第五届安天网络安全冬训营

网络空间威胁对抗技术与实战研讨会

暨 关键信息基础设施保护实践论坛

从微入手、层层防御

山石网科

王中斌

红旗漫卷

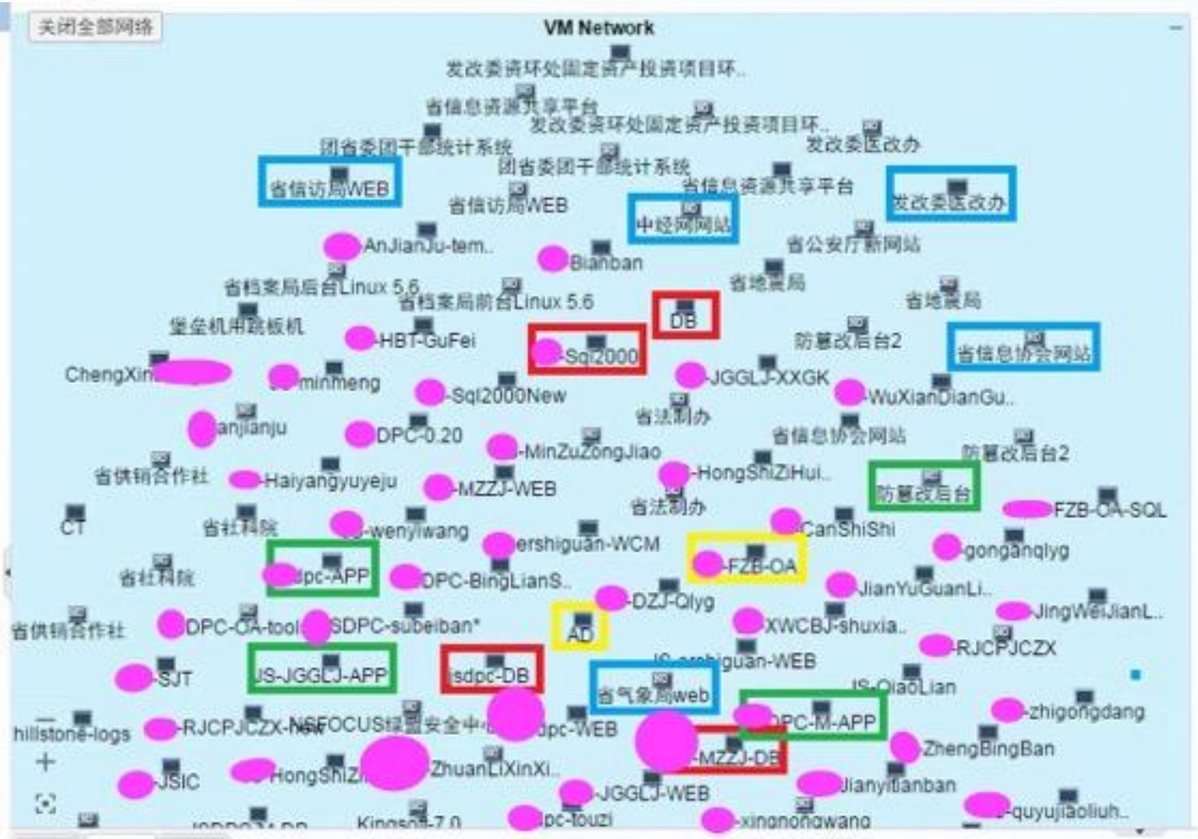
敌情想定是前提，网络安全实战化

提纲

- 从微入手：零信任模型、微分段和可视化
- 层层防御：网络安全的巷战时代

1 从微入手，零信任、微分段和可视化

虚拟化数据中心，你无法保护你看不见的内容

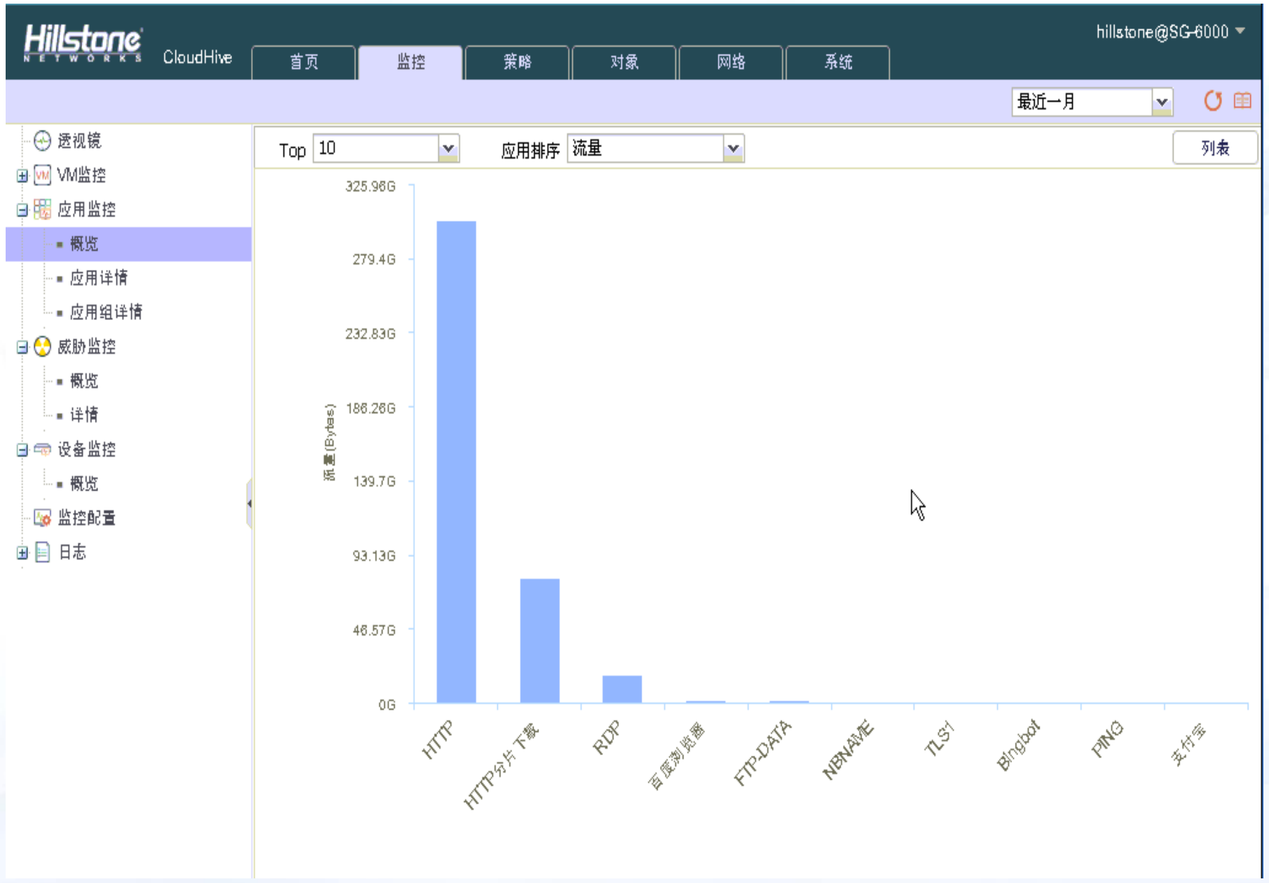


