

BYOD 特刊

enterprise.huawei.com

ICT
新视界

华为企业业务
粤内登字B第13154号
内部发行 / 免费赠阅



超越极限 畅享联接

如果用一个关键词来概括企业IT在不同阶段的发展特点，从早期的“网络化”，到“云化”，即将进入的应该是“移动化”。移动化的企业利用智能移动终端，通过移动网络随时随地、安全方便地访问企业的IT资源，不受时间和空间的限制。移动技术为企业的发展带来前所未有的商业价值，以BYOD为代表的移动办公正成为工作的新Style。



超越极限 畅享联接

▲ 华为企业业务Marketing与解决方案部总裁 张顺茂



张顺茂

如 果用一个关键词来概括企业IT在不同阶段的发展特点，从早期的“网络化”，到“云化”，即将进入的应该是“移动化”。移动化的企业利用智能移动终端，通过移动网络随时随地、安全方便地访问企业的IT资源，不受时间和空间的限制。企业可以利用移动技术开展营销、办公和服务，为客户带来价值，提升员工满意度，并最终为公司创造更大的商业价值。

这就是为什么在Gartner发布的“2012年全球CIO关注的关键技术”中，移动技术会超越云计算，跃居第2位。CIO们对移动技术高度关注的原因是：移动技术正在为企业的发展带来前所未有的商业价值，以BYOD（Bring Your Own Device）为代表的移动办公正成为工作的新Style。

移动技术正改变着企业的商业流程。例如某全球著名的电力和自动化公司利用移动技术改变业务流程，员工在野外作业时，通过移动终端快速扫描、拍照、上传工程完成情况，大幅提升了工作效率；某著名的运动品牌公司也利用移动技术为客户提供在线营销服务，客户通过智能终端随时查看新产品并下单购买，消费者可以随时随地获取该公司的产品信息。

移动办公的部署同样对华为公司的业务起到了促进作用。早在2009年，华为就开始提前布局移动办公。作为一家全球化企业，华为的业务覆盖全球140多个国家，拥有500多个代表处、15万员工。业务的全球化和以客户为中心的企业文化，带来了公司90%的高管频繁出差，70%的营销人员经常拜访客户，80%的服务人员长期在野外工作……这些人需要及时处理客户邮件、审批销售合同、上报工程进展情况等。从2009年开始，华为先后实现了办公OA的移动化、与业务紧密相关的流程移动化，有效解决了上述问题，整个企业的办公效率提升了40%。

华为公司在移动通信领域深耕20余年，积累了丰富的移动、安全网络建设经验。在ICT融合的趋势下，我们期望通过运营级网络经验、丰富的智能终端产品，并结合自身的移动办公实践，为更多的企业客户提供企业移动化解决方案，超越极限，让人们畅享移动化带来的美好工作与生活。**BYOD**

P1 超越极限 畅享联接

[趋势]

P4 BYOD助企业脱颖而出

BYOD乃至BYOA将给企业带来3大好处：生产力的提升、员工使用满意度和工作积极性更高，以及企业运营成本降低。>>

[焦点]

P8 企业IT如何应对BYOD挑战

一套动态的、可协商的、个性化的IT安全策略，将帮助企业很好地应对BYOD/BYOT带来的挑战。>>

P12 BYOD 5大安全隐患

带宽消耗、恶意软件、数据和设备丢失、针对移动设备的攻击，以及安全策略不一致，是BYOD带来的5大安全隐患。>>

P14 BYOD安全宝典

没有灵丹妙药可以独自解决移动设备所带来的安全挑战，完善的安全解决方案将会是广泛的产品组合。>>

[方案]

P18 如何“选型”BYOD方案？

企业员工乐于使用、现网和应用适配性好、企业IT放心并易于部署——只有实现这三者的和谐统一，才是企业最需要的BYOD解决方案。>>

[CIO分享]

P22 房地产巨头的BYOD之路

——访Emaar（埃及）公司CIO Moataz Hassouna先生

BYOD已成为Emaar提高员工满意度，并更好地服务客户的有力手段。>>

[实践]

P24 移动办公改变华为人的工作和生活

移动办公系统帮助华为公司每年节省了数千万美元IT费用，提高了员工满意度，使整个企业办公效率提升了40%。>>



封面标题：BYOD 特刊
封面副标题：超越极限 畅享联接
封面内容：华为技术有限公司企业业务《ICT新视界》编辑部
封面底部：HUAWEI

主办：
华为技术有限公司企业业务
《ICT新视界》编辑部

粤内登字B第13154号

编委：
兰 涛 / 王岩军
李智鹏 / 陈 鸣
汪 伦 / 谢良剑
张明威 / 王越存
Soheila Soheil



王宇明

BYOD乃至BYOA将给企业带来3大好处：生产力的提升、员工使用满意度和工作积极性更高，以及企业运营成本降低。>>

BYOD助企业脱颖而出

▲ 华为UC&C战略规划经理 王宇明

有人说，是3个“苹果”改变了世界：夏娃的苹果让世界有了道德，牛顿的苹果让世界有了科学，而乔布斯的苹果让世界有了数字生活。乔布斯用他的苹果征服了几乎整个世界，掀起一股智能手机与平板电脑的热潮。与此同时，越来越多的人在工作和生活中离不开手机、平板电脑，引发了移动办公的新趋势——“BYOD”。

以前，电子设备的普及，往往是按照先应用于企业办公，再推广到个人的顺序。但随着以iPhone、iPad为代表的移动设备的发展，其强大的计算能力，友好的触控操作体验，出色的多媒体处理能力，视网膜高分辨率屏幕，GPS，陀螺仪，重力感应，多点触控，前后内置高清摄像头，五花八门、极大丰富的APP应用……形成了从个人消费电子向企业移动办公的“逆袭”。

BYOD为企业带来什么？

在IT发展相对领先的北美地区，数以万计的公司和学校已经应用BYOD，根据他们的经验，BYOD使得他们至少在以下3个方面获益：

● 生产力的提升

咨询公司的调查结果显示，以iPad和iPhone为首的平板电脑和智能手机是BYOD大军的主力，苹果公司并没有对其产品在企业领域的使用做大量的推广工作，而是消费者和员工自己做出了选择。这恰恰说明员工最清楚什么样的工具能让工作变得更加轻松和高效。CIO们需要认识到：当员工甚至老板都喜欢一种技术的时候，IT部门应该去支撑这种技术而不是阻止。80后、90后的员工习惯于基于Web的实时通信渠道，而不是通过电子邮件，年轻人喜欢通过FaceTime、聊天工具、微博、微信等方式相互联系，向供应商或律师发送电子邮件逐渐成为一种老套和过时的方式。如果他们平时喜欢在社交网络上聊天，那工作中为什么不能跟同事以类似的方式沟通呢？

