金山网络
www.ijinshan.com

云@金山 Cloud at KINGSOFT

--一种不同的思路做云安全

A different thought in cloud-based security

演讲人：CardMagic（孙明焱）
金山网络 KINGSOFT

Agenda

金山云体系

KINGSOFT cloud artitecture

金山云防御

KINGSOFT cloud defense

金山云查杀

KINGSOFT cloud-based anti-virus

关于演讲者 About the speaker…

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

current product director of KINGSOFT, who is responsible for the development of **“金山毒霸”**

-曾任奇虎360云查杀产品负责人

previous chief developer of Qihoo 360 Cloud-based anti-virus

-曾任Trend Micro技术经理

previous technology manager of Trend Micro

-曾任NEC开发工程师

precious programmer of NEC

-Antirootkit工具DarkSpy的作者(被趋势科技收购)

creator of DarkSpy,a tool of Antirootkit. (purchased by Trend)

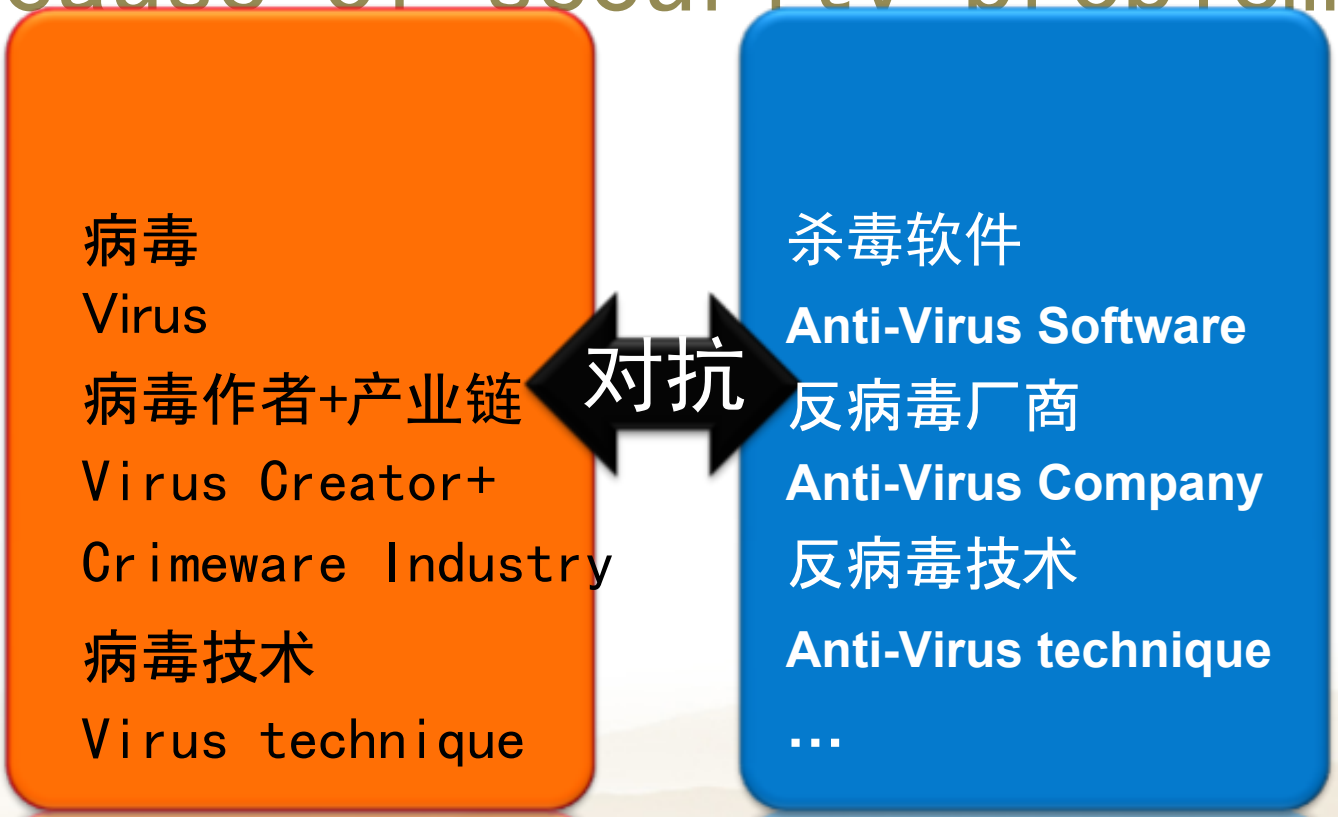
-精通各类安全开发，曾负责开发过各类云安全产品

specialize in various security development.

Develop abundant security products.

金山云体系-信息安全问题的源头

KINGSOFT cloud architecture - the cause of security problem



金山云体系-云端智能鉴定技术

KINGSOFT cloud architecture:

