省级政务云网络安全监测及安全运维汇报

CopyRight © 2013 Westone Co., Ltd. All rights Reserved.

目 录

CONTENTS

一 网络安全监测16年总览

二 统一安全运维17年工作计划

三 政务云平台安全Next...

CopyRight © 2013 Westone Co., Ltd.

一、网络安全监测总览

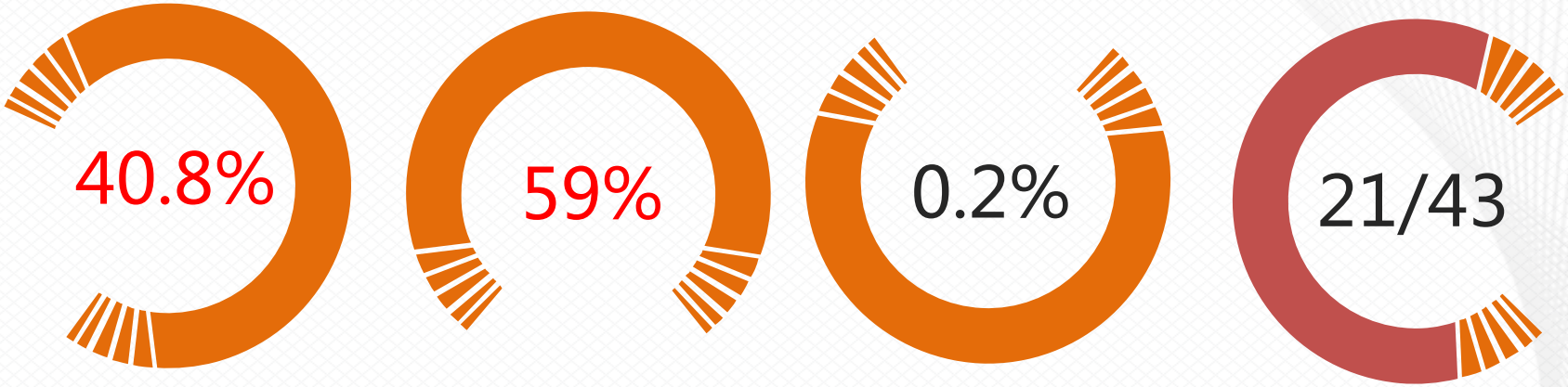
统一安全运维平台为省级政务云提供安全监测和防御

6,123,152 次

CopyRight © 2013 Westone Co., Ltd.

一、网络安全监测总览

事件区域分布



统一出口	云平台	云监管平台	用户/互联网网站
2,501,439	3,611,576	10,137	476

CopyRight © 2013 Westone Co., Ltd.

一、网络安全监测总览

统一出口事件分布

互联网出口

高风险：140，019（5.89%）

中风险：1，500，392（63.06%）

低风险：738，941（31.06%）

政务外网出口

高风险：466（0.38%）

中风险：51，046（41.81%）

低风险：70，575（57.81%）

CopyRight © 2013 Westone Co., Ltd.

一、网络安全监测总览

云平台事件分布

CopyRight © 2013 Westone Co., Ltd.

一、网络安全监测总览

事件级别分布

高风险

病毒木马告警
高危未知恶意代码
命令控制通信
暴力破解攻击
漏洞攻击
……

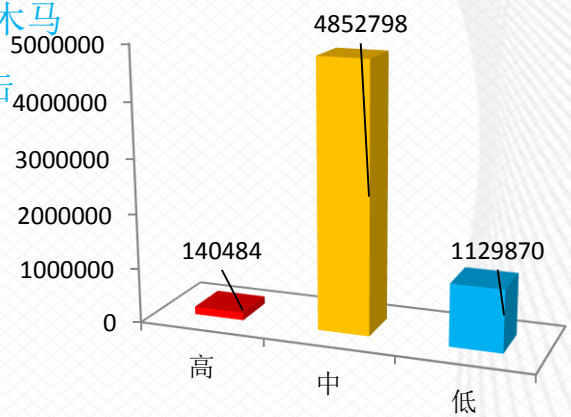
中风险

知名爬虫攻击
信息泄露
欺骗漏洞利用
黑客工具检测
……

低风险

端口扫描
口令猜测
疑似HTTP隧道木马
拒绝服务攻击
……

风险级别分布



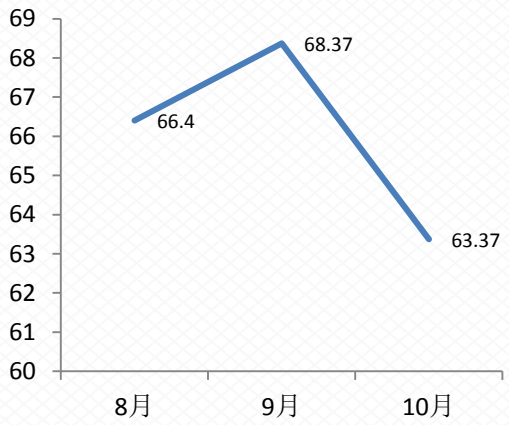
CopyRight © 2013 Westone Co., Ltd.

一、网络安全监测总览

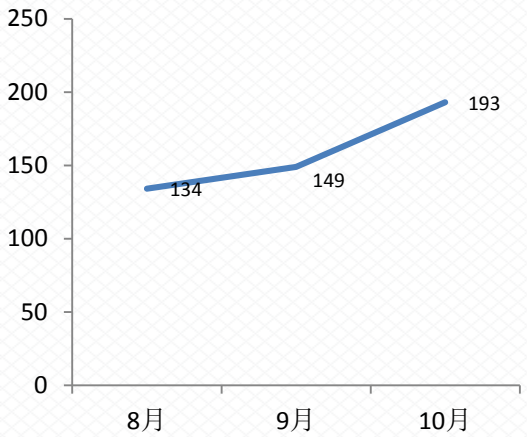
网站安全总览

共监测21家租户43个网站，网站整体得分66.05分，漏洞476个。

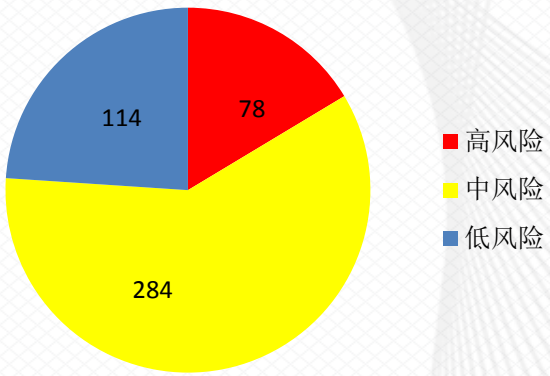
网站安全综合评分



网站漏洞个数



网站风险级别分布



CopyRight © 2013 Westone Co., Ltd.

一、网络安全监测总览

网站	实时监测	漏洞检测	挂马检测	暗链检测	断链检测	敏感字检测
[redacted]1:...	0		0个	⊗	⊗	⊗
[redacted]8...	0	75分	0个	⊘	⊘	⊘
[redacted]营...	0	54分	⊗	⊘	⊘	⊘
[redacted]182.131.17.1...	0	100分	⊗	⊗	⊗	⊗
[redacted]厅-门...	0	0分	0个	⊗	⊗	20个
[redacted].cn...	0	34分	0个	3个	2个	1个
[redacted]04...	0	72分	0个	⊘	⊘	⊘
[redacted]gov....	0	36分	0个	7个	28个	3个
[redacted]...	4	46分	0个	8个	9个	3个
[redacted]9...	0	4分	0个	7个	⊗	⊗

CopyRight © 2013 Westone Co., Ltd.

