深信服网络安全监测解决方案

背景与需求分析

网络安全已上升到国家战略，网络信息安全是国家安全的重要一环，2015 年 7 月 1 号颁布的《国家安全法》第二十五条指出：加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。国家《网络安全法》草案已经发布，正式的法律预计不久后也会正式颁布。保障网络安全，不仅是国家的义务，也是企业和组织机构的责任。对于企业来说，保障网络信息安全，防止网络攻击、网络入侵、网络窃密、违法信息发布，不仅能维护自身经济发展利益，还能避免法律风险，减少社会信誉损失。

Gartner 认为，未来企业安全将发生很大的转变，传统的安全手段无法防范 APT 等高级定向攻击，如果没有集体共享的威胁和攻击情报监测，将很难多方位的保护自己网络安全。因此过去单纯以被动防范的安全策略将会过时，全方位的安全监控和情报共享将成为信息安全的重要手段。

因此，仅仅依靠防护体系不足以应对安全威胁，企业需要建立监测机制，扩大监控的深度和宽度，加强事件的响应能力。安全监测和响应能力将成为企业安全能力的关键，在新的安全形势下，企业需要更加关注威胁监控和综合性分析的价值，使信息安全保障逐步由传统的被动防护转向“监测-响应式”的主动防御，实现信息安全保障向着完整、联动、可信、快速响应的综合防御体系发展。

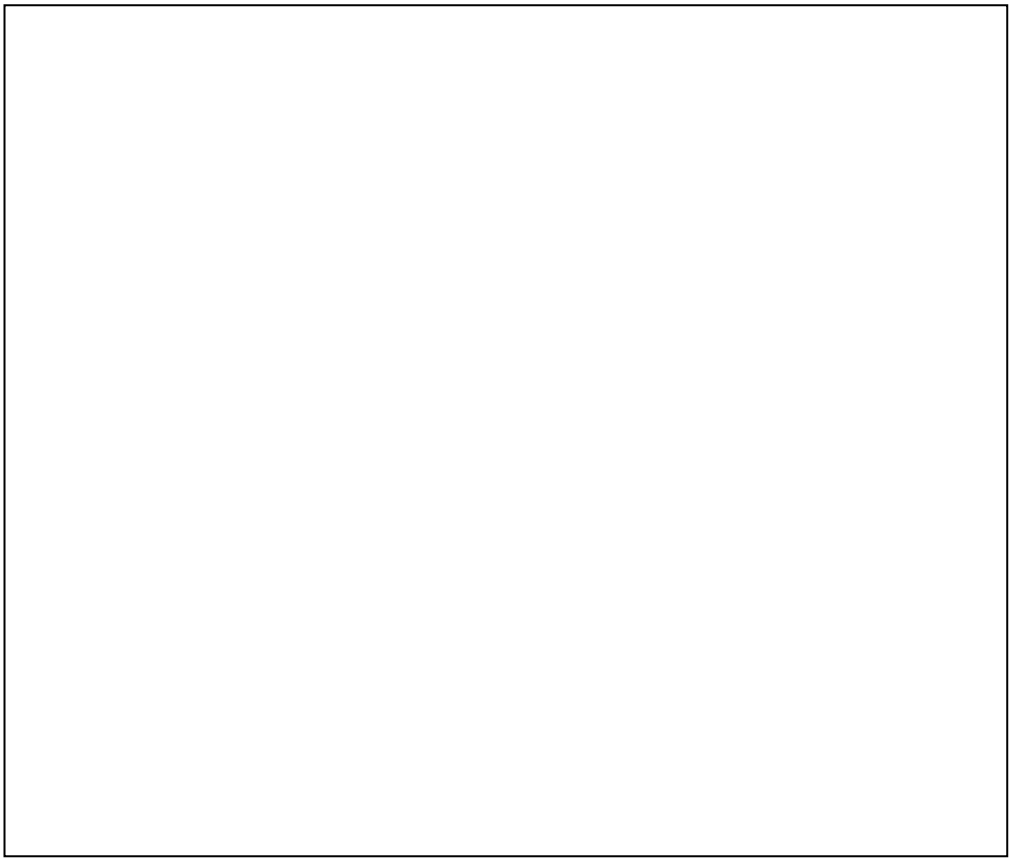
然而，传统的网络安全设备更多关注网络层风险及基于已知特征的被动保护，缺乏对各种系统、软件的漏洞后门有效监测，缺乏对流量内容的深度分析及未知威胁有效识别，不具备多维全面的安全风险监测响应机制，已不能满足新形势下网络安全的需求。