Cloud intelligence of Forensics

海量样本 Enormous Samples

样本相关信息 Information from Samples

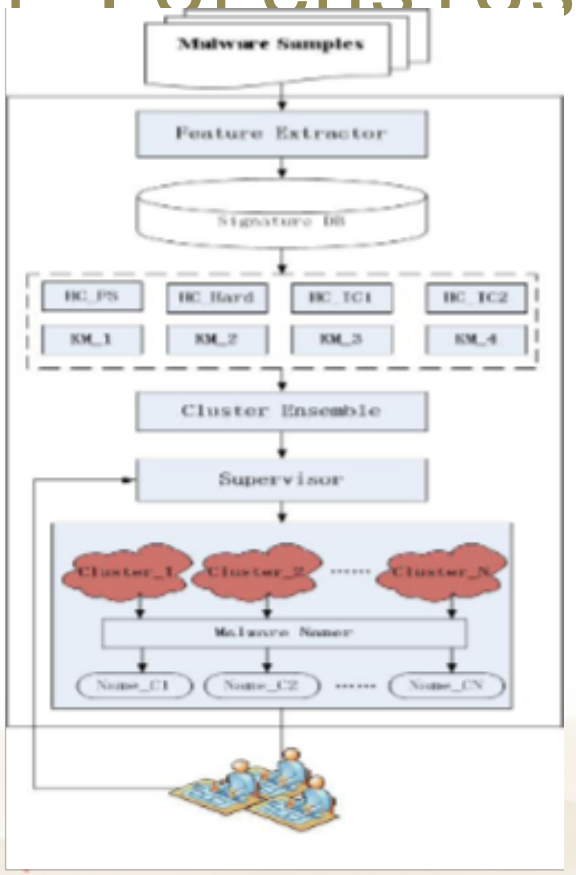
数据挖掘技术 Data Mining technique

10年病毒技术跟进

和积累的经验

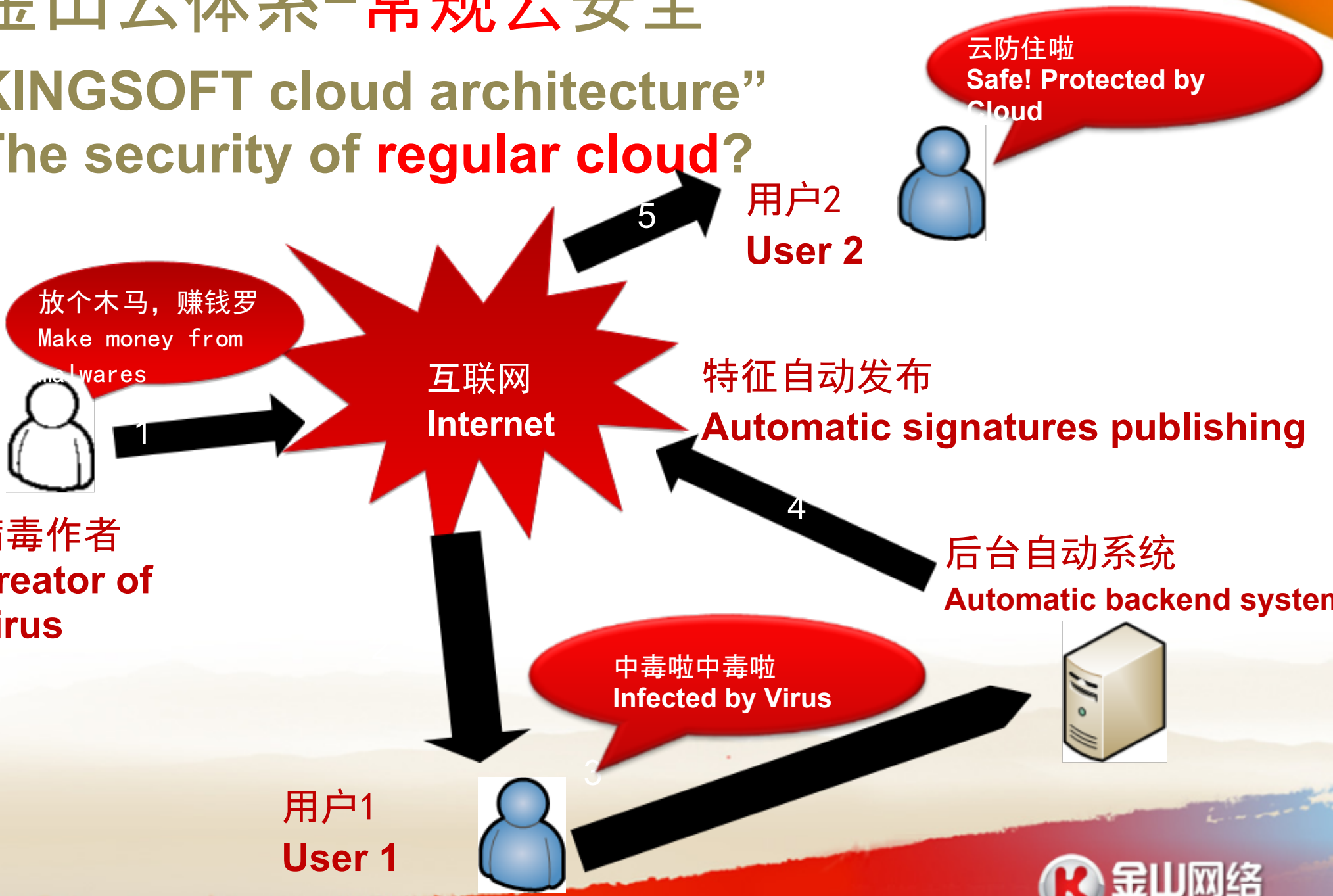
Ten-years knowledge of Virus technique

and accumulated experience.



