# IoT安全监测解决方案

# 目录

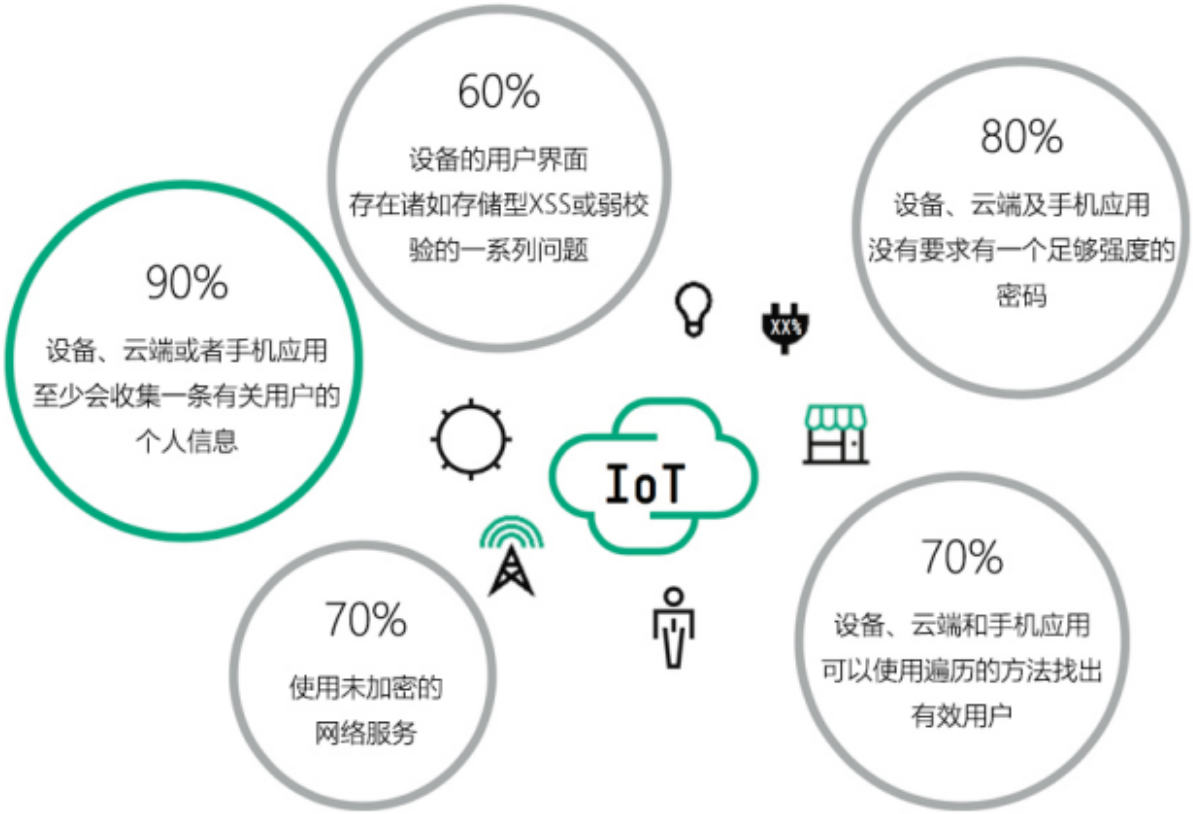
# IoT安全问题

- 根据Forrester的2018年安全威胁预测，IoT的安全差距会越来越大。
- 研究人员相信，IoT会与公有云结合，通过对个人和网络数据的访问、处理、窃取和泄露，引入更多的安全威胁。而且，有更多的为了经济利益的IoT攻击，比如加密货币挖矿和对售货机、医疗设备、车辆的勒索攻击。
- 隐私和数据共享会变得更难管理。比如，如果你是一个智能玩具的制造商，你要如何更好地管理和保护儿童的数据？关于隐私的考虑可能会扩大到保护如果保护国内外政府收集的情报中的个人数据。

# IoT防护很弱

1. 设备本身并不集成安全机制。不像手机、笔记本、台式机，IoT的操作系统的防护基本没有。原因就是在设备集成安全机制的成本太高，还会减缓开发流程，有时候甚至会影响设备性能，如运行速度和容量。
2. 设备直接暴露到网络，因为网络分割很弱。同时可以作为内网的一个中转点，向网络犯罪分子开了后门。
3. 设备中含有基于通用的、Linux驱动的硬件和软件开发过程中留下的非必要的功能。注释：开发者有时会在beta版不会删除一些代码或者特征。
4. 默认的身份信息是硬编码的。这意味着插入设备就可以运行，而不会创建唯一的用户名和密码。

