段。通过将 Workspace ONE 与 VMware Identity Manager 和 AirWatch 相结合，可跨桌面、Web 和移动环境打造业界领先的无缝用户体验。使用在用户、设备、应用和企业之间建立信任的正在申请专利的 Secure App Token System (SATS)，可单点登录 (SSO) 到公共移动应用。
身份验证代理 可利用新的和现有的第三方身份验证方法	Workspace ONE（含 Identity Manager）包括支持第三方身份验证服务（例如 Radius、Symantec、RSA SecureID、Imprivata Touch and Go 等）的身份验证代理。

可自主选择使用任何设备；自带设备 (BYOD) 或企业所有设备

您当下所部署的体系结构可以与未来的设备配合使用。从可穿戴设备到 3D 图形工作站，保持员工高效工作意味着他们的应用需要随时随地可供使用。

然而，其中一些设备可能是企业拥有的设备，需要 IT 部门在设备的整个生命周期内进行配置和管理，而其他很多设备则为员工自带设备。VMware Workspace ONE 使员工能够选择符合其工作方式的便捷性、访问、安全性和管理级别，使他们能够无障碍地采用 BYOD（自带设备）计划，同时可使 IT 部门摆脱设备管理工作。

功能特性	说明
新设备调配功能利用操作系统管理界面自动配置笔记本电脑、智能手机和平板电脑，让它们马上可以供企业使用	通过 VMware Workspace ONE 统一管理平台可实现自助式地配置新购设备。 AirWatch 设备管理利用 Apple iOS 和 OSX、Microsoft Windows 10、Google Android 以及适用于加固设备的各种专门平台提供的企业级移动管理 API 来调配、配置和保护应用及设备。 这还允许设备通过操作系统供应商接收补丁程序，以便以最快的速度处理漏洞，同时将配置和应用管理工作留给 IT 部门。

保护可提高工作效率的应用： 邮件、日历、文档和聊天

Workspace ONE 包含员工希望使用的电子邮件、日历、联系人、文档、聊天和企业级社交应用，而且，采用对用户不可见的安全措施限制附件及文件的编辑和共享方式，从而避免组织出现数据泄漏情况。

远离“围墙隔离的花园”；支持员工实时协作的小组聊天、企业讨论、答疑、内容访问和其他社交工具均可集成到员工现已使用的应用和工具中 — 从提高工作效率转变为真正提高员工敬业度。




功能特性	说明
易于使用的电子邮件应用 尽管它是为企业设计的，却有着能让使用者感到满意的易用性	支持 Gmail、Exchange、Outlook、Yahoo、Hotmail、iCloud、Office 365、IMAP 和 POP3 邮件帐户的更快、更智能的安全电子邮件应用。通过集成到您最常用的服务 （例如 Dropbox、Box 和 Evernote），可以比以往更具条理性。
利用与电子邮件**集成的日历**，可以轻松地设置会议	通过集成电子邮件和日历，您在收到会议邀请时不再需要退出电子邮件应用。只需单击几次，即可查看、响应会议请求或根据您的时间提议新时间，而不必在各应用之间导航。
高级电子邮件附件安全功能可减少数据泄漏	通过使用 AirWatch 安全电子邮件网关保护电子邮件和附件，该网关可实施企业级加密、擦除和“打开方式”控制，从而确保附件安全。
内容管理应用允许业务线在设备上推送和管理安全内容	AirWatch Content Locker 移动应用允许 IT 部门跨各种内部存储库和外部云存储提供程序将文件直接提供给设备，以确保员工获得最新信息。
可提高员工参与度的**企业级聊天功能**	通过集成到现有企业级应用，同时提供可自定义的移动优先聊天和通知体验，安全的企业级聊天平台可连接记录系统。

