智恒科技

WebGuard网页防篡改保护系统介绍

北京智恒网安科技有限公司
www.zhihengit.com

网页防篡改形势依然严峻

智恒科技

2018年12月| CNCERT互联网安全威胁报告第96期

原创：CNCERT 国家互联网应急中心CNCERT 今天

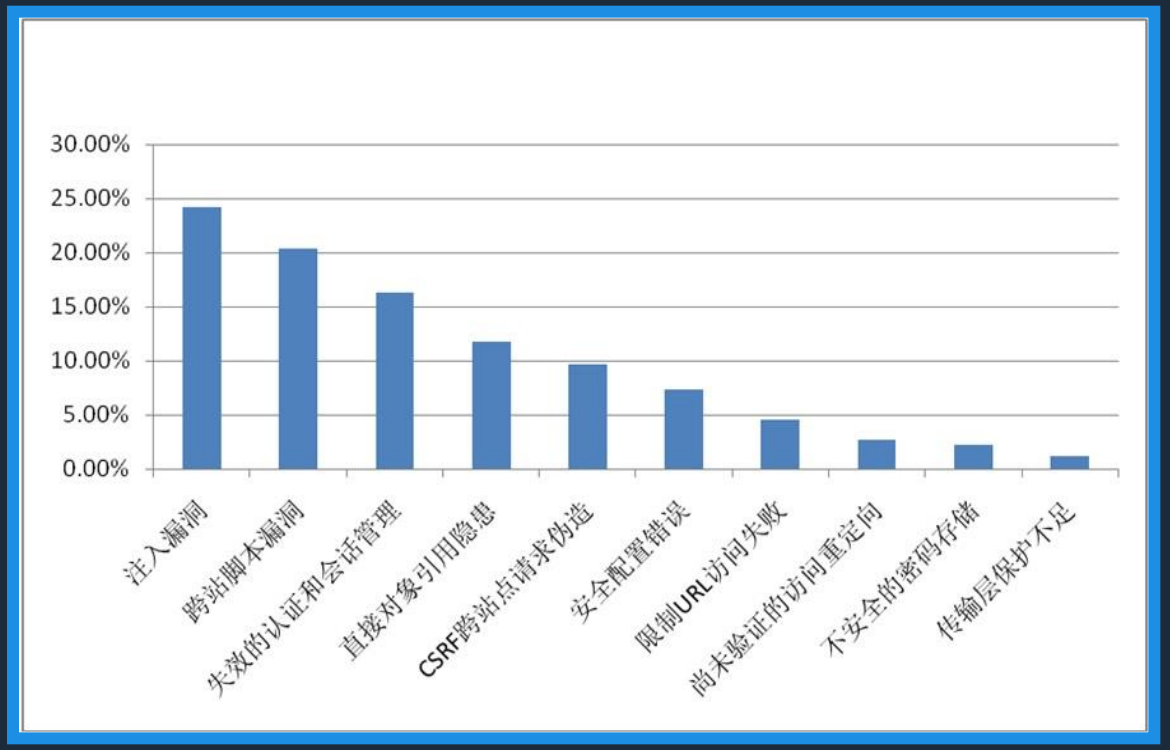
本报告以CNCERT监测数据和通报成员单位报送数据作为主要依据，对我国互联网面临的各类安全威胁进行总体态势分析，并对重要预警信息和典型安全事件进行探讨。

2018年12月，互联网网络安全状况整体评价为良。主要数据如下：

➢境内感染网络病毒的终端数为近78万个；

➢境内被篡改网站数量为1,376个，其中被篡改政府网站数量为80个；境内被植入后门的网站数量为2,317个，其中政府网站有34个；针对境内网站的仿冒页面数量为5,324个；

