深信服 互联网出口终端上网安全防护解决方案

现状分析

终端是战略攻击点	90%的企业人员会使用办公PC上网 80%的企业安全事件来源于终端
安全总是后知后觉	被攻击时毫不知情，爆发时为时已晚
防御正在逐渐失效	传统防御面对高级威胁时显得捉襟见肘

为什么终端上网安全问题难以解决？

看不清安全现状 感知不到威胁	新型高级威胁使 防御失效	终端安全措施难 以落地执行
● 看不清上网的应用和内容 ● 不知道PC是否被感染 ● 看不清威胁的影响面	● 高级威胁隐蔽性强、持续时间长，能轻松绕过防御。 如： APT攻击、社工攻击 0Day攻击等	● 领导对安全不够重视，没有给予足够支持 ● 员工安全意识不强，对措施有抵触心理

终端上网安全的理想建设模型

1、 组织安全建设应该贯穿安全事件的事前、事中和事后；

2、 应该以可视为基础，基于更多元素的可视，最终看得见异常、看得清威胁和安全现状；

3、 边界防御把控传统威胁入口，同时持续检 测漏网之鱼，及时发现高级威胁；

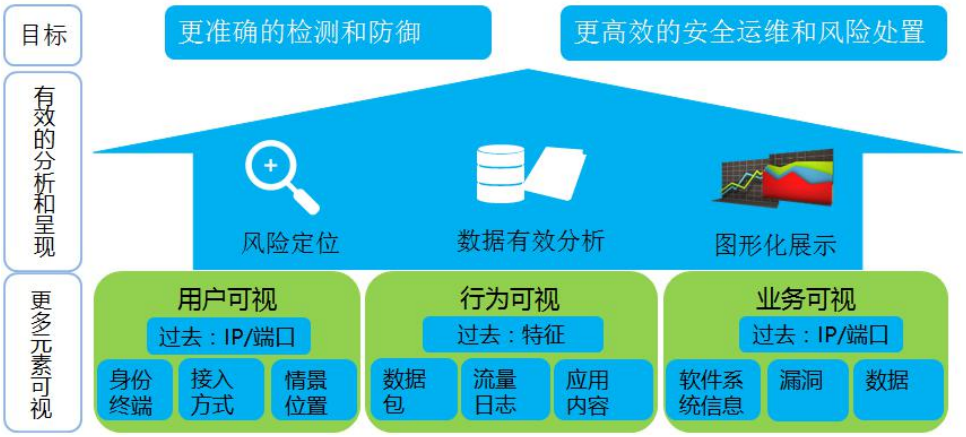
4、 一旦发生安全事件能够快速定位，及时

处置，将威胁的影响面降到更低；

5、 基于可视、检测的结果形成各类自动化安全报表，推送组织各部门，让领导重视安全、让员工理解安全，最终推送终端安全措施的落地执行。

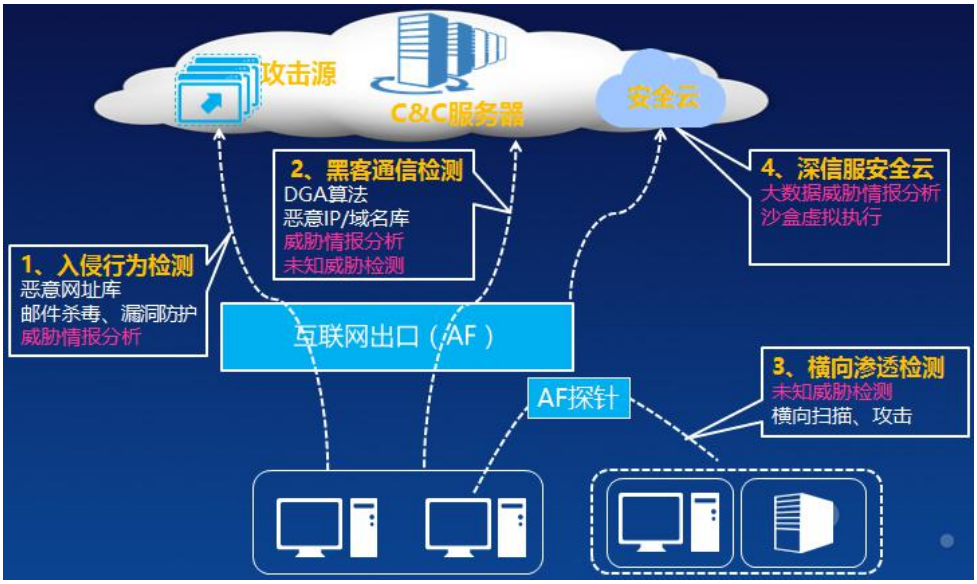
深信服终端上网安全解决方案

