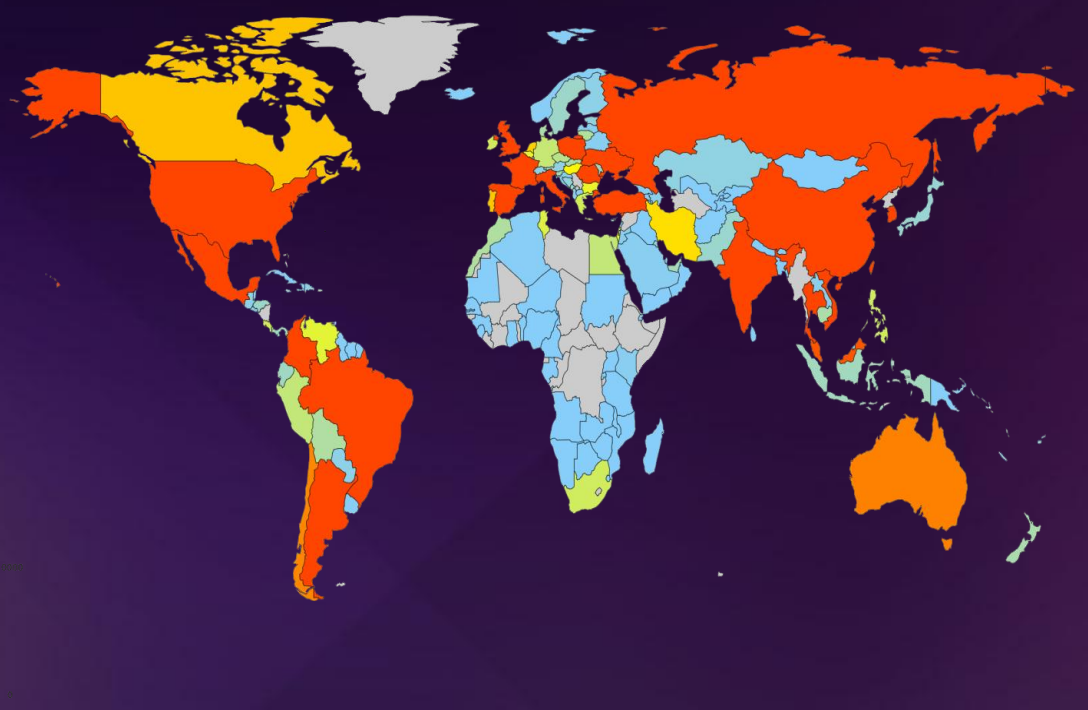
浅谈工控网络终端安全实践

北京瑞星网安技术股份有限公司

全球情况



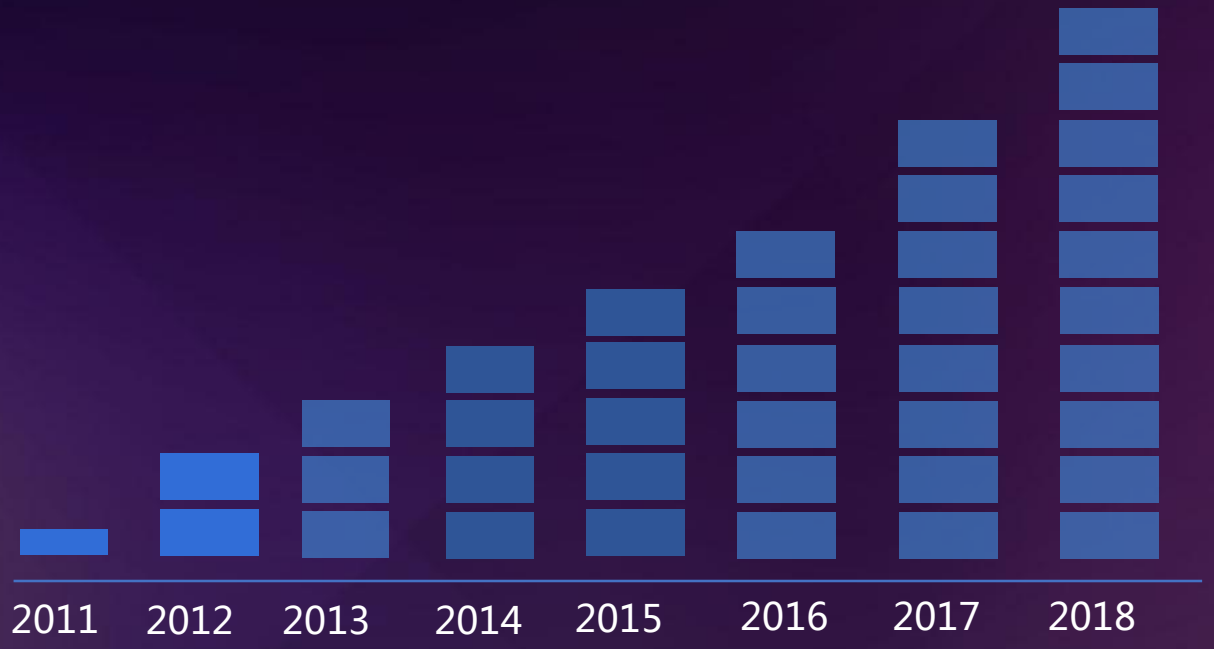
01 2005年，Zotob蠕虫事件导致全美13个汽车制造厂被迫关闭，造成巨大经济损失超过$1,400,000。

