



# 主机的未知安全 威胁检测与防御

李栋

椒图科技副总裁

## 目录

主机安全现状

主机端的未知安全检测与防御技术

内网主机的零信任安全模型

## 针对主机的黑客攻击日益增多

勒索病毒

一句话木马

0DAY攻击

...

## 传统基于安全规则的防护手段效果有限

依赖于安全规则，可以抵御已知攻击，但对未知威胁防护效果滞后，无法应对0DAY和新型恶意代码

病毒库、规则库的堆集只会让系统变得愈发臃肿



## 案例：WEBLOGIC 反序列化漏洞（CNVD-C-2019-48814）

### 漏洞披露时间

2019-04-17

### 漏洞详情

WebLogic Server提供异步通讯服务的wls9\_async\_response WAR包，在反序列化处理输入信息时存在缺陷，攻击者可以通过恶意 HTTP 请求，获得目标服务器权限，在未授权的情况下远程执行命令，漏洞评级为高危。

### 漏洞披露方处理方案

- 1、删除该WAR包并重启webLogic;
- 2、通过访问策略控制禁止 /\_async/\* 路径的URL访问。

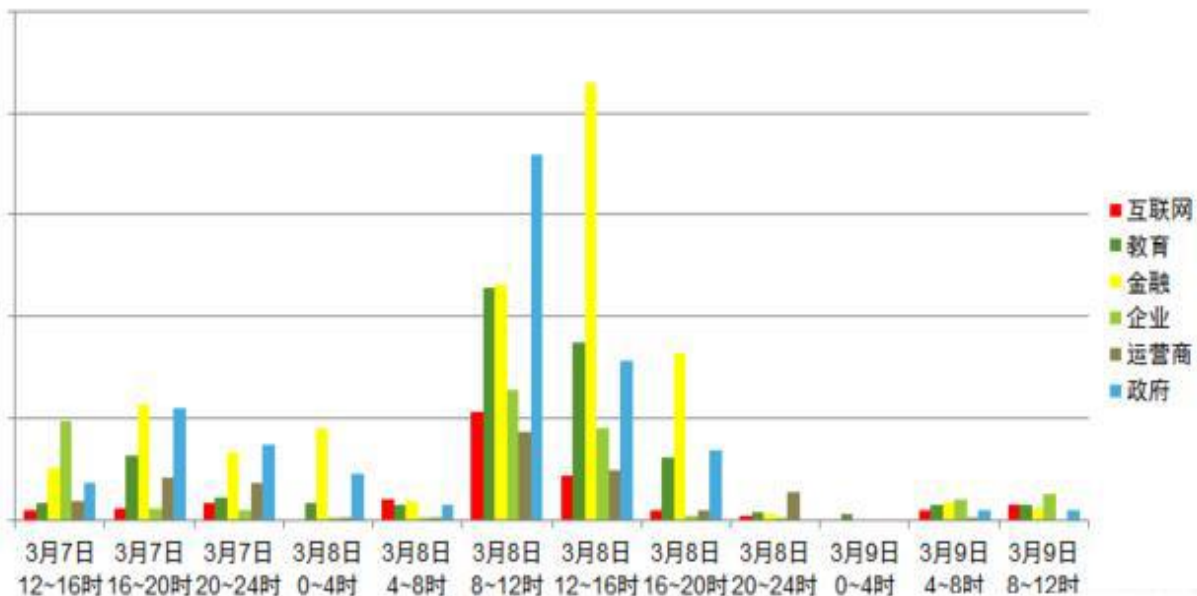
### 处理方式分析

牺牲业务保安全，通过删除WAR包的方式不但会导致部分服务失效而且治标不治本。

## 案例：STRUTS2 漏洞CVE编号CVE-2017-5638

- 3月7日漏洞爆出，厂商当天给出修复方案，但截止3月9日，仍有部分用户没有检测或者修复漏洞。
- 根据TCELL发布《2018年第二季度生产环境Web应用程序安全报告》，漏洞修复平均时长为**38天**！  
给攻击者留下足够的attack free时间窗