造成原因

- 虚拟化技术放大了传统安全域
- 虚拟化环境，没有明确物理边界
- 云内不可视
- 安全责任划分不明
- 维护工作量巨大

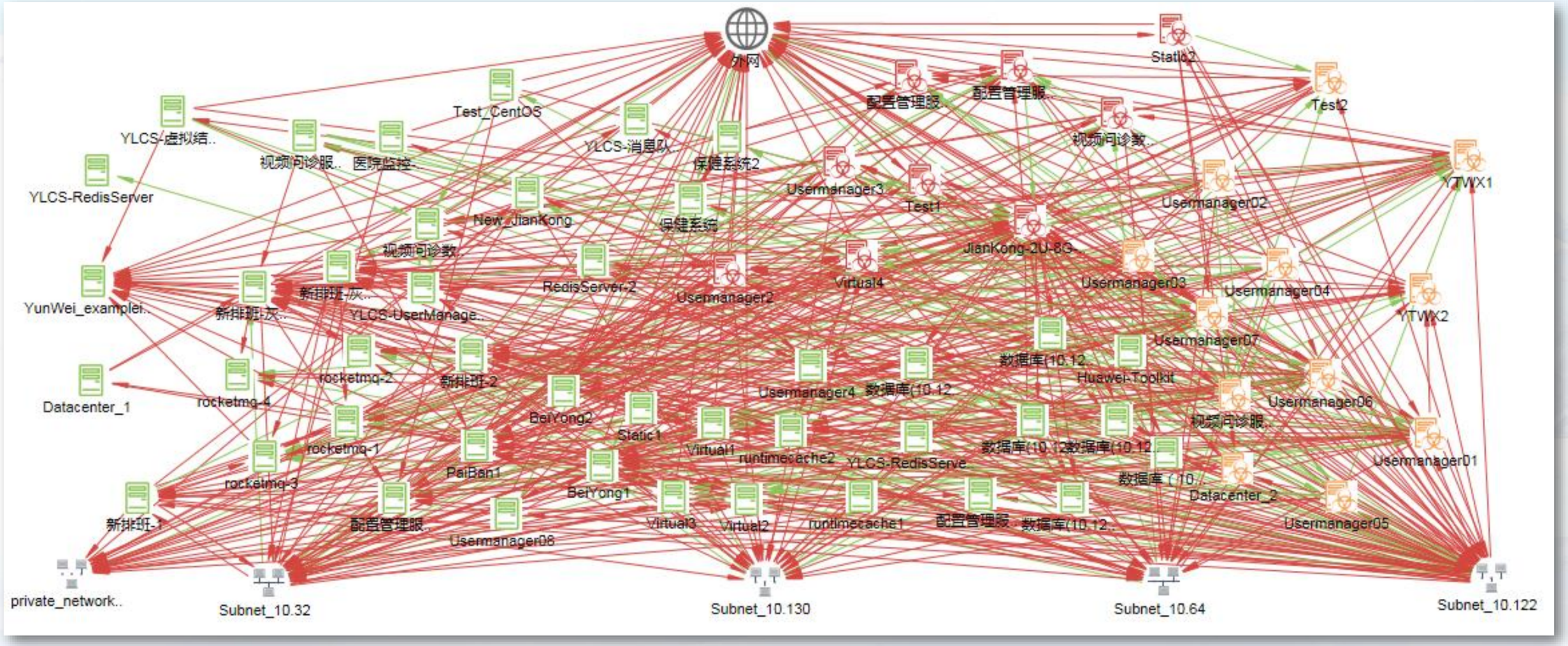
一旦内部某个业务服务器中招，隐蔽性强，危害大

- 传统的安全防护在外部，策略针对外向内攻击
- 在地下黑产中，服务器是优质“肉机”！



1. 某高校“内部缴费平台虚机”发起向外的总计300GHTTP访问
2. 目的地直指国内某网站
3. 同时被美国主机频繁联系
4. 最终确认“内部缴费平台虚机” 已被黑客控制