BYOD设备上的企业应用为员工、客户、同事和供应商提供了一个更好的实时沟通渠道，这种更高效的沟通方式必将提升企业的各项关键业绩指标，包括员工生产力、运营效率和客户满意度。

美国一家健康服务机构采用了基于平板电脑的统一通信与协作客户端，员工可以使用自己的iPad以及Android平板，体验指尖触控操作，完成包括IP语音、IM、语音/视频会议、数据协同/文件共享等全部统一通信和协作功能，并自由地在

各种设备间快速切换会话，平板电脑的丰富功能得到充分发挥，通过GPS获得外勤人员的具体位置，高清摄像头采集救护现场图片，及时传回医疗中心，提前准备手术，多点触控操作将在线专家“拖入”视频会诊会议。项目效果评估表明，该健康服务中心的运作效率因此提高40%。

北美一家银行允许其贷款客户经理使用自己的iPad接入银行网络，客户经理可以实时提交客户的贷款申请，现场查阅贷款规定，查看审核进度，与高级经理通过IM讨论合同条款，甚至可以在客户现场发起跨部门的视频会议，沟通客户的贷款需求和方案。该系统实施后，平均贷款的审核时间，由以往的一到两周缩短到4个工作日，大大促进了业务的增长，提升了客户满意度。

● 员工使用满意度、工作积极性更高

任何企业软件、流程或设备的成功实施都有赖于员工的参与和使用。目前私人拥有智能手机、平板电脑等移动设备的员工比例已经很高，当员工自发将自己的设备带到办公场所时，CIO至少不用担心这些设备会被闲置。另一方面，员工对个人设备上的应用满意度更高，强迫员工去适应复杂难用的企业应用往往很难成功，那些在



强迫员工去适应复杂难用的企业应用往往很难成功，那些在用户体验方面更接近社交网站和个人应用的企业应用更容易赢得员工的认可并促进员工的使用。

BYOD带来的企业运营成本优势，主要体现在更低的管理成本、更低的部署和升级成本，以及更低的硬件成本。

用户体验方面更接近社交网站和个人应用的企业应用更容易赢得员工的认可并促进员工的使用。

在对使用BYOD访问公司数据支持方面，传统企业应用将数据放在一个单一的地点，云计算则让企业应用和数据可被更多用户和设备访问（当然包括BYOD设备）。对于员工来说，这是一次革命性的变化，BYOD结合云计算意味着人们需要的信息始终在指尖——无论他们在客户那里还是在家或者在路上。

浙江电信全省1000多名VIP客户经理全部使用智能手机，开通了微博、翼聊、QQ，大大促进了员工与客户沟通、主动营销的积极性和效率。这1000多名VIP客户经理的平均微博粉丝数达到225名，平均关注数308名，发布博文达到2263篇，营销效果显著，2011年高端客户保留率保持全集团第一。

江苏电信开发宽带装机工作客户端，工作人员使用智能手机安装后，可以在客户现场

完成：服务开通、带宽测试、端口分配、故障诊断、位置定位、工作上报、客户满意度反馈等，员工对该装机工作客户端的满意度也达93%。

● 企业运营成本降低

BYOD带来的企业运营成本优势，主要体现在更低的管理成本、更低的部署和升级成本，以及更低的硬件成本。对于BYOD的员工，企业不再需要采购和更换办公设备，而是提供相对低廉的员工补助；企业的办公设备使用费用也会大大降低。统计发现，北美应用BYOD的近千家企业中，有50%的员工支付所有设备和话费，5%的员工支付设备费用、话费由公司支付。基于APP的客户端也可降低购买软件的支出，云计算应用将资本支出转变为持续的运营支出。如果计算总体拥有成本，与传统企业应用的漫长实施周期和学习曲线相比，BYOD上的应用可以节省大量培训成本，而且由于界面和功能非常友好和熟悉，员工能很快上手。

事实表明，BYOD已经成为必然趋势，最近在北美的一次调研发现，包括IBM、CISCO、南佛罗里达大学、圣保罗大学等72%的知名企业、学校（样本数1000家）支持BYOD，15%计划支持BYOD。Gartner公司预计到2014年，将有90%的企业支持BYOD。

从BYOD迈向BYOA

随着BYOD普及率的提高，未来BYOD的重点将从单纯的设备转向企业应用，即BYOA（Bring Your Own App）。因此除了会带来网络安全、数据安全的挑战外，企业应用的开发和管理方面的挑战更不容忽视，CIO们不光要考虑BYOD，还要考虑BYOA，比如各类个人应用程序以及Dropbox和iCloud等云存储服务，即使是IBM这样的顶级IT服务企业，也对BYOA带来的信息安全挑战头疼不已。

为此，一些企业开始为员工的智能手机和平板电脑开发内部专用程序，包括企业通信协作工具和各类办公应用，这些应用程序使用体验更加接近智能手机、平板电脑上流行的APP应用。有些企业甚至创建企业专用应用程序商店来控制员工移动设备的应用安装。最近的一项IT专业人士调查显示，6275家受访企业中有66%的企业计划开发企业应用程序商店。GE

公司2009年就上线了企业应用程序商店——GE AppCentral，迄今已经向员工提供了35万次下载，包括生产力和服务应用软件。通过企业应用程序商店，GE已经将移动性作为提升业务效率的一项关键策略，同时也成功驾驭了BYOA这股潮流。

现代企业的经营理念，是以人为本，人性化管理，企业统一通信与协作的发展必须做到以人为本，以体验为中心。互联网信息时代成长起来的新生代员工的工作模式和习惯已发生巨大改变，他们希望没有时间、地点、设备差异、网络差异的限制和阻碍，实现自由便捷地工作。就像前几年的SOHO一样，BYOD乃至BYOA，是员工打破生产力和创造力限制的需要，是对人性化工作的追求。它自下而上推动了企业通信协作效率的迅速提升，也在不断挑战企业IT部门的技术和管理能力。CIO们要找到正确引导和管理BYOD/BYOA的方法，顺应员工人性化工作的需求，扬长避短，趋利避害，才能有效促进生产力的提高，在日趋激烈的商业竞争中脱颖而出。**BYOD**

