WEB-APT 检测系统

白皮书

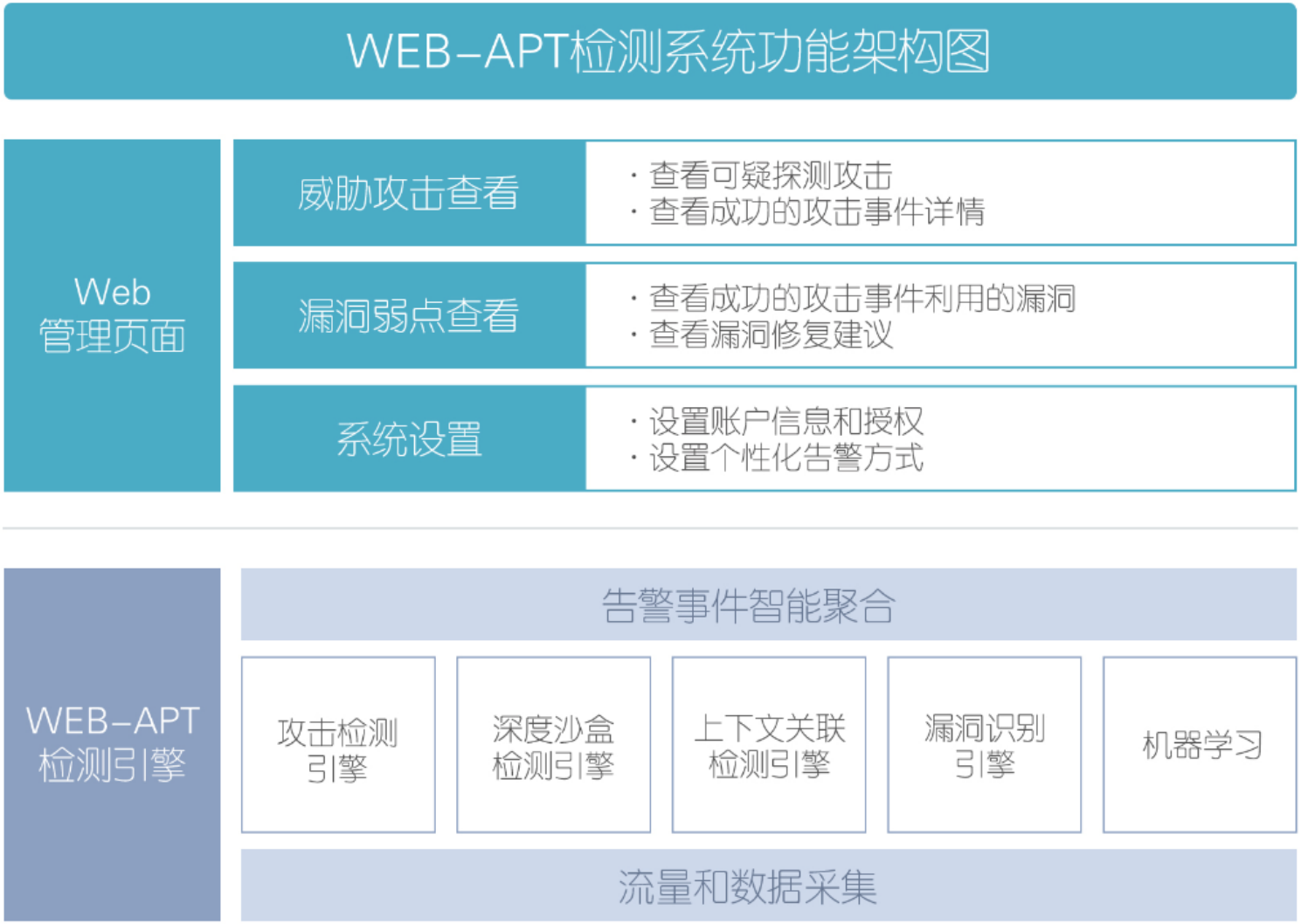
产品简介

根据 Gartner（全球最具权威的 IT 研究与顾问咨询公司）的最新调查，在保护 Web 应用程序的市场上， Firewalls、IPSs 的份额正在逐年递减，并且 Gartner 预测：2018 年末，二者的市场份额会从现在的 40%降到不足 20%。

