360 安域 Web 安全云防护系统

产品白皮书

目录

第一章　产品概述

随着越来越多的行业逐渐向“云”端过渡，适用于不同行业的“私有云”或者“公有云”解决方案层出不穷，随之而来的挑战就是大数据的集中存储和集中分析。特别是随着办公信息化、企业信息化的普及，很多政务系统、OA 系统以及其他对外信息发布系统的上线，也产生了日益庞大的数据。这些数据中不仅仅包含了正常业务数据同时也包含大量的网络攻击行为。大数据作为“未来的新石油”,为我们提供了很多信息的金矿。未来的网站安全服务市场,一定是一个基于云服务的安全运维管理平台。在云计算、IT 服务化日渐普及的今天,企业及成员单位网站迫切需要专业化的队伍供全面的、专业的网站安全保护服务。

360 安域 Web 安全云防护系统,是奇虎 360 公司为国有大中型企业定制的“网站安全防护私房菜”:根据企业的实际需求及网络现状,将 360 网站卫士、360 智能 DNS 系统和运维监控平台、360 网站安全检测系统、360 安域大数据分析系统迁移到企业 Web 安全云防护系统,并整合为一体化云安全管控平台,为企业网站　供网站防火墙、CDN 加速、抗 DDoS、自动化运维、大数据安全分析等功能。

第二章　安域多维安全模型

2.1　传统与现代的产品

传统基于闭环控制的 P2DR 动态安全理论模型，只提供了保护、检测、响应、策略四种安全能力，认为通过定义系统的监控周期、利用各种检测工具、通过各种安全防护手段，再配合有效的响应，就能解决安全问题。

大数据时代，信息的规模和产生的速度已然大大增加，必须辅助于基于大数据的分析技术和基于云的管理能力，使安全从 P2DR 四种安全能力扩展到 P2DRM2A 七种安全能力，真正解决了整个 WEB 业务生命周期的全生命周期的安全问题。

2.2 云防护

加入安域云安全管控平台的网站进行安全云防护,其中包括 Web 入侵防护、DDoS 防护、CC 防护、DNS 防护等,确保网站在保护下不被入侵和攻击瘫痪。

2.3 多 WEB 业务一体化管理

集中管理企业网站及下属成员网站,将企业网站、成员单位网站等相关网站纳入中心集中管控,在各个网站拥有独立的管理权限的同时,由企业管理员直接进行管理,提供网站可信认证、安全防护、实时监测等云平台级安全服务,并根据相应网站安全等级督促整改,全面提高企业整体网络安全环境,同时行成管控、系统监控和攻击监控及时反馈各网站当前运行稳定状况,及时响应攻击事件并详细定位至具体网站,并自动进入防御模式,实时分析攻击数据进行攻击反跟踪,定位出攻击来源与攻击目标。

2.4 大数据安全分析平台

大数据分析提供企业 Web 安全云防护系统网站的日常数据统计、攻击数据统计、未知威胁攻击的挖掘和攻击回溯来源分析,云安全中心将于云端数据实时同步, 以图形化的方式展示,管理员可对历史攻击数据进行自定义查询和提取报告。

第三章 安全理念

3.1 颠覆传统

传统设备中每个设备只是单独的个体，孤岛作战情况严重，遇到问题时职能被动的防御。360 安域集群防御、协同作战、主动防御的三大安全理念，能够很好应对云时代的安全新挑战。

3.2 集群防御

通过云计算与大数据技术，用集群化防御体系来代替传统的单点防御体系，颠覆了现有安全防护理念，通过平台提供便捷的集中管控和统一的安全配置、业务监控和数据分析能力。

3.3 协同作战

利用 360 在终端安全和云安全方面的绝对领先优势，利用基于全球视野而聚焦中国的威胁情报系统，提出了云+端+边界协同作战的思想，通过消灭设备孤岛从而消灭了安全孤岛，为整体的 WEB 业务提供整体的安全。

3.4 主动防御

充分利用云端安全 CDN 的流量清洗能力和攻击样本检测能力，实时动态升级防御规则无需人工参与，提供整体安全威胁态势感知能力，超越传统被动防护理念。

第四章　核心功能

4.1 智能云防护

采用 360 核心安全技术、企业级防 DDOS 设备、650G 国内顶级流量带宽储备，实时检测并拦截跨站、注入、篡改、挂马、黑客攻击，替您抗住一切威胁，让 WEB 业务固若金汤。

4.2 智能云缓存

基于全国 15 个 IDC 骨干节点，无限制缓存网站静态文件、智能压缩、动态 CDN 路由选路，并且对主流搜索引擎爬虫进行分析，在 DNS 层面将搜索引擎流量直接回源，充分保障网站业务的搜索收录。

4.3 高防智能 DNS

基于 360 自研的高防智能 DNS，提供 10-100G 不同等级的 DNS 攻击流量清洗服务，从容应对各种 DNS 攻击，自动切换故障服务器，减少运维人力和时间成本。

4.4 大数据安全分析

全网实时大数据分析系统，为用户展示网站访问数据和攻击防护数据，并提供全网攻击态势感知能力，能够实时监控全球或全国范围内的互联网黑客攻击趋势，同时提供安全周报功能，自动全面评估业务线安全状况。

4.5 智能安全管理

支持将单个或多个网站域名统一接入防护平台，提供全面 WEB 业务系统的统一管理视图，通过设置 IP 黑/白名单，结合时间、域名、URL 等维度，实现灵活的网站访问控制。

第五章　产品优势

5.1 强大的用户基础

360 服务 4 亿 PC 终端用户、7 亿移动终端用户的安全经验和解决各种复杂安全问题的能力，拥有强大用户资源和用户基础将为企业提出最好的解决方案和解决方法，对网站钓鱼和危险网站的拦截达到最高的效果。

5.2 全国最大的企业防护积累

360 通过服务国内的 120 万个网站，云防护体系已经累积了多年攻防实战经验，通过这些经验安域可以从容面对各种形式的攻击。

5.3 等同 360 的防护级别

安域体系是由的 360 本身的 Web 安全体系产生出来的，提供与 360 自身业务

同样的安全防护等级，拦截 99%以上的黑客漏洞攻击。

5.4 顶级云资源

全国利用了提 5 个 IDC 节点，200+万兆 LVS 负担均衡服务器，100+ WAF 服务器，100+Cache 服务器的顶级云资源。

5.5 专业的防 CC 攻击

提供专业的 5 秒识别 CC 攻击能力，实时拦截基于 HTTP 协议的流量攻击。

5.6 企业级防 DDOS 攻击

提供企业级防 DDOS 设备，全国 450G 带宽储备，抵御一切流量攻击。

5.7 高防 DNS

提供高防 DNS 集群，可提供 10G-100G 不同等级的 DNS 流量清洗服务。

第六章 总结

产品功能方面：安域不同于传统的网站防护设备，利用虚拟化技术形成 DDOS 防护、CC 攻击防护、web 攻击防护、DSN 防御于一体的颠覆性立体话的 Web 安全防护体系。

安全防护方面：能有效防护常见的 Web 漏洞攻击，并能够识别多种变型攻击方式，同时能有效针对 DDoS 攻击和 CC 攻击进行防护。

我们相信 360 安域会在不断的更新中做到更好的服务更强大的安全防御功能，为您的业务带来最极致的保护。