金山 KingCloud 企业云安全系统

技术白皮书 V1.2

版权声明

目　录

一、背景介绍

随着分布式网络与虚拟化技术的快速发展，今天的互联网正变得愈发的智能和开放，发达的网络使得企业员工、客户以及合作伙伴之间可以实时共享海量的信息与数据，基于云的协作模式已成为企业与政府机构提升信息化建设的重要手段。然而，海量的信息和便捷的获取渠道却同样给攻击者提供了便利，无论是层出不穷的恶意软件，还是快速更新的新应用，甚至是云计算技术本身，与关键信息数据有关一切都可能成为攻击者窥视的猎物。面对巨大的经济利益，如今的攻击者已将攻击目标锁定在更小更精确的范围，近期被不断披露的 APT 攻击事件，不仅让知名的 IT 厂商瞬间崩塌，骇人听闻的 Stuxnet 攻击更让一个国家核基础设施面临被破坏的危险。

作为全球网民数量最多的国家，IT 应用透到国民生活的各个方面，国家对于企事业单位重要信息系统的安全防护要求愈发严格，随着“等级保护”、“分级保护”、“企业内控”等相关法规与政策的相继颁布，特别是涉及国计民生的央企和政府各级机关对于实施知识产权和涉密信息的保护需求变得十分迫切。打破网络运维和安全防护的界限，构建自主可控的智能安全防御体系，实时监测、发现、清除、恢复、审计信息所存在的各种隐患和异常，是新形势下实现关键信息系统安全稳定运营的重要前提。

1. 安全形势

传统的的信息安全始终始终围绕着防火墙、防病毒、加解密开展，然而随着商业化的安全技术与服务模式的快速发展，对于高性能的安全网关和全网复合安全解决方案的需求逐步替代终端安全解决方案成为用户安全建设的首选。然而随着 2009 年电子商务、网络游戏、电子政府等基于 WEB 的业务模式的快速发展，利益的趋势让等以取用户敏感数据为终极目的的木马间谍软件等恶意软件数量呈现井喷之势。

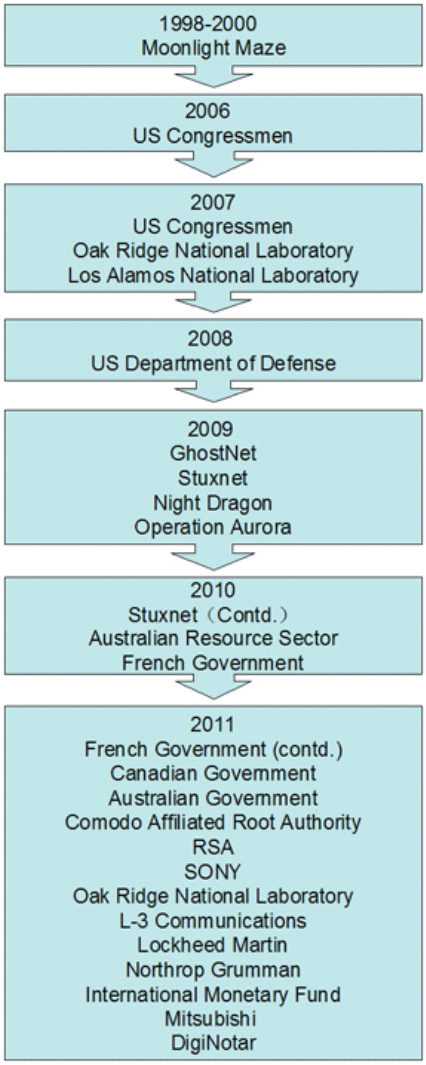
大量的木马、间谍软件、后门程序的出现主要得益于自动化工具的大量出现，同时另外一种更加隐蔽的攻击行为也整悄悄崭露头角，这就是今天已引起国家和企业高度关注的 APT 高级持续性威胁攻击。截止 2011 年 10 月， APT 攻击已在全球多个国家的政府和企业内部发生，造成的损失难以预估，其中荷兰知名的数字证书提供商 DigiNotar 更是因为 APT 攻击而宣布破产。究其原因，APT 攻击的发生很大程度上由于忽视了安全体系建设中最基础和最看似无害的部分，越来越多的案例证明引发 APT 攻击的最致命短板正是企业 IT 管理员最

