绿盟 WEB 应用防护系统（可管理系列）产品白皮书

【绿盟科技】

■ **文档编号**	NSF-PROD-WAF with MSS（原 PAMWAF）-V1.0-产品白皮书-V1.2	■ **密级**	完全公开
■ **版本编号**	V1.2	■ **日期**	2014/6/3

■ **版本变更记录**

时间	版本	说明	修改人
2013/3/10	V0.1	创建文档，内容包括：产品概述、产品架构、产品优势。	乔建
2013/3/11	V0.2	添加主要功能。	卢梁
2013/3/12	V0.3	添加典型部署。	卢梁
2013/3/13	V0.4	添加引言、产品优势、客户利益，修改产品概述、产品架构、产品功能、典型部署。	李天武
2013/3/18	V0.5	添加实施与运营流程、总结	李天武
2013/3/18	V0.6	修改产品体系架构图使用的软件细节	李天武
2013/3/21	V0.7	修改部分文字描述、更新使用的图片	李天武
2014/6/3	V1.2	更改产品与技术名称	李天武

目录

一. 引言 1

二. 绿盟 WEB 应用防护系统（可管理系列） 1

2.1 产品概述 1
2.2 产品架构 2
2.3 产品优势（技术优势&特色） 3
2.4 主要功能 5
2.5 典型部署 8
2.6 实施与运营流程 8

三. 客户利益 10

四. 总结 11

表格索引

表 2.1 绿盟 WAF WITH MSS 响应时间表 4

插图索引

图 2.1 绿盟 WAF WITH MSS 体系架构 2
图 2.2 绿盟 WAF WITH MSS 安全报告 4
图 2.3 绿盟安全云监控中心 5
图 2.4 绿盟 WAF WITH MSS 智能补丁 6
图 2.5 绿盟 WAF WITH MSS 在线部署模式 9
图 2.6 绿盟 WAF WITH MSS 旁路部署模式 10
图 2.7 绿盟 WAF WITH MSS 实施与运营流程 8
图 3.1 绿盟 WAF WITH MSS APDR 模型 11

一. 引言

互联网大潮的影响之下， Web 应用（网站）逐渐承载了各行业重要、甚至主流的业务（例如：网上银行系统、网上证券交易系统、网上营业厅系统、电子商务系统、电子政务系统等）。在这种从线下转向线上的趋势影响下，各行业的各类组织和机构还在不断增加网站上的功能，以便向客户提供更好的支持、更好的体验。

据中国国家互联网应急中心（CNCERT/CC）的数据统计，由于 Web 应用（网站）承载了越来越多重要业务，75%以上的攻击都瞄准了网站。这些攻击都可能导致机构遭受声誉和经济损失，可能造成恶劣的社会影响。管理者们已经意识到网站安全面临的严峻形势，正在采取措施，比如：在网站前端部署 WEB 应用防火墙（Web Application Firewall，也称 WEB 应用防护系统，简称 WAF），起到了一定程度的防护作用。但是，他们仍面临以下挑战：

- 无法快速有效拦截新型 Web 攻击；
- 发生 Web 攻击事件无法第一时间知晓；
- 即使知道发生了 Web 攻击事件，也无法及时发挥 WAF 的最佳防护效果，将危害降到最小。

二. 绿盟 WEB 应用防护系统（可管理系列）

2.1 产品概述

绿盟 WEB 应用防护系统（可管理系列）（NSFOCUS WAF with MSS，原叫 PAMWAF）是绿盟科技在原有 WAF 产品的基础上，进一步融合安全云平台技术，推出的 7x24 小时 WEB 应用安全解决方案。绿盟 WAF with MSS 可以实现将客户本地 WAF 设备与绿盟安全云对接和同步，由绿盟安全专家团队提供专业的网站安全隐患和遭受的攻击威胁监视、响应、防护服务，最大限度降低 Web 应用安全风险，同时帮助用户从繁重的日常安全维护工作中解脱出来，让用户能够专注于自身核心业务的发展。

