统一端点管理：确保数字工作空间的安全与生产率

工作方式的概念已经从“员工在 IT 部门分配的 Windows 系统台式电脑与笔记本电脑前工作”，进化为“移动用户借助漫游服务使用个人台式电脑、平板电脑及智能手机边工作、边娱乐”了。十年前，各企业通常会选用 Microsoft SCCM 与 LANDESK 等“客户端管理工具”(Client Management Tools, CMT)，管理几十、几百或几千个 IT 分配式 Windows 系统。但是，在这个移动设备、自带设备(BYOD)及物联网(Internet of Things, IoT)得到广泛应用的时代，CMT 远远不能满足需要。

相反，随着 IT 企业不断增多，未来将会主要依赖“统一端点管理”(Unified Endpoint Management, UEM)，因为 UEM 能够将“客户端管理工具”(CMT)与“企业移动化管理”(Enterprise Mobility Management, EMM)整合在一起，通过单一界面就能管理、保护各类设备与操作系统——无论是台式电脑、笔记本电脑、平板电脑，还是智能手机，或是 IoT 设备。UEM 将会越来越多地关注用户，而不像管理者那样将重点放在个别设备上。对于用户来说，UEM 能够帮助他们实现一种能够确保简便、一致协作的、能够从任何设备进行信息访问的统一工作空间。

根据 Forrester 报告，现在 15%的企业采用了 UEM 解决方案，但到 2020 年，将会有 54%的企业采用 UEM 解决方案。各企业步入移动化、全球化占主导地位的时代后，就需要考虑是否从独立的 CMT 与 EMM 平台部分或全部转型至采用单一的 UEM 工具，因为通过 Citrix Workspace 交付的 UEM 让这一切成为可能，并且变具有实际意义。

在未来几年内，各企业还需要进一步扩展统一管理解决方案，以纳入新兴的企业物联网(IoT)，包括传感器、信标(beacon)以及其他类似设备。幸运的是，通过 Citrix Workspace 实现的 UEM 已经包含了 IoT 设备。

为什么选用通过数字工作空间实现的 UEM？

通过数字工作空间实现的 UEM 对于多数企业来讲理具实际意义，这样说是有原因的。

简单：CMT 与 EMM 工具采用了完全不同的工作方式，因此，各企业需要为他们分别设立工作团队，并分别进行培训。通过单一界面对所有设备进行“傻瓜”式管理，对于逻辑业务来说具有重要意义。与购置两套或三套管理工具相比，单一的管理工具能够节省大量投资，不仅如此，由于减少了工作人员的配置与培训，还能节省大量的运营成本，让企业能够充分利用现有人力资源做更有战略意义的事情。

一致：对于确保企业用户的生产率与信息保护来说，保持管理、安全与可用性方面的一致性非常重要。即使在设备、应用与信息之间存在意料之外的、非常微小的安全防护差异，也会导致安全基础架构产生漏洞，使黑客或恶意软件得到可乘之机，威胁到企业的安全。对于提高用户生产率来说，保持移动设备访问各类应用时的一致性也非常重要。UEM 能够以多种方式保持一致性：

- 与采用两套相互独立的工具相比，采用一套 UEM 解决方案本身就有利于企业跨越所有设备与用户实施一致的管理与安全政策。
- 采用单一的管理平台，不仅利于保持用户帮助台(Helpdesk)服务与系统故障排查服务的一致性，而且还有利于保持此类服务与 Windows 10 等能够兼容各类设备的操作系统之间高度的一致性。
- 采用单一的管理平台，能够以更加简便的方式提供综合性更高的报告，这在规划、计算硬件成本以及软件升级或更新成本时非常有用。

- Windows 10 自身采用了与常用操作系统、应用开发工具之间保持一致性的规范，以及一套能够跨桌面设备、移动设备的 API。用户能够从单一的、经企业核准的、安全的应用商店获取设备所需的所有应用，并且能够以高度一致的方式，通过企业网络在自己的设备上使用企业的应用及信息进行工作。
- 利用通过 Citrix Workspace 交付的 UEM 解决方案，客户能够对过时的 Win 32 应用进行全寿命周期管理（例如：应用的开发、配置与卸载，是否需要）

