Ivanti 白皮书

允许用户随时随地高效工作的统一端点管理

ivanti

目录

简介

移动设备和 IT 消费化在如今的企业中已经大行其道。如今的用户期望能够随时随地使用各种设备来完成工作，从台式机到笔记本，再到平板电脑和智能手机。根据 *Information Week* 在 2015 年发布的“State of End User Computing”（最终用户计算状态）报告，61% 的受访企业都支持他们的用户将自己的设备连接到企业网络中。40% 的企业为超过 25% 的员工提供 iPhone，而 25% 的企业则提供 Android 手机，10% 提供 Windows 手机，15% 提供 iPad，还有 10% 提供其他平板电脑。[1]

曾经最“严肃”的工作都是用笔记本电脑或台式机完成的，而移动设备仅仅用来查收电子邮件以及在路上或家中完成其他有限的一些工作。如今，用户期望能够在任何设备上都访问到相同的信息，运行许多相同的应用程序和服务，并完成更多同样的工作。同时，许多移动设备已经跨界到了以前被划归给笔记本电脑的领域。根据 *Information Week* 的报告，52% 的受访企业都希望大多数最新的应用程序能够提供 HTML 和移动设备支持。[2]

这种“移动设备平等”的概念对企业提出了巨大的挑战。IT 部门必须实施策略来管理和保护每台设备上访问和存储的敏感应用程序和信息，而又不能损害用户的工作效率，也不能影响他们最喜欢的移动工作方式和对设备的个人使用。不幸的是，如今的许多企业中，端点管理和安全工作都跟不上设备平等的脚步。

数据违规时代的战略缺陷

大部分企业都针对台式机和笔记本电脑部署一套管理系统或一组管理系统，而对智能手机和平板电脑这种移动设备则部署完全独立的另一套管理系统，采用独立的供应商，执行独立的管理战略。在许多情况下，都有两名不同的 IT 人员分别负责关注移动设备和传统的端点系统，同时又使用不同的管理工具来开展工作。

这样的战略存在一项严重的缺陷，尤其是在如今这样一个数据违规频率不断升高、破坏性不断增强的时代。移动设备容易丢失和被盗，从而使得它们以及所访问的企业应用程序和数据容易遭到危害。根据安全供应商 Bitglass 进行的调查，68% 的医疗保健安全违规都是因为移动设备或文件的丢失或被盗而引起的。[3]虽然移动恶意软件尚未造成严重的威胁，但这也是一个侵入公司网络的潜在入口，只是尚未被大规模利用而已。而除了丢失、被盗以及恶意软件之外，部署两套不同的管理系统来管理不同的设备也是一项严峻的挑战，将产生重大的影响。

统一的最终用户体验

针对 PC 和其他移动设备部署两套完全独立的管理应用程序和战略使得 IT 部门难以为用户提供在各种设备上统一一致的用户体验，而用户们却对此翘首以盼。登记、部署和支持多台设备也可能无谓地变成一个复杂而耗时的过程。一套更简单的解决方案应该允许用户根据自己的权限，通过单一的界面来自行部署*任何*新设备，并且针对每台设备提供特定的应用程序和资源。

统一的用户策略

保护敏感的企业信息和网络访问需要拟定一套严格的用户访问和安全策略。随着移动设备的使用情况变得越来越普遍而复杂，对于每位员工所使用的全部终端系统，IT 部门将难于拟定和部署一组统一的身份识别和访问策略以及策略框架。若要部署一套统一的策略，那么使用两套完全独立的管理系统，每套有自己的工作方式，则会把事情变得非常复杂，完全不如使用单一的统一端点管理 (UEM) 解决方案。而如果涉及两位独立的员工，那么事情复杂度更会大大加剧。

在许多公司中，IT 员工负责台式机和笔记本设备，而智能手机则归通信部门的员工来管理，他们掌握的技能迥异，在企业中的优先权不同，而他们自身的视角也不一样。这样安排的结果可能导致在策略创建和部署方面存在无法直观看到的缺口，从而导致给黑客和数据违规留下可趁之机。两种不同的管理平台也可能导致看起来相同的策略实际上存在些微差异，从而导致存在无法看到的缺口。

解决方案是用 UEM 系统创建一组用户访问和安全策略，并且一致而顺利地将其部署到所有用户设备上。比如，能够选择一位用户，应用一项策略或部署一款应用程序，而这一套系统能够理解要将上述这些变更应用到哪些设备上。

管理成本和资源

采用不同供应商、不同支持合约以及不同界面的两套独立管理平台必然耗费更多的时间、更多的培训以及更多的资源，在这方面单一平台具有天然的优势。当涉及两名不同员工时，所需的成本和资源甚至更高。相较于使用单一管理系统而言，不仅是登记、支持成本以及资源要求更高，任何对用户状态或访问权限的变更都需要在两套独立系统中进行策略变更，而这进一步加剧对资源的占用并且容易出错。

花费更多时间和资源来管理设备也意味着对能够增强业务的技术战略投入的时间和资源更少。如今技术变化的脚步很快，而它在企业竞争力方面起到的作用也越来越大，因此 IT 部门需要能够尽可能减少花费在日常管理任务上的时间

1. Wittmann, Art, “2015 State of End User Computing,” InformationWeek Reports，2014 年 12 月
2. 同上。
3. The 2014 Bitglass Healthcare Breach Report, “Is Your Data Security Due For a Physical?”