熟悉的信息终端以及其上运行的各种应用。金山安全软件有限公司最先的数据显示，新增应用程序中，超过 70%包含恶意代码。业界对于构建可信可控的智能终端安全管理体系的呼声愈发强烈。

2. 企业现状

数量越来越多的 PC 终端和应用的增加，传统的反病毒及终端安全解决方案已无法满足企业终端安全需求，日益增加的 0day 漏洞随时可能让企业信息终端成为攻击发起的源头。别是对于诸如 APT 攻击的定向攻击行为，因为其具有极高的隐蔽性和目的性，传统的终端安全解决方案几乎无法检测，企业亟需更加智能，更具有可管理和可审计功能的私有云安全平台。当前企业所面临的挑战：

- 97%的企业部署了反病毒解决方案，但其中仍有 67%的企业发生过恶意软件攻击事件；
- 部署了传统的反病毒解决方案的企业，实际安全防护效果差强人意，超过 50%的受访者认为恶意软件仍是信息安全投资的最重要驱动因素；
- 超过 94%的企业，企业内部员工经常登陆各类社交网站；
- 传统的反病毒解决方案只能识别 19%的 Web2.0 攻击行为；
- 只有 39%的安全专家相信黑名单技术可以有效抵御安全攻击；
- 超过 30%的最新恶意攻击行为不能被当前传统反病毒解决方案所阻断。



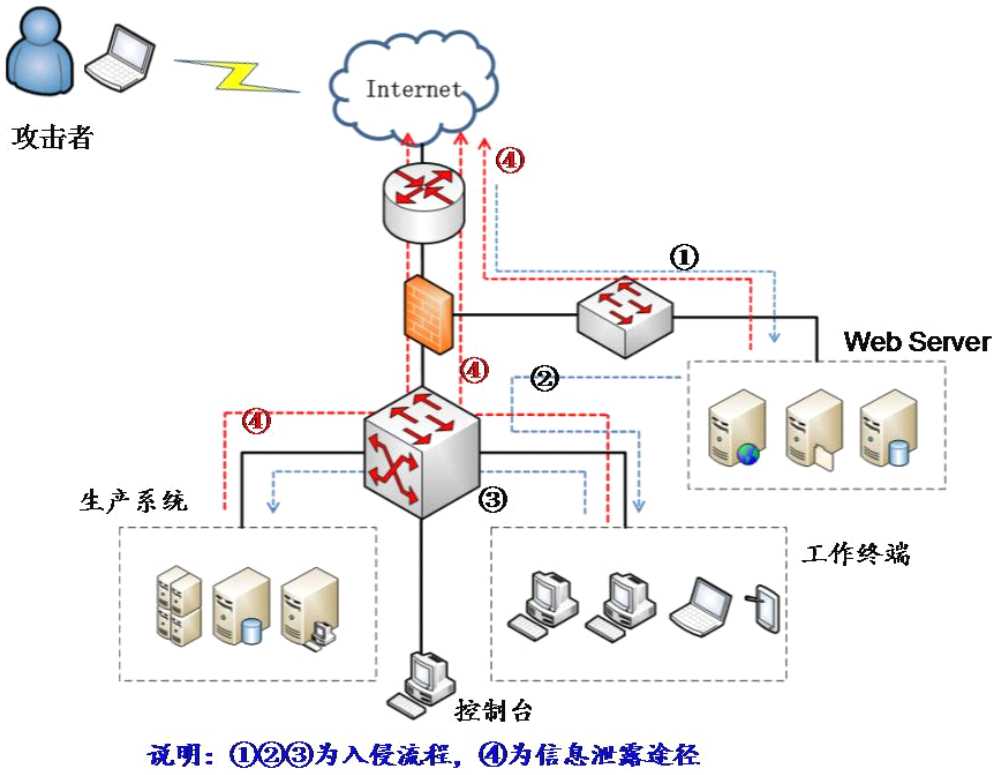
APT攻击事件表

3. APT 攻击

APT（Advanced Persistent Threat）高级持续性威胁，这种攻击行为具有极强的隐蔽能力，通常是利用企业或机构网络中受信的应用程序漏洞来形成攻击者所需 C&C 网络；APT 攻击具有很强的针对性，攻击触发之前针对攻击目标收集大量关于业务流程和目标系统使用