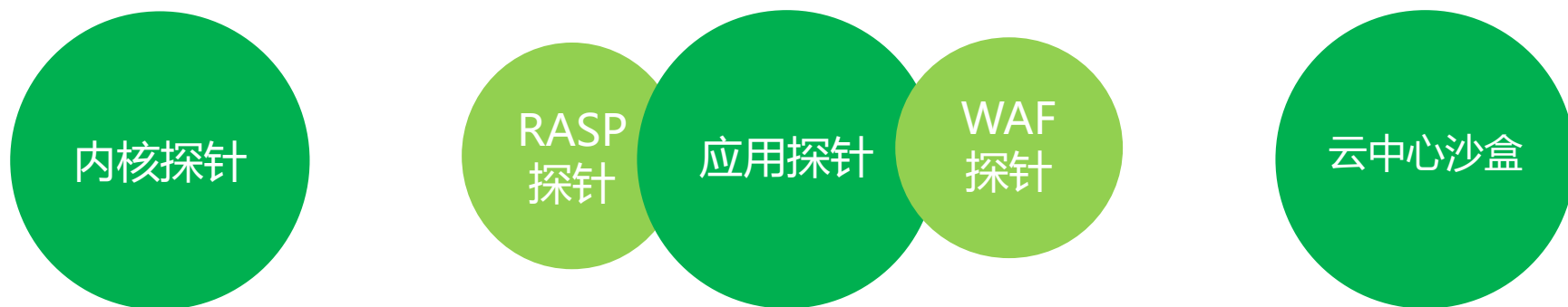
Struts2漏洞各行业检测积极性



漏洞永远补不完，但黑客入侵服务器后的行为却有迹可循

黑客在入侵产生的多种异常行为：提权、端口扫描、反连shell、进程自我复制、监听原始套接字、执行一句话木马、应用执行cmd、创建可执行文件、创建克隆账户.....

在了解黑客入侵行为轨迹后，在系统和应用两个层面监控和拦截，用安全机制补充安全规则，以有限的行为防御无限的漏洞。



## 内核加固

通过构建内核探针对端口扫描、反连shell、进程自我复制、监听原始套接字等黑客在入侵产生的多种异常行为进行监控及防护，同时会对系统中的二进制文件创建、进程创建、进程外连、linux shell操作命令等行为进行监控和防护，实现主机内核加固。

## 应用权限控制

从内核层实现应用权限控制，限制应用过高权限，防止提权、创建可执行文件等操作。



## WAF探针

工作于IIS、Apache、Nginx等web中间件内部，基于防护规则（数字签名）对WEB流量进行监控及过滤，具备所有硬件WAF的防护能力及功能。

### 防护能力

- ✓ 常见网络攻击（SQL注入、XSS、溢出攻击等）
- ✓ CC攻击(独创session验证模式，高效验证正常访问/机器攻击)

### 大数据安全分析

- ✓ 每天1500W+ 攻击记录
- ✓ 4000W+ IP 信誉库
- ✓ 海量 webshell样本，动态结合RASP、沙箱技术，识别未知攻击

### 支持web中间件

- ✓ IIS、Apache、Nginx、kangle、Tomcat、Weblogic、
- ✓ WebSphere、TongWeb、Jboss、Glassfish、Jetty等

