

# Ivanti 统一端点管理

## 挑战

无处不在的工作空间已经到来。为了在这个全新的环境中蓬勃发展而不仅仅是随波逐流,企业需要能够安全地访问、轻松地管理员工、承包商和一线员工使用的任何端点上的业务数据。

在今天,现代数字工作空间意味着要使用多种多样的端点,包括Android、iOS、macOS和Windows 10。对于某些企业而言,这一范畴也许还包括其他沉浸式和坚固设备,如HoloLens、Oculus、Zebra等等。

其中的需求很明确:管理隐私和合规性,同时尽可能降低风险、保护用户体验。也就是说,必须把企业应用程序与用户终端设备上的个人应用程序分离,并加以保护。有了统一的端点管理(UEM)解决方案,这一切便可以简单而安全地实现。

## 业界首创的端到端零信任安全平台,保护您无处不在的工作空间

Ivanti UEM由业界首创的端到端零信任安全平台提供支持,可全面安全访问和保护无处不在的工作空间的数据。

平台对每一台设备都会进行验证,确保只有经授权的用户、设备、应用程序和服务可以访问业务资源。平滑无缝的流程在确保安全的同时保障了所有端点的用户体验。

这是在“无处不在的工作空间”中茁壮成长的企业的选择,而企业移动安全则是一切的核心。这个转变非同小可,但Ivanti UEM可以让它轻松完成。在您的需求发生变化时,我们的UEM会与您共同适应。在此基础上,您还能够借助强大的技术消除密码(零登录或ZSO)、确保用户认证(多因素认证或MFA)以及检测和缓解端点安全威胁(移动威胁防御或MTD)。

## 全面的安全防护

安全、管理和监控任何访问关键业务数据的企业或个人所有的移动设备或桌面。UEM的可视性和IT控制使之变得简单。

无论您是允许自带设备、配发公司设备或两者并行,UEM都能在多种端点上保障安全,同时管理端点的整个生命周期,包括:

- 自动化入网。
- 政策配置和执行。
- 应用分配和管理。
- 管理和安全监控。
- 停用和退役。

UEM构建于一个成熟、安全、可扩展、企业就绪的架构,具有灵活的部署选项,在注重用户体验的同时保持最高质量的安全标准。

Sentry作为电子邮件和内容在线网关,对移动设备和后端企业系统之间的流量进行管理、加密和保护。Tunnel是一个多OS应用程序VPN解决方案,允许企业授权指定移动应用访问防火墙后的企业资源,无需任何用户互动。

## 通过移动和云,放心安全地管理和发展您的业务

**组织和用户控制。**借助UEM,企业得以根据自身进度,采取个性化的移动和安全策略,以满足业务需求。同时确保用户数据隐私和企业数据安全,赋予用户和管理员信息自主权。

**选择的自由。**Ivanti UEM与操作系统和设备无关。管理员可以根据预算选择云或本地部署,而员工可以使用最称心的端点来工作。

**基于经验的采用策略。**易用性意味着更高的采用率。更高的采用率代表了更高的生产力和更快的增长。UEM为工作所用的生产力应用程序提供原生式的用户体验,帮助IT部门提升采用率,既简化了合规性,又减少了安全威胁和影子IT。

**业务抗压力。**超安全。超非干扰。无形的自动化安全确保合规性,同时绝不妨碍您的企业大步向前。

### 主要用例

- **为需要保护敏感数据的企业确保隐私和合规性。**保护任何端点上的业务数据,分隔业务数据和个人数据。
- **通过单一控制台实现多设备、多操作系统和多应用管理。**对于兼具不同操作系统和应用程序的混合设备环境而言,统一管理是重中之重。
- **赋权一线员工。**支持依赖坚固设备和信息台模式设备的医疗、运输、制造和其他行业的现场、车队和移动员工。
- **提供卓越的终端用户选择和无缝的用户体验。**设备选择和用户体验是确保生产力和用户合规性的关键。Ivanti UEM提供精简的入网流程和卓越的设备体验

