IDC
Analyze the Future

信息技术第三平台时代的
安全发展趋势

INFORMATION SECURITY TRENDS ON IT THIRD PLATFORM

合作机构

360互联网安全中心

目录
DIRECTORY

图目录

IDC观点

2013年全年，中国的IT支出已经达到1827亿美元，已全面超越日本也成为仅次于美国的世界第二大IT支出市场。中国的IT开支正在以两位数的速度增长，增速远高于美国等发达国家成熟市场。从信息安全投资比例的角度分析，中国信息安全投资占整体IT支出的比例仅为1%，而对比美国以及日本等发达国家的成熟市场差距较大。然而随着用户对信息安全需求不断的增加，以及政府的政策法规的驱动，中国信息安全市场未来潜力巨大，前景乐观，IDC预计2014到2018年，中国IT安全市场的复合增长率将达到14.5%，位居企业级系统市场的前列。

当前安全硬件依然是中国信息安全产业投资的重点，主要还是集中在安全基础设施的建设，产品的更新换代等；而安全服务的占比与日本以及美国安全服务市场的对比要低的多，对于用户来说，信息安全投入不是单一地依靠买更多的设备，而是需要做好安全规划以及评估安全建设的效果，安全服务在其中扮演很重要的角色。随着信息安全市场的蓬勃发展，安全服务的理念必然逐步改变，国内安全服务市场还存在很大的发展空间。

以移动设备和应用为核心，以云服务、移动宽带网络、大数据分析、社会化技术为依托的IT市场第三平台时代已经到来，引领未来的发展。第三平台安全的发展趋势主要包括：

· 短期来看，云服务提供商将会增加安全技术的投资，比如加密技术、身份管理和访问控制（尤其是双因素认证）以及流量检测技术。云计算密钥管理生态系统是一个新兴的热点，随着成熟的供应商产品和服务不断涌现，在云计算中存储敏感数据一定会而变得更易于实施。

· SDN在安全领域的应用是改善云安全的一个机会。安全功能集成到软件定义的网络产品及架构中，将提供和独立的安全设备和安全软件产品相同的功能。随着SDN的成熟和发展，供应商将安全功能集成到虚拟化的网络服务堆栈，未来企业环境中独立的安全软件或安全设备的需求可能将降低，这种方式将打破传统的安全部署和管理。

· 随着用户对安全服务认知度提高，以及当前信息安全专业人才的短缺，预计将会有越来越多的用户采用安全云服务来更准确的地把握全网安全动态，期待安全即服务模式的快速发展。

· 新型攻击的特点也决定了现有的检测机制恐难以凑效。因此作为防守方，需要改变策略，其中一种方式就是依靠来自外部的安全威胁情报，通过监测威胁情报中是否存在针对特定软件、系统或行业的攻击，企业可以确定其是否在使用易受攻击的软件或系统，然后在攻击发生前部署缓解措施。威胁情报分析市场应运而生，并蓬勃发展。

· 基于大数据安全分析技术的新一代安全运营中心将快速发展。大数据分析技术是一种工具，并不是能够解决所有问题，这要求开发者服务提供商以及最终用户不断的探索，同时在安全领域，专业的安全数据分析师的短缺是现实，未来期待更多的安全分析专业人才的涌现。

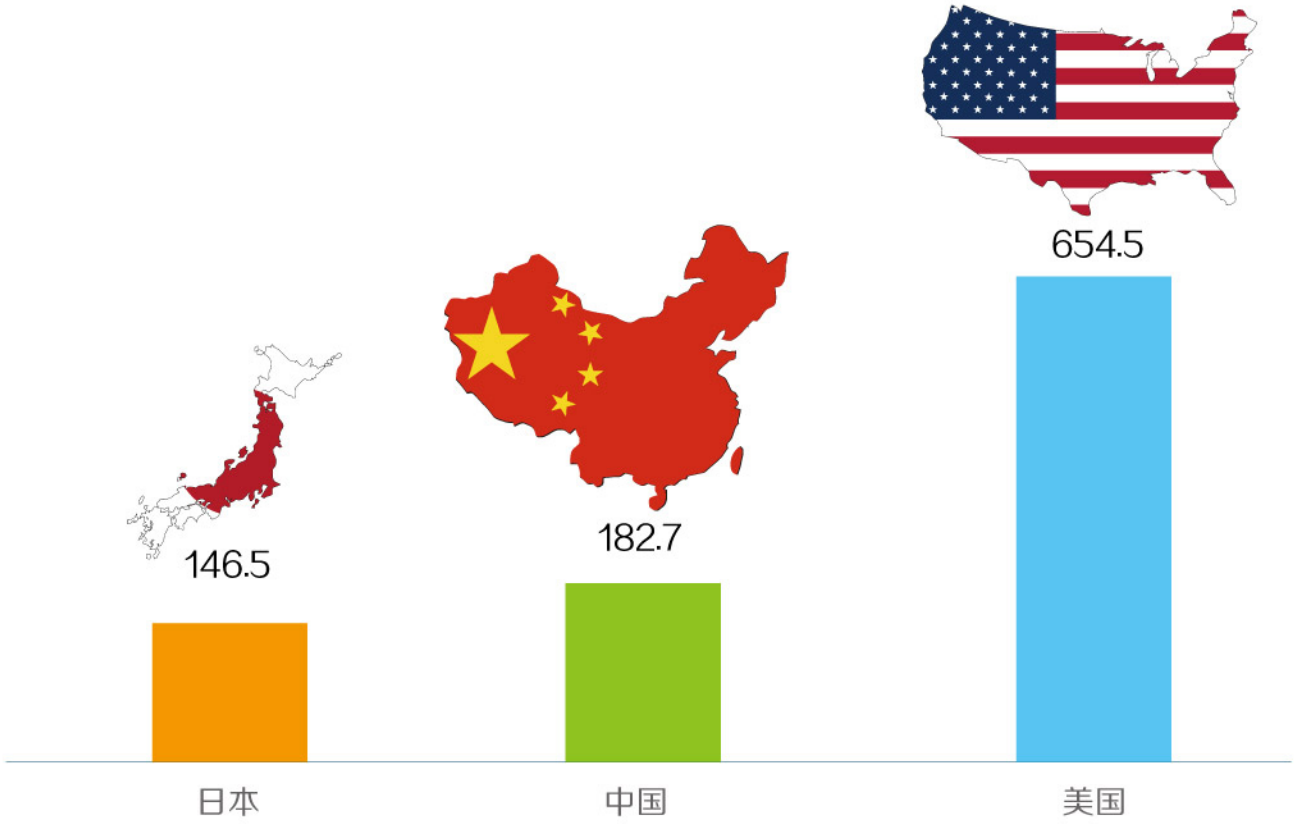
· 全球企业级移动安全市场将保持迅猛增长，预计到2018年其市场规模将达到28亿美元，未来五年的复合增长率为19%。中国企业级移动安全市场总体上还处于起步阶段，预计未来2-3年是移动安全的高速发展阶段。其驱动力来自IT消费化、恶意程序增长迅速、移动数据容器化等。