119.102-Jspstudy > 应用防护 > Web应用设置 > 网站漏洞防护

防止黑客通过Web服务器或Web应用程序的漏洞入侵服务器

**已开启**  
白名单设置

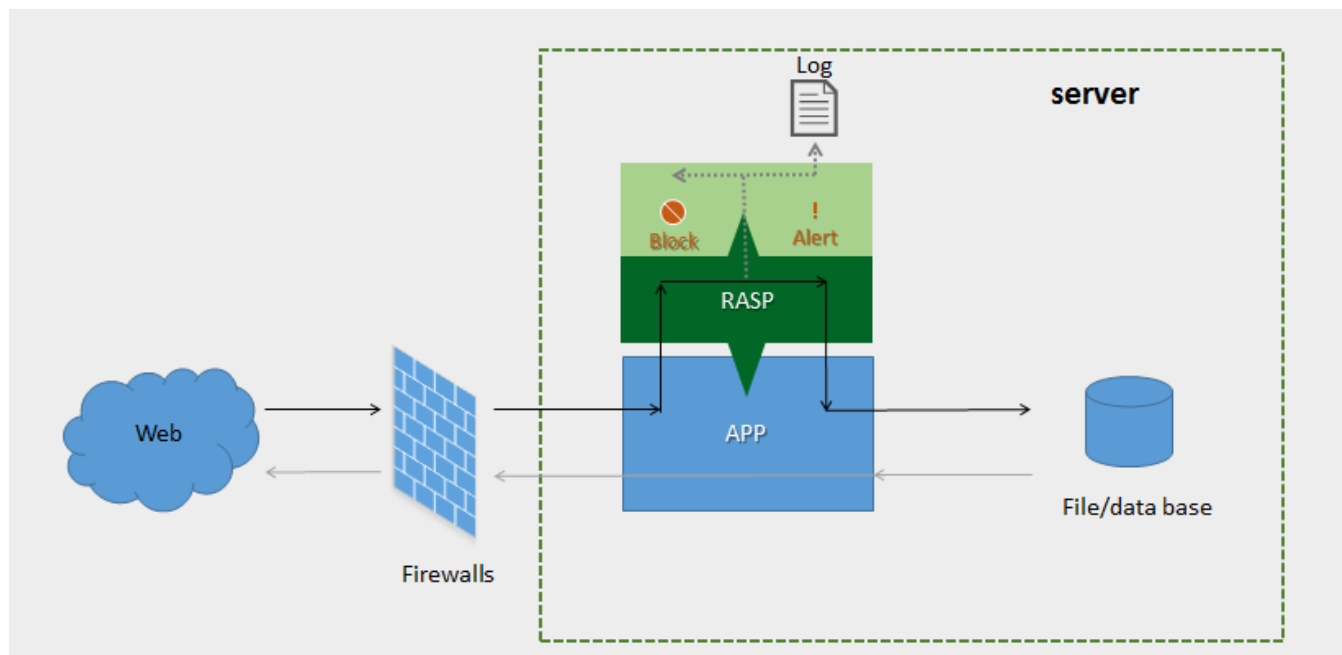
新增	编辑	删除	编号	所有规则	规则描述	检测URL	检测Cookie	检测POST
			211	XSS防护	(I)FRAME标签内JS类型的...	<input checked="" type="checkbox"/> URL	<input checked="" type="checkbox"/> Cookie	<input checked="" type="checkbox"/> POST
			212	XSS防护	DIV标签内采用JS类型的X...	<input type="checkbox"/> URL	<input type="checkbox"/> Cookie	<input type="checkbox"/> POST
			213	XSS防护	META类型的XSS防护	<input type="checkbox"/> URL	<input type="checkbox"/> Cookie	<input type="checkbox"/> POST
			300	防漏洞攻击	一句话木马利用工具防...	<input type="checkbox"/> URL	<input type="checkbox"/> Cookie	<input checked="" type="checkbox"/> POST
			301	防漏洞攻击	一句话木马利用工具防...	<input type="checkbox"/> URL	<input type="checkbox"/> Cookie	<input checked="" type="checkbox"/> POST
			302	防漏洞攻击	一句话木马利用工具防...	<input type="checkbox"/> URL	<input type="checkbox"/> Cookie	<input checked="" type="checkbox"/> POST
			303	防漏洞攻击	一句话木马利用工具防...	<input type="checkbox"/> URL	<input type="checkbox"/> Cookie	<input checked="" type="checkbox"/> POST
			304	防漏洞攻击	一句话木马利用工具防...	<input type="checkbox"/> URL	<input type="checkbox"/> Cookie	<input checked="" type="checkbox"/> POST
			305	防漏洞攻击	禁止使用php://input	<input checked="" type="checkbox"/> URL	<input type="checkbox"/> Cookie	<input type="checkbox"/> POST
			306	防漏洞攻击	禁止使用php://filter	<input checked="" type="checkbox"/> URL	<input type="checkbox"/> Cookie	<input type="checkbox"/> POST
			307	防漏洞攻击	svn信息保护	<input checked="" type="checkbox"/> URL	<input type="checkbox"/> Cookie	<input type="checkbox"/> POST

☒ Web服务器溢出攻击防护  
☒ Web服务器文件名解析漏洞防护  
☒ 禁止浏览畸形文件  
☒ 仅允许下列请求类型 [设置](#)  
☒ 禁止下载特定类型文件 [设置](#)  
☒ 网页浏览实时防护 [设置](#)  
☐ 自动屏蔽扫描器



## RASP(runtime application self-protection)

RASP探针工作于ASP、PHP、Java等脚本语言解释器内部，区别于传统WAF基于流量规则的防护方式，RASP探针是基于脚本行为（无规则）的方式进行漏洞攻击识别及防护，RASP探针会对WEB流量以及文件操作及数据库操作等行为进行监控，在脚本解析、命令执行等关键点上进行监控和拦截，能有效防御SQL注入、任意命令执行、文件上传、任意文件读写、Weblogic反序列化、Struts2等基于传统签名方式无法有效防护的未知安全漏洞，是对传统WAF的有效补充。



### 事件概述

攻击时间	服务器	事件类型	事件分组	攻击源IP	目标IP	攻击阶段	风险等级	状态
2019-04-25 17:31:54	DD-WIN2003_2	应用存在Java反序列化漏洞	漏洞被利用	192.168.175.1	192.168.175.131	攻击		已处理

### 事件描述

反序列化指将在Java序列化过程中所生成的二进制串转换成数据结构或者对象的过程。当在进行反序列化的时候，被反序列化的数据被恶意构造，此时利用恶意构造的数据就可以进行远程代码执行。