部分物理环境，问题同样存在



Gartner 2016 10大技术之一：微分段和可视化

1.Cloud Access Security Brokers

云端访问的安全代理（CASBs）技术

2.Endpoint Detection and Response

终端检测与响应（EDR）技术

3.Nonsignature Approaches for Endpoint Prevention

终端防御的非特征方法

4.User and Entity Behavioral Analytics

用户和实体的行为分析（UEBA）技术

5.Microsegmentation and Flow Visibility

微粒度和流量可视化技术

6.Security Testing for DevOps (DevSecOps)

面向开发运维（安全开发运维）的安全测试技术

7.Intelligence-Driven Security Operations Center Orchestration Solutions

情报驱动的安全管理中心（SOC）预处理技术

8.Remote Browser

远程浏览器技术

9.Deception

陷阱技术

10.Pervasive Trust Services

广义可信服务技术

“Microsegmentation Sample Vendors: Amazon, Arkin, Catbird, CloudPassage, GuardiCore, Hillstone Networks, Illumio, Trend Micro, vArmour and Vmware”

Gartner, Best Practices for Detecting and Mitigating Advanced Threats, 2016, Lawrence Pingree etc.

Gartner于2016年6月13-6月16日召开了名为《高德纳安全和风险管理峰会2016》（Gartner Security & Risk Management Summit 2016），公布了信息安全的10大技术

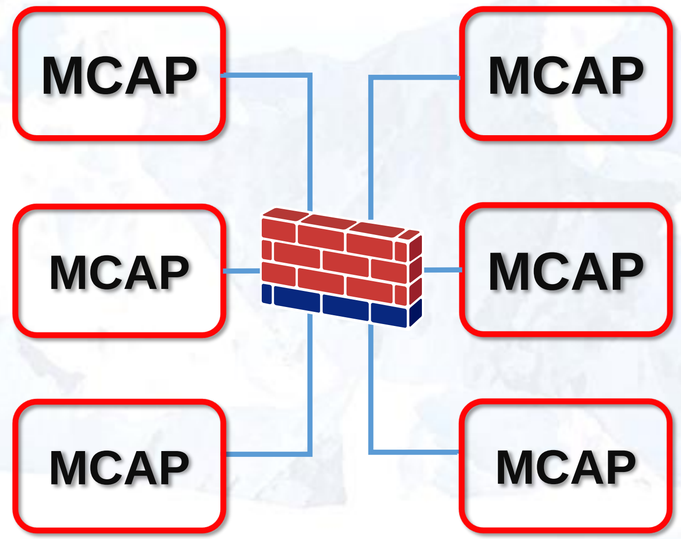
Forrester Research提出的零信任模型

零信任模型

- 围绕数据资产，由内到外设计网络，构筑安全防护。
- 确保对所有资源的访问行为都是安全的，不论是来自内部还是外部。
- 所有访问都不被信任，都被核查，采用最低特权，严格访问控制。
- 检查和记录所有流量，实现流量的可视化

实现思路

- 围绕不同的数据资产划分安全域 （Microcore and Perimeter，微型核心与边界MCAP ）
- 平行对等互联MCAP
- 核心部署高度集成隔离网关（NGFW or UTM）
- 集中管理
- 实现完整网络的流量和威胁可视



如何微分段，可以从如下几点考虑

虚机间互访关系?

- 虚机间都有哪些交互行为?
- 这条业务链是必要的么?
- 等等

跑什么应用?

- 云内还有哪些未知的应用
- 是否存在违规应用
- 应用使用频率和时间是否异常
- 等等

有异常行为么?

- 是否暗藏威胁操作?
- 交互过程是否异常?
- 传输的文件是否带有病毒?
- 等等

资源使用合理么?

- 网络划分合理么?
- 虚机分布状况合理么?
- 带宽占用合理么?
- 连接数是不是太高了?
- 等等

管理员需掌控

客户案例

1. 帮助客户理清了复杂内网环境的互访关系

2. 快速过滤，查看某个指定服务器的访问关系

3. 发现该服务器和其他服务器的异常互访流量

2 层层防御，网络安全的巷战时代

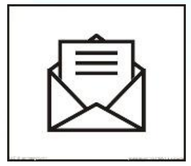
层层防御：针对高级威胁全生命周期的防护策略

	攻击准备		攻击过程		攻陷后		
攻	侦查	恶意软件组装	恶意软件传输	执行攻陷	远程控制	数据发现	数据窃取
防	入侵防御、病毒过滤 基于特征检测		沙箱检测 Payload行为分析		NTA 基于行为分析		

以勒索软件Locky举例

- 通过社工手段向受害者发送垃圾邮件；
- 打开email中恶意宏代码word、执行宏代码下载locky主体
- C&C、黑客远程控制主机
- 遍历磁盘文件夹，加密本地文件；
- 弹出勒索提示信息；