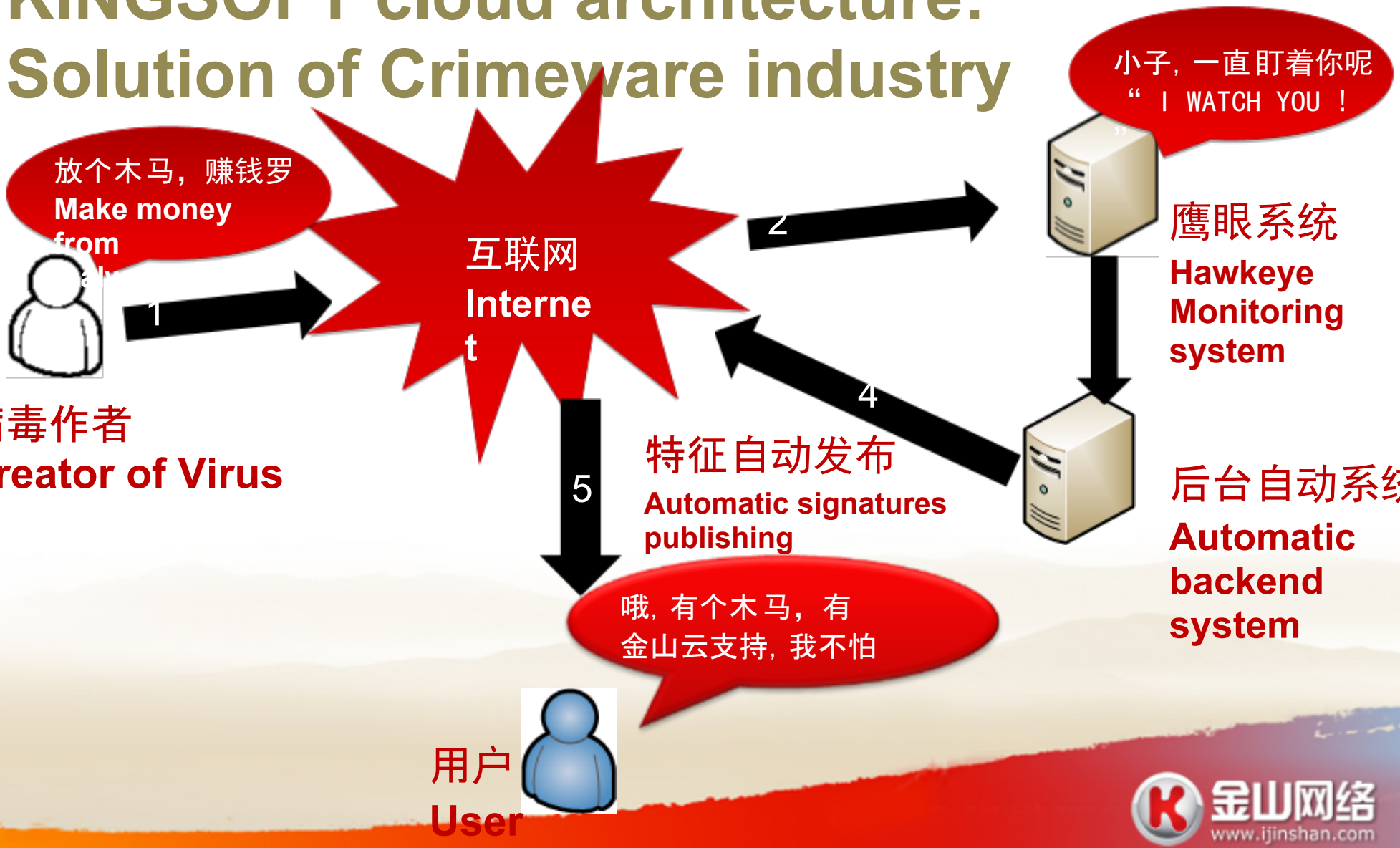
金山云体系–常规云安全

KINGSOFT cloud architecture”
The security of regular cloud?



金山云体系-黑色产业链解决(1)

KINGSOFT cloud architecture: Solution of Crimeware industry



金山云体系-黑色产业链解决(2)

KINGSOFT cloud architecture: Solution of Crimeware industry

- 为什么要产业链：

How does knowing crimeware industry assist us in Virus detection?

- 产业链做为直接鉴定器，鉴定文件与URL

The features of crimeware industry can be the direct verifier in checking files and URLs

- 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

Before a widespread infection, we can predict the possible distributed range based on individual crimware industry's behavior.

- 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

By clustering crimeware industries, the signatures of their behaviors become clear, which contributes to the unit test of virus

金山云体系–黑色产业链解决(3)

KINGSOFT cloud architecture: Solution of Crimeware industry

- 金山黑产业链积累：

KINGSOFT has accumulated years of knowledge in crimware industry.

- 独特的产业链归类系统

The unique industry classification system

- 产业链特征自动提取系统

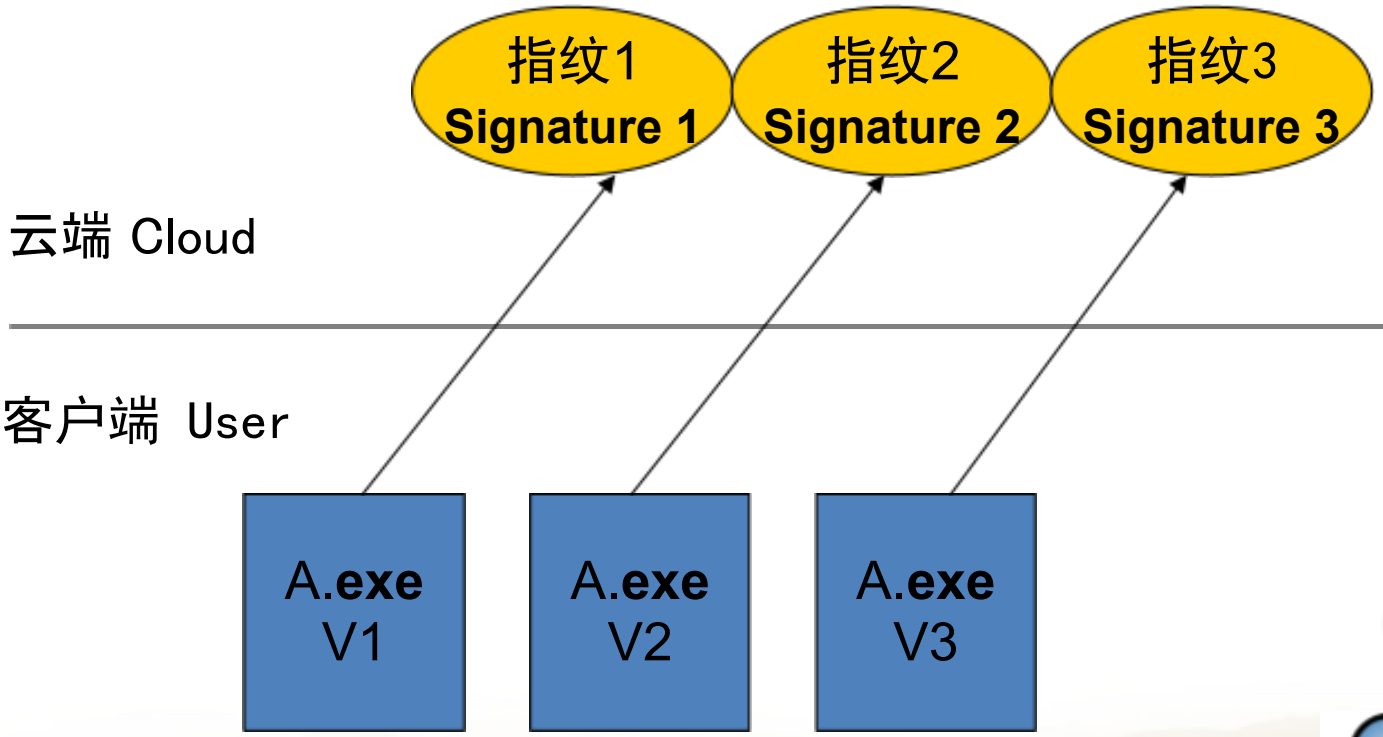
The automatic signatures extraction system

