NetIQ

BYOD – 提高生产力的案例

提高生产力、加强协作的机遇

很久之前，人们只能在便携式计算机或 PC 前工作。员工越来越多地开始在路途中或者家中完成工作或是与他人协作，往往有着灵活的工作时间。如果专业人员能与客户和合作伙伴迅速沟通，业务的发展速度将更快、效率将更高，满意度也会得到提升。现代职员在一天当中的任意时刻都可能在办公室外继续工作，但为了实现这一目标，同时保证不产生麻烦的障碍，职员需要从任意位置访问应用程序和资源，流程需要自然、简单和安全。

移动设备的消费化

在这种以提高生产力和业务灵活性为目标的趋势中，一个重要因素就是移动设备的消费化，大多数情况下，这其中涉及朝着自带设备 (BYOD) 策略的过渡。企业应对这种趋势的方式决定着他们利

BYOD – 这是属于他们、而非属于您的设备

82% 的人认为跟踪功能是对其隐私的侵犯

76% 的人不会为其雇主提供查看其个人设备中有哪些应用程序的访问权限

75% 的人不会为获得公司资源访问权限而允许其雇主安装应用程序，让公司能够定位自身位置

82% 的人担忧或极度担忧其雇主跟踪自己在业余时间使用个人设备浏览的网站

86% 的人担忧或极度担忧他人在未经授权的情况下删除个人图片、音乐和电子邮件配置文件

来源：**www.maas360.com/maasters/blog/security-information/byod-beware-infographic/?A=PR**

焦点文件

业务挑战：

控制对业务的风险，同时让用户保留其个人设备的隐私。

解决方案优点：

- *面向 BYOD 用户的便捷访问*
- *面向业务的安全访问*
- *最低限度的投资 – 利用现有访问基础设施和策略*
- *提高用户满意度和生产力*

用这一独特机遇的效率。生产力的提升不会自动发生。仅仅出于业务安全方面的顾虑就全盘否定创新的变革方法是一种过于简单的做法，因为这类变革方法能够改善用户交互、协作和开展业务的方式。

员工、承包商和合作伙伴需要随时通过任何设备访问相关信息，以支持 SaaS 和内部网服务。IT 组织能否在现有基础设施之上进行创新，他们是否会隔离和约束移动用户？

随着 SaaS 应用程序对于组织的重要性与日俱增，IT 部门也需要确保同时支持 BYOD 和云访问。

公司和其他组织需要积极控制风险、保证私有信息安全，同时为业务提供支持，这一点又加大了挑战的难度。

利用过去的身份和访问投资

如今，我们很容易就会忘记在整个组织范围内交付信息、应用程序和服务的方式变得有多复杂。通过将身份和访问管理布设在公司内部网之上，组织即可提供一个门户，为员工提供满足自身需求的自由。这其中可能包括搜索分散在组织各处的信息，参与知识交换以及与其他组织协作。

内部网虽然往往会带来聚集、合并、储存和集成所有不同类型的业务信息与服务的大笔基础设施投资，但同时也会带来便捷而安全的访问。因此投资于身份和访问管理的组织已经并且即将继续从中获得巨大价值，这也就并不出人意料了。包含强大身份和访问管理技术的内部网可帮助用户快速获取适当访问权限，同时提供统一的体验并管理用户鉴定。对于提供单点登录的组织而言，应用程序已经不再是孤岛，而是单一、高效、统一体验的一部分，让用户通过一次鉴定即可访问一切。问题在于，组织能否为其 BYOD 用户实现相同的优势。

访问成熟度

尽管提高用户生产力和用户满意度的业务优先级通常排名靠前，但控制风险同样重要。为了保护知识产权、财务数据或客户信息，组织已经发展改进了内部流程和基础设施。医疗保健或金融服务业组织还必须应对法规，随着这些法规越来越严格，IT 将继续依靠传统内部网遵循严格的访问要求。组织负担不起抛弃安全访问投资的代价。

基于现有投资而构建

成功实施 BYOD 的诀窍在于保证 IT 将当前内部网访问投资扩展到每一位用户

内部网中的 BYOD

优点：

- 成本转移给用户（预计有 50% 的公司需要员工自行承担成本）
- 用户更满意，生产力更高
- 更多业务时间 — 员工更愿意在私人时间回复业务邮件
- 企业 IT 的灵活性更强，能够采用新的工作模式
- 激发创造力 — 采用新方式使用 BYOD，以便开展业务