关于白皮书

2013年全球由于网络犯罪导致的经济损失超过5000亿美元，而中国也超过了百亿美元，随着信息化的发展，信息安全面临的挑战将越来越严峻。本白皮书探讨了全球及中国在信息安全领域投资的规模以及安全服市场的现状及发展趋势。另外，IDC依据在信息安全领域的研究经验，给出了在以云计算、大数据分析、移动互联以及社交网络为支柱的信息技术第三平台时代信息安全未来的发展趋势。

市场综述

2012年底，中国实现了一个关键指标，已全面超越日本成为亚太地区最大的IT产品和服务消费国，同时也成为仅次于美国的世界第二大IT支出市场。2013年全年，中国的IT支出已经达到1827亿美元，随着企业用户日益增长的IT需求以及政府政策推动带来的IT机遇，中国的IT开支正在以两位数的速度增长，增速远高于美国等发达国家的成熟市场。

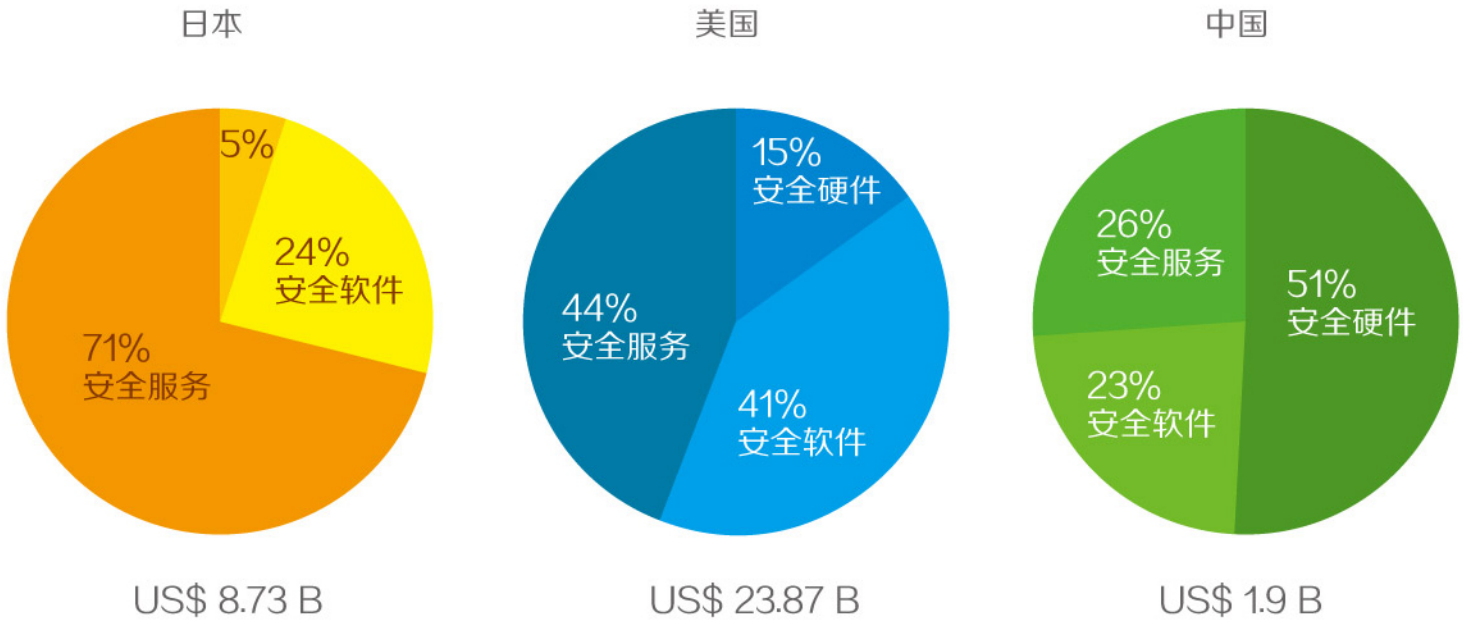


2013年中国、美国、日本IT支出对比 (US$ B)

