华为移动办公解决方案白皮书

华为技术有限公司

HUAWEI

商标声明

HUAWEI 和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

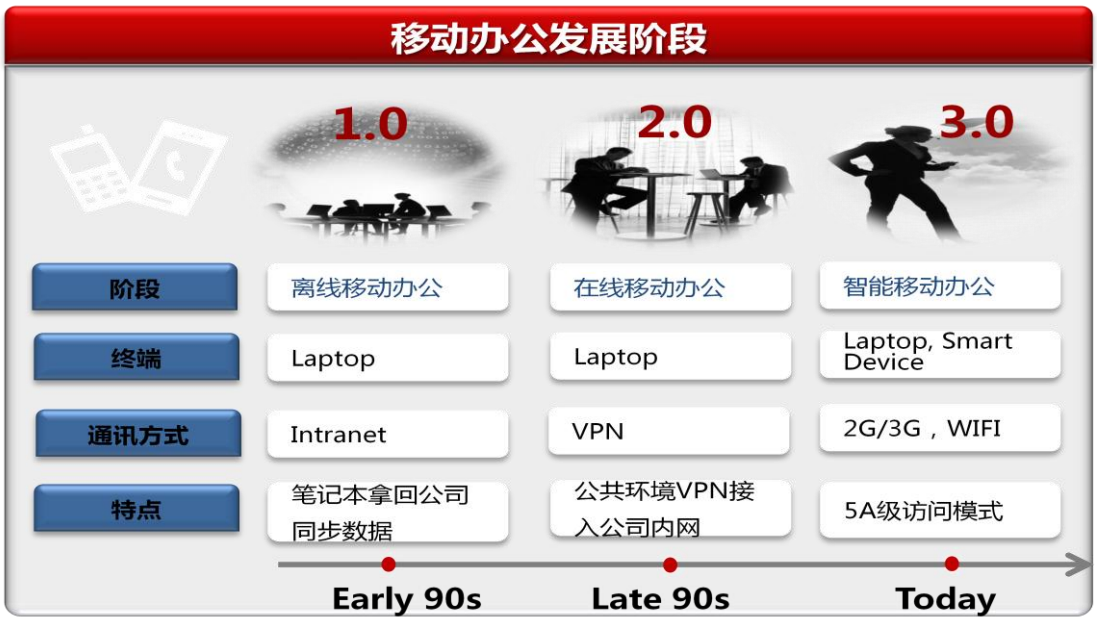
1 趋势

1.1 BYOD 引领移动办公 3.0 时代的到来

BYOD（Bring Your Own Device） 指自带设备进行办公，这些设备包括个人电脑、手机、平板等智能终端，通过这些智能终端，员工可以在任何时间，任何地点进行收发公司邮件，访问公司资源，对公司的业务进行处理，实现移动办公。

BYOD 代表了一种现象，个性化、移动化、智能化，人们的生活和工作被各种各样的智能终端连接到一起，办公不在局限于办公室内传统的PC机，自带设备已经成为了一种潮流，它使得办公和生活的界限变得模糊，让办公有更好的体验。

1.1.1 企业移动办公的发展历程



BYOD不是一蹴而就的现象，是伴随先进的通信和IT技术的发展出现的办公新模式。企业办公从“固定”场景到“移动”起来，从地点限制到无处不在，经历了三个发展阶段（本文主要探究移动办公的发展历程）：离线移动办公、在线移动办公、智能移动办公（**BYOD**）。

Mobile Office 1.0：离线移动办公时代

90年代早期，笔记本电脑和移动终端（PDA）的出现和普及，员工可以带着笔记本电脑和PDA在任何地方均可以工作，但是由于通信技术的局限性，访问公司内部网基本上无法实现。信息交换是通过回到办公室后的同步来实现，这个时间主要是邮件同步、日常文档同步和相关的工作内容交换。

Mobile Office 2.0：在线移动办公时代

随着互联网普及和VPN技术的出现，使移动办公得以真正的实现，员工借助VPN提供的安全通道可以安全地接入运营商提供的网络，在旅馆或国际会议现场接入到公司内部网，实现在线的移动办公。

Mobile Office 3.0：智能移动办公时代（BYOD）

通信技术和IT技术大发展的今天，特别是宽带、3G移动通信技术的应用为移动办公带来了质的飞跃，加上大量智能终端涌现，通过移动网络实现无处不在的接入，使

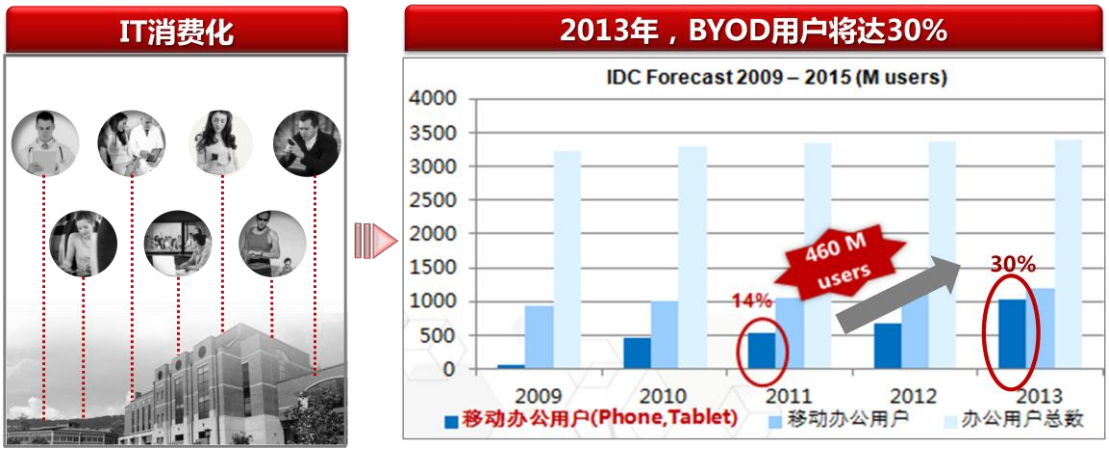
企业办公进入了5A级智能办公时代，即任何经过授权的人(**Anyone**)，利用任何智能设备(**Any device**)，在任何时间(**Anytime**)，任何地点(**Anywhere**)，通过网络访问任何办公资源（**Anything**）。

1.2 ICT 技术的发展催生了移动办公新模式

移动办公3.0是信息通信技术（ICT）发展的结果。随着社会信息化的发展，出现了大量多元化的移动终端，改变了人们生活与工作的传统模式,打破了时间、地域的限制,给予人们更多的获取信息的手段。伴随着宽带与无线通信技术的发展,人们已不满足于固定地点与固定方式的连接，希望随时随地获取和处理重要信息，手机智能化，平板电脑的出现，以及社交网络的延伸，实现了人们自由办公的愿望，使人们的沟通无所不在，工作和生活的界限变得日益模糊，加速了移动办公新模式的出现——自带设备办公（BYOD）。

移动办公经历了由“离线”，到“在线”，再到“智能，实现了办公模式的飞跃，从最初的只能在公司进行移动数据的同步，到可以在特定场所进行实时的公司数据访问，再到现在的智能化阶段，可以在任何时间，任何地点，用任意的智能终端，通过任何网络进行公司的数据访问和业务处理，实现了**“安全”**、**“效率”**和**“体验”**的完美融合。

1.2.1 IT 消费化把智能终端带入办公环境，体验无处不在



IT 消费化趋势推动了个人设备在企业办公过程中的使用。“IT 消费化”是全新信息技术最初出现于消费者市场，然后渗透到企业，大量的可随时在线处理数据业务的智能终端出现在人们的生活中，人们在享受智能终端带来的方便和乐趣的同时，也把它带入到了办公领域中。使办公突破了原有的固定和死板，员工可以通过智能终端在任何地方进行办公，享受终端带来的完美体验。

