



# 智能流量分析 深挖高级威胁

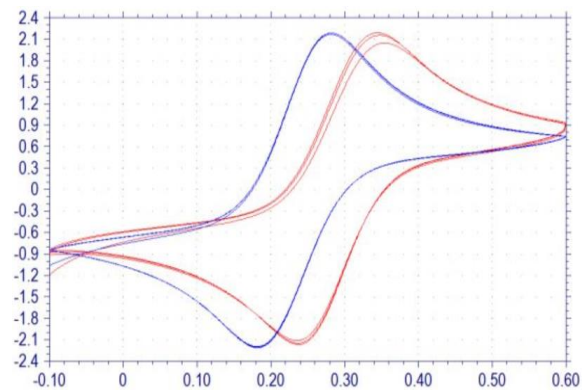
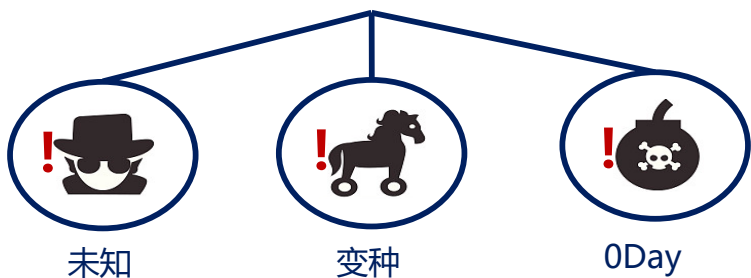
贾彬