来源: IDC World Wide Black Book, Version 2, 2014

信息安全投资对比

据IDC发布最新的研究报告《中国IT安全硬件、软件和服务全景图，2014?2018》显示，2013年中国信息安全投资总额为19亿美元，同比增长13.6%，占整体IT支出的比例仅为1%。而对比美国以及日本等发达国家的成熟市场，美国信息安全投资比例保持在4%左右，而日本信息安全投资比例高达6%。由此可见，我国的信息安全市场规模以及投资比较仍然偏小，与发达国家差距较大。然而随着用户对信息安全需求不断的增加，以及政府的政策法规的驱动，中国信息安全市场未来潜力巨大。IDC预计2014到2018年，中国IT安全市场的复合增长率将达到14.5%。IT第三平台的新兴技术云计算、大数据、移动以及社交网络的发展将是引领未来安全领域增长主要的方向。



2013年日本、美国、中国信息安全投资分布

来源: IDC World Wide Black Book, Version 2, 2014; IDC World Wide Security Product and Service Tracker; IDC China IT Security Big Picture 2014-2018

IDC
Analyze the Future

安全服务期待提升

当前安全硬件依然是中国信息安全产业投资的重点，其领域覆盖了安全基础设施的建设，产品的更新换代等；而安全软件市场在中国有一定的特殊性，比如消费类防病毒软件市场以免费模式为主导，企业级整体安全管理体系不成熟等原因影响了安全软件市场的发展，但欣慰的是我们能看到一些行业如金融、电信，对高阶的安全软件需求依然旺盛，比如安全管理平台的建设，数据防泄露的解决方案，所以随着安全基础设施建设的完善，对安全软件的需求也会增加。

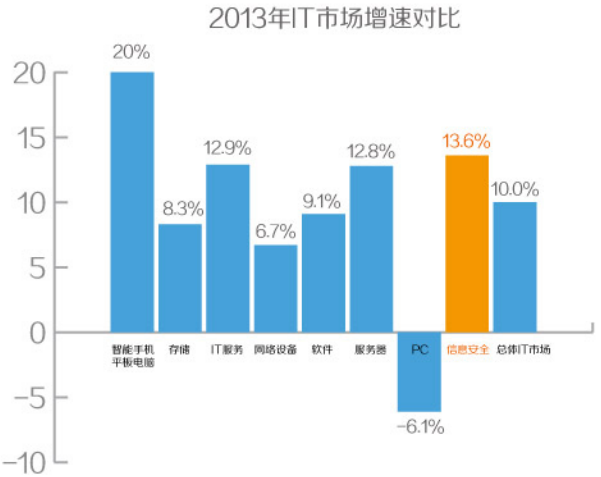
提及安全服务，图2显示了中国与日本以及美国安全服务市场的对比，显而易见在发达国家的成熟市场对安全服务的接受程度远远高于国内，服务收入的占比一定是高于产品收入的占比，比如日本的安全服务市场规模占总体安全投资70%以上，美国的安全服务市场占比也快接近五成，而以往中国用户更能接受“服务就是产品的附属品”这样的定义，只要产品还存在，服务就存在，甚至是免费的，这也成为当今信息安全企业面临的压力所在。对于用户来说，信息安全投入不是单一地依靠买更多的设备，而是需要做好安全规划以及评估安全建设的效果，安全服务在其中扮演很重要的角色。随着信息安全市场的蓬勃发展，安全服务的理念必然逐步改变，国内安全服务市场还存在很大的发展空间。

国内安全服务面临最大的问题在于，安全服务的市场渠道扩展存在困难。目前，安全服务还主要集中在重点行业和大型企业用户，安全厂商对于中小企业的业务仍然以产品销售为主，其次经验不足、安全服务人才短缺也是国内完善安全服务市场急需清除的障碍。随着用户对安全服务理念的认知度越来越高，中国的安全服务市场将期待一定的提升。

中国信息安全市场前景乐观

信息安全行业一直是政策重点扶持的行业，政策也一直是推动信息安全产业发展的第一动力。随着国家安全委员会和中央网络安全与休息化领导小组的成立，标志着当今信的信息安全已上升至国家战略高度。信息安全形势的日益严峻，国家对信息安全产业的重视程度日益提高，随着政府及行业的政策法规推动，必将促使中国信息安全市场空间日益扩大。

从2013年IT整体市场看，总体的IT市场的增长率达到10%，这得益于智能手机及平板电脑市场的拉动，从细分市场来看，除了消费类市场以外，IT服务，服务器以及信息安全市场的增长率超过总体增长率，而信息安全以13.6%的增长率位居企业级系统市场的前列。