全球知名调研机构IDC 的数据显示，2011年全球智能手机出货量预计达到4.72亿部，超过了PC的出货量，而2010 年为3.05 亿部。据IDC 预计，这一数字有望在2015 年末翻倍至9.82 亿部。同时，自带设备（BYOD）办公的比例从2011年的14%将提升到2013年的30%，预计2014年将超越传统的移动办公模式，成为办公的主要方式。

1.2.2 IT 移动化使办公随时发生，效率迅速提升

通信技术的发展，加速了运营商网络的建设，特别是移动网络大量覆盖到城市的各个角落，3G/4G的技术发展，使得智能终端可以直接接入移动网络，人们可以在任何时间、任何地点进行沟通；企业借助运营商网络的延伸，使得办公走出了传统的办公室，企业员工可以通过移动设备在任何地方进行办公。

过去，企业员工在出差或不在公司时无法及时获取公司的相关信息，导致管理人员不能及时处理审批，销售人员不能实时获得库存信息，流动人员实时处理订单，导致企业错过了很多的商机。现在，员工利用智能终端，通过WIFI/3G等无线网络实现和办公网络的联接，可以在咖啡馆里、机场、公园和广场等不同场景下进行移动办公，解决企业传统办公面临的各种问题，提升企业办公效率。

1.2.3 IT 分布化使企业资源走出 Intranet，需要安全的访问

过去，企业的资源因种类少，数量小，通信技术单一，只局限在自身的Intranet中，员工访问只能通过公司内网。随着通信技术和安全技术的发展，使得企业内网可实现与外网的安全联接，内外网互相访问成为可能，企业通过不断壮大，IT资源的种类和数量成倍增长，云计算技术，数据中心，虚拟化技术的应用，让企业的资源实现了分布化，资源之间通过网络联接，员工可以在任何时间，任何地方进行公司资源的访问。

企业IT资源的分布化使得对信息安全的管控变得更加重要，安全访问成为移动办公3.0时代CIO们首先要考虑的问题，企业迫切需要建立一个端到端的安全访问策略，保障员工的终端不发生安全问题，保障企业网络不被攻击，保障企业的应用资源不被非授权者访问，同时考虑对移动设备的安全管理。

1.2.4 小结

“体验”、“效率”、“安全”是移动办公3.0时代的特点，同时也是对企业IT系统提出的挑战，BYOD移动办公解决方案需要充分考虑这三点的结合。

如何把IT与CT技术无缝融合到移动办公3.0中，使ICT技术既能够保证企业资源的安全，同时又能够提升网络接入的效率，移动办公的效率，最终给员工带来好的办公体验，消除工作和生活的对立面，带来和谐的体验，是3.0时代每个CEO,CIO都需要慎重考虑的问题。

2 挑战

BYOD是一种潮流，对于传统的工作模式带来了新的变革，也带来了很多新的挑战。这些挑战是一个变革和改进的过程中存在的阻力，也是驱动发展的动力，需要有一个清晰的认识。

2.1 用户面临的挑战

对用户来说，人手一个或者多个移动终端设备，通过大量新兴的高效率应用软件、生活助理和交流平台来进行工作和生活，把烦人的工作融入科技的便利性中，是一件快乐的事情。同时私人设备的特性，也带来很多的不安，企业应用需要安全，而如何保护私人信息的安全性同样重要。

2.1.1 一致性体验的需求

多样化的设备是移动市场非常精彩的一面，给予用户更多的选择，细分了市场，满足了不同层次的需求。BYOD的特征决定了多平台的接入可能性，而对于用户而言，则面临了用户体验的课题。员工在使用自带设备时，希望接入公司的网络非常简单，不希望做太多的设置，并且希望相关应用能与日常工作时的体验一致，或者有比他们日常工作时更好的体验。

不同平台和设备间操作习惯的保留，让用户尽快的熟悉新软件和新平台，尽量在心理舒适区间中提高对新事务的接受程度，由此可以达到提高工作效率的目的，特别是对于对此BYOD犹豫的用户，尤为重要。

2.1.2 个人隐私的保护

隐私是一个重要的课题，自带设备来办公，如何保护自有信息的不被过渡监控？相信在BYOD的安全课题中，业界关注公司的信息不被泄露，安装特有的手机程序和监控应用软件。员工个人的信息和公司的信息都在同一台设备上，员工最关心的是个

人的隐私数据，需要将相关的监控和管理控制在合适的度量内，保证企业信息的安全同时，也保证用户私有信息的安全性，有效的保护个人隐私。

2.1.3 设备的控制

移动终端是一个开放的平台，可以安装软件满足各种各样的诉求，也可以进行BYOD，结合企业的相关应用。这里就带来一个课题，设备如何进行管理，该管到什么样的度。

BYOD的第一特征就是自带，也就是员工自有的设备，在相关的法律范畴内，所有权的定义也从另外一个方面陈述了这样的一个实事：员工享有设备，他们需要对设备有绝对的所有权和控制权。从某种意义上讲，BYOD是员工和企业双方的一个妥协，在控制这个角度而言，员工需要认可企业处于安全考虑下所执行的控制政策，严格的登录授权、设备安全控件等等。不过设备还是员工自己的，在双方达成契约即BYOD的形势下，员工还是享有在所属终端的控制权，而企业也需要在合理的范畴中，诉诸自己的控制和管理。

2.2 IT 系统面临的挑战

企业的IT主管可能是会对BYOD抱有很多的问题，一方面采用BYOD，他们需要面对很多的变化和调整，会增加他们额外的工作和责任，但是另外一方面他们又是企业架构改进的责任者和推进者，任何的技术革新和变化都能带来效率和效能上的提升，由此就有了革新的动力和目的，IT主管们如何看待这些挑战？

2.2.1 自带设备的管理

自带设备办公中，企业对员工更加开放，员工可以携带多种多样的设备进行办公，企业需要应对不同种类的自带设备，完全开放所有类型的自带设备办公对企业是笔巨大的投资，企业的IT管理者出于成本的考虑，会对自带设备的种类、系统和应用软件做出限制，保证大多数的主流的智能终端都能在公司使用，满足主流设备的应用，使大部分员工都能用自己喜欢的自带设备进行办公。

大量自带设备的使用，设备管理是个巨大的挑战，据统计每年的个人设备丢失率是在15%，企业IT管理者需要为员工设备丢失后，或者员工离职后，如何处理在员工自带设备上的数据进行细致的考虑，保证企业的信息安全。

2.2.2 自带设备的安全管理

自带设备进行办公，安全是前提。员工带了哪些自带设备，在什么地方接入了公司的网络，这些自带设备是如何登陆的？这些登陆是否有安全隐患，是否会导致企业的信息泄露或者被监听，这都需要企业IT管理者对员工的接入有全面的掌控，从而保证企业网络的安全，避免企业网络遭受病毒攻击或是员工信息被窃取。

自带设备在进入公司网络后，为了保护企业信息安全，企业要知道员工的自带设备都在做什么，员工的自带设备在接入公司网络后，有可能长时间什么也不做，有可能一直在访问某些数据，企业IT管理者要对什么也不做的终端进行强迫下线，避免有些恶意攻击者利用已经登录的账户进行非法数据的访问，企业同样要对员工的正常访问进行查看，这样能知道员工用什么终端在什么时间访问了什么数据，这些是企业IT管理人员需要知道的。