2.2 产品架构

绿盟 WEB 应用防护系统（可管理系列）的体系架构主要由绿盟安全云和用户设备构成。其中，用户端主要是由 WAF 构成的设备引擎层；绿盟安全云主要分为四层：数据采集层、数据处理层、数据存储层和数据呈现层。

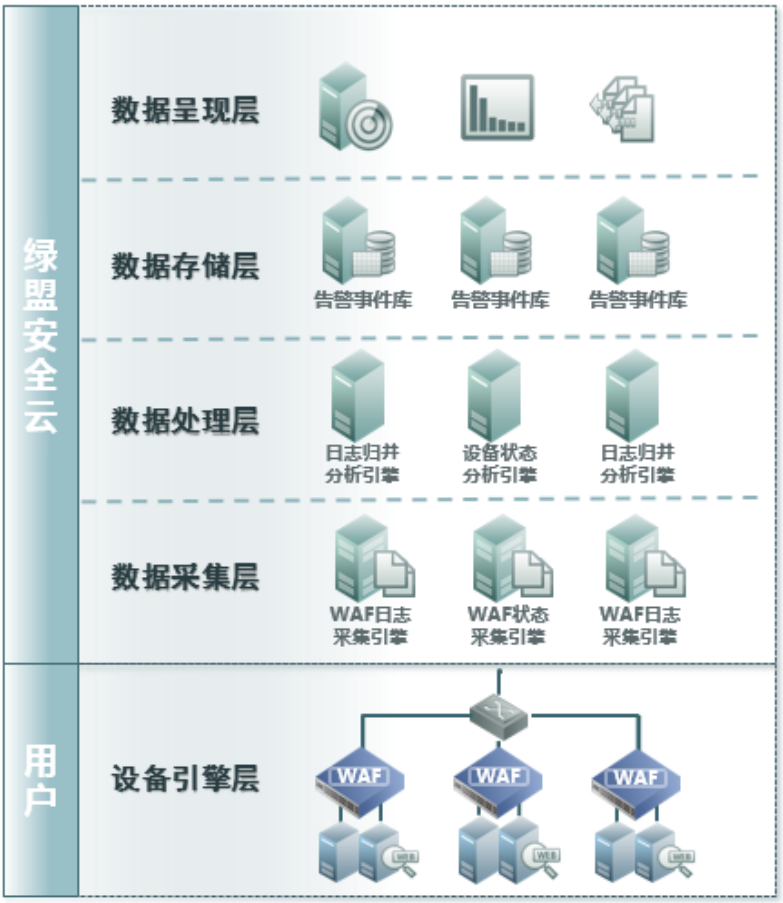

图 2.1　绿盟 WAF with MSS 体系架构

设备引擎层

设备引擎层包括部署在用户网络环境的 WAF 设备集群，通过绿盟科技统一接口与绿盟安全云对接后，会实时地将状态和日志信息通过加密通信协议上传到绿盟安全云。

数据采集层

绿盟安全云的数据采集层负责实时接收用户 WAF 设备上传的状态和日志信息，经过解析后存放到缓存服务器的队列中。

数据处理层

数据处理层从缓存服务器队列中取出 WAF 设备状态和日志，进行归一化和关联分析后，将处理结果保存到数据库服务器集群中。

数据存储层

数据存储层由数据库服务器集群构成，主要存放经过数据处理层归并分析后的 WAF 告警事件，并且提供接口供数据呈现层实时查询。

数据呈现层

数据呈现层将数据库服务器集群中保存的 WAF 告警事件通过 Web 界面实时呈现出来，交由 7x24 小时值守的安全专家团队进一步分析处理。安全专家团队通过这个操作界面，能够结合用户的网站和 WAF 设备情况，进一步诊断识别具体攻击类型及其危害，在 30 分钟之内将分析结果通过电话、短信或邮件方式通告用户，协助用户第一时间调整安全防护策略进行精确拦截。在此过程中，绿盟安全专家团队还会对事件进行持续跟踪，观测安全防护效果，确保用户网站正常运行。除此之外，绿盟安全专家团队还会定期为用户出具专业安全报告，让用户可以对自身网站安全状况及趋势一目了然。