# IoT安全威胁


60%
设备的用户界面
存在诸如存储型XSS或弱校
验的一系列问题
80%
设备、云端及手机应用
没有要求有一个足够强度的
密码
90%
设备、云端或者手机应用
至少会收集一条有关用户的
个人信息
IoT
70%
使用未加密的
网络服务
70%
设备、云端和手机应用
可以使用遍历的方法找出
有效用户

# 依靠传统”老三样”堆积的安全防护并不靠谱


攻击被发现的平均时间

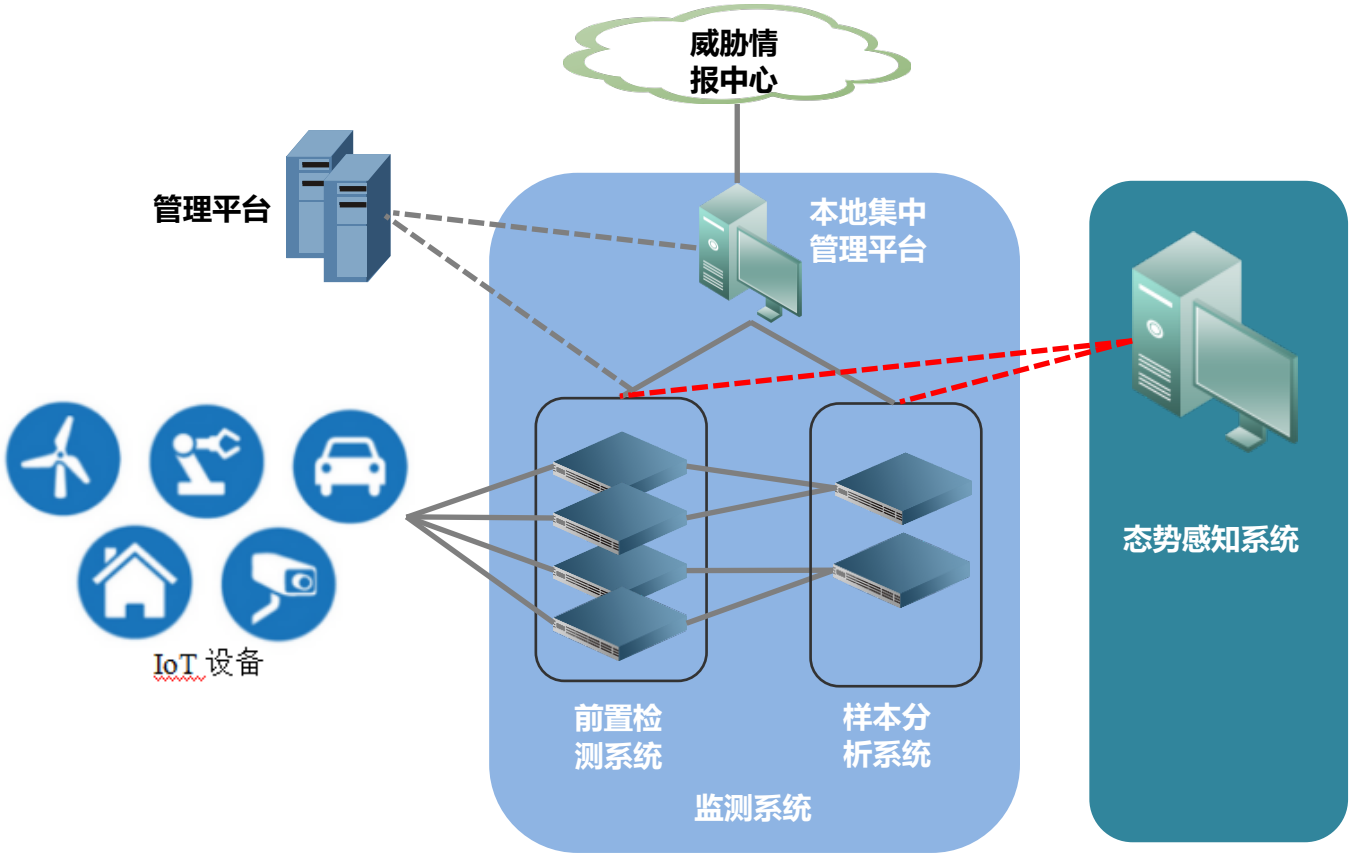
**229天**

企业自行发现的比例

**33%**

# 安全解决方案

# 安全监测平台




## 检测子系统

基于特征库等进行僵木蠕识别，并还原样本，上传告警和日志到管理平台；