目 录

CONTENTS

一 网络安全监测16年总览

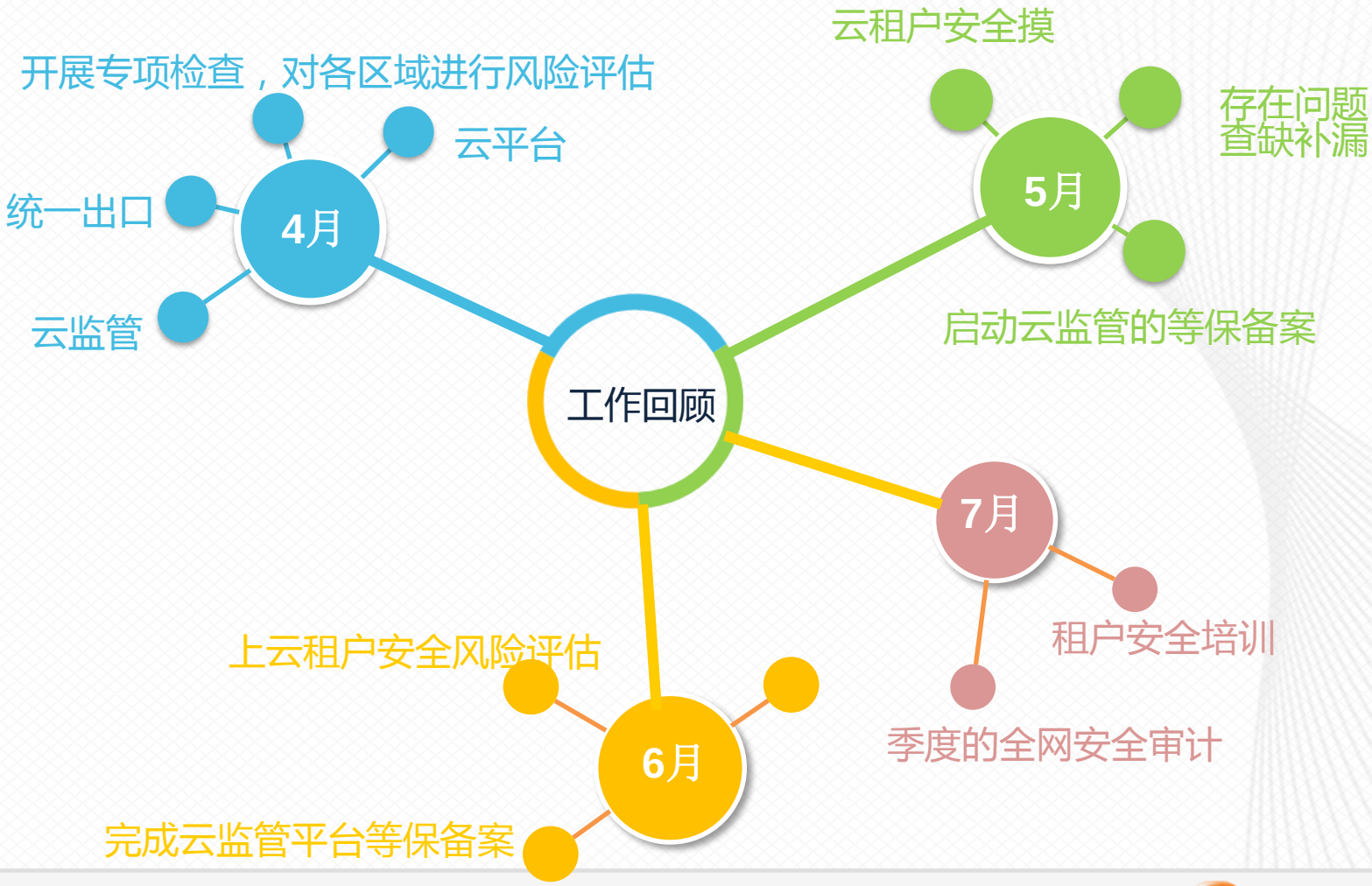
二 统一安全运维17年工作计划

三 政务云平台安全Next...

CopyRight © 2013 Westone Co., Ltd.

二、统一安全运维工作计划

工作回顾



CopyRight © 2013 Westone Co., Ltd.

二、统一安全运维运维工作计划

工作回顾

8月

- 开展审计工作出具报告
- 编制门户网站安全报告

9月

- 整改审计发现问题
- 完善门户网站报告

10月

- 核实云上网站信息
- 出具详细网站漏洞报告

CopyRight © 2013 Westone Co., Ltd.

二、统一安全运维工作计划

安全事件处理

安全例行检查

利用APT监测、主机安全检查、网站安全扫描等系统对全网进行安全例行检查;
不定期为部分租户提供主机安全检查和网站安全检查

现场取证分析

为XXX提供高级威胁监测分析和现场取证服务；
政务云全局的安全监测和取证分析

报告输出

《四川省级政务云主机取证分析报告》
《四川省级政务云安全分析报告》

CopyRight © 2013 Westone Co., Ltd.

案例分享

4月份，APT高级威胁监测系统检测到长时间的SSH暴力破解告警，并相继发生**挂马网址告警**和**沙箱恶意代码告警**等，告警共涉及4台服务器。

还原黑客的攻击过程

- 2016年4月05日 15:26:21 对外网服务器进行分布式SSH密码暴力破解
- 2016年4月13日 01:10:51 开始进入服务器，上传“lcx.exe”端口转发工具，可能进行同网段渗透
- 2016年4月13日 01:14:31 开始在各个服务器中陆续上传工具, 开启HTTP/FTP服务
- 2016年4月13日 04:20:59 控制其中一台服务器：182.140.197.8，下载一个远控木马的恶意文件“cpu70.exe”文件
- 。。。。。。

CopyRight © 2013 Westone Co., Ltd.

案例分享

在整个攻击过程中，出现了一个用于存放远控木马和其他渗透工具的网址 www.wholove.cn．通过其他技术手段在该服务器中发现了如下文件信息：

URL	文件内容
http://www.wholove.cn/rar.exe	winrar工具
http://www.wholove.cn/eb.exe	代理工具
http://www.wholove.cn/cesu.exe	360测速工具
http://www.wholove.cn/xiao7.exe	连接已经无效
http://www.wholove.cn/2008.exe	kryptik木马
http://www.wholove.cn/notepad.exe http://www.wholove.cn/explorer.exe http://www.wholove.cn/111.exe http://www.wholove.cn/64.exe	暂未分析
http://www.wholove.cn/7.exe	木马恶意程序
http://www.wholove.cn/32.exe	木马恶意程序
http://www.wholove.cn/xx.txt	里面为一个IP端口，可能是远控上线地址 211.154.152.185:5334
http://www.wholove.cn/1.txt	大量已经被破解的弱口令网站列表，尝试了一个密码能够正常登陆,形如： url:http://1.227.56.202:80 user:admin pass:admin

CopyRight © 2013 Westone Co., Ltd.