2.3 产品优势（技术优势&特色）

安全云平台 7x24 小时监测

绿盟安全云的监测引擎能够对用户 WAF 设备及其防护网站进行 7x24 小时持续监测，从时间上覆盖 Web 攻击随时出现的可能性。一旦发现异常情况，专业的绿盟安全专家团队可以及时进行诊断、分析，并协助用户调整 WAF 设备的安全防护策略，实现针对 Web 攻击的快速防护。

安全专家团队全天候远程值守

绿盟安全专家团队拥有多名具有行业认证和产品认证资格的安全专家（CISSP、CISP、ISO 27001LA 等），具备丰富的安全专业知识、技能和实战经验。自 2008 年绿盟科技发布 Web 应用防护产品至今，绿盟安全专家团队已主导和参与过 100 多起 Web 攻击应急响应与防护工作。

持续调整优化防护规则，精准拦截 Web 攻击

绿盟安全专家团队具有丰富的 Web 攻防实战经验，持续分析 WAF 告警日志，准确识别常见的 Web 攻击，通过优化和调整 WAF 设备的安全防护策略，可对攻击进行迅速且精准拦截，帮助用户降低 Web 应用安全风险。

攻击类型
SQL 注入攻击
跨站脚本攻击（XSS）
跨站请求劫持（CSRF）
LDAP 注入攻击
SSI 指令攻击
XML 注入
命令行注入攻击
远程文件包含
文件非法上传
文件非法下载

表 2.1　绿盟 WAF with MSS 响应时间表

专家级的定期安全报告

绿盟安全专家团队可为用户提供专业的攻击事件报告、安全月报和安全年报，提供详细的 Web 攻击事件信息和 Web 攻击的态势分析，可为用户的安全规划提供可靠的数据依据。

图 2.2　绿盟 WAF with MSS 安全报告

灵活的部署与应用方式

绿盟 WAF with MSS 提供“Web 应用监护完全托管”和“Web 攻击事件应急响应”这两种方式协助用户防御 Web 攻击，可以完美融入到用户各种安全运维场景。同时，方案也支持在线与旁路部署方式，能满足各种场景的组网需求。

安全智能

安全攻防是一个动态过程，安全产品面对的是充满“智慧”的对手。绿盟科技拥有专门的安全研究机构，能够及时跟踪、发现互联网上新出现的 Web 应用攻击类型，并将有针对性的防护规则和算法研究成果快速应用于 WAF 设备上，帮助客户对抗最新攻击。

2.4 主要功能

Web 攻击监测、分析、响应及防护

用户 WAF 设备和绿盟安全云对接后，会实时将设备状态和日志信息上传绿盟安全云。绿盟安全云将收集到的设备状态和日志信息进行归一化和关联分析，形成一条条 Web 攻击告警事件，实时呈现在监测界面上，供 7x24 小时值守的绿盟安全专家团队进一步分析处理。

绿盟安全专家团队实时观察 Web 攻击告警事件监测界面的变化情况，一旦发现告警事件，会第一时间了解该事件的详细信息，包括告警时间、事件类型、目的 IP 端口、目的域名、来源 IP 端口等，同时结合绿盟安全云对用户网站的扫描和监测结果，对该事件的准确性以及影响程度在 30 分钟之内做出判断。

绿盟安全专家团队经过分析，确认某一告警事件确系 Web 攻击之后，会第一时间通过电话、短信或邮件等方式将分析结果通告用户，并且在取得用户授权的情况下，协助用户快速调整设备的安全防护策略，精确拦截 Web 攻击。

