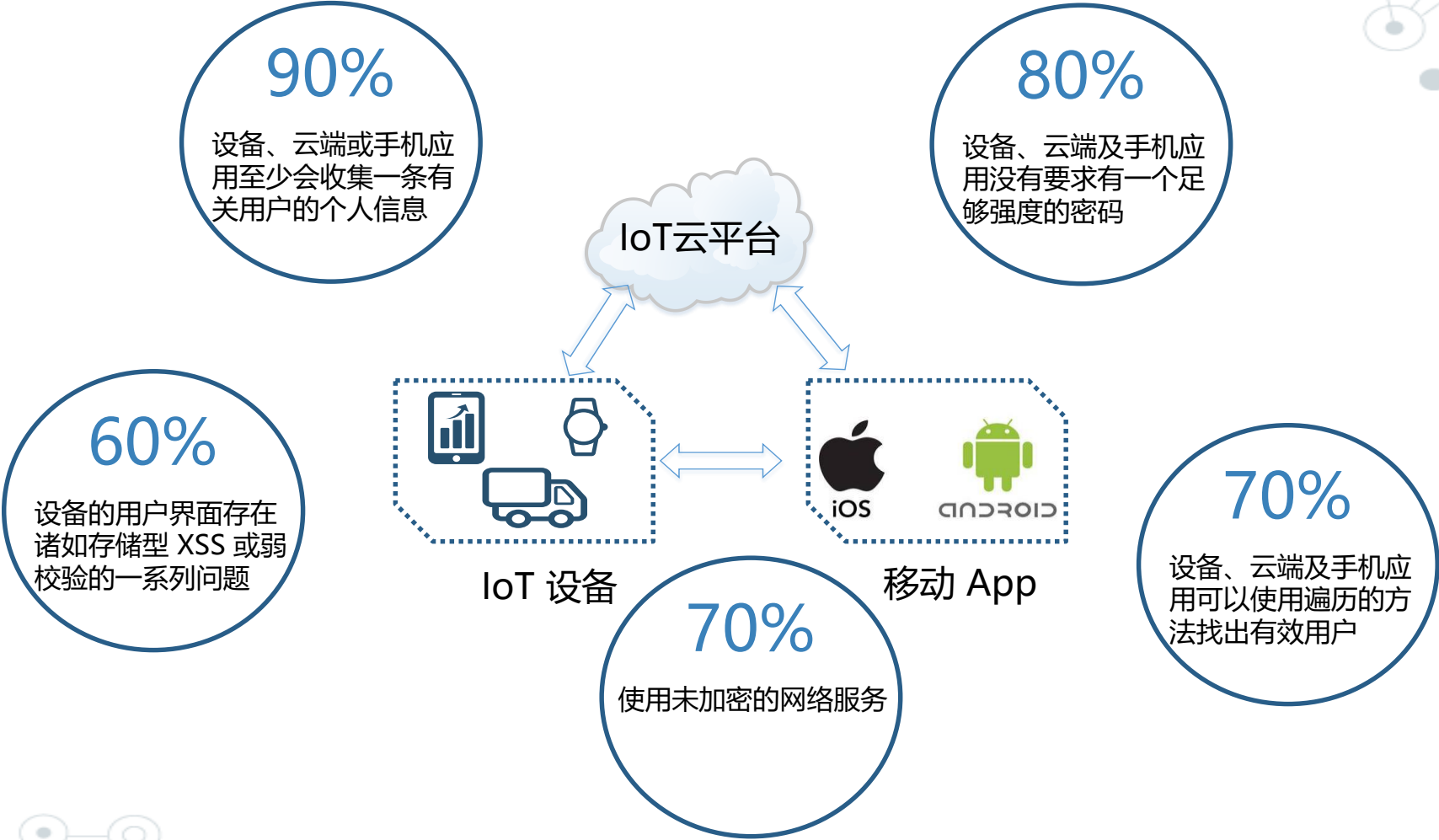


物联网面临的安全威胁



物联网 - 安全事件



XX省公安厅所使用的海XXX监控设备“存在严重安全隐患”，“部分设备已被境外IP地址控制”，要求对设备进行全面清查。

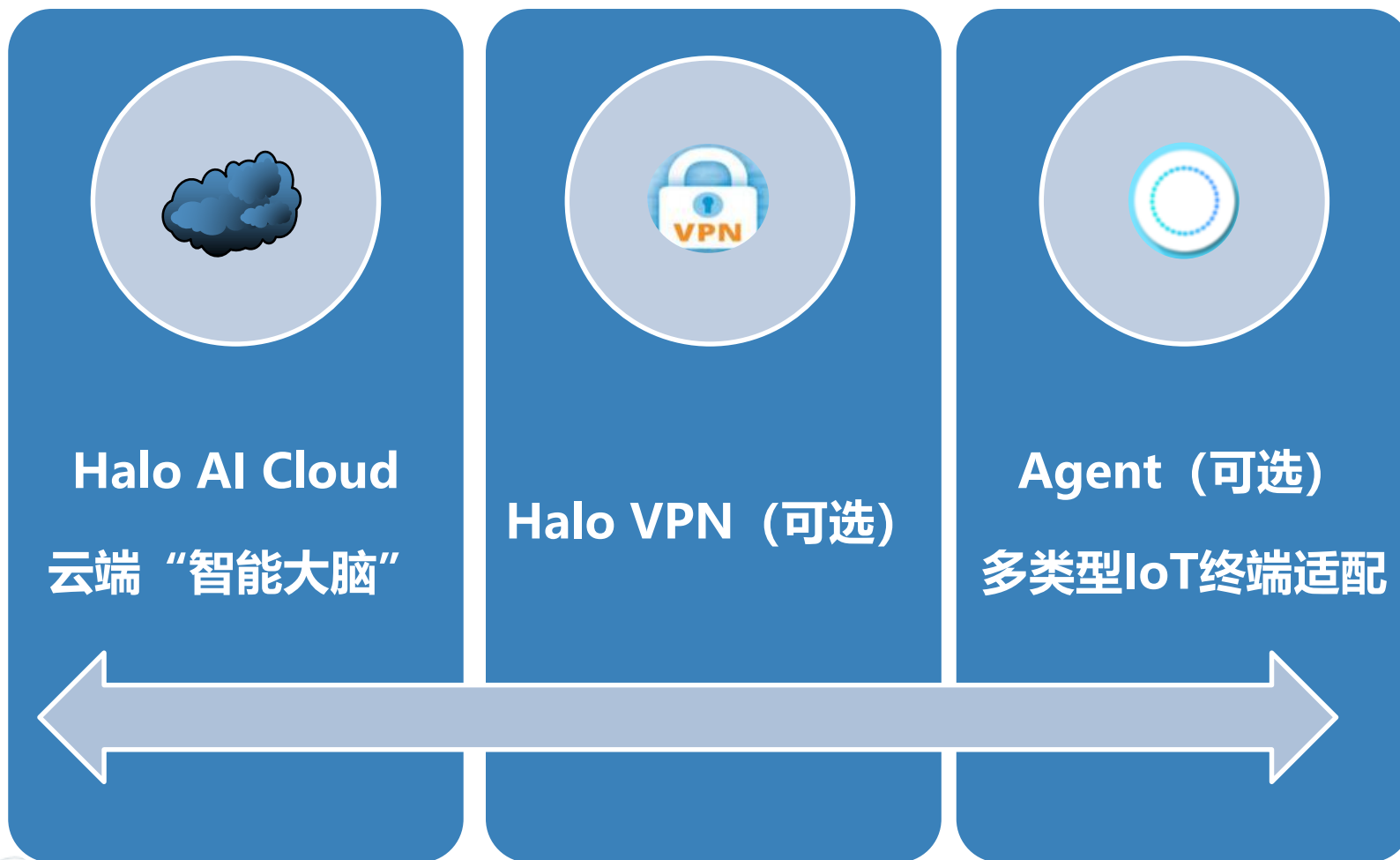


芬兰公寓的中央供暖和热水系统遭到了DDoS攻击，系统死循环，导致供暖切断。

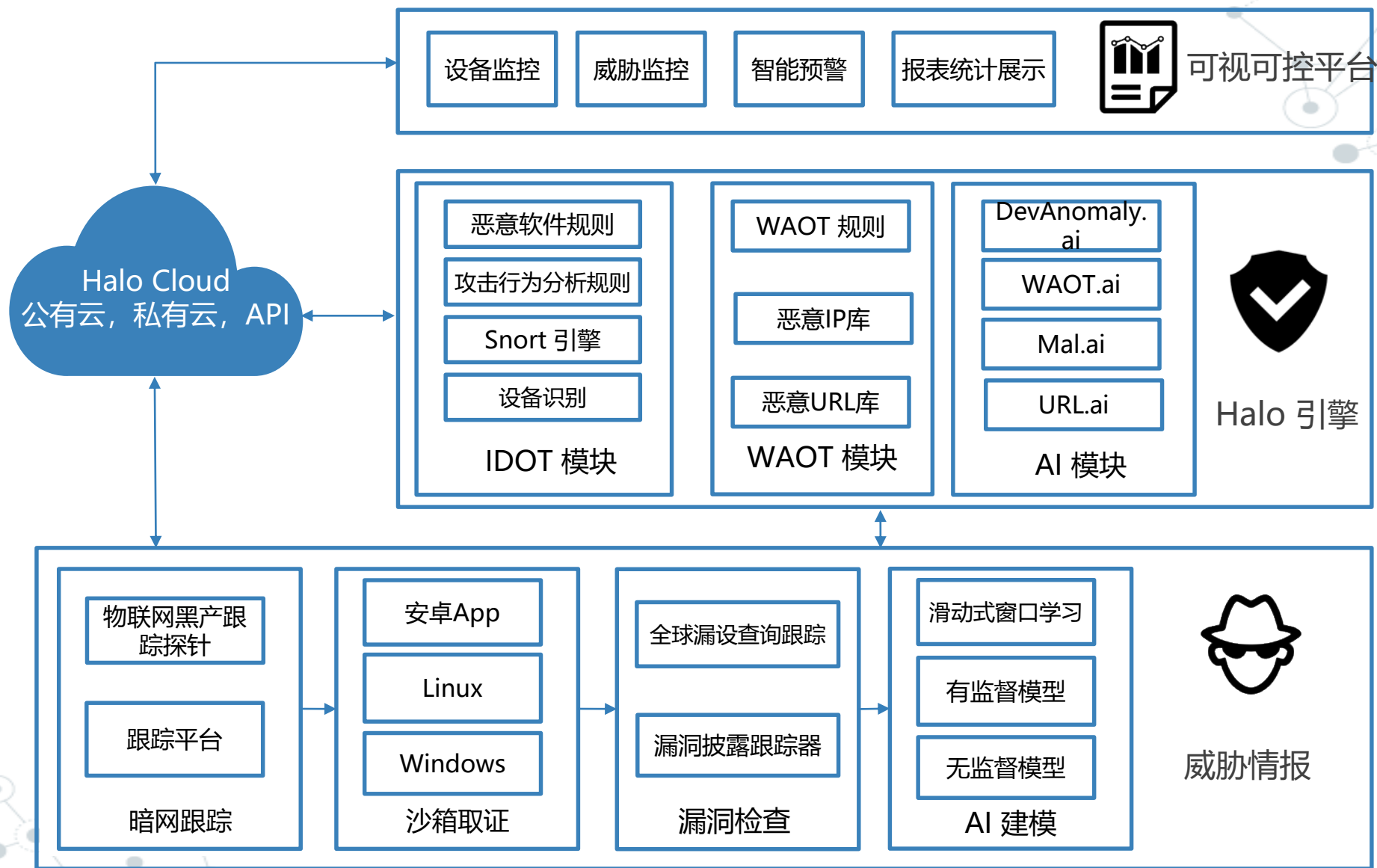


深圳瑞X酒店系统安全漏洞，随时远程控制房间里的温控器、灯光、电视、百叶窗、电子灯等设备。

IoT Halo 组成