### 安全标准和认证

- Common Criteria Certification (通用评估准则认证)
- CSA STAR
- CSfC
- DISA STIG
- EU-US Privacy Shield (欧盟美国隐私护盾)
- FedRAMP Authority to Operate
- FIPS 140-2 Affirmation
- SOC 2 Type II
- CCN (西班牙)

## Ivanti 统一端点管理

设备管理和安全	安全UEM	安全UEM高级版
安全和管理。保护和管理运行iOS、macOS、iPadOS、Android和Windows 10操作系统的端点。可在本地和作为云服务使用。	✓	✓
移动应用管理 (MAM)。通过AppStation保护承包商和员工设备上的业务应用程序, 无需设备管理。	✓	✓
轻松入网。利用Apple Business Manager (ABM)、Google Enrollment和Windows AutoPilot等服务, 为用户提供自动设备注册。	✓	✓
安全的电子邮件网关。Sentry是一个在线网关, 对移动设备和后端企业系统之间的流量进行管理、加密和保护。	✓	✓
应用分配和配置。Apps@Work是一个与苹果批量购买计划 (VPP) 结合的企业应用商店, 有助于移动应用的安全分配。此外, iOS管理应用程序和 Android 企业等功能也简化了应用程序层面设置和安全策略的配置。	✓	✓
安全连接	安全UEM	安全UEM高级版
以应用为单位的VPN。Tunnel是一个多OS的VPN解决方案, 允许企业授权指定移动应用访问防火墙后的企业资源, 无需任何用户互动。		✓
有条件访问	安全UEM	安全UEM高级版
信任引擎。结合用户、设备、应用程序、网络、地理区域等多种信号, 提供自适应访问控制。		✓
无密码用户验证。对于单一云或本地应用程序, 无密码多因素验证以设备为身份。		✓

## Ivanti 统一端点管理 (续)

扩大IT运营	安全UEM	安全UEM高级版
服务台工具。Help@Work 允许IT部门在用户许可时远程查看和控制用户屏幕,以有效地排除故障和解决问题。	✓	✓
报告。通过自定义报告和自动修复操作,掌握所有管理设备的深度情况和控制。	✓	✓
安全的生产力	安全UEM	安全UEM高级版
安全的电子邮件和个人信息管理 (PIM) 应用程序。Email+是一款适用于iOS和Android的跨平台、安全的PIM应用。安全控制包括政府级别的加密、基于证书的验证、S/MIME、应用层面的加密和密码执行。		✓
安全的网页浏览。Web@Work 同时传输中的数据 and 静止数据,实现安全的网页浏览。自定义书签和安全隧道确保用户能够快速、安全地访问业务信息。		✓
安全的内容协作。Docs@Work 允许用户安全地访问、创建、编辑、标记和分享来自 SharePoint、Box、Google Drive 等资源库的内容。		✓
移动应用容器化。部署 AppConnect SDK 或应用程序包装器,为您的内部移动应用程序提供额外的安全防护,或从我们的 AppConnect 集成应用程序生态系统中选择。		✓
衍生凭证。支持使用通用访问卡 (CAC) 和个人身份验证 (PIV) 的双因素认证。		✓

## About 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”，员工使用数不清的设备访问IT网络、应用程序和数据，以便能够在任何地方保持工作效率。Ivanti 自动化平台连接业界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，通过单一操作窗口让企业实现自我治疗和自我安全，而用户则能够自助服务。已有超过40,000家客户，包括78家财富百强企业，选择了Ivanti来为他们发现、管理、保护和服务从云端到边缘的IT资产，并为员工提供卓越的终端用户体验，无论他们在哪里、用什么方式工作。更多信息请访问 [ivanti.com.cn](http://ivanti.com.cn)

The Ivanti logo consists of the word "ivanti" in a bold, lowercase, sans-serif font. The letter "i" is red, while the remaining letters "vanti" are black. A small registered trademark symbol (®) is located at the top right of the letter "i".A vertical bar on the left side of the contact information, transitioning from red at the top to orange at the bottom.

[ivanti.com.cn](http://ivanti.com.cn)

+86 (0)10 85412999

ContactChina@ivanti.com