案例分享

域名	wholove.cn [whois 反查] 其他常用域名后缀查询： cn com cc net org
注册商	浙江贰贰网络有限公司
联系人	王超 [whois反查]
联系方式	qisitaobao@126.com [whois反查]
创建时间	2014年04月01日
过期时间	2017年04月01日
DNS	ns1.tigerdns.com ns2.tigerdns.com
状态	客户端设置禁止删除(clientDeleteProhibited) 客户端设置禁止转移(clientTransferProhibited)

攻击者信息总结如下

服务器信息

域名：www.wholove.cn
IP地址：103.24.1.98
位置信息：香港

疑似C&C地址信息

IP地址：211.154.152.185：5334
位置信息：广东深圳

CopyRight © 2013 Westone Co., Ltd.

案例分享

域名	注册者	邮箱	注册时间	过期时间	更新
haomiss.cn	王超	qisitaobao@126.com	2009-12-01	2016-12-01	
wholove.cn	王超	qisitaobao@126.com	2014-04-01	2017-04-01	

通过邮箱反查该注册人的其他域名,可以发现另一个服务器地址为haomiss.cn

域名	haomiss.cn [whois 反查] 其他常用域名后缀查询： cn com cc net org
注册商	杭州大益商务网络有限公司
联系人	王超 [whois反查]
联系方式	qisitaobao@126.com [whois反查]
创建时间	2009年12月01日
过期时间	2016年12月01日
公司	王超
DNS	ns1.tigerdns.com
状态	客户端设置禁止删除(clientDeleteProhibited) 客户端设置禁止转移(clientTransferProhibited)

CopyRight © 2013 Westone Co., Ltd.

案例分享

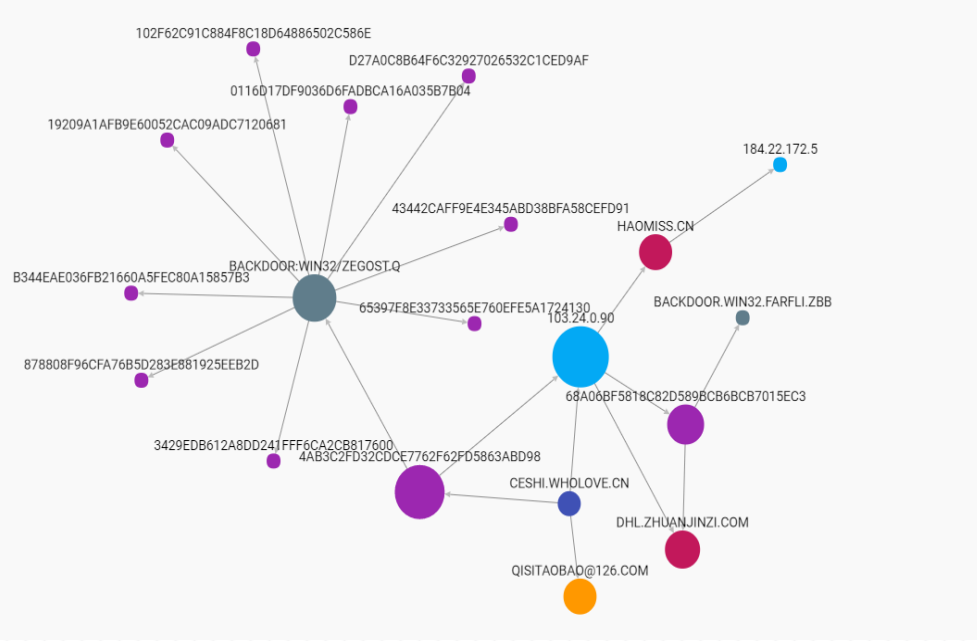
URL	文件内容	IP地区
http://www.haomiss.cn/cx.txt	温馨提示：需要测试购买联系高级代理商！另内部出售各国专线SOCKS5代理（EB）代理以上有所需要联系高级代理商！ 113.196.129.205 113.196.129.209 113.196.129.210.....	
http://www.haomiss.cn/xx.txt	27.129.186.210:5334可能是远控上线地址	河北省保定市 电信
http://www.haomiss.cn/super.txt	211.154.152.185:5332可能是远控上线地址	上海市或者深圳广东
http://www.haomiss.cn/1.txt	大量IP列表	

通过其他技术手段收集该服务器的文件信息，可以发现上述信息。

CopyRight © 2013 Westone Co., Ltd.

案例分享

通过情报分析平台可以发现邮箱“qisitaobao@126.com”所属的多个域名都为**病毒木马的分发服务器**，并且除去前面发现的两个网站以外还有其他的两个服务器dhl.zhuanjinzi.com、ceshi.wholove.cn：



DOMAIN > CESHI.WHOLOVE.CN

Is this malicious? Yes No

FILES THAT TALK TO CESHI.WHOLOVE.CN

MD5	A/V
4ab3c2fd32cdce7762f62fd5863abd98	[DLOADER.Trojan] [Backdoor.Zegost.BZ4] [Mal/PdfExDr-B] [Backdoor*Win32/Zegost.Q] [W32/Farfli.BBBltr] [Win32/DH{gRMDZwkngRCBEQ}] [Win32/Farfli.AK] [BackDoor-FCDQI4AB3C2FD32CD]

WHOIS DETAILS

Property	Value
Organization	王超
Email	qisitaobao@126.com
NameServer	ns2.tigerdns.com (8)

DNS RESOLUTIONS

Date	IP Address
2016-04-15	103.24.0.90 (3 , ClassC=Browse , ClassB=Browse)

CopyRight © 2013 Westone Co., Ltd.

案例分享

从“www.haomiss.cn/cx.txt”的内容可以看出，该攻击者存在大量高质量的代理服务器资源在销售，结合攻击者在网站服务器的文件信息基本可以推测：

该攻击者为专业的黑产从业人员，主要目的可能是攻陷服务器后通过变卖服务器的带宽资源，将控制的服务作为代理服务出售并以此获利。攻击者有多个木马C&C域名，并且已经活动了相当长的时间。

攻击者的重要信息如下：

IP和位置信息：

27.129.186.210 河北省保定市 电信

211.154.152.185 广东深圳

域名联系人信息：

姓名：王x

邮箱：qisxtaobao@126.com

CopyRight © 2013 Westone Co., Ltd.

二、统一安全运维工作计划

当前工作

CopyRight © 2013 Westone Co., Ltd.

二、统一安全运维工作计划

2017年计划

安全检查 1	安全保障 2	两会保障、安全自查 3	应急演练 4	半年度审计检查 5	结果整改 6

网站专项检查 7	安全自查整改复查 8	云监管等保复评 9	重大节日保障 10	年度审计云服务商等保复评 11	年度风险评估 12

CopyRight © 2013 Westone Co., Ltd.

目 录

CONTENTS

一 网络安全监测16年总览

二 统一安全运维17年工作计划

三 政务云平台安全Next...

CopyRight © 2013 Westone Co., Ltd.

三、政务云平台安全

安全服务

政务云安全

渗透测试	应急响应	APT追踪溯源		专家服务
安全态势感知	安全事件管理SOC			安全管理
数据库审计	数据防泄漏			数据安全
网站安全监测	网站云防御	网页防篡改		应用安全
主机安全检查	主机安全审计	主机安全加固		主机安全
下一代防火墙	DDOS防护	APT高级威胁监测	网络安全审计	网络安全

CopyRight © 2013 Westone Co., Ltd.

