

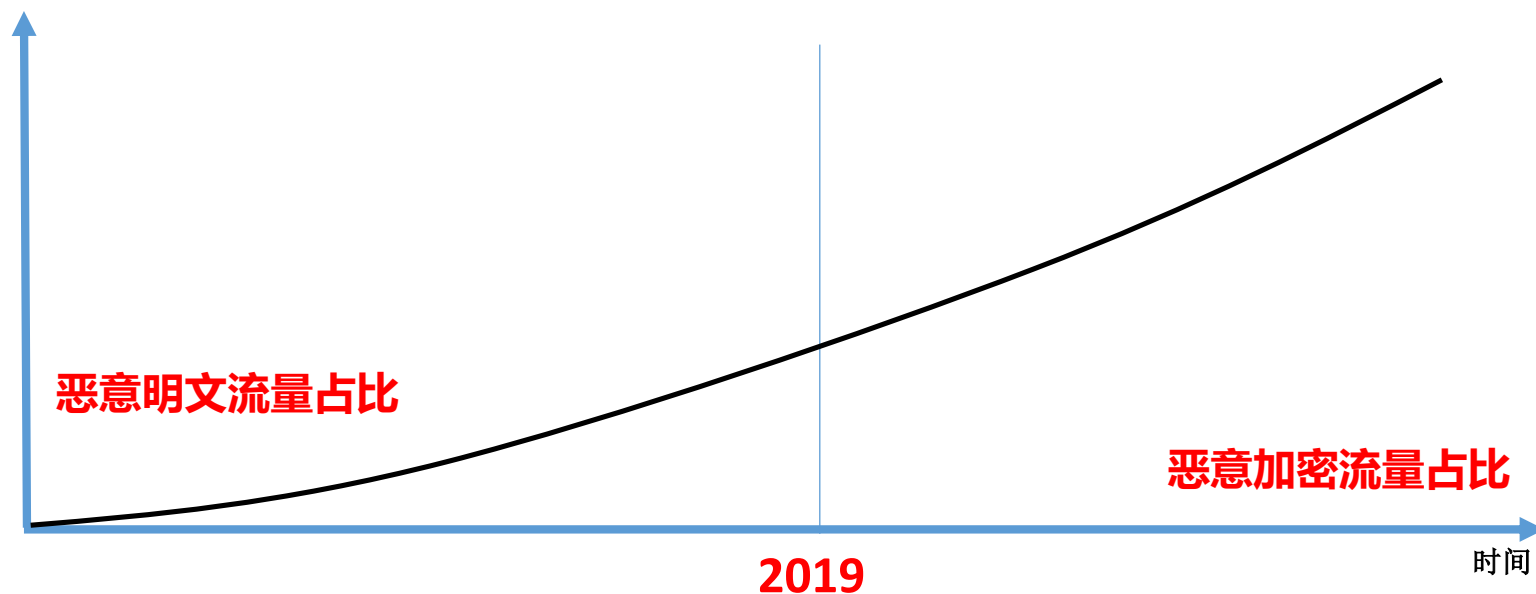


加密流量安全检测的 探索与实践

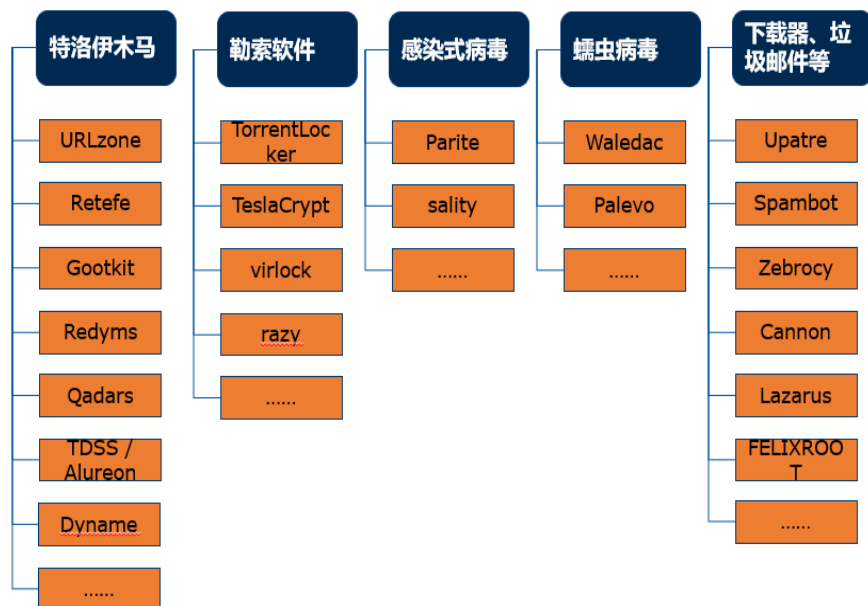
于海东

观成科技联合创始人

