360 终端安全与管理系统

整体解决方案

二零一四年十二月

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

目录

第一章 现状及需求分析 4
1.1 应对防不胜防的计算机病毒 4
1.2 如何落地终端安全管理制度 4
1.3 微软停止 XP 补丁升级服务问题 5
1.4 如何减轻终端运维工作量 5
1.5 满足等级保护要求 6
第二章 建设思路 7
2.1 建设终端病毒防御体系 7
2.2 部署终端安全管理技术措施 8
2.3 部署 XP 防护技术措施 8
2.4 启用统一运维功能 8
2.5 满足合规性要求 9
第三章 建设方案 9
3.1 终端病毒与恶意代码防范 9
3.1.1 功能框架 9
3.1.2 双病毒特征库与双病毒检测引擎 10
3.1.3 360 云查杀检测引擎 11
3.1.4 恶意 URL 检测引擎 12
3.1.5 QVM-II 人工智能检测引擎 14
3.1.6 私有云平台 15
3.2 落实终端安全管理技术措施 15
3.2.1 终端外设管理 15
3.2.2 终端进程与服务管理 16
3.2.3 终端流量管理 17
3.2.4 硬件资产管理 18
3.2.5 终端 Agent 强制安装与运行 18
3.3 XP 安全加固 19
3.3.1 实力保障 19
3.3.2 总体描述 19
3.4 统一运维功能 22
3.4.1 系统自动升级 22
3.4.2 软件分发 24
3.4.3 文件管理 24
3.4.4 终端小工具 24
3.4.5 远程协助功能 25
3.5 符合等级保护要求 25
3.5.1 策略下发 25
3.5.2 终端版本统一监控 26
3.6 方案优势 27
3.6.1 完善的终端安全防御体系 27

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

3.6.2 强大的终端安全管理能力.....27
3.6.3 良好的用户体验与易用性.....28
第四章 非功能性设计.....29
4.1 系统兼容性.....29
4.2 硬件平台要求.....29
4.3 系统容灾.....30
4.4 虚拟化支持.....30
第五章 部署实施.....32
第六章 售后维护服务.....34
6.1 售后服务组织机构-客户服务中心.....34
6.2 售后服务内容.....36
6.3 售后服务手段.....36
6.4 售后服务流程.....37
6.5 顾客档案管理-服务管理系统.....40
6.6 服务响应时间.....40
第七章 效益分析.....42
7.1 安全源自实践，安全不只合规.....42
7.2 持续安全升级，力助系统过渡.....42
7.3 强大管理能力，提高运维效率.....42
7.4 自主知识产权，杜绝后门隐患.....42
第八章 产品配置清单.....43

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

第一章 现状及需求分析

（此处对用户单位做简单的介绍）

随着计算机网络及信息化系统的建设，XXX 建设了全面覆盖的网络信息化系统，成为信息系统办公、管理的数字中枢，促进了业务系统的现代化办公管理、提高了工作效率。XXX 全网共有各类 PC 终端 XX 多台，具有客户端点数目多、分布距离远、内部安全性要求高等特点。

1.1 应对防不胜防的计算机病毒

随着信息技术的不断发展，XXX 业务的运作越来越依赖于计算机，而目前防不胜防的计算机病毒给 XXX 计算机终端的正常运行造成了较大的威胁。随着病毒的大量出现，仅奇虎 360 一家安全企业，到目前为止就已经积累了 20 亿的病毒样本，如果算上未经去重的病毒样本，已发现的病毒样本已经远远超过了 20 亿的规模，而目前大多数的终端杀毒软件，受本地存储资源的限制，本地病毒特征库的规模大约在 1000 万 ~ 1500 万左右，这个数字只占不到 20^{+} 亿已发现病毒样本的 1%，依靠 1%的病毒库去检测网络中肆虐的病毒，这说明传统的本地病毒库的查杀方式已经无法满足对已知病毒的查杀要求。

为了解决层出不穷的计算机病毒，XXX 需要引入一套终端安全管理软件，包含技术先进的网络版防病毒功能，可通过云端的海量计算资源与海量存储资源满足对数十亿病毒进行 100%查杀的防病毒需求。

1.2 如何落地终端安全管理制度

为了更好的管理好终端，XXX 制定了相应的终端安全管理制度，但目前终端安全管理制度的控制点缺乏有效的技术执行措施，仅仅依靠终端使用者的自觉性是很难落实相应的管理制度的，主要存在的问题有：

USB 无线路由屡禁不止：在办公电脑上使用 USB 无线路由，使终端暴露在不

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

可控的无线网络空间，不受控的智能终端或其他无线设备可以任意接入 XXX 办公网，造成极大的安全隐患。

USB 移动存储及各种外设滥用：在办公电脑上任意接入 USB 移动存储，给 XXX 内网带来很大的恶意代码感染风险，蓝牙、红外等外设接口的滥用，也带来非法外联的风险。

随意安装和运行各种软件：通常终端使用者都具有操作系统本地管理员权限，可以任意安装运行各种娱乐、盗版软件，给 XXX 带来了声誉风险及版权风险。

任意使用带宽资源导致网络拥塞：虽然 XXX 在网络边界部署了流量控制设备，制定了带宽限制策略，但无法实现基于应用的流量限制，内网依然存在 P2P 软件占用带宽，影响正常办公的情况。

随意更改主机信息：终端使用者可随意更改主机名、IP 地址、MAC 地址等信息，对资产管理、网络审计等方面造成不便。

为了贯彻 XXX 终端安全管理规范，本次引入的终端安全管理软件还应具备桌面管理功能，可从技术措施上落实终端安全控制点，有效减少终端安全风险。

1.3 微软停止 XP 补丁升级服务问题

在微软公司于 2014 年 4 月 1 日以后停止其 Windows XP 操作系统补丁升级服务，而 XXX 仍有部分计算机终端运行着 XP 系统。受此影响，在 XXX Windows XP 系统迁移至更高版本的系统之前，这些系统都将暴漏在各种网络威胁之中，机密信息、业务的正常运行都将受到严重威胁，一旦这些威胁发生,将产生难以估量的灾难性后果。

本次引入的终端安全软件应提供有效的 XP 防护措施，来解决 XXX 这部分终端的安全隐患问题。

1.4 如何减轻终端运维工作量

XXX 内网计算机终端数目多、分布距离远，日常终端运维管理的工作压力十

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

分巨大，主要表现在：

终端数量巨大、地理分散，导致终端运维支持困难。

统一补丁修复和软件分发问题：如果计算机终端存在的操作系统安全漏洞不能及时修复，将带来极大的安全风险，计算机终端需要统一的管理手段快速统一分发操作系统补丁，但架设的 WSUS 服务器配置较麻烦、维护工作量大，而且也不具备普通软件分发功能。

无法高效进行硬件资产管理：无法精确统计 IT 资产，确定每台电脑的硬件配置情况，无法跟踪硬件资产的历史使用纪录，也不能及时掌握资产变动情况。每次资产统计都消耗大量时间。