三、安全服务-主机安全

云主机安全

通过主机安全运维系统为政务云云主机提供安全检查和加固、配置核查和快照、安全日志审计、主机性能监控等功能，解决云主机安全问题

CopyRight © 2013 Westone Co., Ltd.

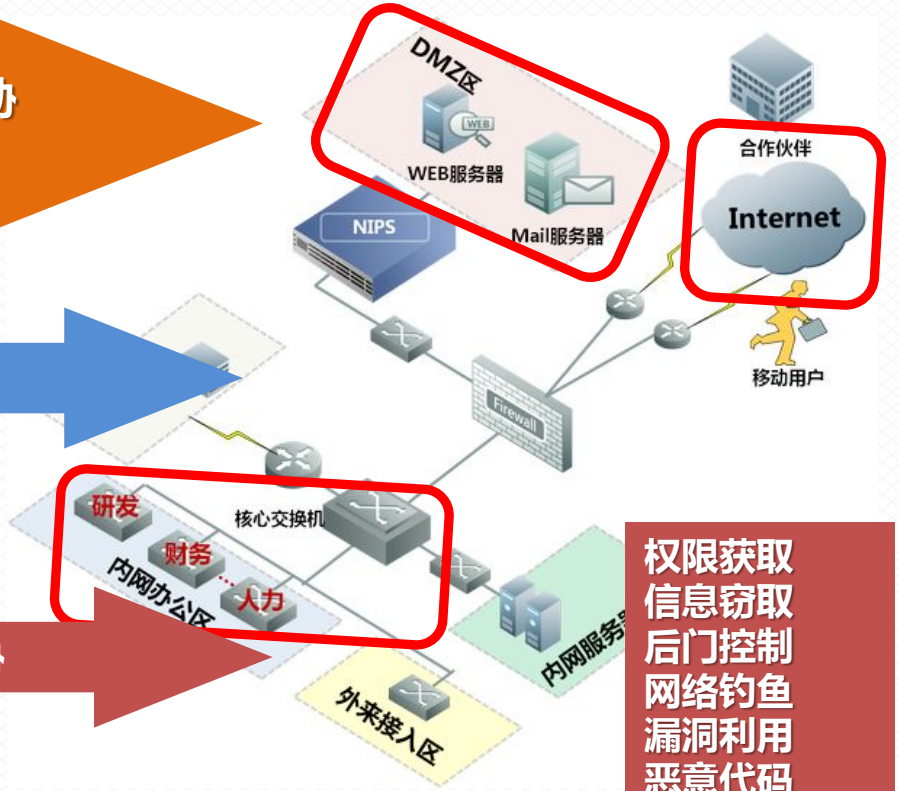
三、安全服务—Web应用安全

网站安全威胁是目前互联网主要攻击手段

针对Web服务的威胁
（占75%以上）

针对网络的威胁

针对终端的威胁



SQL注入
XSS脚本
网页木马
网页篡改
Web漏洞
CC拒绝服务攻击
域名系统漏洞
账户数据库泄露
安全系统漏洞
(OpenSSL)
……

网络探测
网络协议攻击
拒绝服务
信息欺骗、注入
蠕虫、 病毒传播
……

权限获取
信息窃取
后门控制
网络钓鱼
漏洞利用
恶意代码
……

CopyRight © 2013 Westone Co., Ltd.

三、安全服务—Web应用安全

2015年CNCERT/CC共监测到我国境内共24550个网站被篡改。

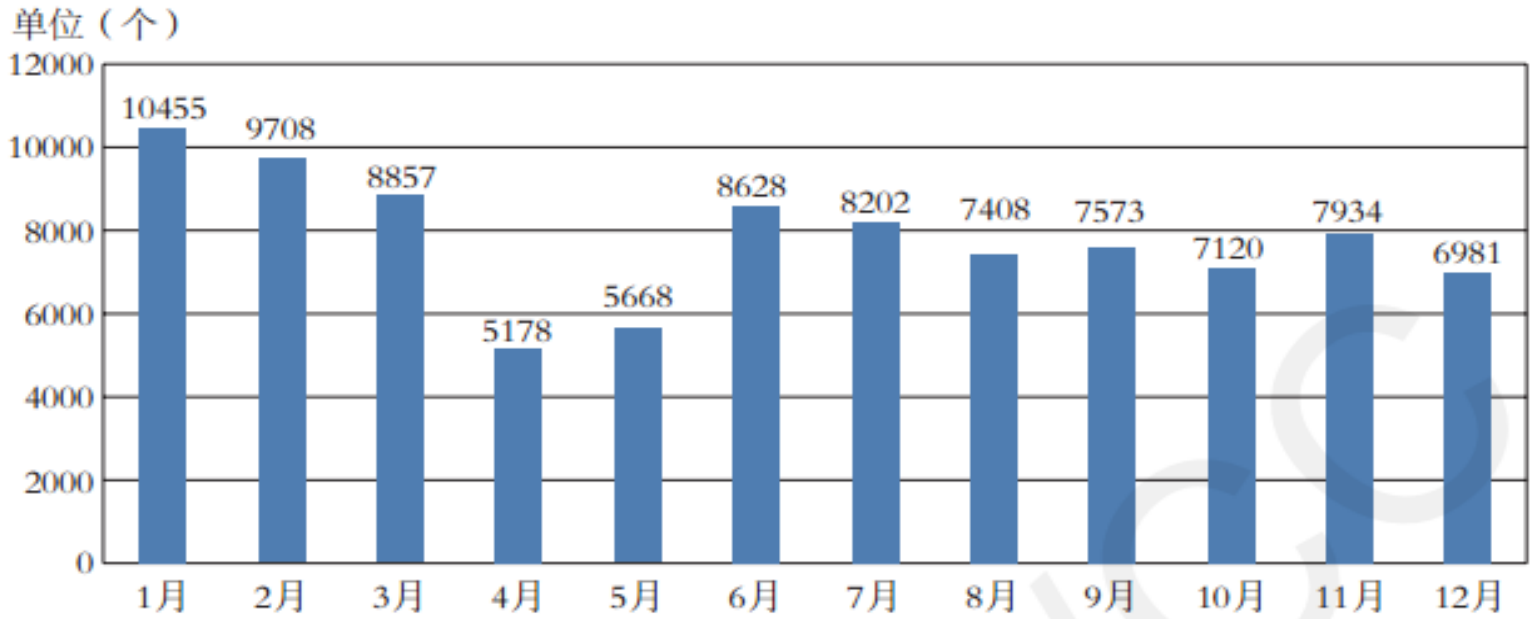


图5-1　2015年我国境内被篡改网站数量月度统计（来源：CNCERT/CC）

CopyRight © 2013 Westone Co., Ltd.

