



思科 BYOD 智能解决方案

任何工作空间的安全性、灵活性和性能

不断增长的用户和设备需求

如今，每个企业的网络中都运行着各种各样的设备。为了管理个人设备的激增，自带设备 (BYOD) 策略已经成为 IT 专业人员的首选策略。用户希望无论使用哪个设备或该设备连接自哪里都能无缝访问公司的资源。此外，还有很多用户没有连接到的设备类型，例如，打印机。由于企业中有如此多的联网设备，因此 IT 组织必须重新定义他们的角色以及总体网络安全性（表 1）。

随着工作与生活之间的界限日益模糊，安全性不再只是如何将人们阻挡在外的问題，还是如何让人们能够进来的问题。此外，新的业务需求（例如使用协作应用程序的需求）也促使网络需要更大的灵活性和更多选择，同时用户也在要求相同的网络性能和安全级别。IT 专业人员必须平衡安全性和方便性，使用户能够有信心地进行协作。

表 1. 您的 BYOD 策略是什么？

策略	限制	基本许可证	增强	高级
执行	仅限公司设备	设备类型众多，但只能访问 Internet	多种设备类型和访问方法	多种提供新服务的设备
示例	金融服务公司限制对机密财务数据的访问	教育机构允许对所有人开放基本服务（例如电邮）	医疗机构根据角色提供差异化服务（例如电邮和选择公司数据）	移动销售企业提供视频和协作会话

在 BYOD 环境中提供最优安全性

思科会帮助各公司接受 BYOD 现象，在这一方面，思科处于领先地位。Cisco® 解决方案使 IT 部门不仅仅能够连接用户拥有的设备，而且能安全地扩展众多用户的体验，支持随时随地使用多种设备。

思科 BYOD 智能解决方案能够在整个组织内实施统一的安全策略，以优化的托管体验满足用户在设备、安全性和业务方面的不同要求。思科是唯一一家提供真正以体验为中心的解决方案的提供商，其解决方案具有情景感知型登记功能，可对资源进行安全的访问。它转变了工作空间，从而提供了高效的用户和 IT 体验，同时并没有影响安全性、可视性和控制力。

高度安全的 BYOD 解决方案的核心组件包括：

- 策略控制的统一访问基础设施
- 有效、无缝的安全性
- 简化管理

策略控制的统一访问基础设施

策略控制的统一访问基础设施可确保对数据、应用程序和系统进行安全的访问，并能为每个设备提供高性能连接。思科是唯一一家能够在整个组织内为有线、无线和 VPN 网络提供单一策略来源的供应商，可显著提高安全性并简化网络管理。

- 思科身份服务引擎是统一的、基于策略的服务支持平台，可帮助确保连接到网络的设备符合公司规章和法规。它从网络、用户和设备收集实时情景信息，通过在网络基础设施内实施策略来做出主动监管决策。策略决策基于尝试访问网络的用户、请求的访问类型、用户发起连接的位置以及用户尝试连接的时间和方式（使用哪种设备）。身份服务引擎包括访客状态、设备分析、网络访问和移动设备管理，可为最终用户提供简单的设备注册和登记。
- 思科 AnyConnect® 安全移动客户端采用增强的远程访问技术，使 VPN 体验更简单且更安全。该软件包括 802.1X 身份验证，可在行业中各种手提电脑和智能手机型移动设备（包括 iOS®、Android®、Blackberry 和 Microsoft Windows Mobile® 平台）中提供无间断 VPN 体验。



- 思科智能网络基础设施包含一整套有线、无线和 VPN 接入点。安全性以独特方式嵌入到选定的网络基础设施中，以提供更高的可视性和更出色的实施。
- 思科有线基础设施包括思科 Catalyst® 和思科 Nexus® 接入交换机产品组合，为最终用户提供经济高效的高可用性、性能和安全性。
- 思科网络基础设施产品还包括思科集成服务路由器，该产品将安全性、无线、统一通信和应用服务智能地集成在一起，具有无与伦比的总拥有成本节省能力和网络灵活性。
- 思科无线基础设施将无线网络的移动性和有线网络的性能相结合，从而简化您的工作环境。新的思科 Aironet® 3600 系列接入点是业界首个 4X4:3 接入点，与竞争对手的解决方案相比，性能最多可提升 30%，同时具有出众的可靠性。
- 利用思科解决方案，网络可作为视频等服务以及保护人员和企业的平台。思科的网络领先地位和专业知识的使思科在提供高度安全的 BYOD 环境方面将其他提供商远远抛在后面。
- 在组织确定其 BYOD 策略后，便可以通过思科网络产品和思科身份服务引擎在所有网络环境中更加安全、可靠地调配和提供跨域应用程序和网络服务了。