深信服网络安全监测解决方案

深信服创新性的推出了网络安全监测解决方案，该方案面向未来的安全需求设计，帮助企业实现多层次、全方

位、全网络的立体网络安全监测。该方案主要采用了深信服下一代防火墙 NGAF 作为监测节点，通过对应用状态、数据内容、用户行为等多个维度的全方位安全监测，并结合深信服云安全中心海量威胁情报快速共享机制，帮助企业构建立体化、主动化、智能化综合安全监测防御体系，有效弥补了传统安全设备只能防护已知常规威胁的被动局面，实现了安全风险全面识别和快速响应。

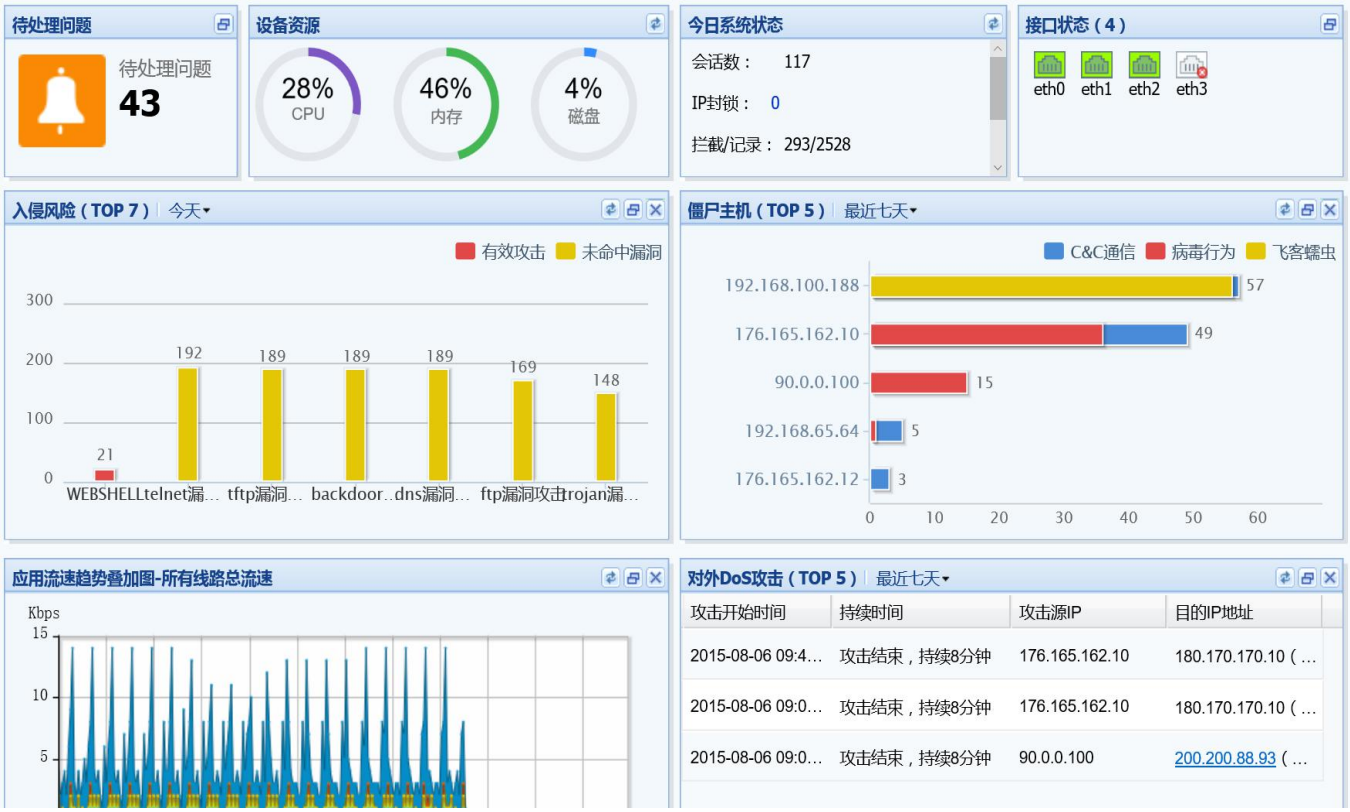
实现网络安全威胁内容的监测 ,帮助用户了解和评估网络安全风险 ,是深信服下一代防火墙(NGAF ）设计目的之一。NGAF 能够深入分析流量内容，有效识别网络中的用户、应用、内容和威胁。NGAF 提供了更加全面的安全威胁监测能力，除了传统的黑名单、木马病毒特征签名检测外，还提供了实时漏洞监测、僵尸主机监测、数据风险监测、黑链风险监测、对外 DoS 攻击等多种威胁监测，满足网络安全监测和防御体系建设的需求。



