金山网络
www.ijinshan.com

# 云@金山

--一种不同的思路做云安全

**演讲人: CardMagic (孙明焱)**
**金山网络**

## Agenda

**金山云体系**

**金山云防御**

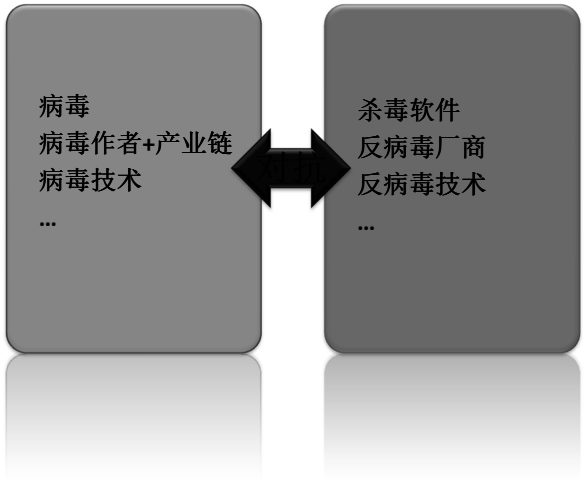
**金山云查杀**

## 关于演讲者

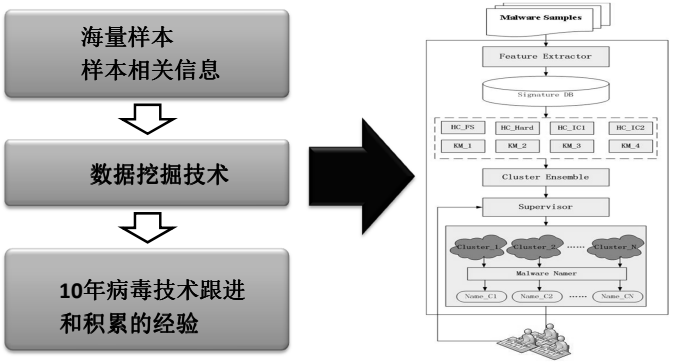
**孙明焱 ID: CardMagic**

**-现任金山网络产品总监，负责金山毒霸相关开发**
**-曾任奇虎360云查杀产品负责人**
**-曾任Trend Micro技术经理**
**-曾任NEC开发工程师**
**-Antirootkit工具DarkSpy的作者(被趋势科技收购）**
**-精通各类安全开发，曾负责开发过各类云安全产品**