三、安全服务—Web应用安全

2015年CNCERT/CC共监测到境内75028个网站被植入后门，其中政府网站有3514个。

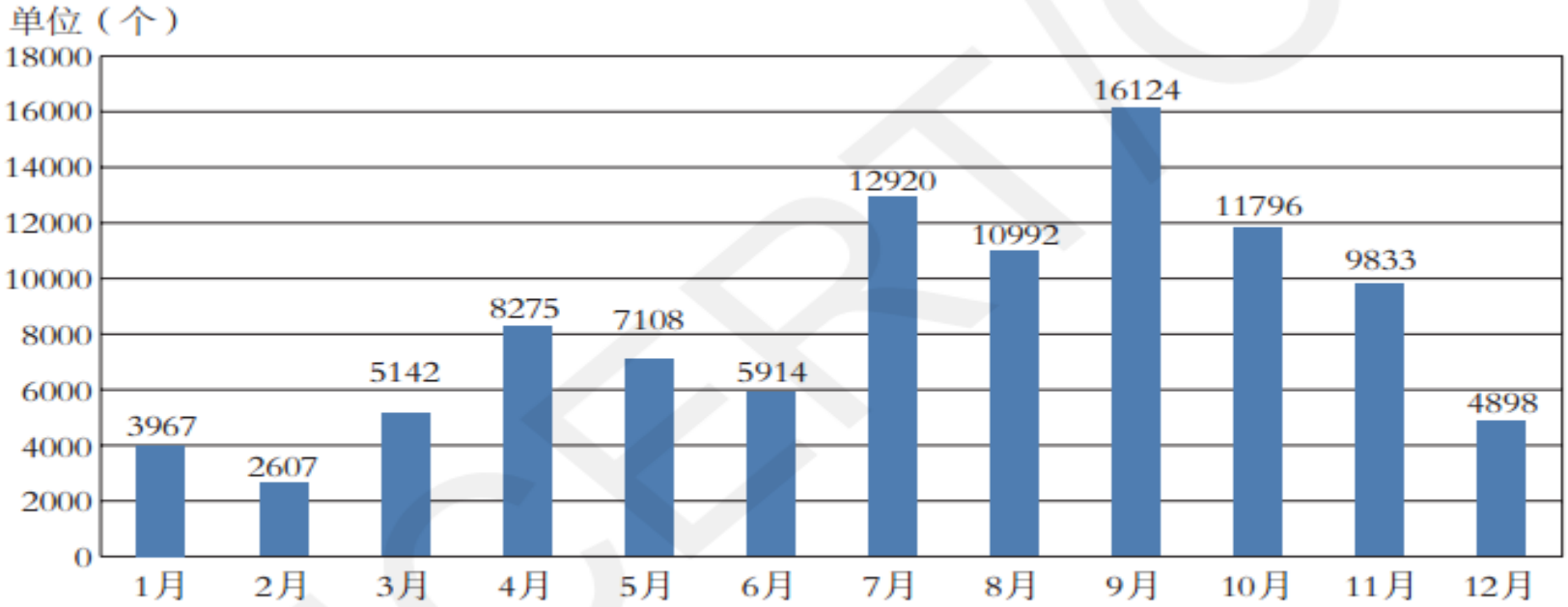
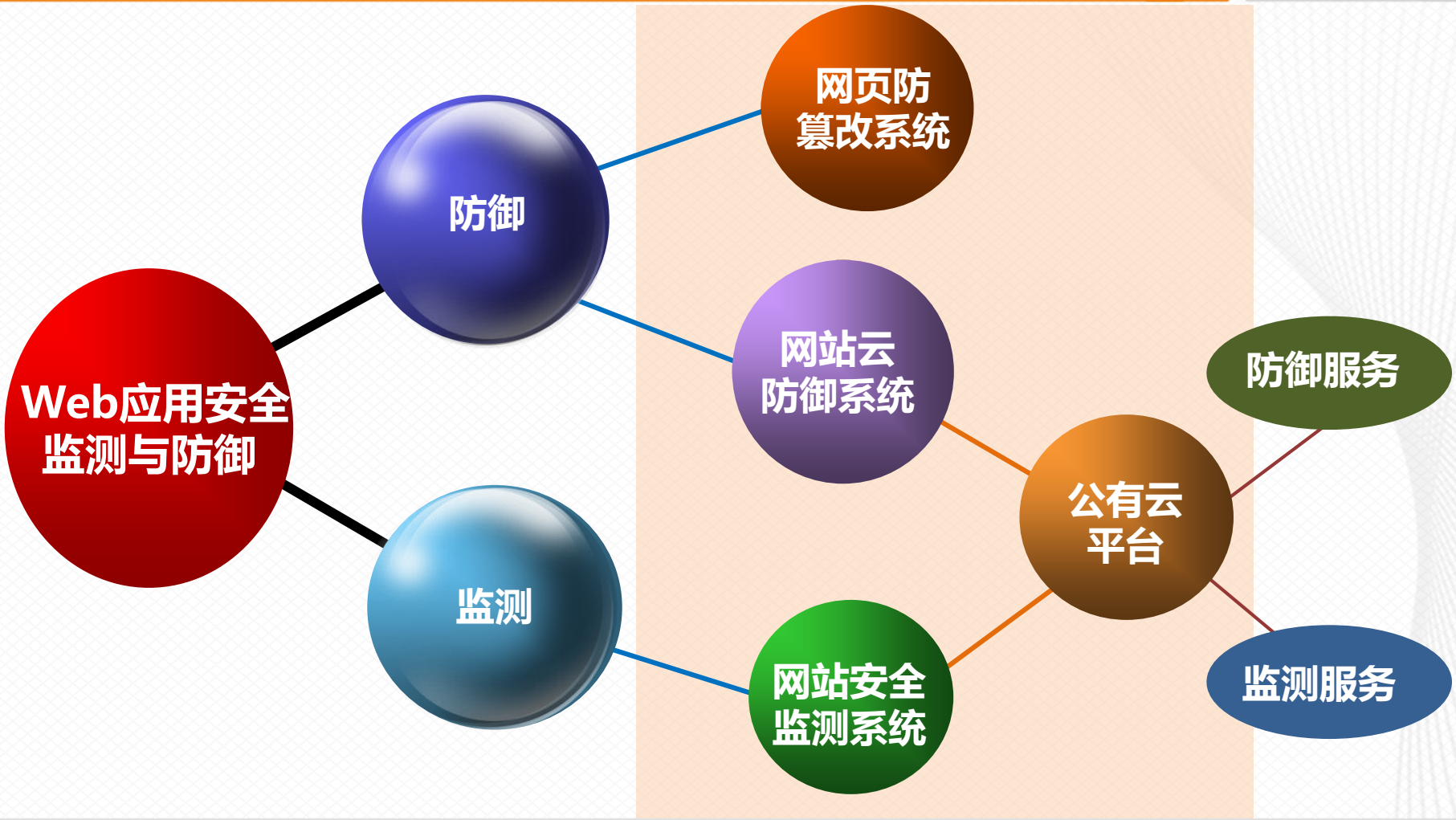


图5-5　2015年我国境内被植入后门网站数量月度统计（来源：CNCERT/CC）

CopyRight © 2013 Westone Co., Ltd.

三、安全服务—Web应用安全



CopyRight © 2013 Westone Co., Ltd.