如何防御？



- 通过社工手段向受害者发送垃圾邮件

- 打开email中恶意宏代码word
- 执行宏代码下载locky主体

- C&C
- 黑客远程控制主机

- 遍历磁盘文件夹，加密本地文件

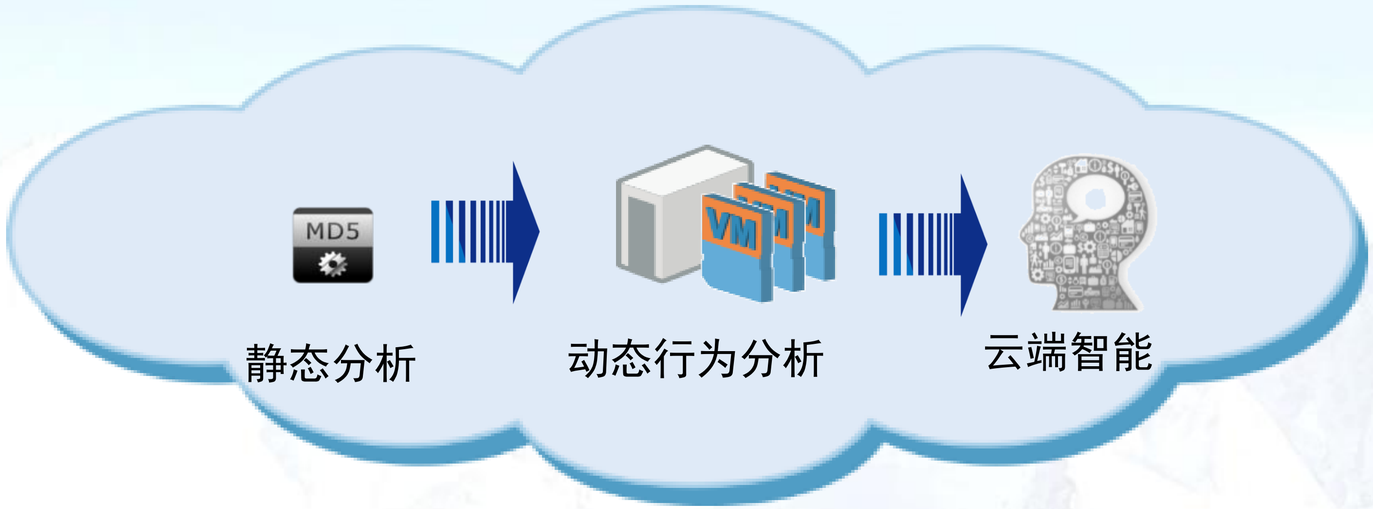
- 弹出勒索提示信息

攻

垃圾邮件过滤	病毒/沙箱检测	Botnet检测	NTA
基于特征检测	文件行为分析	C&C服务器检测	异常行为分析

防

基于云端的沙箱检测方案



未知文件提交

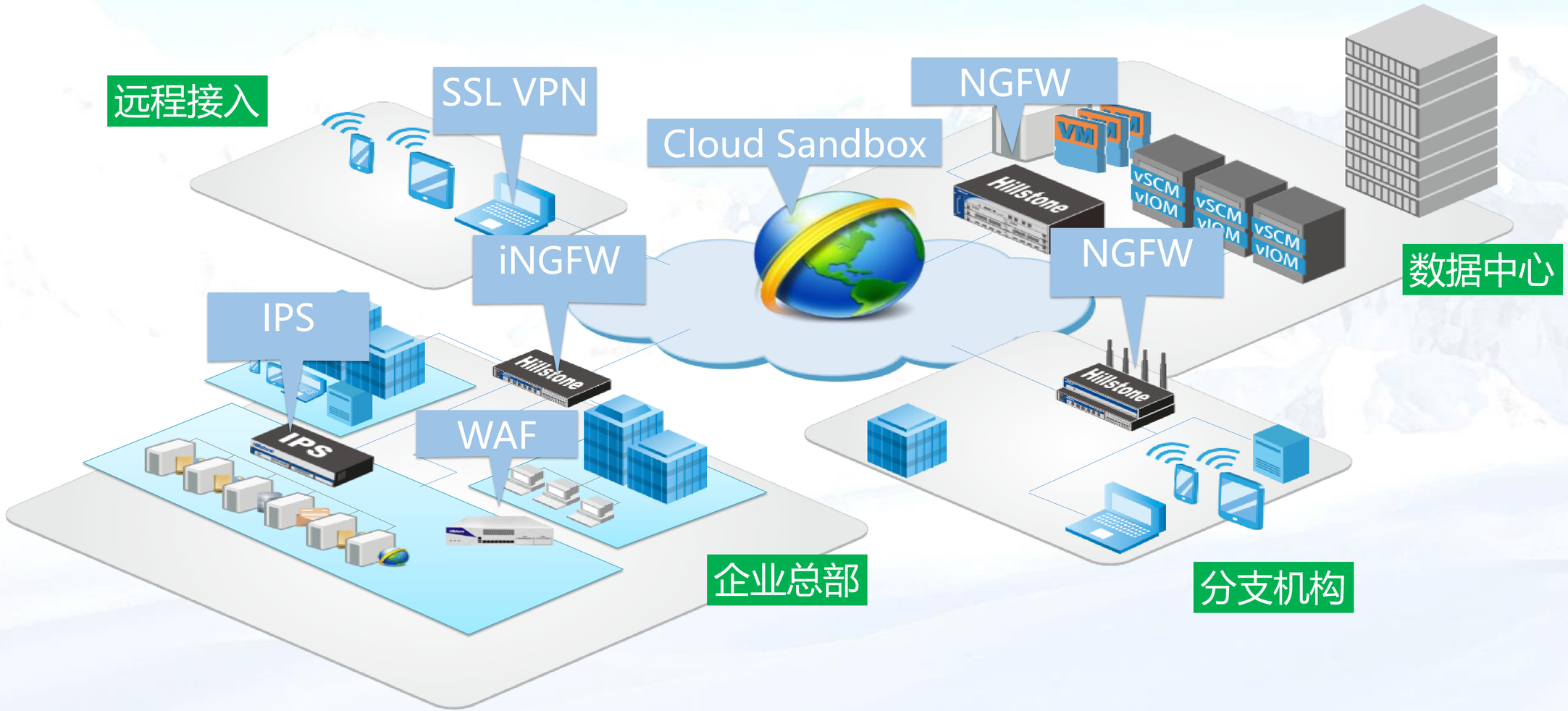
文件分析报告

威胁特征更新

本地检测及防御技术


层层防御：从边界安全部署开启

- 基于应用和用户的策略控制，高性能NGFW
- 对已知威胁的防范（IPS），对web应用服务器的保护（WAF）
- 对未知威胁的防护（沙箱 + NTA）