➢国家信息安全漏洞共享平台（CNVD）收集整理信息系统安全漏洞1,206个，其中，高危漏洞481个，可被利用来实施远程攻击的漏洞有1,067个。



注：广义上的网页防篡改包含被植入后门等操作；

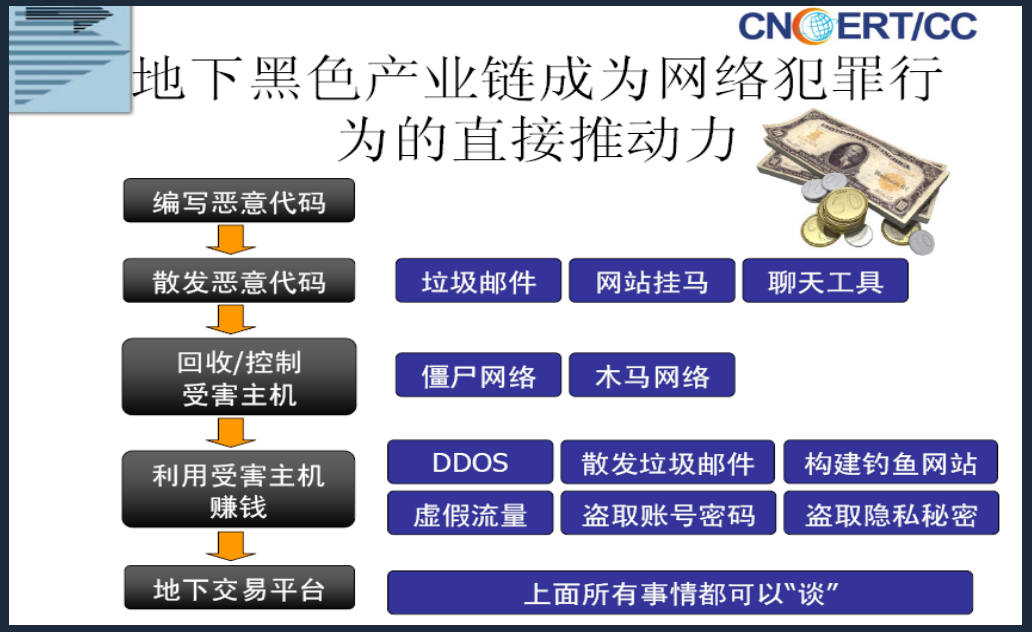
网站被篡改的原因

智恒科技

- 网站应用的复杂性导致编程漏洞增多；
- 传统防火墙、入侵检测等措施突出在网络层防护，但对应用层防护细粒度不足。

- 大多存在侥幸心理，未引起足够重视；
- 没有意识到遭受篡改后的危害性；
- 没有消除最根本原因，从而遭到多次篡改。

网络攻击的发展趋势



网络攻击的发展新趋势

- 技术炫耀型转向**利益驱动**型。
- **黑产庞大**，具有组织性、专业性。
- 恶意代码和在线**数据窃取**成为主流。
- 瞄准特定用户群体的**定向化**信息窃取和威胁。

网站安全相关的处罚

智恒科技

安徽网警依法查处一起违反网络安全等级保护制度案件

8月12日，蚌埠怀远县教师进修学校网站因网络安全防等级保护制度落实不到位，遭黑客攻击入侵。蚌埠市公安局网安支队调查案件时发现，该网站自上线运行以来，始终未进行网络安全等级保护的定级备案、等级测评等工作，未落实网络安全等级保护制度，未履行网络安全保护义务。根据《网络安全法》第五十六条之规定，省公安厅网络安全保卫总队约谈怀远县教师进修学校法定代表人、怀远县人民政府分管副县长。蚌埠市局网安支队依法对网络运营单位怀远县教师进修学校处以一万五千元罚款，对负有直接责任的副校长处以五千元罚款。

发布于：http://www.sohu.com/a/167329934_784435

执法机构：安徽省公安厅网络安全保卫总队；蚌埠市局网安支队

处罚行为：网站因网络安全防等级保护制度落实不到位，遭黑客攻击入侵。

处罚措施：约谈怀远县教师进修学校法定代表人、怀远县人民政府分管副县长；对网络运营单位怀远县教师进修学校处以一万五千元罚款，对负有直接责任的副校长处以五千元罚款。

法律依据：《网络安全法》第21条、56条、第59条第1款。

国内首例高校违法案例诞生，因未落实等保制度致学生信息泄露

9月28日，淮南市网络与信息安全信息通报中心接到国家网络与信息安全信息通报中心通报：淮南职业技术学院系统存在高危漏洞，系统存储的4000余名学生身份信息已经造成泄露。经查，确认淮南职业技术学院招生信息管理系统存在越权漏洞，后台登录密码弱口令，学院未落实网络安全管理制度，未建立网络安全防护技术措施、网络日志留存少于六个月，未采取数据分类、重要数据备份和加密措施，致使系统存储的4353名学生的身份信息泄露。