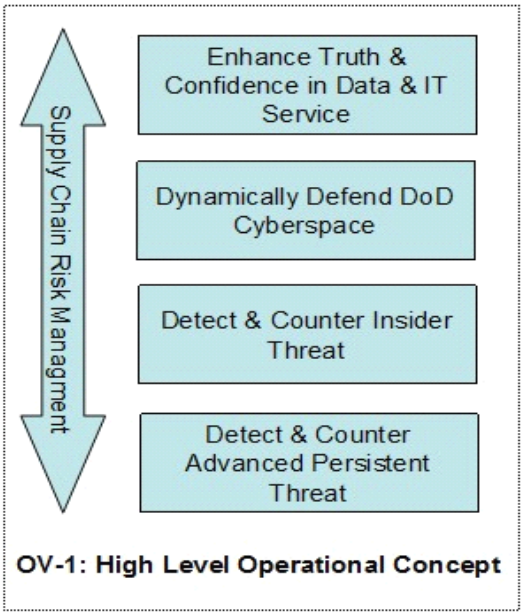
情况等信息；APT 攻击是各种社会工程学攻击与各类 0day 利用的综合体。

在已经发生的典型的 APT 攻击中，攻击者经常会针对性的进行为期几个月甚至更长时间的潜心准备，熟悉用户网络坏境，搜集应用程序与业务流程中的安全隐患，定位关键信息的存储位置与通信方式。例如，在某台服务器端成功部署 Rootkit 后，攻击者便会通过精心构造的 C&C 网络定期回送目标文件进行审查。



典型的 APT 攻击流程

目前，西方先进国家已将 APT 攻击定位国家网络安全防御战略的重要环节。例如，美国国防部的 High Level 网络作战原则中，明确指出针对 APT 攻击行为的检测与防御是整个风险管理链条中至关重要也是最基础的组成部分。



4. 云安全革命

云安全应用的不断发展正逐步改善客户端的压力，过去百兆以上的客户端负载，

如今通过精确的云收集、特征云查询、智能云鉴定、辅助恶意软件库技术手段，成功的被精简到只有 10M 左右的轻客户端。过去终端安全防御赖以生存的本地脱壳、启发式扫描、虚拟机、主动防御、自我保护、驱动对抗等安全防御功能，现在可以通过迁移到高性能的云计算平台来帮助用户更快的应对威胁。而对于企业而言，构建私有云安全运维平台，不仅可以实现服务的按需定制，更可以领先一步相应企业可能存在风险，提供给用户可自管理、自约束、自服务的高性能云安全体验。

5. 私有云安全技术体系

私有云安全体系是由云服务端和客户端共同组成的高性能安全协作运维平台。客户端可实时像云端申请所需安全服务，例如未知文件的属性鉴定、未知应用的行为鉴定以及用户访问 URL 的安全性鉴定，高速的云计算平台可以在毫秒级实现查询结果的客户端同步，进而确保用户系统终端的安全稳定运行，既有效解决了传统终端解决方案“占资源”、“耗流量”的问题，也可以更快的定位和发现各种潜在的威胁。

高性能的云安全运维平台，还可以快速的拓展各种功能和运算资源，实现过去传统网管软件无法有效抵御安全攻击行为，终端安全解决方案无法实现有效网络与设备管理的尴尬，开放的 API 接口和模块化的平台架构，确保了私有云安全平台，可以快速安全用户的需求部署运营功能更加丰富的解决方案。

目前国内知名的互联网安全解决方案与服务提供商金山安全软件有限公司，通过多年公共云安全平台的技术和运维经验积累，实现了高性能、高可用性、高安全体验的金 山 KingCloud 私有云安全解决方案，实现了企业网络运维的监控、保护、审计的多重安全需求。