传统防病毒软件误杀带来的问题：传统防病毒软件为了提高病毒查杀率，奉行从严的查杀策略，导致单位内部应用程序或重要文档文件被误杀，因而产生了大量不必要的维护工作。

现场维护工作量：计算机终端用户报告使用故障时，需要 IT 维护人员亲自赶赴现场处理，但通常大部分上报的故障都是入门级的，完全可以通过远程协助解决。

为了有效减轻终端运维工作量，本次引入的终端安全管理软件还应具有统一运维的功能，并提供日常电脑维护小工具，方便 IT 维护人员快速完成工作。

1.5 满足等级保护要求

等级保护要求二级及二级以上的系统，应部署具有统一特征库升级、统一策略管理的网络版防病毒系统，并可定时进行特征码升级。

因此，引入的终端安全管理系统应满足以上要求并具有公安部销售许可证。

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

第二章 建设思路

根据上文的现状及需求分析，采用 360 天擎终端安全管理系统（简称“天擎”）来进行 XXX 终端安全与管理项目的建设，天擎是奇虎 360 自主研发的以安全防御为核心、以运维管控为重点、以可视化管理为支撑、以可靠服务为保障的全方位终端安全解决方案。为用户构建能够有效抵御已知病毒、0day 漏洞、未知恶意代码和 APT 攻击的新一代终端安全防御体系，并提供企业安全统一管控、终端硬件准入、软件准入、上网行为管理等诸多管理类功能。并且承诺在 2014 年 4 月微软停止免费主流支持服务之后依然向天擎产品用户提供 windows XP 补丁和安全更新。

- **信息收集**

天擎终端可以收集终端上的各种安全状态信息，包括：漏洞修复情况、病毒木马情况、危险项情况、以及各种软硬件情况等。

这些安全状态信息会汇集到服务器端的控制中心，使管理员全面了解网内所有终端的安全情况、硬件状态以及软件安装情况等。

- **立体防护**

天擎具有漏洞修复、病毒木马查杀、黑白名单、硬件准入、软件准入、上网行为管理等多样化的防护手段，从准入、防黑加固、病毒查杀、软件和上网行为控制等多个层次，为 XXX 构建立体防护网，确保 XXX 终端安全。

- **集中管控**

天擎控制中心为管理员提供了统一修复漏洞、统一杀毒、统一升级、上网管理、软件统一分发卸载等多种管理功能，管理员可以通过控制台直接对网内所有终端进行统一管控。

主要的建设思路如下：

2.1 建设终端病毒防御体系

全网部署天擎客户端代理，提供网络版防病毒功能。

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

采用 360 私有云查杀引擎(硬件)，解决传统防病毒软件本地特征库加载量不足的问题。满足对数十亿病毒进行 100%查杀的防病毒需求。

2.2 部署终端安全管理技术措施

在天擎控制中心制定策略，全网禁用 USB 无线路由，并对移动存储及各种外设接口进行管控；

设定办公网电脑软件运行黑白名单，禁止娱乐软件、盗版软件的安装及运行；

根据部门、用户设定终端带宽管理策略，有效杜绝 P2P 软件带来的网络拥塞问题。

对全网终端进行 IP、Mac 地址绑定，有效防止私自修改行为。

2.3 部署 XP 防护技术措施

采用天擎自带的 XP 加固功能，对 XXX 所有 XP 终端进行自动加固。

2014 年 7 月 31 日，由中国网络空间安全协会(筹) 竞评演练工作组主办的“XP 靶场挑战赛”落下帷幕。此次共有 5 家企业的产品成为靶标，在 300 余名顶尖黑客 12 小时的猛攻之下，奇虎 360 公司的 XP 盾甲产品再次经受住了严苛的考验，成功胜出。至此，奇虎 360 已经在国内外组织的有关 XP 防护产品的七次挑战赛及测评中全部胜出，成为实至名归的“七冠王”，彰显了奇虎 360 公司在安全领域特别是 XP 防护领域的绝对实力。

2.4 启用统一运维功能

采用天擎提供的统一运维功能，实现 XXX 全网终端的补丁统一升级、普通软件分发、硬件资产管理、一键加速、一键修复及远程协助功能，协助 IT 维护人员高效的完成终端运维工作。

采用天擎的私有云功能，建立 XXX 内部白名单，将业务应用、系统添加到白名单列表，杜绝误杀现象。

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

2.5 满足合规性要求

采用天擎控制中心进行所有终端的特征码升级、特征码版本监控、统一防护策略管理，满足等级保护要求。

天擎终端安全管理系统具有公安部销售许可证。

第三章 建设方案

3.1 终端病毒与恶意代码防范

本次采用的天擎终端安全管理系统，包含技术先进的网络版防病毒功能，可通过云端的海量计算资源与海量存储资源满足对数十亿病毒进行 100%查杀的防病毒需求。

3.1.1 功能框架

天擎对病毒、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和基于云端的云查杀检测技术，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，采用了如下几种关键的检测技术：

① 双病毒检测引擎

② 360 云查杀检测引擎

③ 恶意 URL 检测引擎

④ 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：

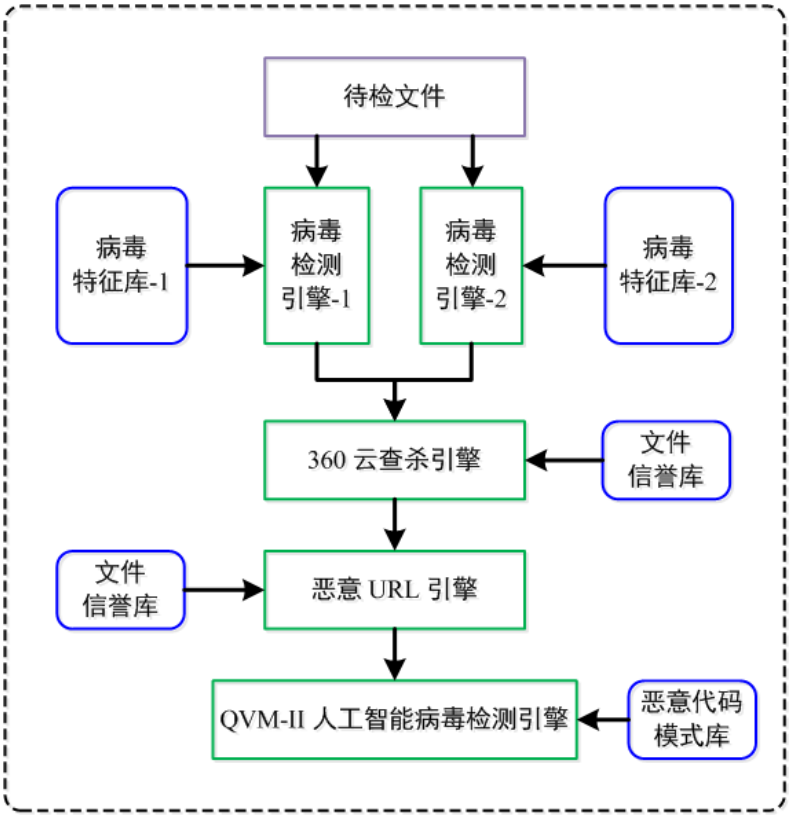


图 1 病毒查杀功能框架

3.1.2 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。

3.1.3 360 云查杀检测引擎

云查杀技术需要大量的样本资源、计算资源、检测技术资源，如果没有这些资源作支撑，则无法构建高质量的云查杀系统，本质上来说，云查杀系统是一个海量资源系统，这个资源系统中，既包括客户资源，又包括硬件资源与软件算法资源：

