CITRIX

白皮书

最佳实务：简便、安全的设备管理

实现企业生产力自动化
为员工提供自由选择权
让 IT 实现全面安全防护与控制

员工选择已经成为了现代化 IT 战略的基石。通过让员工选择自己所需的最佳设备，企业能够提高生产力、灵活性以及工作满意度。选择恰当的战略，IT 能够确保采用恰当的策略与技术，从而能够保护企业信息，同时还能降低成本，并提供更好的用户体验。

你的战略应该能够让你的组织：

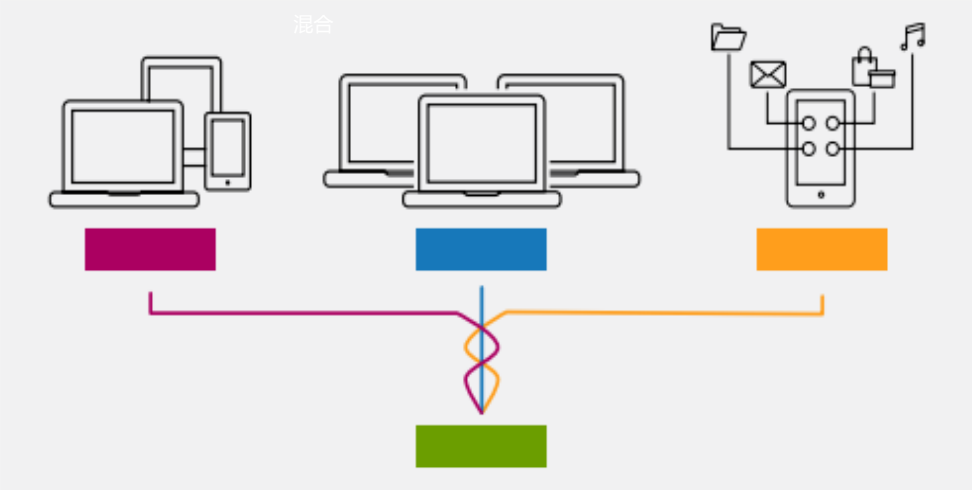
- **为员工赋能** -- 让员工可以选择自己的设备，从而改善生产力、协作能力并促进移动化。
- **保护敏感信息** -- 防止敏感信息遗失，同时解决隐私保护、合规以及风险管理等问题。
- **降低成本、简化管理** -- 通过自助配给、自动化管理与监控降低成本、简化管理。
- **简化 IT 工作** -- 采用一套综合解决方案管理并保护各类数据、应用及服务。

为同时实现员工工作简化以及 IT 安全、控制及管理效率提升，在设计相应战略时，可参照以下 8 项最佳实务：

1. 策略选择

移动化与消费化是大势所趋，IT 变革势在必行，一方面需要推行自由选择，另一方面需要加强 IT 控制，为将两方面任务结合在一起，可考虑下述策略：

- 自带设备（Bring-Your-Own-Device ，BYOD）：让员工使用个人设备工作。
- 自选设备（Choose-Your-Own-Device，CYOD）：允许员工从公司提供的各类设备中选择一种进行工作。
- 公司所有、个人使用（Corporate-Owned, Personally Enabled，COPE）：让员工从公司指定的设备中选择一种运行个人及公司应用。
- 混合方法 :根据不同的用户及分组采用恰当的组合以实现移动化。例如 ,将 COPE 与 CYOD 或 BYOD 相结合。



虽然各策略之间存在着细微差别，但其包含安全防护在内的根本原则都是“统一端点管理”（Unified Endpoint Management，UEM）。主要差别仅是成本。

BYOD 用户自己承担设备及数据流量套餐成本，公司有时会以提供津贴的方式部分或全部报销。对于 COPE 及 CYOD，公司会支付设备及数据流量成本。BYOD 策略可以还需要解决 COPE 与 CYOD 之外的问题，如员工在下班后或休息日查看电子邮件时是否按加班计算等。

2.资格与登记

明确规定谁可以使用个人设备，临时作为公司端点的补充还是永久替代公司设备，或是阶段性替代。可以将这种资格视为一种需要争取的特权、对员工需求的回应、对特定岗位的要求、特定使用例下的附加风险，或者综合前述因素进行确认。

可能通过确立某些准则的方式确定使用资格，如岗位类型、差旅频率、绩效或离线访问敏感数据的需求等。但是，应该为资格给出相对宽泛的定义，让主管有权最终决定哪些团队成员能够获得相应津贴。主管也可以在执行其他部门激励、特权以及纪律措施的基础上适用 BYOD、COPE 或 CYOD 相关规定。