## 样本分析子系统

负责将可疑样本做深度分析，并将异常样本和告警传至集中管理平台

## 集中管理平台

负责收集僵木蠕检测子系统和样本分析子系统上传的告警和样本，威胁情报同步；设备集中管理。

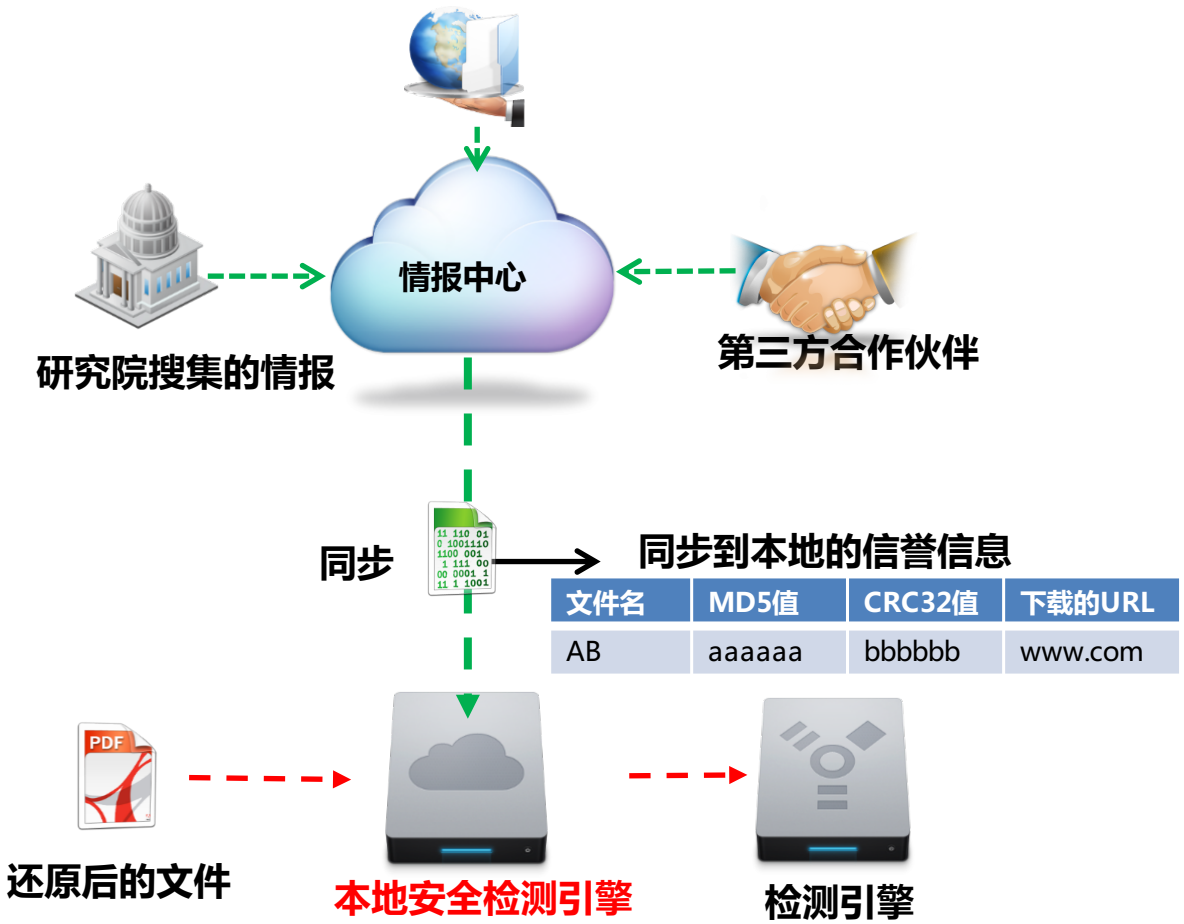
## 威胁情报中心

威胁信息的收集、汇总、分析、交换与分发

## 态势感知系统

可选部署，基于检测系统检测结果采用大数据分析方式，深度挖掘态势和网络信息，并进行呈现

# 基于威胁情报的协同防御




**价值**

- 利用广阔的全球情报，让检测更加高效、精准、及时；

**功能**

- 检测系统跟情报中心对接，及时获取全球最新威胁信息和特征，及时防护本地网络未知威胁；