- 专门团队运营与监控

Specialized team in monitoring and maintaining

金山云体系–普通指纹云

KINGSOFT cloud architecture – Normal signatures cloud



后台快撑爆啦，
成本成本！！
Endless expansion with backend system due to the increasing data flow of signatures

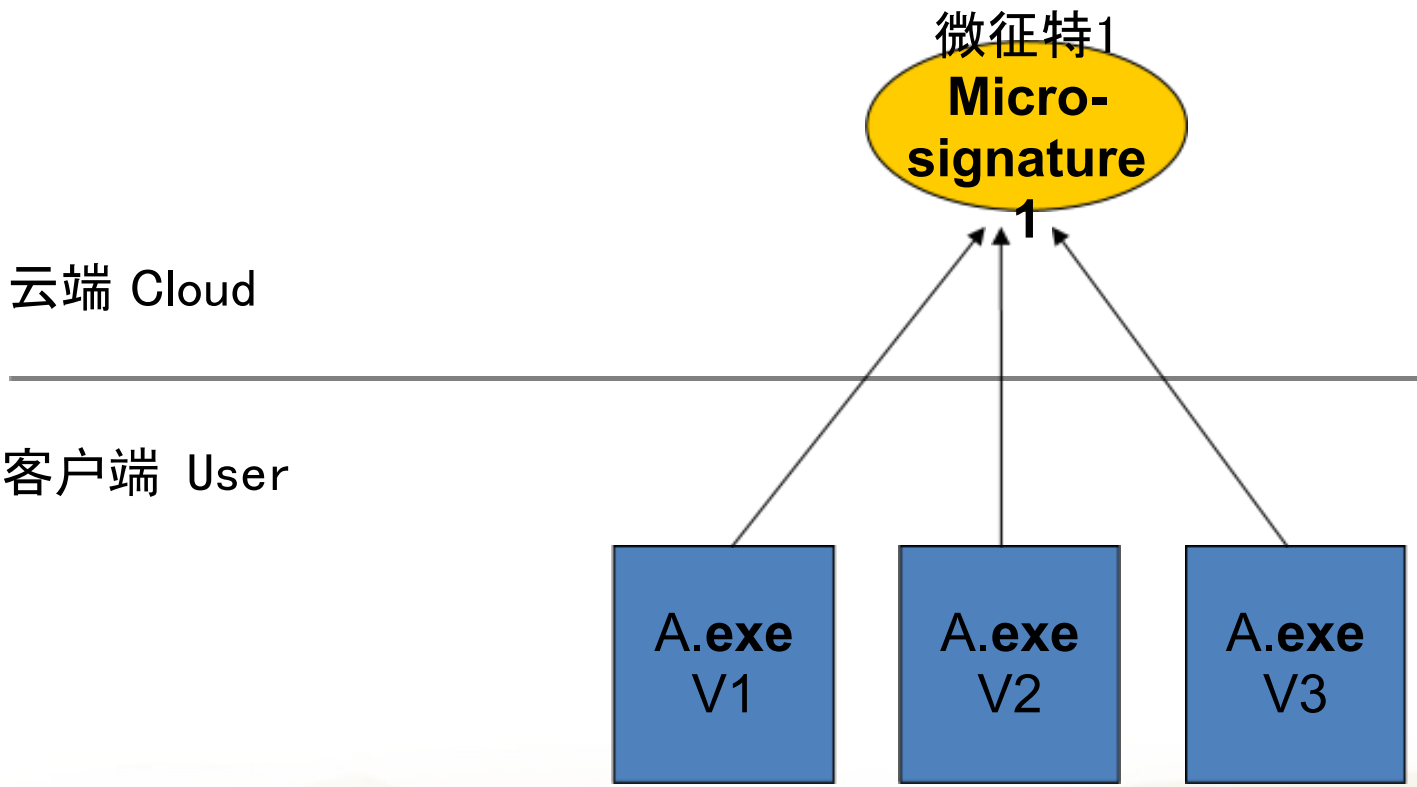
云安全从业者
Provider of Cloud Secutiry

软件又更新，又被误报了!!
Endless new versions of security software.
Misreport again!!

用户
User

金山云体系-金山微特征云

KINGSOFT cloud architecture – Micro-signature cloud



金山云体系–关于金山云体系的一些成果
KINGSOFT cloud architecture – Achievement

- 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

With the Hawkeye monitoring system and the accumulated knowledge in this field, we revealed top 10 crimeware groups in Mainland China.

- 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

KINGSOFT backend system owns more than 30 various forensic devices, containing all different kinds of intelligent forensic techniques.

- 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

Every day, KINGSOFT publishes approximate 300,000 signatures, which include 250,000 white signatures and 50,000 black

