顶级政府网站云防御平台

演讲人：彭戈

移动电话：13802940056

E-mail：pengg@knownsec.com

关于知道创宇

- **未知攻，焉知防**
  - 蝉联第一届&第二届中国信息安全攻防大赛总冠军
- **“创宇盾”防御的典型客户：**

投资方

Tencent 腾讯

- **700+** 员工
- 研发中心：北京、成都
- **20+** 个分公司及办事处

当前互联网形势：反动黑客活动猖獗

2017年5月5日20:05

2017年5月8日19:55

政策 & 法规

网络安全法 2017年6月1日 实行

第五十九条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

关键信息基础设施的运营者不履行本法第三十三条、第三十四条、第三十六条、第三十八条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款。

政策 & 法规

刑法修正案九 第二百八十六条 网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，有下列情形之一的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金：

（一）致使违法信息大量传播的；

（二）致使用户信息泄露，造成严重后果的

（三）致使刑事案件证据灭失，情节严重的；

（四）有其他严重情节的。

如何应对复杂的互联网安全形势？

1.建立网站和信息系统的监测机制

2.加强对于关键信息资产的保护能力
（尤其是暴露在互联网上的关键资产）

创宇盾是什么？

基于云与大数据技术的Web系统防御平台

全国
40
个处理中心

600G