10月12日,安徽省淮南市网警巡查执法官方微博发布通报称，关于淮南职业技术学院未落实网络安全等级保护制度，导致4000余名学生身份信息泄露一事，淮南市公安局网安支队依法对该学院处以立即整改和行政警告的处罚措施。

发布于：http://server.zzidc.com/a/cio/2017/1013/2126.html

执法机构：淮南市公安局网安支队

处罚行为：淮南职业技术学院招生信息管理系统存在越权漏洞，后台登录密码弱口令，未落实网络安全管理制度，未建立网络安全防护技术措施、网络日志留存少于六个月，未采取数据分类、重要数据备份和加密措施，致使系统存储的多名学生身份信息泄露。

处罚措施：责令整改，警告

法律依据：《网络安全法》第21条、第59条第1款。

处罚只会越来越频繁！
越来越严厉！

Webguard系统优势突出

- 技术先进，采用**第三代**防篡改技术，成熟、稳定、可靠；
- 包含应用**攻击防护模块**，有效防止SQL、XSS等各类应用攻击；
- 效率较高，对服务器资源消耗低于**2%**，远高于同类产品 ；
- 汲取广大网管员建议，**操作简便**，大大提高工作人员效率；
- 系统运行于操作系统低层，与Web应用无关，**任意扩展**；
- 全国数以千计的成功应用案例。

文件保护驱动原理图

智恒科技

防篡改的技术变迁

智恒科技

原始阶段

0

人工对比

中级阶段

1

时间轮巡技术

高级阶段

2

事件触发+
水印技术

多因子检测时代

3

事件触发+
过滤驱动技术

防篡改的技术对比

智恒科技

关键对比类别	第二代防篡改技术	第三代防篡改技术
防护机制	篡改后的恢复机制，且是当有外部请求时触发恢复	完全杜绝修改，被修改还能居于触发机制实时恢复
核心技术	密码水印技术	文件驱动保护
工作协议层	应用层，效率低，消耗资源较大	系统层，效率高，对系统资源极少量消耗
对web服务类型支持程度	有依赖性	与web服务无关
使用方便性	使用操作复杂	操作简单

防篡改与WAF的技术对比

智恒科技

关键对比类别	防篡改技术	WAF技术
针对网站文件的防护	杜绝文件篡改	无
针对数据库的防护	通过动态访问模块实现	支持
针对篡改后的行为	完全杜绝修改	通过扫描原始文件比对方式，效率较低
其他功能	无	可实现部分抗DDOS攻击
对web服务器效率的影响	几乎无影响	一定程度上降低效率，且是网关设备，存在单点故障可能