- 样本资源

  构建云查杀系统，需要海量的病毒、木马、僵尸网络等恶意代码样本作为资源支撑，否则，所构建的云查杀系统将因为缺乏足够的病毒样本积累而难以保证对于已知病毒和恶意代码的检测率。本方案中，我们才用的 360 云查杀平台，拥有涵盖了近 20 年的所有已知的病毒、木马、蠕虫等恶意代码的样本文件，其所积累的去重之后病毒样本数量已经超过 20 亿。

  样本资源的基础是客户资源，没有足够的客户资源作支撑，无法收集足够的病毒样本文件，只有广泛部署了终端系统的情况下，才能在短期内收集足够数量的恶意代码样本文件，奇虎 360 在全国拥有超过 4 亿的终端用户，覆盖了全国终端用户的 95%以上，其中绝大多数已经选择加入了奇虎 360 公司的“云安全计划”，这些遍布全国的海量用户为 360 提供了丰富、及时的病毒样本资源，保证了 360 云查杀系统病毒样本收集的及时、有效。目前平均来说，一个病毒从首次在国内互联网上出现，到被 360 云查杀系统捕获之间，只有不到 10 个小时的时间。

- 计算资源

  为了构造有效的云查杀系统，需要大量的计算资源进行支撑，以便对搜集到的样本资源进行深入分析，一般来说，一台标准的服务器（如 DELL R720，配置为：双路 16 核 CPU（Xeon E5-2690，单路 8 核，主频 2.9GHz）、Intel C600 主板芯片组、内存 16GB（ECC DDR3）、硬盘 900GB（SAS 接口）），每天（24 小时）可处理的样本数量大约在 3000 万个左右，因此，对于标准 1000 终端的用户来说，若按照每天每台终端提交 10 个样

本进行深度检测，则大约需要 4 台 DELL R720 这样配置的服务器组成的云查杀系统才能满足查杀需要。在本项目中，360 所提供的云查杀系统的规模已经超过了 20000 台服务器，由这些云服务器所构成的查杀环境，完全可以满足本项目的云端深度查杀需求。

- 算法资源

构建有效了云查杀环境，除了稳定、及时的样本收集资源与足够数量的硬件计算环境之外，还需要先进的未知病毒及恶意代码的检测算法，这样才能够在收集到病毒与恶意代码样本之后，进行有效的分析与处理。因此，对未知病毒与恶意代码的快速检测能力，就成了构建有效的云查杀环境的关键。在本方案中，360 所提供的云查杀环境集成了大量先进的真对未知病毒与恶意代码的查杀算法，这些算法中，有基于病毒与恶意代码静态样本共性特征的 QVM-II 算法（该算法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），也有目前主流的动态沙箱深度分析技术，同时还集成了利用未知漏洞进行病毒与恶意代码传播的基于内存分析的动态漏洞利用攻击分析技术，最后，对于非常复杂、难于分析的可疑文件，还会采用具有多年病毒分析与对抗经验的专家分析团队进行彻底分析。以上这些先机的自动化分析技术与方病毒专家团队人工分析的有效结合，多种手段、人机结合，保证了对病毒与恶意代码分析的万无一失。

3.1.4 恶意 URL 检测引擎

Web 应用是目前互联网的最主要应用，Web 安全问题因此也成了互联网安全问题中最重要的问题，占据了互联网问题中的绝大部分，网银诈骗、网购诈骗、钓鱼网站、网马等通过恶意网址进行钓鱼、诈骗、侵财的攻击事件频发，已经成了 Web 应用的主要威胁，同时也发现，部分 APT（高级持续性威胁）攻击行为也是通过恶意网站（一般是钓鱼网站）对 XXX 低权限终端进行入侵，进而以此低权限终端做跳板不断渗透高权限终端与服务器，最后完成 APT 攻击过程，因

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

此对于访问 Web 过程中的安全防护，已经成了当前终端安全防护的重要组成部分。

从技术上来看，对于终端访问恶意网址的防护主要有三种技术手段：

1、实时分析、动态检测

2、事先分析、静态匹配

3、实时分析结合事先分析，动态检测结合静态检测

第一种技术手段完全依靠在用户访问 Web 过程中对页面及其附属资源的动态分析和主动防御技术（如：IE 控件监控、内存监控、注册表监控）等方法对用户访问恶意网站、恶意链接的行为进行发现和阻断。这种方式的优点是可以对恶意访问行为进行实时发现，但其缺点也比较明显，即：如果对用户访问的 Web 访问进行深度分析，会消耗大量的用户本地资源，如果分析结论的得出也可能需要完整的分析过程之后才能完成，此时可能攻击行为已经部分发生，同时，完全依靠本地的动态分析，也存在一定的漏报可能，这些都是单纯依靠实时分析、动态检测可能会出现的一些问题。

第二种技术手段本质是通过云计算的方式来完成的，即：事先对互联网中存在的链接进行采集，采用动态分析结合沙箱的方式进行事先检测，将存在恶意行为的链接形成静态恶意链接库，终端在访问一个链接之前，终端系统安全代理会将此链接与恶意链接库进行比对，如果发现此链接在恶意链接库中出现，则认为该链接属于恶意链接，进而对其访问行为进行禁止，与单纯蚕蛹实时分析、动态检测的技术相比，采用这种方法可以大幅度降低终端的资源消耗，可以在第一时间发现恶意链接（而不是等整个页面及其资源文件都下载到本地并进行了分析之后），同时由于依靠云端的事前抓取分析、云端用户的检测结果，漏报的可能性非常小。但这种技术也存在一定的局限性：对于新出现的恶意链接，因为还没来得及被云端抓取分析，因此在一定时间内（比如：30 分钟）对这类新出现的恶意网址无法提供检测能力，即会出现漏报；另一方面，对于被挂马的受害网址，如果木马被清除，那么短期内（在下一轮抓取完成之前），该网址仍将被列入在恶意网址库之中，即在这段时间内会有误报出现。

第三种技术是结合上述两种方法，这种方法优势非常明显，即：对于大多数白名单中的网址直接放行，对于黑名单中的网址直接拦截，对于灰名单（即没在

白名单、也没在黑名单）中的网址则采用动态分析、主动防御技术进行实时分析。这种方式的优点非常明显：既利用了云端与其他终端的检测结果过滤了大量的白链接、拦截黑链接，大幅降低了客户端的资源开销，同时对极少量稀有链接又利用动态分析、主动防御技术进行深入的动态分析，起到了查缺补漏的效果。

在本方案中对于恶意 URL 的检测，采用的是第三种方法，即：动态分析结合静态匹配的技术方案，通过上述的技术分析可以看到，可以清晰地看到，本方案可以满足对恶意链接的精确检测要求。