Halo AI Cloud 架构介绍



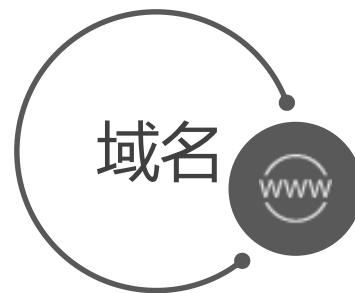
IoT Halo 能力



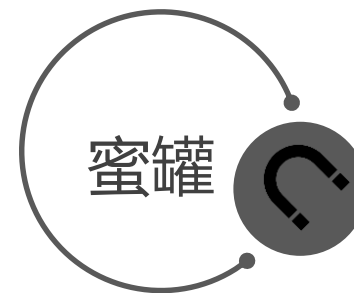
10亿
新增10000/日



2200万
新增50000/日



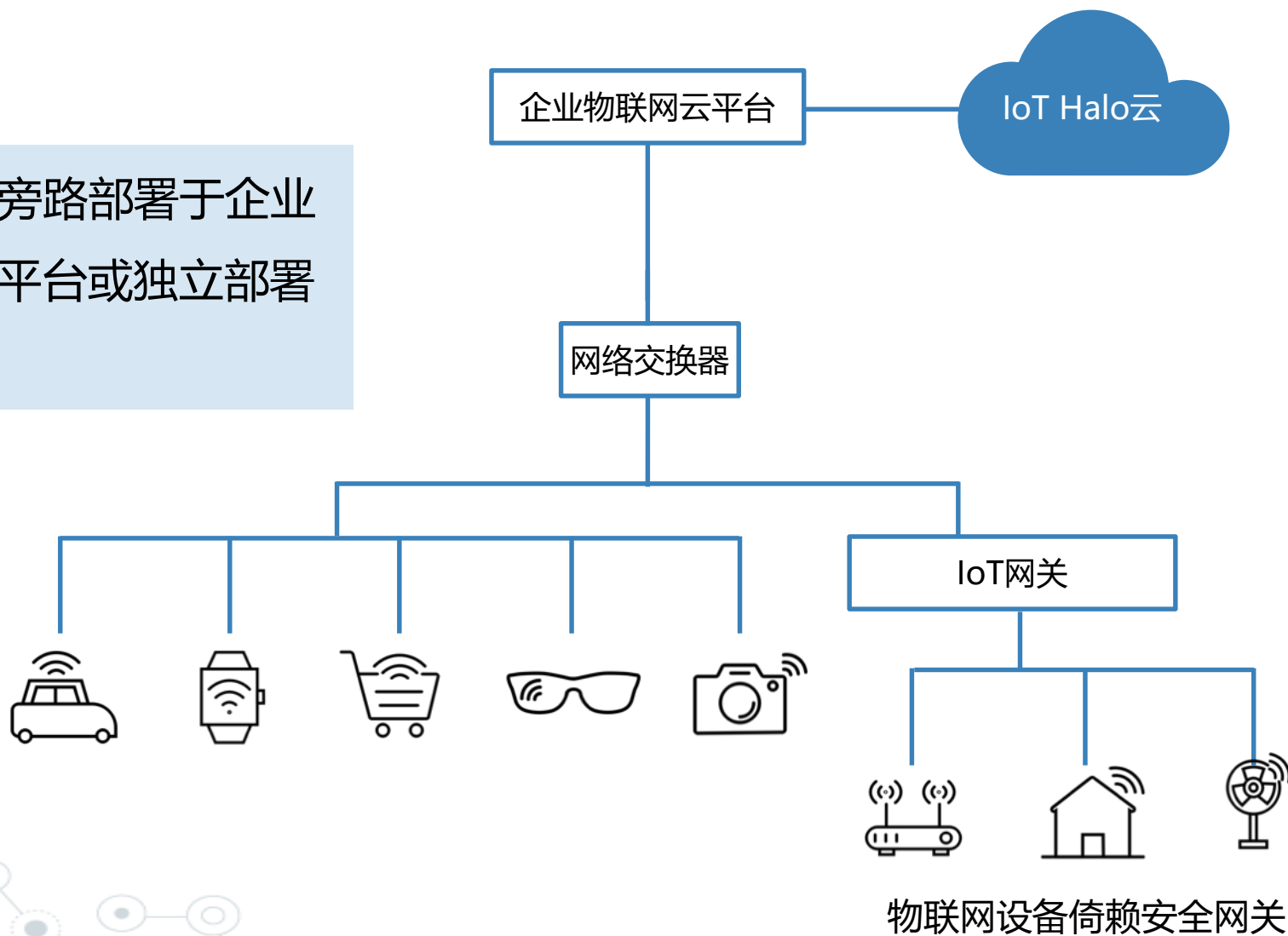
300万
新增5000/日



1万
全球部署

旁路部署

IoT Halo旁路部署于企业物联网云平台或独立部署于公网



适用场景及案例

■ 适用场景

企业已有物联网云平台，但平台建设之初未考虑信息安全，这种情况可与IoT Halo集成，通过API方式调用IoT Halo，使原有企业物联网云平台具备安全能力

■ 案例

T-Mobile

主要功能介绍-设备发现摸底

2

终端设备

6

4

视频类设备

13

3

网络设备

7

17

BYOD类设备

17

9

应用服务设备

15

0

安全及运维设备

0

0

打印设备

1

0

其他设备

21

基本信息

定位

使用审计

接入审计

BYOD例外

刷新

IP地址

192.168.104.16

MAC地址

B4-A3-82-7A-5E-81

网卡厂商

Hangzhou Hikvision Digital

资产类型

视频类设备

应用

设备种类

网络摄像机 (IPC)

主机IP地址

192.168.104.16

~

192.168.104.16

报警类型

所有

主机MAC地址

报警级别

所有

报警时间

2018-06-25 00:00:00

~

2018-06-25 23:59:59

区域名称

所有

排序方式

按报警时间排序

报警描述关键字

查询

报表

序号	主机IP	类型	级别	描述	次数	时间	可信度%	明细
1	192.168.104.16	弱口令漏洞	超度危险	检测到海康摄像头使用默认口令或弱口令, 存在安全风险, 建议及时修正, 其IP地址为: 192.168.104.16。	35	2018-06-25 16:38:59	100	MORE