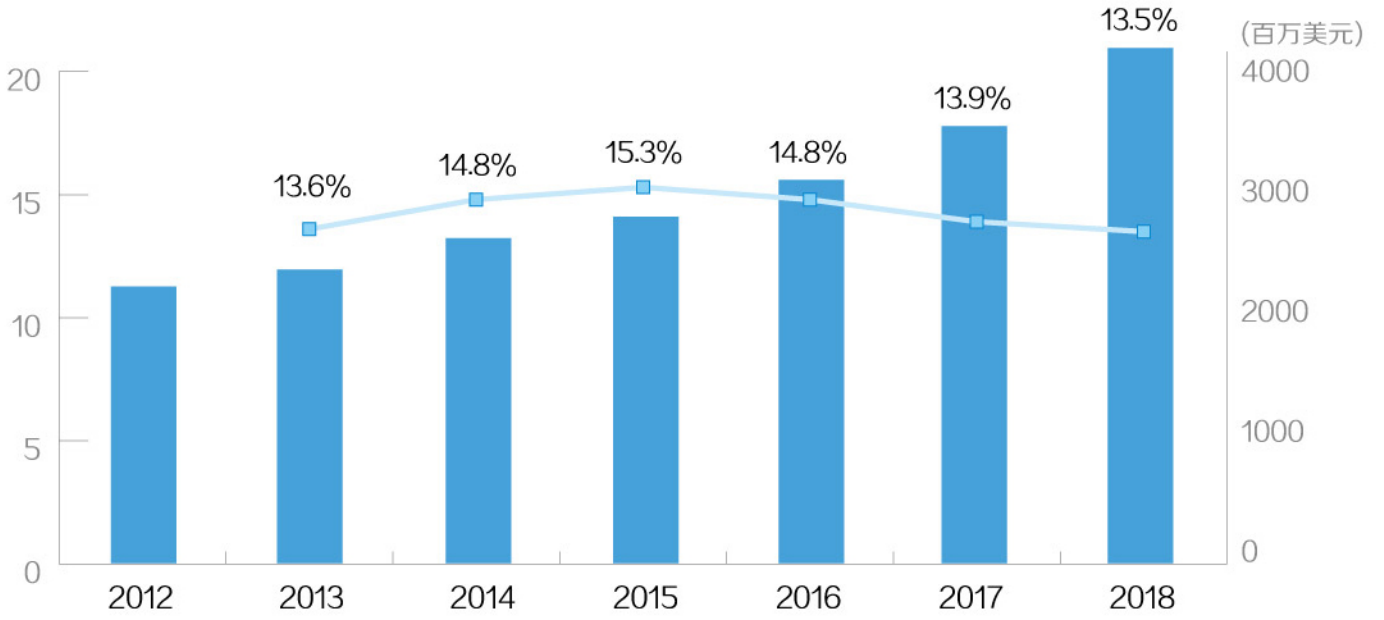


信息安全市场增速显著

来源：IDC World Wide Black Book, Version 2, 2014;

政策驱动促进中国信息安全产业发展

信息安全行业变革刚刚开始，政策变化驱动行业加速成长。国安委及中央网络安全与信息化领导小组的成立，标志着信息安全战略将是国家安全战略的重要组成部分。IDC预计后续的相关信息安全法规将推出，有效完善行业监督管理机制，并将在计算机信息系统安全保护制度、互联网信息服务、电子交易安全、信息采集与利用、法律责任等方面作出明确规定，从而有效完善行业监督管理机制，解决过去因为没有统一完善的信息安全法导致的交叉管理、职能不清晰等问题，将有效完善行业监督管理机制，催生行业中相关需求。在我国信息安全形势不断恶化，而前期投入严重不足的大背景下，国安委的成立、信息安全法的颁布都将成为行业发展强有力的催化剂，IDC预计2014到2018年，中国IT安全市场的复合增长率将达到14.5%。



中国信息安全市场规模及预测, 2012-2018

来源: IDC China IT Security Big Picture 2014-2018

IDC
Analyze the Future

未来展望
FUTURE

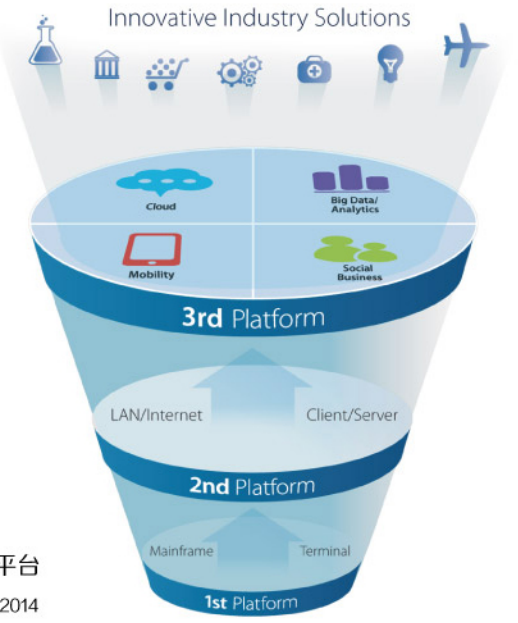
什么是信息技术第三平台?

所谓信息技术第三平台，是以移动设备和应用为核心，以云服务、移动网络、大数据分析、社交网络技术为依托的全新格局。此前，IT市场已经经历了两个平台，分别是20世纪60年代开始的以主机和终端为主的第一平台和80年代开始的以PC为核心，以局域网、服务器、互联网为依托的第二平台。

从第一平台到第三平台，面向的用户数更多，和人的距离也更近，每一个独立的个人，都有可能变成第三平台里的用户或者说是企业的客户。因此，对于IT服务提供商而言，也意味着更多的机遇。如今，第三平台正在渗透到我们工作生活中的方方面面。

IT第三平台技术引领信息安全发展方向

以移动设备和应用为核心，以云服务、移动宽带网络、大数据分析、社会化技术为依托的IT市场第三平台时代已经到来，第三平台与行业用户的转型升级将紧密结合，为行业用户提供高附加值的混搭解决方案，使行业变得更加智慧，促进下一轮生产力的提高和商业创新，满足新一代用户的大规模个性化需求，引领未来的发展。



