360 终端杀毒

通用解决方案

北京朝阳区酒仙桥路 6 号院 2 号楼
电话：+86 10 5878 1000
传真：+86 10 5878 1001
邮编：100025

目　录

北京朝阳区酒仙桥路 6 号院 2 号楼
电话：+86 10 5878 1000
传真：+86 10 5878 1001
邮编：100025

北京朝阳区酒仙桥路 6 号院 2 号楼
电话：+86 10 5878 1000
传真：+86 10 5878 1001
邮编：100025

1 背景

自斯诺登事件曝光以来，网络和信息安全越来越受到国家的重视，新一届政府对国家网络和信息安全的重视程度也达到前所未有的高度，党的十八届三中全会设立了国家安全委员会，习近平总书记亲自挂帅新成立的中央网络安全和信息化领导小组，并一针见血地指出：没有网络安全就没有国家安全，没有信息化就没有现代化。

斯诺登事件余温尚在，美国国安局再次爆出泄密事件，最近某老牌国际品牌杀毒软件又被我国公安部认定存在“窃密后门”，这一连串的事件多了些耐人寻味意味外，更是为我国软硬件全面实现国产化替代夯实了决心。

当前，我国重点行业超过 70%的用户在建设 IT 系统和网络中，长期依赖国际品牌产品，使得很多核心业务暴露在非自主可控的计算环境中。2014 年 9 月，中国银监会、国家发改委、科技部和工信部四部门联合发布了《关于应用安全可控信息技术加强银行业网络安全和信息化建设的指导意见》（以下简称《意见》）。《意见》提出，将安全可控信息技术应用纳入战略规划，制定配套政策，建立推进平台，大力推广使用能够满足银行业信息安全需求，技术风险、外包风险和供应链风险可控的信息技术。

2 存在问题

随着计算机技术的不断发展，信息技术在企业网络中的运用更加广泛，信息安全问题也显得尤为迫切。自从 80 年代计算机病毒出现以来，已经有数万种病毒及其变种出现，给计算机安全和数据安全造成了极大的破坏。而传统防病毒产品在应对新的终端安全威胁时效果欠佳，因为病毒来自与不同的传播途径，例如邮件，网页浏览，U 盘的使用，高危程序的下载安装等多种途径，因此需要同时结合多种技术手段来综合的治理公司办公网所面临的安全问题，巩固办公网安全防线。

通过安装防病毒软件的方式抵御计算机病毒的攻击是增强公司办公网信息

安全行之有效的方法。随着公司办公网络的建成，在网络范围内任何终端中病毒后都可能会快速传播到全网。因此必须通过部署企业级网络版防病毒软件将病毒或木马及时阻截到尽可能小的范围内。通过建设终端安全防护系统，设计一套满足当前信息系统未来发展的防病毒体系：建立网络系统的运维管理规范、技术体系标准，优化办公网网络环境，减少病毒对员工的影响，提高员工的工作效率，为企业的快速发展提供保障。

随着公司内部办公网络及应用系统的不断完善，病毒的日益泛滥为企业的内部数据、重要资料乃至业务运行带来了新的安全问题。

3 方案目标

本方案的目标是从安全的角度出发，基于定制化云查杀技术及企业黑白名单，为企业打造的高度可控云安全解决方案。面对复杂的办公网络环境，提供内网云安全服务，能最大限度保障业务系统和数据安全，有效降低资源占用和运营成本。