### 处理意见

该类型事件的报警，说明服务器的网站已被利用该

### IOC

192.168.175.1 (局域网) 利用 192.168.175.131:7001/\_async/AsyncResponseService 存在的反序列化漏洞 执行命令 已拦截

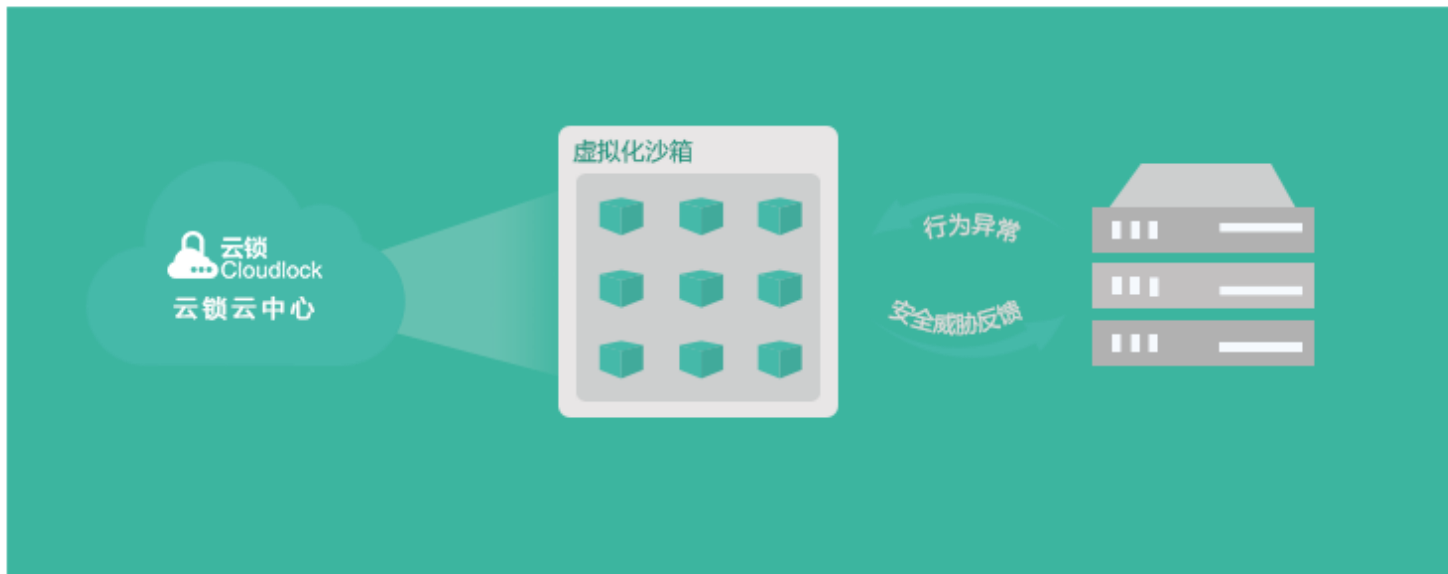


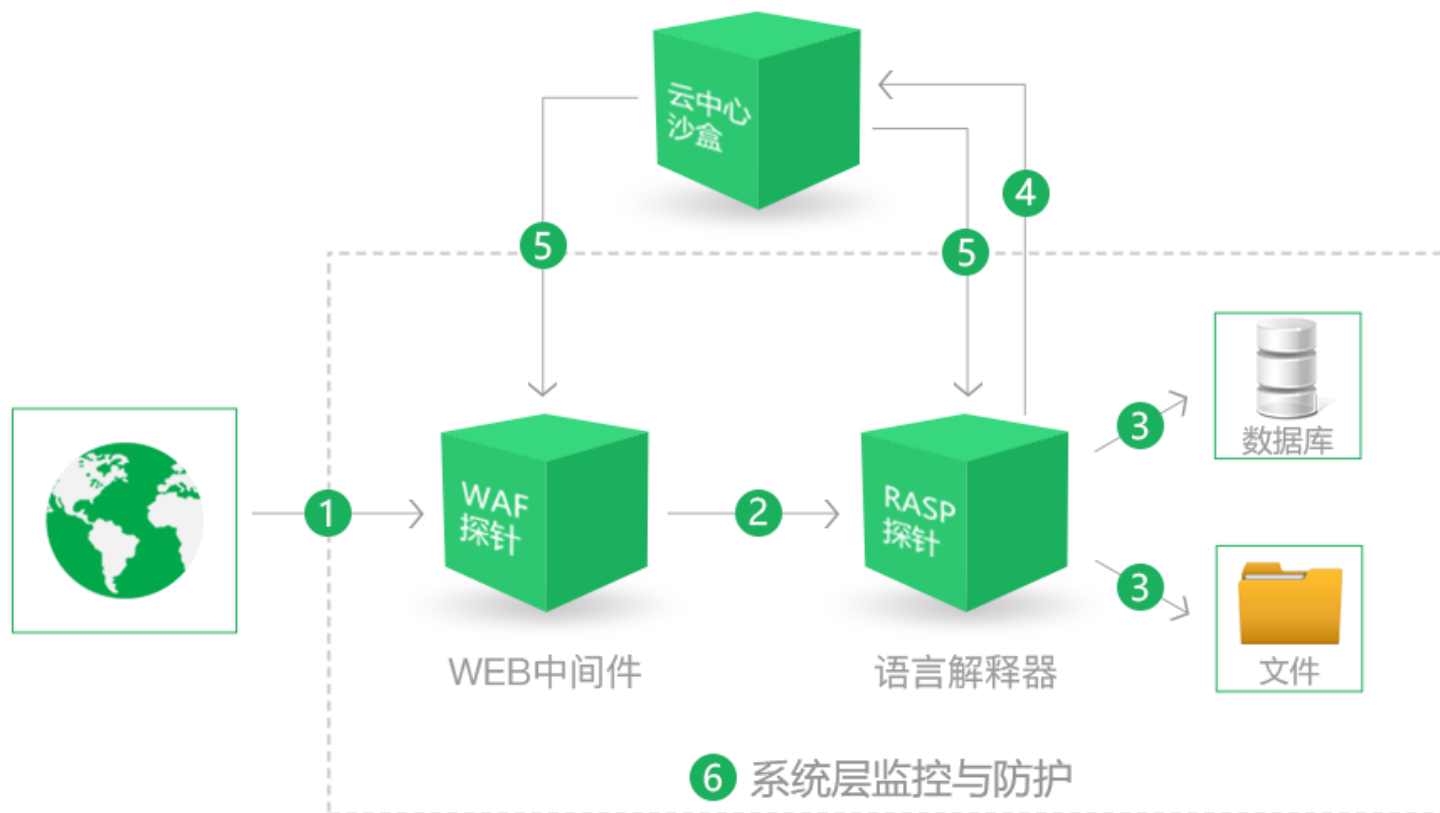
## 沙箱 (sandbox)

基于脚本虚拟机（沙盒）的无签名Webshell检测技术，有效检测各种加密、变形的Webshell基于异常行为的检测技术，可有效检测出未知威胁。通过在内核及应用层探针中设置监控点，持续对系统的行为进行学习，可有效检测出系统中存在的异常行为，并在综合判定后产生告警。