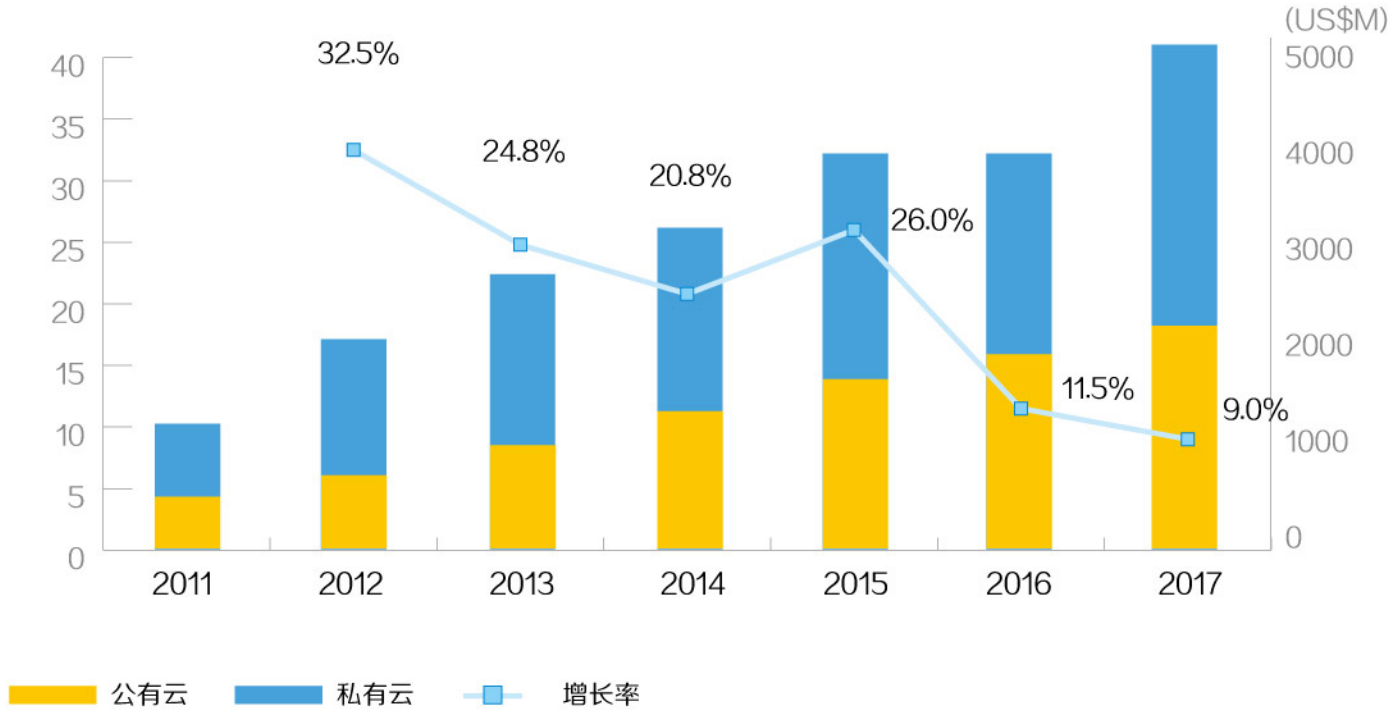
IT第三平台

来源: IDC, 2014

云安全

云计算在信息时代掀起了一场革命，使得信息可以像普通商品一样按需使用按量订购。基础资源的共享和规模经济效益的提升，使云计算为各行各业带来一种富于竞争力的全新服务模式。同时云计算使资源供给模式发生了改变。云计算供应商通过网络提供IT服务，集中投资获得规模经济效益。用户管理各自的IT服务，按需使用资源和付费，降低了成本。云计算更使资源交易发生了改变。云用户可以花更少的时间来管理复杂的IT资源，从而把更多的时间投入到核心业务中。企业越来越多地开始使用云计算服务，但是云计算的安全问题仍然是企业部署这些服务的最大障碍。

根据IDC全球云安全报告显示，2013年全球云安全产品的市场规模达到27亿美元，预计到2017年市场规模将达到51亿美元，五年的复合增长率达19%。



全球公有云和私有云安全产品规模及预测，2011-2017

来源: IDC Worldwide Cloud Security 2013?2017 Forecast

IaaS云环境的安全技术发展

云计算在信息时代掀起了一场革命，使得信息可以像普通商品一样按需使用按量订购。基础资源的共享和规模经济效益的提升，使云计算为各行各业带来一种富于竞争力的全新服务模式。同时云计算使资源供给模式发生了改变。云计算供应商通过网络提供IT服务，集中投资获得规模经济效益。用户管理各自的IT服务，按需使用资源和付费，降低了成本。云计算更使资源交易发生了改变。云用户可以花更少的时间来管理复杂的IT资源，从而把更多的时间投入到核心业务中。企业越来越多地开始使用云计算服务，但是云计算的安全问题仍然是企业部署这些服务的最大障碍。

根据IDC全球云安全报告显示，2013年全球云安全产品的市场规模达到27亿美元，预计到2017年市场规模将达到51亿美元，五年的复合增长率达19%。

IDC认为，短期来看云服务提供商将会增加安全技术的投资，比如加密技术、身份管理和访问控制（尤其是双因素认证）以及流量检测技术。

纵观中国市场发展状况，国内的云计算市场竞争非常激烈，中小型云服务商对安全服务的投入较少，采购第三方安全产品的情况也不多见，其目前就是为了降低成本。为了给用户提供更完善的云服务，中小型云服务商更倾向于与第三方专业安全产商合作打造安全的云服务环境。随着市场的成熟，未来的发展方向还是与全球发展趋势保持一致。