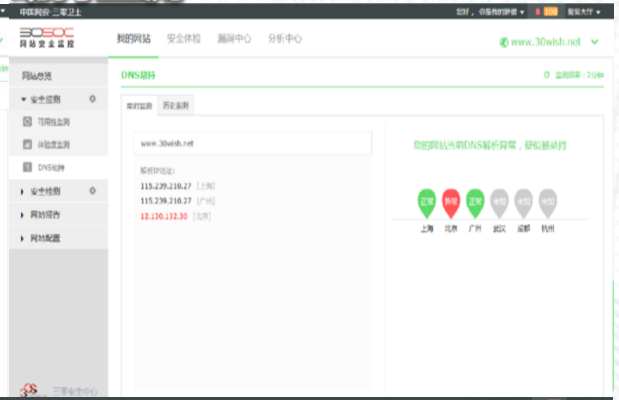
三、安全服务—网站安全监测系统

对每个被保护网站建立监测档案，定期收集网站相关信息进行分析，确定网站安全状

状态监测

性能监测

劫持监测



漏洞检测

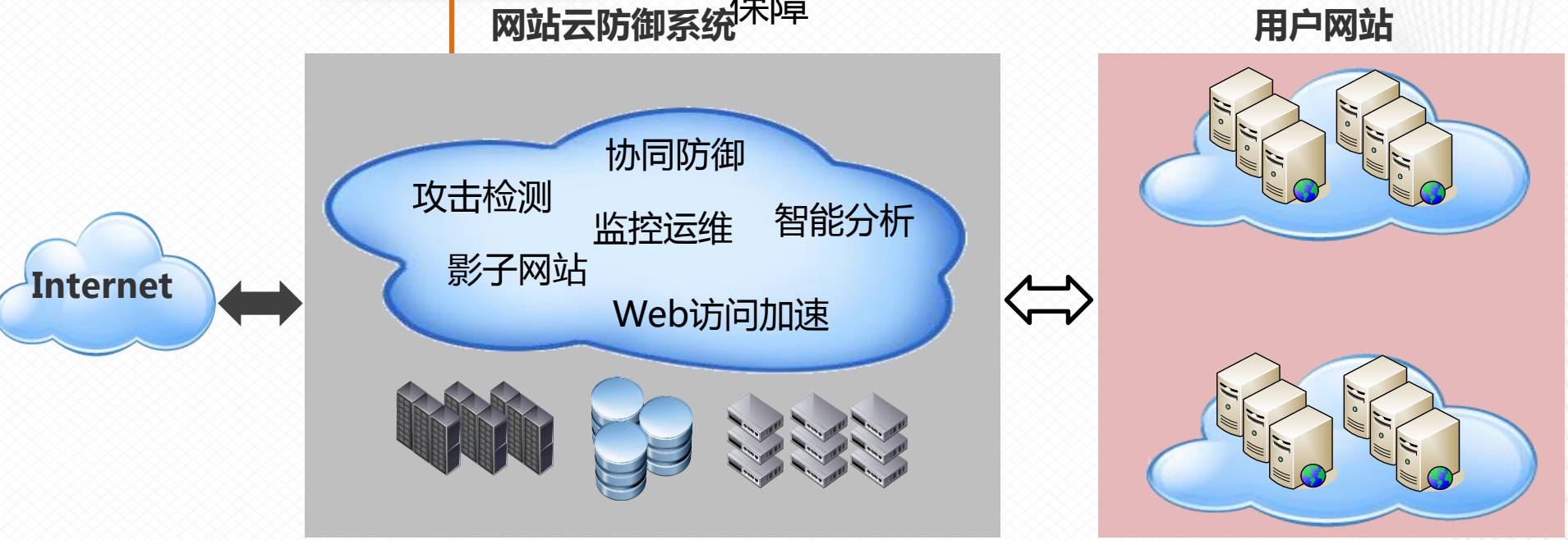
挂马检测

内容检测（指纹、暗链、敏感字）

CopyRight © 2013 Westone Co., Ltd.

三、安全服务—网站云防御系统

以Web防火墙为核心，集成安全大数据分析、威胁情报等能力，基于云端协同技术的WEB应用安全防护平台，为网站提供统一安全保障

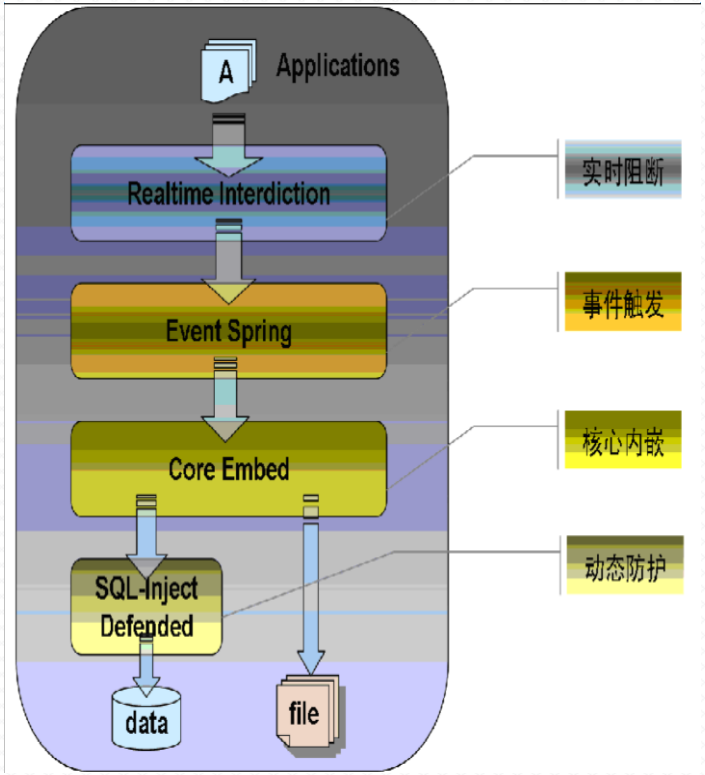


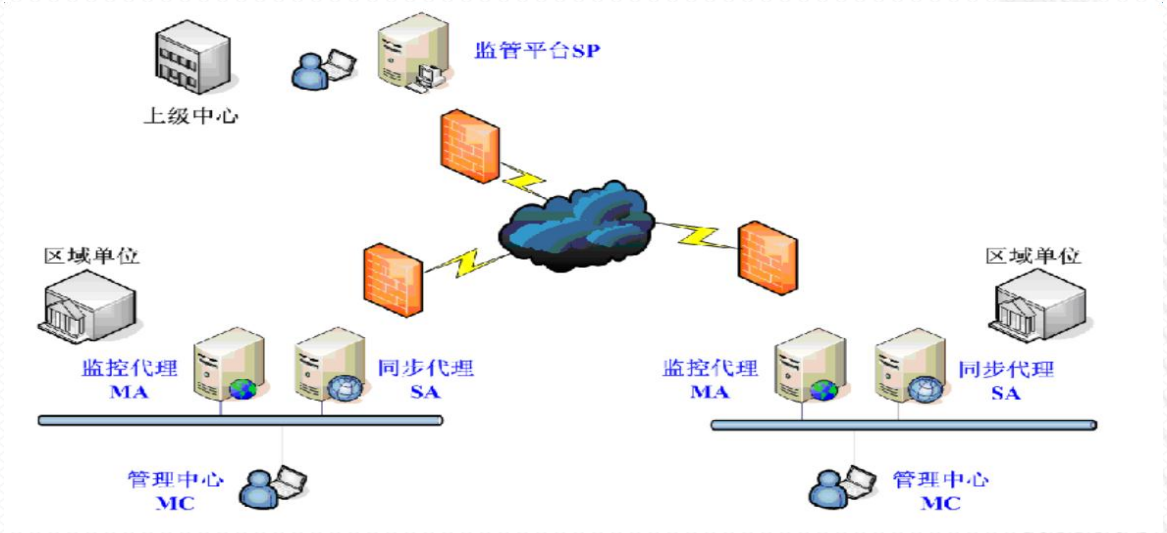
CopyRight © 2013 Westone Co., Ltd.