02 2011年，我国某石化企业某装置控制系统感Conficker病毒，造成控制系统服务器与控制器通讯中断。

03 2014年，Havex病毒病毒席卷欧美，劫持电力工控设备，阻断电力供应，中国发现少量样本传播。

04 2018年，台积电突遭电脑病毒感染，3个厂区停产2-3天，带来重大损失，预计三季度营收约下降1.69-1.71亿美元。

我国情况



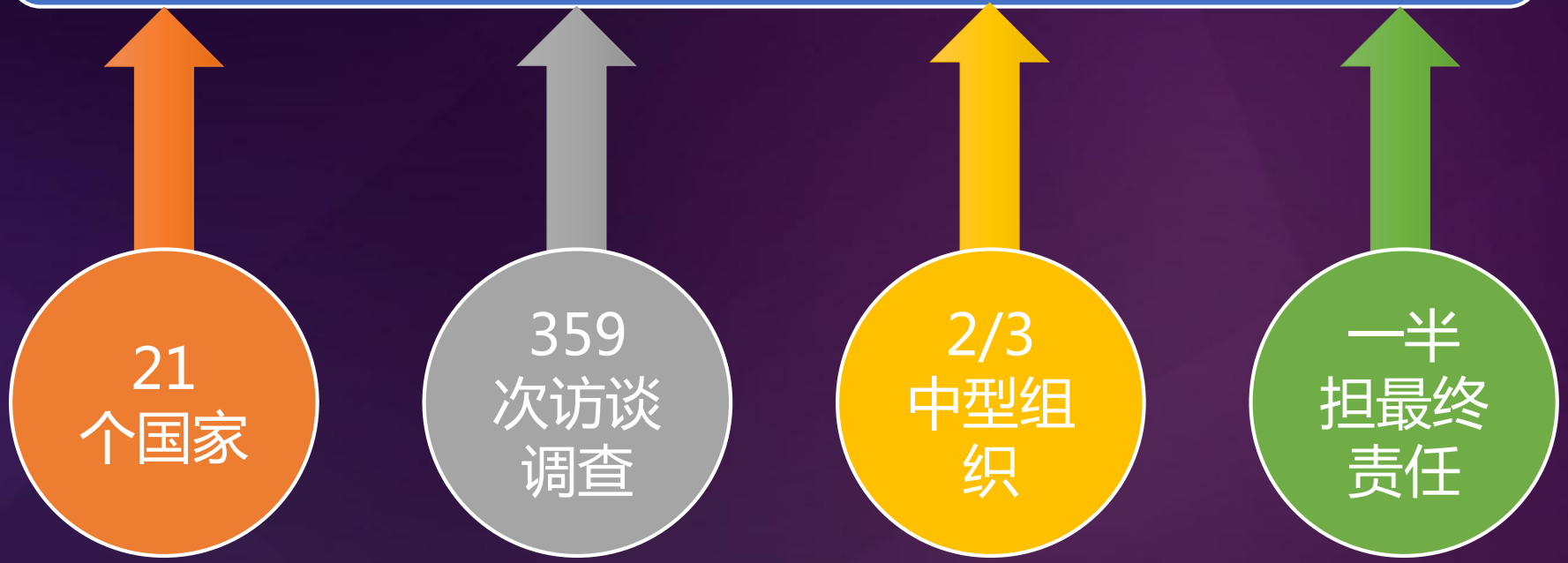
中国是全球网络攻击最大受害国

自2011年以来网络攻击增长**15**倍

其中**30%**针对国家基础设施

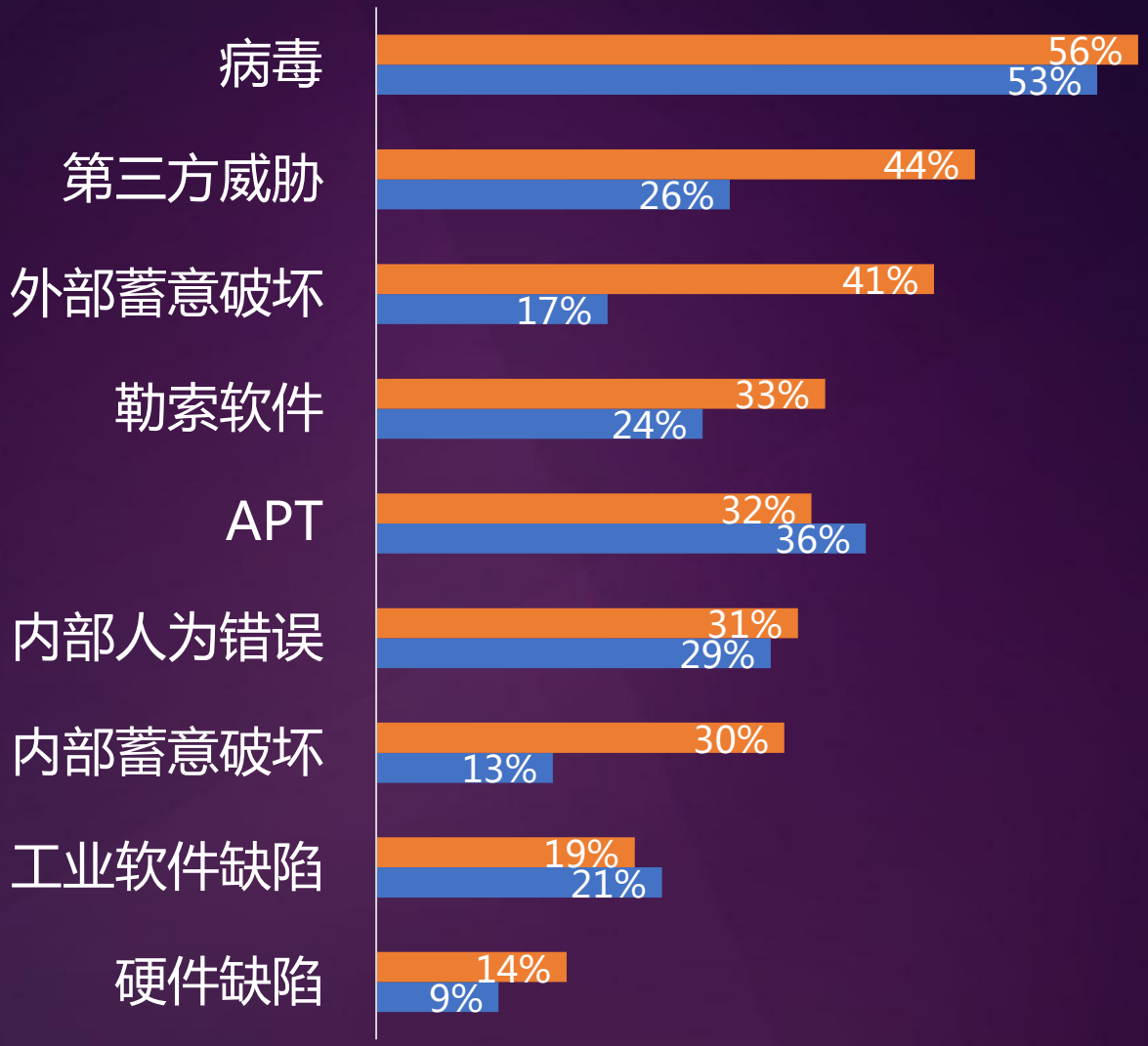
