IDC
Analyze the Future

下一代防火墙

主动防御安全体系之重甲

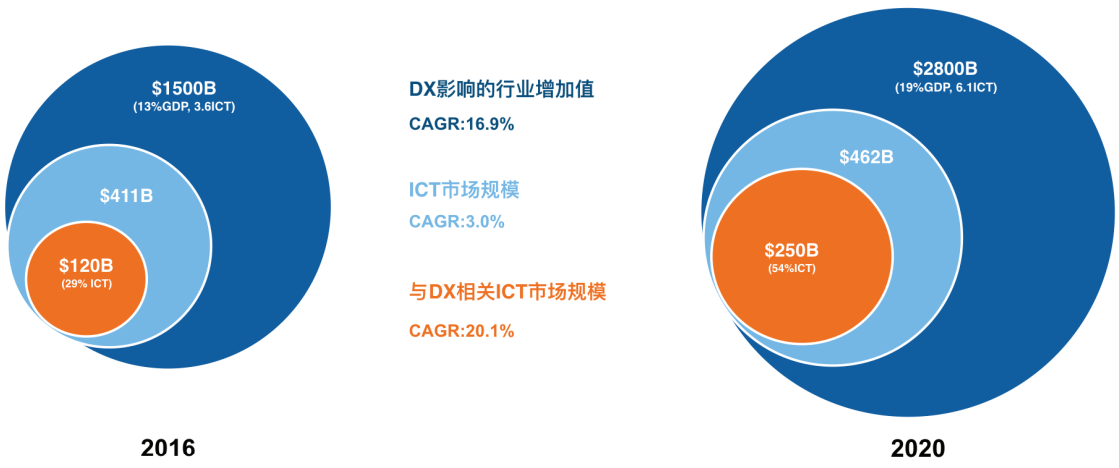
IDC白皮书

赞助者：360企业安全集团

IDC观点

全球企业的数字化转型（以下简称“DX”）浪潮正在如火如荼的进行着，中国政府也已经将DX上升为国家战略，2016年10月9日习主席在中共中央政治局第三十六次集体学习中强调“加快传统产业数字化、智能化，做大做强数字经济，拓展经济发展新空间”。如图1所示，2016年中国与DX相关的ICT市场规模为US$120B，占ICT市场规模的29%，预计到2020年，与DX相关的ICT市场规模将达到US$250B，在ICT市场规模的占比达到54%。虽然DX在ICT市场中的比重快速增加，但这并不是DX的最大价值，DX的最大价值在于能够与行业深度融合激发相关行业市场规模的骤增，IDC统计显示2016年DX与行业深度融合使得相关行业市场规模达到US$1500B，而到2020年预计将高速增长至US$2800B。由此可以看到，中国由于DX所带来的以云计算、大数据、社交商业与移动技术为代表的第三平台技术将广泛应用到各个行业。

图1 中国行业数字化转型的增量商机



来源：IDC，2017

DX正驱动大量数字化原生企业出现，IDC预测：“到 2018 年，拥有DX战略的企业将把外部数据源扩大至少3 到5 倍”。因此，企业数据、支撑业务的IT系统都成为保障企业正常运行的重要资产，IT安全的重要性前所未有的受到全球各国政府和企业级用户关注，这也是中国政府在近几年密集发布政策法规，提升网络安全战略的重要原因。

IDC认为，由于DX使得全球企业IT资产价值大幅提升导致其所面临的网络安全风险与日俱增。但由于DX所带来的IT体系架构的巨大变化，使得传统IT安全产品无法部署，而伴随攻防的不断博弈，传统IT防御体系对攻击的抵御能力也在快速退化。在这样的背景下，以下一代安全技术为核心的IT安全防御体系架构出现了，较传统IT安全防御体系而言，发生了巨大变革。传统安全防御体系存在产品技术先进性不足、信息孤岛多、体系组成部件协同工作能力不足等缺点。第三平台技术使得下一代安全防御体系不得不面临多平台部署、防御智能化、体系组建协同化、敏锐洞察未知恶意软件攻击等复杂而高级的需求。

下一代安全防御体系将是变被动为主动的积极的IT安全防御体系，作为其重要组件之一——下一代防火墙（NGFW）将发挥极其重要的边界防护作用，其智能化、可视化、虚拟化、协同的特性将大幅提高IT边界的安全性。

2016年，中国IT安全市场在政策与DX需求的强力驱动下，保持了25.1%的高速增长，市场规模达到US$3.4B，而其中，具备NGFW特性的边界安全网关市场规模已经达到US$924.7M。

目录

图目录

应用广泛-下一代防火墙在全球IT系统边界防御中不可或缺

IDC认为，云计算、大数据、社交商业与移动技术为代表的第三平台技术是全球企业DX过程中不可或缺的，在此基础上，下一代信息安全、虚拟/增强现实、物联网、认知计算、机器人与3D打印成为第三平台上的6大创新加速器。

随着技术的逐步成熟，下一代防火墙技术将逐步取代传统企业级防火墙、UTM技术，成为边界安全防御的重要技术手段。分析传统企业级防火墙及UTM市场可以充分展现下一代防火墙的市场空间及未来发展趋势。

图2 第三平台技术

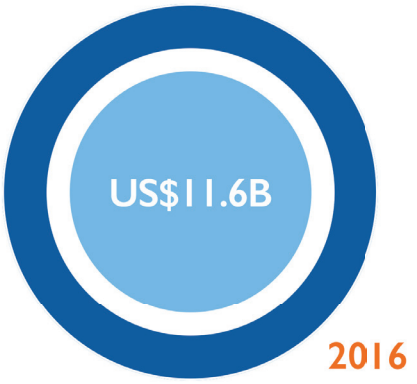
来源：IDC，2017

下一代安全之所以成为第三平台6大加速器之一，正是因为企业在DX过程中，IT资产成为企业成功转型与快速发展的核心，其重要程度不言而喻。IT资产安全所面临的巨大安全风险需要由更为先进的安全技术来保障，而企业所依赖的移动、大数据、云计算、社交相关技术使得企业IT系统较传统的IT系统发生了革新性的变化，使得传统安全防御体系逐渐失效。如何为企业DX保驾护航呢？下一代安全技术应运而生，下一代安全技术相关的领域包括云安全、IoT安全、数据安全、安全服务等，下一代防火墙技术作为新IT系统边界防御的重要技术，起到“承上启下”的作用，不仅“火眼金睛”的识别各类已知恶意代码的攻击，更能“融会贯通”的与IT安全防御系统协同工作，快速发现隐匿极深的未知恶意代码的入侵。下一代防火墙技术将逐渐应用于边界安全网关产品中，成为市场的主流，2016年全球及中国的防火墙、UTM情况如下:

全球防火墙、UTM市场规模

由于网络安全事件频发，IT安全已经受到全球企业级用户的普遍重视，2016年，从单品市场规模看，全球防火墙、UTM市场保持较好的增长态势，市场规模达到US$11.6B，较2015年同期增长9.7%。

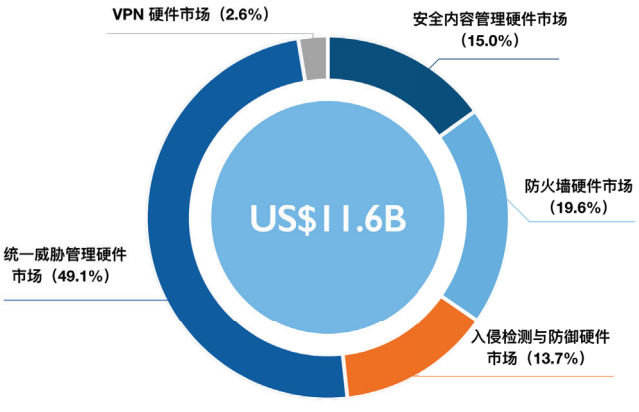
图3 2016年全球IT安全硬件市场规模概况



总计 =US$11.6B
来源：IDC，2017

2016年，全球IT安全硬件市场中，防火墙和UTM占比分别达到了19.6%和49.1%。防火墙、UTM市场总体收入达到了US$8.0B。防火墙、UTM在全球IT安全硬件市场中的占比仍然保持绝对领先的地位。全球DX过程中下一代安全网关仍然是IT安全建设过程中边界安全不可或缺的重要安全产品。

