统一端点管理（UEM）终极指南|电子书

统一端点管理（UEM）终极指南

目录

摘要

全新涌现的移动和云计算技术正在使无处不在的工作空间成为可能，用户因此得以提高工作效率，无论他们在哪里工作，使用什么设备。面临着如此多的用户、终端、操作系统、应用程序和云服务选择，当今的工作者希望能够即时访问所需的内容，而不是翻越重重安全障碍。

无处不在的工作空间大大提升了业务的灵活性，但也意味着更多的数据会在无边界的企业内外自由流动。正因如此，IT部门需要建立一个零信任的信任体系。诚然，在零信任的体系中，每个用户、设备、应用程序、网络和云都面临着被攻破的风险，但这并不意味着我们应该抵制进步。与此相反，这意外着我们应该把事情做好。构建零信任的安全环境需要全新的思维方式和安全技术。和安全领域的几乎所有其他工作一样，良好的习惯和基本流程是一切的开始。好在，这些也是每一家企业今天就可以着手准备的事情。

在企业从传统型企业安全转向可接轨“无处不在的工作空间”的安全环境的过渡过程中，统一端点管理（UEM）发挥了关键作用。在UEM建立的零信任环境中，用户能够放心地采用工作所需的现代化端点设备、桌面、应用程序和云服务。UEM会利用必须的信任模型和策略框架，持续判断是否允许访问企业数据。

我们的最终目标是，确保用户在任何地方工作时都能够通过自选设备享受效率和优质的使用体验，同时保护您的企业免受最新威胁。

本指南意在帮助移动企业领导者制定有效的UEM战略，从而能够把业务流程由传统系统转变为安全、现代的计算架构，为无处不在的工作空间提供支持。在对UEM的工作原理作出讲解之余，本指南还给出了一个典型的UEM 实施方案，并附有详细的最佳实践部署流程和对如何成功实现移动云进程的建议。

介绍

在过去的几十年中，由IT部门掌控的桌面是企业的主要生产工具。然而，今天的移动工作者不想再被束缚在固定的 PC工作站上，而是要求IT部门支持他们需要的移动设备和应用程序，以便他们在任何地方工作都能保持效率。我们正在快速地从客户端/服务器计算架构过渡到移动和云计算，这使得许多IT部门费尽力气才能维持对企业数据的安全控制，但同时又必须向用户提供随时随地的完全移动自由和无缝访问。

令这一状况雪上加霜的是，移动和云计算的基础架构是高度分散的，并无企业边界可言。企业很可能并不拥有所有访问企业应用和数据的端点，例如，自带设备（BYOD）则由员工所有。即使是企业配给员工的设备，也分成了多种不同的部署模式，如“企业拥有、个人启 用”（COPE）和“企业拥有、仅限业务（COBO）”设备，由企业控制的程度也各有不同。即使是由IT部门所有的实体设备，其操作系统的更新和安全补丁也是由设备制造商控制，而用户决定何时安装，不需要任何IT部门的干预。此外，移动用户已经习惯于到苹果应用商店或谷歌应用商店下载应用程序，而不是坐等IT部门指挥。

有人认为这一切注定会酿成灾难，但事实并非如此。这只是现实在不断变化，而我们需要与时俱进。更好的办法是，未雨绸缪，领先于变化。

“首席信息安全官需要面对的是不断扩大的威胁、熟练网络安全专业人员的短缺，以及缺乏网络安全最佳实践意识的非技术人员。” [1]

随着移动设备和云计算的使用面越来越广，IT部门需要进一步掌握这些非自有设备和网络的安全威胁和漏洞。此外，移动威胁和网络攻击随处可见，代表每一个IT部门都可能不得不处理安全泄露，也许是恶意软件攻击、凭证受损，也可能是设备被盗。我们应该为此惶惶不安吗？不，但我们需要做好计划。我们必须有能力迅速和果断地做出反应。

与此同时，首席信息官和首席信息安全官必须确保符合政府法规，如欧洲的《通用数据保护条例》（GDPR）、美国的《健康保险可携带性和责任法案》（HIPAA）以及《支付卡行业数据安全标准》（PCI DSS），后者是一套旨在确保信用卡交易安全的安全标准