1、病毒木马防护

本系统采用云查杀技术，以黑白名单为基础，建立了查杀效率高、误报率低的病毒木马防护机制。

2、恶意代码防护

与病毒木马类似，也采用了云查杀的机制，来实现恶意代码的防范。

4 方案原则

从办公终端安全的实际需求出发，在保障终端稳定运行的基础上进一步完善终端病毒查杀能力，加强终端安全管理能力，全面提高终端的安全水平。

本方案设计会遵循以下原则：

- **整体安全**

方案设计综合考虑终端安全防护的各个环节，综合使用各层次的多种安全手段，提供全方位的安全保障。

- **扩展性**

本次方案能够适应办公终端需求的变化，易扩展易升级，为未来的发展留有接口。

- **稳定性**

本次方案需保证办公终端的稳定、顺畅，实施和运行不对应用系统造成影响。

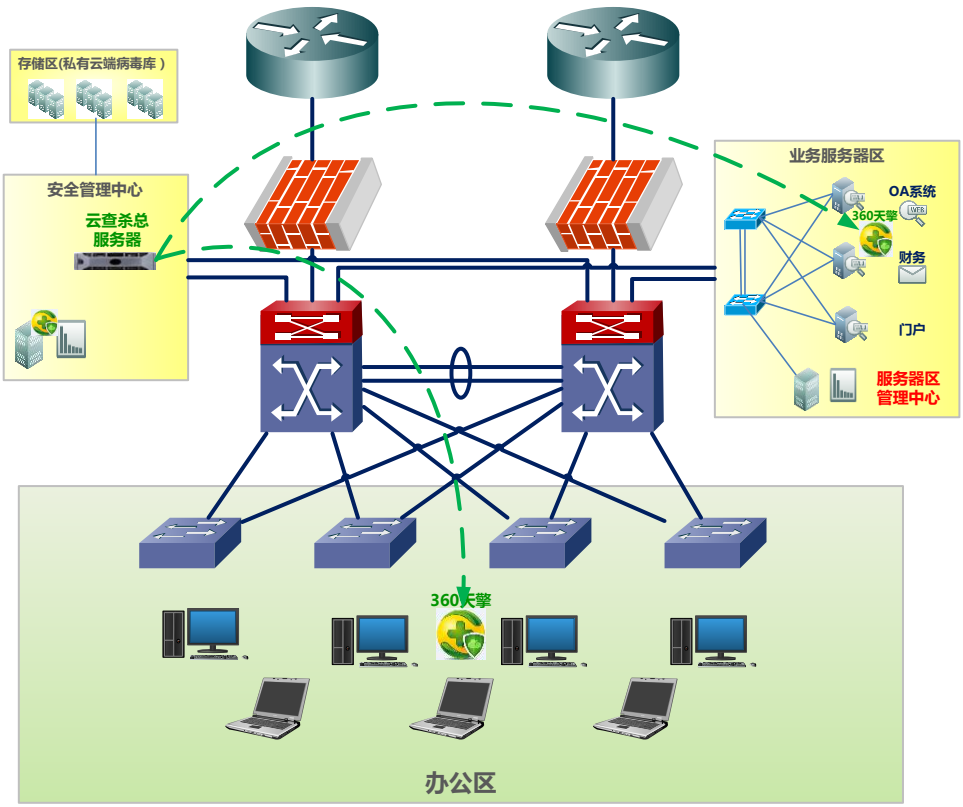
- **国产化**

信息安全保密工作关系到国家安全，所采用的安全产品为完全国产开发。

5 方案设计

5.1 一级部署，单级管理

由于本次替换的终端较少且较为集中，所以本方案采用北京奇虎科技有限公司的私有云杀毒产品来搭建办公网防病毒系统，该系统采用一级部署，控制中心部署在分公司办公网中心机房，直接管理分公司内部的办公终端。系统部署示意图如图 5-1 所示。



5.2 系统自动升级

5.2.1 目标描述

在无须运维管理人员参与的情况下，对 360 私有云杀毒客户端软件、私有云杀毒管理控制台软件、360 私有云杀毒客户端病毒特征库进行自动下载、升级与安装。

5.2.2 设计描述

为了避免升级过程中导致网络拥塞，终端的升级将从内网的升级服务器统一拉取升级文件，即终端不会从位于 Internet 的 360 升级服务器下载升级文件。

当 360 私有云杀毒管理控制台处于隔离网与非隔离网两种环境之下，其升级方案也有比较大的区别，360 私有云杀毒支持对于隔离网环境下的物理隔离升级与非隔离网环境下的内网推送式升级。

1、内网推送式升级：

- 第一阶段：升级服务器（一般来说就是管理控制台）从位于 Internet 上的 360 升级服务器下载全部升级文件至本地。
- 第二阶段：360 私有云杀毒客户端根据自己的实际需要从升级服务器上下载升级所需要的文件并执行升级操作。

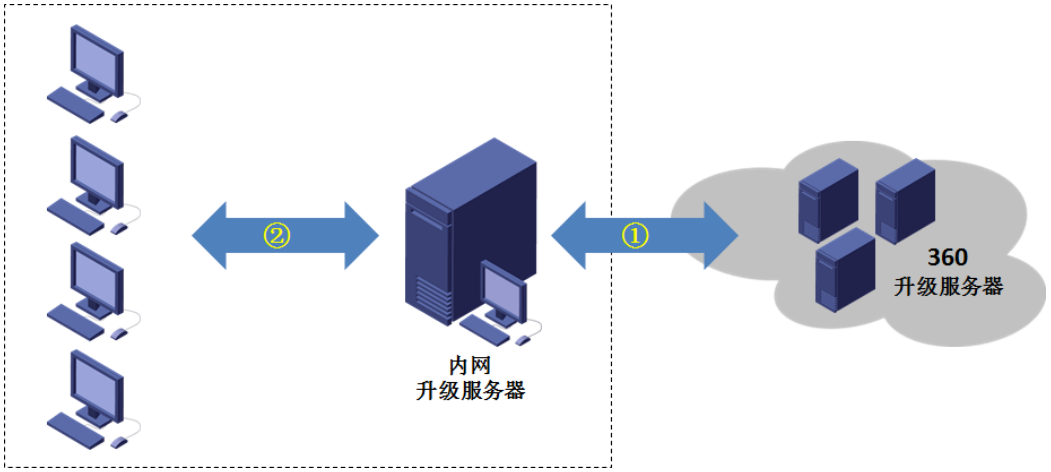


图 5-1 内网推送方式升级流程

2、物理隔离升级：

对于隔离网环境来说，由于内网升级服务器无法连接至 360 升级服务器，因此无法直接完成升级文件的下载，在这种情况下，我们提供了“隔离升级代理”工具完成升级文件的下在工作，具体升级过程如下：