关键基础设施

《2018年全球工业控制系统网络安全状况》

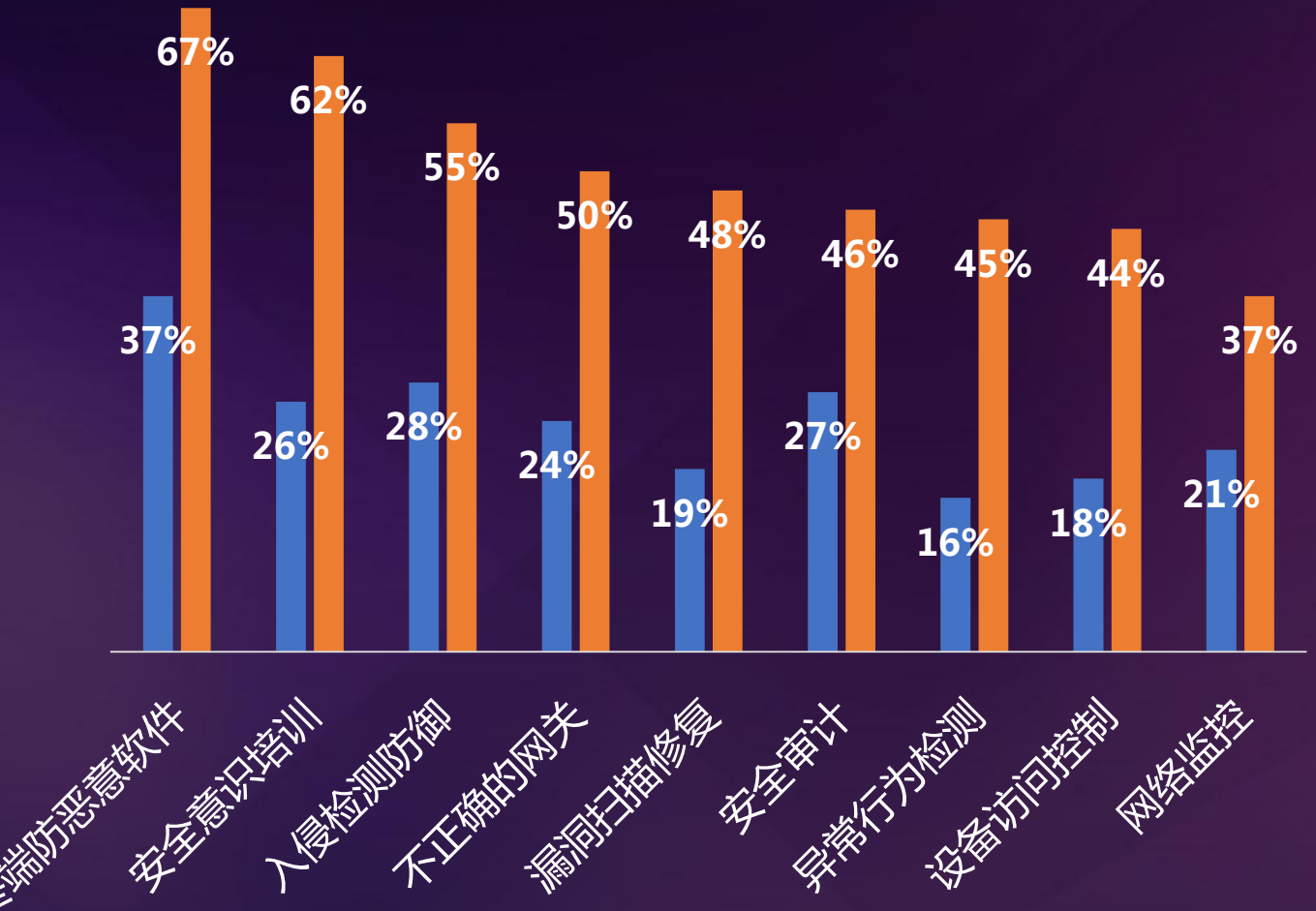


“认知的”和“实际的”工控网络安全威胁

威胁类型	认知排名及占比		实际排名及占比	
恶意软件	1	56%	**1**	**53%**
第三方威胁	2	44%	4	26%
外部蓄意破坏	3	41%	7	17%
勒索软件	4	33%	5	24%
APT	5	32%	**2**	**36%**
内部人为错误	6	31%	**3**	**29%**
内部蓄意破坏	7	30%	8	13%
工业软件缺陷	8	19%	6	21%
硬件缺陷	9	14%	9	9%