有了边界，内网就真的安全了吗?

边界安全，是基于内部网络是安全可信的假设性威胁模型，所有威胁都来自外网。

- 多态和变形技术（如加壳、代码混淆等）
- 利用未知的漏洞（零日攻击）
- 威胁潜伏扩散（APT攻击）
- U病毒带入（BYOD）
- 外部感染病毒（BYOD）

有了边界，内网就真的安全了吗?

如果城墙失守，我们该如何保卫我们的城池?

网络安全的巷战时代

有了边界，内网就真的安全了吗？

- 1942年7月～1943年2月，斯大林格勒保卫战
- 第二次世界大战的关键转折点，法西斯德国从此一败涂地；
- 14万的德军葬身于城内；

巷战起到了关键作用！

当网络边界被攻陷以后

漏洞利用

后门植入

僵尸网络

命令控制

内网侦测

内网扩散

数据窃取

黑客胜利了?

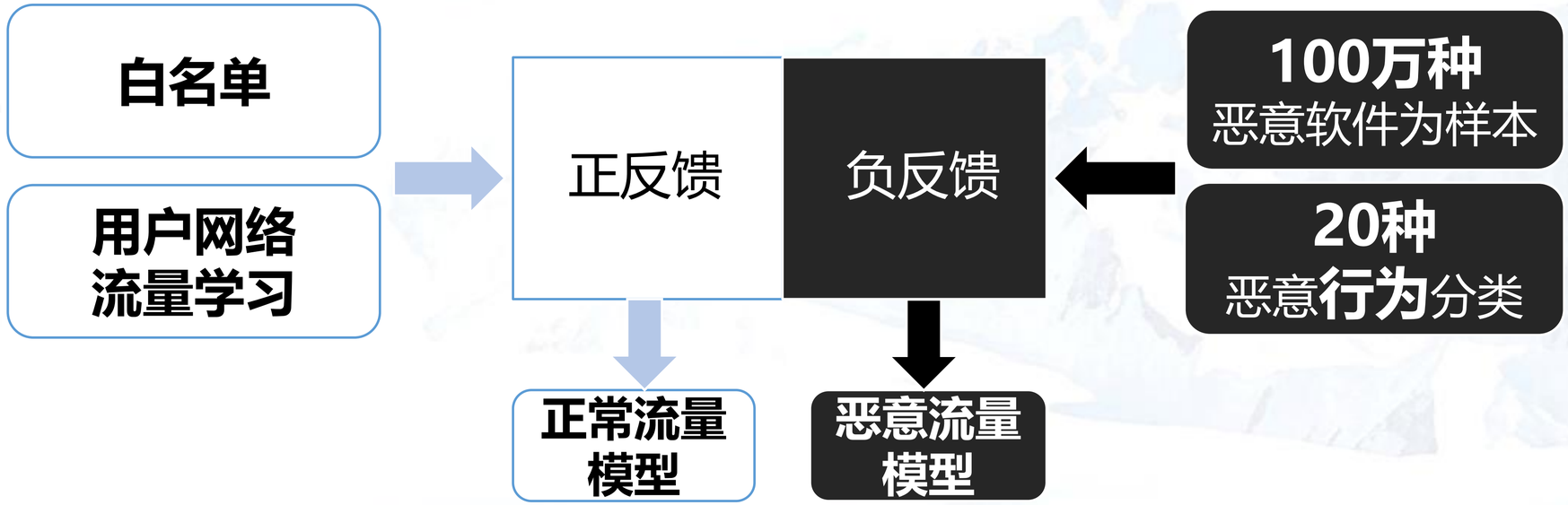
安全防御失效了?