骨干网带宽

数千台
攻击清洗服务器

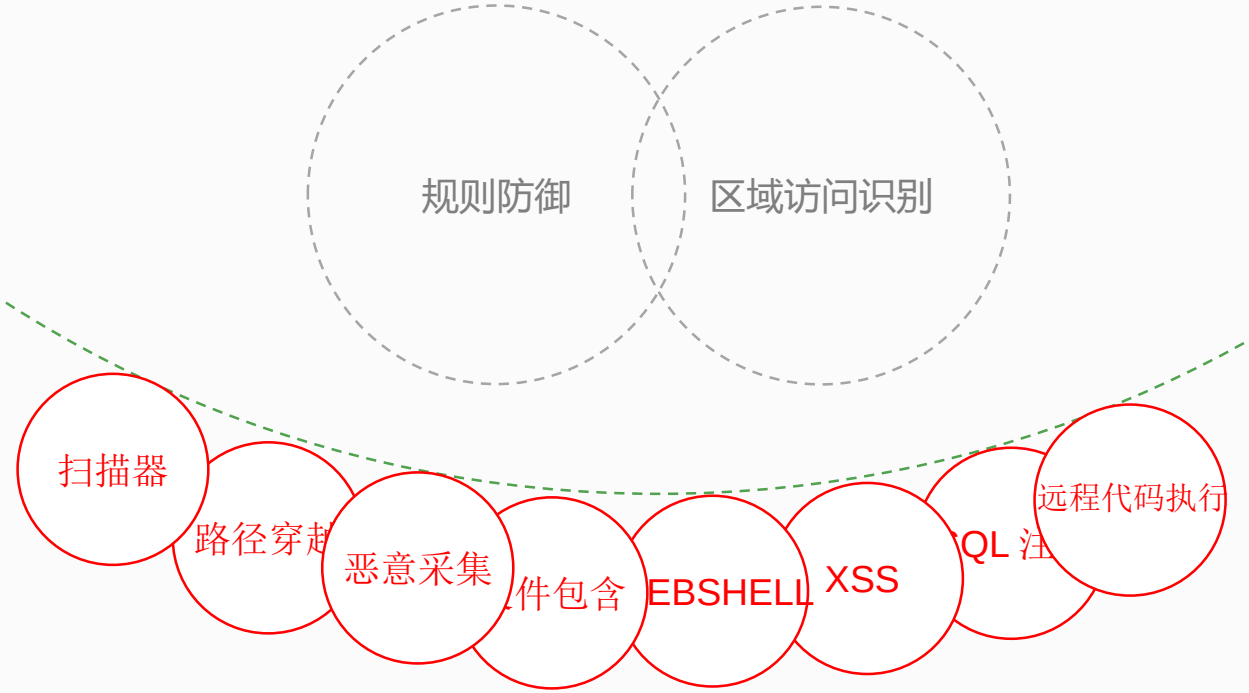
百余人
顶级
WEB安全团队
实时对全国云防御平台数据进行分析

创宇盾解决问题

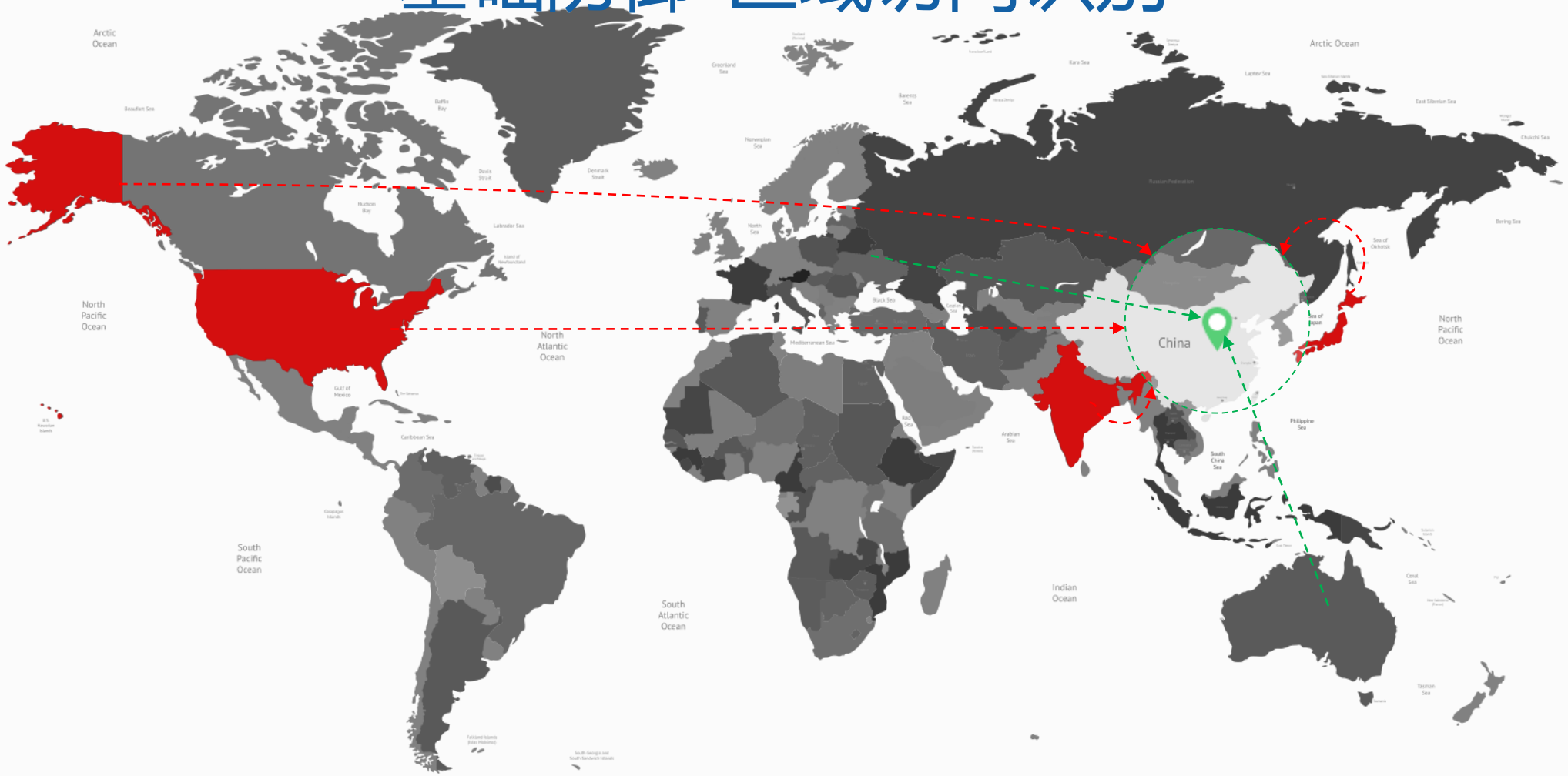
>

- 网站爬虫
- 应用层防护WAF
- 网页防篡改
- 抗DDOS
- 日志系统（60天）

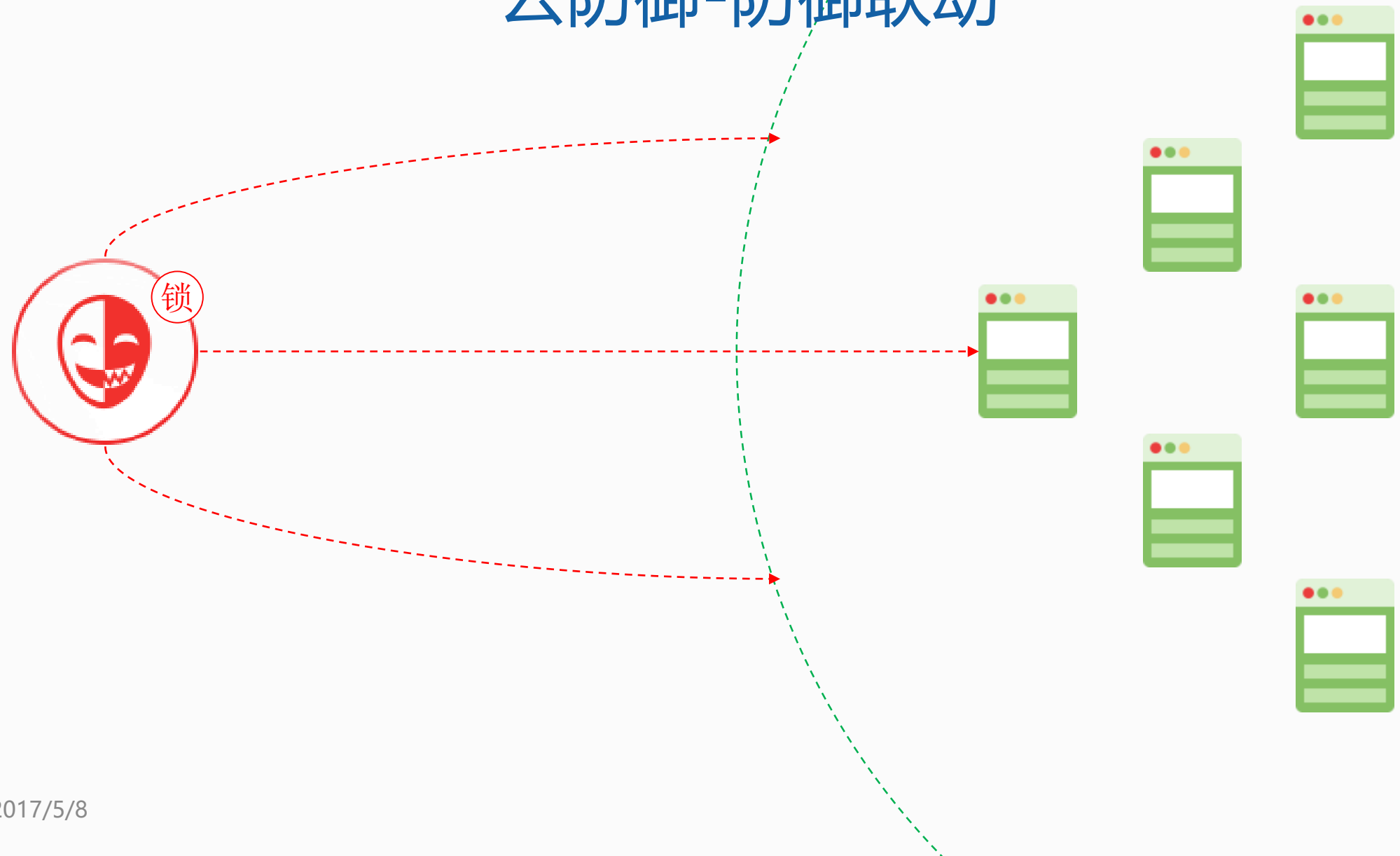
基础防御-规则防御



基础防御-区域访问识别


Arctic Ocean
North Pacific Ocean
North Atlantic Ocean
South Pacific Ocean
South Atlantic Ocean
Indian Ocean
China
被拒绝访问区域