NGAF 可以旁路部署在网络中，通过将相关业务数据流镜像到下一代防火墙进行实时监测，该方式对用户业务系统的完整性、可用性可以做到零影响。NGAF 能够协助用户进行业务系统的安全风险评估，并结合黑客攻击行为进行关联分析，帮助用户找到真正存在风险的薄弱环节。NGAF 也可以串接在网络中在线监测，实时监控入侵、漏洞、僵尸主机、数据泄漏、黑链等安全风险，并提供专业的安全风险运维加固参考方案，助您快速实现自助化安全运维。配合使用 NGAF 的外置数据中心，您可以将监测设备的安全日志集中存储和汇总分析，外置数据中心能够给

出监测设备当前网络环境的安全概况、最近的攻击事件详情、漏洞详情，并支持综合日志查询功能，可以查询监测到的多种类型安全日志。

NGAF 可以将监测到的安全风险在 WEB 页面展现，大部分威胁类型都可以在 NGAF 设备页面的系统状态查看到，进一步点击进去还能看到每一类风险的详细信息，并且提供了客观的威胁描述及参考解决方案。



入侵风险监测

NGAF 提供了入侵风险监测功能，能够自动收集被保护网络遭受到的入侵风险状况，并基于今天、昨天、最近 7 天分别展示。入侵风险包含了多维的风险类型，包括 WEBSHELL、XSS 攻击、SQL 注入、信息泄露、恶意链接、网站扫描、DNS 漏洞攻击、FTP 漏洞攻击、系统漏洞攻击、后门漏洞攻击等。

登录 NGAF 设备就能看到系统状态中的入侵风险情况（如上图），进一步点击入侵风险，还能看到详细的入侵风险状况，包括入侵风险的类型 TOP10、入侵风险排行详情、每种攻击的数量、有效攻击数量、攻击类型、被攻击 IP 等信息，如果配置了深信服外置数据中心，还能进一步看到每个攻击的详细信息，包括源 IP、目的 IP、时间、类型、攻击描述等详细的入侵信息，并能够导出日志信息和进行分类查询等操作。