BYOD展望：随着BYOD普及率的提高，未来BYOD的重点将从单纯的设备转向企业应用，即BYOA（Bring Your Own App）。



Ishita Majumdar



George Vanecek

一套动态的、可协商的、个性化的IT安全策略，将帮助企业很好地应对BYOD/BYOT带来的挑战。>>

企业IT如何应对BYOD挑战

▲ 华为美研所资深项目主管 Ishita Majumdar
华为美研所首席科学家 George Vanecek

BYOD以及BYOT（Bring Your Own Technology，带自己的技术上班）已经成为一股风潮。许多企业开始借此机会尝试允许其员工使用私人的移动设备办公，并访问企业的私密商业信息，包括email、企业名录、日志、文档、应用软件以及其它内容；但与此同时，这些移动设备上还保留着各种员工的私人信息、应用软件和社交账户等，不在企业IT的监控范围之内。BYOD/BYOT的这种双重使用特性意味着这些私人设备需要经常穿梭于完全不同的IT策略域，由此IT经理的工作变得更加复杂和艰巨：一方面，他们要为每一个员工制定一个安全的IT活动域，同时还要保护员工的个人隐私、保证他们能够自由访问处于不同IT域中的信息；另一方面，IT经理还要考虑，企业怎样才能制定一套商业策略，通过引入BYOD/BYOT的优势，实现降低IT成本、提高员工的生产

率和满意度的目标。

IT经理感到“压力山大”，而BYOD追捧者的要求却有增无减。

- 他们希望总能够即时地访问自己想要的信息；
- 他们需要的不仅仅是文本信息，还包括视频以及富媒体内容；
- 他们无法忍受企业传统的刻板的通信、协作和与客户交流的方式；
- 他们还总想把带有强烈消费性色彩的行为方式带到办公场合来……

受此影响，未来企业的办公和运营需求也随之改变：

- 未来企业的员工组成将更加全球化和虚拟化；
- IT运维成本将迫使企业特别是中小企业不得不允许员工使用私人设备办公；
- 对企业信息的访问将来自世界各



个角落，经由公网、私网、安全的或不安全的网络；

- 访问者将从公司的经理和雇员，扩展至集成商、合作伙伴、供应商、客户乃至普通公众……

实际上，在应对BYOD/BYOT所带来的上述挑战时，企业IT面临的重大问题不在于技术能力的缺失，而是如何实行一系列正确和可行的原则和技术，以达到自由访问和严密控制的访问策略之间的平衡。在“自由”与“控制”两者之间寻找平衡，企业IT需要理清3个关键点：

- 员工和企业IT如何协商访问模式？
- 考虑到实时变化的环境，员工和企业IT如何实现双向的动态访问管理？
- 如何让企业IT能接纳个人设备和技术的变化？

为了更加直观地了解上述问题，我们不妨参考文后所附的一个真实的例子——《BYOD的一天》，看看

动态推行的IT安全策略是需要根据用户及其设备所处的环境、情况以及意图持续地进行协商和调整的。

访客James Brown进入华为美研所（Santa Clara园区）后是如何与IT系统互动的，这也是如何设计、管理以及实施企业动态安全策略的一个很好实例。其可行性成立的关键在于，采用一套双边的、动态的、颗粒状的、可实时确定的信任机制。

事实上，企业以往基于鉴权以及公钥基础设施建立起来的静态IT策略是BYOD/BYOT大规模实施的绊脚石。信任必须要持续地进行重新评估，而评估的依据来自于设备和基础设施传感器收集来的动态痕迹和相关信息。需要注意的是，动态推行的策略是需要根据用户及其设备所处的环境、情况以及意图持续地进行协商和再推行的。

总之，如果参考如下机制，那么，一个介于用户以及企业间的健康

10



潘伟

带宽消耗、恶意软件、数据和设备丢失、针对移动设备的攻击，以及安全策略不一致，是BYOD带来的5大安全隐患。>>

BYOD 5大安全隐患

▲ 华为SecoSpace战略与业务发展部高级营销经理 潘伟

IT消费化理念已经深入人心。现在全球越来越多的企业已经开始允许员工带上自己的设备（BYOD）接入工作场所的网络进行个性化办公，这无疑能够使工作更加高效并富有创造力，与此同时，BYOD还为企业逐步转变旧有的刻板IT管理方式提供了很好的机会。

然而，安全性和可用性之间的战争永远不会停止，BYOD就是一个例子，它也带来了诸多挑战。BYOD使用户隐私和可访问性之间的界限日益模糊，于是网络、数据以及设备的安全问题随之暴露出来。今天，企业需要面对林林总总的BYOD安全陷阱，尤其以下5项最为突出。

带宽消耗，工作效率低下

许多企业已经发现，相比于企业自有的桌面终端，移动设备往往不具有同样严格的安全策略执行能力。这一差距诱使许多员工尝试使用其移动设备来访问视频流、在线游戏等许多被企业安全规则拒绝的应用程序，无形中也占据了企业的网络带宽，降低了工作效率。另外，让员工自有设备无序进入工作场合将必然会是安全管理的梦魇，错误的终端配置和恶意的无线接入会导致网络的不稳定，甚至间接在网上造成拒绝服务攻击。



设备感染恶意软件（Malware）

员工自己的笔记本电脑比公司的电脑更容易被感染，因为大多数员工并没有足够的知识和资源来实现充分的自我保护。更棘手的情况是，针对移动终端操作系统和应用的Malware层出不穷，大部分基于零日漏洞攻击，设备尤其是智能终端一旦感染，Malware将通过空中接口或者蓝牙等通道，通过自动调用短信、邮件、文件共享或访问Web页面等手段扩散开来，令企业防不胜防。

数据和设备丢失

据业界权威调查，此项公认为是企业最大的BYOD安全挑战。员工的个人隐私或企业的关键业务数据可能被蓄意破坏。终端的数据偷偷地被感染的Malware发送到网络上，设备之间无

意或恶意的数据共享，或者设备丢失或被盗，都可能给组织和个人造成经济损失。员工自有设备缺乏有效的安全保护，如自动化的配置管理或基于终端的安全软件，设备之间数据流的可见性和数据防丢失措施也无法实现。但是，反过来说，为了安全起见，企业应该收集和监测个人终端的哪些通信数据呢？例如GPS这样的数据是否应该纳入收集的范围，雇主这样做在法理上能否站得住脚？

针对移动设备的攻击

黑客们开始认识到，存在于移动设备的某些数据是潜在的巨大金矿，游荡在公共无线网络的黑客无时无刻不在想法窃取未受保护的数据。而未经授权的应用程序商店也放大了这一风险，因为它们可以轻易地分发移动应用程序，其中一些是

不合法的。黑客可以变得很世故，偏向用少量的代价去攻击高价值的目标，2011年某机构的安全分析报告统计了BYOD终端遭遇到的Malware，其中80%以上可用来对付黑莓手机，这和黑莓手机显著的商务身份有很大的关系。