2.2.3 自带设备的策略管理

自带设备进行办公，策略管理是必备的条件，良好的策略管理保证自带设备不会给企业造成安全威胁。自带设备在进入公司网络时需要有一个完善的接入策略，保证终端都能按需要进行接入，公司配置的智能终端跟员工自带的智能终端有不同的接入策略；用户在不同场景下页有不同的安全策略，在公司和在公共场合和家庭的策略是不同的，不同的设备、角色和场合有不同的策略，这些需要企业IT管理者根据企业的实际情况进行针对的策略制定。

自带设备访问数据，要有不同的访问策略，企业的一般数据全员都有访问权限，企业的核心数据和核心战略，只有企业的高层管理者才有权限进行查看，企业配置的设备有更多的访问权限，自带设备根据不同的接入场合有不同的访问权限，如：自带设备在公司里可以访问企业的研发资料，在家庭和公共场合智能进行一半的企业流程处理。

自带设备的管理需要一个统一的策略，使员工的自带设备在企业的网络中得到更好的管理，从设备的接入、网络选择、数据访问等都需要一个可视的统一的管理，保证企业的信息安全。

2.3 部署面临的问题

BYOD是全新的课题，将企业相关的流程和应用结合进更为广泛的工作环境中。

这样就不仅仅是升级设备那样简单，而是对企业架构的一次重新审视。不过从无数次的历史中可以看到，开放的心态能促进技术的进步和生产力的提高。当BYOD已经来到的时候，用积极和开放的心态去看待，可能你已经走在变革的前端。

2.3.1 现有公司网络的改造

满足自带设备的接入，企业网络需要进行相应的改造，使企业能能快速响应自带设备接入。企业需要部署一个弹性的、开放的、可以与已有网络架构兼容的BYOD网络架构。

授权用户进行自注册，给予用户一定的灵活性，使其快速接入网络，让员工可以聚焦到企业业务上。

2.3.2 安全策略的制定

自带设备在企业应用面临的最大问题就是安全问题，设备的接入安全策略是所有安全的基础,只有保证自带设备安全的接入到企业网络中,才能保证后续的网络安全，应用访问安全是核心，企业的数据需要全面的保护，管理贯穿整个安全流程，完善的安全策略是自带设备成功在企业应用的前提条件。

2.3.3 公司新制度的制定

自带设备进入到办公领域,企业需要有新的规章制度来满足自带设备的安全管控，保证企业的信息安全，员工要知道自带设备能做什么，不能做什么，对自带设备的使用有明确的认识，同时也使公司对自带设备的管理更加简单。

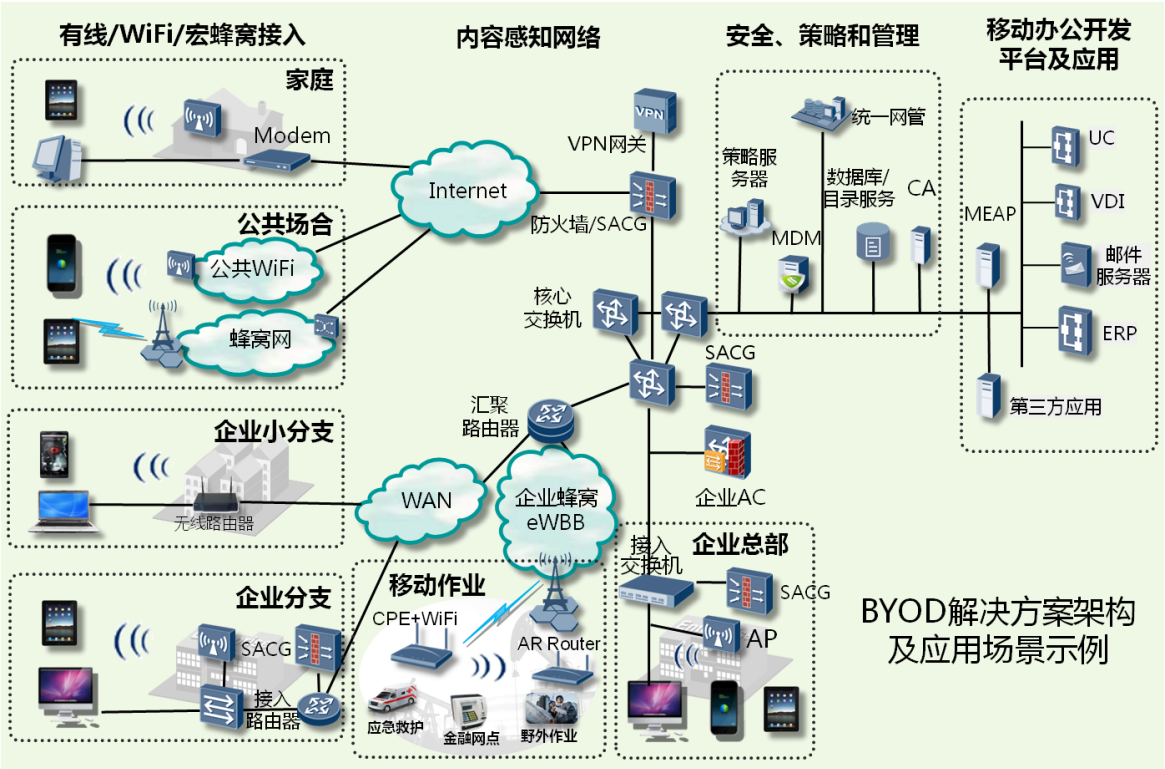
3 解决方案

华为有着企业网络、安全、统一通信与协作、IT、无线、终端等在内的齐全产品线，对ICT发展有着深刻理解和把握。华为移动办公解决方案有效解决BYOD在部署过程中面临的策略、安全、网络、管理和应用等方面的问题，支持各种企业BYOD战略，提供安全敏捷的企业BYOD移动办公空间。

3.1 华为移动办公解决方案架构

完善BYOD解决方案可以提供一个无处不在的网络（固网、WLAN和蜂窝），支持不同种类的自带设备安全访问企业网络，保持自带设备的良好用户体验，提升用户满意度和工作效率。

有着齐全ICT产品线的华为，借助对电信运营、企业运作、客户体验的深刻理解，设计提供完整的BYOD移动办公解决方案，覆盖企业总部、企业分支、企业小分支、移动作业、公共场合、家庭等应用场景。