备注信息

应用

首次上线

2018-06-25 09:47:28

更新时间

2018-06-25 16:42:25

应用及脆弱性信息

开放端口数量

3

详细

脆弱性漏洞数量

1

详细

Redis版本

5.5.2

隶属区域

隶属行政域

所有

上联设备IP

192.168.100.5

上联端口描述

Fa0/5

主要功能介绍-设备发现摸底分类

终端设备

Windows系列

- Windows XP
- Vista
- Win 7
- Win 8、8.1
- Win 10

Linux系列

- Ubuntu
- Red hat
- 麒麟
- Centos
- Debian
- Fedora

网络设备

思科

华为

H3C

锐捷

3com

北电

D-link

TP-Link

Juniper

中兴

迈普

磊科

摄像头

海康威视

大华科技

科达

宇视

博世

天地伟业

亚安

汉邦

Polycom

海芯威视

打印机

佳能

惠普

富士

爱普生

兄弟

京瓷

理光

日冲

利盟

无线设备

思科

华为

H3C

D-link

TP-Link

腾达

小米

小度

腾讯

360

磊科

水星

锐捷

主要功能介绍-非法接入预警

- ◆ 针对智能设备替换为其它设备，如普通PC、笔记本电脑、有线或无线网络设备等进行监控、报警。

当前位置： 查询统计和报表/报警信息

主机IP地址	<input type="text"/> ~ <input type="text"/>	报警类型	所有
主机MAC地址	<input type="text"/>	报警级别	所有
报警时间	2016-11-01 00:00:00 ~ 2016-11-01 23:59:59	查询	报表

序号	主机IP	类型	级别	描述	次数	时间	可信度%	
1	192.168.50.42	系统运行环境变更	警告	系统检测到视频设备 (192.168.50.42) 其运行环境发生了变更。	1	2016-11-01 10:51:16	90	MOR
2	192.168.20.49	系统运行环境变更	警告	系统检测到视频设备 (192.168.20.49) 其运行环境发生了变更。	1	2016-11-01 10:48:53	90	MOR

当前第 1 页 共 1 页

1

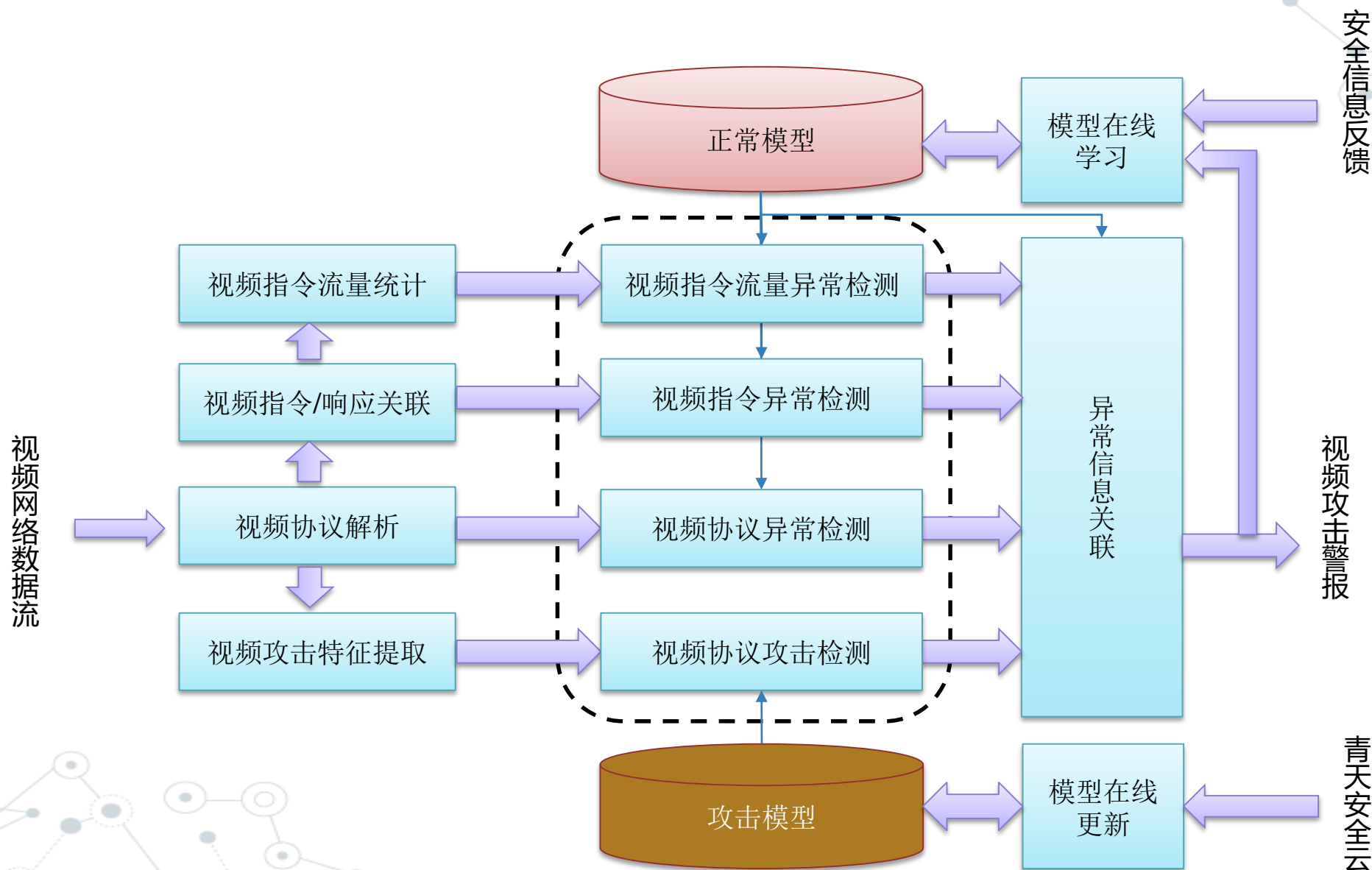
- ◆ 针对智能设备故障下线进行监控、报警。

当前位置： 查询统计和报表/报警信息

主机IP地址	<input type="text"/> ~ <input type="text"/>	报警类型	所有
主机MAC地址	<input type="text"/>	报警级别	所有
报警时间	2017-01-05 00:00:00 ~ 2017-01-05 23:59:59	查询	报表