Gartner：2019 年，**超过 80%** 的企业网络流量将被加密；加密的流量中将隐藏**超过 50%** 的网络恶意软件。

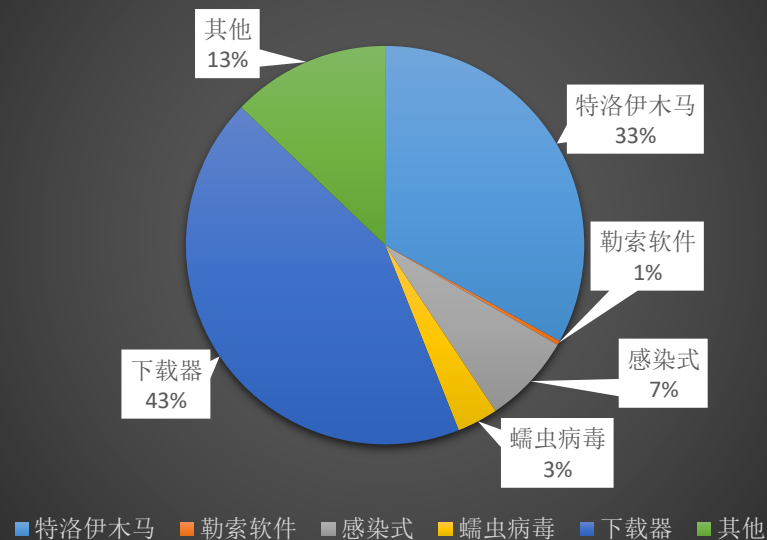


- 共监测到加密通信样本家族数量 **>200种**
- 加密通信样本所占比例 **>40%**