适于移动设备的管理方式：在过去，设备大都是企业分配的、与企业 LAN 相连接的固定设备，采用 CMT 工具时，需要先将台式电脑与笔记本电脑通过 LAN 连接起来，并利用一系列组策略对象搭建企业域进行初始配置，之后才能进行管理。一般来说，用户自己都不能连接、配置或升级自己的设备。这些都是最终的超级用户——IT 部门的工作。

采用过时的 CMT 解决方案时，IT 需要花费大量的时间创建一套或多套定制的系统映像，并通过 LAN 将其推广至几个、几十个或几百个连接台式电脑与笔记本电脑的网络，或者采用价值 25 美元/系统的映像部署服务。采用这种方法，在扩增新设备或更换遗失笔记本电脑时，需要安装所有必需的应用，这是一个既耗时又耗费资源的过程，严重降低的用户的生产率。此外，CMT 应用的发布也需要由 IT 部门负责，并且需要使用很多非常复杂的软件发布包。

相比之下，UEM API 及工具的设计从一开始就支持移动漫游，即用户能够通过自己选择的任何设备实现无线连接。用户可以购买已经预装操作系统与应用的设备，之后通过无线连接，使用企业 UEM 门户与配置应用程序，按照企业的设置与策略，自己完成设备的登记与配置，几乎无需 IT 介入或提供协助。

用户还可以通过企业的应用商店门户下载并安装经 IT 核准的各类应用。企业现大多都已采用了云端 SaaS 以及虚拟应用，因此一般情况根本无需下载应用。如果必要，IT 还能向成百上千的全球漫游设备推送各类应用与更新。

几年前，操作系统与应用的升级还不那么频繁，时间密集性与资源密集性很高，对 LAN 的依赖也很高。但如今，移动操作系统将更多的依赖云服务模型运行，更新的规模越来越小、频率越来越高，这种做法对于移动漫游用户来说非常实用。

容器化

UEM 与移动操作系统 API 能够以多种方式实现“自带设备”(BYOD)以及“企业设备自用”(Corporate Owned &Personally Enabled, COPE)的工作方式，其中一种实现方式就是容器化。利用应用封装、加密及其他类似方法，IT 能够按企业安全策略将设备上的企业应用、个人应用以及数据相互隔离，从而禁止或限制他们之间的交互。

容器化还能实现恶意软件防护以及“数据泄漏防护”(Data Leakage Prevention, DLP)。由于设备上的企业应用与个人应用相互隔离，使用个人应用或浏览器下载的任何恶意软件都不能影响容器化的企业应用，也不能通过联网的设备传送至企业网络。大多数 UEM 解决方案还能在特定的企业应用接入企业 LAN 时，通过自动启用该应用“虚拟专用网络”(Virtual Private Network, VPN)强制实施这种隔离。VPN 仅能连接单个应用，而不是整个设备，能够将个人应用产生的所有恶意软件拒之门外。

同样，大多数操作系统 API 及 UEM 系统都容许 IT 通过配置、强制执行一定数量的策略来限制用户从企业应用到个人应用的进行数据剪切、粘贴操作，或将企业数据、文件粘贴或附加至个人电子邮件信息中，或打印包含敏感信息的文件。

采用 Windows 10 台式电脑、笔记本电脑以及 UEM 后，强制采用“Windows 信息保护”对所有企业应用与数据进行加密，再通过数字化权限管理实现容器化。之后，IT 可利用各类策略防止用户剪切加密内容并粘贴至未采用 Windows 信息保护加密的、不受管控的应用中。对于通过 SharePoint 或共享网络等服务下载的任何数据，都会进行加密处理。