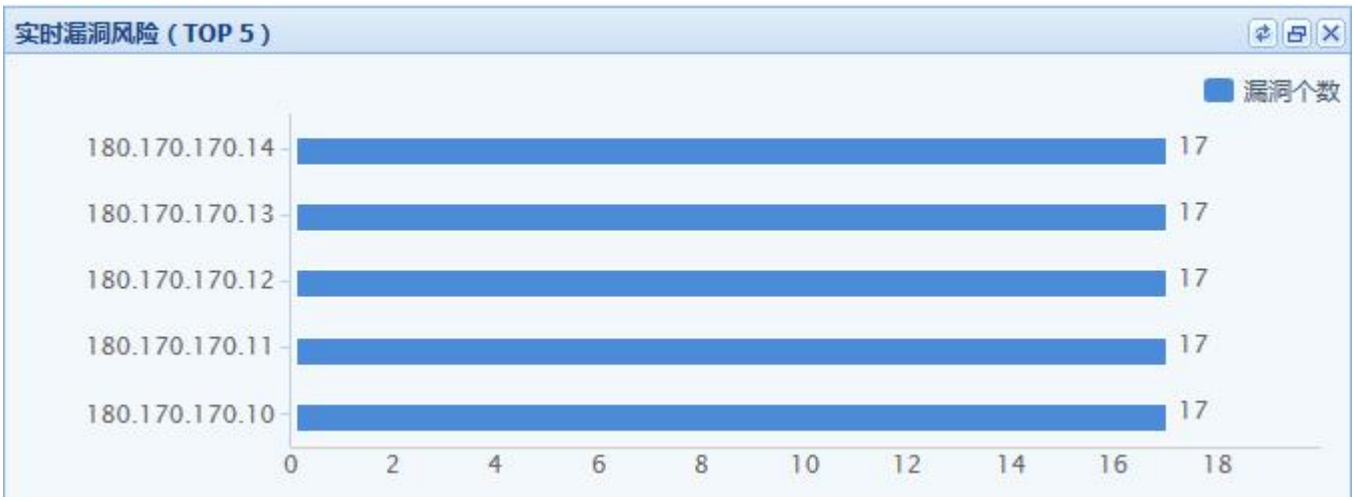
僵尸主机监测

NGAF 能有效识别出那些因感染了蠕虫、木马等病毒而被黑客控制的僵尸主机。攻击者可通过控制僵尸主机进行 DoS 攻击、APT 攻击等各种类型的攻击，以达到致使用户网络或重要应用系统瘫痪、窃取用户机密业务数据等目的。

登录 NGAF 设备就能看到系统状态中的僵尸主机情况（如上图），包含了 TOP5 的僵尸主机 IP 地址和风险行为类型及数量。进一步点击僵尸主机，还能看到详细的僵尸主机风险状况，包括僵尸主机风险类型和数量，具有僵尸主机行为的主机 IP，主机所在区域，活跃行为次数，最近活跃时间，风险行为描述等。此外，还提供了危害影响描述及推荐的解决方案

实时漏洞监测

NGAF 提供了实时漏洞发现功能，可以对经过设备的流量进行实时漏洞风险分析，它的最大优势就在于能实时发现客户网络环境的安全缺陷，且不会给网络产生额外的流量。实时漏洞检测功能能够发现主机、服务和应用的安全漏洞，如底层软件漏洞、Web 应用风险、插件漏洞、Web 不安全配置、弱口令等安全缺陷。



点击进入实时漏洞风险页面，还能看到漏洞风险的服务器总数和漏洞风险总数排行前 10 的服务器域名/IP，发现详情，漏洞风险概况。针对单个服务器 IP，给出了检测到的详细漏洞信息，如漏洞类型，数量，描述，危害等级等信息。深信服还创新性的将实时漏洞检测和入侵攻击风险进行结合，从海量的攻击日志中快速识别出真正对用户业务系统有危害的“有效攻击”，从而大大减少安全运维的动作工作，让 IT 人员将更多的精力放在有效威胁的防护上面。