3.1.5 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：

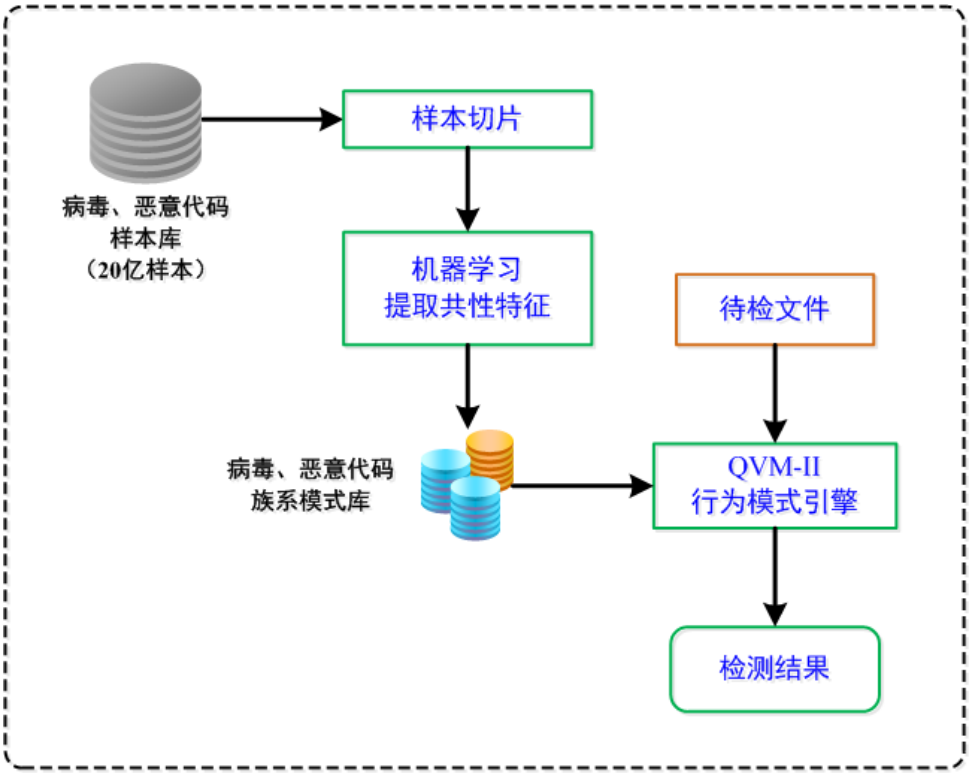


图 2 QVM 技术框架

3.1.6 私有云平台

天擎私有云模块把文件特征库置于内网标准可上架设备，无需连外网，终端可以通过云查杀引擎直接调用内网服务器端特征库执行查杀，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。

3.2 落实终端安全管理技术措施

为了贯彻 XXX 终端安全管理规范，天擎具备桌面管理功能，可从技术措施上落实终端安全控制点，有效减少终端安全风险。

3.2.1 终端外设管理

对主机所能连接的外部设备进行严格管控，具体来说就是对 USB 接口、光驱、软驱、USB 无线路由、平板与手机等设备进行准入控制，同时可以对 U 盘实现只读控制，以此实现主机的数据安全。

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

本系统在设备驱动层对外部设备进行可接入控制，实现对外部设备的严格准入控制。

外设类型	控制方式
USB 接口	启用/禁用
USB 无线路由	启用/禁用
平板与手机	启用/禁用
光驱	启用/禁用
蓝牙	启用/禁用
智能卡	启用/禁用
打印机	启用/禁用
串口	启用/禁用
并口	启用/禁用
U 盘	禁用/只读/读写

3.2.2 终端进程与服务管理

监控所有终端的所有进程、服务的运行情况，统计不同进程、服务的出现时间、终止时间、运行持续时间等信息，可以根据黑白名单策略自动强行启动或强行关闭终端进程。

进程、服务监控

- 进程、服务名称。
- 进程、服务描述。
- 进程、服务启动时间。
- 进程、服务终止时间。

- 进程、服务持续运行时间。
- 该进程、服务是否属于强制启动。

进程、服务强制启动与关闭

- 远程可以强制启动进程、服务，并将该进程、服务列入后继强制启动策略
- 远程可以远程禁止进程、服务，并将该进程、服务列入后继强制禁止策略

3.2.3 终端流量管理

对客户端访问外部子网的流量进行统计与限制，实时统计全网内各客户端访问流量的排名。

3.2.3.1 流量访问策略配置

① 在控制端提供 TAB 页面，对终端/终端组（可通过 IP 地址、IP 区间、子网对应）访问目标网络或目标服务器（可通过 IP 地址、IP 区间、子网对应）的网络流量（速率）上限进行配置（最小单位：KBps）。

② 此配置作为策略下发至各个终端。

3.2.3.2 终端访问流量计数

② 终端在网络层统计各自访问的流量，包括：

- ✧ 该终端的总体访问流量速率。
- ✧ 对特定目标主机的访问流量速率。
- ✧ 对特定子网的访问流量速率。

④ 终端将各自的流量统计数据上报至管理控制中心。

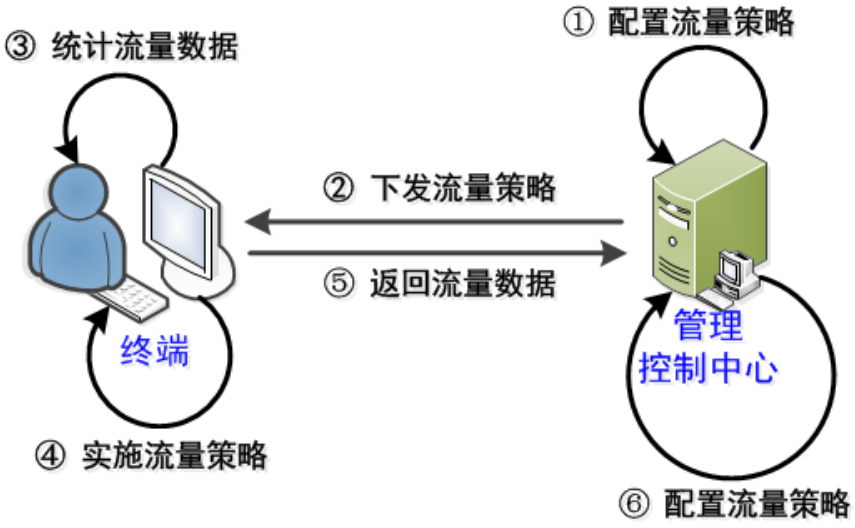
3.2.3.3 终端访问流量控制

⑤ 根据管理控制台为该终端下发的流量控制策略与终端统计出的当前的访问流量，对该终端的流量速率进行整形限制，注意，此处需要根据流量访问策略区分如下三种情况进行流量限制：

- ✧ 对该终端的总体访问流量速率进行整形限制。
- ✧ 对该终端与特定目标主机的之间的通信流量速率进行整形限制。
- ✧ 对该终端与特定子网的通信流量速率进行整形限制。