Windows 10 还提供了 IT 进行跨设备管理时所需的多种至关重要的企业管理功能。IT 能够通过 Azure Active Directory 或第三方 UEM 解决方案，向下推行并强制执行大量的策略与设置，强制使用密码及加密，实现新设备的自我登记，独立于用户安装的应用管理企业配备的应用，通过.msi 软件包分配 Windows 32 应用，强制执行并部署更新，并阻止访问危险网站——所有这些操作都不必接触连接至企业 LAN 的设备。对于不能通过上述方法利用的 Win32 任何应用，都可以通过 Citrix Workspace 的桌面虚拟化解决方案部署到移动设备上。所提供的全部管理功能可能不能完全匹配 CMT 提供的管理功能，但已提供了大多数至关重要的以及广泛使用的管理能力，并且还会不断改进。

从 OS X Lion 开始，苹果也已开始为台式电脑操作系统提供与 iOS 大体相似的、基于策略的、自主登记式管理 API，并且在 macOS Sierra 中会得到更多地应用。

Citrix UEM 解决方案

Citrix XenMobile 是用于管理多种平台的一种综合性集成 UEM 解决方案，可管理的平台包括 iOS, Android、Windows 10 以及 MacOS 设备，包括台式电脑、笔记本电脑以及 Chromebook 网络笔记本。作为 Citrix Workspace 的一部分，XenMobile 将 UEM 与各类应用及桌面虚拟化、文件同步及共享、安全网关服务以及对 Offie 365 的安全与生产率提升功能都整合在一起。

Citrix mVPN 帮助阻止受到恶意软件感染的应用访问防火墙之后的资源，在应用层分配唯一的“移动设备标识符”(Mobile Device Identifier)，而不仅是在设备层进行监控、过滤或阻止个人连接或设备。这种集成能够让用户通过一个统一的应用商店访问各类应用，不仅包括 Office 生产率应用，还包括用户数字工作空间所需的其他所有应用，如旧版 Windows 应用、SaaS、Web 以及移动应用。

通过 Citrix Workspace 交付的 XenMobile，能够立即为所有刚引入的操作系统企业管理 API 提供支持，而且会提供越来越多的支持，此外，XenMobile 还会添加自己独有的、跨设备操作系统确保一致性的各类功能，包括完全符合 FIPS 140-2 的 AES 256 位加密；自有的、能够驾驭各操作系统 API 提供的容器化功能的 MDX 容器化功能；以及自有的、为保护相关敏感信息而利用必要的策略与容器化战略封装个人应用的工具包及 SDK。

这对于 Citrix Workspace 来说非常重要，因为 Citrix Workspace 需要在向用户提供无缝、高效体验的同时，还需要为企业提供一致的、必要的保护。

Citrix Workspace 自己也能提供跨 iOS 与 Android 的移动企业层安全应用，如 Citrix Secure Mail 与 Citrix Secure Web。

Citrix Secure Mail 是一种企业电子邮箱客户端与个人信息管理器，具有与设备自带电子邮件客户端解决方案相似的用户友好型界面，并且在企业设置项里还增加了几十种用于提升安全性与可用性的功能。

使用 Secure Mail 时，会在设备上完全独立于个人应用保存所有企业邮件、联系信息及日程信息。 当用户登录 Secure Hub 后，可通过单点登录的方式访问 Secure Mail，并且 Secure Mail 还能提供多因素身份验证、远程擦除以及转发加密与休眠加密功能。IT 还能对电子邮件的附件、打印以及从其他应用剪切粘贴信息等强制施加限制。

Secure Mail 与企业自有“数据泄漏防护”(DLP)工具相整合，能够监控、限制从企业电子邮箱向外发送的内容。Secure Mail 还能提供出色的便捷功能，如查看受邀参加会议的人是否有时间、在线或电话会议新邀请函内的连接提示、一键参加在线会议等。

Secure Mail 与 Secure Web 移动应用紧密集成，确保所有电子邮件的 Web 链接都在沙箱式安全 Web 浏览器环境中打开。Secure Mail 还与下文所述 Citrix 自有 ShareFile 文件同步与共享应用紧密集成，确保在电子邮件中仅嵌入 ShareFile 链接，而不是文件附件，以严格控制内容共享。