- 第一步：将“隔离升级代理”工具放置在内网升级服务器上，运行该工具，即可完成升级所需信息的收集工作，即搜集到内网服务器中当前升级文件的版本信息，建立升级基线。
- 第二步：将“隔离升级代理”和所搜集到的升级服务器的升级基线拷贝到一台可以连接至互联网 360 升级服务器的机器上，并再次运行该升级工具，此时，“隔离升级代理”工具将根据当前最新的升级文件与第一步中采集到的升级基线进行对比，下载新增、修改的文件，并将下载到的文件保存在“隔离升级代理”工具所在的文件夹中。

- 第三步：再次将“隔离升级代理”文件夹整体拷贝到内网升级服务器之上，再次运行该工具，即可将最新的升级文件成功存放在内网升级服务器上的制定存储位置。

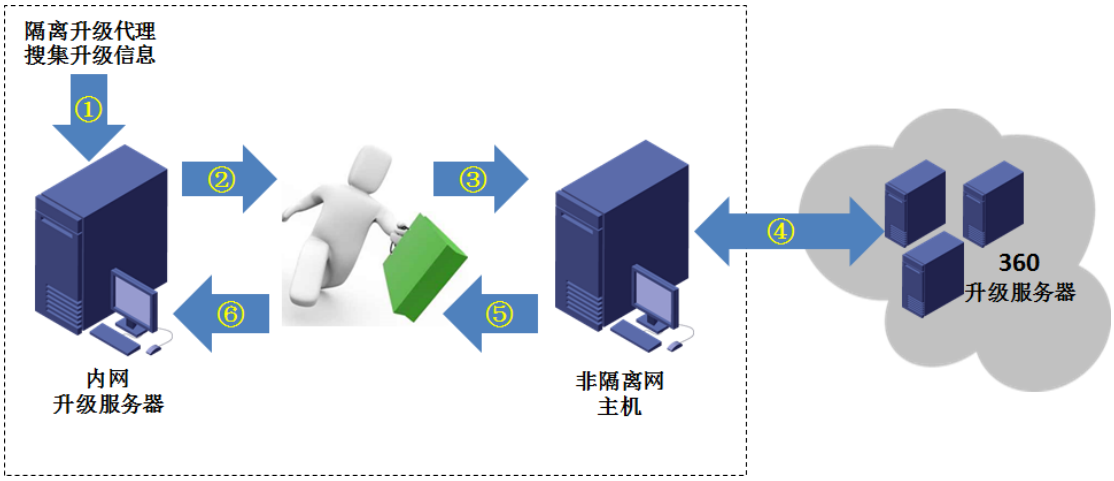


图 5-2 物理隔离网升级流程

5.2.3 升级过程中的带宽利用

为了最大限度降低升级过程中的带宽消耗，保障业务运行带宽不受升级过程影响，360 私有云杀毒采用如下的技术保证升级过程中的网络稳定性与业务稳定性：

- **带宽压缩技术**

  在客户端下载升级文件的过程中，将对升级文件进行压缩处理，尽力降低升级文件传输过程中对带宽的消耗。

- **带宽限制技术**

  内网升级服务器支持对升级文件传输的带宽总流量进行限制设置，可以对升级过程中消耗的总带宽进行上限设置。

- **智能分发技术**

  内网客户端将根据自身的实际需要从内网升级服务器下载不同的特征库升级文件、补丁文件、软件升级包等，而不会将所有的升级文件都从内网升级服务器上下载。

5.3 终端病毒防御

该功能的目标是对互联网中的病毒、木马、蠕虫、网马、僵尸网络、流氓软件、间谍软件等恶意代码进行有效的识别、查杀与隔离

5.3.1 功能框架

本方案对病毒、木马、蠕虫、网马、僵尸网络、流氓软件、间谍软件等恶意代码的识别和查杀采用了多套高性能检测引擎的技术方案，这些技术方案中，既包括传统基于静态病毒特征的多模式匹配的检测技术、也包括无特征的人工智能检测技术，多种检测技术的综合运用，最大限度地保障检测的有效性，具体来说，本方案中采用了如下几种关键的检测技术：