在BYOD的世界，企业想要在惬意地享受BYOD带来的好处的同时，避免遭遇繁杂的安全事故并因此付出高昂的代价，就必须在安全控制手段、安全策略和流程上有所革新。

设备间安全策略的不一致

在一个不成熟的市场，行业标准或政策适用性的差异化案例乏善可陈。琳琅满目的移动操作系统的版本，再搭配各种各样的硬件平台，我们将很容易看到这当中衍生复杂问题将是如何地迅速。厂商会发现其将很难支持不同的配置管理文件，并很难针对不同的业务单元和不同的员工角色实施不同的安全等级控制。

需要指出的是，上述这些挑战并非前所未有。过去，企业能够通过一定的设备或软件/套件锁定装置，以确保用户遵守安全规定，但这种好日子已经一去不复返。在BYOD的世界，企业想要在惬意地享受BYOD带来的好处的同时，避免遭遇繁杂的安全事故并因此付出高昂代价，就必须在安全控制手段、安全策略和流程上有所革新。另外，从合规性的角度来看，企业除了考虑和部署安全风险，还应该明确员工的责任。比如，如果发现员工违反安全策略或损害业务数据，擦除员工终端上的数据在法律上是可以接受的。最后，真正巨大的挑战是，企业如何才能做完这一切而不会干扰到员工的使用。**BYOD**



潘伟

没有灵丹妙药可以独自解决移动设备所带来的安全挑战，完善的安全解决方案将会是广泛的产品组合。>>

BYOD安全宝典

▲ 华为SecoSpace战略与业务发展部高级营销经理 潘伟

端可以和网络连接、相关策略和可以接受的用户行为。企业还必须决定实施哪些技术控制手段以执行企业的政策。至少，企业必须回答某些问题，例如支持什么样的设备和移动操作系统？如何分配和管理员工设备上的应用程序等等。技术控制可以以网络为中心，或以设备为中心，并没有放之四海皆准的单一手段。可供选择的技术控制手段有如下几种：

- **移动设备管理（MDM）**。对个人设备匹配相应的安全策略管理能力是采纳MDM的驱动力之一。MDM能使策略执行针对移动设备本身并提供远程位置锁定和数据擦除的能力，防止设备丢失或被盗。

- **网络访问控制（NAC）**。这种技术的一个主要优点是，建立对网络本身的控制，使企业在网络发生任何损坏之前，能够阻止来自于移动设备的恶意软件的攻击。NAC依赖于网络执行安全策略并控制终端、数据和用户访问行为，它需要相当的智能设计以在网上提供足够的访问控制粒度。

- **安全Web网关（SWG）**。面向移动的Web安全网关也许是MDM的完美补充。它可以

基于设备或云，通过恶意软件过滤、信誉过滤、数据防泄漏（DLP）、应用可视化控制等手段，结合可行的策略控制，解决BYOD带来的网络安全风险。

- **移动安全客户端（ESC）**。它是传统防恶意软件客户端的移动性延伸，是终端上反恶意软件、身份认证（如802.1X）、VPN和远程擦除功能的组合。

- **身份和访问管理（IAM）**。它是使企业能够执行合规和加强基础设施安全的策略平台，同时可简化企业的业务操作。通常情况下，它包含了一个完整的配置和认证系统，用来对网络中形形色色的移动访问角色提供永久或临时的认证。它会收集实时的来自网络和用户的上下文信息，强制执行安全策略，并根据预设的条件触发，预先自动生成管控决策。

- **虚拟桌面基础设施（VDI）**。它创建了一个可以托管应用程序和数据的安全虚拟机（VM），为进入企业网络的移动设备访问VDI提供了一个安全窗口，确保数据的安全和业务连续性，因为VDI不允许数据在用户的个人设备之间以及与企业基础设施之间流动。

没有灵丹妙药可以独自解决移动设备所带来的挑战。完善的安全解决方案将会是广泛的产品组合，可以实时抵挡来自于移动设备的新的安全威胁，对远程用户执行安全合规，并保护网络、数据和客户端的安全。如果制定政策和审视技术控制手段是获取BYOD安全的第一步，第二步则是创建一个战略架构远景。

首先，让我们从MDM开始。一方面，市场驱动厂商追求广泛的、跨平台的MDM覆盖策略，使得原来因为缺乏MDM安全

策略定义和实现标准所造成的适应性的广度和差异化欠佳的情况有所改善。另一方面，由于针对移动平台的恶意软件层出不穷，提高移动设备安全性的呼声也越来越高，企业需要MDM结合恶意软件防护来确保业务的连续性。许多企业这样做了，却失于偏颇，因为他们没有采取相应的网络可视化监控手段。此外，基于设备的恶意软件防护，会受到设备和移动操作系统的限制。想象一下，如果员工用合法的智能手机或平板电脑访问互联网上的恶意信息怎么办？在那一刻企业该怎样去及时阻止移动终端接入可疑的网站或应用程序？

业界一些厂商正在试图将MDM和移动安全客户端、DLP、SWG和其它基于云的服务结合起来，建立强健的、高可用的架构。由于以终端为中心的安全控制方法会受到极大制约，这种架构在今后可能会成为主流。传统的网络解决方案厂商都已经意识到，解决移动安全仅靠终端一隅是不可能的，它们已经开始推出集成的移动安全解决方案，这些方案可以回答几个以终端为中心的安全控制手段无法回答的关键问题：

业界一些厂商正在试图将MDM和移动安全客户端、DLP、SWG和其它基于云的服务结合起来，建立强健的、高可用的架构。

针对BYOD带来的安全隐患，企业必须实施有效的控制手段和策略。企业需要考虑的问题涵盖了技术方案、技术支持、业务流程、HR管理、财务规章和法律责任等多个方面。那么首先，有哪些技术方案和安全策略可供选择？

BYOD 6大安全控制手段

大多数企业首先会通过明确的政策来决定BYOD计划的实施程度，有的选择限制访问某些数据或应用程序，有的会选择要求员工在自己的设备上安装特定的软件。企业将决定允许哪些终

许多企业仍然筹划着对BYOD趋势做出反应，但还没有制定正式的政策，有4种宏观安全策略可以借鉴：协调、遏制、封锁和忽略。



- 你是谁？
- 你从何处接入？
- 你要访问什么数据？
- 哪些数据会流出网络？

因此，网络需要有批准和拒绝用户试图获得特定数据的最终决定权，网络安全一定要被集成进入整体移动安全架构。

制定宏观安全策略

诚然，企业还需要细致考虑如何有机地结合并实施上述技术控制手段。当面向移动平台的安全技术，如MDM和近来兴起的“集装箱”技术（Containerization）还不成熟的时候，对移动访问不管采取什么样的安全控制手段，NAC都是最重要最直接的安全能力，企业必须在工作场所检测非管理的但作为商业用途的员工设备。原因就在于这样一个事实：许多企业仍然筹划着对BYOD趋势做出反应，但还没有制定正式的政策，而且他们可能还无法在个人移动设备上安装终端防护程序，