全网流量统计排名

⑥ 管理控制中心对所有终端上报的流量速率数据进行实时排名刷新，采取 do-by-need 的方式，在用户请求排名的时候，实时计算最新的流量速率的排名列表。



3.2.4 硬件资产管理

支持跟踪硬件资产变更情况，可帮助管理员及时获取硬件资产的变更记录，硬件新增、丢失情况，对硬件变更准确监控，及时预警，方便财务审计，轻松构建专业的企业硬件资产监控与审计平台。

3.2.5 终端 Agent 强制安装与运行

终端 Agent 一旦安装之后，便强制运行，不允许终止 Agent 进程的运行，并且默认情况下不允许卸载，即不能手工卸载 Agent 程序，也不允许第三方工具对 Agent 程序进行删除，如必须卸载 Agent 软件，必须提供卸载密码。

防卸载：天擎终端 Agent 通过在卸载程序 uninstaller.exe 加入了密码验证的逻

辑，要求在卸载过程中必须提供管理员密码，如果密码不正确，则卸载程序 uninstaller.exe 将拒绝执行卸载操作。

防终止：天擎终端 Agent 通过截获窗体的 Windows 消息，获得用户发出的终止 Agent 进程的消息，通过改写 OnExit()函数，在其中加入验证逻辑，改变进程退出的标准路径，以此防止 Agent 被非法终止。

3.3 XP 安全加固

本次引入的 360 终端安全管理系统提供 XP 有效防护功能，可解决 XXXXP 终端的安全隐患问题。

3.3.1 实力保障

2014 年 7 月 31 日，由中国网络空间安全协会(筹) 竞评演练工作组主办的“XP 靶场挑战赛”落下帷幕。此次共有 5 家企业的产品成为靶标，在 300 余名顶尖黑客 12 小时的猛攻之下，奇虎 360 公司的 XP 防护产品再次经受住了严苛的考验，成功胜出。至此，360 已经在国内外组织的有关 XP 防护产品的七次挑战赛及测评中全部胜出，成为实至名归的“七冠王”，彰显了奇虎 360 公司在安全领域特别是 XP 防护领域的绝对实力。

3.3.2 总体描述

根据设计原则的要求，奇虎 360 公司采用了多层防护、标本兼治、技术与安全管理策略相结合的整体设计思路，在 Windows XP 系统之上由内到外采用了四层防护手段，包含了加固、修复、隔离、安全策略自动化等多项举措：

- 系统加固（核心手段）
- 热补丁修复
- 危险应用隔离
- “非白即黑”安全策略

图 3 XP 整体防护示意图

3.3.2.1 系统加固

XP 系统的安全问题从本质上来说是操作系统设计的缺陷，只有从根本上解决 XP 系统设计机制上的缺陷，才能彻底解决问题。目前微软已经清楚地认识到了问题的存在，并逐步在高版本操作系统上（如 Windows7、Windows8）开始尝试加固，但由于 XP 系统已经发布超过 10 年，最新的安全加固成果未能体现在 XP 系统之中。“360XP 加固版”的最大优势即在于将 XP 系统中的安全机制补齐，使 XP 系统在不升级到高版本操作系统的情况下，也拥有同样健全的安全防护机制。

3.3.2.2 热补丁修复

热补丁技术通过替换内存中存在漏洞的可执行代码，在系统底层对 XP 漏洞实施精确的“外科手术”，彻底根除漏洞病灶。热补丁修复技术无需重启系统，可以在系统持续运行的状态下实施“手术”，正因如此，这种修复方式需要有对 XP 系统底层架构和代码有非常深刻的了解，同时也需要有多次成功实施“手术”的“临床经验”，否则极易造成系统的崩溃而影响业务正常运行。

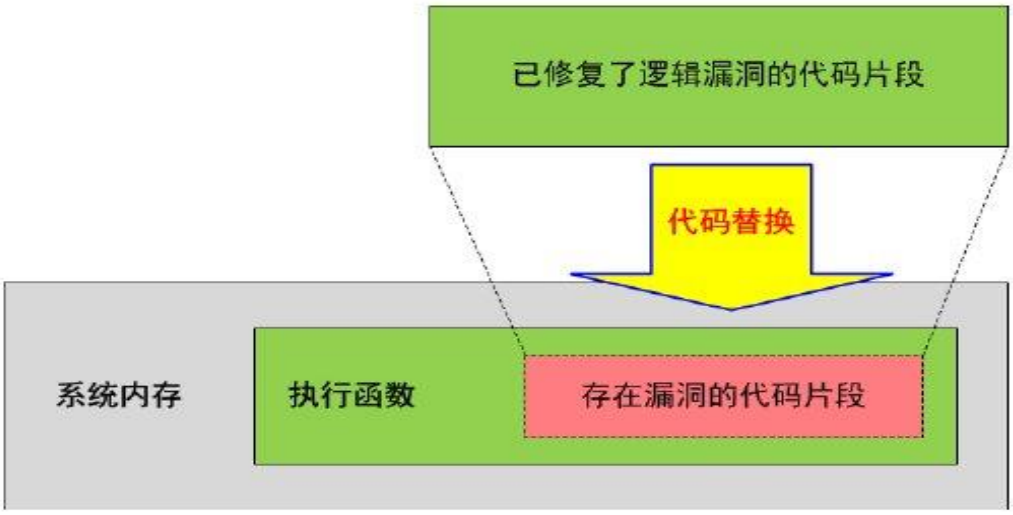


图 4 热补丁修复逻辑示意图

- 3 奇虎 60 公司 20 次先于微软制作、发布热补丁，并在超过 4 亿终端上稳定运行，数据在国内安全厂商中遥遥领先；
- 仅 2013 年，奇虎 360 公司已独立挖掘 15 个微软高危漏洞，并受到微软官网致谢，数量超过其它安全厂商总和；
- 360 漏洞分析实验室研发了自动化漏洞挖掘技术，仅 2014 年 1 月即已挖掘出近 60 个微软漏洞。

3.3.2.3 危险应用隔离

通过长期跟踪发现，漏洞级安全威胁主要集中在少数应用之上（如 IE、Office 等），因此对这些危险应用的监控是解决漏洞安全问题的重要一环，奇虎 360 公司采用安全沙箱（Sandbox）的技术手段对这些危险应用的使用进行隔离，保证在这些应用遭受到攻击的情况下不会对宿主的 XP 系统产生安全威胁。