加密和身份管理技术是基石

根据IDC全球云安全研究结果表明，加密技术和身份管理是公有云安全的基础，也是一组强大组合拳帮助云服务商和企业确保在不可信环境中运行的数据及应用的安全性。

IAM（Identity and Access Management）身份管理及访问控制是信息安全市场的一个分类，在当今云计算时代，越来越多的云服务提供商将采用身份管理及访问控制技术来应对安全挑战，特别是针对企业或个人的SaaS应用服务，双因素认证技术广泛的使用（比如动态密码令牌、短信验证码等）是最大的驱动力。双因素认证技术已经出现在大型的SaaS应用平台，如Gmail、Salesforce.com以及亚马逊网络服务等（AWS）。

随着迁入云计算数据的敏感性和重要性日益增加，加密技术的应用在云计算环境中的应用将会更广泛，尤其是在公有云环境。2013年IDC全球云安全调研结果显示，企业在采用云服务的时候，加密是首选的安全技术。除了云服务提供商实施加密技术来保护自己的环境，IDC发现云计算密钥管理生态系统是一个新兴的热点，随着成熟供应商产品和服务的不断涌现，在云计算中存储敏感数据一定会而变得更易于实施。

SDN是云安全技术的福音同时也是市场抑制因素

软件定义的网络（Software Defined Networking）将可能分散很多网络和IT基础设施的市场以及架构。SDN的核心技术OpenFlow通过将网络设备控制面与数据面分离开来，从而实现了网络流量的灵活控制，为核心网络及应用的创新提供了良好的平台。SDN控制器有一个网络的全球视图，这种全面的视图和网络边缘的网络智能技术结合在一起将为这个控制器监视整个系统和执行安全政策提供新的机会。

SDN在安全领域的应用可以说的云安全技术的福音，也是实际改善云安全的一个机会。安全功能集成到软件定义的网络产品及架构中，将提供和独立的安全设备和安全软件产品相同的功能。随着SDN的成熟和发展，供应商将安全功能服务集成到虚拟化的网络服务堆栈，未来企业环境中独立的安全软件或安全设备的需求可能将降低，这种方式将打破传统的安全部署和管理。

Security as a Service 安全即服务

Security as a service 其实就是安全云的概念，它是将云计算技术和业务模式应用于信息安全领域，实现安全即服务的一种技术和业务模式，使得用户不需要自身对安全设施进行维护管理以及最小化服务成本的情况下获取便捷、按需、可伸缩的信息安全防护服务。安全云不是产品也不是解决方案，是基于云计算的一种互联网安全防御理念，其领域覆盖DDoS防护、病毒恶意代码检测、网络流量过滤、漏洞扫描、Web等特定应用的安全检测，异常流量检测等。

安全云服务在欧美发达国家应用的非常成熟，尤其是针对中小企业。然而在中国，由于管理体系导致企业连接公有云的主动性不高，出于对自身信息可控的考虑，更容易接受私有云的方式。随着用户对安全服务的认知度越来越高，以及当前信息安全专业人才的短缺，将会有越来越多的用户采用安全云服务来更准确的地把握全网安全动态。

大数据安全分析

当今已经进入大数据时代，2013年可以说是大数据应用的元年，很多企业已经应用了商业化或开源的大数据技术来支撑业务系统，大数据的价值越来越高。IDC将大数据定义为：满足4V (Variety, Velocity, Volume, Value), 即种类多、流量大、容量大、价值高指标的数据称为大数据。其定位是，通过高速捕捉、发现或分析，从大容量数据中获取价值的一种新的技术架构。IDC预计到2017年中国大数据市场将达到8.5亿美元的市场规模，复合增长率达到39%。

在信息安全领域，传统的静态防御手段已经不能应对新型的安全威胁，而大数据分析作为一个强有力的新武器来应对它们。 基于大数据的安全分析技术，通过搜集来自多种数据源的信息安全数据，深入分析挖掘有价值的信息，对未知安全威胁做到提前响应，降低风险，实现最佳的安全防护，基于大数据的智能安全分析必然将是安全领域的发展趋势。

在这个领域，IDC预计主要的安全厂商将会通过并购来增强其自身的市场竞争力，先前的例子比如2014年初FireEye收购Mandiant后进军STAP（Specialized Threat Analysis and Protection）市场，Cisco对Source的收购以及BlueCoat收购Solera Networks和Norman Shark公司。

Threat Intelligence 威胁情报成为新兴市场

随着以APT为典型代表的新型威胁和攻击的不断增长，企业和组织在防范外部的攻击过程中越发需要依靠充分、有效的威胁情报做为支撑，以帮助其更好的应对这些新型威胁。针对传统的威胁，我们采用的防御和检测机制基本上是以特征检测为主，而新型威胁更多地利用0day进行攻击，这意味着防守方可能无法提前获知特征信息，从而无法发挥现有检测机制的作用。即便有些新型威胁利用的不是0day，而是利用更老的漏洞信息，但是由于防守方的特征检测库过于庞大，且没有针对性，也会因受困于性能和有效性而频频漏报。

新型攻击的特点也决定了现有的检测机制恐难以凑效。这类攻击的特点包括：潜伏的时候多采用低慢频度的攻击，难以察觉；发起实质性攻击的过程十分快（通常就几分钟，不超过几个小时），并且攻击目标的指向性特别明确，并且同样的攻击过程几乎以后再也不会重复。因此作为防守方，需要改变策略，其中一种方式就是依靠来自外部的安全威胁情报，威胁情报分析市场应运而生，并蓬勃发展。