也无法配置任务策略，无法像控制公司所有的设备一样执行生命周期管理。有如下4种宏观安全策略可以借鉴，相应的安全策略也同时依赖于企业不断变化的安全预期和IT预算。

● **忽略（Disregard）**：相当于忽略了个人设备在企业环境中的存在。这是一个糟糕的选择，企业采取忽略策略将不对当前基础设施做任何政策或技术的变化。注意这里安全压力不等同于安全风险，企业感受到的安全压力处在最小区域，但安全风险可能极大。

● **封锁（Block）**：使用自有设备将受到严格监管。企业将优先考虑其网络和数据的绝对安全，而轻视用户体验和满意度，员工将限定使用企业拥有的设备和SIM卡。由于NAC能够探测到连接设备的类型和合规状态，所以阻止使用BYOD不是多么困难的事情。

● **遏制（Contain）**：要实现这一策略，NAC需要联合广泛的产品然后粉墨登场。一种可能的组合方式是：NAC实现LAN/WLAN环境的身份验证、接入授权、计费和安全审计；IAM负责为设备下发配置文件，感知用户上下文，如发现设备的位置和服务状态；移动安全客户端自动执行下发的设备配置文件，如动态地开启一个VPN安全隧道，实现端到端的加密；至于DLP，可能集成在安全客户端做自我防卫，也可能在网络侧作为应用程序沙箱集成进入移动安全网关；轻量级的MDM可以跨多个手机平台和应用程序提供移动管理功能。通常，遏制策略可以灵活地将网络安全维持在可接受的水平。

● **协调（Embrace）**：近似于完美的策略，它让每个人的BYOD梦想成为现实。这一策略代表了一个巨大的文化转变，但也意味着巨大的技术操作的复杂度和显著增加的IT投资。调查显示，对一个企业，如果使用BYOD的基层员工超过雇员总数的30%，就可以被认为达到了协调的水平。另一方面，从技术上讲，在这种环境下，采用重量级的MDM技术可持续地跨多种移动平台执行设备管理策略将必不可少；部署VDI集中管理和保护敏感数据，将BYOD终端和业务基础设施隔离开来也是一个典型的例子。同时，在遏制策略中用到的技术控制手段需要精心策划并加强，以实现到协调层面的过渡，这包括增强安全政策的缩放性，既可扩展到企业全局，也可为不同部门或地域量身定制；整网的可视性、用户行为的细粒度控制、基于网络的内置DLP引擎的内容过滤和能够解密VPN连接，发现已经被攻击者攻破的合法用户在传播恶意软件等高级功能都是必须的。

重要的是，BYOD仅仅是揭开移动应用大趋势序幕的“冰山一角”。来自研究机构的调查显示，到2014年，移动设备将通过本机的硬件和OS功能“集装箱化”应用程序和数据。集装箱化技术将在设备堆栈中执行应用层防数据丢失，这种功能是需要高度遵守法规的企业成功实施合规审计的必要前提。预计未来会有越来越多的企业选择集装箱化技术结合MDM强制实施更强壮的安全控制能力。

此外，员工已经逐渐习惯了应用程序和IT支持服务

的自助式环境、软件即服务（SaaS）、云计算等技术创新，其本质是呈现以客户为导向、使人们工作生活更舒适的IT价值观，BYOD概念就是这种精神的体现。事实上，业界公认使用移动设备的主要业务风险是数据丢失，而对客户透明的基于云的SWG技术，能够通过黑白名单和内容过滤技术显著减少恶意软件渗透的影响，在已经谈到过的安全控制手段里，可能是最有前途的、可平衡智能手机和平板电脑安全性需求的长远方法。

最后，作为补充，BYOD不只是一个技术问题，它也是一个要求IT部门和人力资源、财务、法律团队协作来有效整合业务战略、安全政策和IT系统的商业问题。企业必须充分预测到安全违规的后果，并提供相应的IT手段以迅速平息不利影响。此外，责任的定义是必要的，不单对企业，以避免任何BYOD实施后可能的法律纠纷。其目的是让大多数员工明白，如果发生设备滥用或危及安全的事件，导致他们个人设备上的数据被擦除，遵守公司的政策将是他们应尽的职责；同样，如果员工没有及时报告任何设备/数据损失或者可疑的破坏行为，可能会导致企业的处罚，包括从擦除程序到终止BYOD权限。对于大多数希望装备更先进安全控制手段把风险降到最低的企业来说，这些做法是确保技术手段能够生效的根本。**BYOD**

BYOD不只是一个技术问题，它也是一个要求IT部门和人力资源、财务、法律团队协作来有效整合业务战略、安全政策和IT系统的商业问题。



赵爱明

企业员工乐于使用、现网和应用适配性好、企业IT放心并易于部署——只有实现这三者的和谐统一，才是企业最需要的BYOD解决方案。>>

如何“选型”BYOD方案？

▲ 华为BYOD首席架构师 赵爱明



技术含量有多高？特性有多丰富？不，这些都不能决定BYOD解决方案最终能否在市场上确立领先地位。“企业员工乐于使用、现网和应用适配性好、企业IT放心并易于部署”，只有实现这三者的和谐统一，才是企业最需要的BYOD解决方案。

员工乐于使用

企业员工使用率高（30%以上的工作相关的任务可以随身处理）是评判企业BYOD应用成功的唯一标准。方案设计需要秉承这样的理念：移动应用在规划与设计时除了要考虑到客户在3P（ThroughPut、OutPut、InPut）上与传统的固定带宽接入、大屏幕显示、鼠标键盘输入为主的办公方式不同，还要充分考虑到最终使用人员的实际IT水平、使用习惯等等。

使用体验好、企业员工喜欢使用的终端才有助于BYOD应用的推广。其典型要求是满足个性化需求，内置工作相关的应用集成，满足客户易用和安全实用的要求；结合行业特点和业务的定制化终端将更好地满足行业客户的移动办公和生产需求。