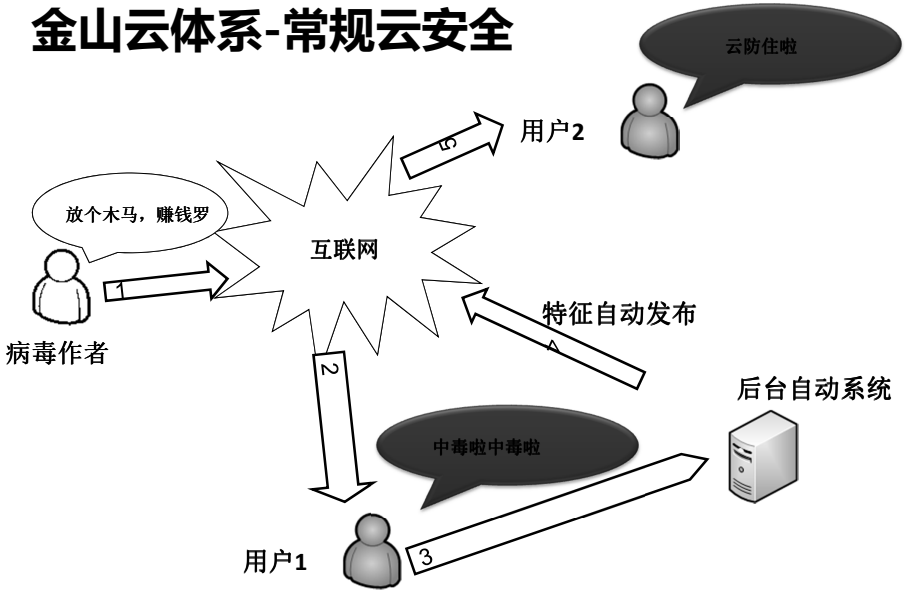
## 金山云体系-信息安全问题的源头



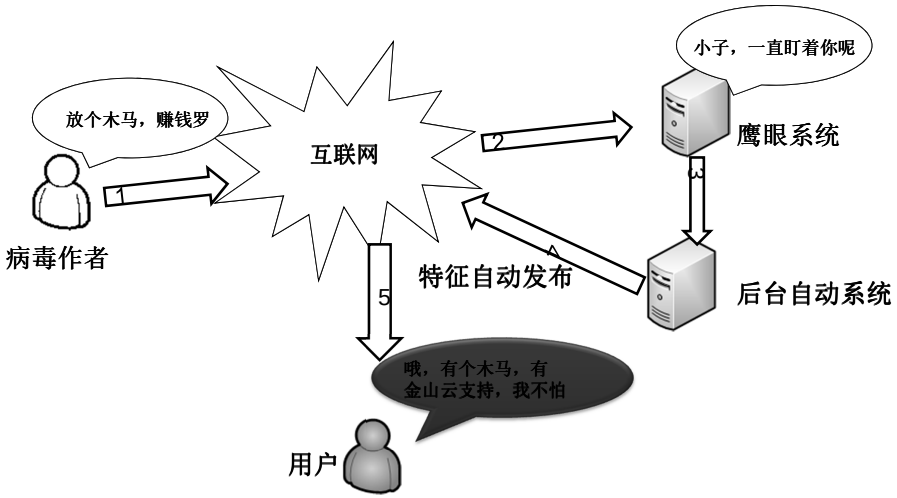
# 金山云体系-云端智能鉴定技术




# 金山云体系-常规云安全




# 金山云体系-黑色产业链解决(1)




# 金山云体系-黑色产业链解决(2)

- **为什么要产业链：**

  **- 产业链做为直接鉴定器，鉴定文件与URL**

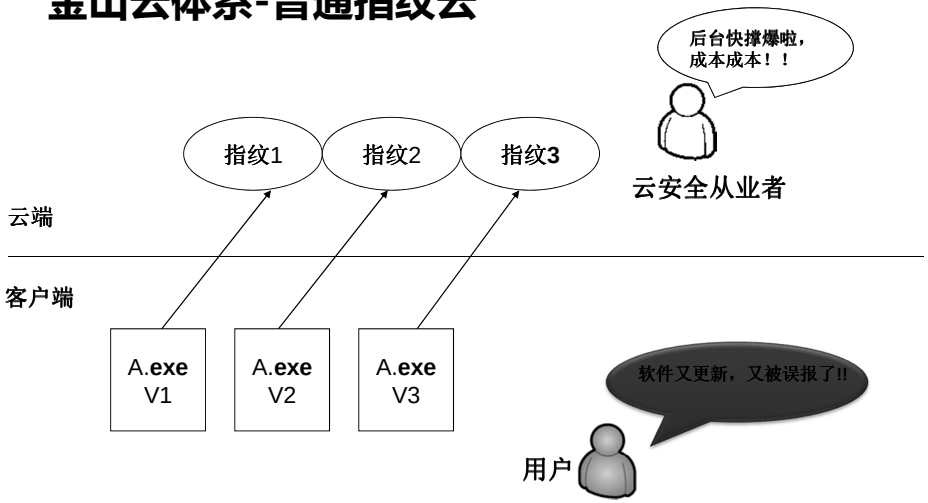
  **- 在病毒还没有大规模传播时，就可以根据病毒集团的运营能力了解病毒可能传播的范围，提前做好准备**