策略控制的统一访问基础设施可创建高度智能的网络，从而能轻松地进行业务转变并提供卓越的保护。

有效、无缝的安全性

思科 SecureX 架构是以网络为中心的情景感知型安全方法，可在整个组织内连贯一致地实施安全策略。它使安全策略更适合业务需求，支持集成式全球智能，并可大大简化服务和内容的交付。对业务目标（例如超越 BYOD 的优化的托管体验）的支持是此方法的核心。结果是对终端用户无缝，而对 IT 组织更加高效的端到端自动化安全措施。

思科可帮助确保任何内容都能安全交付到处于任何位置的任何设备上，而不会影响用户体验。通过思科 SecureX 架构，组织可以提供灵活的端点设备选择和访问方法，同时为设备提供无间断的持续安全性。这包括浏览 Internet 或访问云服务的设备的基于云的 Web 安全性、使用常用协议（例如安全套接字层 [SSL] 和 IP 安全 [IPSec]）的自动 VPN 连接，以及与基于网络角色的访问的集成。

思科优势

- 使用网络和全球威胁智能的独特方法
- 涵盖整个组织的单一策略来源：有线、无线、远程网络、物理或虚拟设备
- 思科 AnyConnect VPN 软件中最广泛的移动设备操作系统支持，包括 iOS、Android 和 Windows Mobile
- 对设备有着最深入、最全面、最准确的了解，并且拥有唯一的基于网络和基于端点的感知功能，可确保可扩展性
- 使用现有身份感知基础设施的可扩展且灵活的下一代实施机制
- 覆盖各种使用案例的模块化方法，并且能自由地根据需要添加功能，从而能充分利用现有的基础设施
- 简单的最终用户登记和设备注册，可保证最终用户和 IT 部门的工作效率
- 从设备到控制器的无线数据安全可靠且经过加密，从而可提供更多保护并且更加合规
- 最高性能、最高质量的无线基础设施：与竞争产品相比，速度提高多达 30%，提供最佳用户体验
- 针对虚拟和原生桌面基础设施的优化体验
- 超越有线、无线和策略的统一管理
- 业界首个支持 802.11r 快速漫游和 802.11u 蜂窝与 Wi-Fi 漫游的标准



策略和执行

思科面向访问控制策略和实施的解决方案包括思科 TrustSec® 和思科身份服务引擎。

- 思科 TrustSec 解决方案提供智能和可扩展的访问控制，通过全面的可视性、特别控制和有效的管理降低整个网络的安全风险。该解决方案以独特的方式建立在现有身份感知基础设施的基础之上，同时帮助确保网络设备之间完整的数据保密性。
- 思科身份服务引擎是业界唯一的安全访问单策略平台，它集成了状态、分析和访客服务，可帮助网络做出更好的情景感知访问控制决策。思科身份服务引擎帮助 IT 管理员适应日益增多的 IT 消费设备，同时实施合规性、增强基础设施的安全并简化服务操作。

使用思科 AnyConnect 安全移动客户端的远程访问

思科 AnyConnect 安全移动客户端使用增强的远程访问技术使 VPN 体验更简单、更安全。此软件包括 802.1X 身份验证，可在行业中各种手提电脑和智能手机型移动设备中提供无间断 VPN 体验。

威胁防范

思科通过思科 ASA 5500 系列、思科 ASA CX 情景感知安全和思科 Web 安全解决方案提供威胁防御。

- 思科 ASA 5500 系列是经过超过 15 年验证的防火墙，能提供高度安全、高性能的连接并保护重要资产，从而实现最大工作效率。它可以进行扩展以满足从分支机构到企业数据中心的各种需求。思科 ASA 解决方案在独立设备中使用，也可以作为思科 Catalyst 6500 系列交换机的模块，可提供全面高效的入侵防御、高性能 VPN 和远程访问，可选的防病毒、反垃圾邮件、反网络钓鱼、URL 阻止和过滤以及内容控制。

