SANGFOR
深信服科技

深信服让IT更简单，更安全，更有价值!

深圳市南山区学苑大道1001号南山智园A1栋
售前咨询：400-806-6868　售后服务：400-630-6430
邮编：518055　邮箱：market@sangfor.com.cn

深信服官方微信

深信服移动官网

SANGFOR 深信服科技 | 深信服智安全 SANGFOR SECURITY

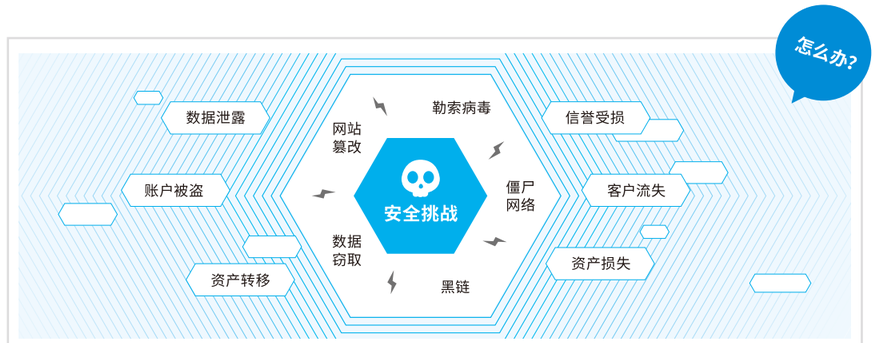
深信服
下一代防火墙NGAF

SANGFOR NEXT GENERATION FIREWALL NGAF

www.sangfor.com.cn

业务数字化转型带来的信息安全新挑战

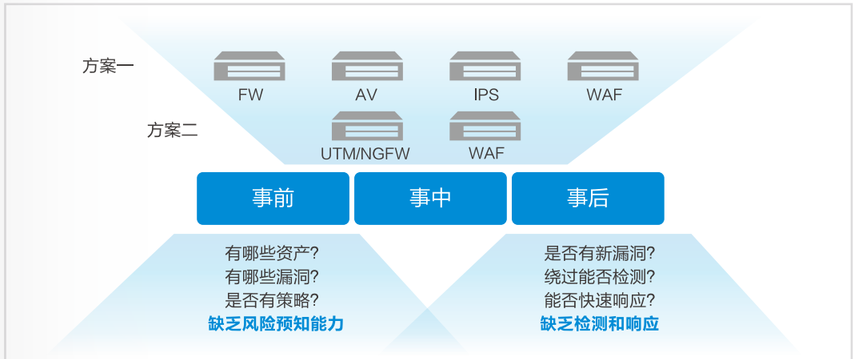
近几年来，各行各业都在加速往互联网化、数字化转型。业务越来越多的向公众、合作伙伴、第三方机构等开放，在数字化业务带给我们高效和便捷的同时，信息暴露面的增加，网络边界的模糊化以及黑客攻击的产业化使得网络安全事件相较以往成指数级的增加，面对层出不穷的新型安全事件如网站被篡改，被挂黑链，0 day 漏洞利用，数据窃取，僵尸网络，勒索病毒等等，传统安全建设模式已经捉襟见肘，面临着巨大的挑战。



传统安全建设方式存在的缺陷

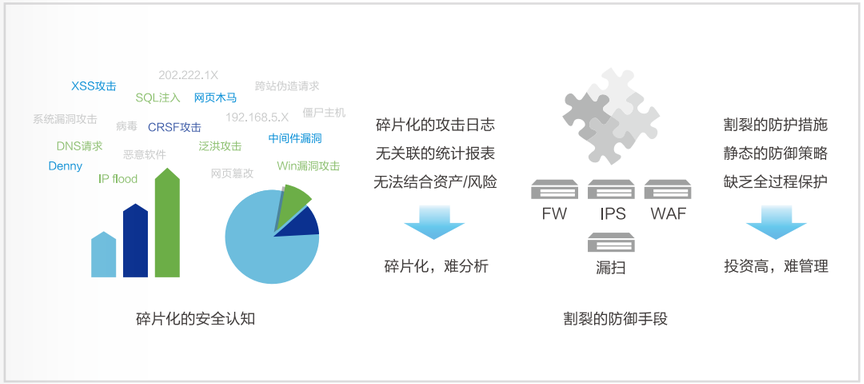
问题一 **传统信息安全建设，以事中防御为主。缺乏事前的风险预知，事后的持续检测及响应能力**