云防御-防御联动

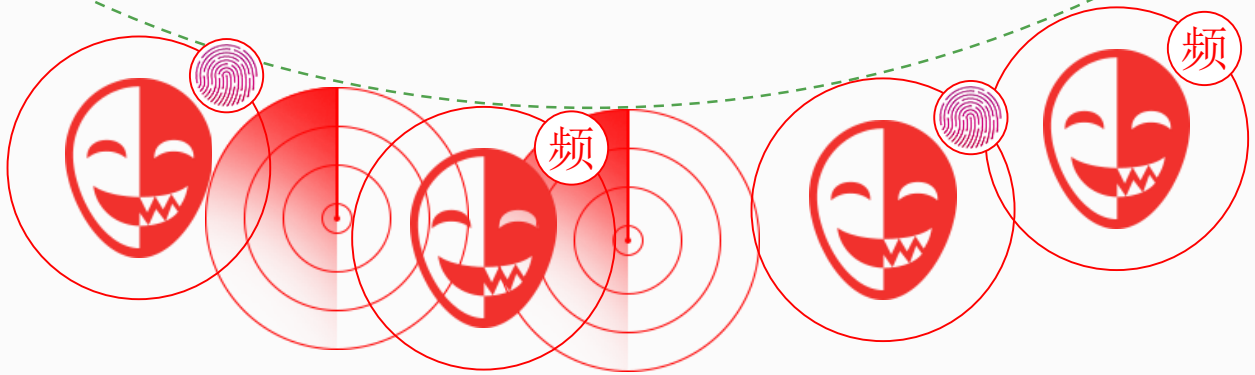


云防御-自动攻击识别

扫描器识别

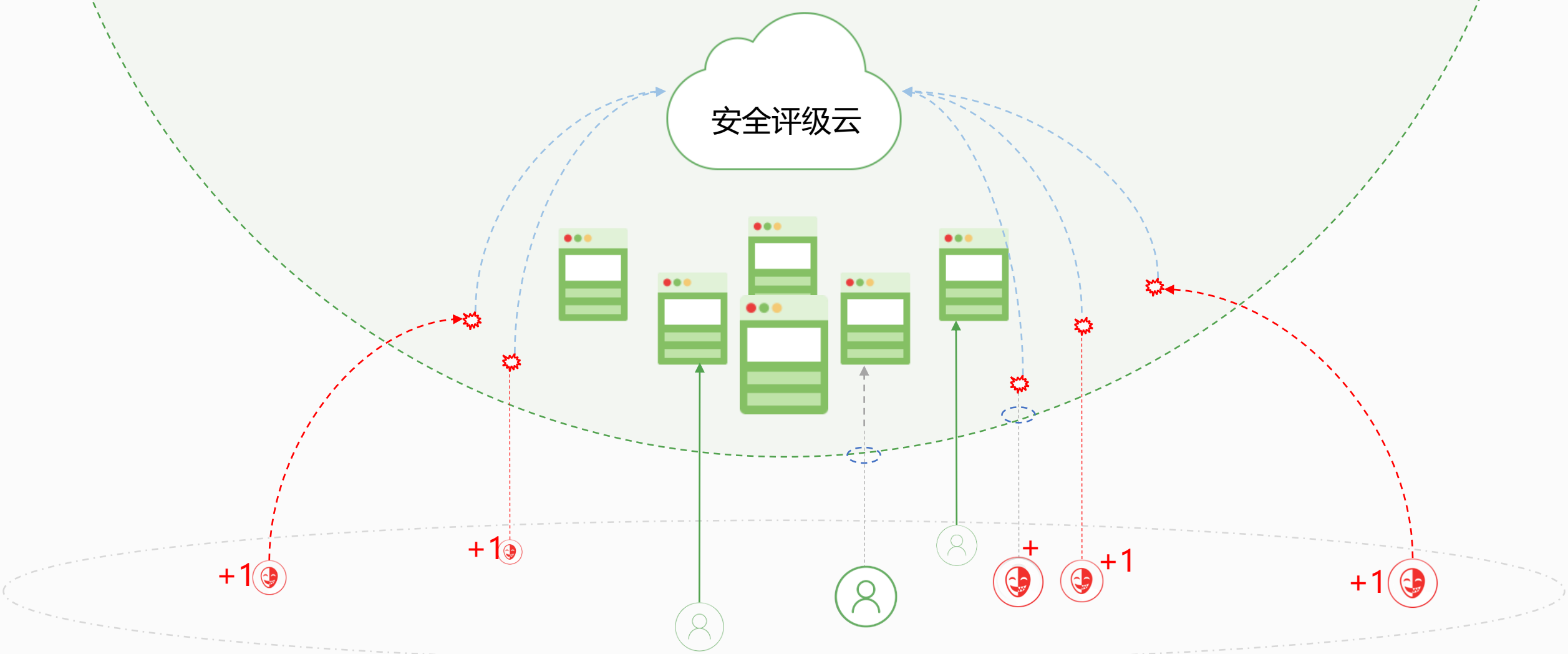
指纹识别

访问频率



专属防御-安全评级云

对所有访问IP进行安全评级并记录入云平台，并依据等级进行智能访问控制。



站锁

后台锁

对访问本站后台管理地址或某些敏感页面的IP进行访问控制。

关键资源锁

对指定页面、内容、站内元素、重要资源等进行完全锁定。

在线锁