- **双病毒检测引擎**
- **QVM-II 人工智能检测引擎**

已知病毒查杀功能框架如下图所示：

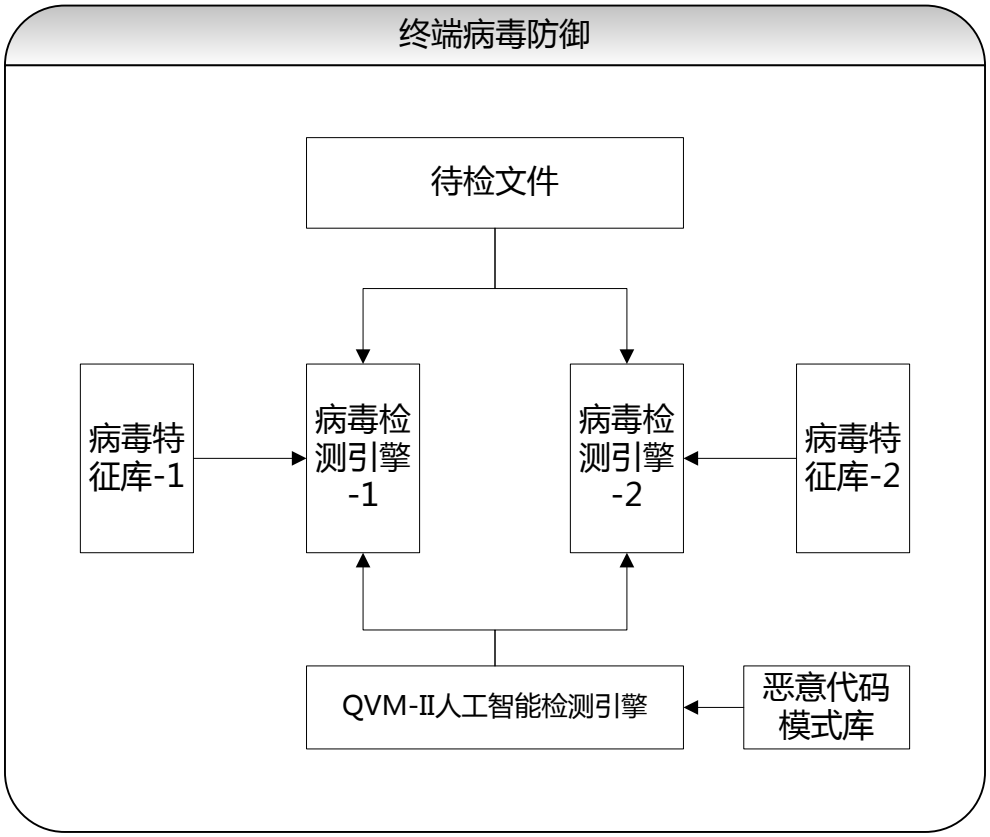


图 5-3 私有云防病毒系统功能框架

5.3.2 设计说明

1、双病毒特征库与双病毒检测引擎

与其他病毒检测产品不同，本方案采用了双引擎的查杀技术，具体来说就是采用实现技术完全不同的两套独立的病毒库、病毒检测引擎对已知病毒进行检测。因为已知病毒检测的关键是病毒库的覆盖度和检测引擎的预处理能力，因此如果其中一套病毒检测引擎出现错误（误报、漏报）的可能性为 P（P < 1），另一套病毒检测引擎出现错误（误报、漏报）的可能性为 Q（Q < 1），那么两套完全独立的病毒检测引擎同时出现错误（误报、漏报）的可能性就是 P • Q（P • Q < min(P, Q)），举例来说，如果第一套引擎出错的可能性是 P = 2%，第二套引擎出错的可能性是 Q = 3%，那么两套引擎同时出错的可能性就是：

(0.02) • (0.03) = 0.0006

可以看到，双病毒特征库，双病毒检测引擎的方案，与单病毒库、单病毒检测引擎相比，在检测的准确率上有大幅提升，由于双病毒特征库，双病毒检测引擎与单病毒库、单病毒检测引擎相比，性能开销（CPU 消耗、内存消耗）会更大，因此本方案中对是否启用双病毒库、双病毒检测引擎采用了配置开关，可以根据终端硬件的配置情况灵活启用或者关闭该功能。

2、QVM-II 人工智能检测引擎

对于病毒和恶意代码的检测，一直存在着两个技术方向，一个是依靠病毒特征匹配的静态检测技术，这种技术的特点是必须依靠已知的病毒特征，一般静态特征匹配的技术适合对已知病毒、恶意代码的检测。另外一种是依靠对病毒行为的动态分析技术，这种技术更适合对未知病毒、恶意代码的检测。这两种技术是目前对病毒进行检测的关键技术，分别实现对已知、未知的病毒及恶意代码检测。

其中采用特征对病毒进行检测的技术又分为两个方向，一个是穷举式病毒特征提取，即针对每个已发现的病毒、恶意代码样本提取各自的病毒特征，这种方式的优点是能够准确识别出已提取特征的病毒与恶意代码，误报率和漏报率都很

低。另一种是针对不同族类的病毒及恶意代码提取出共性的族群特征，并以此作为检测依据对恶意代码进行检测。这种方式的优点是不依赖某一个病毒或恶意代码的具体特征，而是提取某一族群的恶意代码共性特征，因此，这种检测方法对于某一病毒与恶意代码族群内的新生病毒具有非常强的检测能力，同时还能对检测出来的病毒与恶意代码进行族系归类。

QVM-II 人工智能检测引擎采用人工智能与机器学习的方法，对 360 目前已经积累的 20 多亿病毒样本进行多次切片学习，抽取出病毒与恶意代码的共性特征，建立恶意代码的不同族系模型，该算法在北美、欧洲的多项恶意代码检测能力测评之中名列第一。该技术的主要组成框架如下：