图4全球IT安全硬件市场各子市场份额，2016

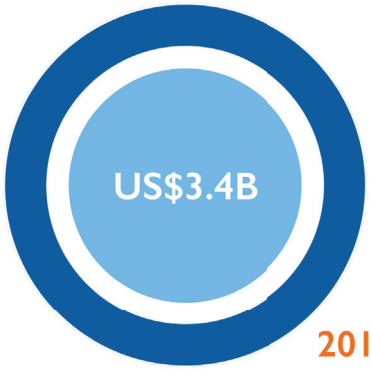


来源：IDC，2017

中国防火墙、UTM市场发展情况

2016年，中国IT安全硬件、软件、服务总市场规模达到US$3.4B，同比2015年，市场增长率仍然高达25.1%。在中国，IT安全建设落后于全球平均水平，在DX趋势的驱使下，市场的增速大幅高于全球平均增速是必然的结果。

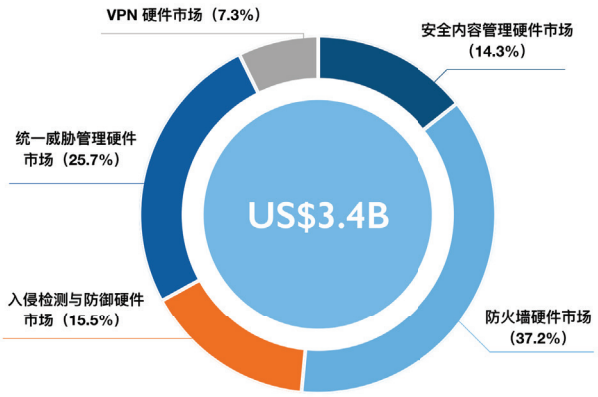
图5 中国IT安全硬件、软件、服务市场2016年厂商市场规模概况



来源：IDC，2017

2016年中国IT安全硬件市场中，防火墙、UTM占比分别达到了37.2%和25.7%，防火墙和UTM市场总体收入达到US$1166.6M。在IT安全硬件性能提升的驱动下，防火墙、UTM性能同时得到大幅提升，这也使得下一代安全网关硬件的部署环境更为广泛，稳定性增强，性价比大幅提升。

图6 中国IT安全硬件市场各子市场份额，2016



来源：IDC China，2017年

【注】以下是IDC对传统防火墙及UTM的定义：

防火墙安全硬件（FireWall）：最主要的功能是网络数据流的过滤，VPN是其中一个可选的模块。在防火墙安全硬件中，VPN并不会集成在所有的该类产品中。防火墙安全硬件也可以提供一些其它的功能，比如防病毒、入侵检测、Web流过滤以及其他的一些安全信息服务。在当前的产品中，这些单独的模块是不能被分离的。

统一威胁管理硬件产品（UTM）：将一些常用的安全功能集成在一个设备中。这类产品和其他产品不同的是：它们必须包括网络防火墙、网络入侵检测与防护、网关防病毒功能。所有这些功能不一定要打开，但是这些功能必须集成在一个硬件中。除了这些强制性功能外，统一威胁管理硬件还应该包括其他的一些安全功能。

机遇难得-下一代防火墙助力企业数字化转型

中国政府密集发布网络安全相关政策法规，表明了政府在加强网络空间安全方面投入的极大决心，同时也看到中国政府在雷厉风行的依法监督企业级用户加强IT安全建设。

2016年至2017年中国政府所发布的重要政策法规如图7所示。

- 2016年11月7日，中华人民共和国全国人民代表大会高票通过《中华人民共和国网络安全法》（以下简称《网络安全法》），2017年6月1日正式生效；
- 2016年12月27日经中央网络安全和信息化领导小组批准，国家互联网信息办公室发布《国家网络空间安全战略》；
- 2017年5月2日国家互联网信息办公室发布《网络产品和服务安全审查办法（试行）》

图7 2016-2017中国政府发布重要政策法规

来源：IDC，2017

企业级用户的管理层将必须正视自身IT系统的网络安全问题，责无旁贷的推进IT安全建设。另外，当前全球网络安全形势严峻，2017 年5 月12 日，名为WannaCry的勒索软件病毒在全球大范围蔓延，100 多个国家和地区的数十万台电脑遭该勒索病毒感染，我国部分Windows 系列操作系统用户也难逃厄运，部分业务系统甚至无法正常工作。这些耳熟能详的安全事件反复印证了企业IT系统所面临的巨大安全风险。因此，数字化原生企业、政府、运营商、金融、教育、能源等重要行业首当其冲，大力投入资金进行IT安全防御系统的建设，而边界安全成为其中的重要建设部分。

中国当前的IT环境是新旧混合的状况，旧的IT系统边界为提升防御效果，需要硬件形态下一代防火墙。DX所带来的云环境基础设施边界同样需要硬件形态的下一代防火墙，但在虚拟化环境下的边界则需要软件形态的下一代防火墙。

而在对防火墙安全性的要求上，用户对其应用防护能力的要求越来越高，从《2016年CNVD 漏洞数据统计简报》中看到，2016年中国的安全漏洞60%来自于应用程序漏洞，对应用的边界安全防护尤为重要。这使得对流经下一代防火墙的流量进行深度分析以抵御对复杂应用系统的恶意攻击成为各个行业共同的需求。