## 脚本虚拟机的优势

- 不依赖文本特征检测
- 可检测自加密的脚本
- 可检测未活动的WebShell
- 支持php asp .net java
- 编写的webshell

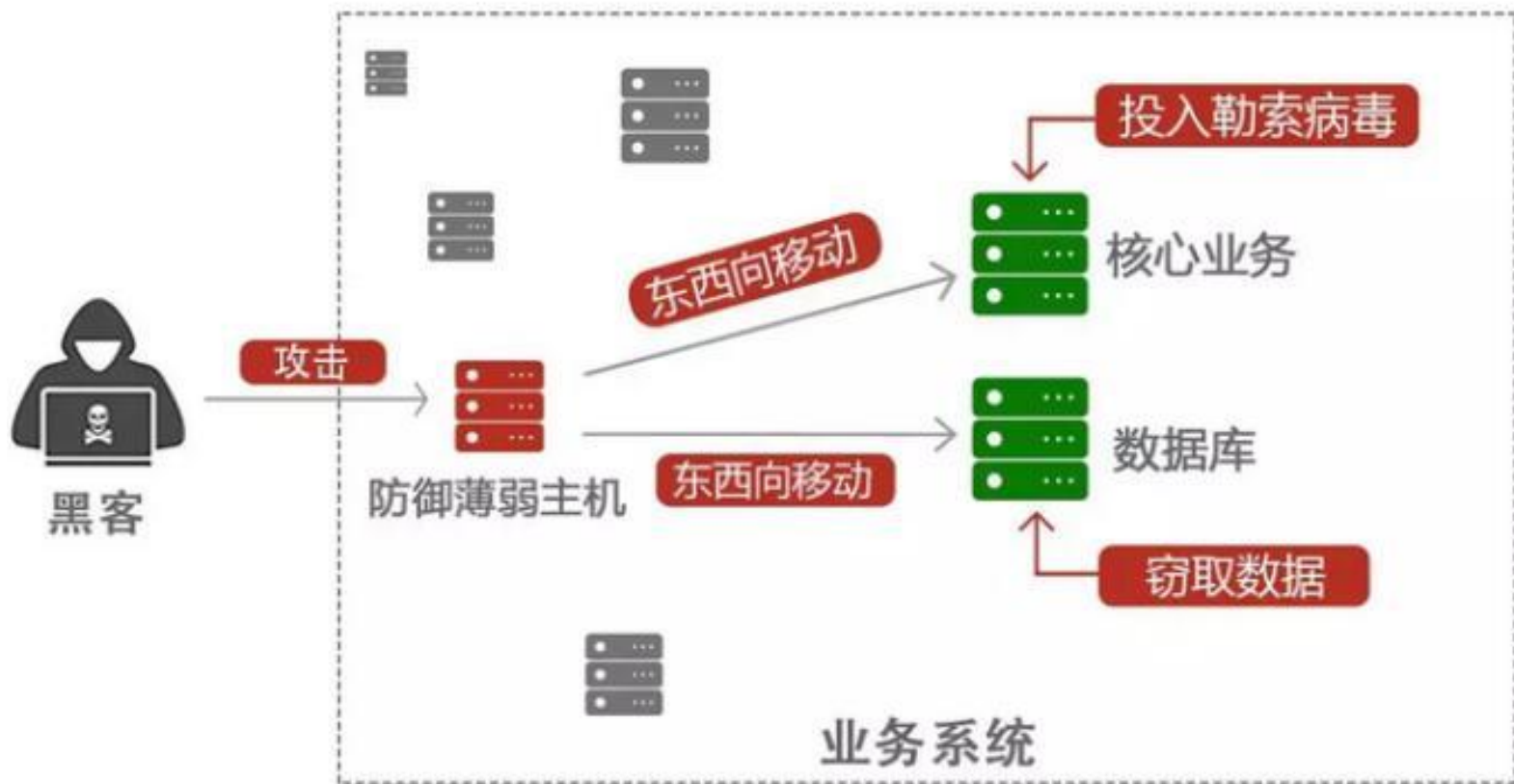






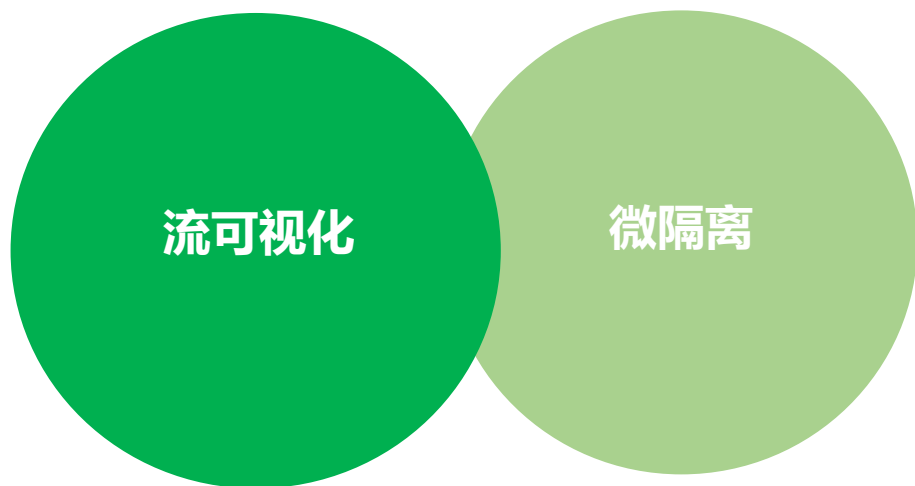
## 东西向移动

无论核心业务的安全防御能力有多强，在默认“内网相互信任”的前提下，只要业务系统中存在防护薄弱的主机，一样可以被攻击者利用东西向移动攻破。



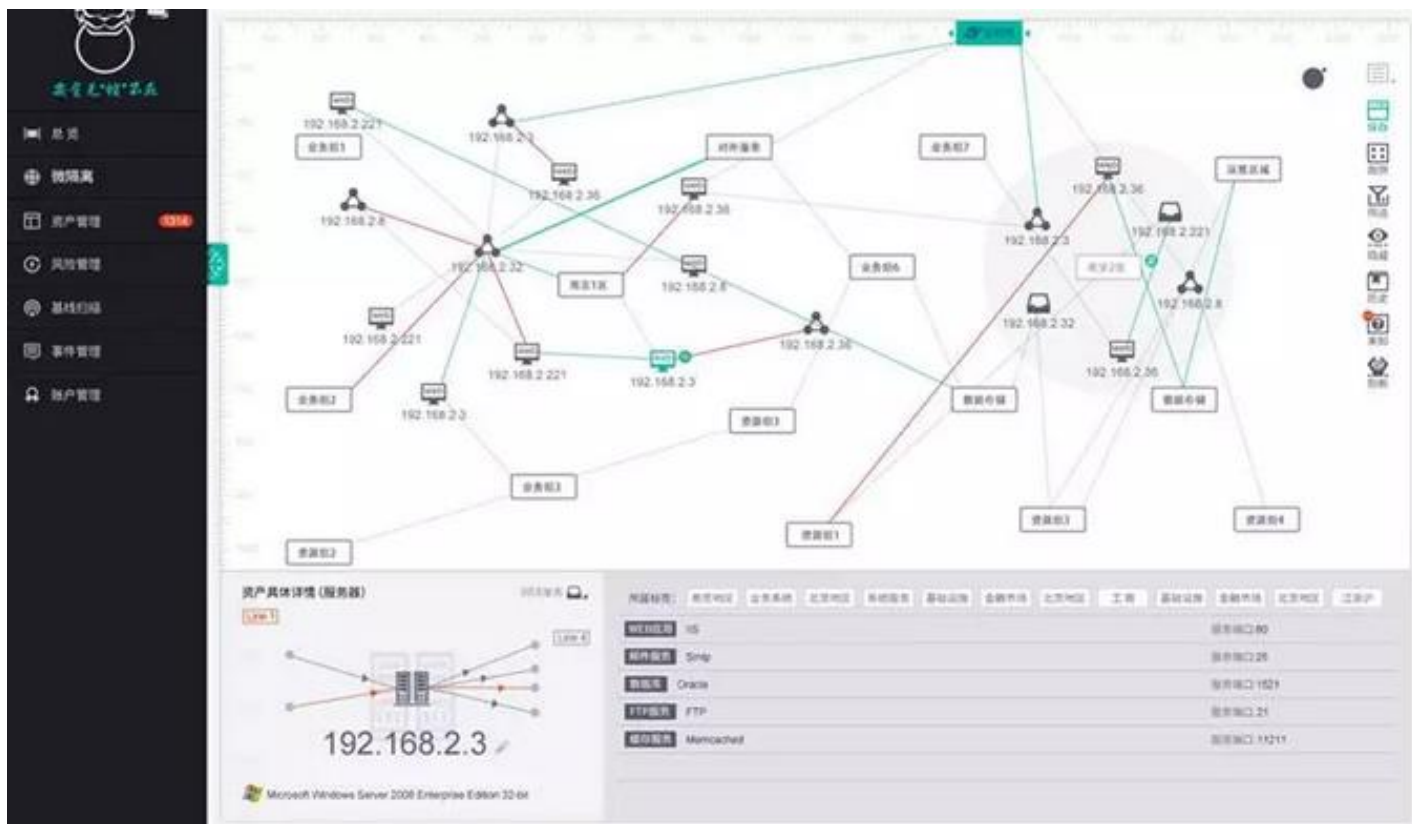
## 内网主机东西向流量监控与防护模型

构建业务环境内主机的零信任安全模型，实现流量可视、可控。



流可视化（Flow visibility）通过监控业务系统数据流并将其可视化,帮助安全运维人员实时准确把握业务系统内部网络信息流动情况。

- 流可视化的功能可以识别到：业务资产可视化；业务资产间访问关系可视化；流量信息可视化；访问端口可视化以及访问数量可视化等。
