高级威胁可感可知

山石网科 资深产品总监 贾彬

ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China

高级威胁的主要特点

攻击成本高

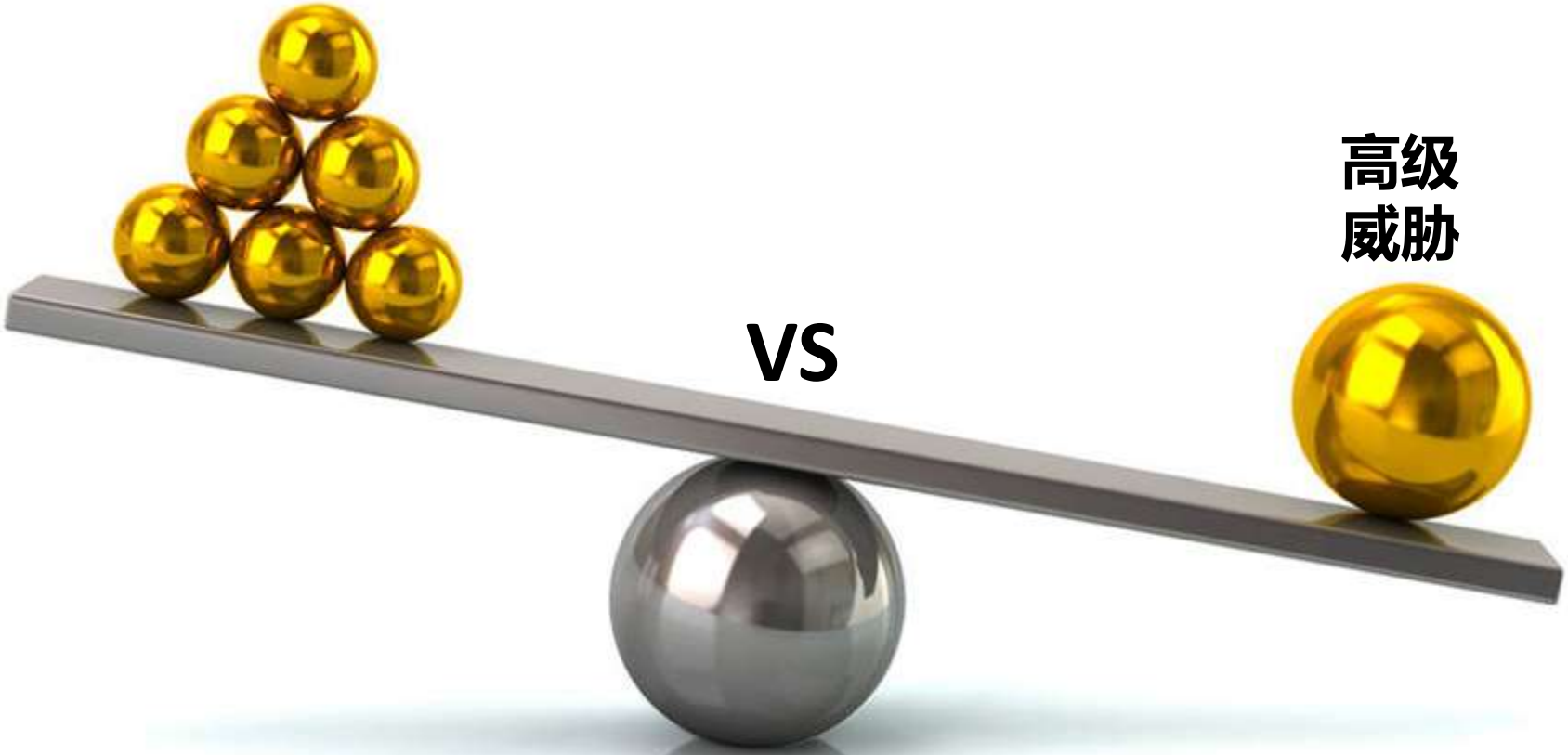
隐蔽性好

周期长

防护难度大

业务针对性强

普通的网络安全运维
独立的安全防护产品



困扰安全运维人员的关键问题

高级威胁是否发生了，我还不知道?