随着统一通信和协作类应用（UC&C）在移动性、虚拟化方面的增强，原先只有在固定办公室里才能顺畅使

用的应用也可延伸到任何场所和任何移动终端设备；差异化QoS确保高端用户总是能在最需要的时候享受到其应有的服务质量。

适合企业应用而量身定制的智能终端和企业移动云的完美结合，必将把企业用户的移动办公体验提升到一个前所未有的新高度，迈向BYOD的步伐将进一步加快。

现网和应用适配性好

在过去的几年中，很多企业都已经在移动办公领域进行了有益的探索，具体诉求和实施进展可能有所不同，但引入新的BYOD解决方案时必然要面临和考虑的问题是：当前的网络架构能否很好支撑新的业务部署？现有应用系统能否实现平滑迁移？华为的BYOD方案着重在如下环节帮助客户解决以上问题。

一是方案规划初期就将对第三方网络设备的支持作为集成验证和系统互联互通的必要内容之一。同时跟合作伙伴一起加强BYOD的咨询服务能力，依据客户现有网络架构和IT能力基础，量身定制最贴近客户需求的技术方案，并基于客户业务发展目标做出前瞻性的规划和迁移计划。

适合企业应用而量身定制的智能终端和企业移动云的完美结合，必将帮助企业进一步加快迈向BYOD的步伐。

引入新的BYOD解决方案时必然要面临和考虑的问题是：当前的网络架构能否很好支撑新的业务部署？现有应用系统能否实现平滑迁移？

二是充分发挥华为在技术积累和工程实施上的经验，为企业客户打造面向BYOD甚至未来理想办公空间WOF（Workspace of Future）的智能企业网络：随着新一代WLAN技术（如802.11ac）的发展成熟，以及3G/4G蜂窝网的规模部署和优化，无线接入带宽将不再是移动办公的瓶颈；智能AP的商用将极大优化远程接入环境下的用户体验，以视频为主流的富媒体应用将在移动终端上大放异彩；ALL IP网络将帮助人们真正做到利用身边最方便获取的终端，随时随地访问所需要的资源（混合云为主），就像如今我们日常生活中使用水和电一样便捷。

三是跟合作伙伴紧密结合，提供最适合其需求和行业特点的移动应用平台MEAP（Mobile Enterprise Application Platform），一方面适配和平滑迁移现有企业应用系统；同时也为ISV、应用集成商提供开发工具、开发应用系统接口，协同开发，满足云时代下大量新业务快速上线的需求。

企业IT放心并易于部署

随着大量公司配属和员工自带的移动设备、社交媒体平台以及混合云应用在企业网络环境下的运用，企业IT面临更大的挑战，包括部署复杂度加大、安全风险提



BYOD趋势下，企业IT需要重点解决的问题是：尽可能简化和集中自动化部署，高效管理和监控接入企业网络的终端和人，根据策略授予其相应权限，并根据需要动态采用相应措施。

升、多方管理的协同等。在BYOD成为一种不可阻挡的趋势的今天，企业IT需要重点解决的问题是：通过尽可能简化和集中自动化部署，实现高效管理和监控接入企业网络的终端和人的一举一动，根据所制定的公司安全策略、行业规范甚至区域性法规要求等授予相应的权限，并需要根据动态采用相应的措施。

传统的单一边界安全方案无法满足企业移动办公方案的安全需求，必须采用创新的“端、管、云”一体化、全方位的方法，来维护涵盖基础网络、终端、企业资产、个人数据和应用程序等在内的信息资产的安全。

部署统一的策略引擎，是实现统一接入、统一策略、统一管理的关键。在确保各种主流授权终端内外网统一安全接入的基础上，策略引擎作为基础网络和终端设备管理的纽带和协同决策部

件，对所有连接到网络上的终端设备（固定和移动）做全生命周期的上线、监控和注销管理。

只有具备了以上能力，IT管理部门才能敢于在企业内最大范围推广BYOD，并放心部署实施。每个公司都应有自己的BYOD战略，可根据自身情况和发展阶段选择合适的BYOD场景。

综上所述，华为在充分考虑企业员工接受程度、现网适配能力和易于IT部署等因素的基础上，顺应客户需求，凭借自身在“端、管、云”方面的积累和独特优势，与合作伙伴深度合作，提供以网络为基础，以安全为保障，以体验为导向的解决之道，并迅速推向市场，取得客户信任，成为最受企业客户信赖的BYOD解决方案。**BYOD**



Moataz Hassouna
Emaar (埃及) 公司 CIO

BYOD已成为Emaar提高员工满意度，并更好地服务客户的有力手段。>>

房地产巨头的BYOD之路

——访Emaar (埃及) 公司CIO Moataz Hassouna先生

▲ 本刊记者 李智鹏 Soheila Soheil

中东房地产巨头Emaar是一家业务遍及全球的著名房地产开发和租赁服务提供商，拥有Dubai Mall等大名鼎鼎的地标性建筑。其在埃及的全资子公司早在2007年就开始在移动终端上部署企业应用，踏上BYOD之路。随着业务的发展，Emaar已将包括通信协作、销售、客户管理等更多的企业应用部署到移动平台上，并将服务范围从公司员工扩展到更多的客户。关于BYOD，他们有哪些成功经验和心得？下一步的规划是什么？

ICT新视界：是哪些ICT方面的需求促使贵公司对部署BYOD产生兴趣？

Mr. Hassouna：实际上，最初促使我们部署BYOD解决方案的诱因是出于员工移动性的需要，我们希望员工能随时随地获取需要的信息，无论他们是在公司内还是在公司外。那还是在2007年，当时移动平台只有一个Windows Mobile，我们开始尝试在Windows平台上部署一些初步的移动应用。而今天，iPad、iPod、各种各样的Android移动终端几乎人手一部，这促使我们进一步扩展我们的BYOD解决方案，使之不仅服务于公司自身，还可以服务于客户，现在我们的客户也可以用自己的终端设备从我们公司的数据中心获取信息。

ICT新视界：Emaar的BYOD解决方案支持客户访问哪些信息？

Mr. Hassouna：一些CRM数据，比如客户需要支付的费用、他们委托租赁的房产的最新情况，客户还可以查询有哪些房产可供租赁……此外，我们正计划为同一个社区的客户设立一个具有部分交互能力的门户平台，以便他们能够互相交换信息、了解社区中的最新情况，并获取更多其它的服务。最为重要的是，这一切都是在移动中实现的，我们希望借此能提高客户和员工的满意度。

ICT新视界：你们为员工提供了哪些移动应用？

Mr. Hassouna：最初当然是收发email，和所有公司一样；接着是语音通信应用，比如在公司办公室内，员工可以将他们的移动设备当作办公电话使用，当然也可以用作私人电话，二者之间可以自由切换；然后是销售软件；现在，我们还发布了基于iPad平台的ERP应用，2012年年底前正式开始运行；此外还有设施管理、社区管理等一系列应用。目前上述大多数应用正在部署之中，2013年我们还将部署文档管理应用，该应用允许工程师随时随地通过手机查看工程进度、相关的施工图纸和一些建筑材料情况等。

