Ivanti Neurons for MDM（原 MobileIron Cloud）

挑战

组织需要在其职员、一线工人和外包人员使用的任何端点上安全地访问和轻松管理其业务数据 。

如今无处不在的工作空间包括使用各种各样的端点，如 iOS、macOS、Android、Windows 设备，以及VR以及耐用型设备，如 HoloLens、Oculus、Zebra 等。

由于需要管理隐私和合规性，并将风险降到最低，因此有必要在端点设备上，将企业应用与个人应用分开并加以保护。统一端点管理解决方案 不仅要安全，还要提供卓越的用户体验。

应用场景

确保主要关注敏感数据保护的组织的隐私和合规性：

保护任何端点上的业务数据，分隔各类端点上的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：

组织身处混杂的设备环境，其中包含 iPhone、iPad、Mac、Android 设备、Windows 笔记本电脑和台式电脑、Zebra、Oculus 等。对这些使用不同操作系统和应用的设备加以统一管理是企业的当务之急。

为一线员工赋能

支持医疗、运输、制造和其他行业中那些使用耐用型设备和Kiosk模式设备的的现场作业、车队和一线工作人员。

提供卓越的最终用户令人愉悦的用户体验：

最终用户体验很重要，Ivanti Neurons for MDM 能提供最简化的入门设置和卓越的设备体验，从而提高了用户的工作效率。

安全标准和认证*

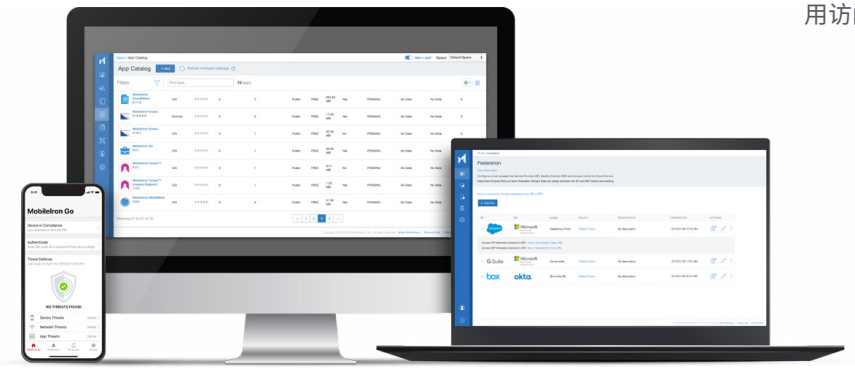
- CSA STAR
- FedRAMP Moderate Authority
- SOC 2 Type II

关于认证的其他信息可参见此处：
ivanti.com/resources/security-compliance

利用 Ivanti Neurons for MDM 在无处不在的工作空间中保护和管理您的设备

Ivanti Neurons for MDM 使您能够安全访问和保护无处不在的工作空间中的数据。Ivanti 的安全保护方法会对设备加以验证，确保只有经授权的用户、设备、应用和服务可以访问业务资源。您可以在任何端点上实现令人愉悦的本地用户体验。

Ivanti Neurons for MDM 将企业移动安全置于企业核心地位，并让您能够在此基础上借助相关技术弃用密码（零登录 zero sign-on）、确保用户身份验证（多因素验证或 MFA）以及检测和降低端点安全威胁（移动威胁防御或 MTD）。



全面的安全防护

Ivanti Neurons for MDM 提供所需的可见性和 IT 控制功能，从而让企业能够保护、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台式机。它使组织能够保护组织内使用的大量员工自有设备，同时管理端点的整个生命周期，包括：

- 设备自动初始化配置
- 策略配置和执行
- 应用分发和管理
- 管理和安全监控
- 停用和退役

Ivanti Neurons for MDM 依托一个成熟、安全、可扩展、高适配的架构，具有灵活的部署选项，以用户体验为先，同时保持最高质量的安全标准。

Ivanti Sentry 作为电子邮件安全网关，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。Ivanti Tunnel 是一款多操作系统 VPN 解决方案，允许企业授权特定的移动应用访问防火墙后的企业资源，对用户完全透明。

我们能让移动业务和云在确保安全的前提下，为您的业务成长助力

发展您的业务：Ivanti Neurons for MDM 让企业得以根据自身进度，采取个性化的移动和安全策略，以满足其业务需求。我们还确保用户个人数据隐私，同时保护企业数据——赋予用户和管理员信息自主控制权。

自由度：Ivanti Neurons for MDM 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方案，而员工可以使用自己最习惯的端点设备来工作。

用户体验驱动：Ivanti Neurons for MDM 为工作中所用的生产力应用提供原生用户体验，帮助 IT 部门提升使用率。这既简化了合规性，又减少了安全威胁和影子 IT。随着用户使用率的提高，IT 部门可以推动整个组织的生产效率和增长率。

实现业务弹性：我们的安全平台可以防止业务中断，而不会对用户造成干扰。各种无形的自动化安全手段确保合规性，同时绝不妨碍您的业务。

主要特性和功能

设备管理和安全

安全和管理：保护和管理运行 Apple iOS、macOS、iPadOS、Google Android 和 Microsoft Windows 操作系统的端点。可在本地和Cloud使用。

MAM模式：通过 AppStation 保护外包人员和员工设备上的业务应用，而无需管理这些设备。

轻松初始化配置：利用诸如 Apple 商务管理 (ABM)、Google Zero-Touch 零接触注册和 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：Ivanti Sentry 是安全在线网关，对移动设备和后端企业系统之间的流量进行管理、加密和安全保护。

应用分发和配置：Apps@Work 是一个可以与苹果批量采购计划 (VPP) 结合的企业应用商店，有助于移动应用的安全分发。此外，iOS Managed Apps 和 Android Enterprise 等功能也简化了应用层面设置和安全策略的配置。

保障生产力

安全的电子邮件和个人信息管理 (PIM) 应用：Ivanti Email+ 是一款安全的跨平台 PIM 应用，适用于 iOS 和 Android 系统。安全控制措施包括政府级加密、基于证书的验证、S/MIME、应用级加密和密码执行。

安全web访问——Web@Work 通过保护动态数据和静态数据来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。

安全内容协作 - Docs@Work 允许用户从 SharePoint、Box、Google Drive 等存储库安全地访问、创建、编辑、标记和共享内容。

移动应用容器化：部署 AppConnect SDK 或应用封装，为您的企业开发的私有Apps提供额外的安全防护，或者也可以从我们的 AppConnect 集成应用生态系统中获取这些Apps。

派生凭证：支持使用通用访问卡（CAC）和个人身份验证（PIV）的双因素验证。

安全的应用级VPN：

Ivanti Tunnel 是一款多操作系统 VPN 解决方案，允许企业授权特定的移动应用访问防火墙后的企业资源，不需要任何用户互动。

扩展 IT 运营

Helpdesk工具：Help@Work 让 IT 部门在用户允许的情况下，远程查看和控制用户的屏幕，以帮助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，深入了解和控制所有托管设备。

有条件访问

信任引擎：结合用户、设备、应用、网络、地理区域等多种信号，提供自适应访问控制。

无密码用户身份验证 – 使用设备作为身份的无密码多因素身份验证机制，可用于SaaS或本地应用认证。

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，员工使用各种各样的设备访问 IT 网络、应用和数据，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能够为设备提供自我修复和自我保护服务，并为最终用户提供自助服务。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

ivanti

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