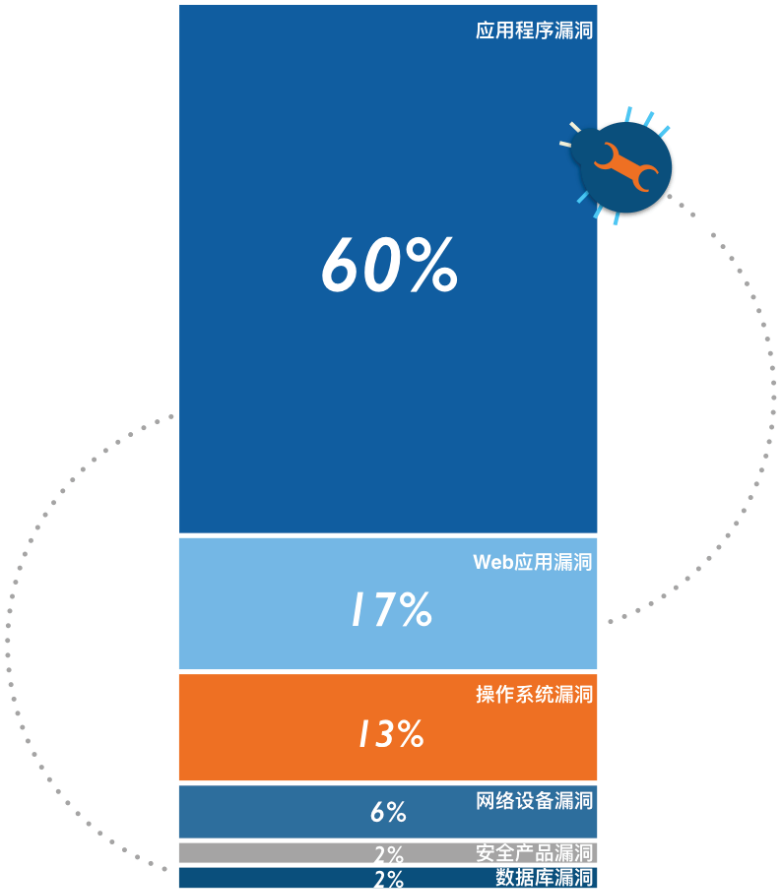


图8 复杂应用蕴藏漏洞

来源：2016年CNVD漏洞数据简报

当然，在不同行业对于边界安全防护的需求各有差异，以下着重从数字化原生企业、政府、能源、金融、教育五个行业简述其边界安全需求。

数字化原生企业

中国已经进入到数字化的时代，我们看到90后正在成为消费的主体，他们享用的服务的典型特征是数字化、个性化、创新化、快速化，因此，90后已经成为引领消费的数字化原生代。中国未来数字化原生代人群将达到4亿人，已经超过美国总人口的数量，由此不难预测，未来中国的企业管理者越来越多的将采用数字化技术。因此，企业进行DX以迎合消费主体人群的消费习惯已经成为一种必然，未来的企业都将成为数字化原生企业。

对于数字化原生企业，确保核心数据安全、确保业务稳定运行是极其重要的工作，因此，加强IT边界防护，加强数据安全防护是IT安全建设的重中之重，而下一代防火墙是性价比最高的IT边界防护产品。通过下一代防火墙，企业可以有效抵御或消减来自网络层的DDoS攻击，精确隔离应用层的僵尸程序、木马、蠕虫对IT系统的入侵，更可以与本地沙箱、云沙箱协同工作，运用威胁情报智能化的识别未知的各类恶意软件入侵，确保企业业务系统的稳定运行。

政府行业

在第三平台技术、智慧城市、互联网＋、行政审批改革、三证合一等的驱动下，中国政府行业信息化市场保持了高速发展。电子政务在横向上从单一机构应用延伸到跨部门的整合协同，在纵向上沿着省、市、县三级联动的方向发展，顶层设计、宏观平台型项目得到普及推广。随着智慧城市的建设要求的不断提高，大量的创新型政府行业IT 解决方案将不断涌现，以适应当前改革的需要。

政府行业信息化领域，直接关系到国计民生，信息安全的重要性更加突出。随着网络安全形势的日益严峻，中国政府将网络安全上升到国家战略高度，2017年6月1日《网络安全法》正式实施，这使得政府行业的所有IT建设过程中都将投入大量资金用于网络安全建设。国家各相关部委出台了一系列标准并展开审查工作，确保IT系统具备健全的网络安全防御体系，最大程度降低系统风险。

从目前趋势看，勒索软件、高级可持续威胁（APT）日益盛行，在政府行业IT环境中，提升网络边界防护能力、屏蔽恶意代码的入侵是政府行业用户保障数据安全，防止机密信息外泄的的重中之重。

能源行业

能源行业的业务系统属于我国关键信息基础设施之一，在《网络安全法》对关键信息基础设施有如下描述“　第三十一条　国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。”

在能源行业中，电力行业的IT安全建设处于领先的地位，从2000年起，电力行业针对电力生产运行中发现的一些实际问题，深入开展了电力监控系统安全防护工作，制定并印发了《电力监控系统安全防护规定》等相关法规和规范性文件，2014年电力行业又发布《电力行业网络与信息安全管理办法（国能安全[2014]317号）》和《电力行业信息安全等级保护管理办法（国能安全[2014]318号）》两个信息安全管理办法文件。电力行业各单位按照“安全分区、网络专用、横向隔离、纵向认证”的安全防护总体策略，持续开展工作，基本建成了覆盖全行业的安全防护体系，有效保障了电力监控系统等关键信息基础设施的安全运行和电力的可靠供应。

但是，在2016年国家能源局发布的《电力企业网络与信息安全专项监管报告》中，提及多家电力企业在“电力监控系统安全防护、信息安全等级保护等方面存在问题”，“互联网出口防护、设备远程维护、工控设备漏洞整改等方面较为薄弱”。电力系统边界安全问题突显。

国家能源局副局长王晓林在接受中电新闻网记者采访时提及：“尽管我们在网络安全工作方面取得了一定的成效，但也应看到，由于网络安全发展水平不平衡、网络安全基础工作开展不到位、部分核心技术和关键设备受制于人等原因，当前我国电力行业网络安全工作依然存在较多的不足和薄弱环节，突出体现在部分单位对网络安全工作的重要性认识不足、网络安全责任未切实落实到位；部分单位网络安全从业人员的专业素养和技能还不能适应和满足自身岗位职责的要求；电力行业网络安全防护体系抵御APT（高级持续性威胁）攻击的能力还需要进一步提升等”。

事实上，石油、石化、煤炭、新能源等行业的IT系统也都面临相同的边界安全、APT攻击的网络安全问题。

当前，边界安全问题与对APT攻击的防御不再是彼此独立的事情，边界安全网关将作为其中的重要环节，协同沙盒等防御与监测体系共同提升能源行业对APT攻击的识别与防御能力。

金融行业

金融行业的业务系统属于我国关键信息基础设施之一，多年来金融行业用户对IT安全建设的重视程度保持着极高的状态，发布多项行业法规，包括：《计算机信息系统安全等级保护基本要求》、《银行业金融机构信息系统风险管理指引》、《商业银行合规风险管理指引》、《证券期货信息安全管理办法》、《保险公司信息系统安全管理指引》等。

在银行业，2016年是中国银行业深化改革之年，中国银行业正在步入一个崭新的金融科技（FinTech）时代，以云计算、大数据、移动互联、区块链和人工智能为代表的新一轮金融科技正在对中国银行业产生前所未有的冲击并将引发巨大的变革。2016年7月，中国银监会就《中国银行业信息科技“十三五”发展规划监管指导意见（征求意见稿）》公开征求意见，意见稿指出总体目标，包括信息科技治理有效性明显提升、信息科技服务能力持续提升、科技成为引领创新的关键引擎、网络和信息安全管控能力显著增强、信息科技风险管理“三道防线”协同水平持续提高。明确提出要求“主动开展架构转型，建立开放、弹性、高效、安全的新一代银行系统。”明确了科技引领金融创新的引擎作用与地位。由此突出网络和信息安全管控能力在银行业发展的重要性。

在保险行业，2016年中国保险行业IT解决方案市场继续保持稳定增长态势。同年，中国保监会公布了《中国保险业发展“十三五”规划纲要》，在“第八章　夯实基础，持续改善保险业发展环境”中提及“加强信息安全基础设施建设，建立完善的信息安全保障体系，提升保险机构信息安全综合防范能力。”

对于互联网金融，互联网金融的兴起正在对传统银行的渠道产生重大变革。中国银监会在银行业“科技十三五规划”中明确提出，鼓励“尝试信息科技公司化运作”，协同创新，跨界合作构建互联网金融生态圈。与此同时，2016年，中国多个部委对互联网金融进行专项整治，推进监管落地，确保互联网金融业务安全稳定的运行。

整体上，金融行业对第三平台技术的需求尤为迫切，数据价值在金融行业将持续放大，甚至成为关乎企业生存的核心资产，而对于数据的保护，不是单一数据加密技术可以解决的，数据安全同样需一套完整的IT安全防御体系架构，由于移动化应用在金融行业的广泛使用，企业边界外延至智能终端，边界网关除了起到对应用的内容识别与防护、数据传输过程的安全性保障、访问者身份的真实性验证等作用外，与各类终端间的协同、与全网IT监测防御系统的协同尤为关键，起到承上启下的作用。