“BYOD已经是大势所趋，我相信所有能够把握机遇、采取主动的公司最终都会获得成功。”

ICT新视界：能否介绍一下贵公司如何制定BYOD的部署计划？依据是什么？

Mr. Hassouna：在制定一个BYOD应用部署计划之前，首先需要建设一个安全的环境。因为接入你的网络的设备并非都是本公司的设备，一些设备属于员工或客户个人所有，所以应认真地检查其安全性和一致性。在此前提下，可以根据公司的业务目标制定应用部署计划。以我们公司为例，我们的业务目标首先是将房屋销售出去，其次是将售出的房屋交付给客户，最后是为客户提供相关服务。所以我们首先部署的是销售软件和交付应用，然后是设施管理和社区管理应用。另外，许多应用是立足于客户的喜好和需求决定的，例如我们现在就有一些应用将在客户中进行测试，听取他们的意见，如果他们喜欢，就继续进行部署。所以从某种意义上来说，客户不仅仅是我们的客户，还是我们的合作伙伴。

ICT新视界：您如何看待BYOD这种办公方式？未来5年将如何发展？

Mr. Hassouna：作为一个IT人员，最初我对BYOD是有所抵触的，因为对IT来说，如何管理这些用户和他们的设备是一个非常大的挑战。我们的本意虽然不希望管理他们，但我们正在管理公司的资产，不能允许任何公司数据发生泄漏和损失，我们对此负有责任。所以在对待BYOD上我们经历了从抵触到最终支持的转变。另外从个人角度而言，我当然更喜欢使用小巧的移动设备，现在我几乎不再使用电脑了。我认为到2016年，移动设备将成为办公的主流，而且任何一家公司都离不开它们。

ICT新视界：除了安全问题之外，部署BYOD应用时还面临了哪些重大挑战？

Mr. Hassouna：ERP可以说是最大的挑战，因为其中包含了公司最为敏感的数据，人们会担心这些数据的安全。

当你在公司之外通过移动应用访问这些数据时，你可能会意识到这些移动设备有可能会失窃或丢失，因为这些设备大多不属于公司所有，是客户的私人设备。所以我们应尽量避免在移动设备上存储过多的公司数据，而对于必需存储的数据，我们则将其隔离开来，以便在设备丢失时能够删除这些数据。为此我们与每一位BYOD终端用户都签署了一份协议，允许我们在设备失窃或丢失时删除这些数据。我们会标记并锁定丢失或失窃的移动设备，一旦它们开机连接Wi-Fi或移动网络，就自动清除相关数据。

ICT新视界：对于BYOD的安全和管理，您还有什么经验可与其他CIO们分享？

Mr. Hassouna：首先要注意的是，应该与所有BYOD用户签署终端用户协议，我们称之为EUA（End-User Agreement），这样当用户的移动终端发生失窃或丢失情况时，EUA将允许你清除所有相关的公司数据；其次还要注意，当员工在公司外部登陆公司网络时，应对他们进行身份认证，以保证安全性；最后我对企业CIO们的建议是——BYOD已经是大势所趋，我相信所有能够把握机遇、采取主动的公司最终都会获得成功。**BYOD**



移动办公系统帮助华为公司每年节省了数千万美元IT费用，提高了员工满意度，使整个企业办公效率提升了40%。>>

移动办公改变华为人的工作和生活

3大挑战，3大需求

经历了20多年发展，华为的业务已经从中国扩展到全球140多个国家，拥有500多个代表处，15万员工。业务的全球化和以客户为中心的文化氛围，使华为员工的日常办公模式面临着新的挑战：90%的公司高管需要频繁出差会见客户，同时日常还要参加大量会议；70%的营销人员需要经常拜访客户，与客户交流；80%的服务人员需要在野外环境工作……在此情况下，要保证员工能够及时处理客户邮件、审批销售合同或者上报工程进展情况等，只有快捷高效的处理才能给客户带来价值。

为此，华为公司IT部门从2009年开始规划和实施移动办公解决方案，在实施的过程中，3大IT需求成为移动办公方案必须要考虑满足和解决的问题。

- 部署哪些移动业务，可以解决员工日常办公面临的挑战？
- 如何保证来自内部和外部的成千上万智能终端访问公司资源的端到端安全性？
- 在对现有网络进行改造的同时，如何保证现有业务的正常运行？

移动办公分步走

Step1：分析业界实践，确定规划原则

规划中，华为充分吸取了业界优秀实践：企业应视移动应用为一种变革，致力于业务价值的提升，而不是局限在某些部门、仅实施协作类应用或仅实现PC机功能的迁移；80%的移动应用（OA除外）重点在销售、服务、BI 和物流等领域。

华为移动办公的规划本着4个原则：

- 全流程规划，不是简单复制；



- 客户、员工和公司3方受益，提升业务价值；
- 统一技术架构，减少开发复杂度并支持可扩展性；
- 提升用户感知，移动UI简洁、易用。

Step2：规划主要的移动业务

在确定移动办公规划原则后，首要考虑的是到底有哪些业务可移动化。通过4个步骤，华为完成了移动业务的规划，明确了哪些业务实现移动化。

- 评估现状，认清方向

据分析，目前大致有70%的企业正在考虑移动化办公，30%的企业已经实现了，在这已经实现的30%企业中，移动应用发展主要经历了3个阶段：OA移动化（20%）、主业务移动化（8%）、业务创新（2%）。华为目前已经全部实现了OA的移动化，主业务移动化正在进行中，如iSales、iSite等移动化业务。

- 识别移动应用的角色和场景

梳理清楚主要的业务场景，以及在这些场景下使用移动应用的主要角色有哪些。华为的主要业务场景为：客户活动、采购物流、现场交付、售后服务。在这些场景中，伴随管理决策和业务审批，移动办公的主要使用角色为客户人员（市场人员、服务人员）、管理者。

- 选择适合移动应用的业务功能

业界对此问题普遍认可的是“简单、易用、易实现”，结合智能移动终端的优点（易操作、易拍照、易定位、易扫描等），华为重点规划了4类业务：信息采集类（工作现场获得数据，通过移动终端录入系统，如故障拍照）；审批类（通过手机参与流程审批，发出指令，如合同决策审批）；查询类（在现场录入查询条件，获得现场支持信息，如PO执行进度查询）；报表类（根据工作需要，在终端上及时获得决策支持信息，如月度销售情况报告）。

- 对需求进行识别和排序

对需求进行识别，聚焦面向客户业务流的效率和用户感知提升。在此原则下，把需求放到三维规划工具中，分别从角色维度、场景维度、移动设备特性维度进行需求识别。识别出的需求，还需