顾虑：

- 与在私人设备上存储公司数据相关的安全问题
- 在现实中，IT 不能彻底摆脱为这些设备的访问进行查错的负担
- 通过 VPN 进行访问通常速度缓慢、较为复杂，可能容易出现问题，甚至不受支持
- 企业需要对其员工开展与访问公司数据相关的安全性和公司良好实践培训

时不会过度昂贵或复杂。IT 尝试在设备级别管理访问时，将无法利用过去的投资。而是必须重新投资，实施新的应用程序保护或访问控制措施。通过集中精力关注用户身份，组织即可利用现有内部网的功能、安全性和专业技能，而不必构建重复的功能。

这也意味着 IT 组织需要停止将其内部网视为需要用铜墙铁壁保护的场所，开始更多地将其视为欢迎用户的位置，而不论这些用户位于何处、使用何种设备。通过集成现有资源提供移动访问能解决许多 BYOD 挑战，但创建用户所需的完整移动访问解决方案还可能要涉及到云。

访问云

组织越来越多地从云端以基于 SaaS 服务的形式获得重要业务服务。现代组织需要向员工、合作伙伴和客户交付超出其 IT 控制范围的服务。这些服务托管在云端，访问权限大多由单独的身份和访问控制基础设施提供。许多 IT 组织都采用这样一种方法：如果无法控制，那么就不必去管理；特别是在 BYOD 用户访问这些服务时。这种观点有几分目光短浅。在许多情况下，整套服务均基于云，而访问控制和安全性对于企业来说仍然十分重要。IT 有责任也有机会保护对于敏感业务信息的访问，无论这些信息位于何处。

NetIQ 的整体 BYOD 方法

部分 IT 组织采用逐例方法满足 BYOD 访问需求，最终只会得到来自多家供应商、相互脱节的工具。集成这些工具或在其基础之上进行构建往往极为困难。NetIQ 在整体上采用由身份支持的访问方法，其解决方案能够解决当今的多种访问难题。

仅有 20% 的组织相信，管理移动设备是保护其信息的正确方法。

便捷的移动访问

组织正在寻找利用移动设备（平板电脑和智能电话）的新途径，以期提高效率并支持新的业务流程。但移动设备与 PC 工作站的工作方式不同。它们通常并没有外接键盘，屏幕所提供的用户体验也与台式机或便携式计算机截然不同。在台式机上可以快捷轻松地完成的操作在移动设备上可能繁琐耗时。NetIQ 支持在移动设备上快速、便捷、安全地访问内部和 SaaS 应用程序。

控制风险

在保护私有信息方面，例如知识产权、客户信息和受监管的数据，仅仅由于需要为 BYOD 用户实现便捷访问并不意味着能放松防备。NetIQ 让用户能在移动设备上迅速访问基于 Web 的应用程序视图，包括内部应用程序和 SaaS 托管的应用程序。NetIQ® 解决方案通过利用现有基础设施，并确保仅正确的人员才能获得访问权限，也为 IT 带来了优势。由于 NetIQ 专注于管理和交付对受保护服务的安全移动访问，而非管理或锁定移动设备，因此无论您采用何种 BYOD 方法，我们的方法都能完美运作。

若要了解如何利用当前投资支持员工和合作伙伴进行安全的 BYOD 访问，

www.netiq.com

由身份支持的全面访问

访问实施			
访问认证	访问请求	访问管理	委托管理
访问授权			
单点登录	用户鉴定	授权执行	特权访问管理
访问监控			
仪表板、风险与趋势	安全性与活动信息	取证分析和报告	日志管理报告

请访问：**www.netiq.com/solutions/identity-access-management/single-sign-on.html**

40% 的组织对自身保护通过移动设备访问内部网的能力并不自信。

来源：**www.sans.org/reading-room/analysts-program/SANS-survey-mobility**

安全性仍然是企业实现 BYOD 的头等障碍

认为以下事宜极度重要的受调查者：

57% 的受调查者认为是数据保护

55% 的受调查者认为是保护对各种公司资源的访问权限

51% 的受调查者认为是控制和了解哪些人能访问敏感信息

NetIQ
北京络威尔软件有限公司
中国北京市朝阳区东三环中路 7 号
北京财富中心写字楼 3603 室
电话：8610 65339000

info@netiq.com
www.netiq.com/communities
www.netiq.com

有关我们在北美，欧洲，
中东，非洲，亚太平洋和
拉丁美洲的办公室详细列表，
请访问 **www.netiq.com/contacts**

www.netiq.com