基于边界和IT控制的桌面安全时代正在让位于无处不在的工作空间。让我们以积极的态度迎接这一变革，企业领导者也应当学习同时确 保移动生产力和全面的移动安全，而拥有零信任安全基础的UEM便是移动安全和移动生产力两全其美的策略。

移动云安全：您需要知道什么？

放之四海而皆准的移动云部署战略并不存在。每个企业的战略是独一无二的，以各自的业务和技术要求为基础。然而，您不是在孤军奋战，因为许多挑战是所有公司都需要面对的。举个例子：每个企业都必须解决如何支持设备选择、安全配置移动应用程序和内容、保护数据免受日益扩大的威胁攻击，还有最重要的——为终端用户提供卓越的设备体验。

下方为您总结了几个常见的可能挑战：

支持设备选择

数字化工作空间极大地改变了企业IT部门的作用。现在的 IT 部门需要支持员工带入企业的各种移动技术，而不是规定员工必须使用哪些技术。但是，为什么要如此迁就？因为如果IT部门不支持移动用户或他们喜欢的设备，移动员工只需绕过IT即可。这可不是好事

移动应用程序和内容管理

人们对移动应用的需求正在迅速增长，移动工作者已经不满足于只能打开企业邮件的设备。而且，随着iOS 等更多平台加大了对企业应用开发支持的力度，这方面的需求只会更大。如果要满足这一需求，企业就不能首先开发基于PC的环境，然后再过渡到移动计算。今后，所有的应用程序和内容开发都必须首先具备移动功能。

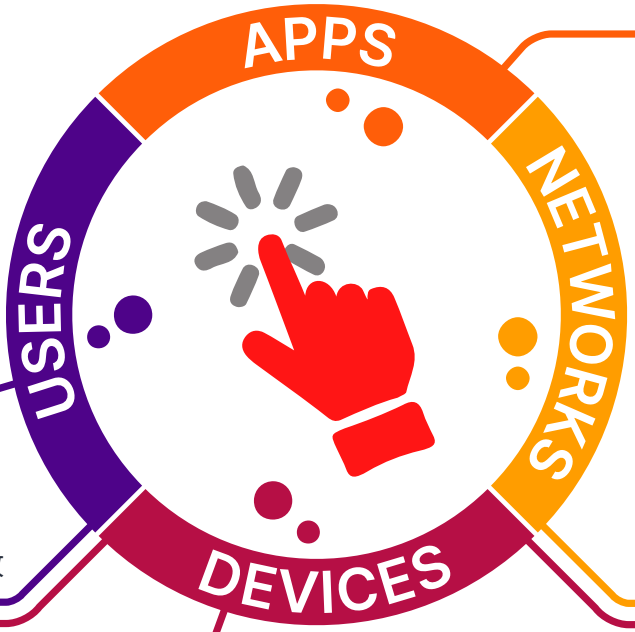
新的安全挑战

最重要的移动挑战之一，是如何确保所有移动设备上的数据和应用程序（包括第三方应用程序）的安全，而不影响本地用户体验。

在移动时代之前，最大的安全风险是恶意软件和病毒，因为开放的文件系统和无保护的内核存在着固有的脆弱性。今天的移动操作系统拥有沙盒文件系统和受保护的内核，所以传统安全威胁的危害已经不大。然而，一种安全挑战变成了种类繁多的其他类型的挑战。移动技术正在面临着越来越多的威胁，有些基于用户，有些基于设备，还有一些威胁基于应用和网络。