链接

华为公司移动办公大事记

- ◆ 2009年，开始移动办公规划，制定3步走策略：OA移动化、业务移动化、业务创新；
- ◆ 2010~2011年，实现OA的移动化和协同，推出安全Pushmail、移动审批、移动黄页查询、移动社交、移动差旅等；
- ◆ 2012年，主要业务移动化，推出华为mobile Portal移动营销平台、iSite基站移动管理系统、iSales销售项目管理；各业务部门也相继发布移动App应用，客户可以直接通过移动终端了解公司产品，下订单；
- ◆ 2013年，更多业务实现移动化；推出针对Android平台的公司配机(iPad)；
- ◆ 2014年~，全面推行平板电脑，并持续进行业务创新。

对企业员工的宣传也是一个不可忽视的因素，让大家知道、了解、使用并喜欢上移动办公的模式，需要IT人员进行不懈地宣传。

要进行需求排序，在平衡收益、成本和业务成熟度下，排出优先级。

第一优先级：面向一线员工、管理者，重要紧急、业务成熟、价值高，提升客户/合作伙伴感知；第二优先级：业务需改进、重要不紧急、IT技术和后台系统需准备。

Step3：对IT基础设施实施改造

移动办公要很好地应用起来，在IT基础设施改造上也要遵循3个原则：

- 对IT基础的改造不宜过大，实施周期不能过长

移动办公是在现有的IT平台上实现，必须以很少的代价并保证业务的连续性，因此改动不能大。考虑到建设周期等因素，IT基础设施的改造实际上可以同步或者先于移动业务的规划开展，特别是无线、安全等网络设备可以先进行部署。从华为的实践来看，对现有系统的改造可大致分为如下3步即可实现。

首先，终端改造。终端侧只需安装华为开发的Any office移动办公平台，一次安装，集成多个业务，如安全Pushmail、Webmail、即时通信espace、W3业务（流程审批、查询等）。

部署MDM（移动设备管理平台），对终端进行全生命周期的管理。

其次，网络改造。网络无线化改造，在主要办公区域部署AP，实现无线全覆盖；部署内网用户安全接入网关（USG），实现对公司内部移动办公业务的安全管理；部署安全虚拟VPN网关（SVN）设备，实现对通过公网接入到公司内部资源的移动办公业务的安全管理。

最后，业务改造。根据前期规划出的主要业务类型，部署MEAP（Mobile Enterprise Application Platform）平台，进行业务开发或者联合合作伙伴开发。

- 安全性问题需要重点考虑，端到端实施

安全问题是移动办公规划必须要考虑的问题，当成千上万的智能移动终端通过公网接入到企业资源，安全隐患随之而来。从终端本身，到传送的网络，再到业务层，处处都可能成为黑客或不法人员攻击的目标。

首先，对终端的获取（硬件配置、软件安装）、部署、运行和回收（注销、丢失等）的端到端生命周期需要进行管理，保证每个过程的安全性。通过部署MDM平台，实现对终端的资产注册管理、终端接入认证、终端安全合规性检查等。

其次，在网络的传送层，从应用到网关实现4层加密，从设备到网关建立起SSL VPN链路，保证网络传送的安全性。

第三，对于应用的安全性，要双向考虑，从保证安全应用的鉴定、授权、发布和管理，到实现对应用访问的安全。

- 根据企业自身情况选择移动办公模式

企业可根据自身的实际情况，选择为公司员工配智能终端或者采用BYOD的方式。另外，对企业员工的宣传也是一个不可忽视的因素，让大家知道、了解、使用并喜欢上移动办公的模式，需要IT人员进行不懈地宣传。华为作为高科技企业，智能移动终端的使用率很高，员工年轻，接受程度也比较好。

改变工作和生活方式

华为依托自身的MEAP平台，为移动办公开发了办公、黄页、咨询和社区等4大类，几十款丰富的移动应用。

移动改变了华为员工办公和生活的方式。如今，华为员工无论是在机场排队候机，还是在宾馆等待办理住宿，打开智能终端，连接“Pushmail”，可随时随地上网处理邮件；打开“待办审批”审批流程，处理完毕即可进行娱乐；在酒店里可通过“移动espace”随时参加即时会议，在移动终端查看共享的会议资料等。

华为每天有数万人在出差状态，“移动差旅”服务可以帮助员工方便快捷地订机票，订协议酒店，获取当地的天气情况，“惠通服务”还会根据员工出差地点，推荐一些旅行自助信息；华为在全球有500多个代表处，“华为身边”服务利用移动终端LBS定位服务，可帮助出差员工快速

定位到当地代表处的位置。员工还可以通过“移动社交”进行内部的互动交流，发表对公司重要事件的看法建议等。

华为在全球为大量客户建设基站，很多都是在野外场景，如何快速获取任务，如何及时上报工程进展情况，让客户满意，公司受益，“iSite 站点实施管理”让员工可以通过移动终端实时查看到自己的任务，分属哪些站点，并查询施工站点位置；在到达站点后，施工人员可以通过手机打卡完成站点进入的记录，减少了手工登记的麻烦；在施工过程中，可以查看上次施工遗留问题，并进行施工进展的更新；遇到重大问题时，还可以通过拍照反馈站点现场情况，及时发送给总部支持人员，实现了问题的快速解决。

移动应用同样可以直接为华为的客户服务，客户可以通过“华为Mobile Portal”实时了解华为的新闻、市场情况；通过“华为网络资料”随时了解华为网络产品和解决方案；通过“华为网络设计工具”让客户自主进行网络设计，没有技术知识，也能根据自己的需求配置出需要的网络方案。**BYOD**

链接

员工“心声”

- ◆ **管理人员**：“现在太方便了，通过智能手机在机场、公共办公区都能及时审批和处理业务了”；
- ◆ **客户经理**：“通过手机及时了解即将接待的客户信息和时间安排，让我们能更从容不迫”；
- ◆ **维护工程师**：“现在不必再等待了，在现场通过智能终端直接拍摄问题，增加描述信息后，回传到系统中，处理速度大大加快了”。



电子版请登陆enterprise.huawei.com阅读或下载

索阅、投稿、建议和意见反馈，请联系编辑部

E-mail: ICT@huawei.com

编辑部地址：中国深圳市龙岗区坂田华为基地H2 电话：（0755）28780808

更可以在新浪微博上随时与我们互动，
请@ICT新视界；

期待您的声音！



版权所有©2012华为技术有限公司，保留一切权利。

非经华为技术有限公司书面同意，任何单位和个人不得擅自摘抄、复制本资料内容的部分或全部，并不得以任何形式传播。