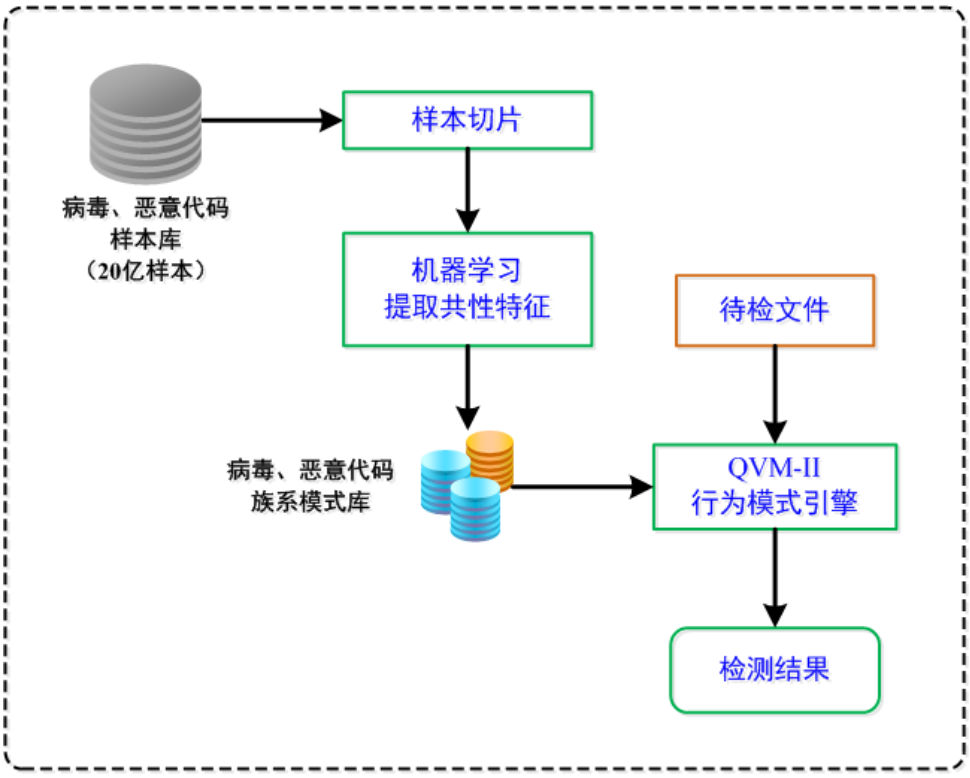


图 5-4QVM-II 技术框架图

5.4 私有云查杀

5.4.1 目标描述

传统统杀毒软件依赖基于黑名单方式的本地特征库匹配技术进行查杀，无法

应对日益严峻的安全威胁，并且日渐庞大的特征库会带来越来越多的系统资源占用，同时本地特征库升级频率远远落后病毒更新速度，难以及时应对新的未知威胁，所以应该使用云安全技术来解决终端的病毒安全问题。

5.4.2 设计描述

私有云安全，是指企业自己使用的云，它所有的服务不是供别人使用，而是供自己内部人员或分支机构使用。私有云安全的部署比较适合于有众多分支机构的大型企业或政府部门。随着这些大型企业数据中心的集中化，私有云安全将会成为他们部署 IT 系统的主流模式。私有云安全是企业 IT 在云计算时代演进的一个重要过程。

360 私有云杀毒把文件特征库置于部署在企业内网中的私有云引擎上，无需连外网，各级控制中心可以直接调用私有云引擎中的特征库执行查杀，其运算速度和数据量都远远超过传统杀软的本地查杀引擎，实现全网协同作战、集体防御的效果，并允许企业根据业务需求自由设定私有的文件的黑白名单，避免内网软件出现误杀、漏杀。

5.4.3 产品形态

为了给客户更多的选择，360 私有云引擎采取两种形态实现，分为软件形态和硬件形态。

1、软件形态

为减少用户的投入成本，360 私有云引擎制作出了基于虚拟机的软件形态版本，可直接安装到 windows 系统平台上使用。

服务器硬件配置要求如下：

4 核 CPU，8G 内存，500G 硬盘，C 盘划分 100G，D 盘划分 300G，E 盘划分 100G

2、硬件形态

为了提高引擎的稳定性，360 还专门制作了私有云引擎硬件平台，用户只需为其配置固定的 IP 地址就可使用。在正常情况下，能支持 2 万终端进行云查询。

私有云引擎硬件平台参数见下方：

360 私有云查杀系统硬件平台。	
技术参数：	
主板	Intel ATOM 系列
机箱	440 x 44 x 499 mm (1U)
电源	单电源（功率：100W）
CPU	Intel ATOM D525 (双核 1.8GHz)
内存	8G DDR-1333 内存
硬盘	3.5 寸 1T SATA 普通硬盘
网络接口	6 10/100/1000 Mbps PCIe GbE ports 5 x Intel 82583V 1 x 82567V GbE PHY
管理接口	2 x GbE LAN ports
其它接口	6 个 USB2.0 接口，1 个 RJ-45 接口
重量	4.5kg
产品认证	CE,FCC,CCC ,UL,CB
功能/性能参数：	
1、	支持 centos 6.4 操作系统，nginx 1.4.3.3
2、	使用自有云引擎 stored，能够高效率进行存储和查询
3、	白名单记录数：3 亿
4、	黑名单记录数：1 亿
5、	数据传输率（KB）：300M/S
6、	隔离网文件鉴定速度：小于 1 秒
7、	在互联网环境下，私有云与公有云文件交互时间：小于 15 秒
8、	每个请求查询 1 个 MD5：QPS 为 1050，CPU 占用 100%，内存占用 200MB
9、	每次请求查询 15 个 MD5：QPS 为 580，CPU 占用 100%，内存占用 200MB
10、	每次请求查询 50 个 MD5:QPS 为 550,CPU 占用 100%,内存占用 200MB