金山云防御 KINGSOFT cloud defense

□□□□

Defense at boundary

□□□□

Program execution

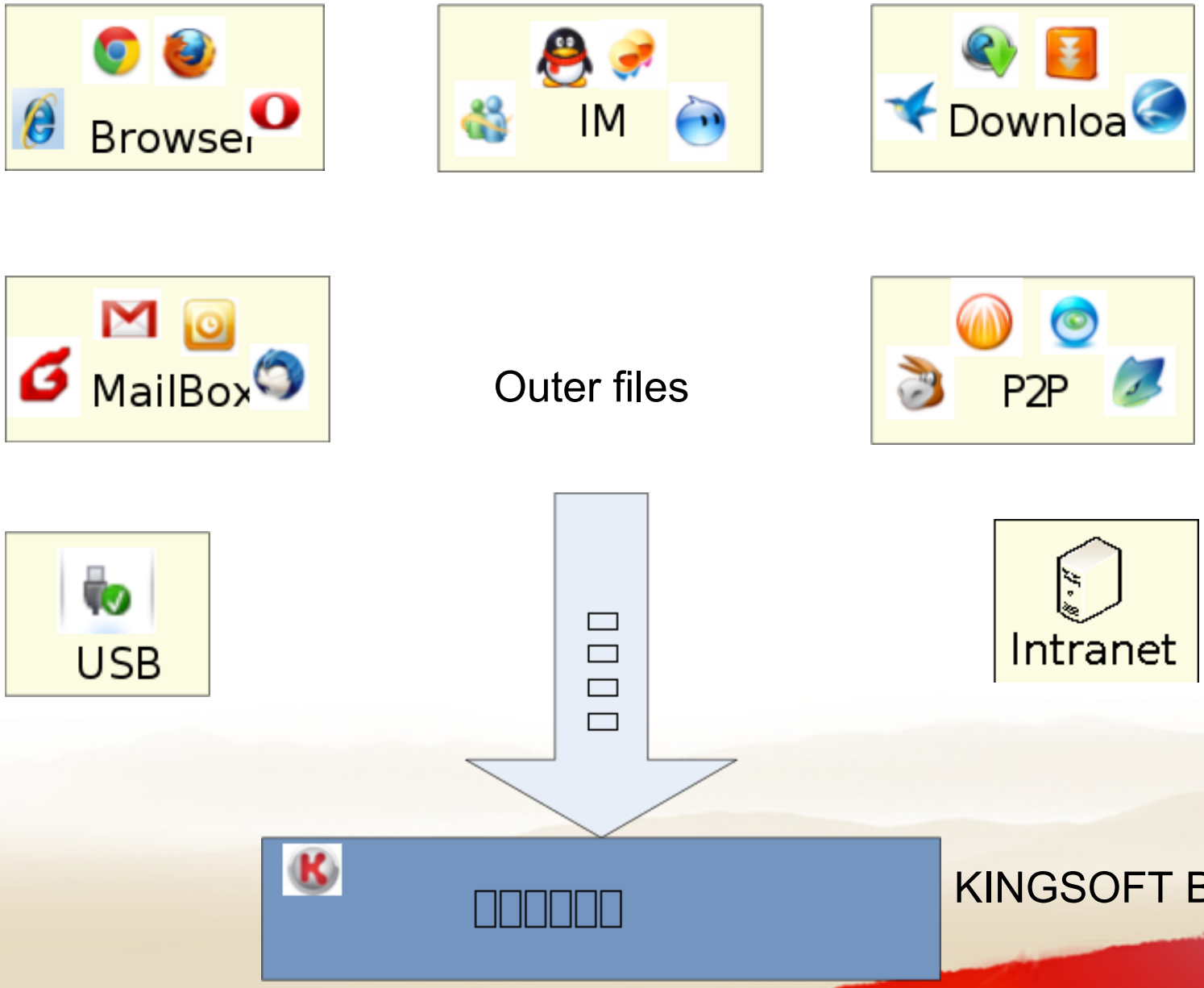
□□□□

System defense

金山网络
www.ijinshan.com

金山云防御-什么是边界防御

What is Boundary Defense?



金山云防御-为什么要边界防御(1)

Why is boundary defense needed?

- 传统主动防御的痛处 **The disadvantages of traditional active defense**
  - 病毒执行后行为变化方法太多
    Enormous unpredictable ways of virus behaviors once they have been executed.
  - 既需要应对文件变化，又需要应对行为变化
    It has to deal with either changes of files or changes in behaviors
  - 随着各种安全策略的增加，不断拖耗系统性能
    With the increasing numbers of security strategies, the efficiency of system decreases.
  - 兼容性不好 Low in compatibility
  - 驱动级更新对抗，稍有不慎便蓝屏崩溃
    A threat of bsod crash while dealing with kernel-mode rootkit
  - 进程执行时文件太多后台无法完全鉴定
    Too much files during processing for backend system to fully evaluate

金山云防御-为什么要边界防御(2)

Why is boundary defense needed?

- 边界防御的优势 The advantages of boundary defense
  - 只做文件对抗

    Only the file scanning is needed.
  - 只有极少情况会触发边界防御逻辑

    Only few circumstances will trigger the logics of boundary defense
  - 轻量级高兼容性实现

    Lightweight and high compatibility
  - 不用根据病毒的行为变化不停改变

    Doesn't need to alter with different kinds of virus behaviors

金山云防御-为什么要边界防御(3)

Why is boundary defense needed?

- 边界防御可行么 Does boundary defense really work?

- 每日边界防御的新增文件数量是有限的（可运营）

  The increasing numbers of files of everyday boundary defense is limited. (Sustainable)

- 边界防御中遇到的威胁是容易定性的（可做解决方案）

  The threats boundary defense system would encounter are easily identifiable. (Can be solved by specialized solution package)

金山云防御-边界防御 V.S. 下载保护(1)

KINGSOFT cloud defense:
Boundary Defense V.S. On-download file scanning

- 最本质的区别 The essential distinction
  - 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。

    Boundary defense is a comprehensive solution to prevent malware from entering systems.
  - 下载保护只是一个具体的产品功能

    On-download file scanning is merely a specific product function.

金山云防御-边界防御 V.S. 下载保护(2)

KINGSOFT cloud defense:

Boundary Defense V.S. On-download file scanning

To illustrate their differences as follows:

- 边界防御是全面的，不光包含下载，并且会不断覆盖新渠道

  Boundary defense is comprehensive. Despites download checking, it covers attack paths continuously.

- 投入精英和最优资源参与边界防御

  Boundary defense has intelligent working members and also the best resources participating in development.

- 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

  Boundary defense has dedicated and comprehensive solution packages to different kinds of files with specialized development teams.

- 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

  We have specialized teams and progress to deal with suspicious files, including identifying black or white, and also detecting pornography distribution.

- 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

  Due to the profound understanding of boundary defense, we keep focusing on new trends in boundary defense security, and developing different solutions.