》》》 Long Way!! 《《《

》》》 Long Time! 《《《

内网安全，能做的，还有很多！

内网安全手段：正负反馈训练

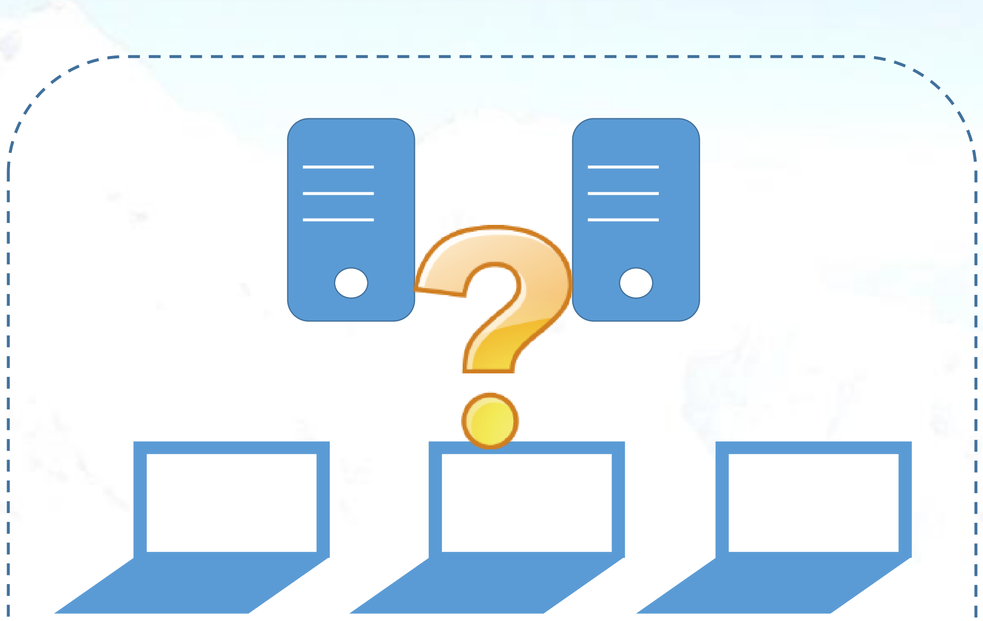


内网安全手段：负反馈训练

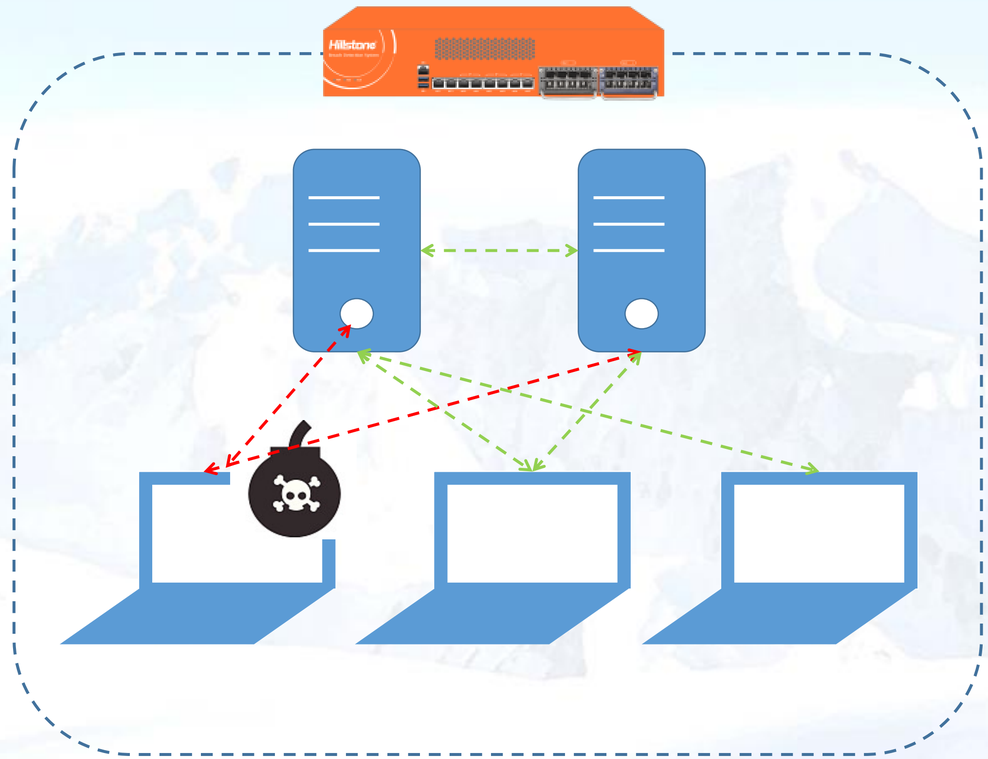
数学建模　　机器学习　　行为归类　　威胁判定

- **圆心：**基于威胁情报收集并加工处理的已知恶意行为；（预定义的负反馈）
- **恶意行为判定：**越接近圆心，威胁疑似度越高；
- **行为族：**分为20类行为族，以确定不同的风险和危害等级；

内网安全手段：正反馈发现异常互访网络流量



内网的主机和服务器之间存在怎样的访问关系?