  **- 产业链聚类后病毒传播特征明显，便于做方案，只需针已病毒集为单位验证即可**

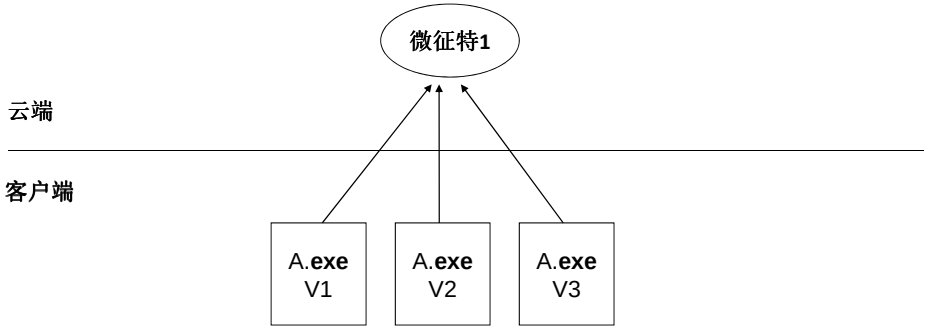
# 金山云体系-黑色产业链解决(3)

- **金山黑产业链积累：**
  - **独特的产业链归类系统**
  - **产业链特征自动提取系统**
  - **专门团队运营与监控**

# 金山云体系-普通指纹云




# 金山云体系-金山微特征云

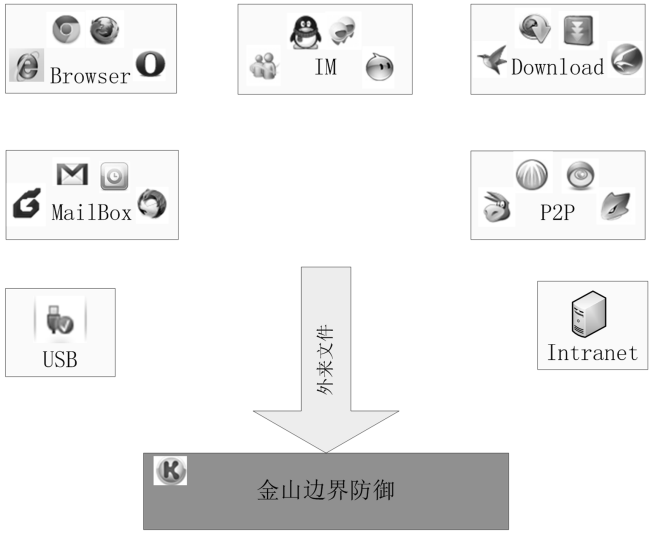



# 金山云体系-关于金山云体系的一些成果

- **通过鹰眼系统以及金山对产业链的积累，在大陆地区首家披露了十大病毒集团**
- **金山云后台拥有30多款各类鉴定器，涵盖各类启发式与智能鉴定技术**
- **金山云后台每天发布约30万特征，其中：**
  **白特征 约25万**
  **黑特征 约5万**

# 金山云防御


# 金山云防御-什么是边界防御




# 金山云防御-为什么要边界防御(1)

- 传统主动防御的痛处
  - 病毒执行后行为变化方法太多
  - 既需要应对文件变化，又需要应对行为变化
  - 随着各种安全策略的增加，不断拖耗系统性能
  - 兼容性不好
  - 驱动级更新对抗，稍有不慎便蓝屏崩溃
  - 进程执行时文件太多后台无法完全鉴定