教育行业

教育部早在2014年8月就发布了《教育部关于加强教育行业网络与信息安全工作的指导意见》并取得了一定的效果。随着网络安全事件对教育行业影响加大，2016年10月教育部办公厅成立教育部网络安全和信息化领导小组，旨在贯彻落实中央关于网络安全和信息化工作的战略部署，切实做好新时期的教育系统网络安全和信息化工作，陈宝生部长亲自担任组长。2017年2月，教育部科技司在《教育部科技司2017年工作要点》中明确了“统筹教育信息化，维护行业网络安全”的重点任务。2017年7月教育部办公厅下发了《各地开展学校大检查》的通知，通知要求，各地教育部门和各级各类学校要切实树立“隐患就是事故”的观念，按照“全覆盖、零容忍”的总体要求，结合危险化学品综合治理和电气火灾综合整治工作，深入开展覆盖电气安全、校车安全、校舍安全、网络安全、食品及饮用水安全、传染病防控、危险化学品安全、特种设备安全及校园周边治理等领域的安全隐患全面排查工作。教育行业的IT安全建设进入新阶段。

教育网具备流量大、内容复杂的特点，内外部的边界安全网关可以有效隔离恶意软件在教育网内部的泛滥，而下一代防火墙智能化、可视化、协同特性对于提升边界安全防护效果具有积极的作用。

另外，2015年，教育部办公厅印发《2015年教育信息化工作要点》中提及“完善教育资源云服务体系。提升国家教育资源公共服务平台技术水平和服务能力，建立健全国家平台运行、资源汇聚与服务的政策机制，实现与20个以上省级平台以及若干地区平台、企业平台的互联互通”。面向云环境，虚拟化特性将使得下一代防火墙可以运行在云平台上，在云边界起到安全防护的作用。

价值提升-主动安全防御体系之重甲

下一代防火墙作为主动安全防御体系的重要组成部分，在网络安全防护过程中起到举足轻重的作用。即便移动化应用带来了企业边界外延，下一代防火墙所处位置仍然是企业IT系统的关键防护环节。下一代防火墙带来了以下四方面的安全防御新体验:

智能化

- 智能化在下一代防火墙中表现在多个方面，从产品自身看可以表现在对策略、流量、行为等的自学习能力；从外部看，聪明的借助主动防御体系的智慧提升自身的智能防御效果，例如，通过将可疑文件传送至云沙箱进行验证从而高效检测其安全性；通过订阅威胁情报实时更新针对僵尸程序、木马、蠕虫的指纹库，从而能够有效应对因新型病毒、勒索软件爆发对内部网络所造成的威胁。

可视化

- 可视化在下一代防火墙中可以帮助管理员快速发现、分析网络攻击行为，从基础层面来看，可以识别内部人员在IM、游戏、下载软件等众多应用的使用情况，起到基础的“监控摄像头”功能；从高级功能角度看，可以将内部的各类日志和策略进行关联分析，将攻击行为的过程还原，帮助管理员快速分析问题、定位问题、解决问题。对于大型的企业级用户而言，其Intranet通常会部署数量较多的下一代防火墙，在这样的场景下，可视化特性将成为企业安全管理员最为依赖的功能特性。

虚拟化

- 虚拟化技术在云环境中得到广泛应用。在公有云环境中，东西向流量通常依赖VPC技术，而南北向流量防护则需要依赖于虚拟安全网关。另外，在中国政府的大力推动下，政务云、金融云、教育云等行业云正在被大规模建设，东西流量的隔离与南北流量防护同样需要VPC及虚拟安全网关。为保护云中租户的数字资产安全，作为安全网关，下一代防火墙需具备虚拟化特性，能够以软件形态部署到云环境中，并与云管理中心形成有效的信息互通，达到弹性的、按需索取资源的效果，同时在业务或者环境发生变化的情况下实现无缝迁移，随时保障云中租户的业务安全。另外，在行业云中也有以硬件资源池形态实现虚拟防火墙功能的技术，以安全资源池的方式保障云环境的边界安全。

协同

- 主动安全防御体系重在各个安全组件间的彼此协同。对于处于网络边界位置的下一代防火墙而言，其协同能力更为重要。从2016年10月美国Dy-nDNS 遭到 DDoS 攻击事件到2017年5月发生的Wannacry勒索病毒在全球肆

虐事件看，网络边界安全网关承担着保稳定、防入侵的重要作用，显然完全依赖设备自身是难以达到理想效果的。作为典型的边界安全网关，下一代防火墙必须积极的通过协同机制与主动安全防御体系各个组件交互信息，对内网而言，内网终端、本地沙箱都是能够快速帮助下一代防火墙发现攻击、定位问题、快速响应的利器；对于外部而言，与云沙箱、威胁情报系统协同是有效提升下一代防火墙智能化的重要技术手段。下一代防火墙逐渐变为国防边境的“尖兵”，通过与各种高精尖系统的协同，高效抵御外敌入侵，捍卫祖国边界安全。

图9 主动安全防御之重甲

来源：IDC，2017

前景广阔-下一代防火墙市场保持高速发展趋势

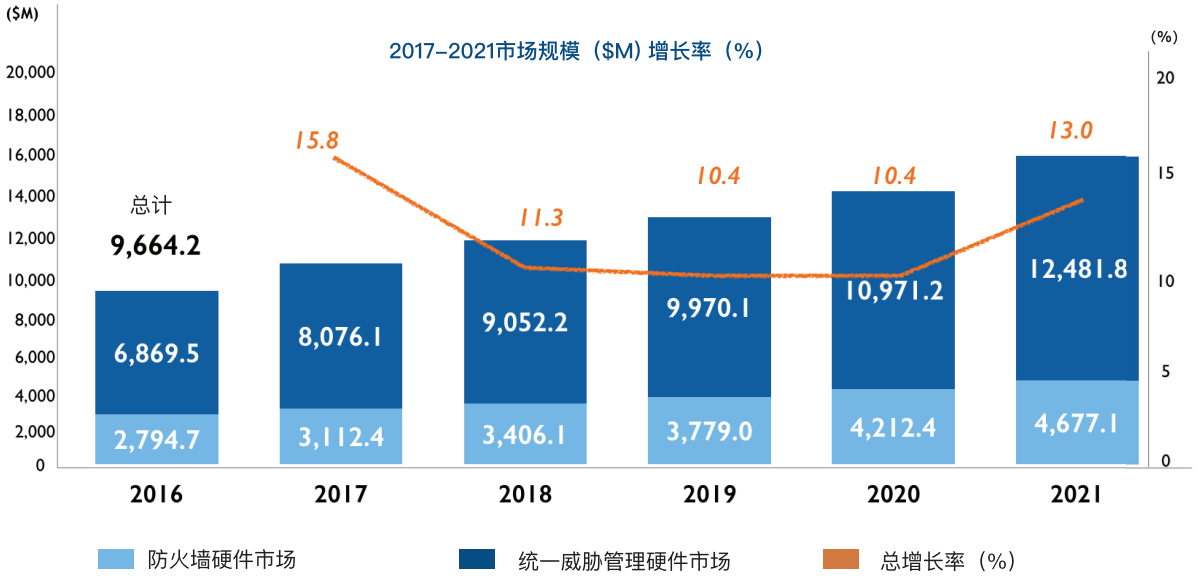
下一代防火墙市场未来展望

IDC公司认为，从全球视角看，传统企业级防火墙、UTM技术将逐渐被下一代防火墙技术替代。因此，分析传统企业级防火墙、UTM的市场情况足以体现未来下一代防火墙的市场空间。