内网主机/服务器对象互访关系拓扑还原呈现，基于网络流量行为基线，发现异常访问。

可视，内网威胁呈现

红色：存在高风险威胁行为

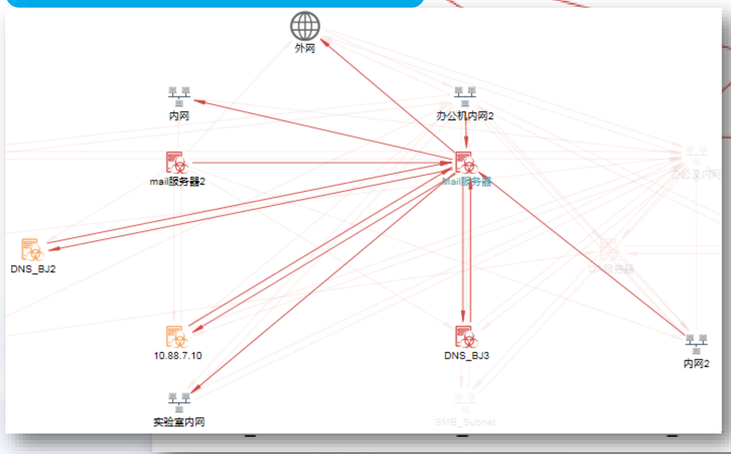
橙色：存在低风险威胁行为

绿色：暂无威胁行为风险

服务器威胁事件列表

	威胁名称	威胁类型	威胁程度	源	目的	最后一次检测时间	威胁数量
+	Suspicious Domain Name Generated by DGA	发起CNC连接	100%	121.18.168.232	10.188.7.10	2017/07/30 11:30:02	41
+	Domain Name on Blacklist	发起CNC连接	100%	60.222.224.144	10.188.7.10	2017/07/29 13:47:45	30
+	Suspicious Domain Name Generated by DGA	发起CNC连接	100%	38.102.150.29	10.188.7.10	2017/07/29 11:45:32	4
	Suspicious Domain Name Generated by DGA	发起CNC连接	100%	156.154.126.65	10.188.7.10	2017/07/29 11:42:42	1
+	Suspicious Domain Name Generated by DGA	发起CNC连接	100%	10.66.5.213	10.188.7.10	2017/07/26 08:29:51	198
+	Domain Name on Blacklist	发起CNC连接	100%	10.66.5.213	10.188.7.10	2017/07/25 23:58:04	35
+	Domain Name Hijacked By ISP	受到外网的攻击	50%	202.106.196.28	10.188.7.10	2017/07/25 11:11:00	4
	Suspicious Domain Name Generated by DGA	发起CNC连接	100%	205.251.195.172	10.188.7.10	2017/07/25 09:31:51	1