11、	在正常情况下，能支持 2 万终端进行云查询

5.5 黑白文件自定义

5.5.1 目标描述

企业办公网上运行着大量公司自主开发的软件，其可能触发终端安全管理软件的安全机制导致误杀而无法启用，影响其正常工作，所以终端安全管理工具应该允许用户对查杀到的文件自行定义并处理，减少误杀几率。

5.5.2 设计描述

360 私有云杀毒在控制中心可以对终端查杀策略进行配置，在终端发现异常文件后将该文件放入加密的隔离区中而不是直接查杀。管理员可在控制中心对查杀到的文件进行判断，将其中的正常文件添加到信任区中。文件添加到信任区后，终端将不再对其进行检查。这种机制可以在保证终端安全效果的同时保证企业的特殊软件正常运行。

5.6 断网保护能力

5.6.1 目标描述

企业内部办公网可能因为线路故障等各种原因导致断网，所以此时应该采取有效的安全机制保证终端的杀毒软件在断网的情况下依然可以有效的工作，对终端便携机进行保护。

5.6.2 设计描述

当网络瘫痪的发生的时候，终端将无法正常连入网络，受此影响，终端也将

无法连接升级服务器进行正常的病毒库升级、补丁升级，在这种情况下，终端的防护将面临着新型病毒、新型漏洞利用攻击的危险，为了应对这个问题，360 私有云杀毒终端采用了智能查杀加虚拟补丁的方案，保证在终端无法升级病毒特征库、无法安装补丁文件的情况下，仍然可以对新型病毒、新型威胁进行有效防御：

- **本地病毒引擎防护**

360 私有云杀毒的终端安装有本地杀毒引擎 BD 和小红伞，同时在终端上会有联网时控制中心下发的最新病毒库。当断网时，本地杀毒引擎和病毒库继续保护终端的安全。

- **智能查杀（QVM-II）**

360 的智能防护技术（QVM-II）采用人工智能与机器学习的方法，对 20 亿的病毒、木马等恶意代码样本进行学习，提取恶意代码的共性特征，并建立恶意代码的静态行为模型，以此作为对病毒、木马、蠕虫的检测依据，可以在不依赖病毒、木马、恶意代码的个体特征的情况下，实现对病毒、木马、恶意代码的准确查杀，这种技术保证了在完全没有病毒特征库的情况下也可以高精度地进行检测。

- **虚拟补丁**

360 的主动防御技术采用对文件打开、执行全过程跟踪的方式对系统中加载、打开、运行的文件进行逐步分析，一旦发现有攻击行为，立即加以阻断，这种主动防御技术可以在系统在没有安装补丁的情况下进行主动防御，这种基于主动防御技术的虚拟补丁可以保障终端在没有安装补丁文件的情况下，在受到攻击的时候进行有效防御。

5.7 全网安全评估

5.7.1 目标描述

伴随互联网的高速普及，木马种类及数量都急剧增长。少量的特征库无法满足安全需求，并且日渐扩大的特征库会带来资源占用问题，两头受制的状况亟待改善。只有通过对全网文件安全状况进行统一分析，才能真正了解企业办公网的

安全状况，让木马病毒无处藏身。

5.7.2 设计描述

360 私有云独创的全网文件安全审计功能，全网的可执行文件信息都汇总到服务器端，所有文件都带有详细信息和云鉴定结果，管理员可以按公司名、产品名、数字签名等方式分类审核文件，便于及时发现和定位未知威胁。包含了全网文件云鉴定的详情和用户自主的信任区与禁用区。

全网文件云鉴定里面分风险文件、安全文件和病毒文件，并可按照数字签名和文件名两种方式展示，风险文件里面包含了正在等待 360 公司鉴定的文件和鉴定之后未知是否为安全的文件；安全文件里面包含了已经被 360 公司鉴定为安全的文件；病毒文件则包含了已经被 360 公司鉴定为病毒的文件。

用户可以在信任区/禁用区中根据业务需求自由设定私有的文件的黑白名单，避免内网软件出现误杀、漏杀。

5.8 终端管理

5.8.1 目标描述

对终端进行分组设置，统计当前在线、离线的用户数量，查看终端登录账号、病毒发现和系统情况。提供查询功能，查询指定的用户是否在线，提供查询功能，查询指定的组内在线、离线的用户数量。

5.8.2 设计描述

1、终端定时打点

- 终端开机之后与管理控制中心进行通信，定时（如：每 30 秒）向管理控制中心执行一次打点操作。
- 管理控制中心为每个终端设置一个定时器，该定时器初始值为 40 秒，如

果在定时器到时，但还没收到该终端的打点信息，则管理控制中心主动向该终端发起一次状态探测请求，若该请求 5 秒内无响应，则该终端置为“离线”状态，同时停止该终端定时器；若该请求 5 秒内返回应答，则该终端置为“在线”状态，同时将定时器清零，重新开始计时。