Citrix Secure Web 是一种安全浏览器替代方案，IT 能够使用它设置 Web 浏览策略与限制，特别是在连接至企业网络及内网时。企业可通过策略监管用户能够访问或不能访问的网页、控制企业防火墙代理访问内容、分析并过滤 URL 以确保其安全。

Citrix ShareFile 是一种企业级安全移动文件同步与共享应用，其功能及便捷性同于或优于用户友好型的 Box 及 DropBox，但具备企业级安全及管理功能。并非强迫用户将所有信息保存在云端，企业可利用 ShareFile Storage Zones 选择将共享文件保存在防火墙之后的本地设备、Citrix ShareFile 云服务或其他公有云服务下。ShareFile 能够将文件保存在基于网络存储系统的内部 CIF 上，并提供 Windows 网络共享及 Microsoft SharePoint 接口，以免在共享时还得将文件迁移至其他服务下。ShareFile 还提供了便利的全功能拖放解决方案，以方便新手在各类设备上创建、编辑及保存基于移动表格的应用。ShareFile 能够帮助企业快速实现手工工作及流程的数字化与自动化，清除重复数据输入、减少文书工作。

更重要的是，ShareFile 能够利用 Citrix XenMobile 强大的安全与管理功能，保护企业数据、无缝整合其他 XenMobile 功能以及生产率应用。

Citrix Secure Hub 是 Citrix 的应用商店，企业可在这里提供仅限访问安全应用的单一应用商店、其他移动应用（第三方开发或企业自己开发的商用应用）、Web 与 SaaS 服务，甚至是基于 Active Directory 组策略的 Windows 桌面及应用。

Podio 是一种强大的、免费的、基于企业云的移动协作平台，能够整合团队会话、流程及内容共享，并且能够与 Citrix XenMobile 安全与管理功能紧密集成。与价值数万美元的企业解决方案相比，Podio 能够提供同等或更好的协作功能。

Citrix Workspace 还可将移动管理扩展至新兴的、基于 IoT 的工作场所，利用各类情境感知环境并结合不同来源的数据，对用户需求作出回应，提高工作效率与生产率。Octoblu 软件可用于创建工作场所自动化服务，如在用户到达工作站时启动个性化桌面；调整暖气、冷气、灯光；当员工进入会场时启动 GoToMeeting 或 Skype 开始会议；利用信标将用户自动连接至附近的打印机。IoT 可实现无限可能。

总结

使用 Windows 10 及 MacOS Sierra，可以为所有端点、设备及应用交付单一的“统一端点管理”(UEM)能力。详细检查这些解决方案，你就会发现 UEM 不仅能够简化管理、大幅削减管理成本、简化移动工作场所、确保移动工作场所安全，还能帮助你的组织步入物联网时代。

使用 Citrix Workspace 交付 UEM 能够简化移动用户管理，并通过跨所有应用的身份管理与身份联合集中管理混合云服务。Citrix Workspace 能够帮助 IT 统一端点管理及访问管理，并且还能帮助 IT 进行深入的性能了解。整个工作空间采用了 Citrix 独有的情境安全技术，能够跨越所有基础架构、应用、网络以及设备进行端到端分析，提供无可比拟的监控功能。从你的最终用户来看，Citrix Workspace 能够为他们提供单点登录，便于他们在任何端点根据生产与协作需要，访问各类应用与数据。只有 Citrix 才能提供集成了管理、安全、应用、桌面虚拟化、移动协作以及企业物联网实现功能的全套 UEM 解决方案。

“工作空间即服务”让你集中 IT 管理、简化升级、节省基础架构成本，确保你能够以更少的投入做更多的事。只有云技术才有可能让你根据业务需要灵活扩增或缩减基础架构。在员工入职时增添新实例，在离职时删除。以服务形式交付 Citrix Workspace 是最快、最简单、最灵活、最安全的数字工作空间技术交付方法。

企业销售
北美 | 800-424-8749
全球 | +1 408-790-8000
位置
公司总部 | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
硅谷 | 4988 Great America Parkway Santa Clara, CA 95054, United States