- IE 沙箱隔离：允许访问网络，限制访问本地资源；
- Office 沙箱隔离：允许访问本资源，限制访问网络。

3.3.2.4 “非白即黑”策略

“非白即黑”的安全策略采用 PE 文件白名单机制，依托于高纯度的 PE 文件白名单库，仅允许白名单库中的文件在系统中运行，而所有未在白名单库中的

PE 文件均被禁止在 XP 系统上加载、运行，这就能在理论上保证所有通过 XP 系统漏洞渗透进来的恶意代码均无法在 XP 系统上实现攻击。

3.4 统一运维功能

为了有效减轻终端运维工作量，天擎具有统一运维的功能，并提供日常电脑维护小工具，方便 IT 维护人员快速完成工作。

3.4.1 系统自动升级

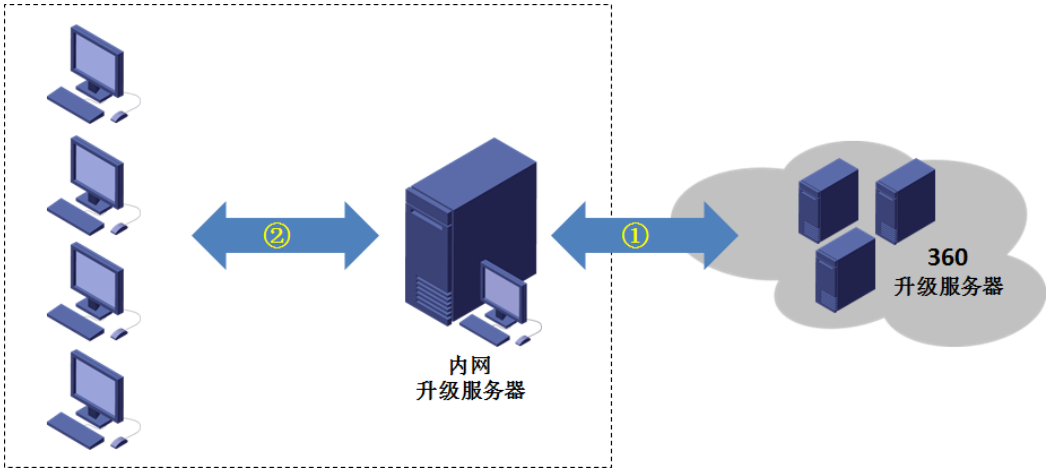
在无须运维管理人员参与的情况下，对天擎客户端软件、360 管理控制台软件、天擎客户端病毒特征库、系统/应用的漏洞补丁进行自动下载、升级与安装。

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。

当天擎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，天擎 360 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。

内网推送式升级一共分两个阶段：

- 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：天擎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。

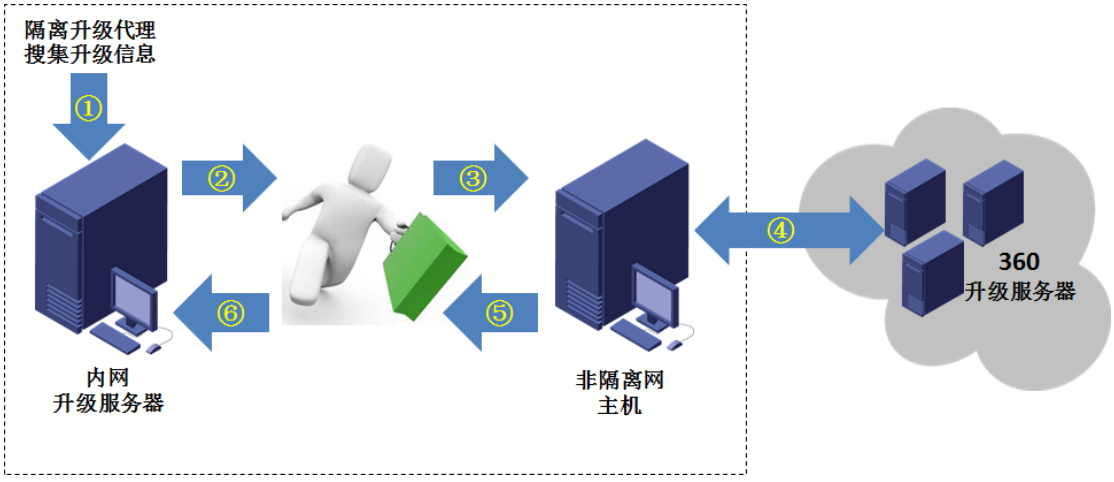


对于隔离网环境来说，由于内网升级服务器无法连接至 360 升级服务器，因此无法直接完成升级文件的下载，在这种情况下，我们提供了“隔离升级代理”工具完成升级文件的下在工作，具体升级过程如下：

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。



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，天擎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。

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

- 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。

3.4.2 软件分发

管理控制台可以对指定终端（或终端群组）强制推送软件，被推送的终端无法选择是否接收被推送的软件，同时，被推送的软件到达终端之后，可以选择是否立即安装。

- ✓ 控制端可以选择推动的终端（通过 UserID、IP、网段、IP 区间）。
- ✓ 推动可以选择定时进行。
- ✓ 推送过程中压缩传输。
- ✓ 可以指定推送后的存储位置（存储路径）。
- ✓ 可以指定推送过程总带宽上限。
- ✓ 可以指定推送后是否立即安装。

3.4.3 文件管理

天擎提供的文件管理功能，可实时审计全网 PE 文件（可移植的执行文件），及时追踪内网中的可疑文件。此外，文件管理功能允许 XXX 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，支持文件名、MD5、证书签名等方式识别文件。

3.4.4 终端小工具

为 IT 运维人员提供灵活易用的终端管理与优化工具，方便管理员快速处理终端问题，提高终端管理的运维效率。

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

集成 360 安全卫士的终端安全管理工具。

XXX 软件商店	管理员在管理端上传终端所需的办公软件，终端可以点击下载并安装
开机加速	对开机启动项进行管理，优化开机速度
系统垃圾清理	清理系统临时文件缓存与 IE 临时文件缓存
硬件信息查看器	查看硬件物理信息与状态信息
网络查看器	查看网络的状态

3.4.5 远程协助功能

天擎提供按需支援远程协助功能可对 XXX 网内需要帮助的计算机终端进行远程维护操作，帮助远程计算机终端进行异地操作和检查系统问题，充分发挥与共享信息中心的技术优势，为信息中心节省普通终端故障处理时间、提高运维服务的效率，达到成本与服务质量的双重效益。

3.5 符合等级保护要求

采用天擎控制中心进行所有终端的特征码升级、特征码版本监控、统一防护策略管理，满足等级保护要求。

3.5.1 策略下发

策略管理的目的是对包括外设、流量、应用等控制对象下发控制策略，具体要求可以按照 UserID、IP、部门、子网、IP 范围、设备分组等进行策略制定。根据项目要求，我们在方案中设计了三维策略控制体系：

- 时间

在什么时间段内实施控制，即控制生效。

- 对象

  对什么对象实施控制（用户（UserID）、服务器设备（IP）、部门、子网、IP 范围、应用、流量、其他）。

- 控制内容

  对象的控制范围的具体值（应用是否可以按装、终端是否能够准入、流量的具体限流值）。

在策略下发的时候，将根据控制对象进行定点推送，与策略无关的非受控对象不会收到所推动的策略。

3.5.2 终端版本统一监控

统计终端上的系统信息与软件信息，为管理员管理系统提供详尽的依据，同时根据所搜集到的终端信息生成报表。

操作系统	Windows 操作系统的版本、补丁信息
Office	Office 的版本、补丁信息
浏览器	IE 浏览器的版本、补丁信息
防病毒软件	防病毒软件的版本、补丁信息