山石网科 资深营销总监

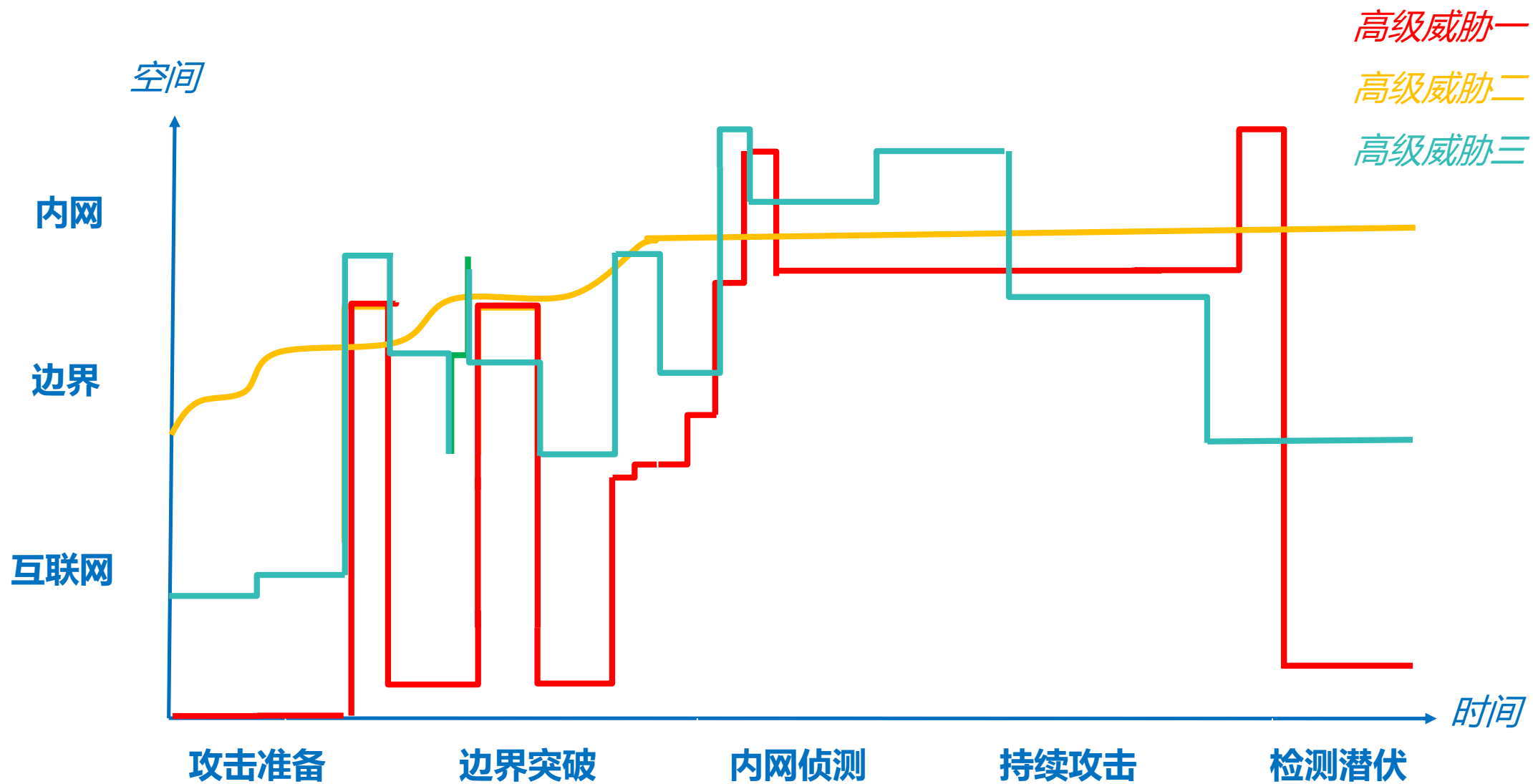
## 目录

1. 高级威胁不在神秘的面纱
2. 揭开面纱的NTA网络流量分析技术
3. 山石智·感利用NTA技术检测发现高级威胁





利用 **先进的攻击手段** 对 **特定目标** 进行 **长期持续性** 网络攻击的攻击形式





- **穿透网络边界防护**  
签名指纹匹配检测技术依赖于特征库
- **隐藏进入网络的真实意图**  
安全意识意识薄弱, 疏于防范
- **绕开网络边界的检测及防护**  
互联网移动办公时代的负面影响
- **内部网络“假设性”安全**  
传统“筑强”防护的思路误区

新型网络攻击工具

多样化的传播路径

安全建设及意识匮乏

随着空间和时间的变化，网络威胁行为具有不同的特征和属性.....

但是，无论网络威胁如何变化，依然有固定的行为模式

## Market Guide for Network Traffic Analysis

Published: 28 February 2019 ID: G00381265

Analyst(s): Lawrence Orans, Jeremy D'Hoinne, Sanjit Ganguli

Network traffic analysis is a new market, with many vendors entering since 2016. Here, we analyze the key NTA vendors to be considered by security and risk management leaders.

### Key Findings

- Applying behavioral analysis to network traffic is helping enterprises detect suspicious traffic that other security tools are missing.
- The barrier to entry in this market is low, and the market is crowded; many vendors can monitor traffic from a SPAN port and apply well-known behavioral techniques to detect suspicious traffic.