➢ 安全以可视为基础



- **更多元素的可视：**在用户、行为、业务等维度实现更多元素的可视
- **有效分析和呈现：**基于可视化数据，进行综合分析，实现风险定位，并图形化展示威胁
- **可视的最终目标：**最终为实现更准确的检测和防御，以及更高效的运维和风险处置提供支撑

➢ 基于全攻击链的持续检测



基于黑客攻击链的所有环节的持续检测技术：

1、 入侵行为检测（黑客入侵阶段）

- 通过恶意网址库、邮件杀毒、漏洞防护等防御手段防护各种传统威胁的入口；
- 威胁情报分析对高级威胁进行持续检测；

2、 黑客通信检测（突破防御之后，失陷主机与 C&C 服务器通信阶段）

- 通过 DGA 算法、恶意 IP/域名库等阻断木马与 C&C 服务器的通信；
- 威胁情报分析技术利用全球最新的威胁情报帮助快速定位最新 C&C 服务器地址；
- 通过未知威胁检测技术对病毒与 C&C 服务器通信过程中的异常流量和异常行为进行持续检测；

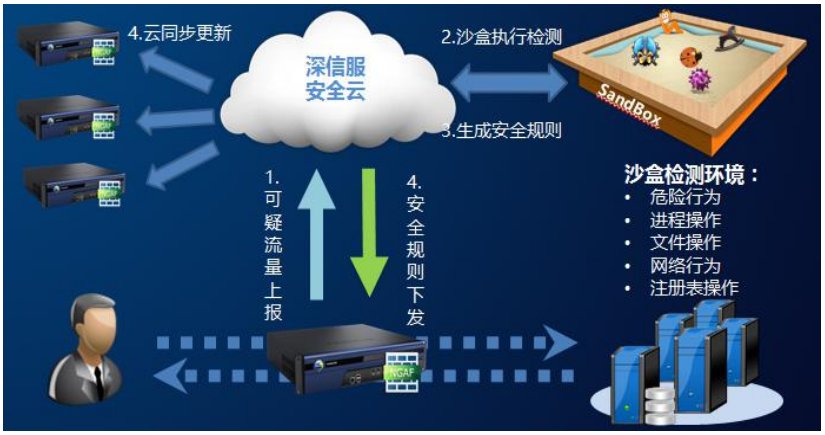
3、 横向渗透检测（病毒的横向渗透阶段）

- 通过 AF 探针结合安全云的未知威胁检测技术，对病毒的横向扫描和攻击行为就行沙盒检测；

4、 深信服安全云（贯穿在整个攻击链的每个过程）

- 客户网络中的 AF 与深信服安全云联动，通过沙盒技术的虚拟执行，进行未知威胁检测；
- 客户网络中的 AF 与深信服安全云联动，通过威胁情报分析平台，帮助客户获得威胁情报；