威胁向量

沙盒移动操作系统是安全的，像恶意软件这样威胁可以通过操作系统设计得到缓解。要防止移动设备上的数据丢失，我们需要关注的重点是其他风险载体



恶意或高风险应用程序

通常会收集数据，如个人身份信息（PII）和设备位置，并与第三方广告和分析系统分享。

数据丢失

数据可能会在云服务和工作应用程序中通过打开方式、复制、粘贴和转发操作而丢失。

设备篡改

利用操作系统漏洞对设备进行越狱或root、绕过安全防护，并从未经授权的应用程序商店安装恶意应用程序。

外观造型

轻便的造型使移动设备更易于丢失或盗窃。

永远在线

移动设备联网程度极高，经常通过不受信任的网络访问敏感数据，从而增加了Wi-Fi嗅探、非法接入点和中间人攻击造成数据丢失的风险。

什么是统一端点管理？

根据Gartner的描述，统一端点管理（UEM）工具能够把多种端点类型（设备）的管理集中到一个控制台。UEM是一种全面的解决方案，可管理分布在整个无边界企业内的现代移动设备、桌面、应用程序和内容。UEM 解决方案专用于帮助企业通过零信任策略，确保只有授权用户、端点、应用程序、云服务和网络可以访问企业资源，利用现代操作系统和移动技术实现业务转型。

UEM工具是基于通用性设计的。它的功能包括：

- 配置、管理和监控iOS、macOS、Android和 Windows 10。也可以管理可穿戴式终端，以及一线工人常用的加固型设备。
- 统一应用配置、管理配置文件、设备合规性和数据保护。
- 提供多设备用户的单一视图，有助于提供更有效的终端用户支持和详细的工作环境分析。
- 作为协调点，协调关联终端技术的活动，如身份服务和安全基础架构等。

UEM的优势

UEM的目的是帮助您的企业把关键业务转为安全的移动和云计算，从而：a）为IT部门提供保护数据所需的控制权；b）为员工提供保持效率所需的用户体验。

利用移动和云计算安全地拓展您的业务

组织和用户控制

建立移动安全协议，保护您的设备、应用程序和数据，而不影响用户体验。您可以通过UEM实现扩展，随着业务需求和预算要求的变化增加新功能。例如：

- 在移动设备和桌面上分隔个人数据和企业数据，在确保用户隐私的同时保护企业数据。
- 管理一个企业应用商店，让员工安全方便地访问企业监管应用。
- 实施多层安全控制，保护移动设备和数据，而不影响用户体验。
- 有选择地擦除移动设备和桌面上的企业数据，同时保留个人数据。
- 启用自助服务，便于用户注册和登记设备、检查合规性、排除故障以及处理其他基础的设备管理问题。

自由选择。

UEM独立于操作系统和设备，因此用户可以自行选择喜欢的设备，无论是企业设备还是自带设备，都能在任何地方工作并保持效率。IT管理员也可根据业务需要采用云或内部部署模式。有了UEM，您可以：

- 启用多操作系统环境，支持iOS、macOS、Android和Windows 10设备。
- 允许用户快速访问企业资源，如企业邮件、日历和云服务，包括Office 365、G Suite、Dropbox、Box、SharePoint等。

以经验为本的实施进程。

要确保快速、广泛地采用UEM，最好的办法是尽可能无缝的用户体验。如果员工在企业工具中获得熟悉、原生的设备和应用体验，他们会更有可能接受合规措施，避免影子 IT行为，同时保持效率。其他优势：

- 通过无密码多因素认证（MFA）提供无缝的即时认证。
- 让用户在使用电子邮件、SharePoint和其他企业内容管理系统和云服务时能够轻松访问、注释和共享文件。
- 支持多用户配置文件，允许多名员工共享一台设备。
- 帮助用户快速补救设备上的问题，为企业政策合规提供便利。

安全的业务弹性。

有了无形和自动化的安全防护，您的员工可以专心完成他们的专业工作，也就意味着保持工作效率。自动化安全能够保护数据的完整性、简化合规性，降低移动威胁的风险。具体地说，就是：

- 提供即时、自动、设备内的移动威胁保护，即时检测和补救设备、网络和应用程序层面的威胁及网络钓鱼攻击。
- 实行基于证书的身份管理，确保只有授权用户才能访问设备。
- 支持应用程序容器化，确保每个应用的数据都经过加密，免受未经授权的访问，并在删除时不损害私人数据。
- 部署单个应用程序的VPN技术，仅允许授权应用程序访问企业网络。
- 配置DLP策略，防止未经授权的文件共享或复制粘贴操作造成数据丢失。
- 执行有条件的访问，在设备不合规时自动触发操作，如合规通知或设备隔离。
- 加密电子邮件附件，确保只有授权应用程序才能查看。