传统意义上的安全建设，无论采用的是多安全产品叠加方案，还是采用 UTM/NGFW+WAF 的整合类产品解决方案，关注的重点都在于如何防护资产在被攻击过程中不被黑客入侵成功，但是并不具备对于资产的事前风险预知和事后检测响应的能力。从业务风险的生命周期来看，仅仅具备事中的防护是不完整的，如果能在事前做好预防措施以及在事后提高检测和响应的能力，安全事件产生的不良影响会大幅度降低。所以未来，融合安全将是安全建设发展的趋势。



问题二 **传统安全建设是拼凑的事中防御，缺乏有效的联动分析和防御机制**

传统安全建设方案，搜集到的都是不同产品碎片化的攻击日志信息，只能简单的统计报表展示，并不能结合业务形成有效的资产安全状态分析。另外在防护机制上只能依赖静态的防御策略进行防护，无法及时应对业务发生的变化，不同安全设备之间也无法形成有效的联动封锁机制，不仅投资高，运维方面也难管理。



深信服 NGAF 安全理念

什么是融合安全？

融合安全不是单纯的功能叠加，而是依照业务开展过程中会遇到的各类风险，所提供的对应安全技术手段的融合，能够为业务提供全流程的保护。融合安全包括从事前的资产风险发现，策略有效性检测，到事中所应具备的积极防御手段以及事后的持续检测和快速响应机制。

深信服 NGAF 应用效果：全程保护

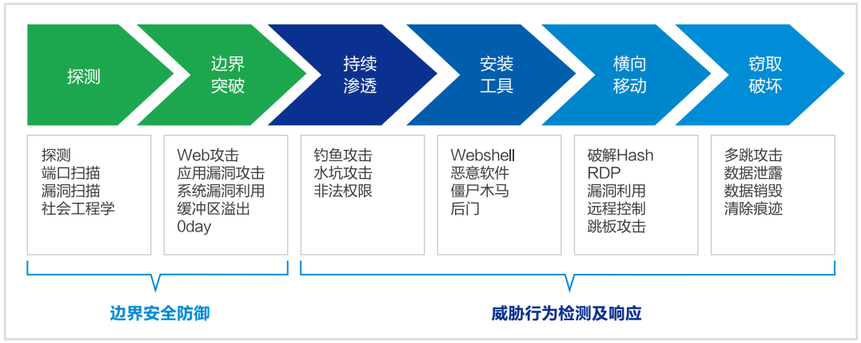
事前预知：资产 / 脆弱性 / 策略有效性识别

深信服 NGAF 能够在事前对内部的服务器进行自动识别，并且还能自动识别服务器上开放端口和存在的漏洞，弱密码等风险，同时还能判断识别出的资产是否有对应的安全防护策略以及是否生效。

事中防御：完整的防御体系 + 安全联动 + 威胁情报

深信服 NGAF 在事中防御层面融合了多种安全技术，提供了 L2-7 层完整的安全防御体系，确保安全防护不存在短板，同时还能通过安全联动功能加强防御体系的时效性和有效性，包括模块间的联动封锁，同云端安全联动，策略的智能联动等。此外，深信服 NGAF 还广泛的开展第三方安全机构合作，通过国家漏洞信息库，谷歌 Virustotal 恶意链接库等多来源威胁情报的输入，帮助用户能够在安全事件爆发之前就提前做好防御的准备。

事后：威胁行为的持续检测 & 快速响应

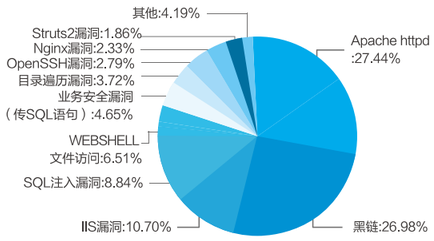


传统安全建设主要集中在边界安全防御，缺乏针对绕过安全防御体系的威胁行为的检测能力，如果能够针对黑客入侵后的威胁行为进行持续检测并快速响应，可以极大程度降低安全事件产生的影响。深信服 NGAF 融合了事后检测及快速响应技术，即使在黑客入侵之后，也能够帮助用户及时发现入侵后的恶意行为，如检测僵尸主机发起的恶意行为、网页篡改、网站黑链植入及网站 Webshell 后门检测等，并快速推送告警事件，协助用户进行响应处置。