集成化的魅力

随着企业移动设备管理 (EMM) 平台在企业中变得越来越重要，其供应商开始兜售与现有台式机和笔记本端点管理平台相集成的概念。这是一个好趋势，但这种假想中的、在差异非常大的系统之间进行的集成无法如同单一 UEM 系统、界面和供应商关系那样获得同样的成本节约和易用性。而当情况变坏时，两套不同系统的供应商就会不可避免地互相推诿责任。

现实情况是，统一端点管理为每位*用户*的所有设备提供一组一致的策略和支持，而不是在移动设备和传统系统与设备之间人为制造隔阂。

这样的系统应当能够在所有设备上都提供以下功能：

系统管理，针对所有用户设备，覆盖所有设备的完整生命周期，包括设备发现和清单生成、操作系统映像、软件分发、支持以及远程控制。

安全实施，包括补丁管理、端点安全、软件分发、更新以及身份验证和访问策略实施。而针对移动设备，则在怀疑丢失或被盗后提供远程锁定和擦除功能。

资产管理，包括管理软件许可证、合约、保修以及租赁安排。

部署，包括用户为新设备和设备影像进行登记和注销。用户自助部署是很多移动设备管理 (MDM) 解决方案都提供的一项功能，因此全面设备管理解决方案也应当提供。

移动应用程序和数据

COPE（企业所有，个人使用）和 BYOD（携带自有设备）环境（在这些环境中，设备同时用于个人和工作用途）还存在其他重大问题。IT 部门做出任何会损害用户喜好的个人应用程序、原生用户体验以及网络浏览的尝试都只会遇到来自用户的阻力，而用户也会寻找变通方法来应对，这通常可能造成负面的影响，或者抵消 BYOD 或 COPE 策略的任何尝试所带来的优势。另外众所周知，消费应用程序和网络浏览行为中都充斥着恶意软件和其他危险，可能感染设备和企业网络，从而导致敏感的知识财产和客户信息被盗。

EMM 平台采用的常见解决方案是集装化，这会在设备上存储的企业和个人应用程序以及信息之间强制创建出隔离，因此企业信息无法被其他任何个人应用程序、浏览行为、软件（包括恶意软件）看到或访问。个人应用程序也无法看到或访问用户的企业联系人以及其他相关信息。

集装化通常会在每台设备上创建出完全隔离的企业和个人容器。不幸的是，这种方法被证实非常不便，并且对用户而言累赘不堪，他们必须不断在容器之间来回切换，而每次要进行工作时都必须登录到企业容器。

更方便的办法是“应用程序封装”，这将创建并强制隔离每个企业应用程序及其相关联的数据。因此用户可以随时访问设备上的任何应用程序，而不需要在互相独立的个人和企业容器之间来回切换并反复登录/注销。企业应用程序和数据始终都和个人应用程序以及可能存在的恶意软件互相隔离开来。理想情况下，应用程序封装应当是一种简单的流程，IT 部门只需要实施几个步骤，而且不需要编程。

EMM 包也提供了特殊的安全移动电子邮件和浏览器应用程序，企业可以要求员工始终使用这些应用程序来访问企业数据。但是，用户仍然抵触使用专门的电子邮件客户端。员工不希望放弃自己熟悉的原生电子邮件客户端以及它们的各种功能。他们也不想使用不同的电子邮件客户端来分别处理个人的和工作的电子邮件。更为切实可行的解决方案则是提供保护，允许用户使用他们偏好的电子邮件客户端，而不将企业信息暴露在危险中，同时提供安全浏览器，仅用于访问企业网络和应用程序。实际上设备上存储的电子邮件越少，安全性就越高。

理想情况下，所有这些应用程序和数据安全功能都应该紧密集成到同一套统一端点管理系统中，以便通过单一的屏幕、单一的一套企业策略来管理用户的笔记本电脑、PC 机、移动设备、应用程序以及信息归档，并开放通道让员工能够管理所有事务。

Ivanti 解决方案

用于管理用户设备的 Ivanti 解决方案消除了传统台式机和笔记本系统以及对应的移动设备系统之间的人为隔阂。它不要求企业和用户面对两套完全不同的管理系统所带来的问题，Ivanti 产品专注于统一端点管理，提供了单一的企业 IT 管理屏幕和一组策略来管理每位企业用户运行的所有设备的整个生命周期。使用 UEM 时，关注的是用户而不是设备。借助 UEM 方法，Ivanti 提供了市面仅有的全面管理解决方案，可在所有不同设备上为*用户*提供他们所期待的、相同而无缝的使用体验。