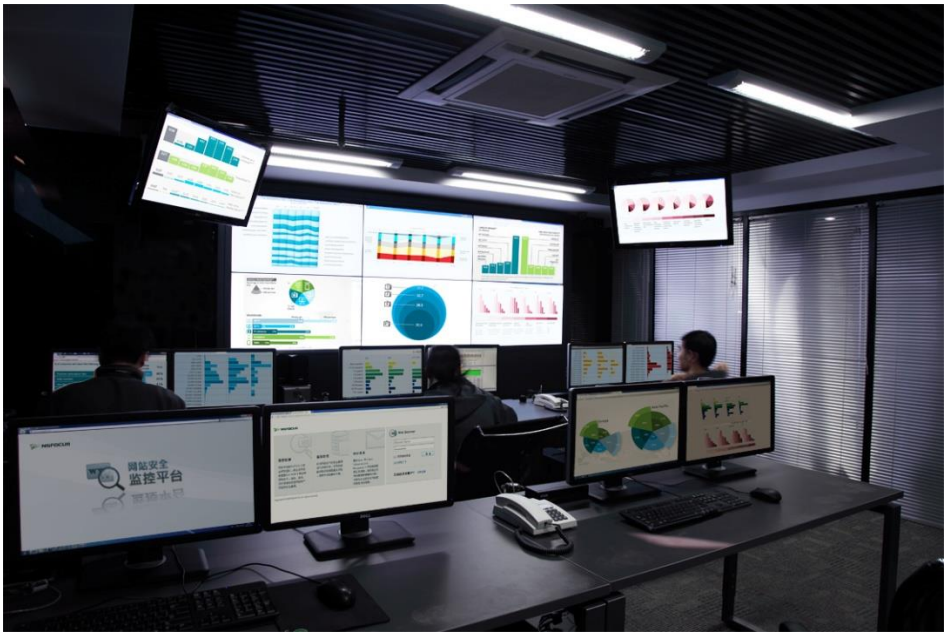

图 2.3 绿盟安全云监控中心

设备远程维护

除了协助用户监测和防御 Web 攻击，绿盟安全专家团队还会远程协助用户维护 WAF 设备，包括设备监控、系统升级、故障排查、设置调整等。其中，设备监控主要包括以下信息：

- WAF 设备的 CPU 使用率
- WAF 设备的内存使用率
- WAF 设备的磁盘使用率
- WAF 设备的引擎状态
- WAF 设备的端口状态
- WAF 设备的关键进程运行情况
- WAF 设备的配置变更记录
- WAF 设备的证书信息
- WAF 设备的实时流量数据

智能补丁

为了增加功能，网站经常会调整，调整就可能引入新的漏洞，要防护这些新漏洞，要求 WAF 具有动态调整能力。如何做到呢？答案来自云端。用户将 WAF 设备与绿盟安全云对接后，绿盟安全云可以定期对用户网站进行远程扫描，扫描结果报告经过绿盟安全专家团队处理后，生成一个可执行的、有针对性的“智能补丁”，下发到 WAF 设备并应用到安全防护策略中，使 WAF 能够定期“真切地看到”网站漏洞的变化，并通过应用“智能补丁”做出动态调整。这为 WAF 防护网站安全提供了关键的补充。