# 金山云防御-为什么要边界防御(2)

- 边界防御的优势
  - 只做文件对抗
  - 只有极少情况会触发边界防御逻辑
  - 轻量级高兼容性实现
  - 不用根据病毒的行为变化不停改变

## 金山云防御-为什么要边界防御(3)

- 边界防御可行么
  - 每日边界防御的新增文件数量是有限的（可运营）
  - 边界防御中遇到的威胁是容易定性的（可做解决方案）

## 金山云防御-边界防御 V.S. 下载保护(1)

- 最本质的区别
  - 边界防御是一个整体的解决方案以保证恶意文件不进入系统。
  - 下载保护只是一个具体的产品功能

## 金山云防御-边界防御 V.S. 下载保护(2)

具体差异表现在如下几点：

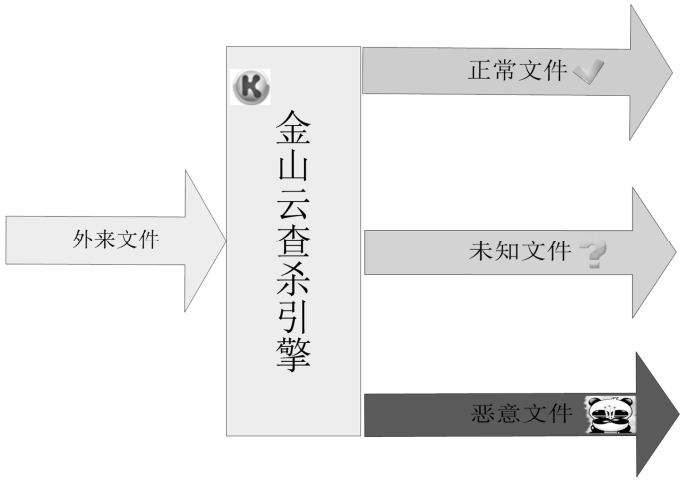
- 边界防御是全面的，不光包含下载，并且会不断覆盖新渠道
- 投入精英和最优资源参与边界防御
- 对各种入口进入的各类文件有完善的解决方案和相关的专门开发和产品运营团队投入
- 云端有专门团队和专门流程应对处理边界防御文件，包括：鉴定黑白，运营外挂色播等。力保边界所有文件均有鉴定结果
- 由于对边界防御概念的深刻理解，会不断关注并挖掘边界防御安全新动向，并开发解决方案

## 金山云防御-金山边界防御的优势和积累

金山做边界防御有如下优势和积累：

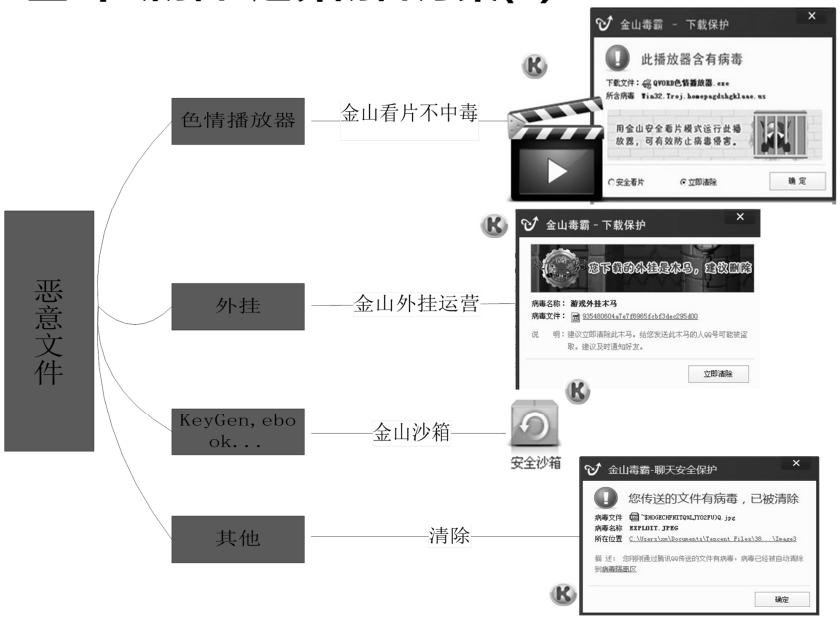
- 基于特征的云，保证在边界的文件特征数量极其收敛
- 后台30多种自主开发鉴定器（各种启发式以及专项鉴定）
- 金山长期积累各种鉴定器以及分析人才
- 从上到下对边界防御的深刻认识