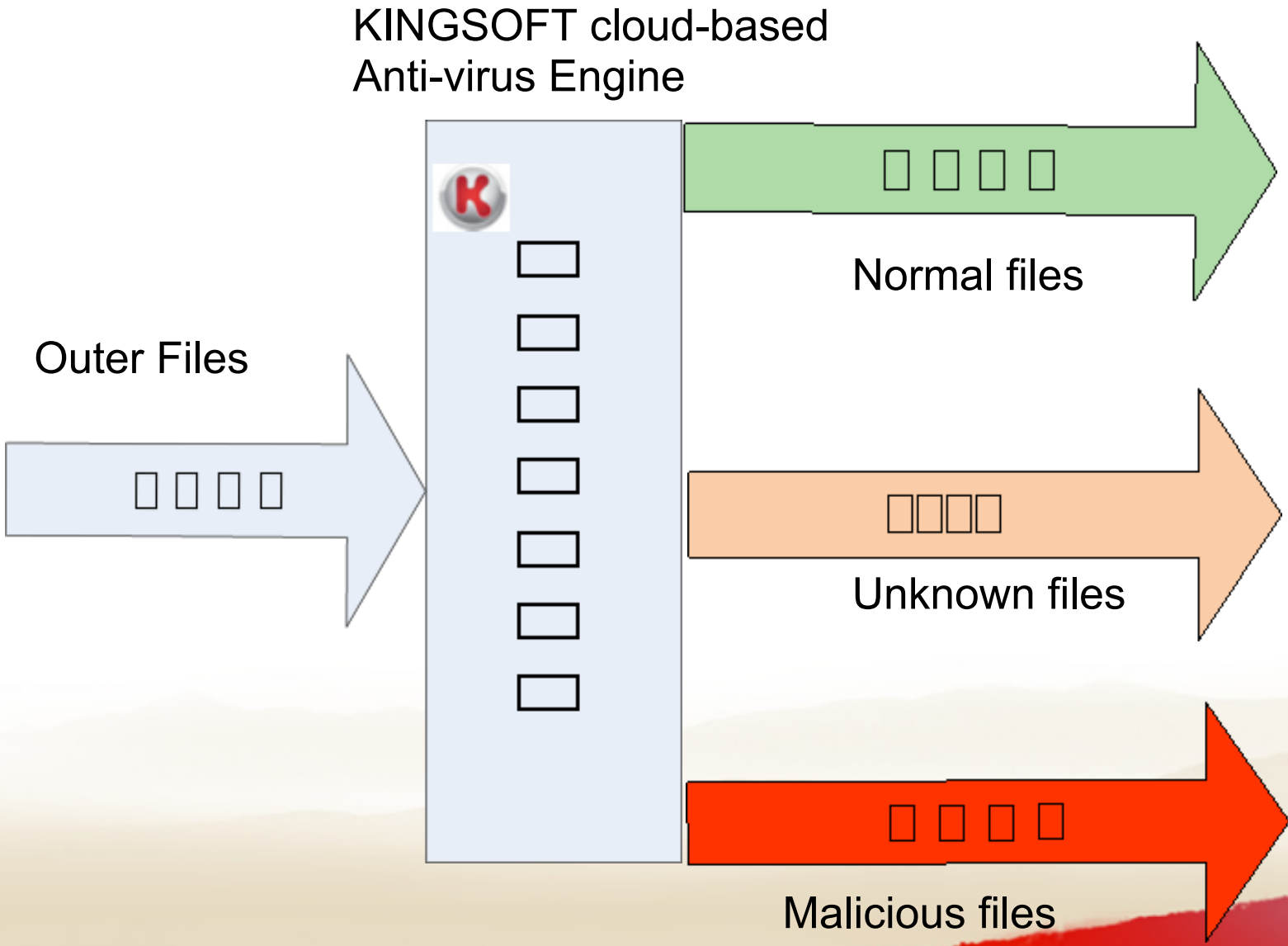
金山云防御-金山边界防御的优势和积累

KINGSOFT cloud defense: The advantages we acquire

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
  Based on the signature cloud, we promise a converging numbers of signatures.
- 后台30多种自主开发鉴定器（各种启发式以及专项鉴定）We have more than 30 different kinds of self-developed heuristic and special domain verifier.(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
  We have long experience in developing verifier and recruiting talented analyzing members.
- 从上到下对边界防御的深刻认识
  A profound and comprehensive knowledge of boundary defense.

金山云防御–边界防御方案(1)



金山云防御–边界防御方案(2)

KINGSOFT cloud defense: Boundary defense solution (2)

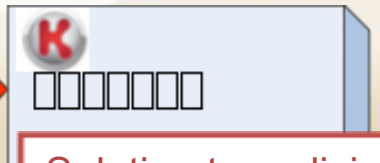
Normal Files

We identify this file to be safe!

UnknownFiles

Your file needs to go through an advanced analysis.

Malicious Files



Solution to malicious files.

金山网络
www.ijinshan.com

金山云防御-边界防御方案(3)

Boundary defense solution (3)

Malicious files

Pornography player

Plug-in

KeyGe rebo ok..

Others

This player contains virus!
You can choose from…
1. To see the film in a safe mode.
2. Remove this file immediately.

此播放器含有病毒

用金山安全看片模式运行此播放器，可有效防止病毒侵害。

安全看片　立即清除　确 定

金山毒霸 - 下载保护

Malware detected!
Suggestion: Remove now!