6. 企业云安全需求

1) 安全有效的终端系统关键位置保护，有效抵御各种恶意软件攻击；
2) 完善的企业 IT 生产环境基线，确保企业 IT 生产环境的稳定运营；
3) 精确的文件安全鉴定服务，确保企业 IT 管理者灵活的制定各种策略；
4) 实时 IT 生产环境监控，可实时识别并发现终端异常行为，确保网络稳定运营；
5) 完备的系统文件访问控制策略，确保核心数据的安全受控，防止文件外泄；
6) 快速有效的恶意攻击事件应急响应；
7) 快速准确定位各种攻击事件，完善的事件审计日志与取证机制。

二、金山 KingCloud 私有云安全解决方案

面对愈发严峻的信息安全风险，企业 IT 管理者需要在企业内部实施更加智能的 IT 终端运维安全解决方案，通过高性能的云安全运维平台，实现企业网络运行环境的可控、可信、可视、可审计、可回溯，真正实现企业 IT 管理者对网络环境的自主掌控。为了满足企业迫切的终端安全智能安全解决方案的需求，本文将阐述金山 KingCloud 私有云安全系统，通过为企业构建开放式的私有云安全运维平台，为企业提供高性能、高可靠、高可管理、可审计的全新终端安全运维体验。

1、金山 KingCloud 企业云安全系统的介绍

金山 KingCloud 私有云安全系统，是北京金山安全软件公司经过深度分析企业用户需求后，依托多年云安全技术与经验积累打造全新的基于私有云平台的终端安全解决方案，着重实时掌控企业 IT 生产环境变化，应对企业复杂的终端安全需求。丰富的终端运维经验能够帮助 IT 运维管理人员构建满足企业运维需求的终端安全基线，实现干净可用的初始化环境，简单方便的网络环境检测过程，无需管理员干预即可掌握整个网络应用环境，一旦确认应用类型即可下发灵活的权限控制策略，极大降低了管理员的管理门槛。

多种终端安全管理功能选择

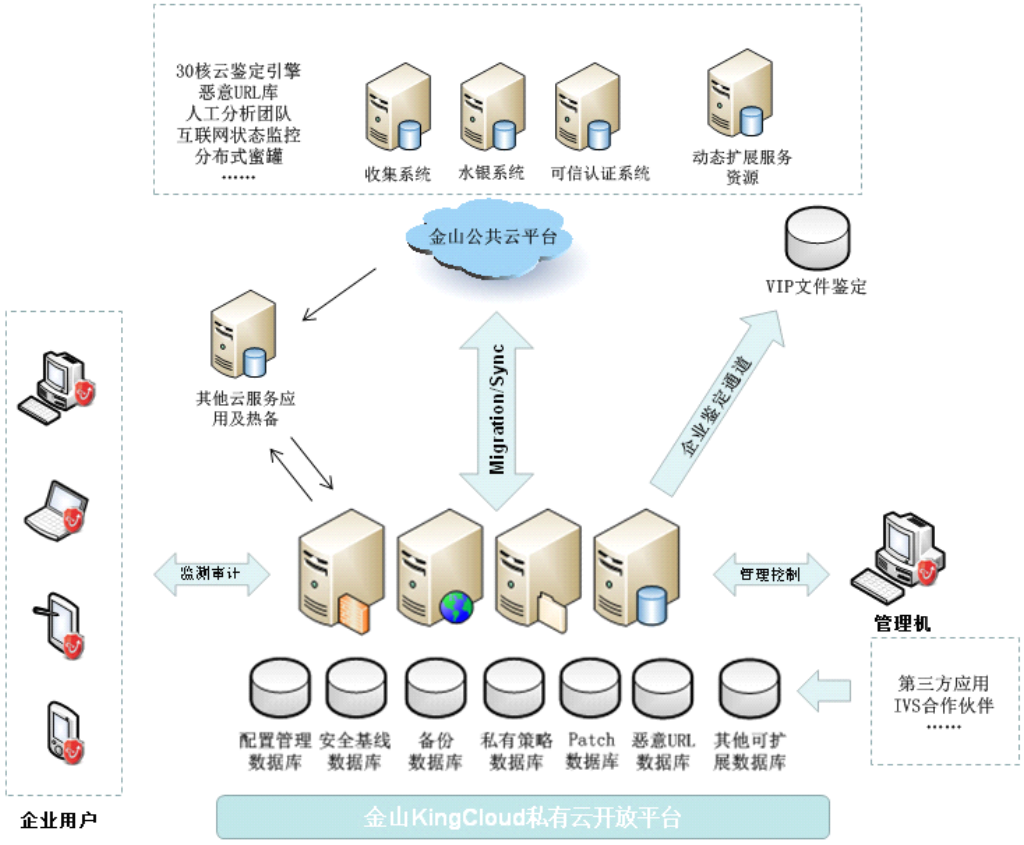
作为新一代企业 IT 运维级安全解决方案，金山私有云充分考虑终端资源滥用问题，细粒度的应用控制策略和低于 10M 的内存资源占用，确保了在现有的 IT 环境中最大限度的优化终端系统可用性。强大的云防御功能可以精确抵御各种非授权行为对网络的破坏，管理员可根据用户业务类型严格限定用户的访问权限和文件操作权限，无论是企业文件服务器、终