- 右图中图标代表安装agent的主机资产，主机间的线代表访问关系，线的颜色代表访问绿色-合规流量；红色-违规流量（被拦截）；灰色-未设置规则流量；黄色-监控模式流量。



微隔离（Micro-segmentation）是主机端分布式防火墙技术，可以细粒度控制主机、主机应用间的访问关系：

## 1. 东西向流量防护

可以基于角色、标签定义主机、主机应用间的细粒度访问控制策略。比如在一个安全域内允许A类主机（如web服务器）去访问B类主机（如数据库），其他类型的主机去访问B类主机将被禁止；或者A类主机的web应用可以去访问B类主机的数据库应用，A类主机的其他应用访问B类主机的数据库应用将被禁止。

## 2. 南北向流量防护

解决主机非法外连问题，可以定义主机允许访问的特定IP、IP段、域名，不在规则外的访问将被禁止。

策略名称	访问类型	源地址	资产角色(源)	源属性	访问状态	目标地址	目标端口	资产角色(目标)	目标属性	操作
linux	双向	192.168.19.94,	any	any	允许访问	192.168.19.101,	any	any	any	编辑
1111	双向	192.168.19.115,	any	any	允许访问	192.168.19.94,	any	any	any	编辑
123	双向	192.168.29.23,	any	any	允许访问	192.168.100.199,	any	any	any	编辑
test	入站	192.168.1.140, 192.168.1.111,	any	any	禁止访问	192.168.1.103, 192.168.1.135,	any	any	any	编辑
11	出站	192.168.119.156,	any	any	允许访问	192.168.29.15,	any	any	any	编辑

访问类型:

允许访问

禁止访问

日志类型:

入站

出站

高级筛选

Q云中心服务为您找到相关结果约 6,029,483 条

日志时间: 2019-4-18 11:09:56

访问类型: 出站

所属服务器: 192.168.19.86 (192.168.19.86)

状态: 允许访问

192.168.19.86 对 mirrorlist.centos.org 的 80 端口进行访问, 由于全部策略处于监控模式, 有生效策略后会被拦截!