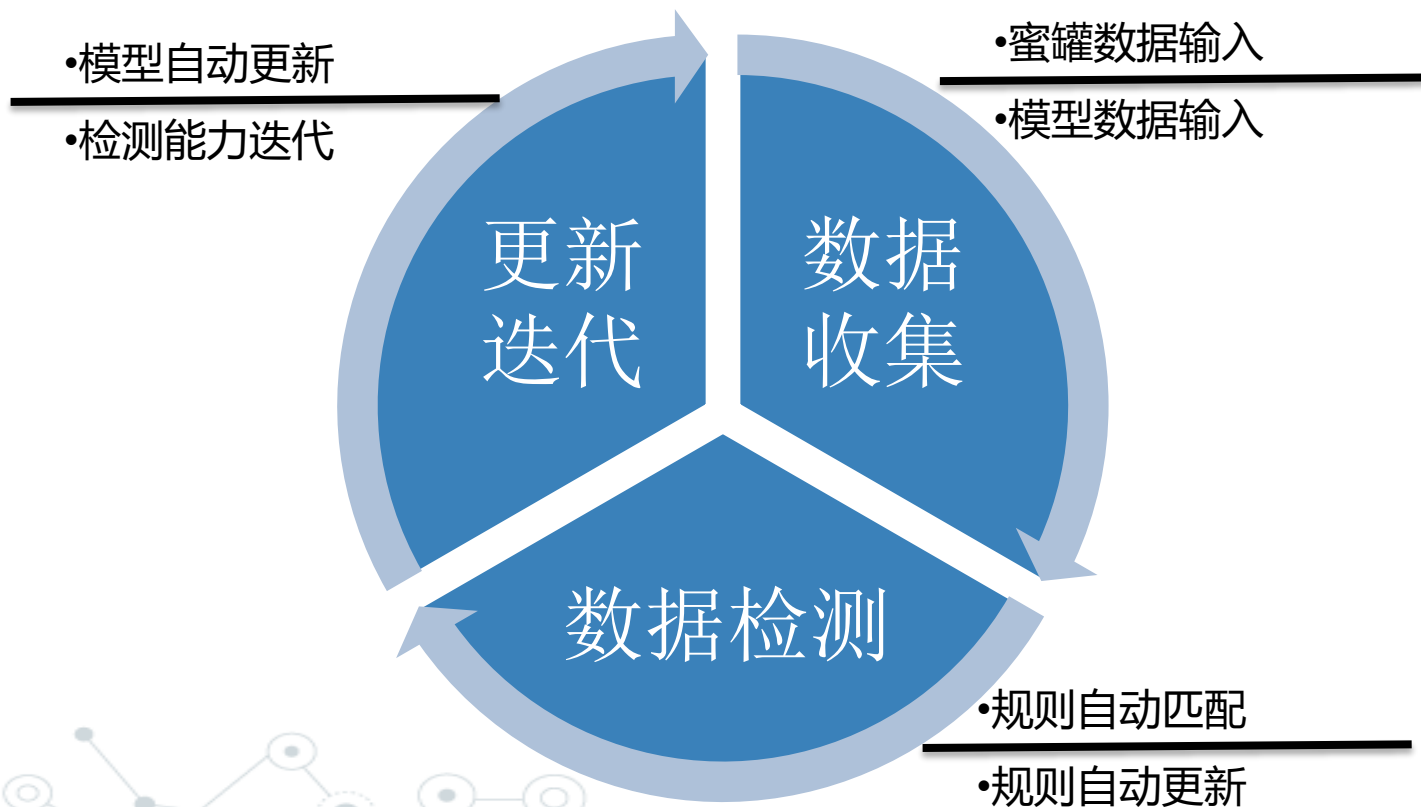
序号	主机IP	类型	级别	描述	次数	时间	可信度%	明细
1	192.168.50.73	非法接入主机	严重警告	系统检测到非法接入主机:192.168.50.73,Mac地址:70-62-B8-CB-E4-87	4	2017-01-05 22:30:21	100	MORE
2	192.168.20.89	设备离线	严重警告	系统检测到 设备离线	2	2017-01-05 22:30:21	100	MORE
3	192.168.20.76	非法接入主机	严重警告	系统检测到非法接入主机:192.168.20.76,Mac地址:8C-AB-8E-89-A4-78	4	2017-01-05 22:30:21	100	MORE
4	192.168.20.72	非法接入主机	严重警告	系统检测到非法接入主机:192.168.20.72,Mac地址:08-57-00-6E-97-CD	4	2017-01-05 22:30:21	100	MORE
5	192.168.20.79	非法接入主机	严重警告	系统检测到非法接入主机:192.168.20.79,Mac地址:28-F3-66-B0-7A-29	4	2017-01-05 22:30:21	100	MORE
6	192.168.50.56	非法接入主机	严重警告	系统检测到非法接入主机:192.168.50.56,Mac地址:CC-B2-55-CC-EA-26	4	2017-01-05 22:30:21	100	MORE
7	192.168.50.61	非法接入主机	严重警告	系统检测到非法接入主机:192.168.50.61,Mac地址:0C-82-68-F5-C4-FB	4	2017-01-05 22:30:21	100	MORE
8	192.168.20.51	非法接入主机	严重警告	系统检测到非法接入主机:192.168.20.51,Mac地址:C0-61-18-28-C1-DD	4	2017-01-05 22:30:21	100	MORE