端工作站、瘦客户端、移动 PC 或者智能终端，金山 KingCloud 私有云安全系统都可发挥极佳的安全防御效果。

金山 KingCloud 私有云安安全理念

强大的云监测、云修复和云防御等诸多特点，除了能通过私有云平台来检测并抵御各种恶意软件威胁，还能对被破坏的系统文件、浏览器设置、软件应用环境等关键位置进行修复。独有的云修复功能，可在企业内网终端发生异常宕机或蓝屏时，快速恢复系统初始状态，为企业 IT 信息系统的安全稳定运营提供强大的运维保障。业界领先的 APP 识别和最全的黑白名单库，强化了金山对未知应用和恶意行为的识别和检测率，将为企业用户提供无与伦比的 0day 威胁检测和响应能力。领先的金山云安全平台，还能够满足跨国跨区域客户终端集中管理的需求。

值得注意金山 KingCloud 私有云可以帮助 IT 管理者实时掌控企业 IT 生产环境点滴变化，无论是受信软件还是未知应用，甚至系统内存、CPU 资源调用情况，企业生产环境关键位置所产生的任意微小变化都将第一时间上报企业 IT 管理。完善的白名单技术和基于云的主动防御技术，让绝大多数可疑攻击行为都逃不脱金山私有云安全平台的掌控，管理员只需针对恶意行为或文件进行统一策略下发，便可瞬间切断隐藏在企业机构背后的黑手。



金山网络的“云安全”体系结构

KingCloud 将互联网上成熟的云安全服务应用到企业内部，通过私有云平台为企业提供灵活可管理的安全保障，经验丰富的金山技术工程师配合人性化的服务模式，将为企业 IT 应用打造专属的安全基线和定制化功能开发。

➢ **稳定高效的智能客户端**

KingCloud 私有云系统客户端是金山安全软件多年云安全运维经验的革命，客户端系统具体执行对目标文件或网址做出正确的响应，这套客户端系统集成了包括金山毒霸、金山卫士、金山急救箱等诸多产品优势，以及面向第三方合作伙伴的开放 API 接口，满足顾客个性化的安全需求。