3.2 华为移动办公解决方案特点

◆ **安全防护，一网通行**

- 网络不裸奔，全网数据监控
- 数据不泄密，移动应用控制
- 管理不担心，设备统一管理

◆ **高效网络，无处不在**

- 覆盖范围广，接入速率高
- 业务部署快，开通效率高
- 简易安装，便捷网优
- 节能环保

◆ **协同办公，一致体验**

- 业务不间断，有线无线无缝切换
- 终端多样化，业务一键切换
- 应用智能化，感知无距离

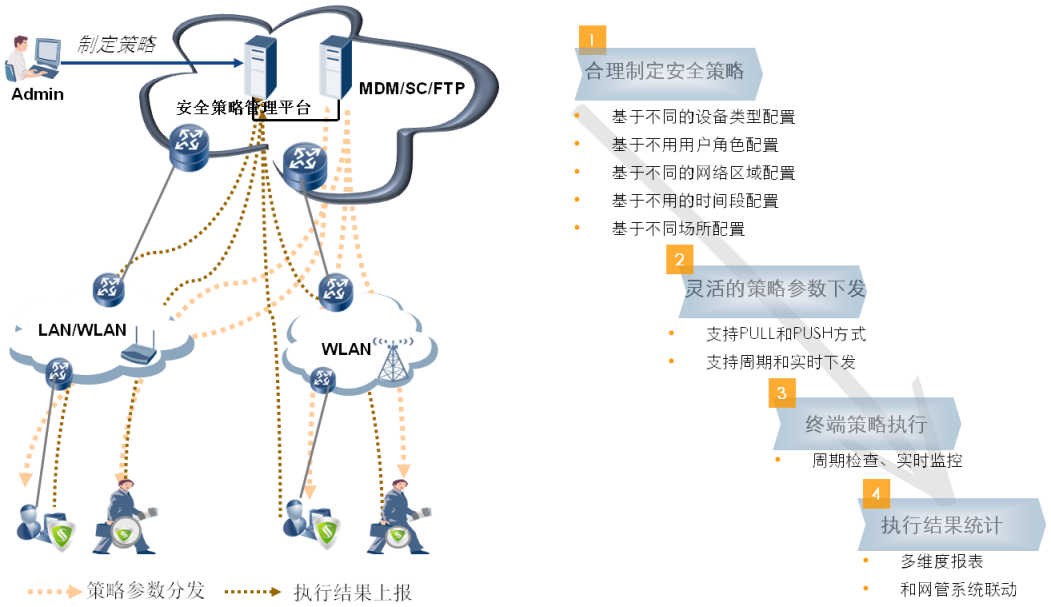
3.3 安全防护 一网通行

华为BYOD移动办公安全解决方案，基于统一策略，执行终端安全和管道安全，保障自带设备移动办公享受到全方位的安全防护。

3.3.1 统一策略

华为BYOD统一策略方案能够在整个组织内根据不同用户角色、不同设备类型、不同场所、不同时段、不同区域采用不同的策略，确保对资源的安全访问。统一策略方案实现与移动设备管理（MDM）解决方案的策略集成，提供涵盖整个组织的单一策略来源（有线网络、无线网络、远程网络、物理设备、虚拟设备），对移动设备实施完善、最准确的管理，为用户和IT部门提供了优良的体验、又不影响安全性、可见性和控制力。

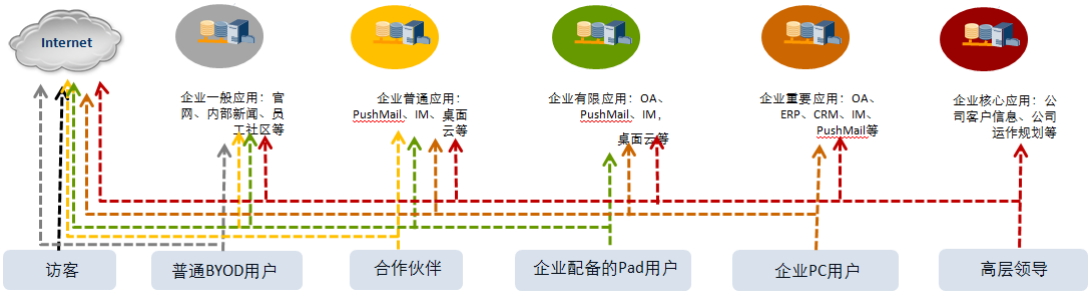
华为BYOD统一策略管理流程如下：



■ 访问控制策略

华为BYOD方案支持多种准入控制手段，包括安全准入控制网关SACG、802.1X交换机、NAC安全接入网关以及基于终端主机防火墙的软件准入控制。把准入控制与终端的安全状态相结合，对于不符合安全策略的终端进行隔离修复，强制终端用户实施企业的安全策略。IT部门能够制定用户使用何种设备、在何时、在何地、如何访问公司网络的策略，控制接入网络的终端用户网络访问权限，实现最小授权访问控制。有效防范非法终端对企业业务资源的访问，确保业务正常运行，保护公司信息安全。

BYOD访问控制应用场景举例如下：



- 对于企业高层领导，根据其身份和角色定义，允许访问所有的网络资源；
- 对于内部员工，提供相对宽松的模式，允许员工访问完成工作必须的业务系统。对于少数的重要业务系统，禁止一般的员工访问；
- 对于企业配备平板的用户，接入网络后只能访问企业配给的相应企业业务资源，不能访问其他的企业资源；
- 对于合作方员工，提供严格的控制模式，只允许合作方访问特定的业务系统；禁止访问重要的业务系统和一般的办公系统；允许根据安全策略，定义是否允许合作方的员工通过企业的网络访问互联网；
- 对于普通BYOD用户，例如：员工使用自己的移动终端接入、只能访问企业普通的业务资源、不能访问企业重要的业务系统和重要的办公系统；
- 对于访客，禁止访问企业的内部网络资源，包括重要的业务系统、一般业务以及合作方共享系统等，只允许访客访问互联网。

■ 安全加固策略

BYOD接入网络中，病毒、蠕虫和间谍软件等网络安全威胁损害客户利益。移动用户能够从家里或公共热点连接互联网或办公室网络，常在无意中被感染病毒并将其带进企业环境，进而感染企业网络。企业网络中可能存在大量易感染终端，这些终端可能存在安全漏洞，或者终端安全设置不当，容易被探测和攻击，或者没有部署杀毒软件或杀毒软件没有及时更新。

对于如上现状，IT部门可以通过配置检查检测防病毒软件策略检查终端是否安装了企业规定的杀毒软件（可以选择多种），以及杀毒软件是否更新，作为判断终端当前安全状态的一个依据，阻止没有部署杀毒软件的终端或者杀毒软件长期不更新的终端接入网络。保证企业内网运行的终端杀毒软件能够及时更新并且有效运行，减少病毒感染和扩散的风险。通过配置检查屏保策略、检查文件共享策略、检查账户安全策略等来弥补员工由于安全保密意识薄弱带来的安全漏洞，保护信息安全。

系统漏洞是当前局域网的一个重大风险，如果局域网内存在大量没有部署关键补丁的不安全终端，局域网遭受病毒攻击并且导致网络拥塞的风险就会变大。终端及时

部署安全补丁，减少局域网脆弱主机的数量，能够大大减少病毒在网络中大面积传播的风险。华为BYOD统一安全策略方案把补丁的检查作为一个重要的检查项，支持检查操作系统补丁、IE的SP补丁、OFFICE的SP补丁等。当检查到终端没有部署必需补丁的时候，能够协助终端快速完成补丁修复。

■ 行为监控策略

企业除外部黑客、病毒攻击带来的安全威胁外，移动存储介质滥用、IM监控工具的使用、非工作时段的web访问、不安全的WiFi接入、个人外设使用等带来的内部安全威胁也不容忽视。企业员工对网络资源的不合理使用，不仅严重影响工作效率，而且还存在违反法律法规的风险。

华为BYOD安全策略可以管理Modem、ADSL、ISDN、PPPoE拨号设备，禁止终端用户使用拨号设备，防止终端绕过企业的监管连接互联网，使得企业网络直接面对来自互联网的攻击。也可以根据需要，允许通过拨号接入互联网，但是对于拨号等行为进行审计，记录拨号开始和结束的时间。可以监视非法架设PROXY服务器的非法外联，当发现违规架设PROXY服务器，可以记录违规PROXY服务器的地址/端口等信息，上报服务器，由管理人员进行跟踪和处理。确保企业的所有互联网出口流量都经过统一架设的出口网关，通过出口网关过滤不安全的网络访问，保障企业内网安全。提供WEB访问监控功能，记录终端用户的WEB网站访问信息，上报服务器进行统一管理和审计。通过这样的手段，一方面可以管理员工的上网行为，上班时间屏蔽一些与工作无关的网站；另一方面，提供审计和责任追溯的途径。

华为BYOD安全策略提供USB设备管理，能够区分USB鼠标/键盘和USB存储设备，针对USB存储设备，提供允许/禁止/只读控制能力。提供USB存储设备文件操作的监控功能，能够识别和记录创建文件、拷入U盘、拷出U盘、内部复制、删除文件等操作，并且上报服务器进行审计。提供U盘加密功能，在启用加密写功能后，终端用户拷贝到U盘的文件都是经过加密的，只有该企业的用户并且安装了TSM安全代理的终端，才能查看和使用这些加密文件。U盘加密功能对U盘没有特殊的要求，使用普通的U盘即可提供该功能，并且使用U盘加密功能，并不会破坏该U盘上原有的非加密数据，加密数据和非加密数据能够同时使用。