成功的UEM战略有哪些重点

把用户体验放在首位。

用户体验必须是任何移动能力策略的核心，如果设备、应用程序或内容不符合用户要求或难以访问，它就不会被采用——无论IT部门如何推广。也就是说，任何 UEM平台都必须能够保证用户体验。要做到这一点，您可以：

允许选择设备和操作系统。

IT部门必须落实一个可支持iOS、macOS、Android和Windows 10等现代操作系统的多系统UEM方案。

分隔个人和工作应用程序和数据。

IT部门应该能够把同一台设备上的业务和个人应用程序和数据分隔开来（也许企业所有的自助服务台设备除外），而不是要求员工拥有单独的个人设备和业务设备。这不仅能简化应用程序的管理，也能保护设备上的用户个人数据的隐私。如此一来，如果员工离开 公司，IT部门可以擦除设备上的所有业务资源，同时保留个人应用和内容的完整

保障原生设备体验。

这也许是最重要的一点，用户应该能够无缝使用UEM解决方案的设备和应用管理功能。数字化工作环境中的员 工应该能够快速认证和访问企业应用和数据，而不需要每次都输入用户名和密码。用户还应该能够使用自我服务工具，以此管理基本的设备功能和排除故障，而不需要提交服务台工单。

简化IT管理

这种战略中的IT管理不是一项小任务，而是必须有能力管理和保护多操作系统环境，包括各种移动设备、桌面、应用程序、云服务和内容。所以，每个UEM解决方案应该让使 IT部门能够：

简化访问控制和认证。

保护敏感的业务数据意味着IT部门需要确保只有受信任的用户和设备才能访问移动端和云端的企业应用程序。主机检查器可以与Windows Management Instrumentation、Windows Defender、Microsoft Security Essentials或Ivanti的Connect Secure VPN 客户端进行互动，以获得更高的精细度。问题是，移动设备上的用户名/密码认证可能很麻烦、令人恼火又不安全。因此，UEM解决方案应该采用无密码多因素验证等更先进的功能，允许用户快速完成验证。

支持关键业务流程的移动服务。

数字化工作环境中的员工需要随时掌握重要数据，以便做出核心业务决策。试想这样的零售环境，销售人员可以在店中随处使用移动应用程序来协助顾客，查询库存而无需跑到后面仓库，也可以完成支付，不需要在收银台前大排长龙。UEM解决方案应该能够通过企业应用商店，简化为特定用户或用户 群部署业务应用的流程。

UEM的实现过程

大多数企业的机构移动化进程始于为终端用户提供基本的效率工具，如公司邮箱和日历等。这有助于取得员工的信任，而信任对确保余下的UEM进程的成功至关重要。这是一个良好的开端，不过，只有在企业在借助移动云计算催生真正意义上的业务转型时，UEM的真正优势才会显现。

分层的安全策略是这个转型的基础。为什么？因为在移动-云模式中，基于周界的安全已经不够。分层安全提供的多种安全类型能覆盖移动设备、应用程序和网络，有助于保护设备、应用程序和云存储中的静态数据。最重要的是，分层的安全措施在幕后运行，对终端用户不可见，即安全操作永远不会干扰移动工作效率。

UEM部署最佳实践

UEM部署通常分为以下四个步骤：

第一阶段：规划

要开始规划过程，首先要知道您的企业如何定义成功，以及您认为多快能取得这种成功。

规划阶段的一个关键步骤是向整个企业上下的关键利益相关者征求反馈，以决定什么算是成功。例如，某些公司把成功定义为一项简单直接的部署，为用户提供安全策略、电子邮件和Wi-Fi配置文件。

在基本的部署中，设备注册主要由熟悉移动操作系统及其功能的IT人员完成。如果公司规划的不仅仅是基本的UEM部署，计划阶段则应当解决以下几个问题：

1. **您的员工是否拥有移动设备和现代操作系统方面的经验？**
   精通技术的用户会比刚开始接触移动设备的人更能自力更生。技术经验不足的用户也许需要更多的IT支持。
2. **用于什么场合？**
   每一项部署都高度依赖于最终的使用案例，成功的实施需要有直接相关经验的供应商。确定一个支持多种使用案例的供应商，包括：