- 每日新增加密通信恶意样本数量 **>1000个**

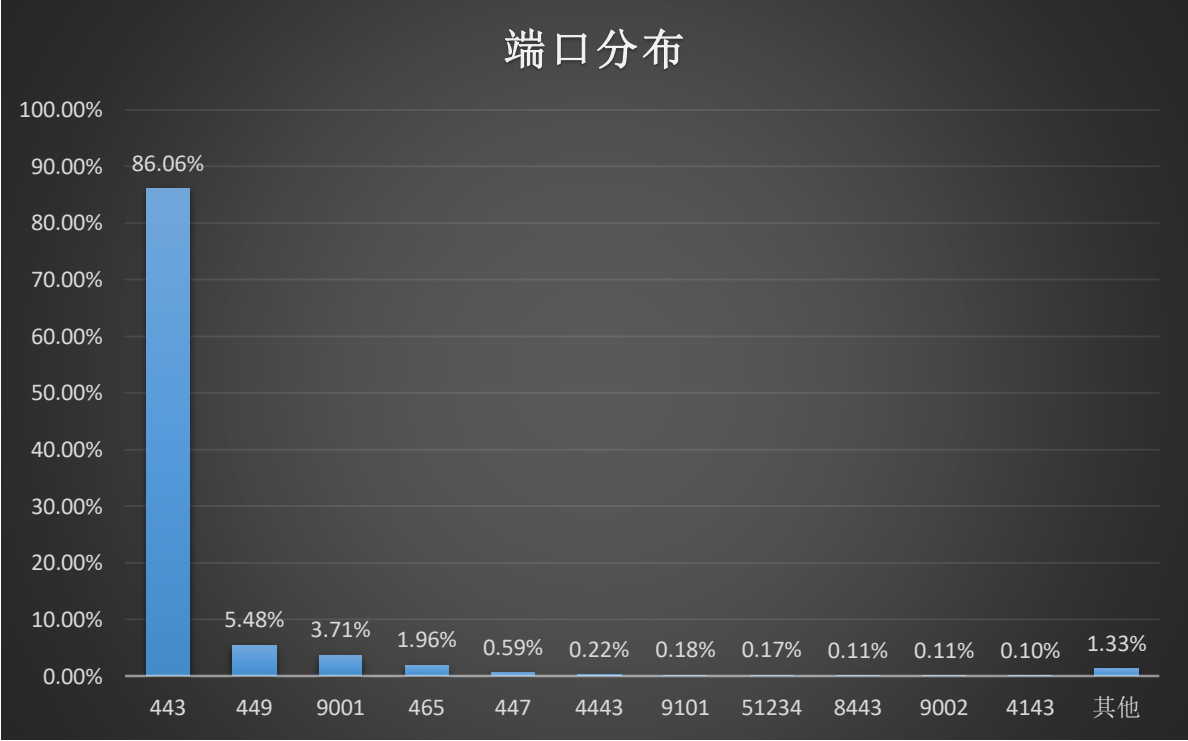


- 几乎涵盖所有类型
- 端口不固定
- 加密协议分布广泛

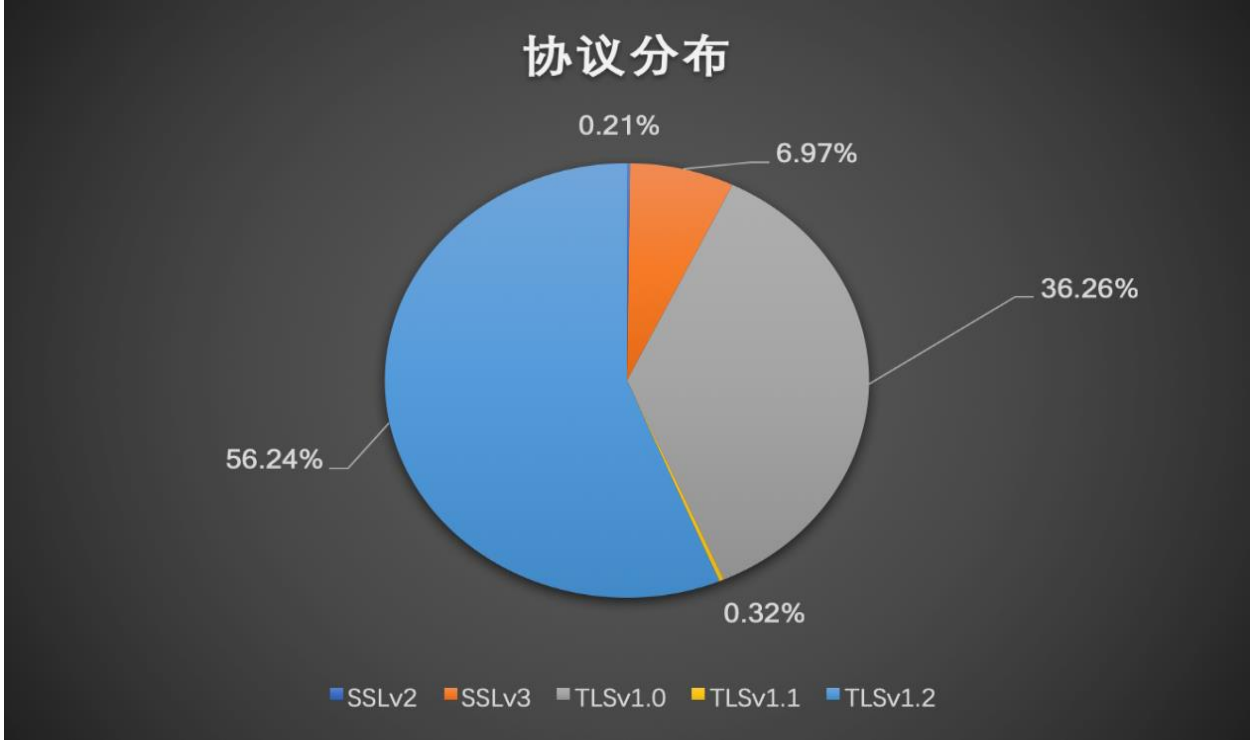