WebGuard系统的亮点

智恒科技

- 系统底层技术
- 安全加密传输
- 动态网站的防护
- 支持断线检测
- 多角色用户管理

- 文件过滤驱动保护技术
- 快速同步通道
- 自动快速生成拓扑图
- 代码严谨

- 策略导入与导出；
- 进程黑白名单管理
- 多种告警方式
- 丰富的日志报表
- 支持跨平台同步与管理

- 支持分布式部署
- 双机冗余部署
- 最大限度支持多级文件夹
- 多系统无缝集成

安全性 + 高效性 + 多功能性 + 可扩展性

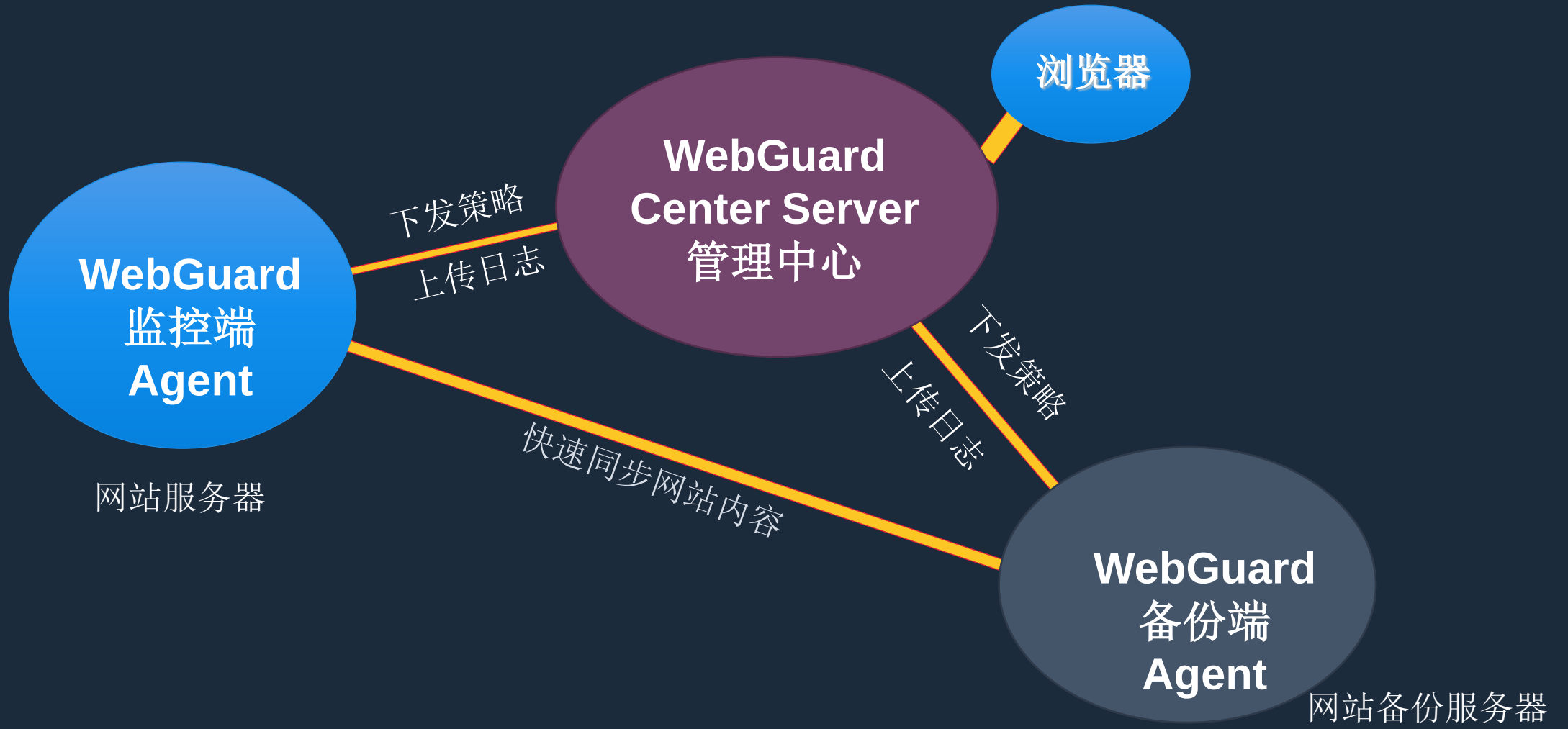