立即清除

安全沙箱

Safety Sandbox

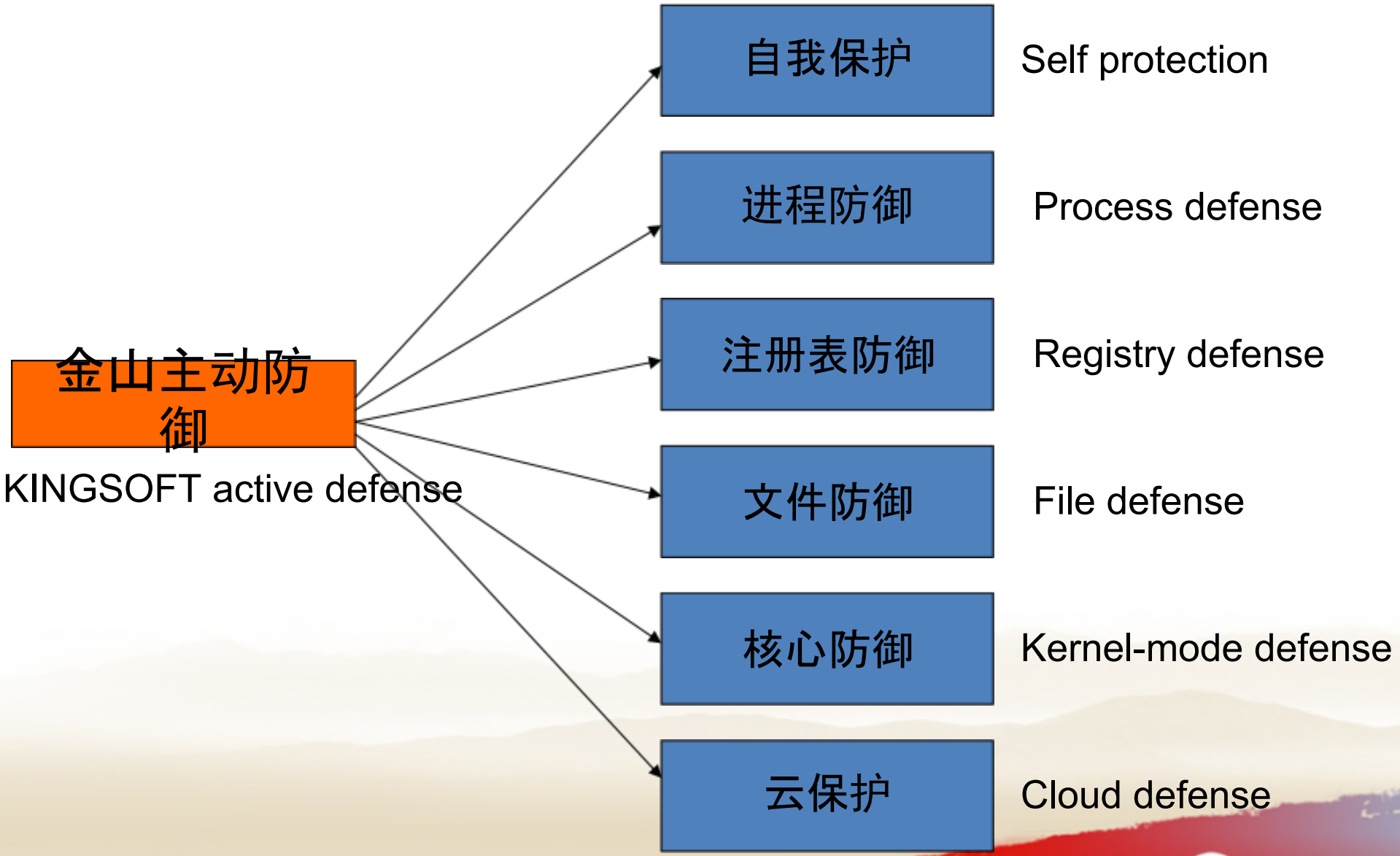
金山毒霸-聊天安全保护

您传送的文件有病毒，已被清除

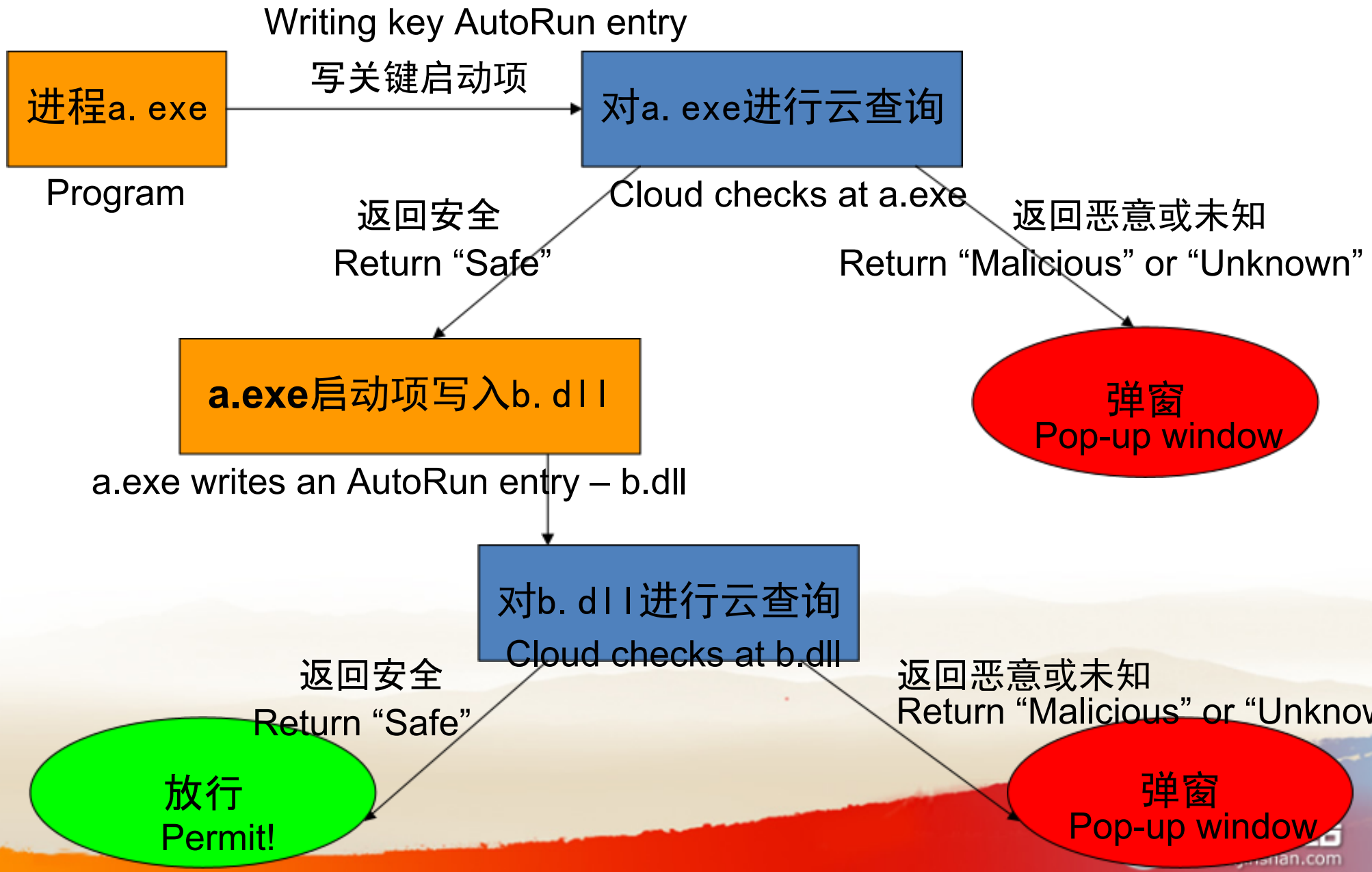
Your file is infected and being removed

金山云防御-金山系统防御构成

KINGSOFT cloud defense: Assembling



金山云防御-全面基于云 Based cloud



金山云查杀-反思查杀遇到的问题

The problems encountered in Anti-virus

- 为什么每次扫描要那么长时间

  Why does it take like forever In every scanning?

- 为什么要那么多种扫描:全盘扫描/快速扫描....

  Why do we need so many scanning methods: “Full Scan” / ” Quick Scan” …?

- 检出率为什么这么低

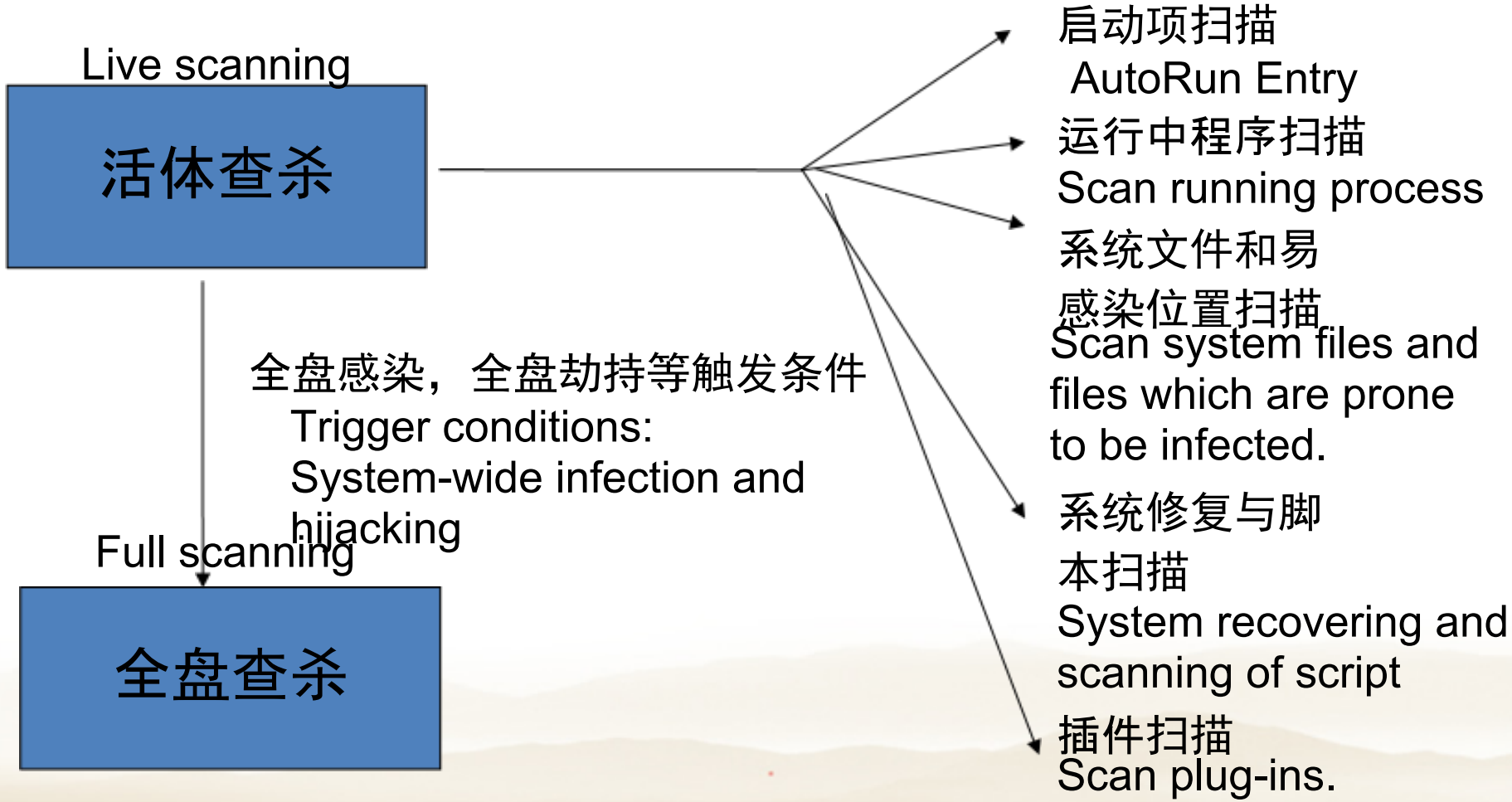
  Why is the detection rate so low?

金山云查杀-解决方案 KINGSOFT Solution

一键云查杀

One-click cloud-based Anti-virus

金山云查杀--一键云查杀 One-click cloud-based Anti-virus



金山云查杀--一键云查杀特点

Characteristics of One-click cloud-based Anti-virus

- 启动项非白即黑

No ambiguity in AutoRun entries – they are either white or black.

- 系统文件替换

  To substitute the infected system files

- 未知文件99秒云鉴定

99 seconds in unknown file verification

- 云特征扫描

Scan with the signatures provided by cloud

- 系统云

Systematic cloud

- 专有团队保证活体查杀的鉴定

总结 Conclusion

- 金山云体系 KINGSOFT cloud architecture
  - -基于特征 Based on signatures
  - -自主鉴定器 Automatic forensic device
  - -产业链 Crimeware Industry

- 金山云防御 – 边界防御

KINGSOFT cloud defense – Boundary defense

- 金山云查杀 – 一键云查杀

KINGSOFT cloud-based Anti-virus : One-click cloud-based Anti-Virus

Thank you for your participation!

与中国的软件产业共同进步！