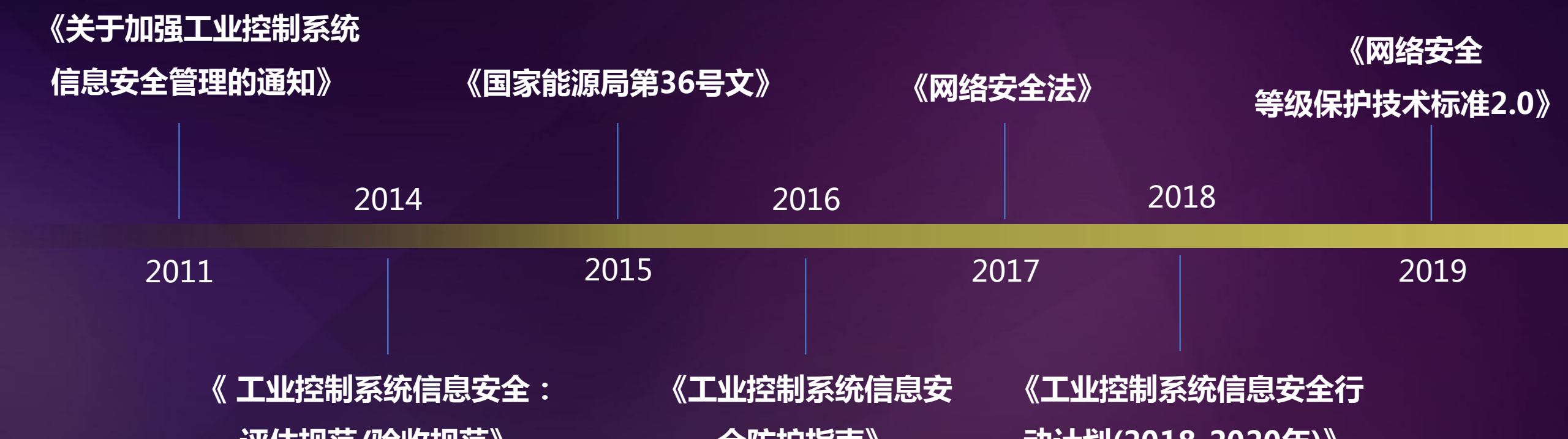
“认知的”和“实际的”工控安全措施效果



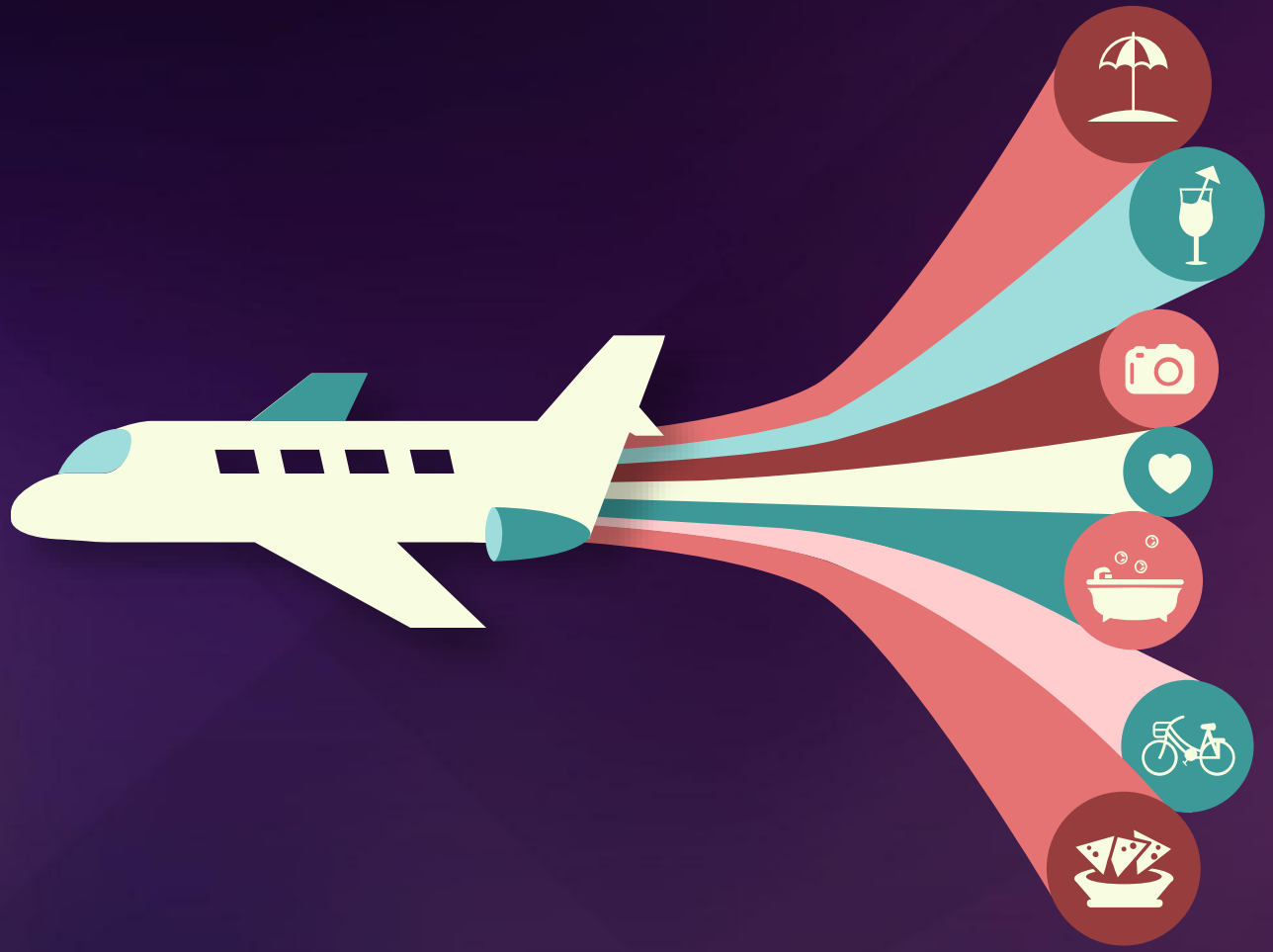
安全措施	认知排名及占比		实际排名及占比	
终端防恶意软件	1	37%	1	67%
入侵检测防御	2	28%	3	55%
安全审计	3	27%	6	46%
安全意识培训	4	26%	2	62%
不正确的网关	5	24%	4	50%
网络监控	6	21%	9	37%
漏洞扫描修复	7	19%	5	48%
设备访问控制	8	18%	8	44%
异常行为检测	9	16%	7	45%

最有效的安全措施

政策大事件


《关于加强工业控制系统信息安全管理的通知》
2011
《 工业控制系统信息安全：评估规范/验收规范》
2014
《国家能源局第36号文》
2015
《工业控制系统信息安全防护指南》
2016
《网络安全法》
2017
《工业控制系统信息安全行动计划(2018-2020年)》
2018
《网络安全等级保护技术标准2.0》
2019