深信服 NGAF 核心优势：全程可视

全程可视：提升业务全过程风险的安全认知能力

▶ 事前对安全风险的认知：识别资产脆弱性及策略有效性



业务和用户策略防护风险（13）	
1.邮件服务器未配置入侵防御系统、WEB应用防护。	存在风险
2.财务系统未配置入侵防御系统、WEB应用防护。	存在风险
3.CRM系统未配置入侵防御系统、WEB应用防护。	存在风险
4.研发代码服务器未配置入侵防御系统、WEB应用防护。	存在风险
5.ERP未配置入侵防御系统、WEB应用防护。	存在风险

深信服 NGAF 不仅能够在事前对内部的服务器进行自动识别，而且还能自动识别服务器上开放端口和存在的漏洞，弱密码等风险，同时还能判断识别出的资产是否有对应的安全防护策略以及是否生效。

▶ 事中对保护过程的认知：攻击事件匹配不同攻击阶段

深信服 NGAF 通过攻击阶段图来匹配不同阶段所检测到的攻击行为，并且可以了解到具体的攻击事件，攻击来源和攻击类型等信息。

▶ 事后对保护结果的认知：基于信息资产纬度的安全现状展示 + 综合风险报表

深信服 NGAF 通过首页信息资产状态展示以及综合风险报表提供给用户一个直观可视的安全交付结果，让用户能够快速感知到网络的安全现状，并对攻击过程进行回溯举证。

深信服 NGAF 优势

全程可视	简单交付	高效稳定
风险的可视	一体化策略部署	单次解析
保护过程的可视	全过程运营中心	多模匹配算法
保护结果的可视	综合风险报表	软硬件双冗余架构
优势1	优势2	优势3

全程可视：深信服 NGAF 通过将事前、事中、事后各个阶段防御和检测到的风险和资产进行关联，帮助用户能够直观的看到当前信息资产的安全状态，清楚的了解到哪些资产存在风险，遭受到了哪些攻击，以及攻击产生了哪些危害。

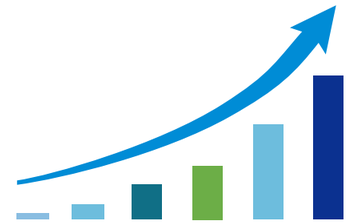
简单交付：深信服 NGAF 通过场景化的部署向导帮助用户实现设备的快速上线和一体化的安全策略配置，而安全运营中心则是旨在帮助用户实现简单运维，从事前的风险评估和防御能力评估到事中及事后的安全事件监测与分析，最终形成待办事项，形成一个动态的运维闭环，使得安全不再是静态的防御和被动的响应。

高效稳定：深信服 NGAF 采用单次解析引擎及多核处理架构，实现报文内容的多线程并行检测，能够有效提升应用层处理性能，同时采用了分离平面设计，将数据转发与内容检测平面分开进行处理，在应用层内容检测发生问题的时候也不会影响网络层面的数据转发。

