新一代智能防火墙
- 基于大数据分析的全面网络安全架构

尚 进
研发资深总监, 山石网络

2014/05/16

目录

1 网络安全的现状

2 现有方案面临的挑战

3 山石新一代智能防火墙

4 山石智能防火墙中的数据分析技术

网络安全的现状

- 侵入是不可避免的

“目前世界范围内的主机只有两种状态 – 已检测到的侵入和还没有检测到的侵入”

- 传统特征库方法无法防御当前攻击

  APT, 未知 Malware

  漏洞, Zero-Day

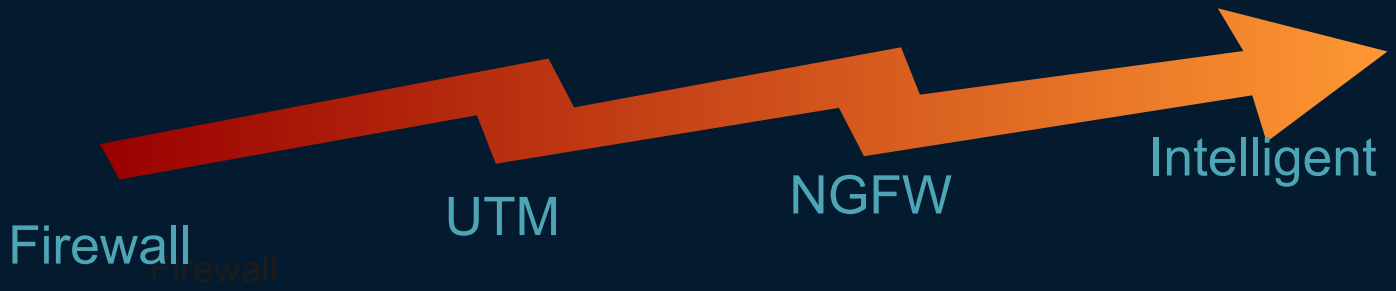
- 恶意软件和攻击的规模

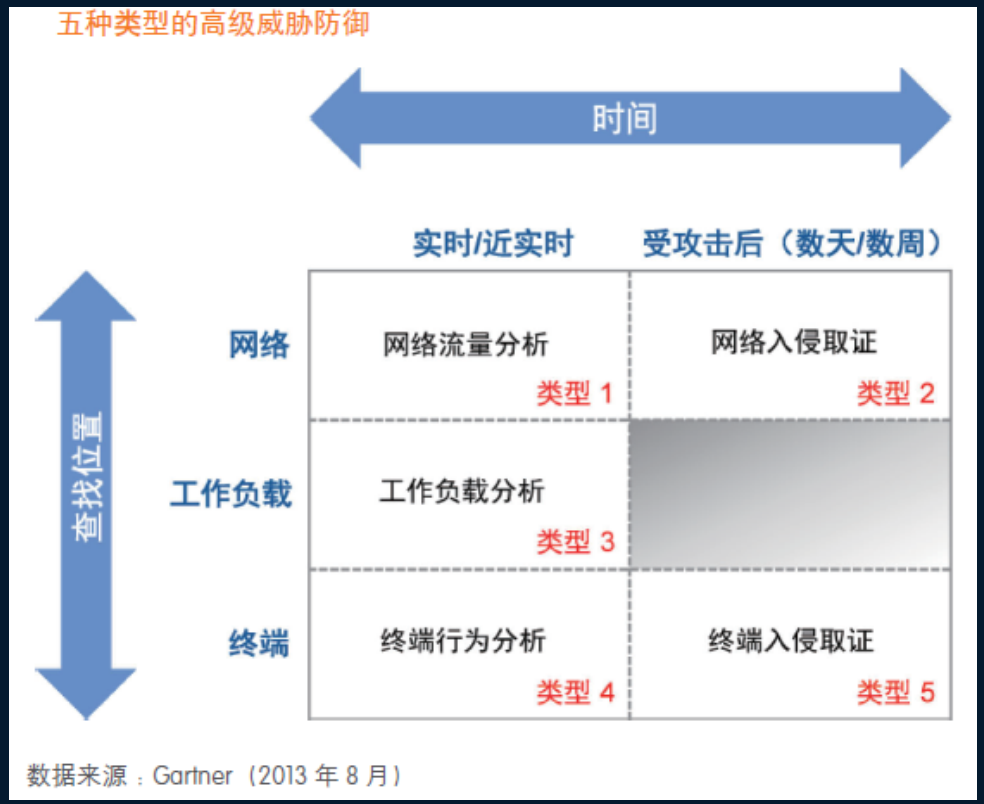
  - 每天全世界大约200, 000 新malware样本，厂商样本库过亿，样本家族在几千范围，绝大多数是变种。
  - DDoS Spamhaus, 300G 攻击

现有方案面临的挑战

- 只关注阻挡没有考虑侵入后检测防御的重要性和长期性;对Malware完整生命周期的检测不够
- 沙箱 (Sandboxing/Virtual Machine) :逃逸手段众多
- 行为异常分析: 观测对象单一, 对时间、场景的自适应学习不够
- DDoS/CC/扫描攻击: 单一流量维度, 固定阈值, 误报多, 识别晚
- 网络边界模糊:移动, 云计算, 迁移