主要功能介绍-视频指令异常检测系统



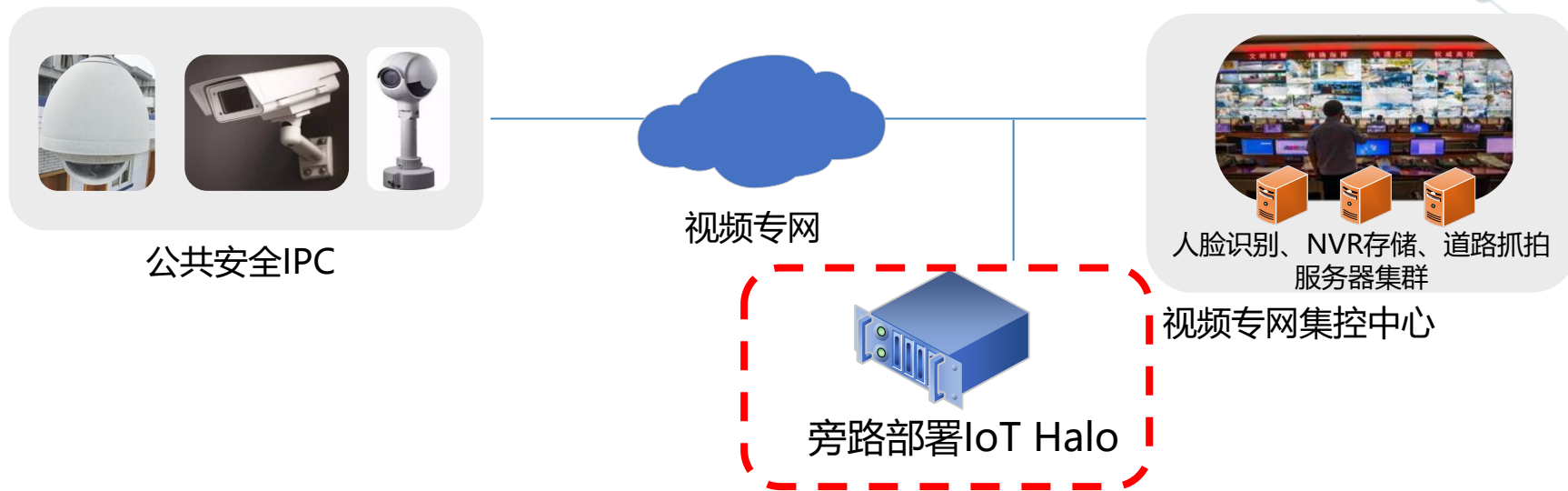
主要功能介绍-全流程闭环管理

全流程闭环管理：实现收集-检测-更新迭代的全流程闭环管理能力，并实现三个全自动，即模型更新迭代全自动，规则策略全自动及威胁检测全自动。



- 闭环流程主要体现在数据收集、检测和更新迭代三个方面，通过此闭环流程建立**完整的安全威胁检测生态**，提高系统检测效率
- 根据自动化建模，自动化规则更新迭代等能力，为系统提供全自动的安全检测和更新迭代过程，在模型更新后同时**自动更新检测规则**，减少人工干预