客户端同时具有样本收集功能，在庞大的云安全数据库支持下采用对应防杀策略：

◆ 白加黑双重诊断，快速识别在系统敏感位置出现的可疑文件；

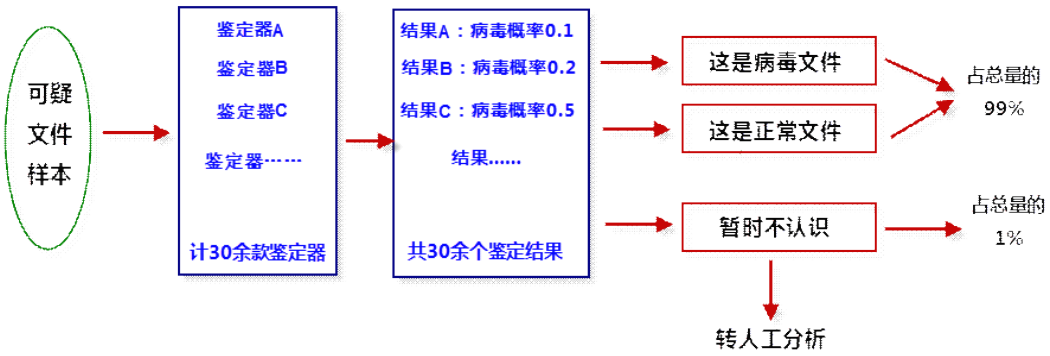
◆ 对外部环境进入电脑的可疑文件采用非白即黑或受限运行等防御策略进行拦截或清除。

➢ **完善智能的私有云服务端**

金山 KingCloud 私有云服务端，包括分布式的可疑文件收集中心、云安全防御中心、文件云鉴定器、安全基线受信文件中心、海量数据存储中心、安全趋势智能分析中心等多个模

块，高安全需求的用户还可以享受金山专业的安全分析服务与应急响应，配合客户端严格的安全策略，可为用户提供高质量的云安全服务。

自 2006 年至今，金山已独立开发使用的 30 余款云鉴定器，相当于不同的病毒分析方法，涵盖了启发式分析、虚拟机、沙箱技术、主动防御技术等多种复杂的识别引擎。依赖云端服务器的强大性能和分布式计算能力，云鉴定很快就可以得出结论：90%的文件在金山毒霸云安全系统中鉴定完毕仅需 30 秒。



金山云安全服务器样本综合鉴定系统

金山 KingCloud 私有云特有的云端安全基线是目前国内最大最全面的企业级终端运维基线策略，目前已收录基线各种策略规则 30 余万条，可帮助管理员精确管控企业内部各类应用。

2、金山 KingCloud 客户端主要功能

金山私有云客户端

1. 极速云扫描

金山 KingCloud 私有云系统严格监控企业办公 PC 的敏感区域，特别是容易引起病毒感染的 WINDOWS 系统文件夹、可执行程序，以及产生的非法恶意修改行为，KingCloud 私有云云检测模块均可快速识别并清除病毒木马等恶意攻击行为，优化的扫描规则实现了在不影响用户正常工作体验的同时，极速清除潜在的安全威胁，通常扫描时间小于一分钟。

2. 细粒度云扫描

金山 KingCloud 私有云系统提供了针对工作环境 PC 的完整磁盘扫描防护，对于顽固病毒、间谍软件、后门程序等恶意代码提供全面的安全解决方案，彻底清除隐藏在系统内部的黑手。此模式将对 IT 生产环境中终端系统进行全部文件逐一过滤扫描，彻底清除非法侵入并驻留系统的全部恶意代码。

3. 自定义云扫描

对于任意由金山 KingCloud 私有云平台文件鉴定器发现的各种可疑行为，自定义云扫描将给用户提供全面的文件分析鉴定，帮助管理员快速发现各种潜在的威胁，特别是对于针对性木马、后门等恶意程序，以及潜伏的 C&C 命令网络具有良好的检测效果。管理员可以根据需求制定任意个区域。

4. **移动介质云扫描**

采用高启发算法，可以发现绝大多数利用 U 盘等移动介质传播的病毒木马等恶意软件，并可完美修复由恶意代码造成的移动介质内的文件破坏。Stuxnet 震网蠕虫的传播正是借助 U 盘等移动介质发起 APT 攻击。

5. **快速系统修复**

系统修复引擎可修复由恶意软件破坏的系统文件，确保 IT 生产环境终端快速恢复，维护系统安全稳定运营。

6. **强大的实时保护**

- 边界防御：

  边界防御是一种效果好、占用资源低的新型防御方式。防御点前移至恶意攻击代码进入系统的入口，拦截时机更早，病毒更难对抗。边界防御主要防御点有：防黑墙、上网安全保护、即时聊天安全保护、视频播放安全保护、网络下载保护、U 盘实时保护等。