如今，随着互联网和云计算技术的高速发展，黑客们已将注意力从以往对网络服务器的攻击逐步转移到了对 Web 应用的攻击上，利用先进的攻击手段对特定目标进行长期持续性网络攻击，而且经常使用 0day 漏洞来发起未知攻击。

WEB-APT 检测系统（WEB 高级威胁检测系统），是百度云安全基于“全流量镜像技术”及“大数据处理技术”研发的一套智能 Web 入侵检测与威胁感知系统，专注于识别 Web 应用攻击，能够深度挖掘黑客针对 Web 的拖库、远程命令执行、敏感文件泄露、Webshell 后门等攻击事件并发出准确的报警。

产品架构


WEB-APT检测系统功能架构图
Web
管理页面
威胁攻击查看
· 查看可疑探测攻击
· 查看成功的攻击事件详情
漏洞弱点查看
· 查看成功的攻击事件利用的漏洞
· 查看漏洞修复建议
系统设置
· 设置账户信息和授权
· 设置个性化告警方式
WEB-APT
检测引擎
告警事件智能聚合
攻击检测
引擎
深度沙盒
检测引擎
上下文关联
检测引擎
漏洞识别
引擎
机器学习
流量和数据采集

产品特色

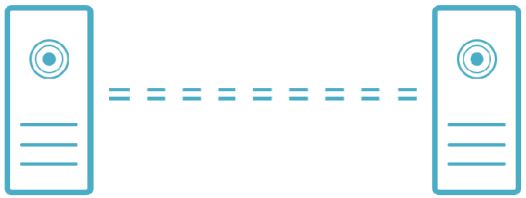
WEB-APT 检测系统的核心价值是运用先进的沙箱、机器学习以及人工智能等技术，为客户及时发现危害严重的数据库盗取、敏感文件下载、系统受控等攻击事件，并发出准确的报警。

1、精准

1.1 双向流量，精准规则

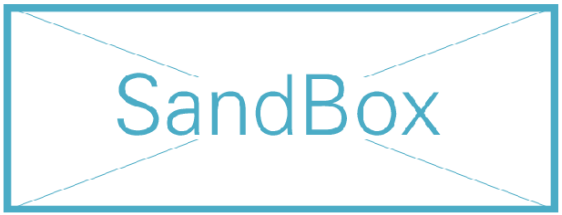
WEB-APT 检测系统基于全流量镜像技术部署于交换机的镜像端口，实时获取目标服务器的所有 HTTP 请求及响应的双向数据包，包含爬虫无法覆盖的移动端 APP 流量数据。

WEB-APT 检测系统基于百度十六年甲方安全经验积累的精准规则，完整还原用户访问的整个过程，双向分析请求与应答内容，力求精准检测，并聚合同一黑客的同一次攻击行为，大大减少报警量。



1.2 沙箱技术

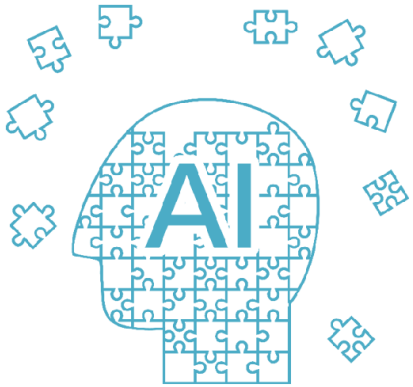
WEB-APT 检测系统在特殊的文件行为识别上采用了沙箱技术， 百度自研的 PHP、JSP 沙箱都已获得专利，可以在支持的沙箱中‘引爆’文件，通过文件行为识别恶意攻击；



2、智能

WEB-APT 在攻击识别上不再依赖于传统的规则检测，通过机器学习，结合由百度云安全专家及百度 IDL 专家共同构建的异常数据神经网络数据分析模型，分析异常数据，识别出黑客攻击，甚至是未知攻击。目前，分析模型日处理数据达数十 TB，产出异常十几 MB，准确率达 90%以上。

在 2015 年，WEB-APT 检测系统所采用的异常数据神经网络数据分析模型，通过全网百万级访问行为分析，发现一起大规模的地下 CC 攻击团伙，并发布了《从异常挖掘到 CC 攻击的地下团伙》报告。在文章发布三天之后，同行业公司报出同样的监测结果。