安全要求



- 安全物理环境
- 安全通信网络
- 安全区域边界
- 安全计算环境
- 安全建设管理

非物理环境安全要点


边界防护
访问控制
入侵防范
恶意代码防范
身份鉴别
集中管理
关键信息隐藏
分区过滤
可行验证
数据保护
可信验证
安全审计

功能

防病毒
（恶意代码防范）

漏洞补丁
（入侵防范）

防火墙
（边界防护、入侵防范）

行为审计
（访问控制、安全审计）

资产管理
（身份鉴别、安全审计）

安全管理

三权分立

三权分立权限
身份鉴别、安全访问控制

功能模块化

按需选用
远程动态装卸

集中管理

级联、分组
策略、命令

网络支持

单向要求、IPv4/IPv6
过NAT,多IP、动态IP

100%国产自主引擎

全面

识别能力：各平台、类型
技术体系：传统+人工智能
平台支持：主流、通用、国产

高效

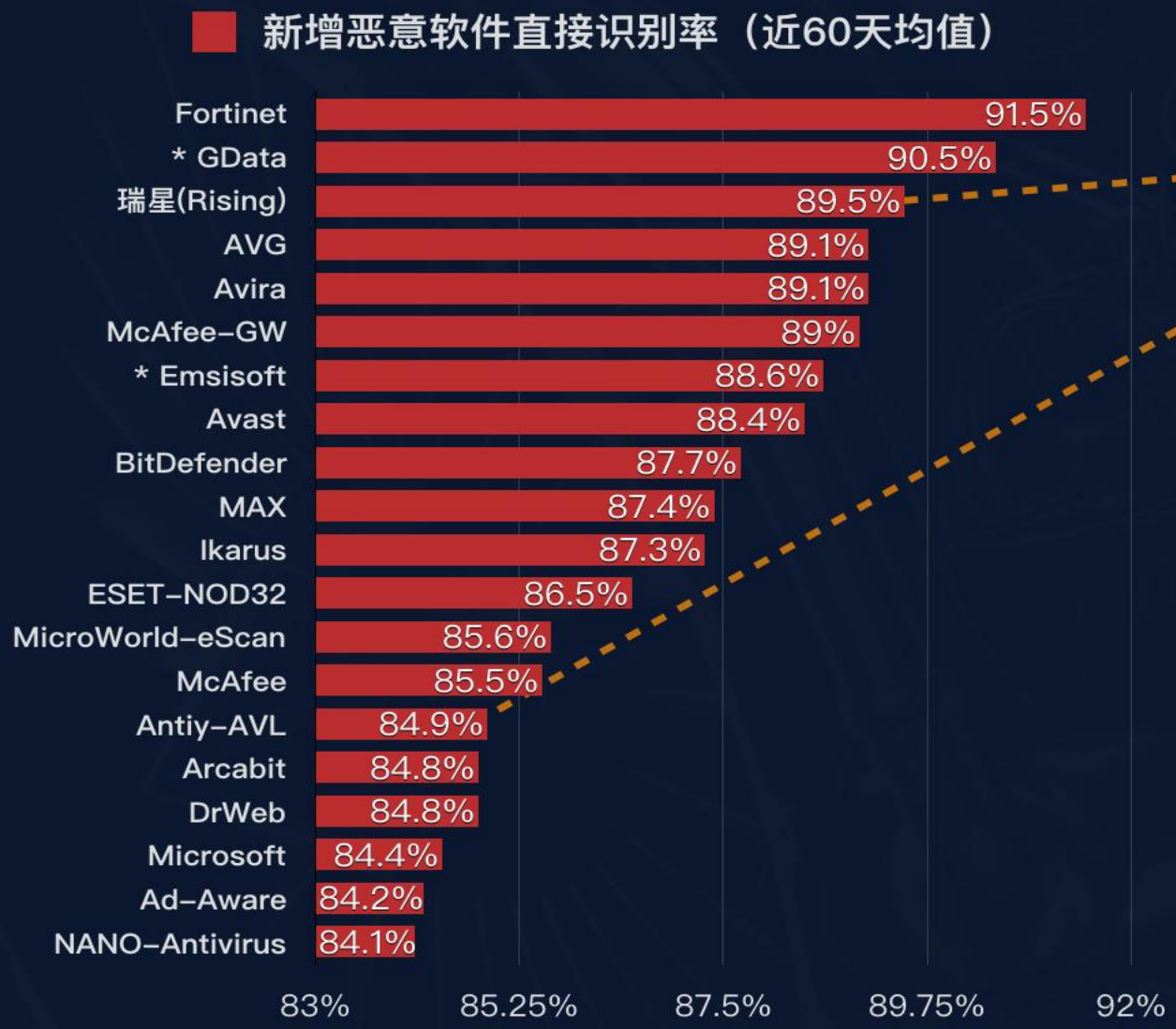
自动、无休快速更新
已知拦截、未知识别

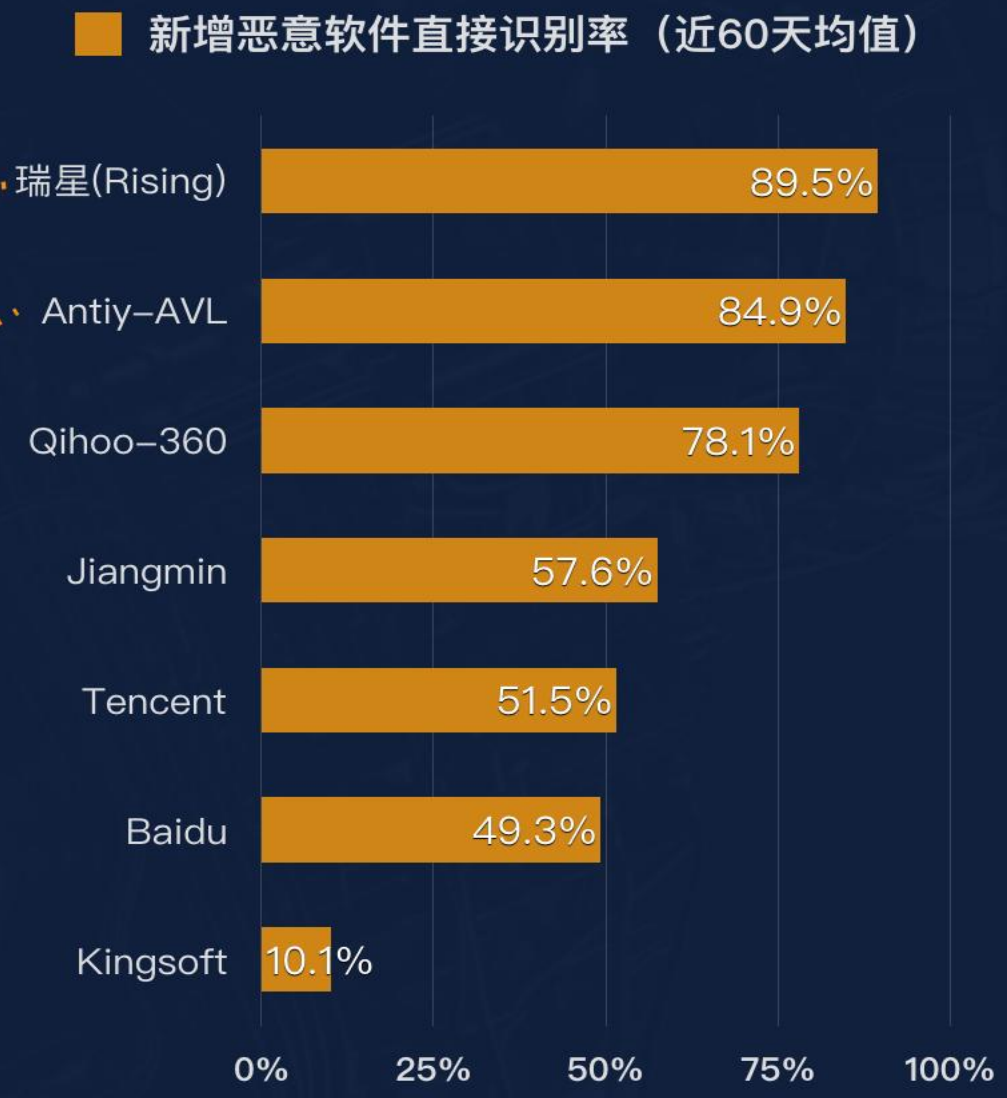
先进

技术方向：人工智能、云化监测、文件/网络流混合
运营模式：无人化运营

强悍

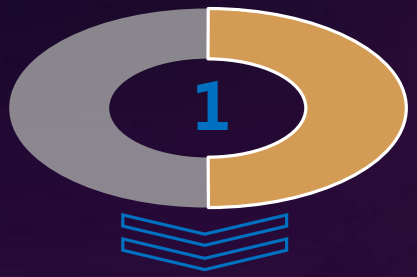
识别能力：
全球领先、国内最强





* 图表数据由瑞星根据VirusTotal.com的扫描结果自行统计

子产品功能