- 系统防御：

  金山 KingCloud 私有云系统全面集成新一代云主动防御技术——全新 K+(铠甲)防御技术，独创对流行病毒样本的广谱防御能力，内含启发式规则和多点继承判断，全面对抗流行病毒样本手段。

7. **集成百宝箱功能**

百宝箱为您分类汇总了金山毒霸杀毒软件的全部功能，同时提供多款系统辅助工具，可以帮助您优化修复系统，操作简单，使用方便。

8. **漏洞扫描**

及时有效的修复系统、软件漏洞，可避免被黑客利用控制您的电脑窃取账号、密码等重要信息。

3、金山 KingCloud 云查杀服务器主要功能

金山 KingCloud 云服务端登录界面

金山 KingCloud 云服务端界面

1. 灵活的客户端分发

管理员可以根据企业网络环境采用 WEB 页面安装方式，在较短的时间内完成网络内大量客户端的安装，简单快速地实现整个网络反病毒体系的部署，最大限度贴合网络实际环

境。

2. 领先的云防御功能

1) 细粒度应用识别

金山 KingCloud 私有云系统可自动识别企业 IT 生产环境中存在的各种应用协议，管理员可通过可视化界面对已识别的应用进行自定义分类管理；

2) 安全基线

金山 KingCloud 私有云系统可根据企业业务需求，帮助用户指定满足业务需求的最佳安全基线，管理员可根据安全基线按需调节基线强度，简化终端运维管理，确保企业核心业务系统的绝对安全；

3) 详尽的文件审计

自动收集 IT 生产环境中存在的各种未知文件信息并记录云鉴定结果，为管理员优化 IT 生产环境提供详尽的数据支撑；

4) 灵活的策略管理

对于存在于 IT 生产环境中的各种黑、白、灰文件，管理员可根据企业业务需求自行设定基于文件的威胁管理策略，确保各种危险或非必要应用破坏 IT 生产环境的可用性，最大限度降低各种针对性攻击的触发途径。

5) 完备的终端安全策略

- **核心机**

顶级防御策略，严格限制客户机只运行安全基线内文件，其他文件一律禁止运行；

- **受限机**

高级防御策略，只允许客户机运行安全基线和云鉴结果为安全的文件，其他文件一律禁止运行；

- **审计机**

中级防御策略，自动清除用户自定义的威胁文件和文件审计中云鉴定为恶意软件的文件，其他文件放行；

- **公共机**

低级防御策略，具备传统杀毒的全部策略，客户机只清除文件审计中云鉴定为病毒的文件，其他文件一律放行。

6) 云安全策略设置

云安全计划

- 加入云安全计划，发现可疑文件后，自动查询金山云服务器获取最新的鉴定结果；
- 对于内网用户，发现可疑文件，可通过离线 VIP 鉴定渠道鉴定文件结果；

文件审计设置

- 自动将金山云鉴定为安全的文件移入安全基线
- 自动将金山云鉴定为威胁的文件移入威胁列表

3. 强大的云扫描

管理员可通过管理节点对全网或指定的客户机发出病毒木马等恶意软件扫描指令，有效遏止爆发式病毒传播，避免网络内病毒交叉与重复感染；自动检测多途径的恶意攻击源，实时监测各类恶意代码入侵特征，全方位体现恶意软件及威胁的实时防护。

4. 漏洞修复

针对病毒利用系统漏洞传播的新趋势，金山私有云率先采用了分布式的漏洞扫描及修复技术。管理员通过管理节点获取客户机主动智能上报的漏洞信息，再精确部署漏洞修复程序；其通过 Proxy（代理）下载修复程序的方式，极大地降低了网络对外带宽的占用。全网漏洞扫描及修复过程无需人工参与。