2、状态统计与查询

- 统计全网在线与离线终端的数量，同时给出这些终端的 IP、登录账号、病毒、操作系统等信息。
- 对终端进行分组配置。

5.9 系统兼容性

5.9.1 目标描述

支持多种版本 Windows 操作系统。

5.9.2 设计描述

1、所支持的操作系统版本

Windows Server 2003（32 位 & 64 位）

Windows Server 2008（32 位 & 64 位）

Windows XP

Vista

Windows 7（32 位 & 64 位）

Windows 8

2、管理架构

系统采用 B/S 架构，管理员可以随时随地的通过浏览器打开访问，对天擎进行管理和控制。

5.10硬件平台要求

5.10.1目标描述

保证 360 私有云杀毒软件的正常运行

5.10.2设计描述

1、控制中心

CPU ： 普通双核以上，建议 i3 处理器

内存：最低 2GB，建议 2G 以上

硬盘：最低空闲空间 50G，建议空闲空间 200G 以上

2、终端

CPU ： P4 以上处理器

内存：不低于 512MB，建议 1GB 以上

硬盘：10GB 以上空闲空间

5.11系统可扩展性

5.11.1目标描述

当前可支撑 5000 终端用户使用，最多可支持 1 万终端，在未来发生扩容的情况下，亦可通过增加子控制中心（即分级管理）的方式满足扩容要求。

5.11.2设计描述

私有云杀毒 360（专业版）提供多级管理的功能，通过多级分管，将终端划归到不同的管理控制中心之下，可以实现扩容情况下的灵活扩展方案。

目前对于标准的服务器（如 DELL 720R，双路 Sand Bridge CPU，单路 8 核，16G 内存，300GB 硬盘）可以有效管理 10000 终端。

未来进行扩容，每增加 10000 终端，相应增加 1 个子控制中心即可满足扩容后的终端管理要求。

6 技术支持及售后服务

6.1 保修期内服务

6.1.1 远程技术支持服务

在保修期内，奇虎 360 将为用户提供免费的远程技术支持服务，服务内容包括：

- 远程电话支持

为本项目设立专用的 7×24 小时直拨服务热线电话，用户可以随时拨打热线服务电话进行免费技术咨询，包括硬件使用和维护方法、软件使用方法和解决用户使用中发生的各种疑难问题。在用户的技术支持请求或故障报告后，将立即予以答复。对于无法立即解决的技术问题，要了解问题的详细情况并告诉该单位预计的答复时间，接到故障报告后的答复时间最长不得超过 8 小时。

- 远程邮件支持

用户还可以通过邮件方式与我方联系。通过邮件与我方联系时，请在故障报告中填写产品的版本信息、许可证信息、主机使用平台名称和尽可能详细的问题描述，以便于我方能尽快解决您的问题。

6.1.2 现场支持服务

在设备试运行期间和保修期内，当用户的产品出现紧急故障时，根据用户需要，奇虎 360 将安排售后工程师进行紧急现场服务，并保证在到达现场的 24 小时内解决问题，故障不解决，工程师不撤离现场。若遇到重大技术问题，奇虎 360 将及时组织有关技术专家进行会诊，并采取相应措施以确保系统的正常运行。

6.1.3 咨询服务

奇虎 360 将免费为用户提供技术咨询服务，如为用户提供系统管理的技术指导、协助用户做好备份计划、完善工作日志和机房制度、制订操作守则等。同时，奇虎 360 可以根据用户需要提供全面的安全咨询服务，并发出安全警告，消除由于各种应用的不断发展、系统扩充等原因所带来的安全隐患。

6.1.4 备品备件支持服务

奇虎 360 承诺为本项目提供备品备件支持服务。基于业务运行的重要性及响应时间考虑，对于经奇虎 360 工程师判定出现硬件故障的设备，我方保证在 12 小时内免费提供不低于故障设备规格型号档次的备用设备供用户使用，以保证业务系统的正常运行，直至故障设备修复。

备品备件支持服务的具体流程如下：

（1）接到报修电话后技术服务人员对故障现象进行了咨询和判断；

（2）当断定为硬件故障后，对于在质保期内的产品且用户需要提供备机服务，技术服务人员将与用户联系有关备机的发货和故障机的返修事宜；

（3）上门替换故障机，故障机返修；

（4）故障机维修完毕后，奇虎 360 技术服务人员将及时与用户联系有关故障机的发货与备机返还事宜；

（5）上门替换备机，备机返还。

6.1.5 软件升级支持服务

奇虎 360 对提供的软件提供补丁安装、免费升级（若软件有升级版本）和技术支持。软件版本升级后，以电话和电子邮件的方式通知用户，用户可通过网上下载新的版本或补丁。

6.1.6 产品常规检测服务

奇虎 360 可以根据用户需求定期对硬件系统的性能和发生故障的可能性进行广泛深入的常规检查分析，并为用户提供一份可读性很强的检测分析报告，该报告将指出硬件系统存在的潜在问题以及对应的解决方法，以便为用户的日常维护工作提供参考依据。