WebGuard

for

any Web Server

WebGuard系统组件架构示意图

智恒科技



WebGuard可选组件-动态防护模块websec

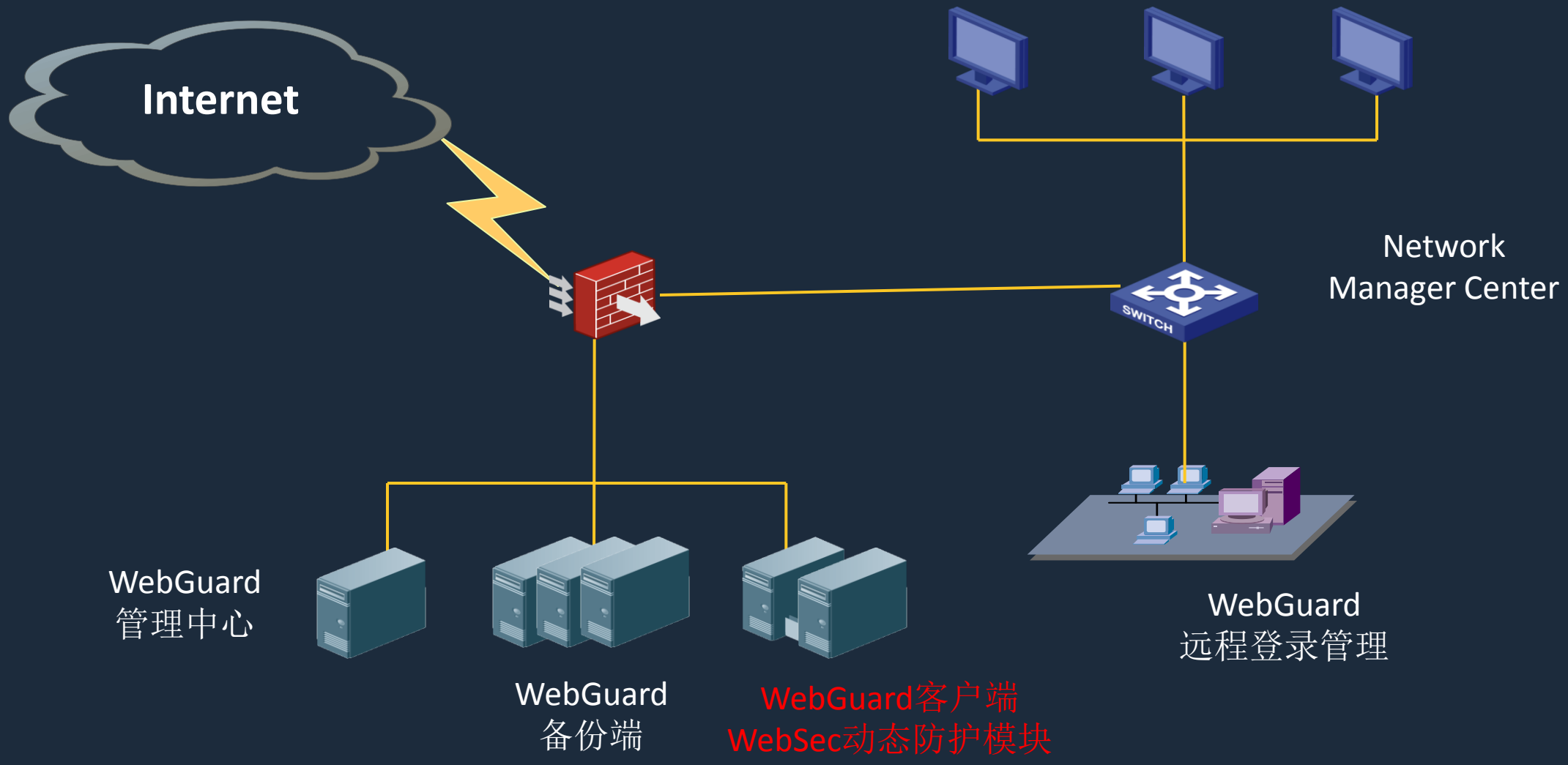
- 支持SQL注入攻击防护；
- 支持跨站脚本攻击防护；
- 支持对系统文件的访问防护；
- 支持特殊字符构成的URL利用防护；
- 支持对危险系统路径的访问防护；
- 支持构造危险的Cookie攻击防护；
- 各类攻击的变种防护；
- 支持自定义检测库；