常规防护

公有云/私有云查杀、病毒专杀

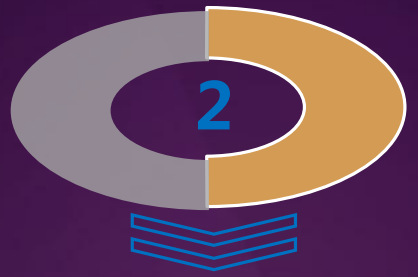
定期定时全盘扫描

自定义查杀、U盘接入扫描

文件监控、主动防御

白名单管理、隔离中心

仅升级病毒库



特色技术

变频查杀技术、病毒跟踪技术

虚拟化环境P2P扫描技术

绿色杀毒 U盘、NAS存储防护

防勒索保护，防篡改安装保护

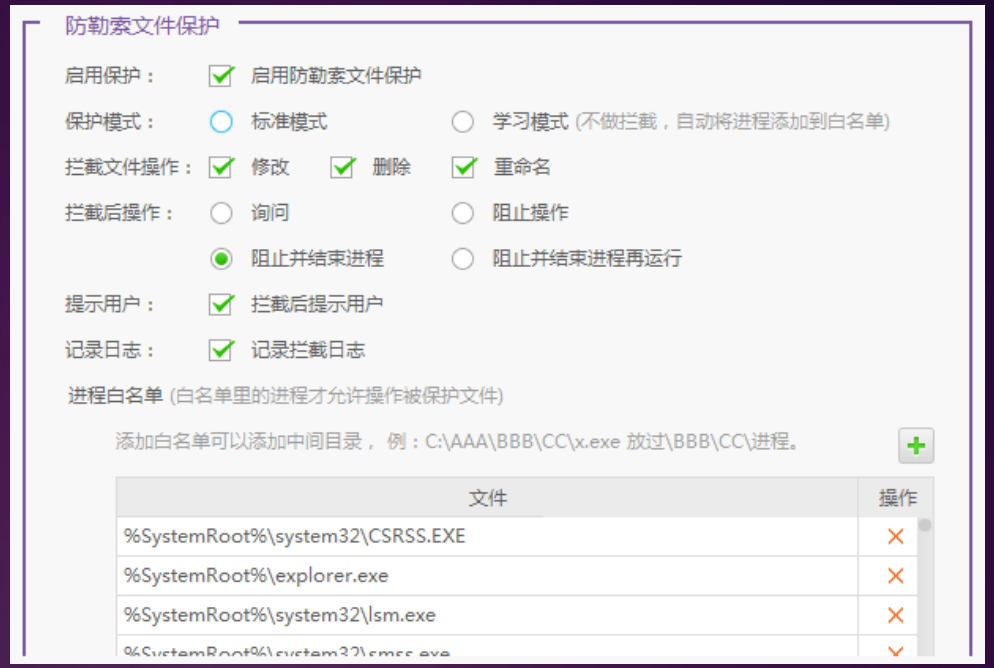
命令行、线程扫描，强力查杀

按场景的监控模式调整

特别技术

变频杀毒技术

自调节CPU占用，性能、速度上择优控制



绿色杀毒U盘

免安装、病毒库最新染毒环境PE处理

防勒索保护

源进程白+目标保护或排除方式

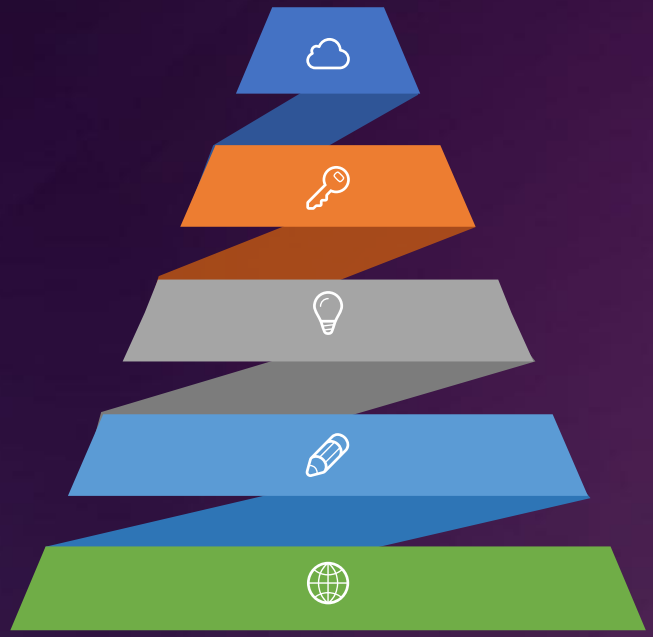
可防已知、未知勒索，学习模式

子产品功能

统一漏洞扫描、集中处理

补丁导入，内网分发

未修复漏洞、风险终端TOP排行



漏洞补丁黑白名单

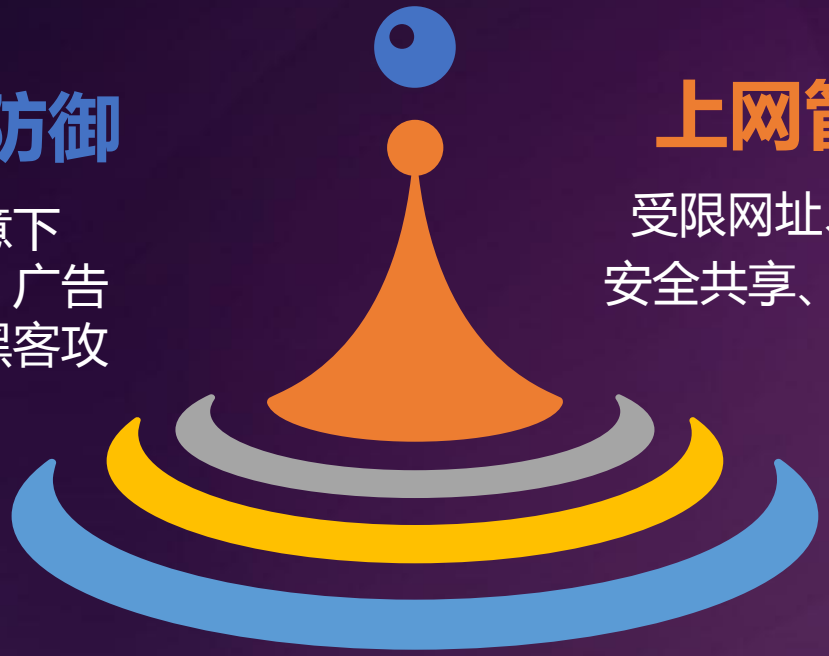
多补丁源，及时获取

补丁修复优先组，先实验、再推广

子产品功能

上网防护： 9大防御

拦截木马网址、钓鱼网址、恶意下载、跨站脚本攻击、对外攻击，广告过滤、搜索引擎结果检查、防黑客攻击、反ARP欺诈



上网管理：6大管控

受限网址、受限程序、流量管理