加密通信恶意软件分类



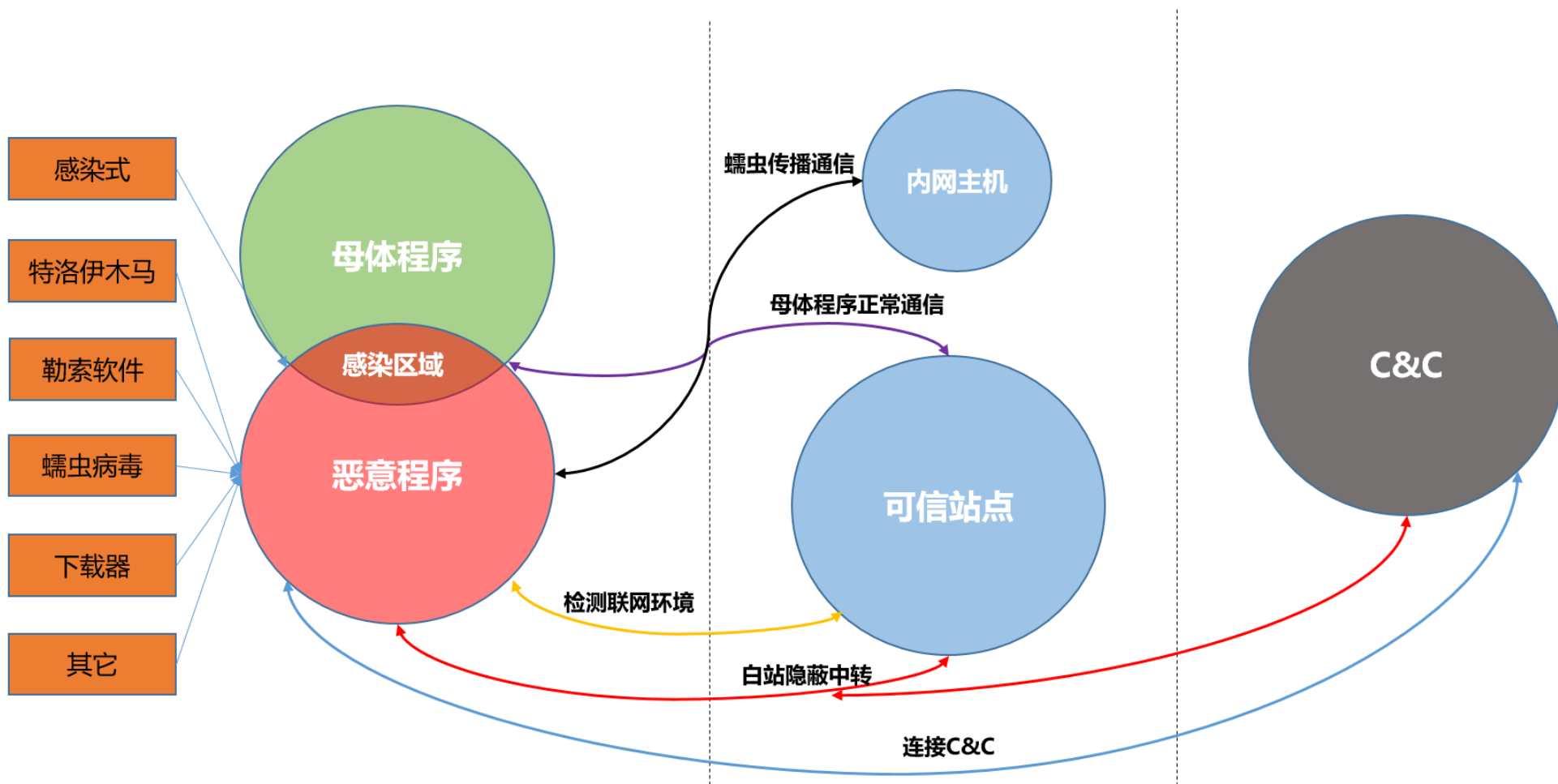
端口分布



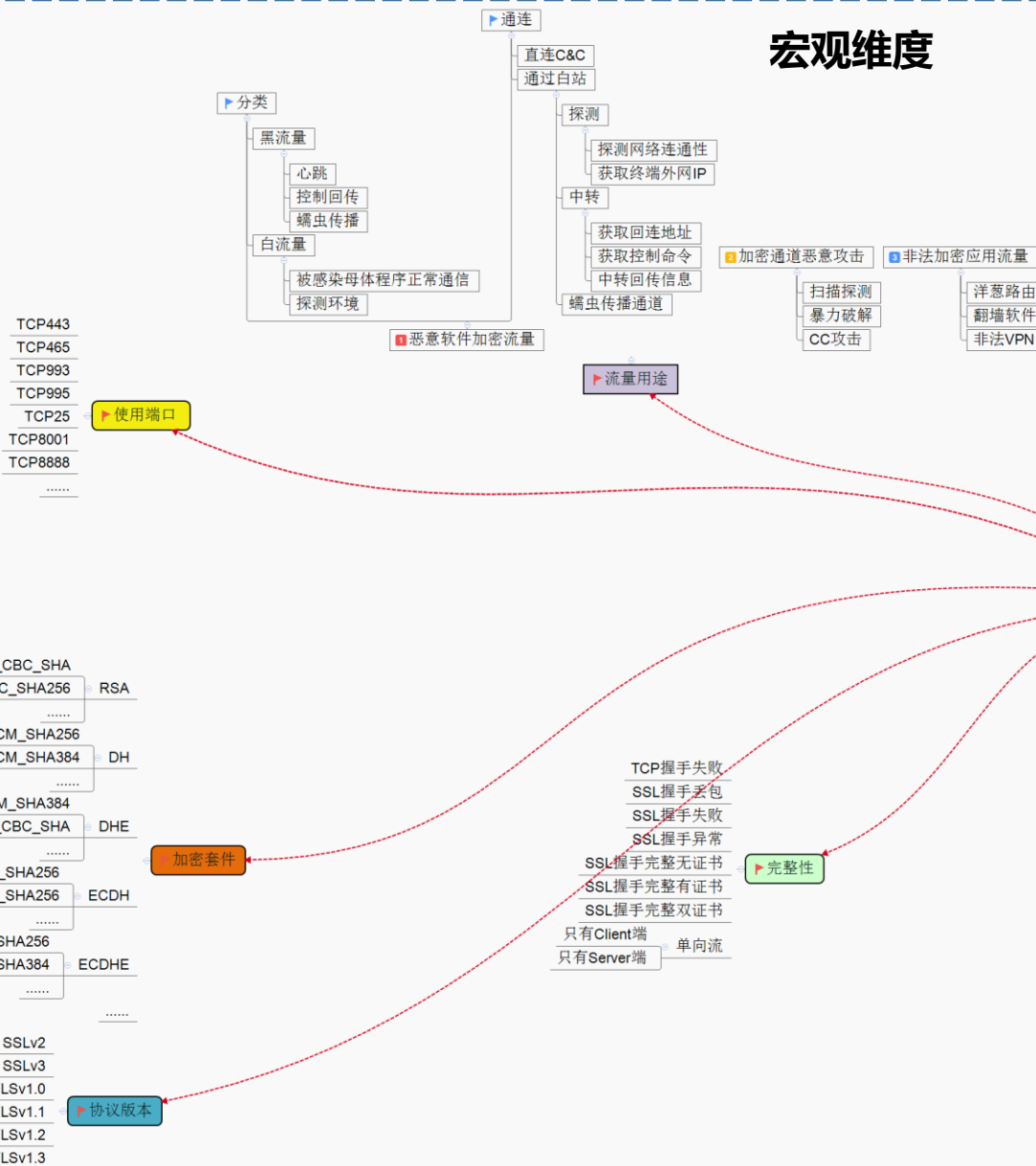
协议分布