5. 客户机管理

支持管理员对所选客户机进行客户机信息查看、权限设置和无效节点清理等操作。

三、典型案例

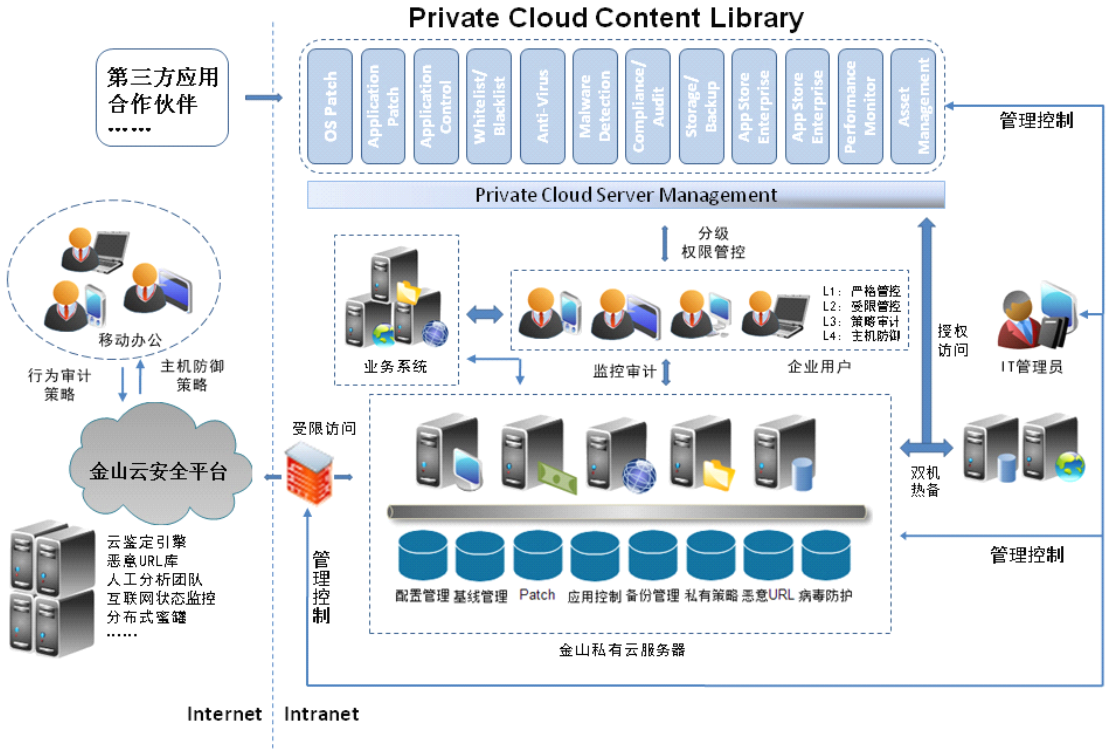
国内某大型跨国 IT 制造型企业，亟需引进成熟的私有云查杀解决方案，帮助企业建设基于云安全技术的私有恶意软件云查杀及未知定向攻击行为审计与溯源平台，实现企业 IT 运维部门自主可控的恶意软件查杀与审计服务，提高企业 IT 生产环境的可用性与终端安全防御能力。具体需求如下：

1. 提供黑白文件、网址特征查询，可疑木马样本上报等服务；

2. 维护私有特征库，查询、更新文件、网址特征记录，统计感染恶意软件信息；

3. 实现企业自建私有云办公平台的功能融合，实现精确的预警、查杀和文件审计功能；

4. 提供主动的未知攻击行为鉴定与防护解决方案，提高终端安全防御能力。



某跨国 IT 产品与技术提供商拓扑机构

通过部署金山 KingCloud 私有云安全系统，企业 IT 管理员可对总部与全球各分支机构进行实时统一的安全策略管理，确保了企业 IT 生产环境的稳定运营，显著提升了信息终端的可用性，实现了企业恶意软件检测、清除、审计、溯源的完整的安全运维体系，有效杜绝了企业关键信息系统的泄露途径。

四、服务支持

如果您希望了解更多关于金山 KingCloud 私有云安全系统的详细信息，请登录 www.ejinshan.net 或直接拨打我们的客服电话 4000339009。

北京金山安全软件有限公司

地址: 北京市海淀区小营西路 33 号金山软件大厦

电话：010-62927779

传真：010-59770977

Email: kcloud@ijinshan.com