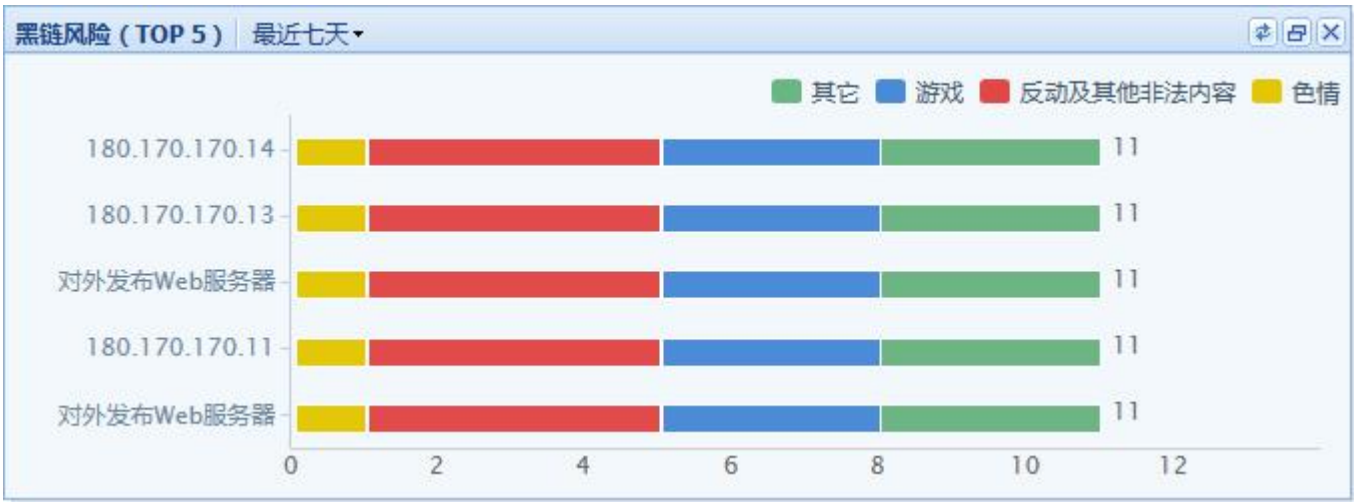
数据风险监测

数据风险监测主要是为了发现和阻止一些重要信息资源泄漏。数据风险监测包含了源代码泄漏、重要配置泄漏、敏感信息泄漏、账号信息泄漏、其他信息泄漏的监测。账号、源代码、重要资源文件等敏感信息的泄露不但会给用户造成损失，黑客还可利用这些信息对内网中重要的业务系统进行渗透攻击，进一步窃取用户单位中更机密的核心数据。

点击进入数据风险页面，还能看到数据风险详细信息，如风险类型和数量，危害影响，参考解决方案，数据风险详情等。在数据风险详情里面，还能看到具体的服务器风险信息和防护情况等。

黑链风险监测

NGAF 提供黑链检测功能，黑链的本质是一种网页篡改。攻击者通过利用网站存在的程序漏洞上传或获取网站的 WEBSHELL 后门，进而篡改网站内容并植入黑链。黑链不会显现在网页上，只有在网页代码中才能看到链接。攻击者可在网站中添加赌博、色情等黑链，用户的对外业务将受到严重影响，还会面临网站被降权或者受到相关部门通报的风险。



NGAF 黑链检测能够将发现黑链的网站域名/IP 及被植入的黑链类型实时显示出来。点击进入黑链风险页面，还能看到黑链风险详细信息，如黑链类型分布、危害影响、参考解决方案、风险主机排行等。在风险主机排行信息中，能够看到风险主机被发现的黑链页面，黑链类型，风险概况，黑链详细信息，发现时间，植入黑链的页面总数。

对外 DoS 攻击监测

NGAF 能够实时检测内部主机对外的 DoS 攻击 ,DoS 攻击判定的本质是该访问行为是异常流量。对外发起 DoS

攻击的内网主机很可能感染了病毒，并已被黑客控制。内网外发的 DoS 攻击将会造成严重的网络拥堵，导致用户业务中断，也会影响被攻击网络的业务的正常运行，甚至因此而受到网络监管部门的通报，甚至承担法律责任。