Ivanti 的旗舰级产品 Ivanti 管理套件的功能包括：

发现并生成清单：不管设备安装什么操作系统，Ivanti 都会自动发现所有连入网络的受管和未受管 PC 机、笔记本、智能手机、平板电脑和其他移动设备，并相应地生成清单。利用 Ivanti 云服务设备，IT 部门甚至可以发现远程位置的设备并生成清单，并通过低带宽的连接来管理它们，无需 VPN。

操作系统部署和分发：Ivanti 在所有相关用户系统上简化并自动化 Windows 和 Mac OS X 操作系统的安装和迁移，同时保留用户、应用程序、设置和文件，从而将它们恢复到现有的或新的计算机上。

软件分发：Ivanti 自动在所有设备上进行软件分发，不管是 Windows、Mac 计算机还是 iOS 或 Android 移动设备均可实现。借助获得专利的企业分发技术，可以在几分钟内以最低的带宽占用在成千上万台设备上分发大型软件包。

简单的、基于用户的管理：允许 IT 部门针对每位用户携带的所有设备来实施单一的用户配置和安全策略。利用这一功能，通过一套单一的策略部署可以在几分钟内连接并部署一位新员工的所有设备。

软件许可证管理：这些工具提供了自动化的软件审计和软件许可证监控，可以帮助企业恰到好处地购买实际需要的数量，并提供详细的信息，帮助与供应商谈判许可证协议，从而控制成本。聪明地使用软件许可证管理可以帮助企业节省数千甚至数十万美元。

通过系统仪表盘和报告则可以看到所有系统（包括 PC 机、Mac、智能手机和平板电脑）的运行状态。SmartVue 可以为 CIO、部门领导以及 IT 总监提供及时的可视化图形和图表，帮助进行业务文稿演示来展示 IT 部门工作的价值所在以及进行决策制定。它甚至可以提供投资回报收益报告的相关工具。Ivanti 还包括了全面的阈值监控和警报工具，因此 IT 部门能够在问题发展到影响业务之前就解决它们。

远程控制和问题解决，方便 IT 部门接管设备并修复支持问题，或在需要时在系统之间传输文件。

电源管理，可创建和部署整个网络的电源管理策略。

全面移动设备管理，包括上述已经提到的功能以及远程设备定位、锁定和擦除。

基于角色的工作区，用户可以在此访问所有 IT 服务 — 包括他们所依仗的服务台和安全更新，并有权访问自己的所有设备。

这是一个可选模块，与 Ivanti 管理套件紧密集成，可提供资产管理、软件和硬件生命周期管理以及服务管理，提供流程以维持用户的工作效率和企业的效率。

Ivanti® 移动安全套件还通过增加以下功能来为 Ivanti UEM 解决方案提供补充：

移动应用程序封装，可用于设备上每个单独的企业应用程序及其相关信息。只需几步就可以封装应用程序，也无需任何编程技能。可以部署应用程序特定的身份验证，从而在用户能够访问企业应用程序之前进行验证。应用程序级的 VPN 提供了方便安全的加密连接，可连接到公司网络和系统。

Ivanti 安全移动电子邮件，系 LetMobile 出品，让移动用户能够从自己熟悉和喜爱的原生设备电子邮件应用中访问企业电子邮件，而不是强行让用户使用特殊的安全电子邮件客户端。所有企业电子邮件和附件都通过特殊的安全网关传输给企业用户，绝不会在任何方面影响用户体验。如果设备丢失或被盗，LetMobile 可利用完整的 IT 访问控制以及数据窃取保护来保护电子邮件、附件、联系人和日历。此外，IT 部门可以通过自动订立特定的安全参数来实施基于内容、上下文和地理位置的移动数据违规防护 (Mobile DLP) 规则。

安全浏览器可访问内部企业网站、内网以及 Web 应用程序。通过云服务设备提供访问，无需 VPN。

借助统一的 Ivanti 方法实现设备和应用程序管理，企业 IT 部门得以依靠这套解决方案来降低端点管理成本和资源需求，弥补端点安全方面的空白，提供无缝的用户体验，并为用户携带的所有设备提供支持，从而最终提高用户和 IT 部门的工作效率。

是时候采用以用户为中心的 IT 了

曾经，PC 机和笔记本电脑是两个不同的世界，并拥有不同的功能，这与现在它们和移动电话的对应关系相似。那时候的逻辑也是为它们分别开发和部署独立的管理系统。但现在，用户依赖所有设备来完成工作。在这种环境中，两套独立的管理系统只会让用户和 IT 部门背上不必要的负担。Ivanti 的统一端点管理打消了这个顾虑。通过聚焦用户安全与管理，不仅实现了集中控制，还能随时随地为使用任意设备的用户带来统一的操作体验。