NTA是一种功能和能力，而非纯粹的一个产品；

NTA融合了传统的基于规则的检测技术，以及机器学习、数据建模和其他高级分析技术；

NTA针对关键的网络区域对东西向和南北向的流量进行分析，而不会试图对全网进行监测。

NTA用以检测企业网络中的可疑行为，尤其是失陷后的痕迹。

——Gartner



成立于1979年，就IT的研究、发展、评估、应用、市场领域，协助客户进行市场分析、技术选择、项目论证、投资决策。

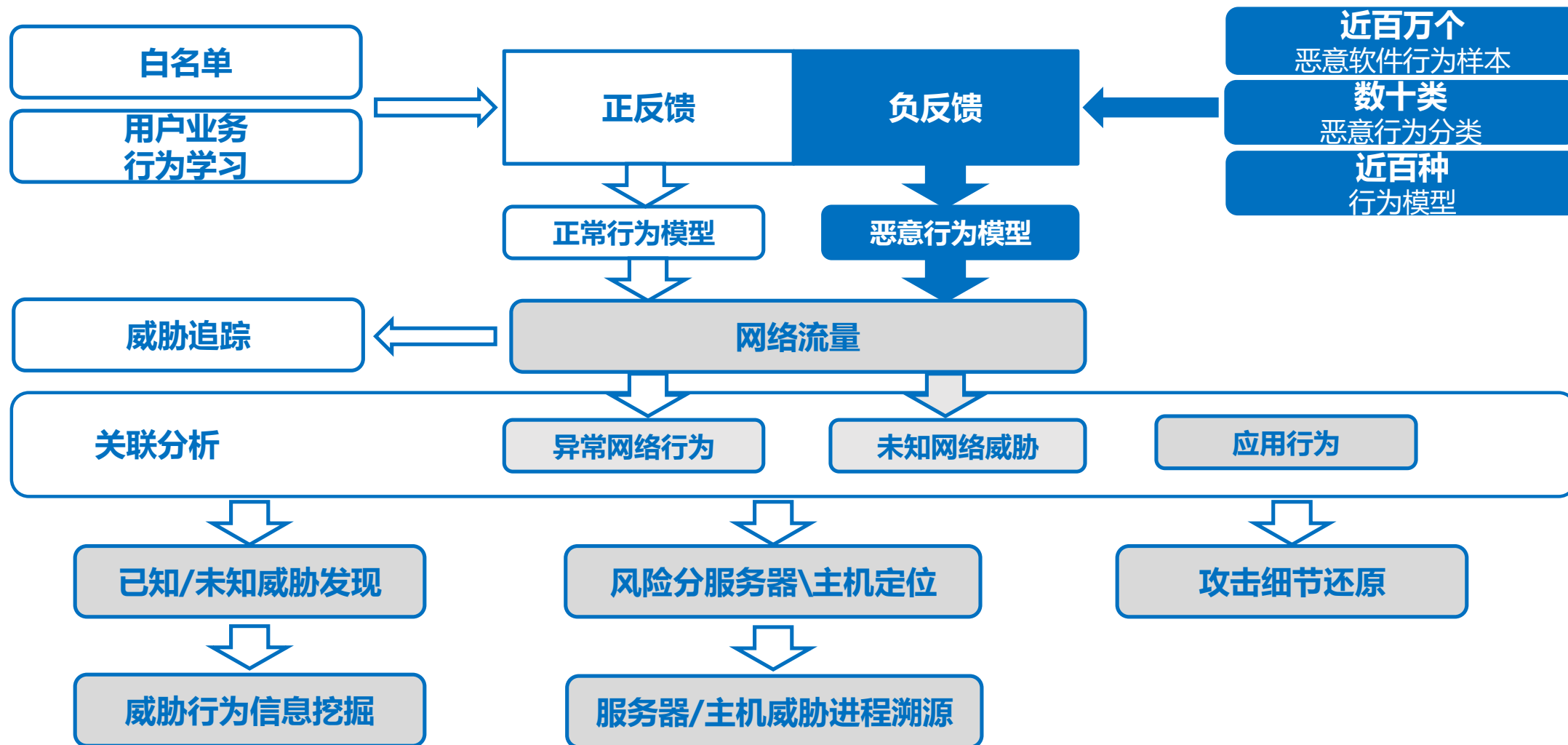


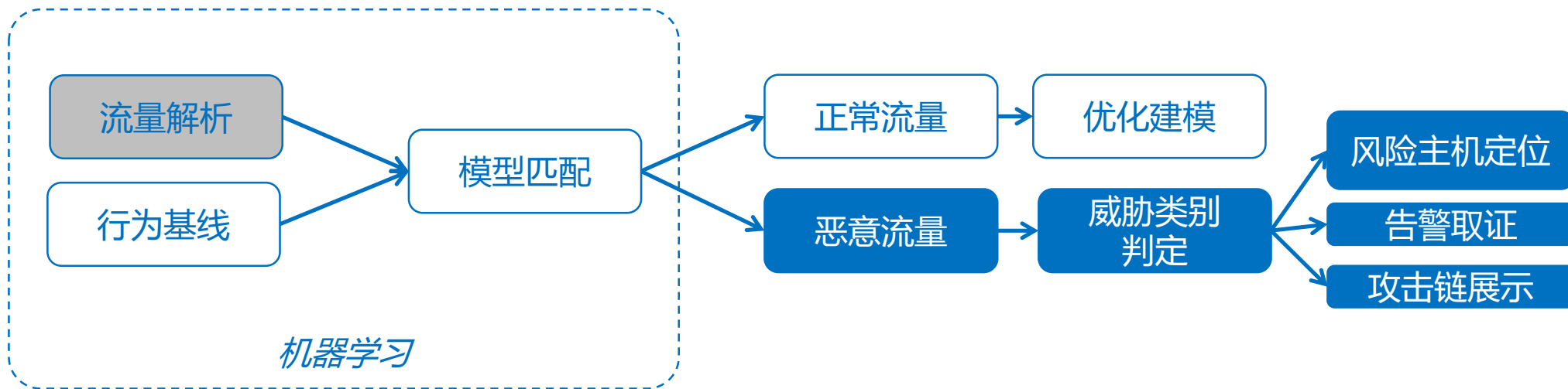


## Garnter发布2017年的11大顶尖信息安全技术

1. 云工作负载保护平台 (Cloud Workload Protection Platform, CWPP)
2. 远程浏览器技术 (RemoteBrowser)
3. 欺骗技术 (Deception)
4. 端点检测和响应 (EDR)
5. 网络流量分析 (Networktraffic analysis, NTA)
6. 管理检测和响应 (MDR)
7. 微分段 (Microsegmentation)
8. 软件定义边界 (Software-defined perimeters, SDP)
9. 云端访问安全代理技术 (Cloudaccess security brokers, CASBs)
10. 面向DevSecOps的OSS安全扫描和软件组成分析技术 (OSS security scanning and software composition analysis forDevSecOps)
11. 容器安全 (Containersecurity)







- 采用adaptive learning 算法，动态根据不同网络使用情况，精准计算预测值。
- 自动检测当前状态与预测值差异，发现异常行为实时告警。
- 周期性学习。



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







“聚焦于内网风险态势感知，致力于核心业务安全”



Hillstone Networks

Based in Beijing, China, Hillstone Networks is a network security vendor, with a regional headquarters in Santa Clara, CA. The vendor introduced its NTA product, named Server Breach Detection System (sBDS), with two appliances in 2017. Hillstone’s NTA product extracts Layer 7 metadata and applies clustering, an unsupervised learning algorithm, to identify deviation from normal activity. sBDS also includes an IPS and an antivirus engine. It also implements some limited deception features (for example, emulating the