3.6 方案优势

3.6.1 完善的终端安全防御体系

- **立体布防，层层防御（空间维度）**

天擎本身具有终端安全防御，云端公有/私有云查杀的功能特性，如果与 360 的另一款产品天眼威胁感知系统（部署在网络边界）相结合，便可以构成“云 + 端 + 边界”的整体防御体系。通过在网络边界、终端系统部署查杀设备与查杀软件，同时结合云端查杀的多点立体布防，可实现对已知病毒及恶意代码、未知病毒及恶意代码、利用已知漏洞和 0day 漏洞（未知漏洞）发起的攻击渗透、乃至利用上述技术手段发起的 APT 攻击行为进行深度检测与精确阻断。从空间维度上做到立体布防，层层防御。

- **动静结合、全程查杀（时间维度）**

天擎终端安全管理系统采用动静结合的多层次、全生命周期的病毒防御体系。结合了传统本地查杀引擎、360 公有云查杀引擎、QVM-II 机器学习查杀引擎、主动防御技术、沙箱技术、非白即黑的白名单策略等高级病毒查杀与防御技术，对病毒及恶意代码从进入网络、终端落地、运行时等生命周期的不同阶段进行多层过滤、动静结合、全程查杀。

3.6.2 强大的终端安全管理能力

天擎终端安全管理系统集成了强大的终端安全管理功能，可以方便用户通过天擎终端安全管理系统对内网终端进行高效管理。通过 360 在桌面管理方面的多年积累与沉淀，天擎可以提供补丁分发、终端流量管理、终端系统优化、终端系统加速、终端垃圾清理、终端蓝屏修复、终端硬件资产与状态监控、终端体检、终端升级、终端系统修复、终端软件管理、企业级软件商店等几十个安全管理功能，使系统具备国际一流的终端安全管理水平。上述功能每天被国内超过 4 亿用户使用，通过了稳定性、性能方面的全面考验，并在持续不断的进行创新与改进。

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

3.6.3 良好的用户体验与易用性

得益于互联网行业的企业基因，360 的所有产品在产品易用性与用户体验方面得到了国内个人用户以及企业用户的一致认可，天擎终端安全管理系统在产品易用性方面要求极其苛刻，绝大多数功能设计都要求一键完成，包括：一键加速、一键清理、一键修复、一键升级、一键体检等等，具备灵活的分组管理，批量策略下发、分时扫描、终端强制控制、软件静默安装、一对一远程协助等易用功能，从产品设计到开发过程中全面贴合企业及管理员的安全管理需求，最大程度降低用户安全管理运维成本，提高用户的工作效率。

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

第四章 非功能性设计

4.1 系统兼容性

支持多种版本 Windows 操作系统、linux 操作系统，包括：

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

redhat，centos 6.2 及以上版本（32 位 & 64 位）

管理架构：B/S

4.2 硬件平台要求

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

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

4.3 系统容灾

在网络瘫痪无法接入网络的情况下终端仍能够正常脱网工作进行正常的病毒查杀。

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，天擎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：

- 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。

4.4 虚拟化支持

支持虚拟化服务器的运行，保证虚拟化服务器终端能够进行正常的病毒查杀。

为了方便服务器的操作和管理，XXX 对于部分服务器采用 VMware 虚拟化技术，天擎采用了虚拟机支持和与 VMware 深度合作的方案，保证了其可以在不影响虚拟机上高效稳定地运行效率的同时有效地进行杀毒的工作。

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

- 虚拟机支持

  天擎的控制中心和客户端均支持在虚拟机上运行，对于虚拟机的支持度较好，对虚拟机本身的影响较小。

- VMware 深度合作

  为进一步降低对虚拟机性能的影响和提高虚拟化服务器的安全水平，奇虎 360 公司正在和 VMware 公司开展深度合作，在 Hypervisor 层加强对于虚拟化服务器的防护。

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

第五章 部署实施

（根据实际情况修改部署拓扑图，参照技术白皮书）

XXX 内网与互联网隔离，需要在内网部署一台天擎控制中心，将天擎私有云平台接入内网并做好相应配置，在所有内网终端上安装天擎客户端代理，在办公网安装隔离网升级工具，定期从 360 相关的服务器下载病毒库、木马库、漏洞补丁文件等，更新到控制中心后，所有天擎终端都可以自动升级和修复漏洞。由专人负责控制中心的日常运行，定时查看各终端的安全情况，下发统一杀毒、漏洞修复等策略。本次天擎部署拓扑示意图如下：