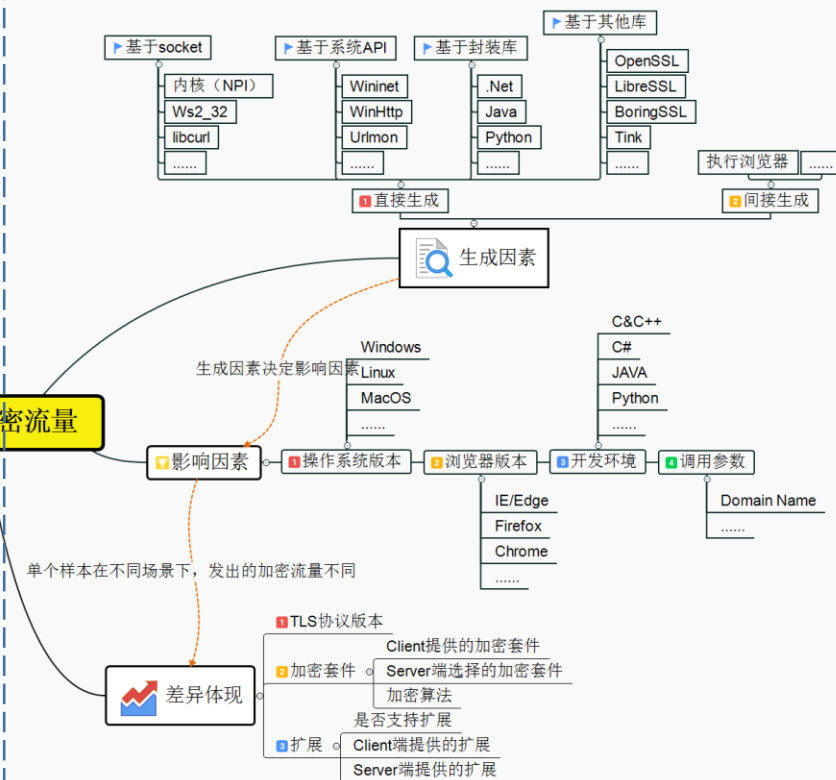
• 常见恶意软件使用加密通信方式汇总

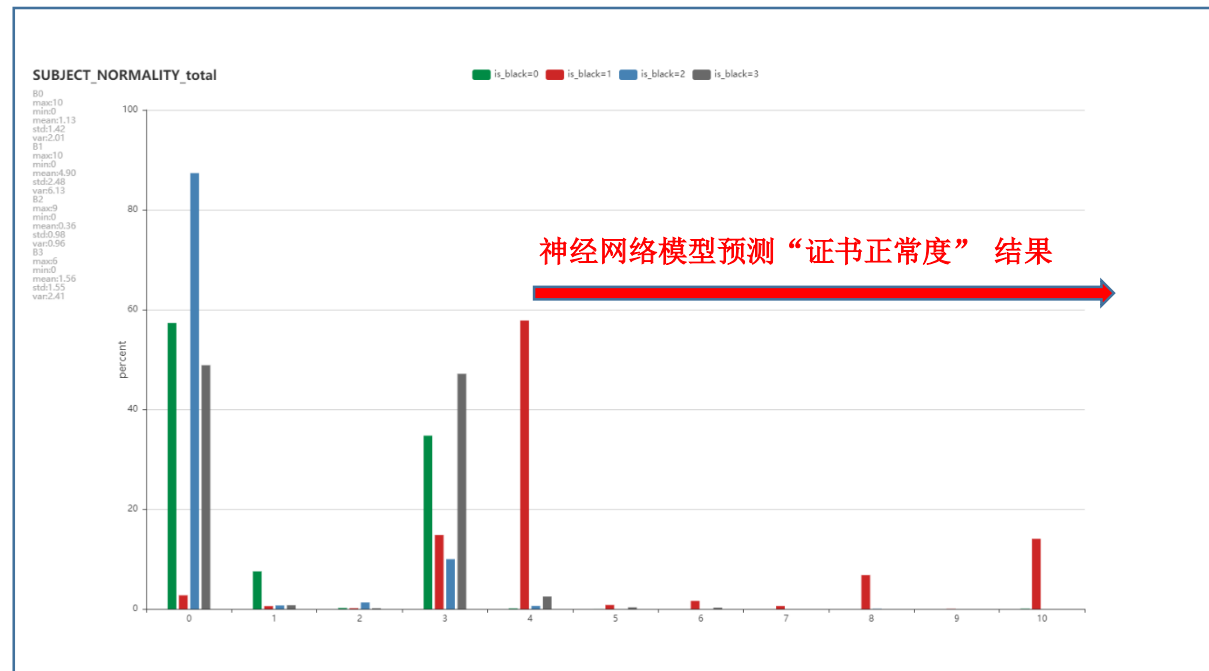
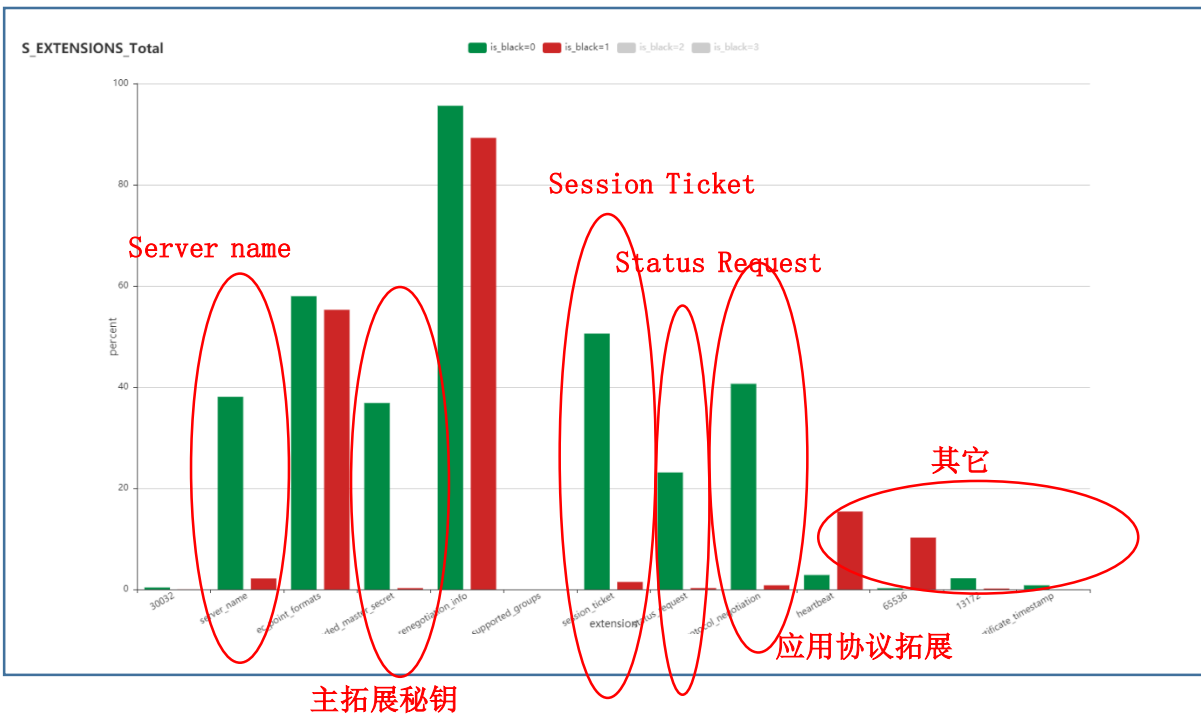