全球防火墙、UTM市场发展情况

在全球安全形势日益严峻的环境下，防火墙、UTM市场的规模将持续保持快速增长，IDC预测到2021年，防火墙、UTM市场规模将达到US$17.2B。2017到2021年，全球防火墙、UTM市场整体复合增长率达到12.2%。

图10 全球防火墙/UTM市场预测



防火墙硬件市场 CACR 10.8%

统一威胁管理硬件（UTM）市场 CAGR12.7%

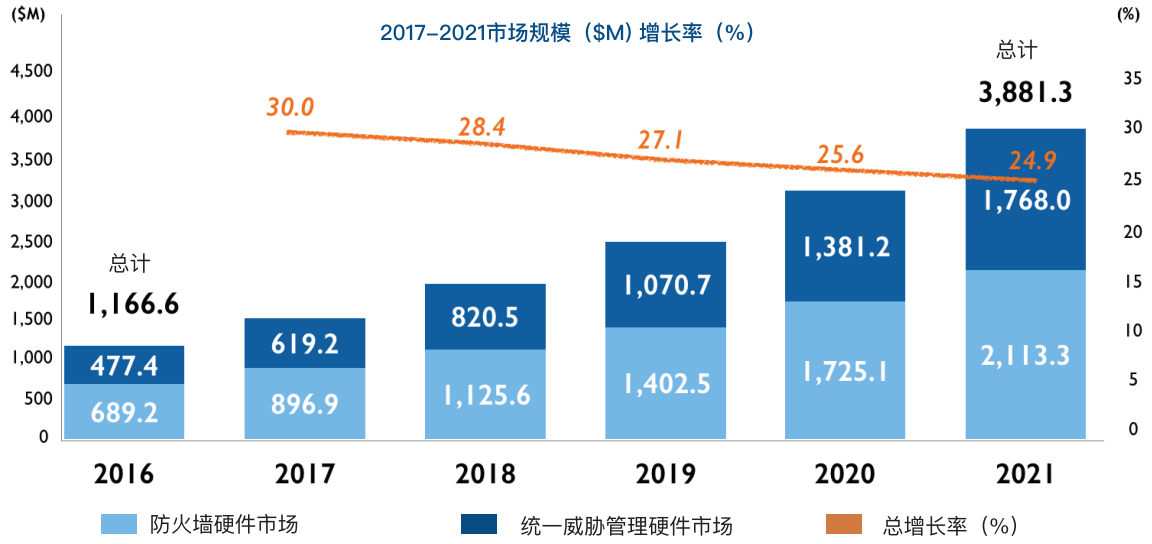
总市场 CAGR 12.2%

来源：IDC，2017

中国防火墙、UTM市场发展情况

中国防火墙、UTM市场的增速将远高于全球同类市场，IDC预测到2021年，防火墙、UTM市场规模将达到US$3.9B。2017到2021年，中国防火墙、UTM市场整体复合增长率将达27.2%。

图11 中国防火墙/UTM市场预测



防火墙硬件市场 CACR 25.1%

统一威胁管理硬件（UTM）市场 CAGR29.9%

总市场 CAGR 27.2%

来源：IDC，2016

360企业安全集团新一代智慧防火墙最佳实践

成功案例分析——IDC调研北京邮电大学校园网及数据中心边界安全防护的情况

客户概述

北京邮电大学是教育部直属、工业和信息化部共建、首批进行“211工程”建设的全国重点大学，是“985优势学科创新平台”项目重点建设高校，是一所以信息科技为特色、工学门类为主体、工管文理协调发展的多科性、研究型大学，是我国信息科技人才的重要培养基地。

随着北京邮电大学校园网规模的快步增长，校园网出口历经数次扩容。目前学校有多路外网连接，包括教育网的接入以及联通、电信、移动等运营商的高带宽互联网接入，承载校区本部3万余师生的网络访问。

北京邮电大学数据中心是学校信息化应用的核心，数据中心包含服务器一百多台、虚拟机七百多个、应用的数量上百个，主要的应用除了基础网络服务外，还包括各个职能部门的业务系统，教学平台、人事系统、财务系统、资产系统、房产系统、办公OA、档案系统、招生系统、就业系统、科研系统、图书馆管理系统和电子资源、学生管理系统。另外，还有托管的科研用的服务器、学生维护的IP-TV、BT下载娱乐类的应用等。

业务需求

北京邮电大学对于边界安全的 需求主要包括校园网和数据中心边界安全需求两部分。

校园网需求

北京邮电大学在快速发展过程中，业务系统大量增加，随着师生PC及联网智能终端数量的快速增长，使得校园网得到在校3万余师生的频繁使用，而在互联网访问过程中难免会有恶意攻击的侵扰。随着网络攻击形势的日益严峻，攻击方法纷繁复杂，过去的安全产品难以有效的起到边界防护效果，因此，校信息中心网络管理员积极寻求更好的技术手段来提升校园网络的边界防护水平，而随着下一代防火墙技术的成熟使得其成为首选。具体需求如下：

- 高校网络与一个小型运营商规模相等同，网络流量和承载的用户规模十分巨大，因此对设备在复杂环境下的组网能力、性能、可靠性要求极高。这是北京邮电大学考虑的首要问题。

- 为了最大程度避免校园网用户遭受攻击，并进一步在校园网内蔓延，在接入互联网后，首先要防止用户访问被植入木马、病毒、勒索软件等包含恶意URL的网站以及钓鱼网站，其次是要对流量中可能隐藏的恶意程序进行高效率的检测和阻断。