对于承包人，最好是选用 BYOD。很多企业本来就希望承包人自己携带设备，这样还有助于独立承包人的合规管理。

3.允许使用的设备

为防止设备种类繁多导致失于控制，你可以限定公司所支持的移动设备类型。策略的详细程度取决于具体的用户需求、安全风险以及支持资源。总体来说，在策略中对设备类型、操作系统版本、型号规定的越细致，就需要在恰当测试与支持指定设备方面耗费更多的资源。

为了明确所有权，BYOD 参与者应该通过正常消费渠道而非企业的采购部门购买个人设备。你可以尝试着借助公司的供应商关系资源为员工争取一些折扣。

有些员工可能还想添加一些辅助设备，如显示器或键盘。在这种情形下，你应该明确由谁来负责采购以及谁享有所有权。

4.推行

成功实施的关键在于沟通。为员工提供一份指导，帮助他们决定是否参与相关计划以及了解如何根据自己的需求选择恰当的设备。还应该让他们了解如何访问、使用、存储数据，如何就非托管消费者应用及服务等创建、使用工作账户。

应该严格隔离工作及业务相关数据，以确保符合电子取证以及数据留存相关要求；同样，不得通过个人账户发送工作电子邮件。适用于公司设备的使用策略也应该同样适用于 BYOD 设备。

另外，你还应该编制一套用户采用方案，帮助参与者快速参与并尽快适应。你可以向员工发送一份带有自助服务入口链接的电子邮件，帮助他们尽早适应并提高生产力。

5.成本分担

BYOD 带来的一项好处就是降低成本，因为在该模式下，员工会承担与工作所用个人设备相关的部分或全部成本。公司一般会以津贴的方式报销 18%到 20%的设备成本。参与者应该知晓任何津贴都应该缴纳相应的个人所得税。在个人所得税较高的地区，你可以相应的提高津贴数额，以确保为所有员工提供的补助净额都相同。

在选择提供补助时，应该确保每个员工的全周期参与。应该以定期发放补助的形式确保个人设备的使用周期不会超过公司同等设备的预期使用寿命。如果员工在 BYOD 适用周期内离开公司，那么你可以索回部分津贴。

记住，在企业内推行 BYOD 计划时，成本分担会产生很大影响。以“一刀切”的方式突然推行时，员工会在一开始以及每个更新周期的开始阶段，一起登记并申领相应津贴，从而会导致在这些时点上成本迅速增加。应该让员工根据自己设备的使用寿命参与计划，这样就可以在一定程序上缓解此类影响。另外，当企业不提供津贴时，也会导致员工一窝蜂地参与进来。

此外，在推行 BYOD 策略时，无论是否分担成本，都应该明确规定由谁来承担在公司防火墙之外的网络接入成本，包括移动网络、公共 Wi-Fi、家用宽带等。

6.安全与合规

无论是员工自有设备还是公司所有设备，最重要的一项要求就是在不影响用户体验的前提下保护数据。当在计划中允许员工将个人应用与数据用于工作时，可以通过“移动应用管理”（Mobile Application Management，MAM）将个人、公司应用及数据与公司内容隔离开来。

在个人设备上安装公司应用会增加风险。但是，将统一端点管理、应用与桌面虚拟化以及安全文件共享整合在一起后，就不必再担心此类问题了。商业信息会安全地保存在你的数据中心或云上。当确实需要在移动设备上保留数据时，你可以通过容器化、加密以及远程擦除等机制保护公司数据。你还可以禁用打印或客户端存储（如本地驱动器及 USB 存储器）访问。

你还可以根据设备所有权、状态或位置，采取一定的策略来控制并保护应用与数据访问。登记、管理所有设备；设定密码要求；检测越狱设备；对不合规、遗失设备或离职员工或解雇承包人的设备进行全面或选择性擦除。通过应用通道访问、黑名单、白名单以及动态、上下文情境感知策略等确保应用安全。

为保护网络安全，你可以采用“网络访问控制”（Network Access Control，NAC）技术验证接入网络的人员身份、核实相关设备是否安装了最新版的杀毒软件以及安全补丁。

在防火墙之外，虚拟化与加密能够缓解大部分安全漏洞威胁，包括 Wi-Fi、WEP 加密、开放无线网络、3G/4G 及其他消费级访问方法。各类网络安全能力可深入了解并预防种类内、外移动化威胁；阻断非法设备、未授权用户及不合规应用；并可与“安全信息与事件管理”（Security Information and Event Management，SIEM）系统相整合。