对于试图部署和管理安全控制来阻止高级攻击的企业安全团队而言，威胁情报可以让他们事半功倍。添加威胁情报到现有的信息安全计划可以加强威胁评估，并提供更多的关键数据来显示哪些安全控制可以部署在企业环境中以阻止最新的攻击。威胁情报的一大卖点是企业可以利用这些信息在攻击启动之前就抵御攻击。通过监测威胁情报中是否存在针对特定软件、系统或行业的攻击，企业可以确定其是否在使用易受攻击的软件或系统，然后在攻击发生前部署缓解措施。

那么什么是威胁情报？我们经常可以从CERT、安全服务厂商、安全厂商、政府机构和安全组织那里看到安全预警通告、漏洞通告、威胁通告等，这些都属于典型的威胁情报。而随着新型威胁的不断增长，也出现了新的威胁情报，例如僵尸网络地址情报、0day漏洞信息、恶意URL地址情报，等。这些情报对于防守方进行防御十分有帮助，但是却不是靠单一

的防守方自身能够获取和维护的。因此，现在出现了安全威胁情报市场，有专门的安全企业、安全服务公司和组织建立一套安全威胁情报分析系统，并将这些情报以订阅或购买的方式销售给企业用户。现在的情报分析市场还有一个很重要的特点，就是给客户提供的情报的特定性越来越强。情报提供者会根据企业的网络及应用的环境信息，提供给他们特定的威胁情报，而非简单的通用情报，这其实可以看作是安全服务的另一种形式，即安全咨询服务。还有一种方法是加入信息共享和分析中心，是指大家分享特定行业的威胁数据，然后整合到本地分析和工具中。

针对这个新兴的市场，IDC给出了明确的定义Threat Intelligence Security Service （TISS），即威胁情报安全服务。TISS市场有几个方面组成：

· 数据供给 / 发布 – 企业用户向情报提供商订阅或购买威胁情报数据，将标准化的威胁情报（XML格式）整合到信息安全计划中。

· 安全咨询服务 – 根据企业用户特定的应用环境提供风险评估以及安全咨询

· 托管安全服务 （MSS） – 将企业用户的网络纳入监测的范围，以获得该用户的特定安全情报信息，通过高级的分析手段报信息

IDC针对TISS市场研究报告显示，市场规模会从2014年的9亿美元增长到2018年的14亿美元，复合增长率达到12.4%。

为了阻止老练的攻击者，企业信息安全计划需要有足够的灵活性，并引进新方法来提高决策过程。添加威胁情报到信息安全计划，无论是通过内部部署还是从服务供应商获取，都可以帮助企业优化安全措施，并专注于阻止攻击的领域。随着威胁变得越来越复杂以及针对性越来越强，企业应该抓住一切可以利用的机会来更多的了解用来对付它们的技术，并运用这些知识来建立一个更有效的安全计划。

基于大数据安全分析的新一代安全运营中心

在信息安全领域中，大数据分析对安全运营中心（SOC）及安全信息与事件分析系统（SIEM）的影响最为深远，这也是与它们先天性的大数据分析特质密切相关。SOC　安全运营中心是以资产为核心，以安全事件管理为流程，建立一套实时的资产风险模型，协助安全管理员进行事件分析、风险评估、预警管理和应急响应处理的集中安全管理平台。SIEM系统是安全运营中心的核心组件，一般都具有安全事件及日志的采集、存储、分析等功能，这与大数据分析的流程是完全相同的，因此SIEM具有天然的大数据分析技术的特质。企业客户进行大数据安全分析的时候，首选平台应该是日志管理及SIEM等系统，可以说在安全分析领域中，SIEM扮演非常重要的角色。

安全运营中心的一个重要发展趋势就是采集的安全数据种类越来越多，不仅包括传统的资产信息、事件信息还包括了漏洞、性能、流量、配置管理、业务等信息，同时安全数据的产生速度和信息量也将是急速增长。企业客户将更加倾向于采用集中化的构建模式和更加精准的安全分析判断问题的能力以及更加快速的安全响应机制，所以这对安全分析的准确性和分析结果价值度的要求越来越高。这些需求必然促使安全运营中心的技术平台对大数据分析技术的依赖。

基于大数据安全分析技术的安全运营中心需要具备以下的显著特征：

- Velocity 高速率 – 高速率的日志采集能力及事件分析能力
- Variety 多样化 – 多种日志类型，支持半结构化和非结构化数据的采集，具备异构数据间的关联分析能力
- Volume 大容量 – 海量的事件存储能力及数据分析能力
- Valuable 高价值 – 分析判断的结构上有价值的信息，意味着需要有效的数据分析方法和工具
- Visualization 可视化 – 安全分析结构的可视化能力

不论未来安全运营中心的技术如何发展，如何与大数据分析技术结合，帮助企业用户解决安全问题以及与用户业务的融合的趋势依然不变。大数据分析技术是一种工具，并不是能够解决所有问题，这要求开发者、服务提供商以及最终用户不断的探索，同时在安全领域，专业安全数据分析师的短缺是现实，未来期待更多的安全分析专业人才的涌现。

IDC
Analyze the Future

企业级移动安全

根据IDC全球企业级移动安全市场报告显示，2013年市场规模达到12亿美元，同比增长32%。企业级移动安全市场将保持迅猛增长，预计到2018年其市场规模将达到28亿美元，未来五年的复合增长率为19%。