三、安全服务—网页防篡改系统

网页防篡改系统特点：

四重防护、纵深防御；环境普适、全面支持 ；分布部署、统一监管





CopyRight © 2013 Westone Co., Ltd.

数据安全事件愈演愈烈

2012.12 第十一届全国人大常委会第三十次会议通过了《关于加强网络信息保护的决定》

2013.06 “棱镜门”事件，爱德华.斯诺登将美国国家安全局的秘密文档披露给了《卫报》和《华盛顿邮报》，随即遭到美国政府通缉

2014.11 国内130万考研用户信息遭泄漏，包括考研用户的姓名、手机、座机、身份证、住址、邮编、学校、专业等敏感数据

2014.12 12306铁路客户服务中心网站再次爆发用户账号串号的问题，大量用户身份证等信息遭泄露

2015.02 万豪、喜达屋、洲际等高端品牌酒店，多家知名连锁酒店网站存在严重安全漏洞，海量开房信息大量泄露，一览无余

2015.02 美国第二大医疗保险公司Anthem遭遇迄今最大一起数据泄密事件，约数百万公司职员和客户的个人资料曝光

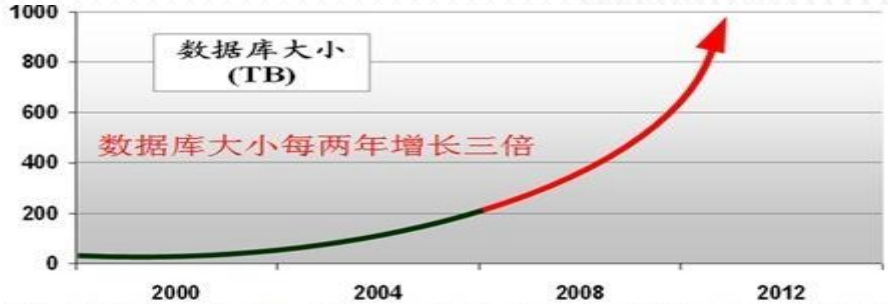
2015.04 数千万人社保信息疑似遭泄露，国家人社部随即出面辟谣

2015.05 权威机构预测2019年数据泄露造成损失将达2.1万亿

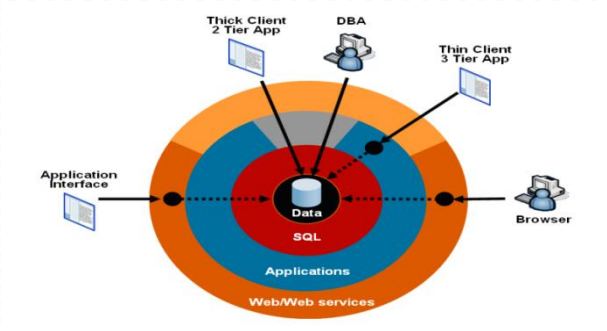
CopyRight © 2013 Westone Co., Ltd.

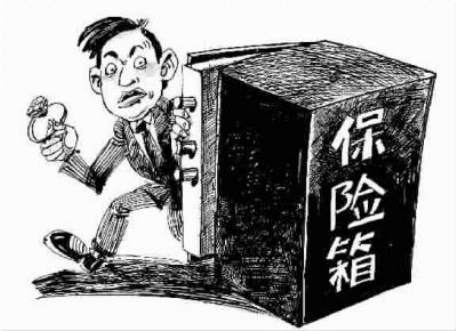
数据库是数据安全重点保护对象

- 数据库是各种信息的集散地（办公、财务、人力、物资、各种业务—交易、医疗、证券等）



- 数据库处于企业信息安全防御中心，是信息安全‘兵家必争之地’





金钱不一定是数字
但数字就是金钱！

CopyRight © 2013 Westone Co., Ltd.

对于有价值、敏感、重要的信息，行业有严格的管控要求

ISO/IEC 27001对数据库主机审计的要求

- 应产生**记录用户活动**、以外和信息安全事件的日志，并按照约定的期限进行保留，以支持将来的调查和访问控制监视
- 日期、时间和关键事件的**细节**
- 成功的和被拒绝的对数据以及其他资源尝试访问的**记录**
- 访问控制系统引发的**警报**
- 审计日志包含闯入和秘密人员的数据，应采取适当的**隐私保护措施**
- 定期评审监视活动的**结果**
- 系统**警报**或故障
- 应**保护日志**设施和日志信息免受破坏和未授权的访问
- 防止信息**泄漏**的机会
- 应收集、保留**证据**，并以符合法律规定的形式提交

- **发现：**
- 记录用户活动
- 关键事件的细节
- 访问记录
- **审计：**
- 访问控制警报
- 隐私保护措施
- 定期评审结果
- **取证：**
- 保护日志
- 防止泄漏
- 收集保留证据

《信息安全等级保护测评》对数据库主机审计的要求

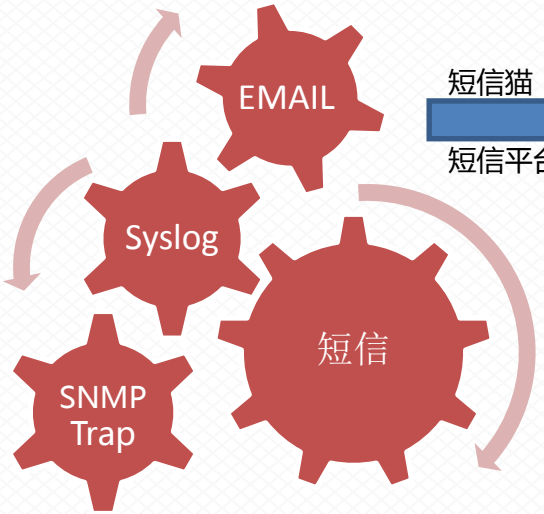
要求：
- 审计的选择要求和**策略**，审计日志的**保护措施**；
- 为授权用户浏览和分析审计数据提供**专门的审计工具**（如对审计记录进行分类、排序、查询、统计、分析和组合查询等），并能根据需要生成审计**报表**；
- 审计范围覆盖到**每个用户**；
- 对特定事件指定**实时报警**方式（如声音、EMAIL、短信等）；
- 定义了审计跟踪极限的**阈值**；
- 跟踪监测到可能的安全侵害**事件**；

- **发现：**
- 策略
- 覆盖每个用户
- 实时报警
- **审计：**
- 专门的审计工具
- 报表
- 阈值
- **取证：**
- 保护措施
- 安全事件

CopyRight © 2013 Westone Co., Ltd.