医疗保健：

- 共享设备
- 安全EMR访问
- 临床通信
- 护士与药房的通信
- 安全会诊

制造：

- 设备
- 供应链管理库存控制

零售：

- 共享设备
- 销售终端
- 库存管理 非接触式交易
- NFC技术和分析

医疗运输

- 实时票务
- 行李控制
- 驾驶员管理
- 售票台
- 资产追踪

3. **您的企业将支持哪些现代操作系统、移动设备、云服务和桌面？**
   要回答这个问题，您需要了解员工最喜欢的是哪些设备和云服务（尤其是自带设备），以及它们是否能支持您的业务需求和安全要求。

4. **您的网络基础架构的复杂程度如何？**
   要启用配有一套内部网络服务的单一数据中心，所需的资源会少于网络和基础架构要求复杂的多站点启用。外包IT服务将需要额外的规划。

5. **您的IT管辖框架、政策和流程有多成熟？**
   有效的IT管辖能确保符合进度和预算的项目开发和解决方案交付，满足您的目标。缺乏稳定或成熟的IT管辖方案的企业可能需要更多的时间和人力资源来实施 UEM 解决方案。

6. **您的员工教育和培训资源是否有效？**
   拥有现成的培训和教育框架及基础设施的公司能够提高UEM的推广速度，增进员工和服务台人员对方案的采用。建立员工教育计划需要更多的前期工作，但会培养更多精通移动技术的员工，减少服务台求助次数。

7. **您的IT团队是否有证书验证方面的经验？**
   证书验证是移动方案中的重要安全能力。拥有这方面专业知识的员工能够加快部署和设置过程。

8. **您的IT部门是否能够开发和部署移动企业应用程序？**
   任何为您的公司开发应用程序的人都应该具备相当的经验和知识，有能力提供优秀的移动用户体验。这是确保您的移动战略取得成功的关键。如果您的公司内部没有熟练的应用程序开发人员，您就需要将这一关键职外包出去。

9. **您的公司有哪些安全要求？**
   移动设备上的信息保护和数据安全是所有UEM部署的关键组成部分。与风险容忍度较高的公司相比，属于高度管制行业的公司的风险容忍度更低（因此也有更多的安全要求）。

第二阶段：设计

这个UEM部署阶段的任务是设计您的移动策略的管理政策。

1. **定义角色。**
   首先，决定您要如何协调管理任务，例如服务台支持、用户注册和设备配置管理等。举个例 子，您需要多少个服务台支持级别？您的内部应用程序将由谁开放和管理，现有员工还是第三方开发商？谁来监督政策和配置过程？

2. **定义可视性。**
   其次，决定每名IT管理员将管理哪些用户和设备，以及他们会有多少控制权和可视性。别忘了，您的设备和用户管理政策可能会因业务部门或地理区域的不同 而有所差异。例如，一些地区会各有各的隐私法规，如欧盟的GDPR和美国的HIPAA。您的安全政策将需要确保这些地区的移动员工能够满足合规标准。

3. **分派行动。**
   第三，为您的部门中的每个IT角色分配管理任务。想 一想，根据您的可视性政策，哪些管理员会负责应用程序、政策和配置的分配？

4. **管理分配。**
   在这个最后的步骤，您必须决定部署哪些应用、政策和配置、由谁部署以及何时部署。确定各个分配角色将由哪些IT管理员负责，同时防止管理员执行任何 未经授权的操作。

第三阶段：部署

在UEM方案的部署阶段，您需要选择如何部署您的平台，是在企业本地还是基于云的解决方案？

选择一：本地解决方案

企业本地解决方案会封装为易于安装的软件包，可直接插入企业网络并在一天之内启动和运行。

选择二：基于云的解决方案

基于云的UEM部署会紧密关联企业的信息传递和安全系统，如企业邮箱和企业目录。基于云的部署通常以订阅的方式提供。

第四阶段：启用

您的UEM解决方案准备就绪后，您必须确保您的服务台管理员也做好了充分准备。也就是说，他们能够：

- 理解他们可能面临的多系统管理问题。明确地指出解决每种类型的设备、应用程序、服务器或网络问题的故障排除步骤、上报流程和责任。
- 求教于设备专家，就您的服务台工作人员将面临的所有设备获取深度洞见。
- 获得与他们将提供的支持水平相应的必需资源。
- 确保他们拥有易用的故障排除资源，如问题解决脚本和在线知识库。
- 利用持续教育的机会，确保他们在移动设备升级、基础架构更新等方面能够与时俱进。