高级威胁发生了，当前的安全建设是否能够有效防护?

网络安全建设存在哪些漏洞?

哪些资产成为高风险点?

核心业务是否遭到破坏?

业务流程是否被恶意篡改?

ZERO TRUST SECURITY

基于AI的网络大数据分析

- 感知核心资产
- 定位业务风险
- 发现高级威胁
- 透视攻击路径

山石网科智·源-让高级威胁可感可知

智能网络大数据分析平台致力于成为客户网络及业务安全的主控中心，通过智·源平台进行网络风险和业务健康度的态势呈现、分析、预测和处置。

全局态势呈现

- 全局网络安全态势呈现
- 全局业务流量态势呈现
- 全局运维管理态势呈现
- …

风险及业务分析

- 业务核心资产感知
- 业务流量互访关系透视
- 业务风险异常判断及定位
- …

智·源平台

响应处置

- 安全处置决策建议
- 网络威胁溯源跟踪
- 威胁处置联动策略
- …

情报共享

- 同行业业务参考基线
- 网络威胁情报共享
- 威胁热点推送关联
- …

高级威胁可感—全局安全风险态势

全局安全风险态势，基于网络攻击路径的多个阶段，还原高级威胁

高级威胁可感—全局业务风险态势

全局业务风险态势，基于网络流量分析，发现潜在业务风险，及风险潜在发生区域

高级威胁可知

透视业务风险 01