WebGuard管理中心

智恒科技

WebGuard部署示意图

智恒科技

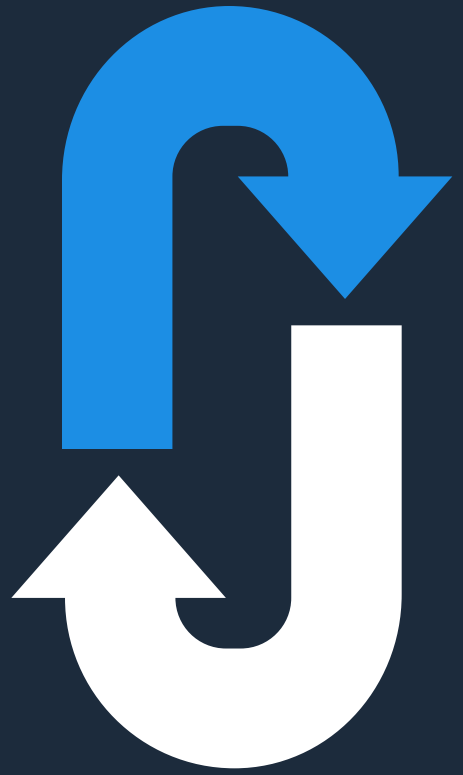


WebGuard部署常见两种策略

智恒科技

方式一：常规部署模式

✓需在内网更新网站内容或外网通过VPN接入内网更新；
✓适用于大规模网站的部署或实体服务器；



方式二：仅保护模式

✓无需安装备份端程序，通过许可进程更新页面内容，更新完内容后需 及时刷新开启保护策略；
✓适用于中型网站部署或公有云环境；

WebGuard资质证书

智恒科技

计算机信息系统安全专用产品

销售许可证

证书编号 0504190434

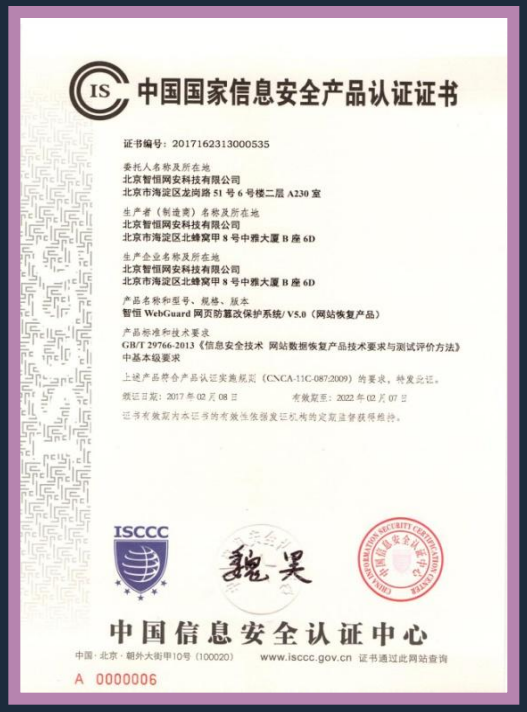
北京智恒网安科技有限公司：

根据公安部《计算机信息系统安全专用产品检测和销售许可证管理办法》及有关规定，经审查，准许你单位生产（代理）的 智恒 Web 网站安全防护系统 V5.0 网站数据恢复产品（基本级） 安全专用产品进入市场销售，特发此证。

有效期自 2019 年 04 月 08 日至 2021 年 04 月 08 日

2019 年 04 月 08 日

中华人民共和国公安部监制



中国国家信息安全产品认证证书

证书编号：2017162313000535

委托人名称及所在地
北京智恒网安科技有限公司
北京市海淀区龙岗路 51 号 6 号楼二层 A230 室

生产者（制造商）名称及所在地
北京智恒网安科技有限公司
北京市海淀区北蜂窝甲 8 号中雅大厦 B 座 6D

生产企业名称及所在地
北京智恒网安科技有限公司
北京市海淀区北蜂窝甲 8 号中雅大厦 B 座 6D

产品名称和型号、规格、版本
智恒 WebGuard 网页防篡改保护系统/V5.0（网站恢复产品）

产品标准和技术要求
GB/T 29766-2013《信息安全技术 网站数据恢复产品技术要求与测试评价方法》中基本级要求

上述产品符合产品认证实施规则（CNCA-11C-087:2009）的要求，特发此证。

颁证日期：2017 年 02 月 08 日　　有效期至：2022 年 02 月 07 日

证书有效期为本证书的有效性依据认证机构的定期监督获得维持。

ISCCC

中国信息安全认证中心

中国·北京·朝外大街甲10号（100020）　www.isccc.gov.cn　证书通过此网站查询

A 0000006

证书号第 7893335 号

实用新型专利证书

实用新型名称：一种网站安全管理系统

发明人：杨峰;尹智庆

专利号：ZL 2018 2 0289107.6

专利申请日：2018 年 03 月 01 日

专利权人：北京智恒网安科技有限公司

地址：100038 北京市海淀区龙岗路 51 号 6 号楼二层 A230 室

授权公告日：2018 年 09 月 25 日　　授权公告号：CN 207910813 U

本实用新型经过本局依照中华人民共和国专利法进行初步审查，决定授予专利权，颁发本证书并在专利登记簿上予以登记。专利权自授权公告之日起生效。

本专利的专利权期限为十年，自申请日起算。专利权人应当依照专利法及其实施细则规定缴纳年费。本专利的年费应当在每年 03 月 01 日前缴纳。未按照规定缴纳年费的，专利权自应当缴纳年费期满之日起终止。