■ MDM管理策略

为确保移动设备上的数据合规，华为BYOD方案借助MDM管理策略，使得管理员可以更加清楚地了解终端设备状态，根据终端设备对于公司策略的符合情况控制这些设备对公司的访问（例如要求注册、要求锁屏、禁止越狱），并能远程卸载非法软件、

远程擦除丢失或被盗移动设备上的数据。

■ 基于终端属性的策略控制

BYOD接入网络后，将自身终端的DHCP、HTTP等报文重定向给策略引擎，策略引擎通过解析报文可以提取用户名、设备类型等信息。接入设备内置探针，从终端的LLDP、DHCP、HTTP等报文中提取设备信息，通过Radius协议或SNMP Trap形式将这些信息上报给策略引擎。

3.3.2 终端安全

统一客户端的“终端安全”保障手段包括接入认证、准入检查、权限控制、“安全沙箱”及MDM安全管控。这5部分环环相扣，从终端接入、数据访问、数据存储等不同角度保障企业数据在BYOD终端上的安全。

■ 接入认证

BYOD设备往往具有机型多样、操作系统多样、版本多样的特点，因此，这些设备对各种接入认证方式的支持程度、实现技术也存在不同程度的差异。

华为BYOD移动办公解决方案提供了丰富多样的用户认证方式，其中包括1）用户名、密码认证；2）支持通过RADIUS、LDAP、AD、SecurID服务器等进行远端认证；3）支持移动智能终端音频Key证书认证；4）用户登录时，客户端软件提取终端的硬件特征码发送给接入网关进行匹配，只有帐号和硬件特征码都通过网关校验的终端才被允许接入。这种手段在提高认证强度的同时，也对同一帐号关联的硬件特征数作限制，从而控制接入企业的BYOD终端数量、减轻管理负担和开销、降低不合规终端接入的可能性。5)支持上述多种认证方式的组合认证 ,以进一步提高对用户的认证强度。譬如，要求用户必须同时通过VPNDB认证和证书认证才可登录网关。

这些认证方式不仅能有效识别合法和非法用户、实现接入控制，而且由于解决方案为各类主流智能终端操作系统（iOS、Android、BlackBerry、Symbian、Windows Mobile等）都提供了上述认证方式的支持，企业可根据接入认证要求的安全强度，选择合适的认证方式，譬如，安全强度要求较高，则可选择证书认证接入，而不必顾虑BYOD设备机型多样、操作系统多样而可能带来的支持程度差异、甚至无法全部支持证书认证的问题。

■ 准入检查

“准入检查”是指在移动终端接入企业内网之前,对终端的安全合规性进行检查。

用户会根据个人的喜好和需求对BYOD设备做各种安装和设置，而处于这种状态的设备直接连接企业内网是有安全隐患的， 譬如，用没有设置锁屏密码的手机直接访问内网数据，一旦用户丢失了手机，其他非法人员就能直接看到手机上打开的企业数据。

在接入企业内网之前，对BYOD设备进行合规性检查显得尤为重要。基于终端准入检查策略,企业管理员可以根据实际需求给终端下发各项策略,比如,1)密码策略。具体包括是否强制设置锁屏密码、密码的最小长度、密码过期时间、自动锁屏时间、检查新旧密码是否相同、密码出错尝试次数限制（若超限则启动擦除）等。2）应用控制策略。通过使用应用控制策略，可以定义哪些应用是必装的，哪些是允许安装的，哪些是不允许安装的。

若终端不满足准入检查策略，则客户端弹出提示消息，提醒用户作出相应修改，否则不允许接入企业网络。

■ 权限控制

自带设备用户通过认证和准入检查后，完善的访问权限控制策略对企业内的不同用户进行精细的访问权限控制，比如:

1) 企业邮箱的邮件转发、附件下载、附件上传、附件在线浏览权限的控制；
2) 安全浏览器对企业内网URL访问控制、上传和下载文件的权限控制；
3) 离线使用移动办公客户端权限的控制；
4) 为不同权限的用户呈现不同的企业应用、赋予不同企业应用的使用权限；
5) 针对设备归属的权限控制策略;
6) L3VPN资源访问权限的控制;

这些策略仅在用户使用移动办公客户端时控制和限制用户对企业内网资源的访问，而不对BYOD设备使用用户个人数据和应用产生任何影响,不影响BYOD设备的用户体验。

■ 安全沙箱

不同于传统的办公用固定PC、手提，也不同于“标配机”，BYOD设备存在个人数据和企业办公数据并存的现象，如何保证这两类数据的隔离、既保证企业数据的不

被泄密又不影响BYOD设备用户的个人体验、不侵害用户的个人隐私是BYOD方案的关键点之一。采用“安全沙箱”技术应对以上问题。

1) 数据本地加密

通过安全浏览器访问企业内网的过程中，在终端本地生成一些临时文件、Cookie、浏览历史记录以及用户下载文件等数据会被自动地加密保存。

通过安全邮件客户端下载的邮件、邮件附件也会被自动加密保存在本地。

数据在线加解密，本地加密数据、文件的密钥不在移动终端上保存。只有用户成功登录了SVN网关，才能从网关上获取定期变更的解密密钥。

2) 数据隔离

不允许企业数据和个人数据之间进行拷贝、剪切、粘贴等动作。

从企业角度看，这种手段既保证企业数据不被外泄，也可防范个人数据中可能存在的企业违规信息（如新闻、娱乐信息）及病毒、木马等非法程序在企业内部进行传播和感染。

从用户的角度看，用户个人数据都被隔离在“安全沙箱”之外，因此，不必担心个人数据会在移动办公的过程中流入企业内网而引起个人隐私泄露。

3) 访问痕迹清除

企业管理员可通过管理后台给终端下发“访问痕迹清除”策略，即在企业用户退出安全浏览器时，自动清除访问期间生成的临时文件、Cookie及浏览历史记录等信息。

4) 虚拟桌面/虚拟应用

通过虚拟桌面，移动智能终端用户可以安全地远程登录到SVN虚拟网关，从而实现对内网办公PC或服务器的访问。不同于传统PC虚拟桌面软件，SVN推出的虚拟桌面/虚拟应用软件支持Android/iOS等主流移动智能操作系统。

企业用户可通过SVN VDI加密访问企业内网的办公PC或服务器，但企业内部的任何数据均被保存在企业内网的PC或服务器上，无法将虚拟桌面/虚拟应用拷贝到企业外部。

■ MDM安全管控

除了通过“安全沙箱”保障访问企业内网时的安全性，如何避免用户在移动终端上的其他操作（如对企业公文浏览页面截屏并外发）可能带来的安全隐患？在移动终端不慎丢失后，如何避免终端的数据泄露？是否有办法把终端找回？ 这些问题通过“MDM安全管控”环节可以得到妥善解决：

1) 设备硬件控制

对移动终端设备摄像头/蓝牙/Wi-Fi/USB网络共享/GPS/VPN/蓝牙扫描/启动热点功能/USB存储模式/麦克风/云服务和备份服务/截屏的控制 ,管理员可根据企业的实际情况下发策略，在员工接入企业内网期间，禁用其中的部分或全部功能。