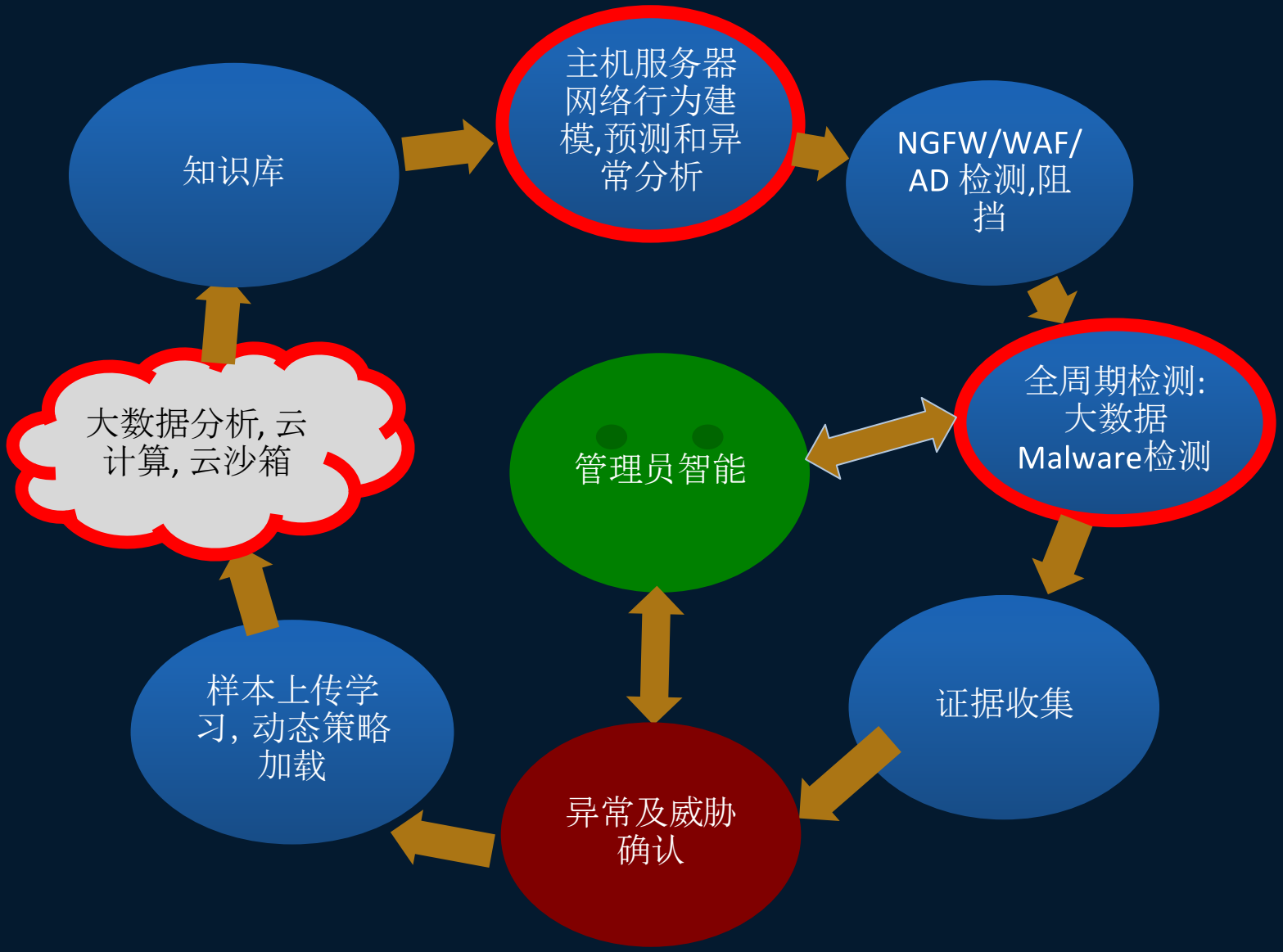
下一代网络安全解决方案





预测，阻挡，检测，调控等全方位、全生命周期的监控

山石全面网络安全架构: 智能防火墙



网络行为异常分析模型

- ✓ 对象:主机, 服务器的网络行为
- ✓ 数据挖掘: 多维度，L3-L7, 应用
- ✓ 定制的针对网络行为的自适应实时建模和异常检测算法

异常发现更早, 异常源更准确

- ✓ 服务器:DDoS, CC, 扫描
- ✓ 主机: Bot, Spam, 等
- ✓ 主机、服务器行为关联

基于大数据的Malware 分析和检测

- ✓ 云端实验室
- ✓ 云端数据挖掘
- ✓ 云端Machine learning
- ✓ 智能知识库的下发
- ✓ 智能再学习

总结

- 网络安全面临的挑战呼唤全方位、全周期、多角度的新一代全面智能网关
- 基于数据挖掘、Machine Learning、云计算的全新数据分析技术为新一代智能网关提供了强大的技术支撑
- 山石智能防火墙是新一代智能网关的领跑者

非常感谢！

如有问题，请联系我们

服务热线：400-828-6655

www.hillstonenet.com.cn