三、安全服务—数据库审计系统

实时事件监测及预警管理，事前、事中、事后全方位防护



短信猫

短信平台

支持对Oracle、MS-SQL 、DB2、MYSQL、Caché DB、POSTGRESQL和Sybase 等主流数据库

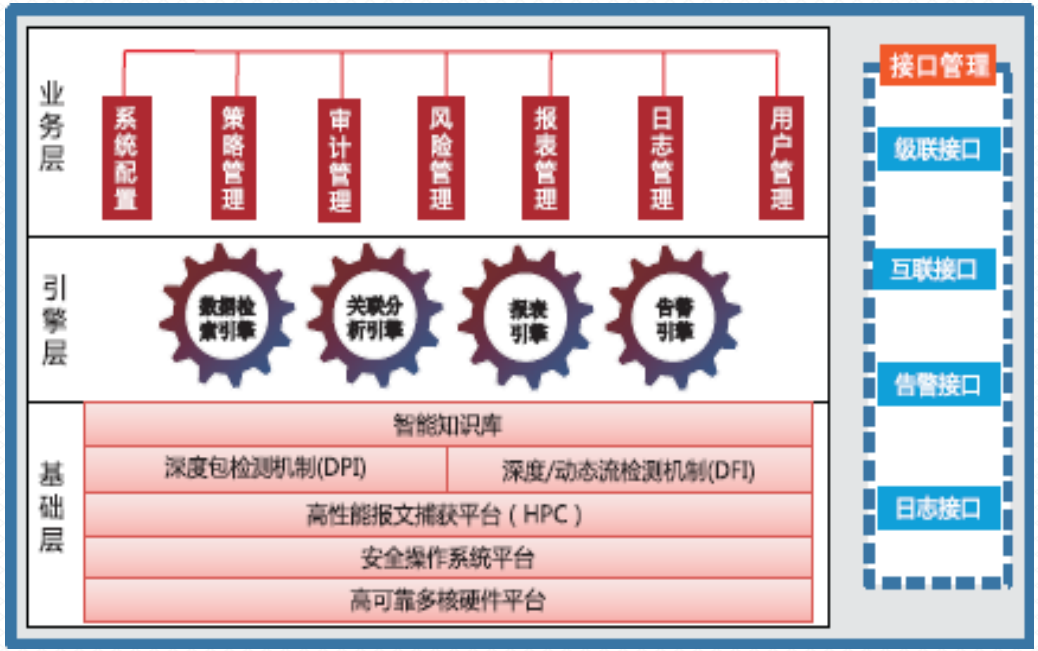
CopyRight © 2013 Westone Co., Ltd.

三、安全服务—数据库审计系统

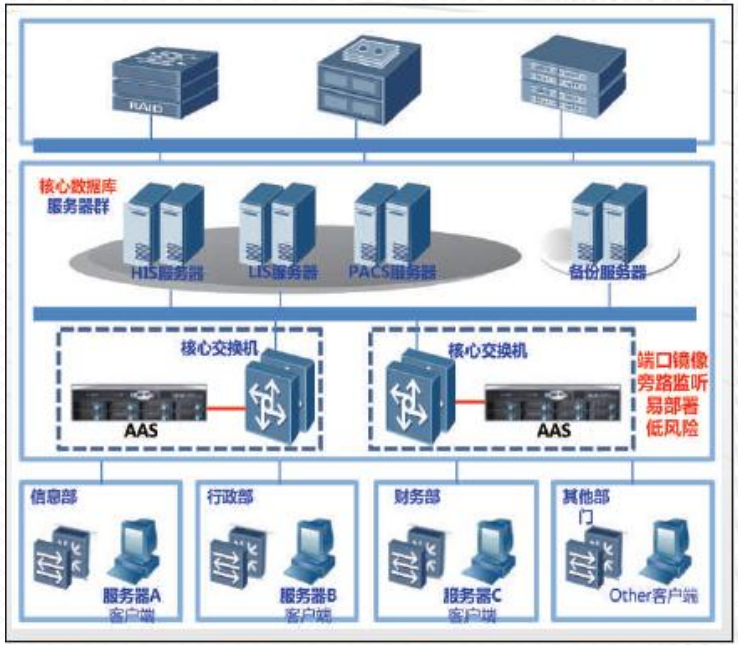
数据库审计系统**旁路部署**，**不更改客户的网络拓扑，不需要在服务器上安装任何插件，不需要提供任何数据库及应用账户名及密码**，系统同时支持**分布式集中部署架构**，可实现**分级运维、集中监控**。

目前正在与云服务商交流上云的模式和流量牵引方案。

系统架构图



系统部署图



CopyRight © 2013 Westone Co., Ltd.

态势感知

态势感知提供基于监管视角和租户视角的全局态势总览、安全预警，辅助安全决策等。

CopyRight © 2013 Westone Co., Ltd.

专家服务

专家服务

渗透测试：利用专家经验和渗透工具进行模拟攻击，发现系统脆弱性，验证系统防御能力，提交渗透测试报告；

应急响应：提供7*24热线支持和5*8的应急响应服务，并提供防御策略建议指导，处理各种突发安全事件；

安全值守：重大活动期间的安全值守：在召开“两会”、“党代会”“五一、国庆、春节”期间进行安全值守，保障业务安全运行

APT追踪溯源：提供威胁事件的追踪溯源分析服务，分析攻击者的来源、途径、目的和黑客组织等情报信息。

CopyRight © 2013 Westone Co., Ltd.

乌镇互联网大会工控联网设备安保工作

项目情况

针对浙江省的工业控制系统及设备，进行全方位在线扫描，对存在潜在威胁的系统进行漏洞渗透测试并发布风险评估报告。

防护效果

中国网安及时发现共**124个**浙江省连接在互联网上的工控系统，并发现诸多易渗透的重要工控系统后台以及大量疏于防范的生产现场视频设备，向相关部门提供威胁预警，并定期发布浙江工控威胁态势报告，为**第二届世界互联网大会**的顺利进行保驾护航。

- 桐乡市双桥油库
- 浙江元立金属制品集团有限公司
- 浙江秀舟纸业热电能源监控系统
- 平湖热电厂监控系统
- ...

世界互联网大会 乌镇峰会 Wuzhen Summit

CopyRight © 2013 Westone Co., Ltd.

G20会议网络安全保障

项目情况

受成都市网络安全监管机关委托，网安公司利用工业控制系统接入互联网威胁态势感知系统对区域内联网工控系统进行安全扫描、识别和监测，结合相关漏洞的分析及渗透测试，对威胁态势进行评估，形成安全分析日报，协助机关开展安全检查和整改工作，确保大会安全顺利举行。同时网安还受邀参与9月在杭州举行的G20峰会的安保工作。

防护效果

- **全域感知，重点监测。**对全市范围内联网工控系统进行全域感知，对电力、水务、 燃气和轨交等关键基础设施和重点工业企业工控系统和政府网站进行重点监测，及时掌握全市网络空间整体安全态势。
- **及时预警，协助整改。**在感知和监测基础上，专家团队结合安全分析及测试手段，验证系统问题、及时预警，并协助机关对会议活动现场开展安全检查并及时下达安全整改通知。

此次保障过程中发现多条直接暴露在互联网上的工业控制系统和上千条网络视频监 控系统和设备，及时查明并落实整改了包括水务、燃气、石化等多个工业控制系统存在的高危和中危安全漏洞。

中国网安与各单位通力配合，携手确保了成都市网络空间整体安全形势平稳。

CopyRight © 2013 Westone Co., Ltd.

关键信息基础设施安全

这些事情交给你们，放心！

CopyRight © 2013 Westone Co., Ltd.

Westone·卫士通
Information Industry INC.

谢 谢！

2016/11/28