借助条件访问实现数据安全性和端点合规性

为了保护最敏感的信息，Workspace ONE 整合了身份管理和设备管理，基于一系列与身份验证强度、网络、位置和设备合规性有关的条件强制实施访问决策。

功能特性	说明
整合了身份管理和移动管理的**合规性检查条件访问**策略实施	通过 Identity Manager 配置对移动、Web 和 Windows 应用进行的应用级条件访问策略实施，以便按网络范围或通过 AirWatch 施加的任何设备限制（root 设备、应用黑名单、地理位置及其他）实施身份验证强度和限制访问。
由 AirWatch 提供支持的 **设备管理与合规性**	自动满足设备合规性以提供高级数据泄漏防护，包括阻止 root 设备或越狱设备、白名单和黑名单应用、“在应用内打开”限制、“剪切 / 复制 / 粘贴”限制、地理围栏、网络配置以及通过 AirWatch 策略引擎实施的各种高级限制和策略。
应用和设备分析 可提供实时可见性	记录应用、设备和控制台事件以捕获有关系统监控的详细信息，并在控制台中查看日志或导出预定义报告。
与 VMware NSX 集成的 **智能网络**	作为附加功能提供的 VMware NSX（含 AirWatch）隧道可进一步将来自应用的流量分离到数据中心内的具体工作负载中。这可显著减少会对组织造成严重损害的 恶意软件 / 病毒的攻击途径。

实时应用交付和自动化

Workspace ONE 充分利用 Windows 10 的全新功能，并采用业内领先的 AirWatch 移动管理系统，使桌面管理员可随时自动分发和更新应用。该产品整合了屡获殊荣的 Horizon 虚拟化技术，并可自动执行应用交付流程，从而可以提供更好的安全性和合规性。

功能特性	说明
远程配置管理允许员工从任意位置调配新购设备	Workspace ONE（含 AirWatch）配置无需使用笔记本电脑映像，并为员工提供了即时可用的顺畅体验。 根据动态智能组管理配置，动态智能组可考虑设备信息和用户属性并随着它们的更改而自动更新。
通过 AirWatch **分发 Windows 软件**以自动完成软件生命周期管理	AirWatch 软件分发允许企业自动安装、更新和删除软件包，并且还提供了脚本编写和文件管理工具。为软件、应用、文件、脚本和命令创建自动工作流，以在注册过程中或按需在笔记本电脑上安装和配置。 凭借 AirWatch，您还可以将软件包设置为根据条件（包括网络状态或定义的时间表）进行安装，自动部署软件更新并在更新发布时通知用户。
通过 Horizon **部署虚拟应用和桌面**以提供安全的托管桌面和应用	Horizon 提供安全的托管虚拟应用和桌面，允许用户处理高度敏感的保密信息，而不会泄露公司数据。 用户可以使用任何设备类型在任意位置访问虚拟应用和桌面，从而可以灵活地在任意位置高效工作。
资产跟踪通过单个视图提供公司代管设备详细信息，无论这些设备位于何处	Workspace ONE（含 AirWatch）允许管理员远程监控和管理所有连接到您企业的设备。因为 AirWatch 是多租户，所以您可以在一个控制台中管理不同地理位置、业务部门或其他分部门的设备，然后使用基于角色的访问控制功能定义和委派管理权。
利用**远程协助**，可以轻松地支持员工	Workspace ONE（含 AirWatch）远程协助功能可为终端用户提供远程协助和故障排除方面的支持。要收集有关设备的信息，请执行设备查询以收集最新的配置文件列表、设备信息、已安装的应用和证书。要帮助进行故障排除，请远程访问文件系统日志和配置文件以对问题进行诊断。远程查看命令使 IT 管理员能够请求用户共享设备屏幕。

了解更多

如需进一步了解 VMware Workspace ONE，请访问 http://www.vmware.com/products/workspace-one/。要购买 VMware Workspace ONE 或任何 VMware 移动商务解决方案，请拨打 010-59934306、

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

有关详细的产品规格和系统要求，请参阅相关产品 文档。

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
中国北京海淀区科学院南路 2 号融科资讯中心 C 座南楼 1 层 邮编：100190 电话：+86-10-5993-4200
中国上海办公室 上海市淮海中路 333 号瑞安广场 15 楼 1501 室 邮编：200021 电话：+86-21-6034-9200
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 © 2014-2015 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 产品受 http://www.vmware.com/cn/support/patents 网站 列出的一项或多项专利保护。VMware 是 VMware, Inc. 在美国和 / 或其他法律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：VMW9528-DS-VMW-ID-MGR-DGTL-WKSPC-A4-101 01/16