- 上传本地检测未知威胁样本，由云端及时进行详细分析；

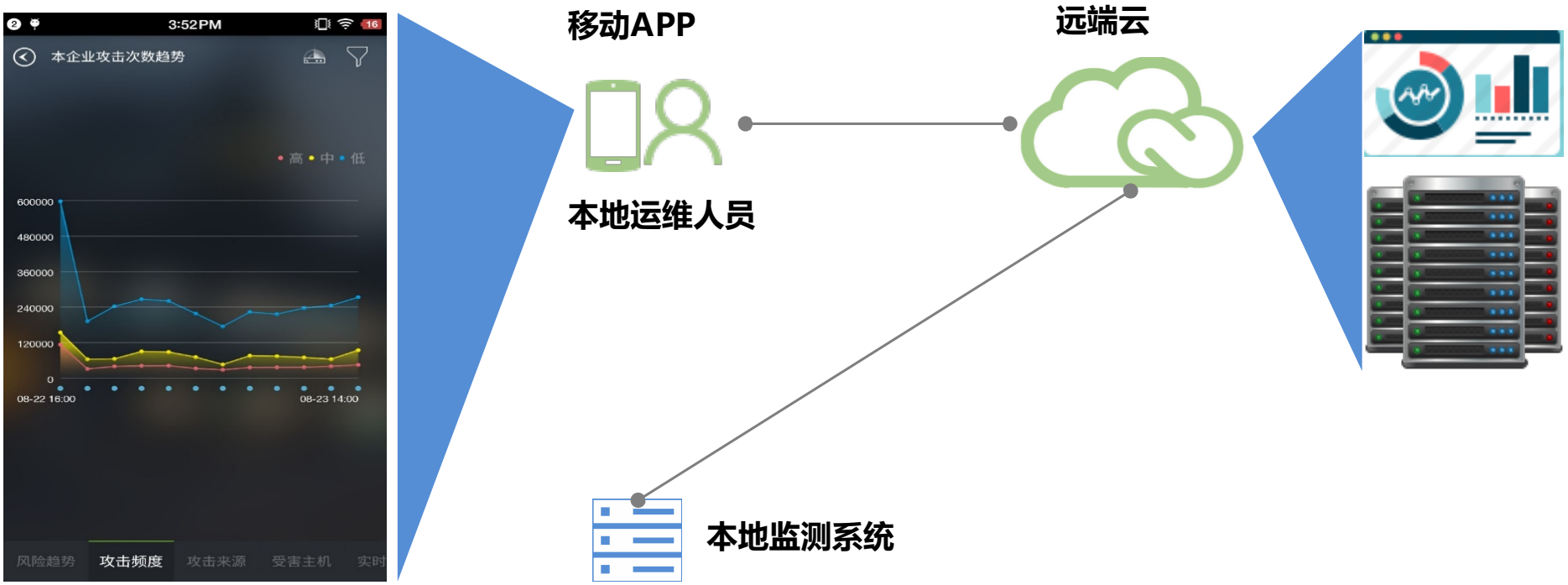
# 实现对IoT的集中管理


- 设备状态监控，实时告警；
- 策略批量下发，简化运维；
- 对接云端，完成特征库和情报实时更新

# IoT态势平台实现对威胁综合分析和溯源


- 控制端主机追踪，网络地图分析，文件病毒监控；
- 定制报表；
- 基于Flow数据溯源；

# 移动终端远程监控，实时获取最新IoT安全信息




- 本地检测系统跟安全云对接，实时上传检测告警等信息
- 云端结合最新资讯实时分析上报检测结果
- 云端将分析结果实时推送给运维人员移动APP上，及时掌握重要安全检测告警和资讯等信息