用户在退出时，系统会自动将这些配置恢复到登录前状态，不影响用户在非办公期间的BYOD设备使用体验。

2) “越狱”检测

若检测到终端“越狱”，则根据策略做不同级别的响应：审计、提示、告警或断网。

3) 行为监控

监控员工在接入企业内网期间的网络传输、文件操作等行为，记录日志并发送后台进行审计。

4) 远程锁定/GPS定位/远程擦除

若终端丢失，员工可通过自助管理页面对BYOD设备进行远程锁定和GPS定位；若确认无法找回终端，可以远程擦除终端上的数据。

在员工离职、更换办公终端等场景下，管理员也可通过管理后台给BYOD终端下发选择性数据擦除指令，即仅仅擦除企业数据和卸载相关应用，而保留BYOD终端上所有的个人数据，这样既保证企业数据不外泄，又不破坏用户个人的数据和应用，用户完全可以继续正常使用自己的个人终端。

5) 数据备份/恢复

备份通讯录、日历、邮件等关键数据到企业备份服务器。若终端丢失，可从备份服务器将相关数据恢复到其他办公终端。

3.3.3 管道安全

管道安全提供加密隧道传输能力，有效保障企业数据在传输途中不被非法窃听和篡改。与之配合的Eudemon防火墙设备，则提供病毒检测、IPS入侵防护、URL过滤、网络攻击防范、ACL过滤、应用程序流控等能力，进一步保障企业数据在自带设备上传输的安全。

■ 传输加密

安全邮件客户端模块、安全浏览器模块、VDI、eSpace等集成了安全SDK的第三方应用都是传输加密的（L4VPN）；而集成了L3VPN虚拟网卡的华为手机、平板也可对相应应用进行传输加密，保证自带设备传输数据的安全性。

解决方案支持标准的L2TP over IPSec方式对数据传输进行加密。

■ 流量监控

自带设备发起的数据在到达SVN之前会先经过防火墙设备。报文只有通过了包过滤、会话检查、DDoS攻击防范等网络威胁防护环节，才能被路由分发到SVN设备。

报文经SVN设备解密、解封装回注防火墙，防火墙再对这些报文中的明文数据进行URL过滤、病毒和木马的检测和过滤、入侵检测、DDoS应用层攻击检测和过滤，最后才将干净的流量送往企业内网。

相应地，来自内网服务器的应答在到达用户终端之前，也会经过防火墙的上述防护环节。

3.4 高效网络 无处不在

为了保障大量自带设备进行移动办公，企业需要提供大容量、高密度的WLAN覆盖，便于所有自带设备都能迅捷接入网络，进行高速访问。在企业WLAN网络覆盖之外，员工自带设备可在移动运营商的蜂窝网络与WLAN网络之间漫游切换。通过网络加速优化广域网，可使BYOD用户获得最佳体验。

3.4.1 企业 WLAN 网络高密覆盖

高密的WLAN网络覆盖能让更多的自带设备接入到网络中，通过无线漫游、故障诊断和干扰定位等功能，保证自带设备上业务的不间断，当出现故障时，及时进行故障的定位和干扰排除。

■ 高密覆盖

通过智能多用户调度，自动感知自带设备的数量，灵活调整物理信道竞争参数，降低碰撞几率，大大提升网络的吞吐量，有效提升用户体验。实现在高密度覆盖场景，AP部署数量可减少30%；20用户时上行速率比普通AP高一倍；下行速率高32%。

1) 千兆11ac AP：1.3Gbps@5G，兼容11a/b/g/n，满足高带宽、高密度覆盖

2) 3*3 11n/11ac 智能天线提升网络吞吐量：智能天线动态检测用户位置，根据用户位置发射信号，减少干扰；强干扰环境下，空口吞吐量可提升40%

3) 万兆接口高带宽AC：11n/11acAP的部署，作为业务的集中处理单元，GE 接口的AC已不能满足需求。万兆AC的部署，对高密覆盖场景，减少上行交换机端口和AC数量的需求

■ 无线漫游

自带设备的用户在WLAN的一定范围内可以自由漫游，且在移动过程中保证已有业务不中断，提升用户的移动体验。

■ 故障诊断

网管服务器侧预集成客户侧诊断项，支持诊断项动态增加，同步推送信息到客户端。当自带设备用户首次连接时，自动诊断终端环境配置、网络配置参数、自修复已知问题，用户不需要对终端进行额外配置。出现故障时，用户可以自行进行排查、修复。

当自带设备出现网络故障无法接入时，基于用户名、MAC、用户位置eSight进行一键式诊断。故障状态包含无连接、802.11连接、认证、IP地址分配、成功等状态，故障点包含无线&有线网络、Radius server、DHCP server等。 针对失败的故障诊断自动发起诊断项清单检查，确定失败具体原因及修复建议。

■ 干扰定位

当WLAN网络出现信号异常时，通过AP所在位置的频谱分析信号，显示干扰源类型，排查故障隐患。系统检测干扰强度、干扰位置以及发生时间，及时告警通知网络管理员，帮助快速定位，根据干扰源检测结果来进行网络调优。

■ 精准部署

使用WDA（ WLAN Deployment Accuracy）设计模型，基于业务/用户/终端三维度定义合理门限，对部署区域进行评测，依据评测结果进行精准部署。

3.4.2 电信级 WLAN 与蜂窝网络协同运行

用自带设备进行办公，经常会在蜂窝网络和WiFi网络间进行切换，华为通过无线基站领域的经验积累，实现了WiFi和蜂窝之间的无缝切换 ,保证了用户的业务无间断，提升了用户的办公体验。

■ 电信级WLAN产品

高集成度路由器架构的AC有着高转发能力，支持灵活组网形式。高可靠性AC支持设备间与设备内热备，多种备份方式灵活选择，既提高可靠性又不增加过多投资。

华为是无线基站产品的领先设计者，RRU 模块经过防水、振动、冲击、碰撞、温度循环、交变湿热等系列测试，可靠性获得全球100多个运营商网络验证。WLAN AP继承了无线产品的可靠性设计技术，经过严格的防雨、高低温环境等测试，可靠满足电信级网络要求。

根据定期上报的无线环境信息，网络自动选择合适信道，减小网络内/网间同频干扰，以及非WLAN设备的干扰。AC根据无线环境的变化自动调整AP发射功率，控制AP覆盖 ,在满足覆盖要求的前提下降低干扰。网络基于用户数和流量的智能负载均衡，提升系统性能。

■ WLAN与蜂窝网络协同

WLAN与蜂窝网络多层面融合，充分发挥多网协同特点，网络效益最大化。蜂窝网络将WLAN热点推送给用户 ,帮助用户及时发现和接入热点 ,提升用户体验。WLAN基于TGW可信接入PS域，提供无缝业务体验。 WLAN和蜂窝使用统一认证/计费，提升用户感受。

■ CPE+WiFi完成最后一公里

配置有蜂窝通信系统的大型企业可以采用CPE+WiFi AP解决最后一公里接入问题，避免对特定制式终端的依赖性，改善移动办公网络环境，有效提升蜂窝网络资源利用率，支持移动作业的数据业务需求。

■ 精确选点与部署运维

蜂窝网络采集终端行为、业务识别等数据，通过栅格化的数据业务话务地图呈现热点，结合实物地图最终确定需要部署的WLAN热点。热点精确定位指导选址，可帮助避免“盲目部署”、“热装冷用”，大大缩短建网周期。精细化网络分析可提供精细化管理和咨询决策，网络综合评估可做分流效果评估、现有各网络扩减容评估等。

采用大容量电信级网管，在网络级、AC级和AP级之外，引入AP域级管理，按AP布放密度划分不同的AP域，设置相应射频参数、制定业务推送策略及进行AP维护/升级，降低管理复杂度。

3.4.3 广域网加速实现移动用户最佳体验

自带设备在连接广域网经常出现网络时延大和网络不稳定现象，用户体验差，影响办公效率。 华为移动终端广域网优化方案通过协议优化、压缩、去重、缓存等技术，帮助移动用户实现快速的网络访问和最佳体验，提高工作效率。