日志时间: 2019-4-18 11:09:46

访问类型: 出站

所属服务器: 192.168.29.53 (192.168.29.53)

状态: 允许访问

192.168.29.53 对 monitor.yunsuo.com.cn 的 80 端口进行访问, 由于全部策略处于监控模式, 有生效策略后会被拦截!



内核加固、RASP、沙盒等技术能大幅提升主机端的未知安全威胁检测与防护能力；流可视化与微隔离可以降低内网渗透的风险，但并不能承诺“万无一失”，正因如此，我们需要及时、进准的攻击溯源系统，帮助用户快速定位并修复安全风险点。





## 资产管理

主机资产

网站资产

应用资产

数据库资产

内核模块

环境变量

启动服务

安装包



## 安全运维

漏洞扫描

补丁管理

病毒、后门、webshell扫描

基线检查

批量运维

性能监控



## 流量控制

流可视化

微隔离



## 动态防御

入侵检测 (HIPS)

漏洞利用防护

RASP应用运行时自我保护

应用权限控制

操作系统内核加固

Webshell/病毒查杀

文件防篡改/完整性保护

防爬虫/防恶意扫描



## 攻击溯源

命令审计

安全日志

攻击路径回溯

事前预防

事中控制

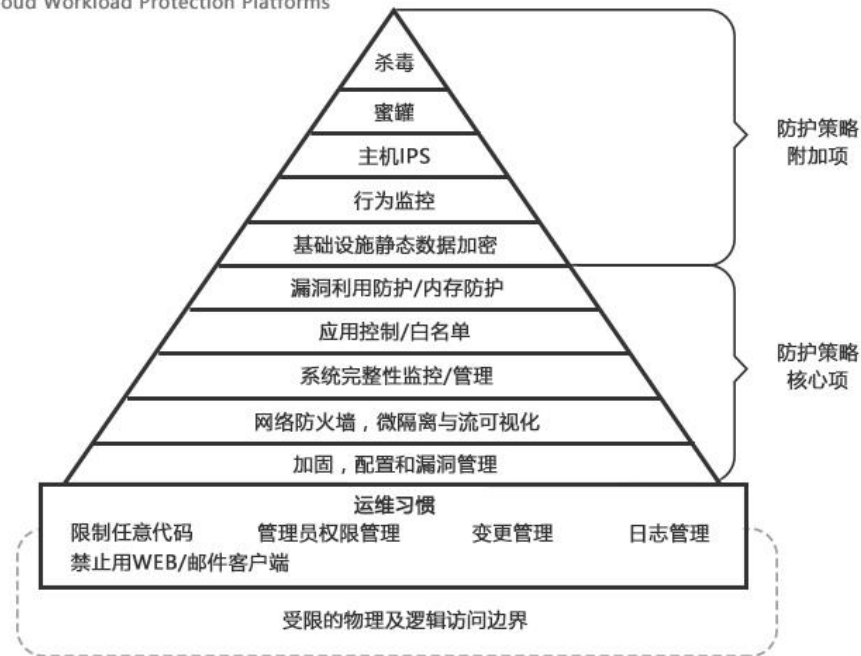
事后追溯

**云锁**是中国用户总量领先的主机安全产品，在国际上率先达到Gartner定义的cwpp（云 workload 保护平台）标准、EDR(终端检测与响应)+EPP(Endpoint Protection Platform)标准，兼容多种虚拟化架构和操作系统，可以高效支撑现代混合数据中心架构下的主机安全需求。


云锁基于服务器端轻量级agent，安全加固服务器操作系统及应用，云锁waf探针、rasp探针、内核加固探针能有效检测与抵御已知、未知恶意代码和黑客攻击；同时云锁融合资产管理、微隔离、攻击溯源、自动化运维、基线检查等强大功能，帮助用户高效安全运维服务器。

### CWPP

Cloud Workload Protection Platforms







# THANKS

**2019 北京网络安全大会**  
2019 BEIJING CYBER SECURITY CONFERENCE