- 由于互联网上充斥着良莠不齐的各类信息，因此，要确保学生做到健康、合法的使用互联网，所以，需要对师生的访问内容、网址进行适当的安全管控。

数据中心需求

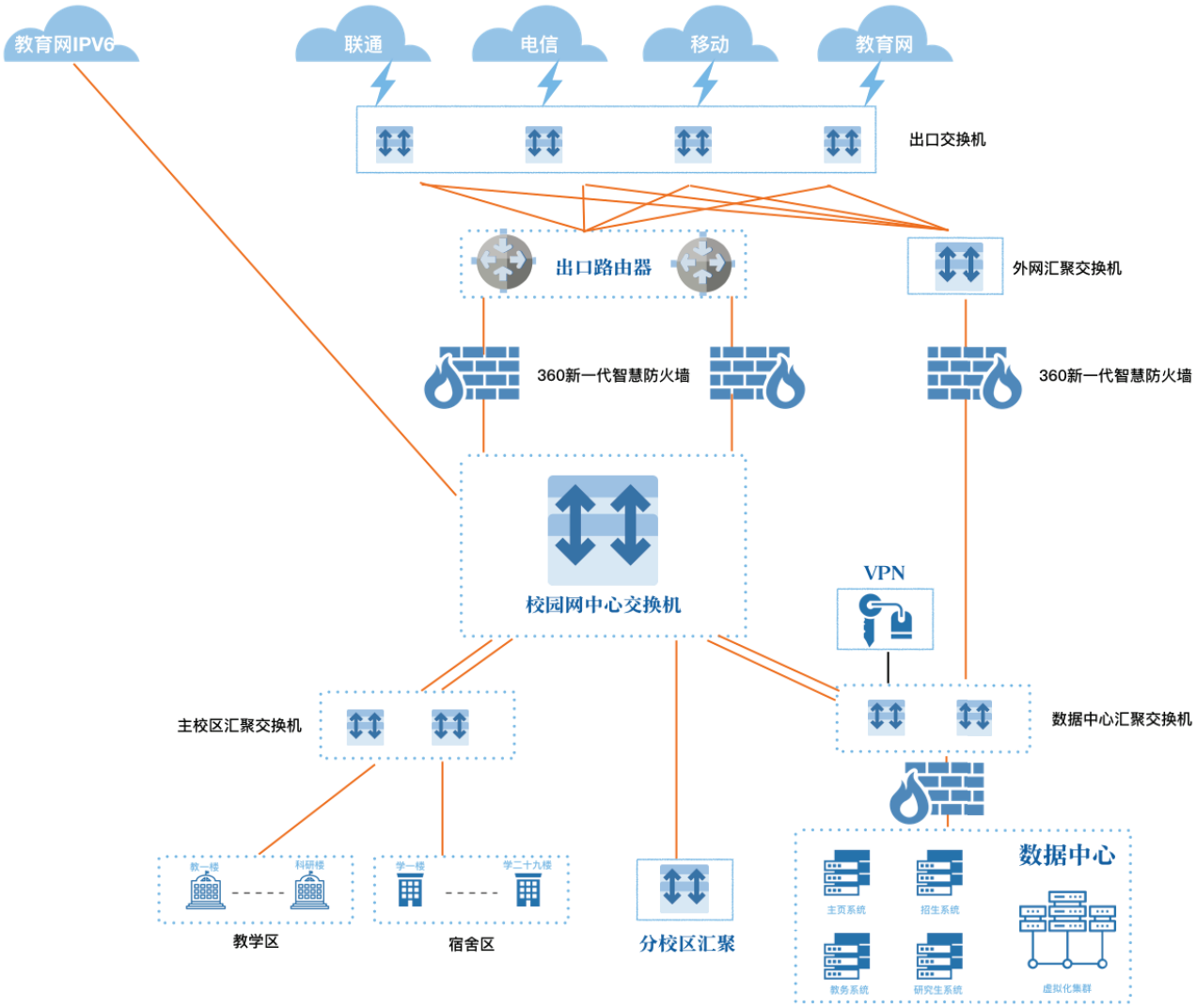
- 数据中心服务器群庞大，其中可能潜藏诸多安全漏洞，而对数百台服务器进行漏洞修补存在着周期长且继发宕机风险的问题。通过边界安全防护产品构筑安全屏障，对已知和突发的漏洞攻击进行准确、及时的防护，是数据中心边界防护的一项主要需求。

- 数据中心由于IT业务的运营而产生的数据是非常重要的IT资产，因此，数据中心服务器必然成为“高价值”的攻击目标。对数据中心进行持续而精准的安全监测与检测，及时发现并解决问题，是信息中心一项刚性需求。过去，由于旧有的传统的IDS设备误报率较高，网络管理员常被“淹没”在海量的日志中，因此，信息中心网络管理员亟待新技术予以支撑。

解决方案

北京邮电大学信息中心网络管理员通过详细的测试，最终选择了使用360企业安全集团所生产的新一代智慧防火墙产品（以下简称“360新一代智慧防火墙”）。通过如下部署，从校园网和数据中心两个部分进行边界安全防护，如图11所示。

图12 北京邮电大学校园网及数据中心网络拓扑



来源：IDC，2017

校园网边界部署新一代智慧防火墙

- 通过HA的方式部署360新一代智慧防火墙，在提供高性能、缜密安全防护的同时，确保网络稳定性。360新一代智慧防火墙所采用第四代SecOS操作系统实现了管理平面、数据平面的独立运行，确保设备在极端条件下依然稳定可靠；

- 通过启用360新一代智慧防火墙的漏洞防护、防间谍软件、反病毒、URL过滤功能，高效拦截常见的间谍软件、病毒、木马的入侵，防止内网用户访问钓鱼网站、恶意URL；

- 360新一代智慧防火墙专属的“天御云”安全服务，可为360新一代智慧防火墙提供云端的协防能力。在360新一代智慧防火墙本地启用病毒云查杀、URL云识别后，将与“天御云”协同防御从而进一步增强边界防护能力；

- 通过URL分类控制、网页内容关键字过滤等功能，对师生访问网络的内容进行控制，确保合法用网。

数据中心边界部署新一代智慧防火墙

- 360新一代智慧防火墙深度集成漏洞防护、间谍软件防护等应用层安全功能，通过单引擎一次性数据处理对穿越数据中心边界的所有流量进行深度威胁检测。启用入侵防御策略后，可对缓冲区溢出、跨站脚本、拒绝服务等3000余种漏洞利用攻击进行防护，同时，基于本地预置的恶意程序特征，通过双向检测恶意程序植入后可能产生的C&C（命令与控制）通信等异常行为，实现对已知的木马、间谍软件进行高效防护。

- 基于威胁情报订阅服务，高确定性的情报IOC（黑域名、黑IP、黑文件MD5）将实时推送至360新一代智慧防火墙，由防火墙对命中的恶意流量进行实时阻断，进一步提升对流行威胁的防护能力。同时，当突发漏洞大规模爆发后，“天御云”自动向360新一代智慧防火墙推送应急处置告警，信息中心管理员仅仅通过一键点击，设备即可自动完成特征库更新及策略加载，确保对最新的入侵行为准确、有效的识别，加快应急响应速度；

- 360新一代智慧防火墙将对服务器外联产生的网络行为数据进行采集，并上报至“天御云”大数据分析引擎，“天御云”一方面通过大数据技术挖掘偏离正常基线的异常行为，另一方面，将行为数据与威胁情报进行对撞，从多个维度检测网内的失陷服务器，最终将检测结果回传至360新一代智慧防火墙并向管理员作出告警。

价值分析

北京邮电大学校园网边界安全防护建设是校信息中心经过几年的长期测试、反复验证后进行的，用户认为“360企业安全集团新一代智慧防火墙在可视化、智能化、协同及稳定性方面表现出色，切实帮助用户发现并解决了网络中的安全问题”。综合来讲，客户认为360企业安全集团的新一代智慧防火墙所带来的价值如下：

降低安全防护的TCO：过去信息中心曾经部署过传统的防火墙、IPS等产品，由于都是串联在网络中成本增加很多，现在通过一个设备替代了以前串联的网关设备，成本大幅降低；

威胁感知能力大幅提升：过去网络发现问题时很难通过串联的安全设备分析问题，网络管理员排查问题难度很大。目前，采购360企业安全集团的新一代智慧防火墙后，能够通过产品的威胁感知能力和可视化特性，快速发现并定位问题；

边界防护能力明显提升：360企业安全集团的新一代智慧防火墙与360“天御云”协同，能够快速防范全球最新流行的网络攻击。受访者认为：“目前现有网络的企业版杀毒软件采用的是360的‘天擎’，而360最大的优势就是可以通过庞大的终端安全用户群积累大量的威胁特征，这些特征通过‘天御云’同步到360新一代智慧防火墙中，能够使其在网络边界快速精准的识别恶意软件的入侵行为”。

关于360 企业安全集团

360企业安全集团业务简介

360企业安全集团是专注于为政府和企业提供新一代网络安全产品和服务的综合型集团公司。集团以“保护大数据时代的安全”为企业使命，以“数据驱动安全”为技术思想，创新建立了新一代协同防御体系，全面涵盖大数据安全分析、边界安全、终端安全、网站安全、移动安全、云安全、无线安全、数据安全、代码安全等全领域安全产品及解决方案，已经为包括中央部委 和大型央企在内的超百万家企业级客户提供了全面有效的安全保护，并赢得了客户的一致好评。