3.5 协同办公 一致体验

BYOD移动办公最终是要给用户一个很好的办公体验，这是移动办公解决方案的精髓，而协同性，一致性是BYOD时代一定要解决的问题。大量的各种类型的设备，PC、Pad、各种智能手机，桌面云等等都应用到办公中，如果每个设备上应用的办公软件都不一样，在不同场景下办公都需要切断重新进入会议，这样的工作效率必然是非常低的。

华为移动办公协作解决方案已在公司内部(8.5万BYOD移动用户遍布全球)，及客户中大量应用，并在移动、视频、云协作三方面持续深化。

3.5.1 协同办公

随着全球信息传递的速度加快，多数企业营运据点不再局限于单一国家，而是透过全球化的布局方式，让整体营收能够屡创佳绩。正因为如此，不但商务人士出差开会的频率极高，各分公司之间的联系也愈加紧密，无形之中也增加了企业营运成本，市场上有许多厂商，纷纷针对跨国企业推出多种视讯、语音沟通解决方案，用户通过自带设备进行通信与协作，提高工作效率和工作体验。

■ 多终端、多场景下同时体验融合会议

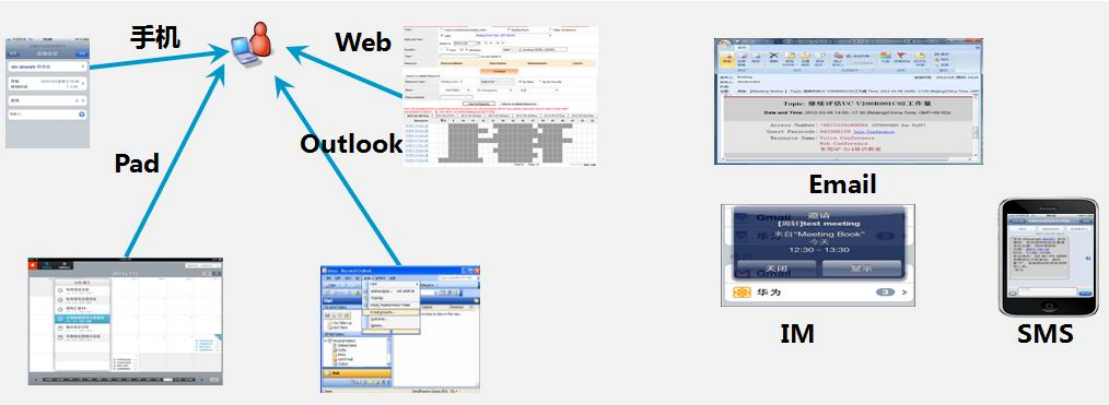
用户可以在公司内、家中、机场和咖啡馆等诸多地方通过自带设备加入会议，保障了公司信息安全及时传达，提高了工作效率。

- 在移动终端上直接进行会议预约、召集和接入；
- 会议进行中可以进行禁音、邀请、删除等会议控制；
- 会议日历自动送达和提醒，与手机日历自动关联，让日程管理更简单直接；
- 安全的一键入会，避免复杂的入会操作；
- 支持多媒体会议；
- 在移动终端接入高端智真会议

■ 同一界面一键切换多种会议模式

用户在自带设备上能完成VOIP、CTD(点击回呼)、IM/UM、Presence、话机通讯录、本地通讯录、群组、企业通讯录、发起语音会议和多媒体会议、会议日历、一键入会等功能，避免了传统方式所需要的多个单独移动客户端的安装和切换，为客户提供了真正的统一通信，便于用户轻松聚焦工作。

■ 多种方式协同的会议预约和通知



在会议预约和通知上，实现多种方式协同。

预约方式： 在PC客户端、手机、Pad、Outlook上均可进行会议预约；

邮件通知： 在预定时和会议当天向用户发送会议通知和提醒PC、手机、Pad均可通过通知中的链接加入会议

短信通知： 发送到用户手机，用户答复后系统会呼叫其手机让其加入语音会议

IM通知： 以系统即时消息的方式发到用户eSpace客户端，保存在公告会议通知类

日程推送： 向Outlook终端推送会议日程（手机、Pad需启用PushMail功能）

会议列表： PC、手机、Pad上的eSpace版本支持会议列表，可看会议详细信息，可点击参加会议，召集人可更新会议信息。

■ 桌面共享

会议系统支持桌面共享功能，利用此功能使用者可以方便的将桌面操作情况和应用操作步骤共享给全体与会人员，使协同工作、应用培训等功能轻松而方便。而通过操作权的切换，某一用户可将自己桌面的操作权交给其他远程用户，达到了远程控制桌面的效果。桌面共享功能提供给用户灵活的远程控制、共享应用的使用感受。

3.5.2 一致体验

■ 多终端、多环境下业务体验不变

通过eSpace客户端，能够实现多种类型的业务，如语音通信，协同办公，通讯录，即时消息等，在各种场景下，能够分别在PC，智能手机(不含视频共享)，Pad等终端上有着一致的办公体验。

其技术实现的基础是IP话机、PC客户端、手机客户端、Pad客户端支持IDEO UCD设计，支持用户体验在多个终端下保持不变。

■ 多终端，多网络一键切换，体验不变

通过一键切换，可实现IP话机/PC软终端切换至手机，手机切换至IP话机/PC软终端，保证体验不变。

BYOD设备可以与企业固定办公网络进行无缝切换，包括手机移动UC与固定IP电话、PSTN号码、PLMN号码间的切换、平板与公司电脑会议系统间的切换、会议中不同号码的切换。

■ 桌面云实现个人办公“移动化”，桌面一致，数据不丢，体验不变

BYOD用户可以通过登录移动桌面云进行企业业务的处理，体验与PC呈现保持一致，无需培训。一般应用带宽只需20KB/s，在3G网络也有良好的体验，支持IOS、Android、Blackberry、Windows Mobile等常用平板、智能手机的接入。

核心数据保留在云端、通过网关或者VPN接入、传输加密、只传显示信息，保证数据安全，避免了广域网被窃听的风险。通过录像手段监控移动办公行为，做到有据可查。

3.5.3 安全浏览器和 Pushmail

随着各类企业应用的Web化（譬如，会议系统、考勤系统、文档查询系统等），通过浏览器访问企业内的各项应用的需求日益凸显出来，需要更安全的浏览器和邮件系统，保证企业信息的安全。

■ 安全浏览器

安全浏览器支持HTTP、HTTPS等标准协议，同时，由于自身具备L4VPN功能，不必在终端上安装和启用其它VPN拨号软件即可顺畅地接入并访问企业网站，保证自带设备接入网络的安全。同时，应用层HTTP或HTTPS报文的收发也都通过安全浏览器底层的安全SDK进行。