中国企业级移动安全市场总体上还处于起步阶段，部分行业客户是第一步先部署移动应用，然后在移动平台的基础上再实现安全保护，也有部分行业客户尝试同时部署应用和安全。总之当前大多数用户还处于观望和简单尝试阶段，预计未来2?3年是移动安全的高速发展阶段。

企业级移动安全产品分类

根据IDC全球在 2014年企业级移动平台调研结果显示，安全及合规是企业客户在建设移动应用项目中最为关注的要素，如果没有完善的安全保障措施，移动应用难以大规模的推广部署，IDC 将企业级移动安全软件市场划分为以下几个方面：

· 移动威胁管理Mobile Threat Management（MTM），包括针对移动设备的防恶意软件（包含防病毒和防间谍软件）、防垃圾信息、入侵防护以及防火墙。

· 移动信息防护与控制Mobile Information Protection and Control（MIPC），MIPC 提供数据保护解决方案，包括针对移动设备的文件、磁盘、应用程序加密以及非加密技术的数据防泄漏技术。此外还包括虚拟数据分割，hypervisor等。

· 移动网关访问及防护Mobile Gateway Access and Protection（MGAP），MGAP 在网关层提供设备控制以及策略执行，包括移动VPN 客户端，网络访问控制等。

· 移动安全脆弱性管理Mobile Security and Vulnerability Management （MSVM），此类产品提供移动终端设备数据擦除、锁定、密码管理、安全策略以及合规管理。

· 移动身份认证及访问管理Mobile Identity and Access Management （MIAM），MIAM 在移动设备会话过程中提供身份认证及授权技术（比如PKI 证书、SSL 证书以及密码管理），支持移动设备网络访问以及单点登录。

企业级移动安全是个很广泛的话题，这个领域中有不同类型的厂商，IDC将这些厂商分为以下几个类别：

· 提供移动终端解决方案（包括移动设备管理，身份认证）的传统安全厂商，比如EMC/RSA、Symantec、McAfee、Trend Micro、Kaspersky、IBM等。

· 支持移动网关接入的网络安全厂商，比如Check Point、Cisco、Juniper、华为等。

· 提供移动安全组件（通常是企业级移动管理的一部分）的移动厂商，比如AirWatch（被VMware收购）、GoodTechnology、MobileIron、BlackBerry等。

· 纯粹的移动安全厂商，Mobile Active Defense,、Mocana,、NetMotion Wireless 、Zscaler

· 企业级软件厂商，CA Technologies、Citrix、Dell、LANDesk、Microsoft以及 SAP

企业级移动安全发展趋势

根据IDC企业级移动安全研究结果显示，当前大部分的移动安全支出是在移动设备管理（MDM），身份管理和访问控制以及数据保护方面。预计未来的投资方面将会转向到保护企业应用和内容，而不是单一的设备保护。

· IT消费化

伴随随IT消费化在企业应用中的进一步渗透，企业员工携带移动设备办公BYOD趋势早已推波助澜，移动以独特的创新方式全方位冲击着企业IT的变革，不可置疑，除满足企业业务需求之外，对于解决突如其来的企业IT安全问题也诸将给企业带来一定的挑战。对于企业IT部门来说BYOD不仅仅带来移动设备管理难题，更大的挑战在于如何针对BYOD制定安全策略，实现企业网络的机密性和完整性的需求将更加迫切。

· 移动恶意程序

移动恶意程序增长的速度惊人，大部分的移动恶意软件的设计目的是直接从智能手机窃取数据。随着越来越多的企业用户的安全意识增强，设置了例如只允许下载授权的应用策略，有效的降低了风险。但是网络犯罪者正在寻找一种新型的攻击，典型的一种方式是在应用程序以外创建一个恶意广告网络，当应用软件连接到恶意网络时，恶意软件将会推送到移动设备从而有效的避开应用安全防护。

· 应用程序保护

在精细的管理和安全的企业应用的需求驱动下，移动安全厂商纷纷提供了相关的解决方案，可以为单个应用程序制定安全策略，有时被称之为“应用程序包”。 企业可以对某一个应用程序制定特定的安全策略，如申请密码保护、VPN的隧道连接、高级的加密技术等。

· 移动数据容器化

企业用户需要确保其移动数据是受保护的，许多用户通过加密、数据防泄露、安全访问控制等手段来扩展数据防护的能力，这些操作都是通过运行在一个受保护的容器中来隔离应用和数据。由于数据是加密的，必须经过认证授权才能访问。企业只需要将安全策略下发到容器中而不是对整个设备进行控制，这种解决方案同时也带来良好的用户体验。

· 移动安全和企业移动平台深度融合

移动开发部署平台、企业移动管理平台和移动安全在当前移动平台的部署体系中多为分散独立的模块，彼此之间缺少融合集成，未来这三大模块将把部分特性融合，比如安全特性，将会在多个解决方案中贯通，另外在移动应用开发、发布、管理，用户身份认证管理服务等方面均需三类产品的融合支撑。各类厂商之间将通过并购整合或统一行业标准来实现产品的互通。

移动信息化已是大势所趋，企业移动平台的标准建立需要一个开放的战略思维考虑，企业用户需要具备长远的、前瞻性的眼光建立有效的移动战略部署规划，通过融合移动安全和移动业务平台有效的提高ROI投资回报率、业务运营效率以及核心竞争实力。

IDC中国（北京）：中国北京市东城区北三环东路36号环球贸易中心D座1202-1206室
邮编：100013
+86.10.5889.1666
Twitter: @IDC
idc-insights-community.com
www.idc.com