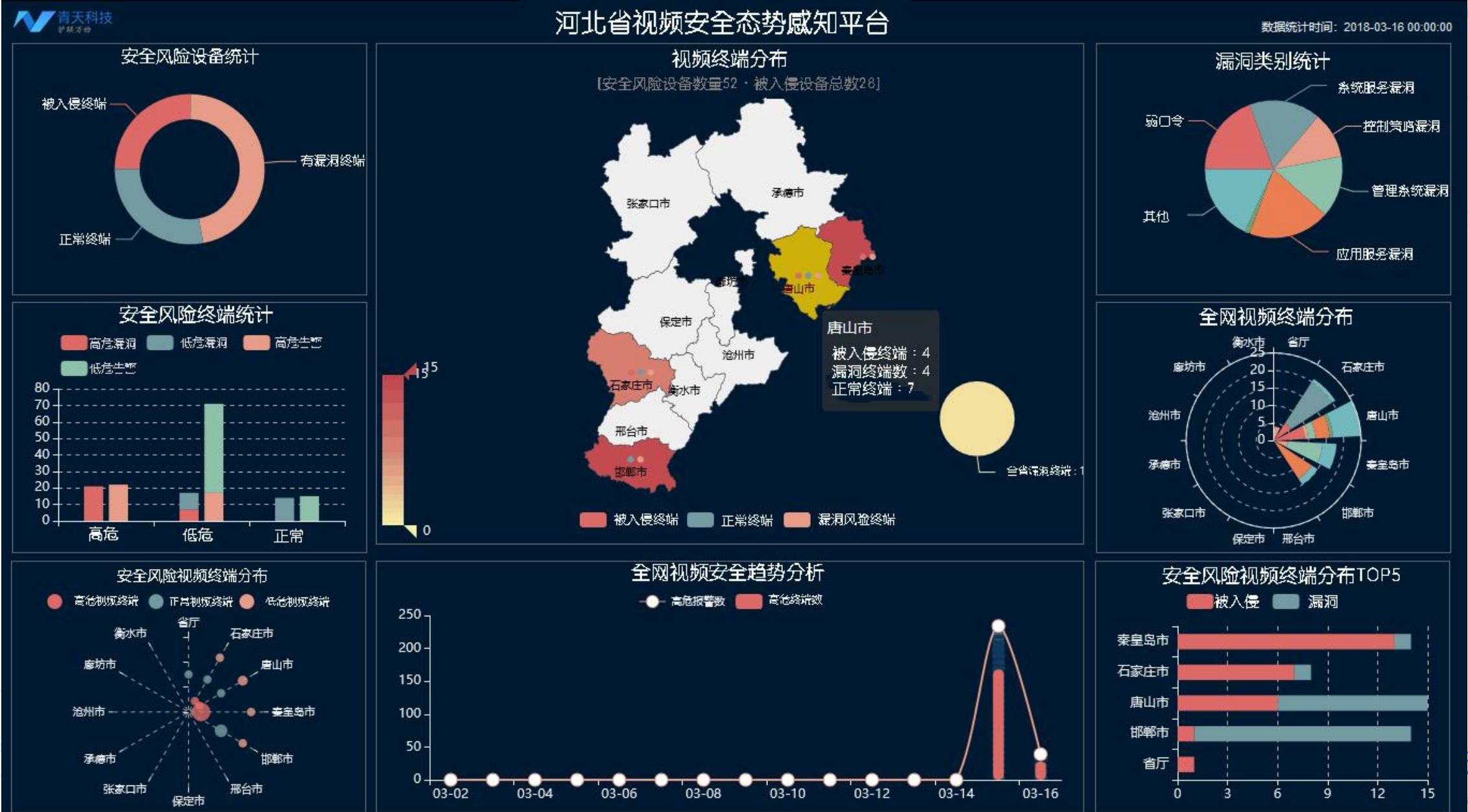
前端视频终端安全防护解决方案



■ 方案特点:

- IoT Halo一键**旁路部署**，现网业务不受影响，兼容所有IPC，现网原有安全策略不受影响；
- IoT Halo基于AI和大数，对现有视频指令进行机器学习、建模，可实现预测性**主动防御**，变变动安全为主动安全；
- IoT Halo基于蜜罐和沙箱技术并结合大数据，可以第一时间掌握视频安全威胁情报，为用户应急响应和风险控制争取更多宝贵时间；
- IoT Halo实现对IPC的，安全可视化，安全事件的报警、溯源、定位，让用户了解到海淀区公共视频监控的安全全景；
- IoT Halo可实时检测和有效应对针对IPC发起的各类勒索软件、挖矿病毒、DDOS、SQL注入等攻击，确保未被感染IPC的安全，同时对于已受感染的IPC可在IPC有异常行为时第一时间发现，避免感染网内更多IPC，同时IoT Halo与原有网内安全设备进行联动，实现原有和新增的1+1>2的效果，有效保护海淀区公共安全8万个摄像头的安全，避免了因黑客入侵而带来的一系列危害，真正的确保海淀区的公共安全。

视频安全态势感知平台：可视化界面



THANKS!

联系人：姜超华 13926011148

chaohua.jiang@newskysecurity.com



← **敬请关注!**
获取更多IoT安全资讯

青天科技：护联万物
助力IoT方案更安全