6.1.7 系统优化建议与实施

奇虎 360 的技术人员可以根据系统的特点和运行现状，帮助陕西省人民检察院在系统应用过程中不断的优化系统性能，以满足不断变化的业务发展情况。

6.1.8 设备迁移服务

如用户的网络结构需要更改或者网络需要搬迁，奇虎 360 可提供设备迁移服务，其内容包括为最终用户重新设计网络结构、更改网络配置等，同时其过程和结果均以文档形式记录保存。

6.1.9 应急响应服务

为了保证用户系统的正常运行，确保系统在出现紧急故障时能够得到及时响应，奇虎 360 建立了以副院长为首的应急部门，同时针对重大项目将成立以副院长为首的专门应急小组。奇虎 360 将为本项目另外专门设立一位应急负责人，手机将 7×24 小时开机，在系统出现紧急故障时用户可以随时进行联系。

6.1.10移机服务

移机是指用户的机房位置发生变化时，其中的本项目设备需要迁移到新的机房中。奇虎 360 可以免费为每个部署点提供免费移机服务。用户提出移机服务请

求后，奇虎 360 和第三方厂商的技术服务人员将到达用户现场对新、旧两处机房的环境和设备的运输线路进行现场勘查，并向用户提交《移机计划》。

《移机计划》中主要包含以下内容：

- 设备准备情况：如设备状态、备机准备等
- 环境准备情况：如新机房线路、电源、空调等现场环境的准备情况等
- 工具准备情况：如运输工具、上架安装工具等
- 路线准备情况：在用户的协助下，选定一条对移机时间影响最小的路线等

《移机计划》经用户审核同意后，根据用户需求实施移机服务。在实施移机服务时，应注意以下事项：

- 尽量采用设备原包装进行运输，如果路线路况情况不佳，应对设备包装进行必要的加固措施
- 实施移机服务的前一天，应对实际路线进行踏勘

移机工作完成后，奇虎 360 和第三方厂商的工程师将对设备进行连续监控，保证设备在新环境中运行正常。

6.2 专属 VIP 服务

奇虎 360 力争为本项目用户提供最优质的服务，特免费赠送专属 VIP 服务内容如下：

6.2.1 专门的热线支持

奇虎 360 在为本项目提供 7×24 小时热线支持的情况下，还为本项目指定专门的服务工程师，为最终用户提供电话、邮件等支持。

6.2.2 专门的团队

奇虎 360 将为本项目成立专门的实施和服务团队，为用户提供电话、邮件、现场服务等支持，团队成员稳定且经验丰富，能够保证本项目的有效实施和后续服务的及时性和有效性。

6.2.3 信息安全通告服务

奇虎 360 可根据用户需要通过电话、传真、期刊、邮件等方式（用户可选择）为用户提供信息安全通告服务。奇虎 360 将及时通告用户最新的安全动态和安全技术的发展趋势，包括时效性很强的漏洞、攻击手法、病毒的预先通知，帮助用户的安全管理员在最快的时间内了解重要的安全信息。

6.2.4 用户专用档案服务

奇虎 360 将为本项目建立专门的用户服务支持档案，并设定 VIP 权限，用户对服务支持的要求、产品类别型号、使用情况、每次服务支持解决问题的情况等信息都将保存在用户服务支持档案中，以便奇虎 360 更有针对性地提供服务。

在每次处理完系统故障后，奇虎 360 将会把故障现象、故障判断过程、故障处理过程、故障所造成的损失和系统参数变化情况等信息记录在用户服务支持档案中。

奇虎 360 将长期保存本项目的所有用户服务支持档案，直至本项目最终用户要求删除时为止。

6.2.5 定期技术交流及培训服务

奇虎 360 将与本项目最终用户协商，进行定期的技术交流，与最终用户共享信息安全领域的最新技术信息，进行相关软硬件的技术培训，提高用户单位系统维护人员的技术水平，减少人为故障。

6.3 保修期外服务

在保修期外，奇虎 360 将依然按照保修期内的服务标准为本项目用户提供技术支持及售后服务。保修期外的服务分为免费服务和收费服务两个部分。

6.3.1 免费服务

1、免费电话技术咨询服务

在保修期外，本项目用户可以随时拨打 7×24 小时技术支持热线进行免费技术咨询，包括硬件使用和维护方法、软件使用方法和系统使用过程中发生的各种疑难问题。

2、远程技术支持服务

在保修期外，奇虎 360 依然按照保修期内的服务标准免费为本项目的最终用户提供远程技术支持服务。

3、信息安全通告服务

奇虎 360 可根据用户需要通过电话、传真、期刊、邮件等方式（用户可选择）为用户提供信息安全通告服务。奇虎 360 将及时通告用户最新的安全动态和安全技术的发展趋势，包括时效性很强的漏洞、攻击手法、病毒的预先通知，帮助用户的安全管理员在最快的时间内了解重要的安全信息。

6.3.2 收费服务

在保修期外，奇虎 360 将依然按照保修期内的服务标准为本项目用户提供现场技术支持服务，仅收取服务成本费，不再加收任何其他费用。