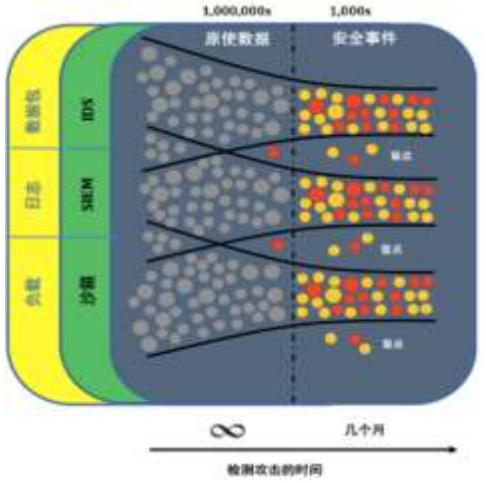
- 业务异常及威胁判定
- 业务风险原因
- 潜在业务风险区域

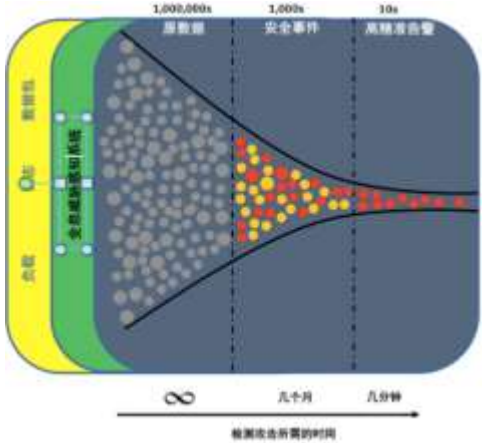
02 智能业务风险减缓

- 威胁情报辅助业务威胁检测
- 行业参考基线辅助业务安全决策
- 联动安全设备，业务威胁应急处置

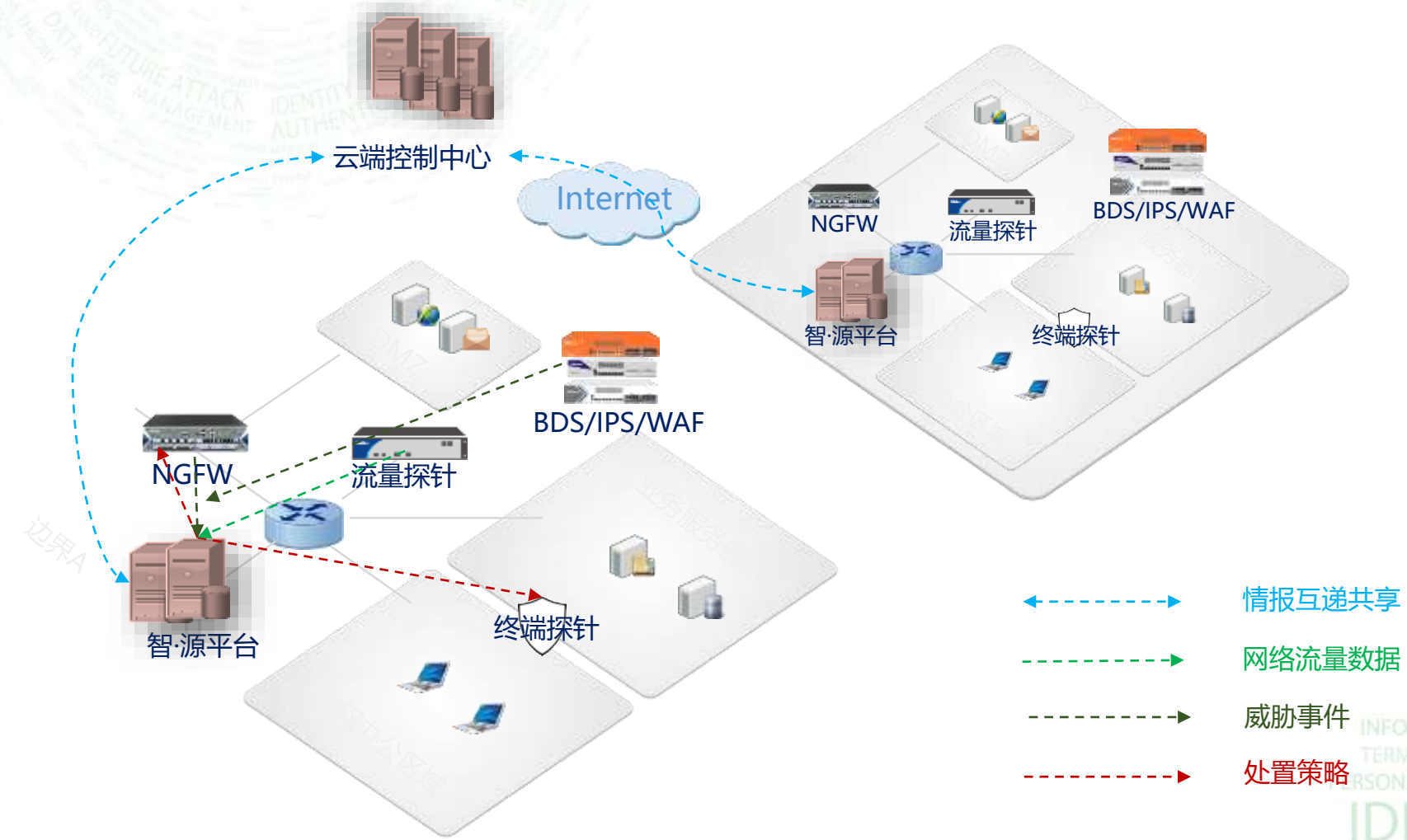
核心技术

- 全息数据收集
  - 网络流量
  - 服务器数据
  - 应用数据,用户数据,日志
- 分布式安全智能
  - 大数据分析
  - 分布式检测
- 多层 - 机器学习
  - 监督机器学习
  - 无监督机器学习
  - 基于多种数据类型的机器学习
  - 多层机器学习检测
  - 多租户机器学习





山石网科全局网络安全解决方案



ZERO TRUST SECURITY

山石网科

为您的安全竭尽全力

Security that Wroks!

ZERO TRUST SECURITY

ISC 2018
ISC互联网安全大会

360互联网安全中心

谢 谢！

ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China