当本站由于各种主动或被动原因无法访问时，由云平台提供不间断服务。

库带锁

防止“撞库”攻击。（即使完全没有漏洞的站点也有可能遭受“撞库”攻击）。

整站锁

在敏感或特殊时期锁定整站内容。

攻击防御

创宇盾是怎么保证网站不被黑客攻破？

站点

专属防御
防御能力
99.99%

基础防御
防御能力
70%

安全替身
防御能力
100%

云防御
防御能力
90%

整站锁

资源锁

安全评级云

防御联动

自动攻击识别

规则防御

区域访问识别

用户收益

按需提供的云防护

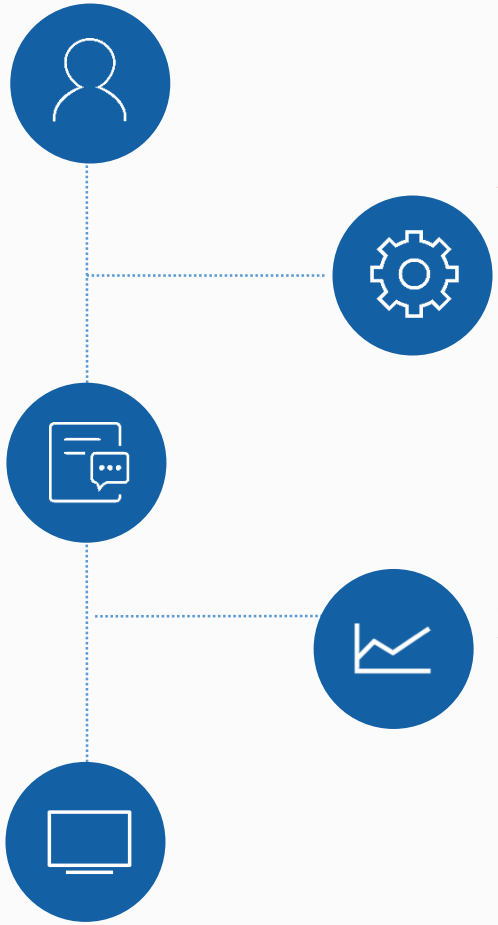