安全共享、ADSL共享、非法外联

IP规则

自定义规则：黑白名单，IP、端口
IP防篡改

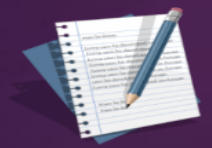
网络准入隔离

终端符合安全标准

终端具有不合规项

- 有未处理漏洞
- 未安装知道安全软件
- 客户端未在线
- 发现客户端感染指定病毒名或指定病毒类型
- 发现客户端有arp出站攻击记录
- 发现客户端有非法外联行为

客户端告警提示



生成违规记录

针对已安装客户端的终端

子产品功能

文档操作打印审计

- 文档操作审计：指定磁盘位置的文件的复制、删除等文件操作
- 文档打印审计：记录客户端打印内容的概要信息

完整外设管控

- 总线类型、设备类型、具体设备三层维度
- 移动设备、外设端口、无线网卡等从审计到准入控制一揽子解决

U盘管理准入

- 禁止使用未登记U盘
- 允许使用已登记U盘
- 禁止使用已登记U盘。

U盘准入

设备使用记录

允许禁用只读

准入分组控制

智能设备识别

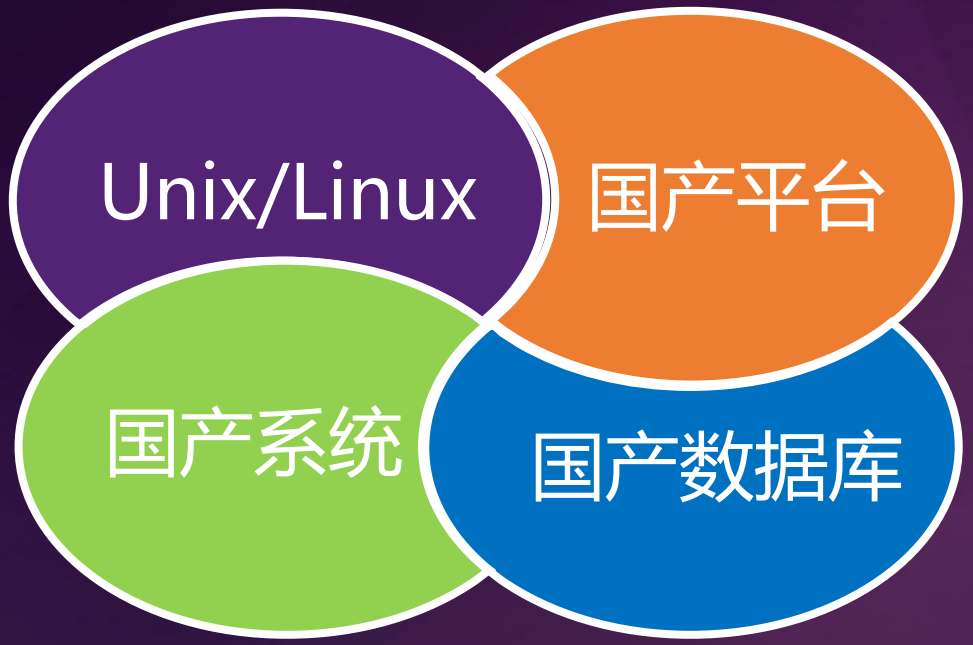
子产品功能


硬件管理
客户端硬件详情
检测硬件异动情况
统计终端硬件信息
软件管理
统计已安装软件
保护、禁止指定软件
查看已装软件详情
启动项管理
查看全网终端开机
启动项，并针对性
集中管控
统计开机用时
软件分发
协助用户推送需部
署的软件
统计推送软件的部
署情况