宏观维度

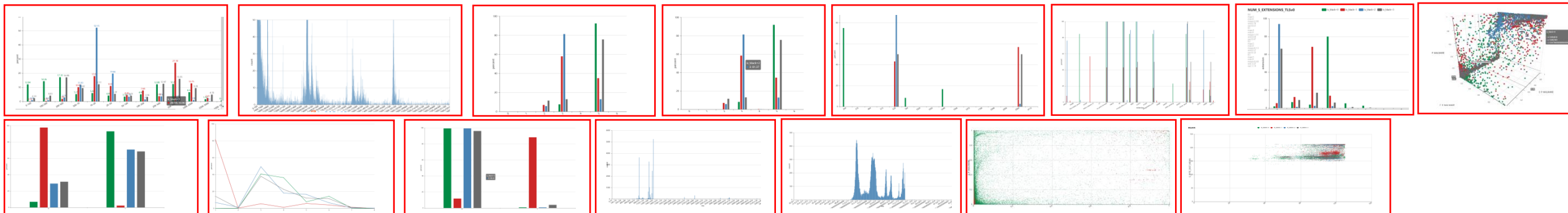


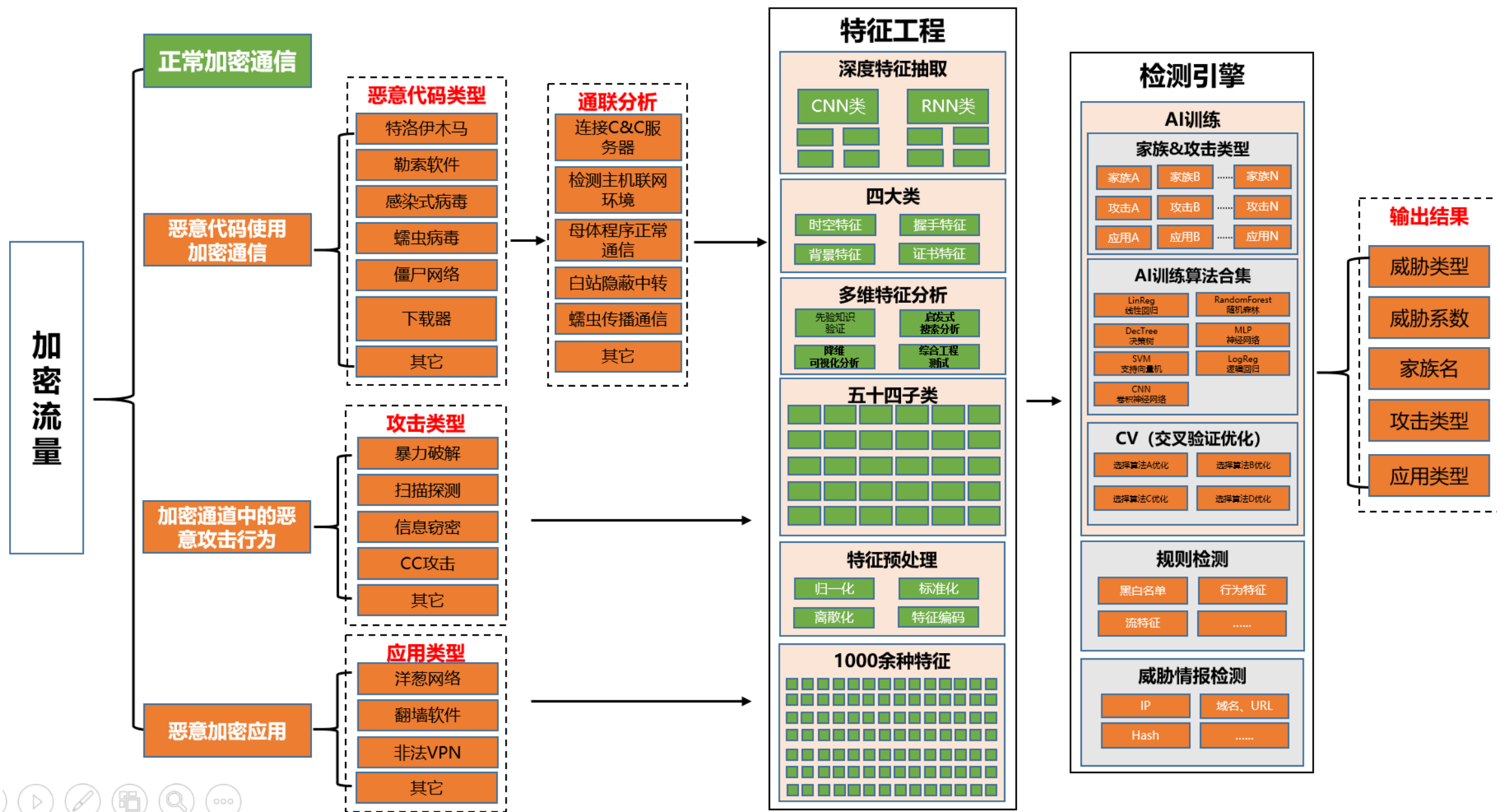
微观维度





1000余种特征，生成370类可视化特征对比图

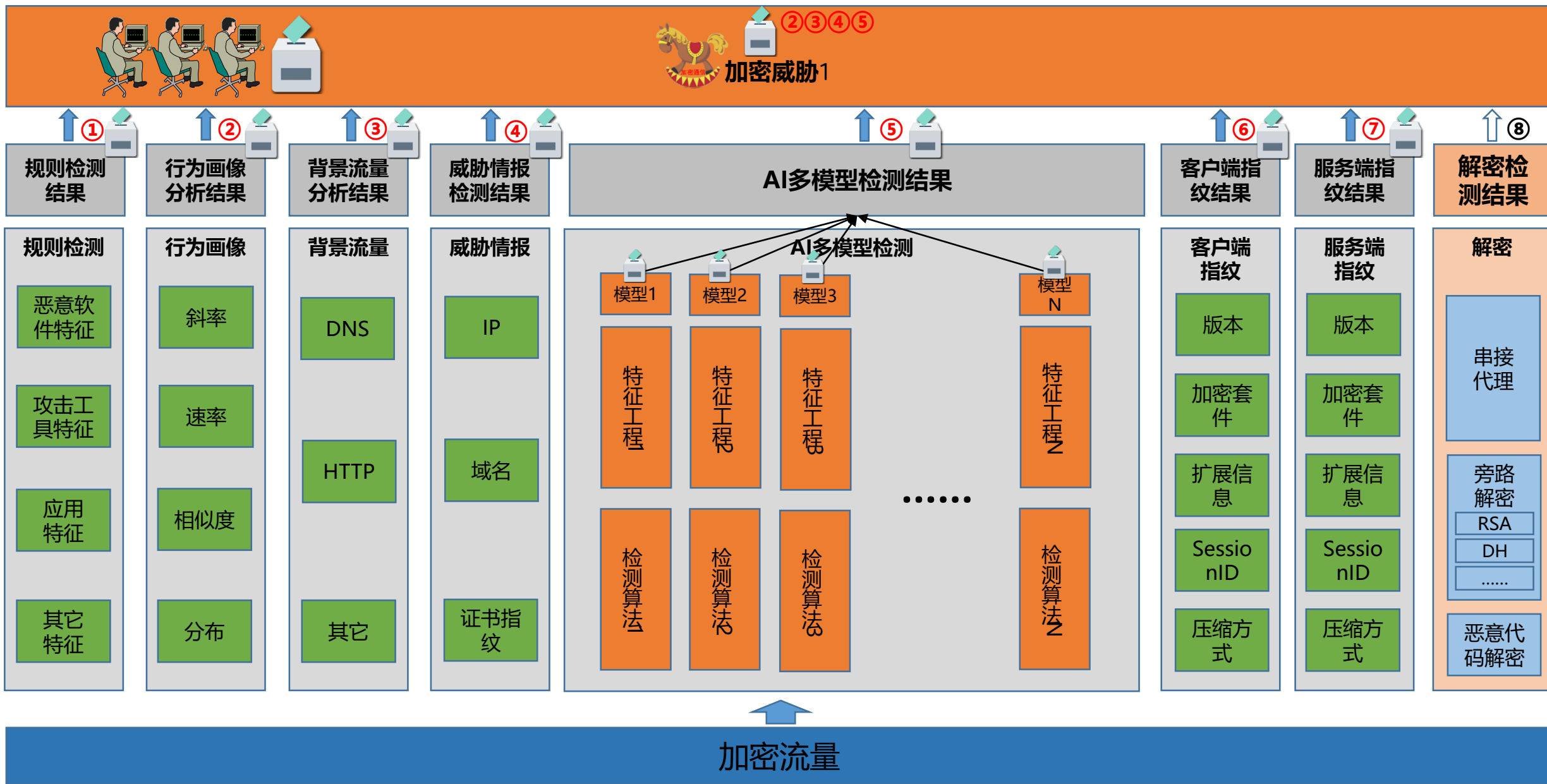


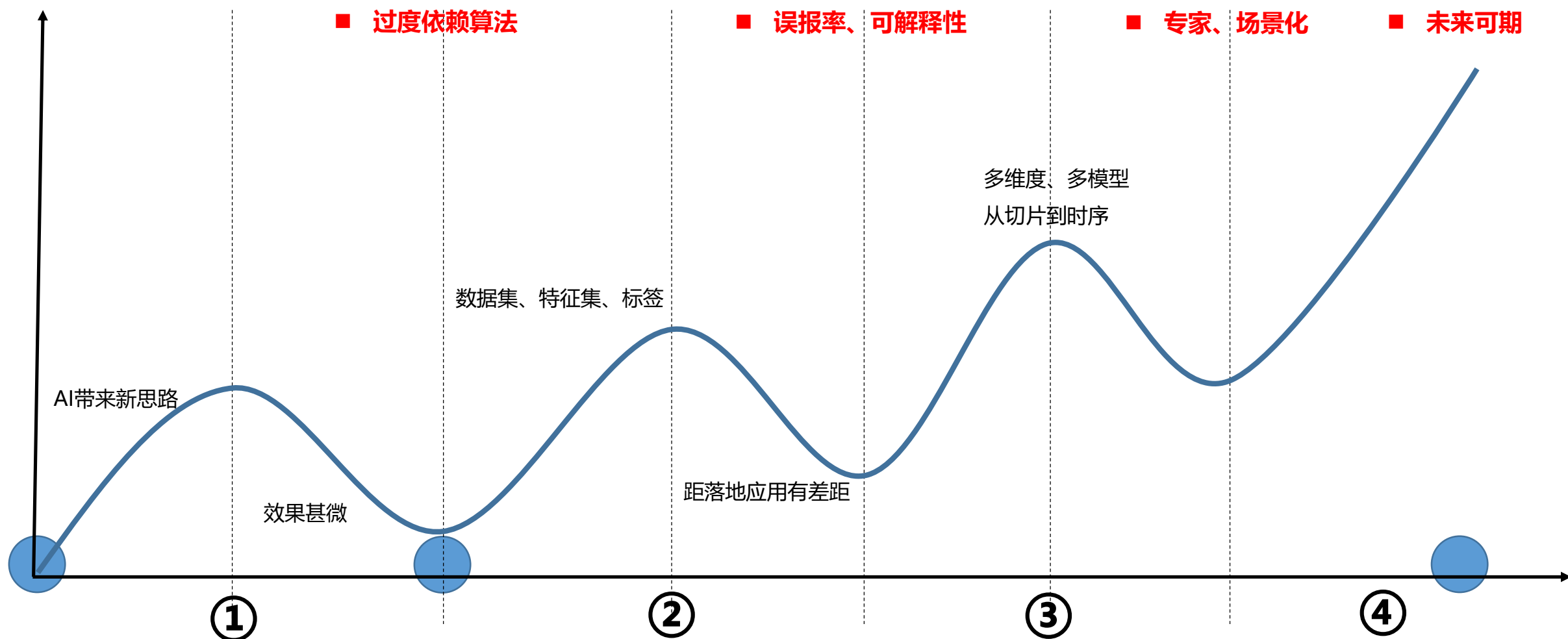


加密威胁检测综合决策体系