- 从防入侵，抗DDoS到永远在线
- 安全替身功能可重构网站内容

攻击溯源

- 提供最专业的反向APT工具与支持，对攻击来源了然于胸，为攻击取证提供详尽依据

直观展现

- 结合地理信息图直观展现网络攻击情况
- 多视角、详尽的报表帮助用户及时了解Web系统安全态势



简单部署，零维护

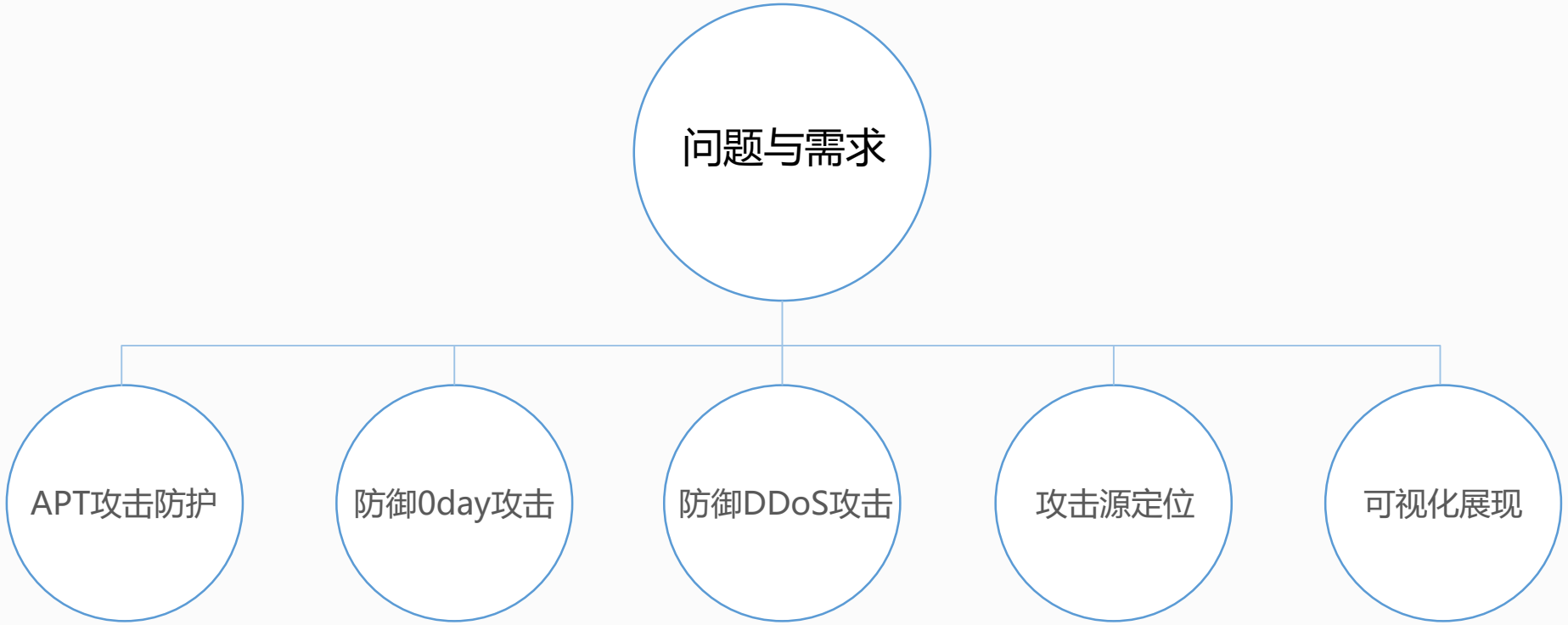
- 部署时只需重新设置DNS，无需更改架构设计和设备配置；百余人专业团队实时维护云防御策略，保证用户的防御体系高枕无忧