IT 应该准备一套立即终止数据与应用访问的机制或措施，包括自动解除工作相关 SaaS 账户配给、选择性擦除等，以应对 BYOD 参与者离职、违规或个人设备遗失等情形。此类机制对于 COPE 或 CYOD 设备来说也同样重要，另外还应该采取措施防止在重新分配的公司设备上存有接手用户无权访问的数据。

为防止员工随便使用任何设备访问公司应用或数据，部分公司会采用一定的管控措施，不允许随便使用 BYOD。在这种情形下，由 IT 直接管理个人设备，包括登记、验证、授权以及设备资源访问等。

7.监控与管理

对于确保策略合规以及投资收益确认来说，持续监控与管理至关重要。

有些 UEM 解决方案能够通过部分监控与管理的自动化，提升 IT 的生产能力及效率，如针对各类违规指定相应措施。此类措施可能包含设备的部分或全部擦除、将设备认定为不合规、回收设备、通知用户限时改正（如删除黑名单中的应用）以及其他更为严格的措施。

8.设备支持与维护

由于设备为用户自有，因此 BYOD 计划通常会减少 IT 的维护任务。如前所述，此类策略应该明确如何解决各类支持与维护问题、如何承担相关成本等，以尽量避免给 IT 增加工作负担或工作复杂性。在大多数的 CYOD 或 COPE 计划中，IT 仍会全面负责设备的支持与维护。

如何通过 Citrix Workspace 实现安全的设备管理

任何设备管理计划都必须包含安全访问在个人设备上保存的公司应用与文件的技术。Citrix Workspace 拥有公司实施安全、简便、高效 BYOD、CYOD 以及 COPE 策略时所需的各类关键能力，包括统一端点管理、Windows 桌面与应用虚拟化、安全文件共享、应用交付等，从而让你能够在保持一定的安全与控制水平的前提下，为员工使用的任何设备交付企业应用与数据。

统一端点管理

采用 Citrix Workspace，你可以实现基于身份认证的应用、数据及设备配给与控制、退出用户账户自动解除配给、选择性擦除遗失设备。采用 Citrix Workspace，你不仅能够管理包括物联网设备在内的各类设备，还能在应用层级执行安全与控制措施，从而能够在不影响在 BYOD、CYOD 或 COPE 设备上使用个人内容的情况下，恰当保护公司数据。利用 Citrix Workspace 端点管理

你能够选择最恰当的 MAM 战略，包括 Samsung KNOX 或 Appconfig、Citrix MDX（能够在不登记设备的情况下，另行提供一道应用加密）或 Intune MAM。

Windows 桌面与应用虚拟化

你不必再在每个个人设备上安装、管理 Windows 应用与桌面了，你可以按需为任何设备交付各类服务。由于是在数据中心或云端管理各类应用与数据，因此，IT 能够在适用于公司设备的统一环境下，集中地对个人设备提供数据防护、进行合规管理、访问控制及用户管理，与管理公司设备一样简便。

应用商店

员工通过简单的点击，就可以在统一化的应用商店内访问各类移动、Web、SaaS、企业以及 Windows 应用了。无论员工选用哪类设备（Windows 或 Mac 电脑、iOS、Android、Windows 移动设备或 Google Chromebook）、在什么位置或使用什么网络，都能获得一致的用户体验。

安全访问

借助于统一管理框架，IT 能够对任何设备上的应用、桌面及服务访问进行保护、控制及优化，同时还能利用审核与报告功能来提升合规与数据防护水平。仅 Citrix 能够在移动设备与防火墙后的公司资源之间提供独特的微型 VPN，进一步为应用数据提供保护。

安全数据共享

员工能够安全地与公司内、外的任何人共享文件、进行协作，并且还能跨设备实现文件同步。基于策略的访问控制、审核、报告以及远程设备擦除等功能可为业务内容提供进一步的保护。

采用最合适的策略与技术，你能够恰当平衡员工选择自由与 IT 安全管控。如欲利用 Citrix Workspace 实现简便、安全的设备管理，请登录 www.citrix.com/workspace 了解详细信息。

CITRIX®

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

© 2018 Citrix Systems, Inc. 版权所有。本文件所用 Citrix 字样、Citrix 标识以及其他标志均为 Citrix Systems, Inc.与/或其子公司已在美国专利与商标局或其他国家注册的智慧财产。其他标志均归各自权利人所有。