关于360企业安全集团新一代智慧防火墙

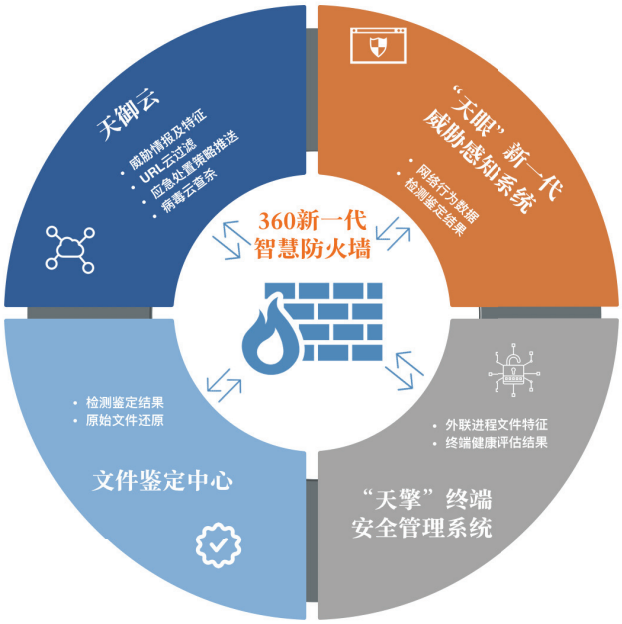
360企业安全集团新一代智慧防火墙（以下简称“360新一代智慧防火墙”）是一款能够全面应对传统网络攻击和高级威胁的创新型下一代防火墙，可广泛运用于政府、运营商、银行、证券、保险、制造、能源、教育等各行业企事业单位的业务网络边界。360新一代智慧防火墙兼具复杂环境组网、深度应用识别、精细化访问控制以及高性能应用层威胁防御能力，并超越性地集成了互联网威胁情报、异常行为分析、安全可视化等新一代安全技术，通过与云端安全服务、终端安全管理系统和本地的安全设施实现智能化的协同联动，帮助用户在网络边界构建安全大数据驱动的动态防御体系，并实现针对全网威胁的智慧防御。

360新一代智慧防火墙同时提供了硬件设备和虚拟化版本两种形态，可广泛适应传统网络边界和虚拟化云环境部署。

协同联动构筑“边界塔防”

随着攻击手段多样化和威胁特征复杂化，凭借防火墙单点、本地的防护能力已无法确保边界的安全。360新一代智慧防火墙具备广泛的协同联动能力，可分别与云端、网络、终端等位置的安全系统进行协同，并基于多系统间的数据共享和策略协同，打破传统安全架构中各种安全设备独立运作、单点防护而形成的信息孤岛，在网络边界构筑更为牢固的“塔防”体系。

图13 360企业安全集团“边界塔防”体系



来源：IDC，2017

云端协同

“天御云”是专为360新一代智慧防火墙提供安全服务的公有云平台，作为“智能外脑”，其为防火墙提供病毒云查杀、恶意URL云过滤、威胁情报推送以及云沙箱检测等高级防护功能的支撑。

依靠360得天独厚的安全大数据优势，“天御云”提供的“黑文件”样本特征超过30亿、日拦截恶意网址过亿次，防火墙在本地无法确定的可疑文件、URL等的特征摘要将送至云端进一步检测。同时，基于“360互联网威胁情报中心”所生产的情报，“天御云”将高确定性的情报IOC实时推送至防火墙，实现对新威胁的快速阻断。

基于云端协防，360新一代智慧防火墙能够获得对抗复杂攻击和新威胁所需的关键知识，从而确保威胁检出率和防御实时性。

本地协同

针对隔离内网用户，360新一代智慧防火墙提供了与用户本地的“文件鉴定中心”、“天眼”等系统的数据共享和联动方案。

“文件鉴定中心”可通过离线导入或单向摆渡的方式将数十亿的恶意文件样本特征、黑域名、黑IP等导入本地，并对防火墙开放调用，以进一步提升防火墙的威胁识别能力。“天眼”新一代威胁感知系统则可将其检测出的高级威胁预警信息实时推送至防火墙，并由防火墙完成处置。

与本地系统间的协同机制，使防火墙可以更加有效的利用外部数据源和计算资源，打破本地特征库检测的局限，进一步提升其在网络边界的威胁检出能力。

终端协同

针对终端系统的病毒防护、桌面管理在用户的安全防护体系中发挥着同等重要的作用，尤其是随着用户网络边界的模糊化、内网的“零信任”化，将安全防护边界下延至终端，实现精细化的网络管控和防御已成为迫切的刚需。

利用“天擎”终端安全管理系统共享的数据，360新一代智慧防火墙可以准确识别网内的终端资产及健康状态，并针对不同风险级别的终端执行动态的访问控制。同时，基于“天擎”的实时监测，终端发起外联行为的进程信息也将被同步至防火墙，防火墙则对此类信息进行“二次查验”实现协防。

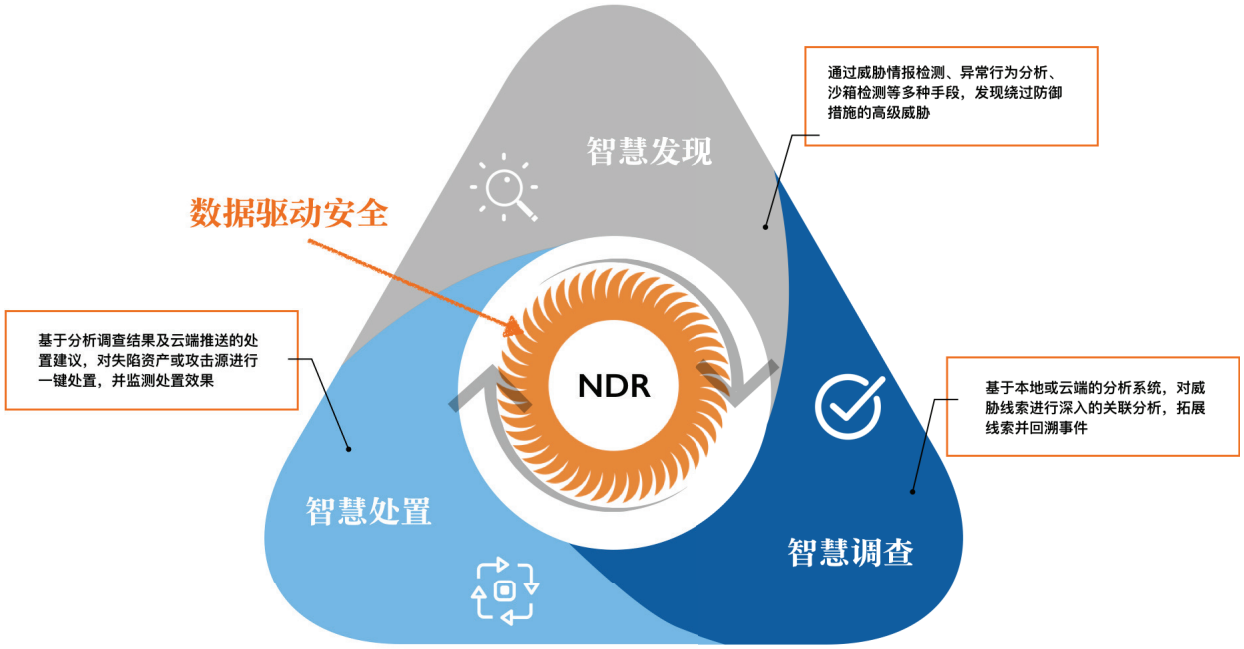
通过打通边界和主机两个原本割裂的防护体系，360新一代智慧防火墙犹如找到了一个“得力助手”，令其在网络边界监测和防护的范围变得更大、管控粒度更细。

基于NDR模型的自适应威胁管理

当前，被动防护无力对抗新型威胁已成为业界共识，边界安全同样需在被动防护的基础上叠加演进至积极防御。企业不但需要在网络边界构筑“塔防”体系，同时更应加强检测和响应能力的构建。