如何选择 UEM解决方案提供商

在UEM领域，其中一个最常见的问题是如何找到一个能满足您的所有独有要求的供应商。这里的几个关键衡量标准可以帮助您缩小搜索范围，提高搜索速度：

选择计算和终端用户体验。

回想一下，五年或十年前的移动设备是什么样子。一些品牌已经几乎销声匿迹。很可能的是，五年后的移动技术会和现在非常不同，特别是在移动设备层出不穷的情况下。与其试图预测哪个移动平台会在这个竞争激烈的市场独占鳌头，不如选择一个允许用户自选最能保持效率和业绩的设备、且在任何变革下都有能力管理不断更新换代的设备环境的供应商。如果供应商能够管理任何设备，同时在设备入网时提供无缝直观的终端用户体验，就无需担心应该支持哪些移动设备和桌面。

专为“无处不在的工作空间“设计的安全平台。

移动云计算正在快速成为下一个主流企业计算模式。支持这种模式的关键，是要找到一个供应商为您提供能够随着您的业务需求增长而拓展的安全平台。这意味着您要寻找的方案应该经过彻底的专业设计、可保护和管理多款现代操作系统，并拥有强大的可扩展性。以简单的插件或既有基础架构组件形式实施的UEM解决方案，可能会不够全面或集成程度不足，无法为成长中的企业提供必要的可扩展性和可靠性。

庞大的合作伙伴生态系统。

供应商除了应该拥有宏大的愿景和专业UEM平台之外，还 应该保持一个由最佳解决方案提供商组成的多样化生态系统。这样便可确保您能获得广泛的技术解决方案选择，以满足现时的业务和基础架构要求。

客户成功的经验。

审查UEM供应商的客户资料和分析专家的评价。供应商不仅应该拥有多样化的全球客户群，也应该在 UEM领域的排名、客户评价和获奖方面名列前茅。 通过研究这些因素，您便可以肯定供应商是否具有相 当的成熟度、经验和可信度，以满足您的长期移动需求。

可选的部署方案。

企业对移动和桌面设备有不同的数据保护要求。一些企业可能会有强制性的合规要求，也有内部IT人员，因此选择将数据保存在本地，而其他企业可能会灵活选择，把数据存储在云中。还有一些企业可能会选择二者结合，以满足不同地理区域的需要。寻找一个能提供可选的部署方案的供应商。

总结

进入无处不在的工作空间不仅仅是购买最新的移动设备，或在员工手机上安装电子邮箱。这意味着用零信任平台改造您的企业，在确保合规的同时为您的用户提供所需要的自由，让他们无论在哪里工作都能保持效率、获得成功。无处不在的工作空间正在成为现实。与其陷入被动，不如让合适的UEM解决方案帮助您快速、无缝地完成这一转变，为现在和未来做好准备。

关于Ivanti

Ivanti让无处不在的工作空间成为可能。在“无处不在的工作空间”，员工可能会在任何地方工作，并使用多种设备来访问IT网络、应用 程序和数据，以保证工作效率。Ivanti自动化平台集成了业内领先的统一端点管理、零信任安全和企业服务管理解决方案，通过一站式平台实现为企业实现自我修复和自我安全，并为终端用户提供自我服务。已经有4万多位客户，包括78家《财富》百强企业，选择了Ivanti为他们检测、管理、保护和维护从云端 到边缘的IT资产，同时为员工提供卓越的终端用户体验，无论他们在哪里、使用何种方式工作。更多信息请访问 ivanti.com.cn。

ivanti

ivanti.com.cn
+86 (0)10 85412999
contactchina@ivanti.com

1 https://www.csoonline.com/article/3244248/data-protection/top-5-cybersecurity-questions-for-the-ciso-in-2018.html

2 https://www.idc.com/getdocjsp?containerId=prUS41240816