对外DoS攻击（TOP 5） 最近七天

攻击开始时间	持续时间	攻击源IP	目的IP地址
2015-08-21 03:18:09	攻击结束，持续8分钟	176.165.162.14	180.170.170.14（中国上...
2015-08-21 03:16:26	攻击结束，持续8分钟	176.165.162.13	180.170.170.13（中国上...
2015-08-21 03:14:43	攻击结束，持续8分钟	176.165.162.12	180.170.170.12（中国上...
2015-08-21 03:12:58	攻击结束，持续8分钟	176.165.162.11	180.170.170.11（中国上...
2015-08-21 03:11:14	攻击结束，持续8分钟	176.165.162.10	180.170.170.10（中国上...

NGAF 能够实时检测并记录对外的 DoS 攻击情况。点击进入对外 DoS 攻击页面，还能看到内网主机对外发起 DoS 攻击的详细信息，如对外攻击 TOP5 主机信息，对外攻击详情，危害影响，参考解决方案。对外攻击详情还包括单个攻击的开始时间，持续时间，攻击者 IP，被攻击者 IP，并能够结合外置数据中心看到攻击日志详情。

威胁情报预警与处置

一些存在范围广、危害破坏大的高危漏洞给我们的网络安全造成巨大的隐患，如 OpenSSL 心脏滴血漏洞、Bash 破壳漏洞、微软 IIS 高危漏洞等。为了解决高危漏洞爆发后快速帮助用户修复和保护这些漏洞威胁，深信服在 NGAF 设备上专门设置了一个威胁情报预警与处置模块。该模块能够和深信服云安全引擎平台联动，深信服云中心能够在热点安全事件爆发后的 48 小时内提供完整的 0Day 漏洞检测和防护方案，并推送给 NGAF 设备，NGAF 可自动对被保护对象进行扫描检测，并对扫描发现的热点威胁提供一键防护功能，用户只需按动一键防护按钮，设备即可自动生成针对所有被发现的威胁的防护策略。截至 2015 年 8 月，深信服 NGAF 已推出了以下类型的威胁情报预警与处置方案。

待处理问题

对于监测发现的重要安全问题，NGAF 还会生成待处理问题列表，提醒用户及时修复安全问题。点击具体的待处理问题，还能看到这些问题的风险提示，还可以进一步查看风险问题详情，详情中有对问题的详细描述及建议的解决方案，用户只需要参照解决方案提示步骤，即可快速完成这些安全问题的修复。

此外，深信服云安全中心会实时同步最新的安全威胁识别特征到 NGAF 设备上，实现了海量的威胁情报快速共享。当单个 NGAF 发现了无法实时确认的可疑内容，就会同步上报到深信服安全云中心，云中心通过虚拟沙盒演练等方法进行判定，一旦确认是威胁行为，将快速生成识别特征并下发到全球在线的 NGAF 设备上，基于这些技术手段，NGAF 能够准确识别未知威胁和 APT 攻击。

深信服 NGAF 全面专业的深度内容“监测-响应”体系，能够实现多层次、全方位、全网络的立体网络安全监测，实现立体化、主动化、智能化综合安全防御，有效帮助客户构建完整、联动、可信、快速响应的综合防御系统。

深信服方案价值

积极主动发现安全问题，提升安全部门价值；

提供自助式、智能化运维方法，改变传统被动滞后的运维状态；

威胁识别更全面，实现完整、宏观的安全防护，改变微观、割裂的安全状态；

全周期，多维度的威胁事件发现能力，对事前、事中、事后的威胁类型全面侦测；

基于内容和行为模型的深入监测和威胁事件全局关联，有效发现高级持续攻击行为；

相比传统方案，节省了大量采购、部署、运维成本，同时提供更全面的安全监测保护效果；

灵活的部署模式：既可以在线部署，也可以旁路部署，实现最优的网络安全监测和防护选择。