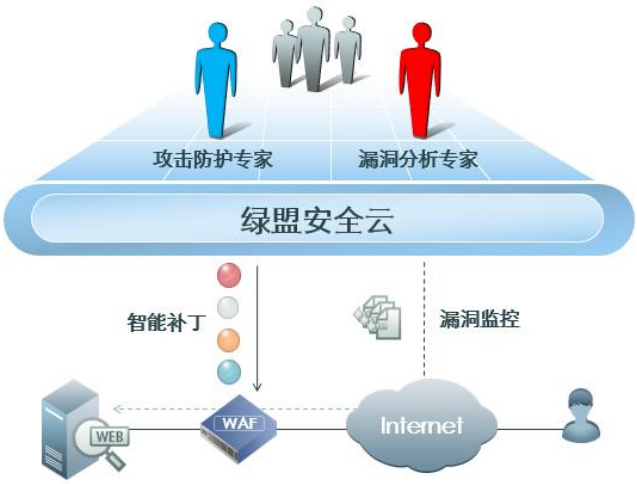

图 2.4 绿盟 WAF with MSS 智能补丁

网页篡改在线防护

绿盟 WAF with MSS 提供事中响应防护以及事后持续监控的在线防护解决方案。事中，WAF 设备实时过滤 HTTP 请求中混杂的网页篡改攻击流量（如 SQL 注入、XSS 等），并将告警事件上报绿盟安全云，由绿盟安全专家团队进一步分析，及时优化和调整 WAF 设备安全防护策略，对网页篡改攻击进行更精准的拦截。事后，WAF 设备自动监控网站所有需保护页面的完整性，检测到网页被篡改，即时上报绿盟安全云，并且将篡改前的正常页面对外显示，让网民可继续正常访问网站。绿盟安全专家对该事件进行分析确认后，第一时间通过电话、短信或邮件方式通知用户，提醒用户恢复被篡改页面，并且持续跟踪事件处理效果。

网页挂马在线防护

网页挂马为一种相对比较隐蔽的网页篡改方式，本质上这种方式也破坏了网页的完整性。网页挂马攻击目标为各类网站的最终用户，网站作为传播网页木马的“傀儡帮凶”，严重影响网站的公信度。

当用户请求访问某一个页面时，绿盟 WAF with MSS 会对服务器侧响应的网页内容进行在线检测，判断是否被植入恶意代码，如果确实被植入了恶意代码，则会对其进行自动过滤，并且产生告警事件，上传绿盟安全云，绿盟安全专家团队可以将该事件第一时间通报给客户，或者放到定期的统计分析报告中，为用户呈现网站安全防护效果。

敏感信息泄漏防护

绿盟 WAF with MSS 通过绿盟安全云和安全专家团队，可以更精准地识别并更正 Web 应用错误的业务流程，识别并防护敏感数据泄漏，满足合规与审计要求，具体如下：

1. 可自定义非法敏感关键字，对其进行自动过滤，防止非法内容发布为公众浏览。
2. Web 站点可能包含一些不在正常网站数据目录树内的 URL 链接，比如一些网站拥有者不想被公开访问的目录、网站的 WEB 管理界面入口及以前曾经公开过但后来被隐藏的链接。WAF 提供细粒度的 URL ACL，防止对这些链接的非授权访问。
3. 网站隐身：过滤服务器侧出错信息，如错误类型、出现错误脚本的绝对路径、网页主目录的绝对路径、出现错误的 SQL 语句及参数、软件的版本、系统的配置信息等，避免这些敏感信息为攻击者利用、提升入侵的概率。
4. 对数据泄密具备监管能力。能过滤服务器侧响应内容中含有的敏感信息，如身份证号、信用卡号等。

2.5 实施与运营流程

绿盟 WAF with MSS 的实施与运营大致分为 5 个步骤来保障用户网站业务安全运行，即：信息采集与设备部署、安全基线设置、Web 攻击监测、Web 攻击响应、安全报告交付。同时，绿盟 WAF with MSS 灵活的实施与运营流程可运用于政府、运营商、金融、能源等企事业单位的安全运营体系中。

图 2.5　绿盟 WAF with MSS 实施与运营流程

2.6 典型部署

绿盟 WAF with MSS 可以应用于政府、运营商、金融、能源等企事业单位的 DMZ 区或数据中心。在本方案中，用户通过绿盟 WAF with MSS 可实现将分布在各地的 WAF 设备与绿盟安全云、安全专家团队的对接和同步，由绿盟安全专家团队对各处的业务系统统一进行 7x24 小时全天候的 Web 应用安全监护，协助用户降低 Web 应用安全风险。