■ PushMail

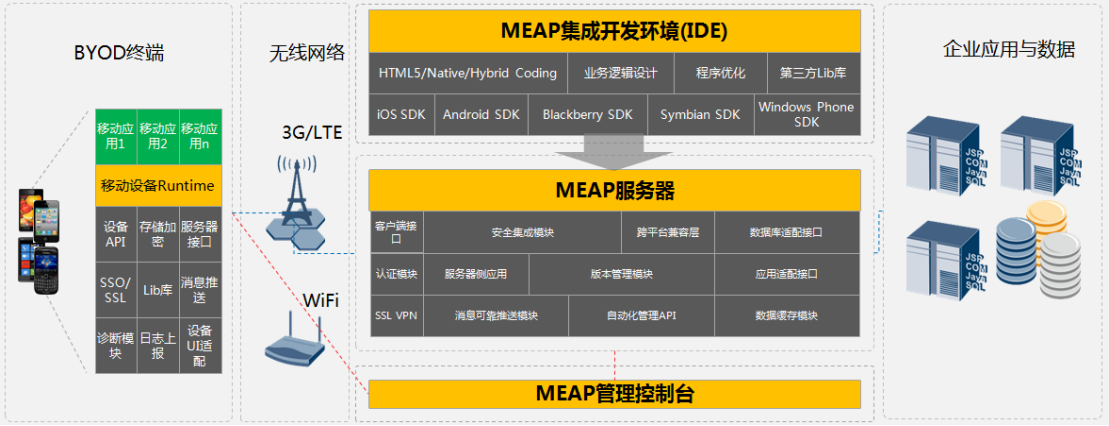
Pushmail客户端是支持DirectPush技术的邮件客户端。Pushmail的主要用途是为用户提供安全受控的即时邮件推送服务。

Pushmail客户端通过移动VPN或内置的应用层隧道与企业移动接入网络建立加密隧道，在用户查看企业邮箱时提供安全通信防护，附件浏览和下载控制。

针对于智能终端和Pad设备的操作特点，Pushmail客户端提供以下特性，为用户提供优质体验。

3.5.4 MEAP 第三方应用发布平台

华为与业界领先企业合作提供MEAP平台，通过集成多种移动应用开发工具、提供企业后端数据的安全访问能力、封装移动应用服务标准组件和业务组件、集成移动设备/应用程序管理控制功能，极大地简化了企业移动应用开发、部署和管理过程，满足各种企业移动应用部署的需求，为BYOD的成功部署解决了后顾之忧。



- 集成开发环境，一次开发，跨平台应用多次发布
- 移动应用与数据集中适配对接，极具扩展性
- 全生命周期开发流程：设计、开发、测试、部署、维护
- 应用安全特性集成：SSL/SSO/数据加密，MDM联动

3.5.5 关键技术

■ 语音编解码

移动会议系统把语音的清晰连贯放到很重要的位置。在语音交互方面，通过采用国际先进的语音编/解码技术和音频压缩算法，在各种网络带宽条件下均保持声音清晰连贯，使得在网络状况极其恶劣的情况下仍保持较好的音频效果；采用高效的AGC(自动增益)/AEC(回声消除)/NS(噪音抑制)/VAD(静音检测)技术及自动修包机制、网络防抖动算法等音频优化手段使得通话清晰连贯，保证通过自带设备接入会议的体验。

■ 视频编解码

会议系统视频采用H.264/MPEG4视频压缩算法，具有良好的带宽适应性和视频压缩率，适应从56Kbps拨号上网到宽带的网络环境，独有的码流控制机制和带宽自适应机制保证了自带设备在网络状况较差时系统仍能提供较理想的视频效果。

■ 音视频QoS保障技术

QoS是Quality of Service（服务质量）的缩写，它表明信息在数据通信系统中传递时所获得的性能保证。音视频会议的音视频QoS保障是指音视频会议系统的一种能力，即在有影响音视频质量因素存在的IP网络上，为保障音视频业务提供所需要的服务。在网络条件保持不变的情况下，通过在音视频会议终端和MCU等网元上进行速率和误码控制等处理，可以在

一定程度上做到QoS保障，提高音视频会议的音视频效果。常用的QoS保障技术包括IP优先权，速率调整，丢包重传（ARQ），前向纠错（FEC），后向纠错（PLC）等，通过这些技术，使自带设备办公有更好的体验。

4 总结

4.1 华为移动办公解决方案全景图

华为移动办公解决方案融合华为产品和合作伙伴的产品，秉承安全、效率、体验三大理念，在深刻理解客户需求和体验的基础上，发挥自身在端、管、云方面的全面优势，开放合作,帮助企业客户构建业界一流完整的移动办公解决方案。

4.2 优势一：安全防护 一网通行

华为移动办公安全解决方案，从身份、隐私和遵从三点出发，提供端到端的安全防护，保证移动办公安全的同时，有更好的体验，在获得权限的情况下，一网通行。

- **认证授权：安全策略统一配置和下发，一网通行**

  基于一个角色，多套策略模版，一次配置，通过Any Office策略平台统一下发，Any Office平台内嵌不同类型的版本，可根据多种策略的组合，选择激活，使不同类型的用户获得不同的权限。

- **接入控制：4C的环境感知，5A的访问体验**

基于4C的环境感知，使用户获得5A的访问体验。
C：角色--管理者、员工、合作伙伴、访客等
C：终端类型---PC，手机，哑终端等
C：网络位置---公司内网，外网等
C：时间感知---上下班时间等。
5A: Anyone 、Any device、 Anytime、 Anywhere、 Anything，实现任何人，通过任何设备，在任何时间、任何地点，进行任何业务的办公。

- **链路安全：端到端VPN加密，构建安全数据通道**

基于如下技术，提供端到端的VPN加密；
1）基于RSA高安全密钥分发算法；
2）数据加密支持3DES，AES356高强度算法；
3）支持SHA-1验证，数据防篡改、防抵赖 。

- **威胁防护：网络侧硬件级多层次立体防护**

1) 外边威胁防护包括：DDoS防攻击与非法访问、防黑客跳板入侵 、防病毒、木马传播和恶意邮件内容过滤。
2）内部威胁防护：非法访问控制、内部员工恶意入侵、防病毒、木马传播和Web内容过滤。
3）内部安全管控：URL过滤非法访问控制、恶意Web页面访问控制和Web页面/邮件正文/附件关键字过滤。

- **数据防护：沙箱数据隔离技术，安全隔离个人和企业数据**

华为提供沙箱技术，实现用户数据和公司数据的分离，提高数据的安全性。

- **应用安全：企业级App Store安全应用发布和管理**

灵活的MEAP发布平台，保证企业应用的发布和管理。

- **管理安全：全生命周期移动设备的安全管理**

华为从采购、部署、运行和回收四个维度进行管理，保证移动设备的全流程安全管理。

4.3 优势二：高效网络 无处不在

- **智能技术+业界吞吐率No.1 提升覆盖效率20%**

  华为采用智能天线技术，提升网络吞吐率，增大覆盖面积，有效节省设备。

- **“3”小时部署复杂场景移动办公，提升业务开通效率**

  华为提供快速的移动办公部署，提高业务的开通效率。

- **快速安装，提升6倍部署效率**

- **不同场景下POE承载AP，节能20%**

  华为提供动态的POE控制，对无业务的端口进行休眠，有效节能。

4.4 优势三：协同办公 一致体验

- **多终端、多环境下保持一致体验**

  华为提供多种应用，实现多种终端上通讯录、即时消息、状态呈现、多媒体会议的一致体验。

- **移动中多终端，多网络一键切换，办公体验不变**

  华为提供终端网络和业务的自由切换，提升用户的办公体验。

- **桌面云实现个人办公“移动化”，桌面一致，数据不丢**

  华为移动桌面云，实现移动安全化，保证用户数据不丢失，提升企业的信息安全。

5 缩略语表

缩略语清单

英文缩写	英文全称	中文全称
WLAN	wireless local area network	无线局域网
AP	Access Point	接入点
AC	Access Controller	无线控制器
SSID	Service Set Identifier	服务组合识别码
Radius	Remote Authentication Dial In User Service	远程认证用户拨入服务
IP	Internet Protocol	因特网协议
SSL	Secure Socket Layer	安全套接层协议
GE	Gigabit Ethernet	千兆以太网
AAA	Authentication, Authorization and Auditing	认证、授权和审计
ACL	Access Control List	访问控制列表
ARP	Address Resolution Protocol	地址解析协议
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议
SNMP	Simple Network Management Protocol	简单网管协议