answer of a web server). Each appliance embeds a management and monitoring interface, and centralized cloud monitoring is also available (Hillstone CloudView). sBDS integrates with Hillstone firewall to add blocking capabilities. Hillstone sBDS does not decrypt SSL/TLS traffic.

Hillstone NTA primarily targets the data center, with many dashboards focused on this use case. The vendor prices its NTA solution using the traditional appliance model, with upfront cost for the hardware, and subscription and support as yearly fees. It also offers NTA as a service, where the cost of the devices is included in the yearly subscription.

Table 1. Representative Vendors in NTA

Vendor	Product, Service or Solution Name
Awake Security	Awake Security Platform
Bricata	Bricata
Cisco	Stealthwatch
Corelight	Corelight Sensor
Corvil	Corvil Security Analytics
Darktrace	Enterprise Immune System
ExtraHop	Reveal(x)
Fidelis Cybersecurity	Fidelis Elevate
FireEye	SmartVision
GREYCORTEX	MENDEL
Hillstone Networks	Server Breach Detection System
HPE Aruba Networks	IntroSpect
IronNet Cybersecurity	IronDefense
Lastline	Lastline Defender
Plixer	Scrutinizer
HighBar SS8	SS8
Vectra	Cognito Detect


Source: Gartner (March 2019)

Gartner 《网络流量分析 (NTA) 市场指南》  
唯一的中国网络安全厂商

为您的安全竭尽全力!

Security that Works!



The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that form a grid or mesh-like structure, creating a sense of depth and movement.

# THANKS

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