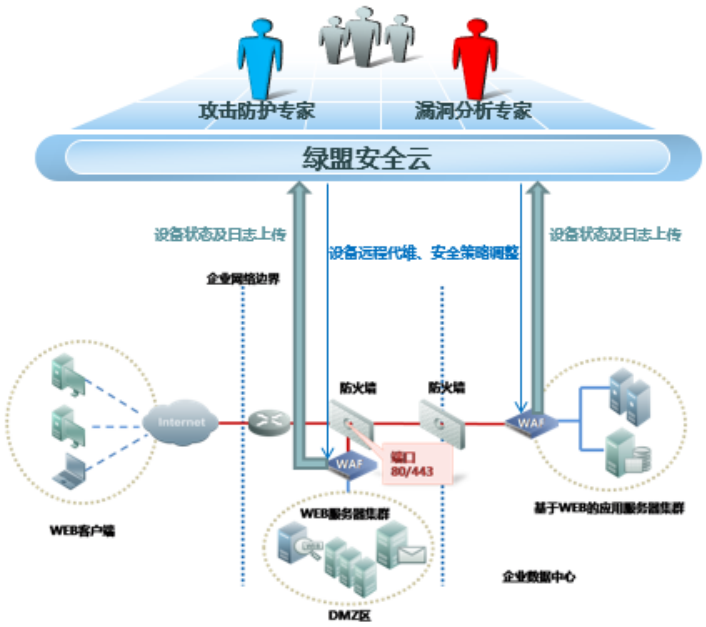

图 2.6　绿盟 WAF with MSS 在线部署模式

在部署了多业务网段服务器的网络环境中，绿盟 WAF with MSS 也可以采用旁路方式部署，提供一种逻辑在线防护机制。该种部署灵活性较好，可以实现业务分流，对核心系统影响较小。旁路方式部署的技术原理如下：

1. **流量牵引：**通过路由方式，将原来去往目标网站 IP 的流量牵引至 WAF 设备。被牵引的流量为攻击流量与正常流量混杂的 HTTP 流量；
2. **流量检测和过滤：**WAF 设备通过多层的攻击流量识别与净化功能，将 Web 攻击流量从混合流量中过滤；
3. **流量注入：**经过 WAF 过滤之后的合法流量被重新注入回网络，最终到达目的网站。
4. **对返回流量检测：**网站响应的 HTTP 流量在返回给客户端之前，仍然需要流经 WAF 设备，WAF 可提供安全检测，经 WAF 检测后的流量最终返回给客户端。