大数据支持

- 通过大数据挖掘分析得到的安全评级结果，清晰识别潜在威胁

客户案例1-公安部

背景：公安部已经部署防火墙、IPS/IPS、WAF等安全设备



客户案例1—公安部

中华人民共和国公安部

部署创宇盾后，平均每天抵御约

5万 次恶意扫描

10几万 次信息收集

2万 次SQL注入攻击

1.5万 次跨站注入攻击

其他攻击约加起来在万次以上

展开

攻击者

IP	位置	类型	次数
54.243.164.122	Ashburn	SCANNER	3
107.167.176.81	-	SCANNER	1
103.241.48.57	-	SCANNER	1

目标

域名	位置
pintu360.com	Beijing
jsnews.jschina.com.cn	Nanjing
www.xmxyk.net	Beijing

攻击者来源

地区	次数
China	4173
United States	525
Hong Kong	417

目标地区

地区	次数
China	5053
United States	117
Virgin Islands, British	96

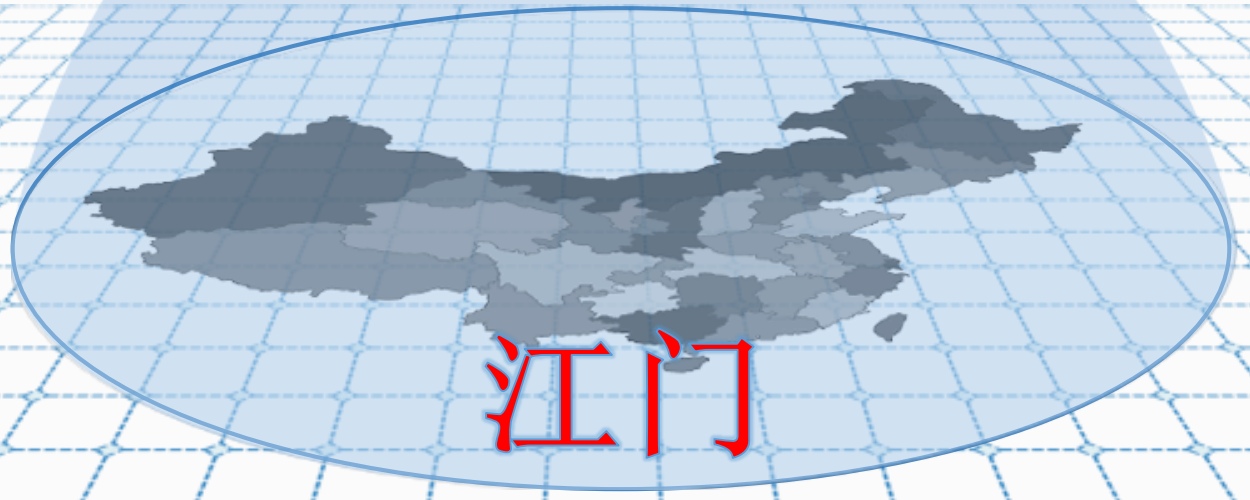
攻击类型

类型
SCANNER
SQLI
COLLECTOR

典型案例2　江门市直单位网站群60+ 整体云防御

- 上线半年多

- 被篡改 零
- 被通报 零



接入主站数 3,037
未接入 112
防御子站数 10000
未防御 434
高防子站数 3,422
中防子站数 2,800
低防子站数 3,778
今日攻击数 831,273
昨日 1285306
今日攻击态势
500000
00:00
WEBSHELL
LRFI
COD
XSS
FILEI
SQLI

全国
2925
0
3037
开启防御站点数量

站点分布 TOP5
江西省 6067
广东省 91136
浙江省 6944
北京市 13956
四川省 9096

站点攻击热点目标TOP5

攻击次数 831,273

攻击IP地理位置分布
中国
中国香港
比利时
美国
马来西亚

攻击类型统计
53,381
WEBSHELL
SQLI
FILEI
XSS
CODE
LRFI

攻击者列表
120. 27. 226. 163 中国 221, 955
218. 30. 106. 142 34, 672

http://finance.gansudaily.com.cn/system/20...
攻击者IP:182.50.121.216 中国

老彭

广东 广州

扫一扫上面的二维码图案，加我微信

谢谢！

KNOWNSEC
知 道 创 宇