- 思科 ASA CX 情景感知安全是一项模块化安全服务，可将 ASA 平台扩展后提供精准的可见性和可控性。该服务使用思科 SecureX 框架通过思科 AnyConnect 安全移动客户端和思科 TrustSec 解决方案从本地网络获得端到端网络智能。思科 ASA CX 情景感知安全还从思科智能运营中心 (SIO) 获得几近实时的全球威胁信息，在提供网络智能和精细控制方面其能力超过下一代防火墙。
- 思科在 Web 安全方面提供了多种选项。思科 IronPort® S 系列 Web 安全设备通过众多创新技术（包括合理使用策略控制、信誉过滤、恶意软件过滤、数据安全以及应用可视性和控制）结合在一起化解 Web 安全风险。思科 ScanSafe 云网络安全服务实现了“软件即服务” (SaaS)，无需用于维护的硬件或前期资产投入，可提供优异的实时 Web 威胁防护。

数据保护

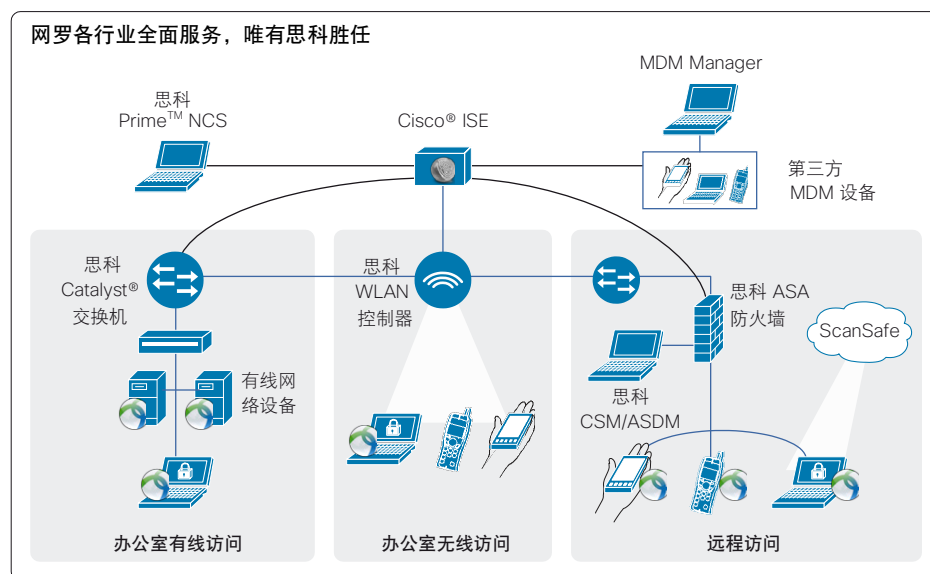
思科虚拟化体验基础设施 (VXI) 通过统一虚拟桌面、语音和视频，提供下一代虚拟工作空间。它帮助 IT 部门提供极其灵活和安全的聚合式基础设施，丝毫不损用户的体验。为确保更多保护，数据不存储在用户设备上。而对数据中心资源的安全访问在虚拟机级通过用户分段和情景感知策略实施进行。

简化的管理：充分的可视性加速了故障排除

思科 Prime™ 网络控制系统 (NCS) 是全面的管理平台，无论设备、网络或位置如何，都可将具有完整可见性的融合用户访问和身份管理集成到端点连接中。这种充分的可视性可加速解决客户端设备相关网络问题这一常见的客户难题。思科 Prime NCS 还通过与思科身份服务引擎进行集成来监视端点安全策略，以提供合规可视性。该可见性包括整个有线和无线基础设施中网络、用户和设备的实时情景信息。

图 1 列出思科高度安全的端到端 BYOD 解决方案框架中包含的产品。

图 1. 思科 BYOD 解决方案框架



为什么选择思科？

思科在安全网络领域处于领先地位，在网络安全创新方面有着有据可考的骄人纪录。思科 SecureX 架构以独特的方式将三种主要元素结合在一起：提供情景信息并以一贯的方式实施安全策略的网络；全球威胁智能；以及业内最广泛的安全产品组合之一。

更多详情

<http://www.cisco.com/en/US/products/hw/vpndevc/index.html>