2019 北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE





1

加密威胁递增的趋势不可阻挡

2

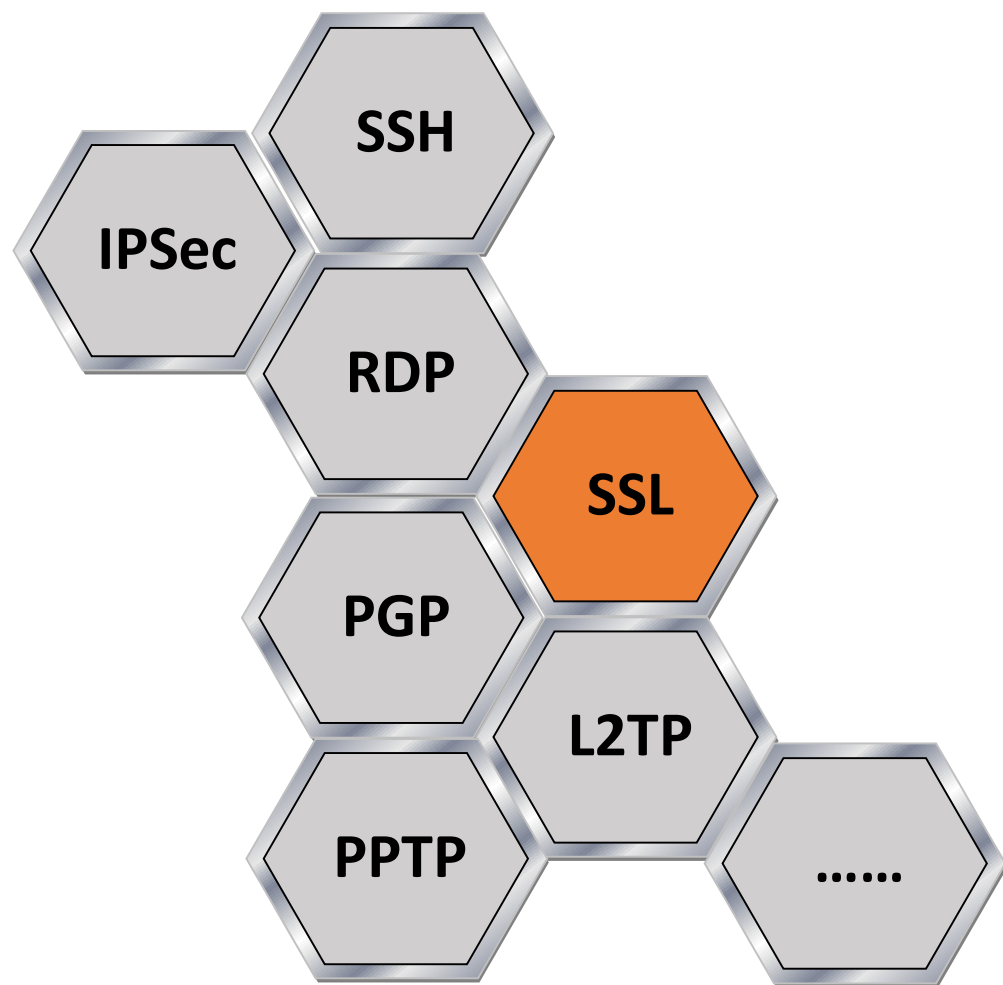
加密威胁检测具备落地应用的条件

3


短期定位：人机结合的检测分析机制

4

加密威胁检测需要体系化的解决方案



加密威胁检测是一条艰难又漫长的道路，而我们会一直坚定地走下去！

The background is a solid blue color with a subtle, abstract pattern of thin, light blue lines that create a sense of depth and movement, resembling a stylized grid or wave pattern.

THANKS

2019北京网络安全大会

2019 BEIJING CYBER SECURITY CONFERENCE