深信服 NGAF 品牌实力

高速增长，年复合增长超 70%

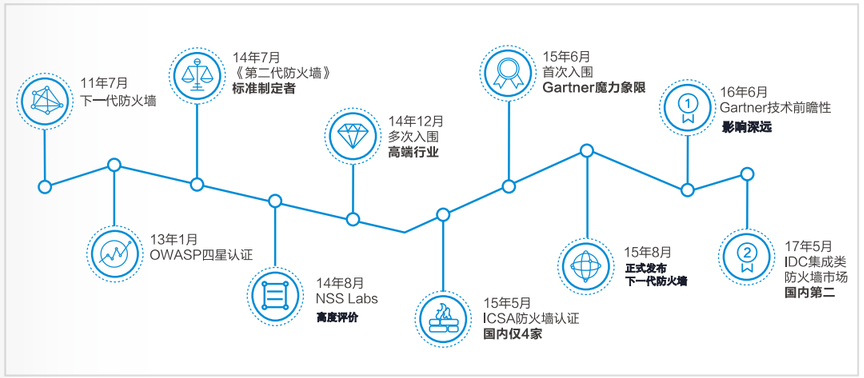
2011年发布下一代防火墙
4万家用户一致好评
5.4万台在线稳定运行



2011 年 7 月，深信服在国内安全市场推出下一代防火墙，自产品发布至今以来，年复合增长率超过70%，增长迅猛 。

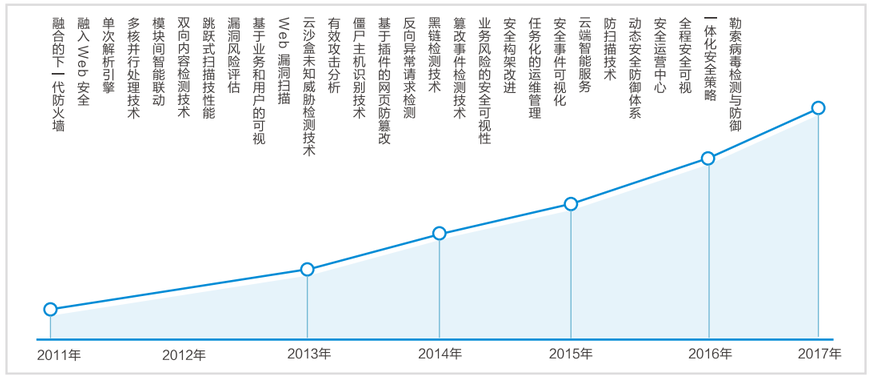
截至 2017 年 6 月，深信服 NGAF 在全国的用户数累计超过 40000 家，在线稳定运行的设备超过 5.4 万台，用户覆盖各行各业。据全球 IT 咨询机构 IDC 的分析报告显示，2016 年深信服 NGAF 在中国集成类防火墙市场排名第二，占 14.3% 的市场份额。

第一品牌，专业认可度高



深信服 NGAF 经过多年的深耕，获得了越来越多权威机构的认可。如主导参与了国内第二代防火墙标准的制定，获得 NSS Labs 的推荐级评价，连续多年入围移动，电信设备集采目录，连续多年入围 Gartner 防火墙魔力象限等等。

持续创新，引领安全新趋势



持续创新一直是深信服保持快速增长的源动力。深信服 NGAF 自发布以来，产品坚持自主创新，不断迭代，平均每年更新发布 5 个版本，2011 年以来累计提交了 30 多项安全专利技术，引领安全新趋势。

专业安全团队

深信服在应用安全领域有着 10 年以上的技术积累，背后离不开一个不断成长壮大的安全团队来支撑：

超 1500 人规模的安全研发团队：专门从事安全产品研发、安全服务工具开发、威胁样本分析、应急响应、安全咨询服务等工作；

在北京设立了深信服千里目安全研究实验室：专门负责国内外前瞻性技术研究和漏洞挖掘。截至 2016 年底，累计挖掘近百个原创高危漏洞；每月发布安全月报并提交至安全主管部门，如 CNCERT、网络安全保卫局、CNVD 等。

在深圳成立组建了雪豹安全团队：由 30 多位博士及博士后组建的雪豹安全团队，专门负责安全技术难题的攻坚和创新，自主研发了大数据行为分析建模算法，异常行为模式匹配算法等来支撑产品的理念落地。

近几年来，深信服安全团队也积极参与了多项国家级网络安全保障支撑工作：如国家“九三大阅兵”活动，G20 峰会网络安全技术支撑单位，国家“互联网网络安全威胁治理行动”活动重点支撑单位，“首都网络安全周”活动重点支撑单位等。因为在安全事件应急处置及漏洞通报方面表现突出，深信服还获得了第七届国家互联网应急响应中心国家级支撑单位的荣誉。

SANGFOR 深信服科技

追逐梦想 永攀高峰

深信服智安全 SANGFOR SECURITY | 深信服云IT SANGFOR CLOUD