360新一代智慧防火墙基于NDR模型构建了自适应的边界威胁管理体系，针对可能绕过防护措施的高级威胁，实现从及时发现、到高效分析、再到快速处置的管理闭环。NDR（Network-based Detection and Response）是指通过对网络流量产生的数据进行多手段检测和关联分析，主动感知传统防护手段无法发现的高级威胁，进而执行高效的分析和回溯，并智能的协助用户完成处置。

图14 360企业安全集团NDR模型



来源：IDC，2017

智慧发现 - 及时预警高级威胁

基于精准的应用、用户和内容识别能力，360新一代智慧防火墙可在网络流量中提取出50余类行为数据，例如应用操作、URL访问、DNS解析、文件收发等，通过“天御云”、“天眼”等系统对这些数据执行威胁情报检测和异常行为分析，并将检测结果反馈至防火墙，再由防火墙对网内的失陷主机、风险主机和异常行为发出预警，实现对高级威胁的感知。

相较传统基于静态特征的防护和检测手段，由威胁情报驱动并充分利用大数据分析的威胁检测技术，通过在海量、多维的安全数据中寻找规律、建立关联、发现异常并作出预警，实现了人类脑力和能力极限的超越，帮助用户“见所未见”，对潜伏和高隐蔽性威胁作出及时洞察。

智慧调查 - 高效分析威胁事件

360新一代智慧防火墙提供了配套的威胁感知和分析平台，管理者可通过本地的“智慧管理分析系统（SMAC）”或云端的“云镜”网络威胁感知中心，对预警的威胁信息展开高效的关联分析、线索拓展、过程回溯等调查研判工作。得益于多类安全数据间的深度关联，系统提供了应用、用户、内容、威胁、地理位置等多维信息的图形化关联展现，并自动聚合了与威胁事件相关的各类日志，用户通过递进式的数据钻取和全局日志模糊搜索，实现针对异常主机、威胁事件的高效分析。

利用对安全数据的分析结果和可视化呈现，管理者可在短时间内完成专家级的安全分析工作，进而支撑安全管理决策。

智慧处置 - 快速执行隔离阻断

随着突发性的安全事件呈现高发态势，唯有确保及时、准确采取处置措施，才能在争分夺秒的攻防对抗中争取主动。基于“360安全应急响应中心”的持续运营，当高危漏洞或恶性攻击事件发生后，云端将迅速通过更新威胁情报或特征签名的方式做出响应，并及时将应急响应通告和处置策略推送至360新一代智慧防火墙，用户通过“一键处置”确定后，系统将自动化的加载运用云端推送的情报、特征和策略，同时还将对处置策略的生效情况进行检测和反馈，确保网络边界在最短的时间内对新威胁完成免疫。

由云端提供的应急响应支撑和“一键式”的处置操作，大幅降低了用户应对突发事件的技术门槛和响应时间，将积极防御的对抗性思维运用于日常。

智能化的运维管理

“互联网+”时代，网络应用的空前繁荣使得边界安全管理不再墨守成规，防火墙正由原先的“冷系统”变得更具“热度”。360新一代智慧防火墙通过诸多智能化管理特性的设计，以专业化产品易用性的极大提升，满足用户日益多样的安全管理需求。

可视化管理

“看见”网络内传输的各种流量，是对其执行精细控制的前提条件。360新一代智慧防火墙对网内的应用、用户、内容、威胁等提供了多种形式的可视化展现。设备所提供的“数据中心”和“分析中心”功能，分别实现了针对应用使用情况的监控统计和关联分析。

“数据中心”可实时统计消耗带宽最多的应用、发生频次最高的攻击等TOP信息，帮助用户洞察网络全局应用概况。“分析中心”则提供了针对网络活动的关联分析面板，可分别以应用、传输内容、URL、威胁等为主要条件，统计与其相关的多维度信息，并在此基础上提供以任意元素为条件的递进式数据钻取，满足网络管理者深入分析应用、用户、内容和威胁的需求。

安全策略核查

安全策略始终是边界防护的核心，而复杂网络环境下的安全策略规模则更为庞大，管理者往往难以从中发现冗余和疏漏，造成安全策略无法实现最佳管控效果。

360新一代智慧防火墙通过对所有安全策略的规则条件进行智能分析，可快速发现存在冗余关系的安全策略并给出优化建议。同时，“天御云”可对网络应用、URL访问、文件传输等行为命中的策略进行更为精细和长周期的监测，便于及时发现误被放行的越权访问。此外，系统提供的“违规配置核查”功能，能够对安全策略执行自动化的检查，例如检查设备是否配置有全通策略、或开放了高危端口的访问等。通过对设备管理漏洞的持续性、自动化监测，从而及时封堵疏漏环节。

全景式集中管理

对于分布式部署防火墙的用户而言，需要通过执行统一的安全策略，从而确保各节点防护强度的一致性。然而，在日常运维中，即便是对全网设备进行一次统一升级，或是紧急下发一条应急处置策略都困难重重。

通过360新一代智慧防火墙配套的“智慧管理分析中心（SMAC）”，可对数百台防火墙进行分权分域的集中管理。利用SMAC强大的数据存储和运算能力，可提供全网设备统一监控、全局威胁实时预警、安全配置违规核查、安全策略批量下发等智能化的运维管理功能，实现全网统一监控、统一管理和统一运维，大幅提升管理效率并确保全网安全的“一致性原则”切实落地。

研究方法

本研究中所提供的信息是IDC对中国的IT安全市场信息持续研究的成果。IDC获取信息主要通过一手资料研究和案头研究，两种方法共用，相互关联、互相佐证，以确保信息的有效性和准确性。信息获取方式如下：

IDC选取了若干行业客户进行调研分析，客户范围覆盖政府、金融、教育、运营商等多个行业，通过对CIO或IT主管的访谈，IDC获取了第一手研究资料，深刻剖析了行业客户对于信息安全防御体系的诉求和建设状况。

另外，IDC还通过案头研究，主要包括（但不局限于）互联网网站、厂商介绍和新闻稿件、IDC全球分析报告以及IDC专有数据库等，对研究主题提供进一步补充。

关于白皮书

本白皮书探讨了下一代防火墙在中国IT安全市场的现状和发展趋势，对下一代防火墙特点进行了说明，研究认为行业IT数字化转型过程中面临大量应用系统的迁移与重构，其中蕴含大量的应用安全漏洞，下一代防火墙在其中提供重要的安全防御能力。具备硬件与软件形态的下一代防火墙灵活适应不同的业务环节，无论在IT基础设施的建设过程，还是在IT业务系统的建设过程中都发挥着重要的作用。

本白皮书旨在阐述下一代防火墙的重要性，说明行业用户根据自身情况需要什么样的边界防御产品，重点阐述了边界防御应具备的特征，同时就中国行业用户在通过下一代防火墙构建边界安全防御体系过程中应注意的问题，给出IDC的建议和观点。

关于IDC

国际数据公司（IDC）是在信息技术、电信行业和消费科技领域，全球领先的专业的市场调查、咨询服务及会展活动提供商。IDC帮助IT专业人士、业务主管和投资机构制定以事实为基础的技术采购决策和业务发展战略。IDC在全球拥有超过1100名分析师，他们针对110多个国家的技术和行业发展机遇和趋势，提供全球化、区域性和本地化的专业意见。在IDC超过50年的发展历史中，众多企业客户借助IDC的战略分析实现了其关键业务目标。IDC是IDG旗下子公司，IDG是全球领先的媒体出版、研究咨询、及会展服务公司。

IDC China

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
邮编：100013
电话：+86.10.5889.1666
Twitter:@IDCidc-insights-community.com
www.idc.com