# 金山云防御-边界防御方案(1)

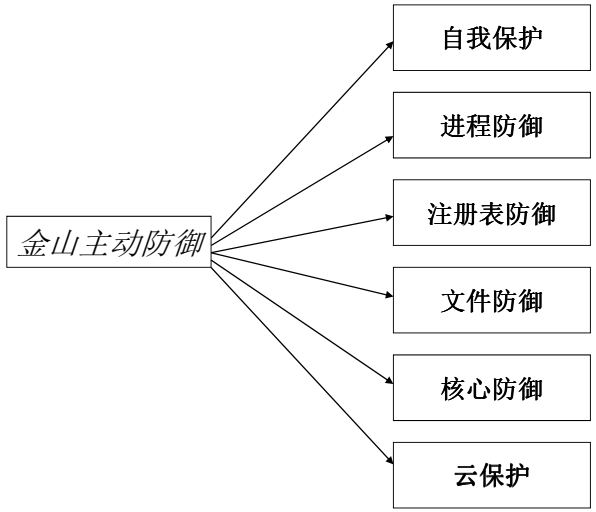



# 金山云防御-边界防御方案(2)

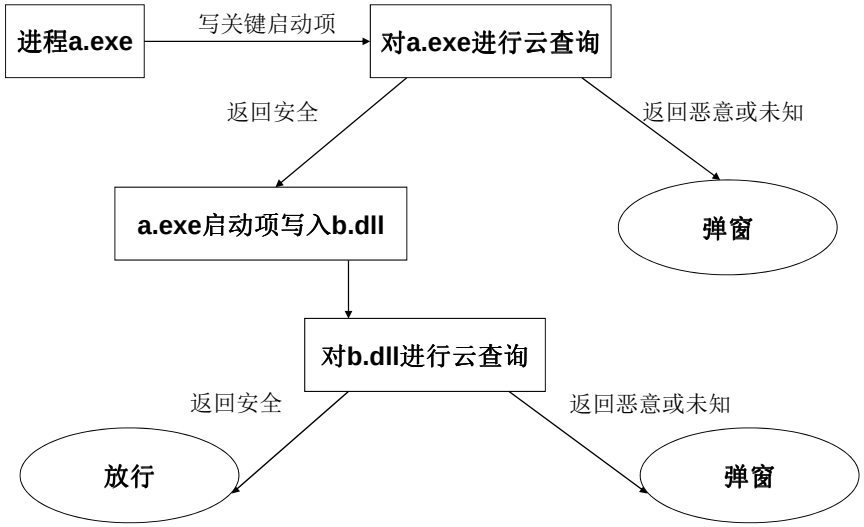

# 金山云防御-边界防御方案(3)




# 金山云防御-金山系统防御构成



# 金山云防御-全面基于云

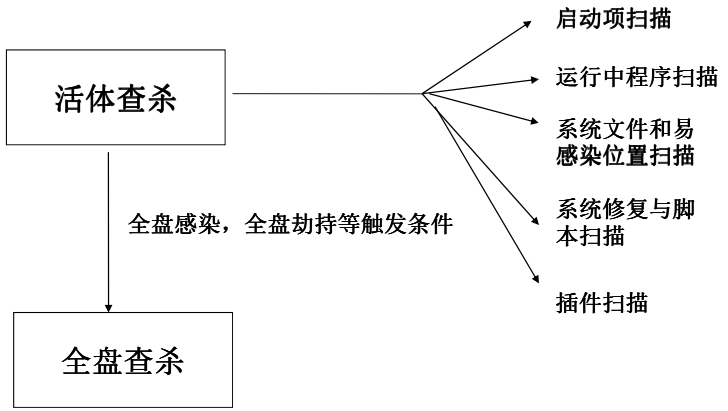



# 金山云查杀-反思查杀遇到的问题

- 为什么每次扫描要那么长时间
- 为什么要那么多种扫描:全盘扫描/快速扫描....
- 检出率为什么这么低

# 金山云查杀-解决方案


# 金山云查杀-一键云查杀



## 金山云查杀-一键云查杀特点

- 启动项非白即黑
- 系统文件替换
- 未知文件99秒云鉴定
- 云特征扫描
- 系统云
- 专有团队保证活体查杀的鉴定

## 总结

- 金山云体系
  - -基于特征
  - -自主鉴定器
  - -产业链
- 金山云防御 - 边界防御
- 金山云查杀 - 一键云查杀