专利证书记载专利权登记时的法律状况。专利权的转移、质押、无效、终止、恢复和专利权人的姓名或名称、国籍、地址变更等事项记载在专利登记簿上。

局长
申长雨

2018 年 09 月 25 日

第 1 页（共 1 页）

中华人民共和国国家版权局

计算机软件著作权登记证书

证书号：软著登字第0730006号

软件名称：智恒WebGuard网页防篡改保护系统
[简称：WebGuard]
V5.0

著作权人：北京智恒网安科技有限公司

开发完成日期：2014年04月10日

首次发表日期：2014年10月16日

权利取得方式：原始取得

权利范围：全部权利

登记号：2015SR098934

根据《计算机软件保护条例》和《计算机软件著作权登记办法》的规定，经中国版权保护中心审核，对以上事项予以登记。

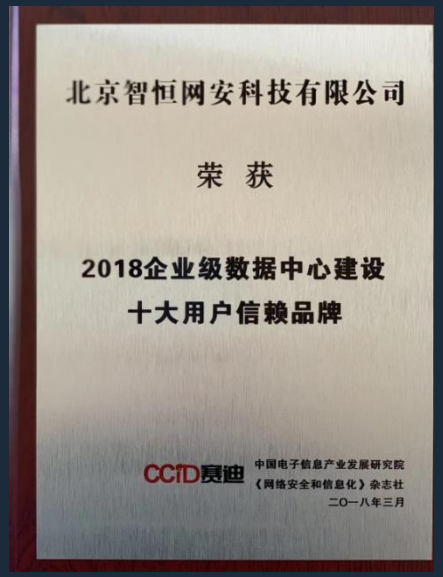
No. 00730006

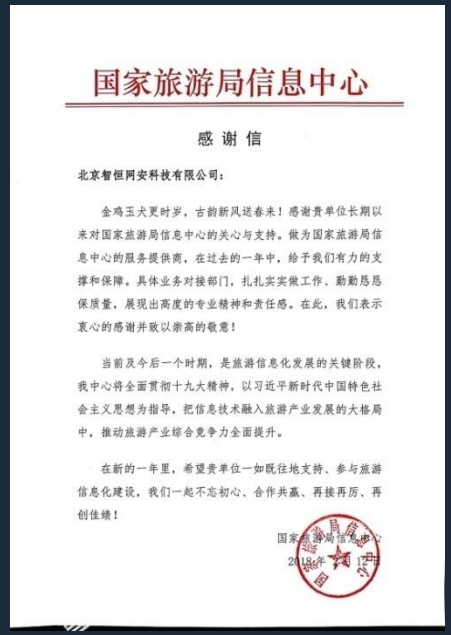
计算机软件著作权登记专用章

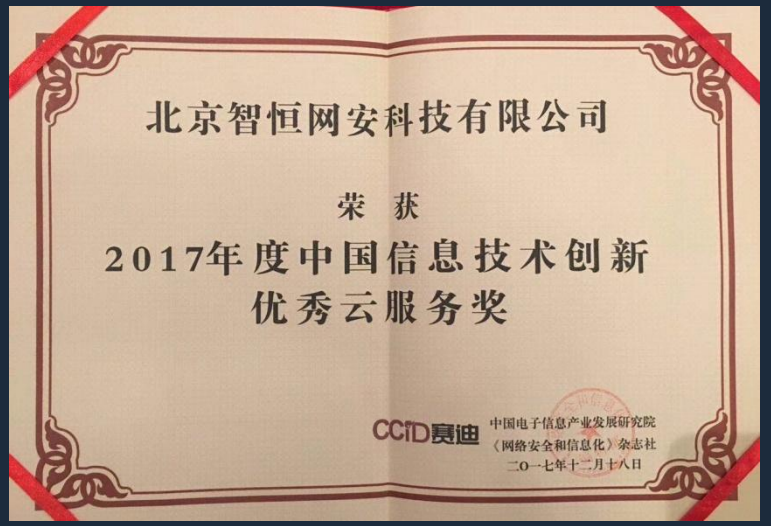
2015年06月01日

公司获得的资质、荣誉及感谢信

智恒科技

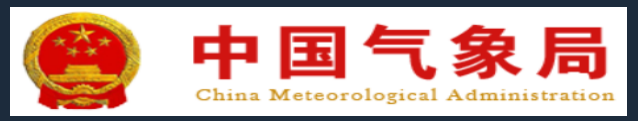


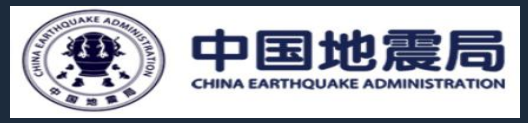




WebGuard获得全国数万用户好评

智恒科技





WebGuard已经累计部署10w+

公司参与的社会活动

智恒科技

谢谢聆听！

注：所有我们的网页防篡改购买用户将免费获得一次网站风险评估漏洞扫描服务。