服务器威胁范围

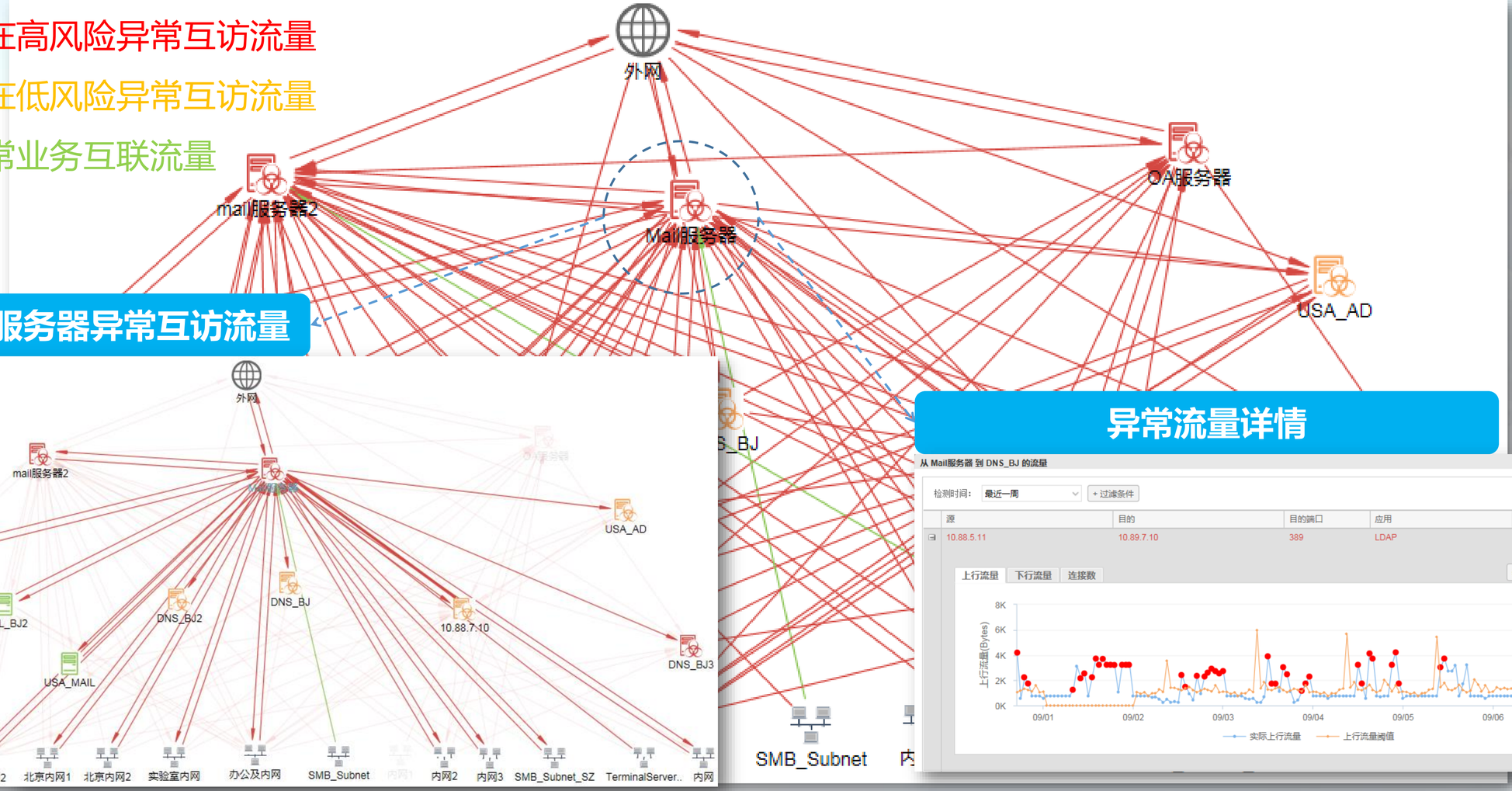


可视，内网异常互访呈现

红色：潜在高风险异常互访流量

橙色：潜在低风险异常互访流量

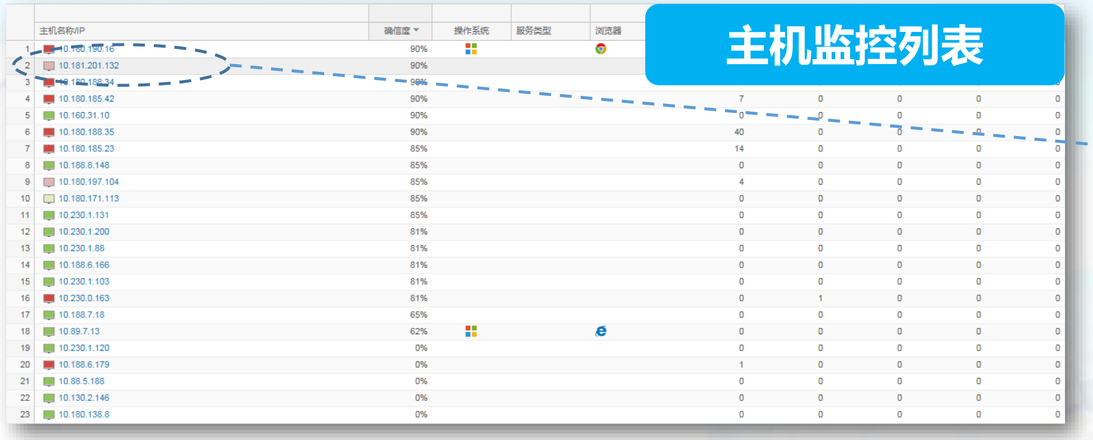
绿色：正常业务互联流量



邮件服务器异常互访流量

异常流量详情

可视，主机异常流量监控



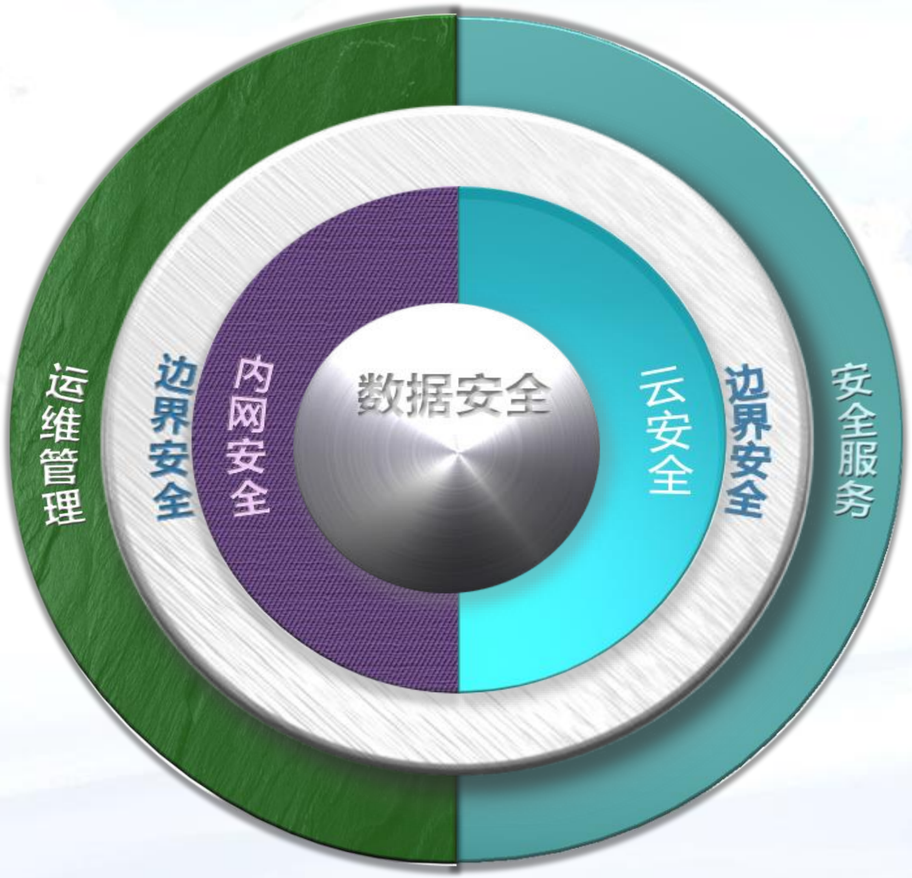
主机监控列表

异常流量

蓝色：实际网络行为

绿色：学习或检测中的网络行为基线

更多细节，请关注山石网科



第五届安天网络安全冬训营

网络空间威胁对抗技术与实战研讨会

暨 关键信息基础设施保护实践论坛

Thank You

wtc.antiy.cn

红旗漫卷

敌情想定是前提，网络安全实战化