3、漏洞被动感知（PVS）

WEB-APT 检测系统 内置了 Web 漏洞指纹库,通过分析 HTTP 双向数据包，有效识别数百种 Web 漏洞，整个过程不会产生任何流量。当黑客发现 Web 漏洞时，WEB-APT 检测系统也能根据数据包的特征发出漏洞预警。支持的漏洞类型包括，SQL 注入攻击、文件上传、命令执行、敏感信息泄露等，并覆盖 95%以上的常见 Web 应用框架。

经过实际测试，PVS 检测各类扫描器的漏洞确定行为的同步检出率不低于 85%，对漏洞触发(漏洞利用)的同步检出率不低于 90%。

4、网络资产自识别

WEB-APT 检测系统通过分析所有 HTTP 请求及响应的双向数据包，可以学习到客户的网络架构和资产列表。WEB-APT 检测系统与扫描器和爬虫的区别是，只要客户流量中发生过的访问，全部可以识别，再基于学习到的网络资产，进一步分析是否存在由运维配置不当导致的弱点信息，如运维平台弱口令，管理平台对外等非漏洞问题导致安全威胁。

产品规格

技术指标	WEB-APT 检测系统
攻击检测类型	SQL 注入
	命令执行
	代码执行
	webshell 上传
	任意文件读取下载
	文件包含
	敏感信息泄露
网络资产识别	支持常见的 1000 种开源软件及开发框架
报表数据	支持查看告警事件，完整展示攻击链行为日志
支持协议	HTTP、MySQL

部署模式	旁路部署，分布式部署
	不依赖硬件，运行安装 Centos6.6 和 6.7 即可
网络处理能力	单机支持双向 200Mb 到 2Gb 流量
	集群支持双向 40G 流量
告警通知	邮件、微信、短信通知
维护成本	零维护
服务时间	7*24 小时服务
技术支持	管家式安全专家团队支持

百度云安全介绍

概况

- 百度云安全是国内领先的面向互联网企业的网站加速、安全防护和搜索引擎优化服务提供商，旗下包括百度云加速、百度安全宝、百度云观测、百度云分析等多个产品。我们致力于为云端网络安全和性能提升，帮助企业维护业务的快速、可靠运行，给用户带来更安全、更快速的体验。

- 2015 年 4 月，百度收购安全宝，百度云安全市场份额超过 30%，是国内拥有最多客户资源的企业网络应用安全保护平台，同时也加大了对企业客户全方位的服务能力。未来，百度云安全除了为企业客户提供安全及加速服务，还将进一步提供搜索推广、建站服务和大数据等全方位支持，为企业提供从入网建站到安全防护、搜索推广到客户挖掘等全产业链的企业服务。

百度云加速

百度云加速是为网站提供网络加速、安全防护和搜索引擎优化等一站式服务的管理平台，在全国骨干网上部署大量节点和带宽资源，整合百度自有 CDN 技术以及防攻击体系，为广大网站提供加速、缓存和页面优化等功能，网站平均提速 2 倍以上。此外，流量经过百度云加速节点的同时，恶意的黑客攻击和 DDoS/CC 攻击也会被拦截过滤掉，有效保障网站的安全和稳定。

安全宝

百度安全宝是国内第一家完全基于 SaaS 模式为用户提供安全防护服务的云安全服务品牌。百度安全宝独特的“替身式”安全理念，能帮助用户以较低的资金和运维投入，大幅提升网站安全性、访问速度和高可用性(HA)，解决黑客入侵(SQL 注入、XSS 等)、DDoS、CC 攻击等各类安全问题。同时，通过安全宝在中国首创融合 CDN 的安全网络，可以在保障用户安全性的同时，让用户网站速度不但没有下降，反而有 30%-200%的提升。目前，百度安全宝已经与国内主流云平台以及 AWS 中国达成安全服务合作。

如需了解安全宝的更多信息，请浏览 http://www.anquanbao.com

地址：海淀区上地十街 10 号百度大厦,100085
服务热线：400-80-54999　邮箱：INQUIRE@ANQUANBAO.COM