Linux/国产化支持

Centos
Solaris
Redhat
AIX
……

中标麒麟
银河麒麟
中科方德
凝思磐石
……



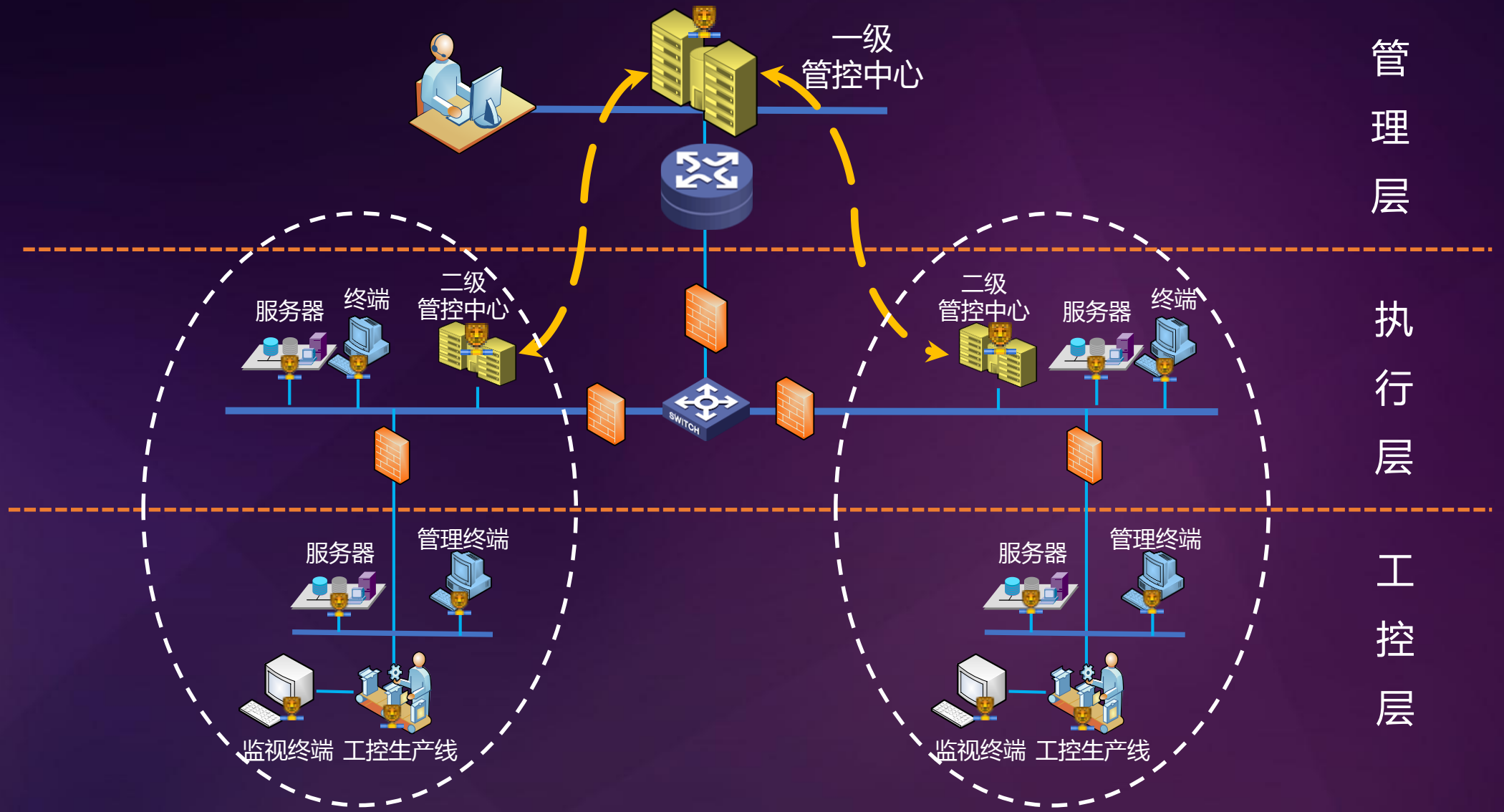
龙芯
兆芯
申威
飞腾
……

达梦
神通
南大通用
人大金仓
……

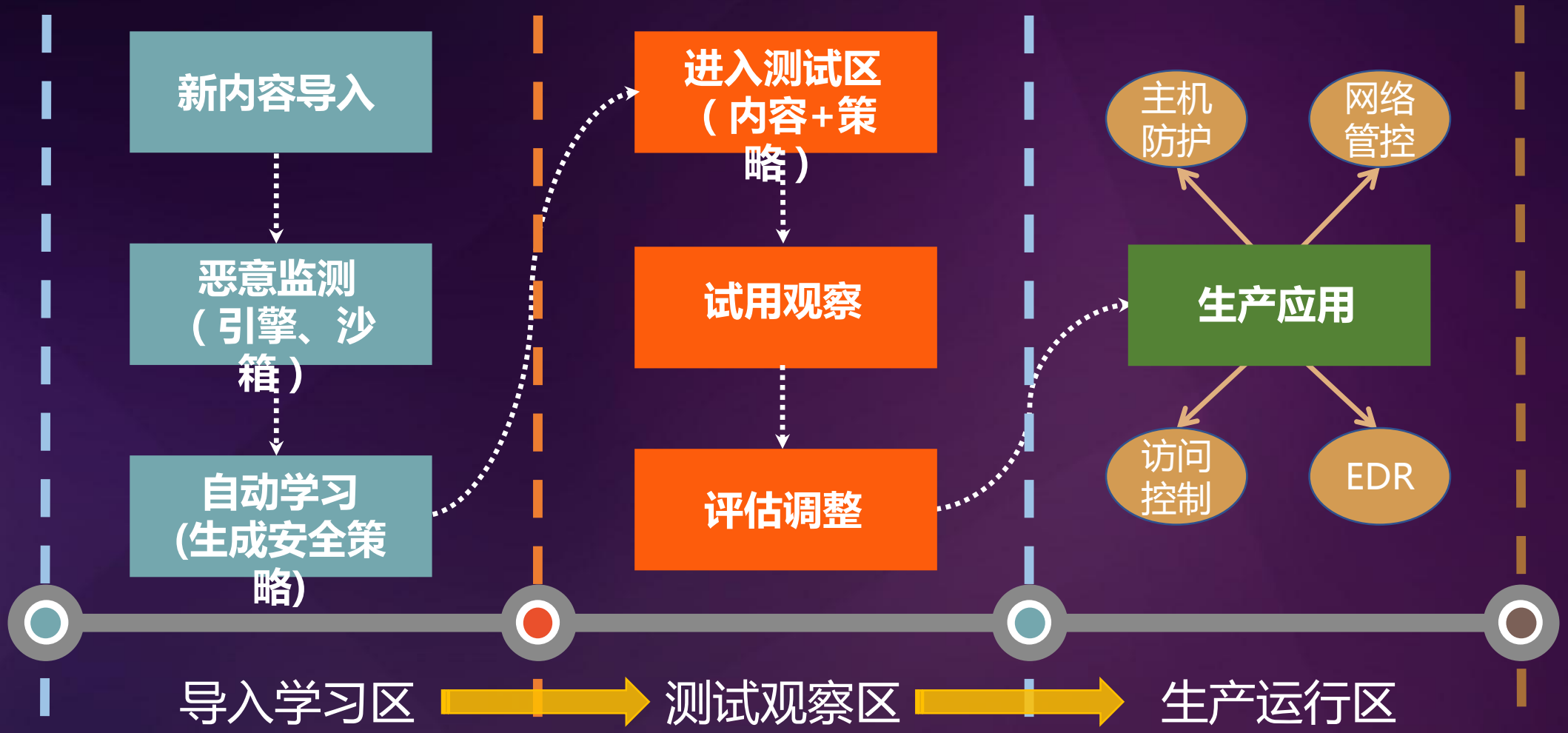
可运维、可管理

- 分区、可运维、自动化
- 安全检测+白名单模式
- 入侵防御、访问控制
- 检测与响应（EDR）相结合
- 情报支持、数据分析、未知发现

工控终端防护体系


一级
管控中心
二级
管控中心
服务器
终端
二级
管控中心
服务器
终端
SWITCH
服务器
管理终端
服务器
管理终端
监视终端
工控生产线
监视终端
工控生产线
管
理
层
执
行
层
工
控
层

分区运维


新内容导入
恶意监测（引擎、沙箱）
自动学习(生成安全策略)
进入测试区（内容+策略）
试用观察
评估调整
主机防护
网络管控
生产应用
访问控制
EDR
导入学习区
测试观察区
生产运行区

RISING 瑞星

www.rising.com.cn

北京瑞星

杨绍波

13811193889

yangsb@rising.com.cn