未知威胁持续检测（沙盒技术）

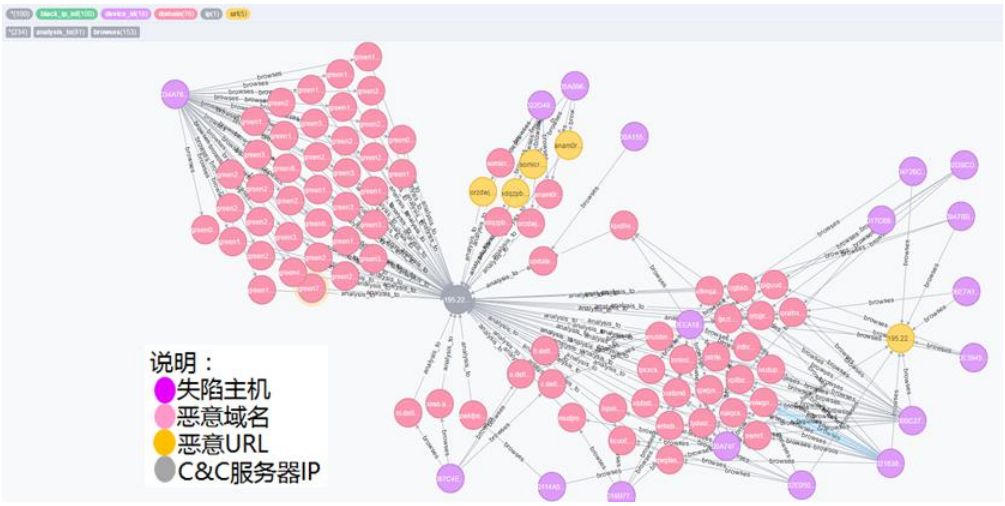


大数据威胁情报分析平台

深信服大数据威胁情报分析平台情报来源（仅 Virustotal 每天有 20G 情报）：

- 国内外数十个知名的安全机构，如：CNVD、CNNVD、Virustotal、Threatcloud 、Malware 、Abuse 等；
- 深信服在线的近万台安全设备上报的安全威胁情报；
- 深信服安全云检测平台、安全服务团队监测获得的海量威胁情报；

下图是深信服大数据威胁情报分析平台近期分析到的一个僵尸网络的部分内容：



传统静态特征方案的不足：

1、 发现威胁少或不全

2、 看到的只是单个威胁信息，无法发现威胁背后的整个僵尸网络的危害。

➢ 及时响应安全事件，将威胁影响面降到更低

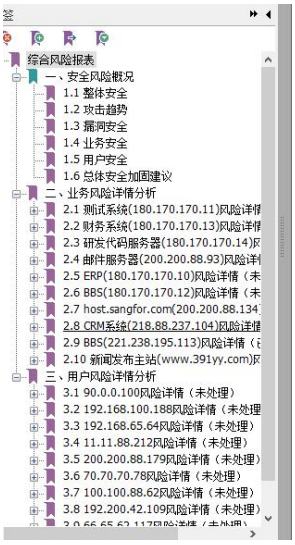
1、 AF 将可以日志汇总发送到深信服安全云

2、 安全云通过自动化威胁分析平台，结合全球最新威胁情报分析日志

3、 安全云将有效的威胁情报通过微信推送给管理员

4、管理员结合威胁内容对安全事件进行处理

➢ 自动化报表驱动安全措施的落地执行



（内部测试数据）

- 通过业务风险报表、用户风险报表等自动化安全报表，对组织的终端安全现状和业务风险现状进行分析汇总，并给出整改意见，帮助组织各部门及时发现安全问题。
- 定期的安全运营报告，帮助组织的安全部门更好的展现其业务价值。

方案优势

- 方案形成一个完整的安全闭环：防御、检测、响应
- 深信服安全云组件：未知威胁检测（云沙盒技术）、大数据威胁情报分析平台等

成功案例

交通运输部 中国移动四川分公司 中国联通湖北分公司 终端电信云南分公司

外交部 海康威视 浙江大学 上海政法大学 东风汽车 招商银行 中铁六局集团