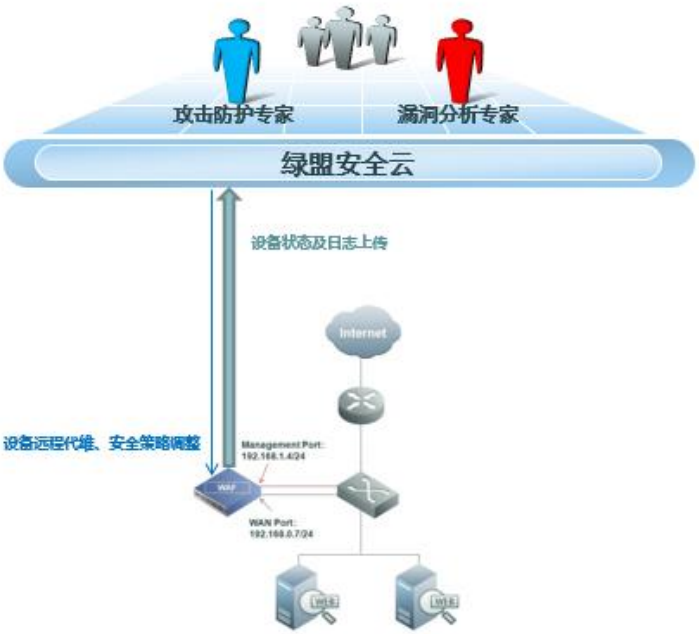

图 2.7　绿盟 WAF with MSS 旁路部署模式

三. 客户利益

◆ **最大限度降低 Web 应用安全风险**

绿盟 WAF with MSS 可以帮助用户将本地 WAF 设备与绿盟安全云对接和同步，由安全专家团队对网站安全隐患和遭受的攻击威胁进行全天候监控，发现 Web 攻击事件，第一时间分析、响应和防护，最大限度降低 Web 应用安全风险。

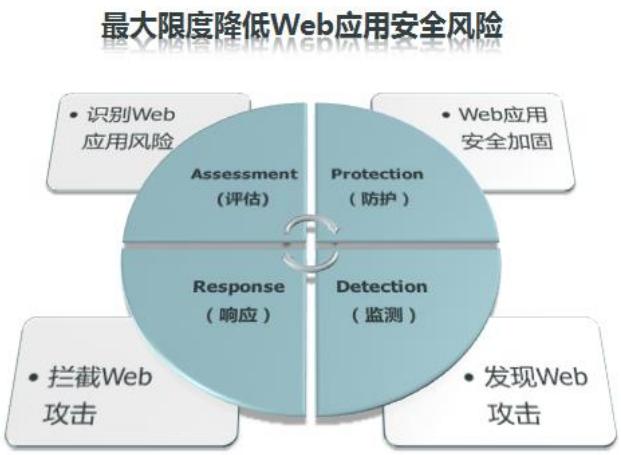

图 3.1　绿盟 WAF with MSS APDR 模型

◆ **有更多精力专注于核心业务**

用户通过绿盟 WAF with MSS，可以将 WAF 设备接入绿盟安全云，由绿盟安全专家团队 7x24 小时远程维护，设备监控、系统升级、故障排查、配置调整等工作完全不用自己操心，可以大大减少自身的安全设备维护工作量，从而能够将更多的精力专注于核心业务的发展。

◆ **提升自身团队安全能力**

Web 应用攻防，归根结底还是人与人在经验和智慧上的对抗。用户通过绿盟 WAF with MSS，可以直接获得绿盟安全专家团队丰富且专业的知识、技能和经验，无需从零开始培养安全人员，能够在短时间内快速提升自身团队安全能力，增强抗 Web 攻击能力。

四. 总结

随着 Web 应用的丰富，各类攻击工具不断的普遍和强大，互联网上的安全隐患越来越多。随着客户核心业务系统对网络依赖程度的增加，Web 应用攻击事件数量将会持续增长，损失严重程度也会剧增。因此，政府、运营商、金融或是企业等各类组织都必须有所对策，以保护其投资、利润和核心业务。

为了弥补目前 Web 应用攻击防护方案的不足，我们需要一种完善的解决方案以保护重要信息系统不受 Web 应用攻击的影响。这种解决方案不仅能够检测目前复杂的 Web 应用攻击，而且必须在不影响正常业务流量的前提下对攻击流量进行实时阻断。这类解决方案相对于目前常见的安全产品，必须具备更细粒度的攻击检测和分析机制。

绿盟 WEB 应用防护系统（可管理系列）（NSFOCUS WAF with MSS）是绿盟科技在优秀的 WAF 产品基础上，进一步融合安全云平台技术，推出的 7x24 小时 Web 应用安全解决方案。绿盟 WAF with MSS 凝聚着绿盟安全专家团队的集体智慧，提供了业界领先的 Web 应用攻击防护能力，保证 Web 应用的连续性和高可用性。同时，针对当前的热点问题，如 SQL 注入攻击、网页篡改、网页挂马、敏感信息泄漏等，绿盟 WAF with MSS 提供最佳的安全-成本平衡点，有效降低 Web 应用安全风险。