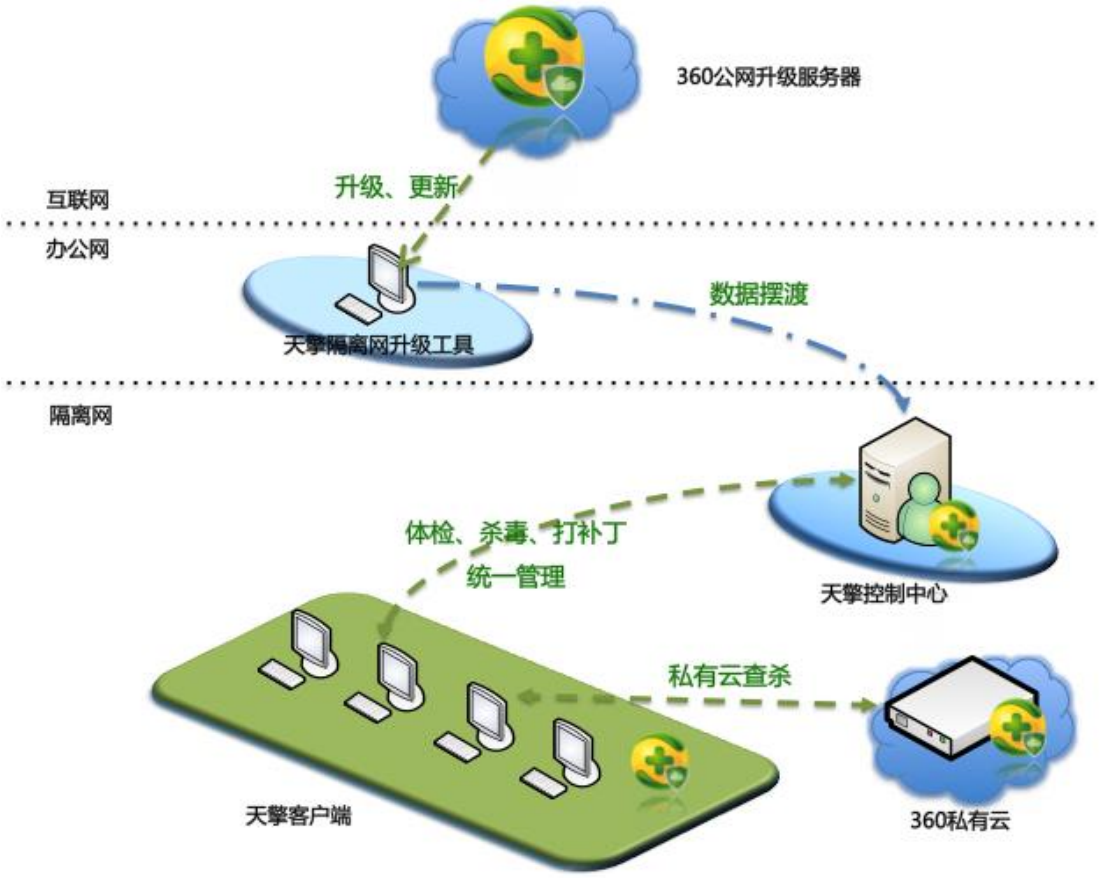


图 5 部署拓扑图

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

部署过程

1、安装天擎控制中心。

2、安装私有云平台（硬件）。

3、部署天擎终端。

4、定时登录控制中心，查看各终端安全情况。

5、发统一杀毒、修复漏洞等策略，确保终端安全。

6、定期使用隔离网工具下载数据，并更新到控制中心。

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

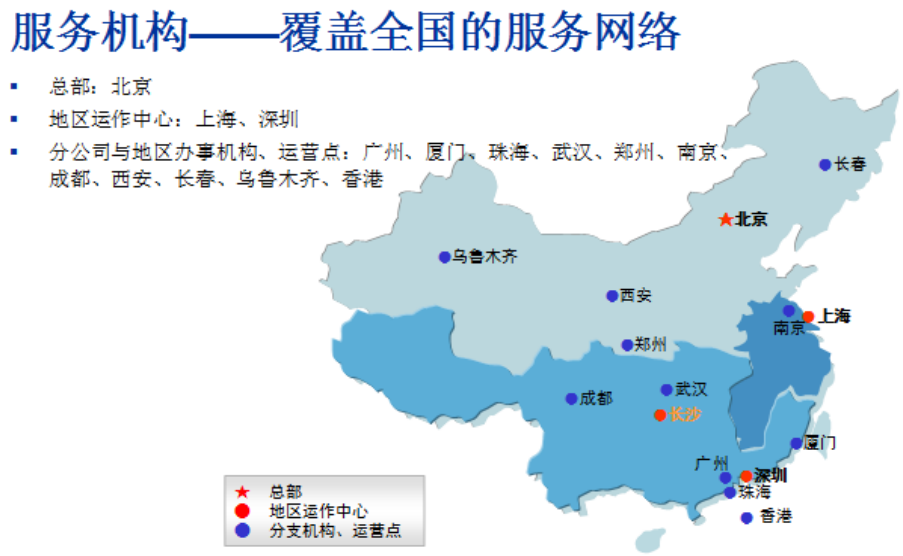
第六章 售后维护服务

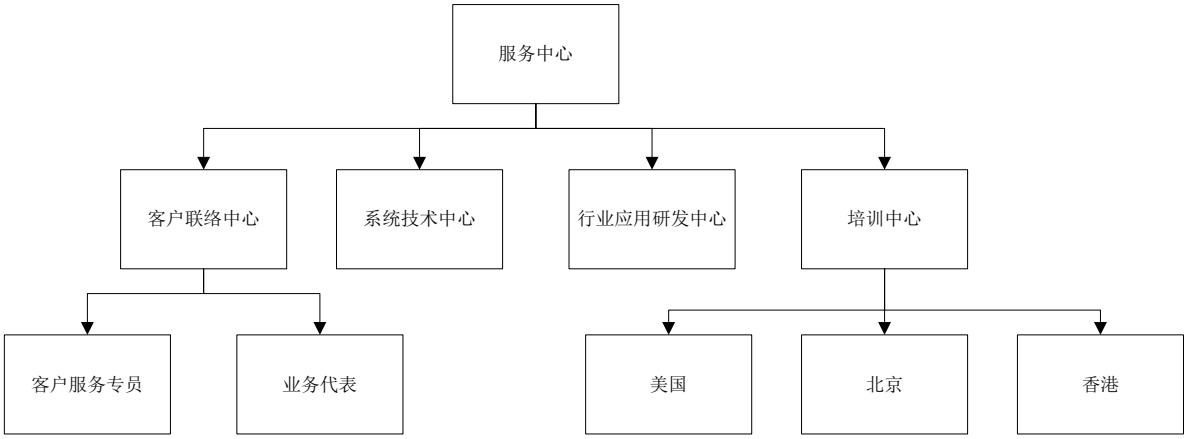
6.1 售后服务组织机构-客户服务中心

360 的技术支持服务体系是“双轨、三层”的以面向客户的客户服务中心、技术中心为主体，其他部门配合的一体化的技术支持体系。由设置在北京总部的客户服务中心和遍布全国的技术支持队伍共同完成技术服务。客户服务中心统一受理客户的各种请求，并根据客户的请求及时安排合适的工程师响应用户请求并解决问题。

客户服务中心负责所有用户的投诉申报、建议和故障请求的接受、记录、跟踪。为保证客户的请求能够及时响应和处理，客户服务专员根据故障处理流程，及时反映和上报相关人员。同时定期或不定期进行主题电话访问，主动发现并解决问题。

为确保技术体系和服务体系有效配合，由 360 首席技术长官 CTO 作为技术服务体系的总负责人，负责整个公司的技术发展规划，技术方向、技术产品的总体设计；协调客户服务部、技术、应用中心和商务部，以及 360 所有可以调用的资源为客户提供服务支持；并对客户重大故障的处理和协调。360 科技集团的技术支持服务体系的组织结构如下：





360 客户服务专员以及项目经理。客户服务专业的职责是定期查询、跟踪、收集、反馈客户系统运行的信息，收集客户服务意见和服务文档；项目经理的职责是在系统建设中和保修期内响应、落实、督查客户技术服务的要求，代表 360 兑现技术服务的承诺。从售前、售中和售后三个层面为客户提供全方位服务。

服务经理

- 制定 360 客户服务的规范；
- 制定重点客户的专门服务措施；
- 对客户重大故障的处理和协调；
- 处理客户的建议和投诉；

- 协调与公司其它部门之间的关系。

服务专员

- 负责按星级管理建立客户档案
- 负责接收和记录来自客户或其它方面的技术支持请求；
- 负责向客户征求意见，及时传达公司对客户的关怀；
- 负责接收和记录来自客户或其它方面的建议、投诉；
- 监督技术支持人员及时响应支持请求，及时解决问题和故障；
- 记录问题和故障处理结果，并存入客户档案；
- 接收技术支持人员的维修请求。

6.2 售后服务内容

奇虎 360 公司根据项目合同的具体约定，将提供如下相关的服务内容：

- 系统的优化服务；
- 系统的故障排除服务；
- 系统升级改造的咨询服务；
- 系统的需求变更服务；
- 多体系的技术培训服务。

6.3 售后服务手段

奇虎 360 公司提供的售后服务手段包括：

现场服务：可根据用户的实际需要提供现场服务，维护工程师可在与客户约定的时间内到达客户现场。

远程支持：在客户许可的情况下，360 工程师可通过远程实施服务。

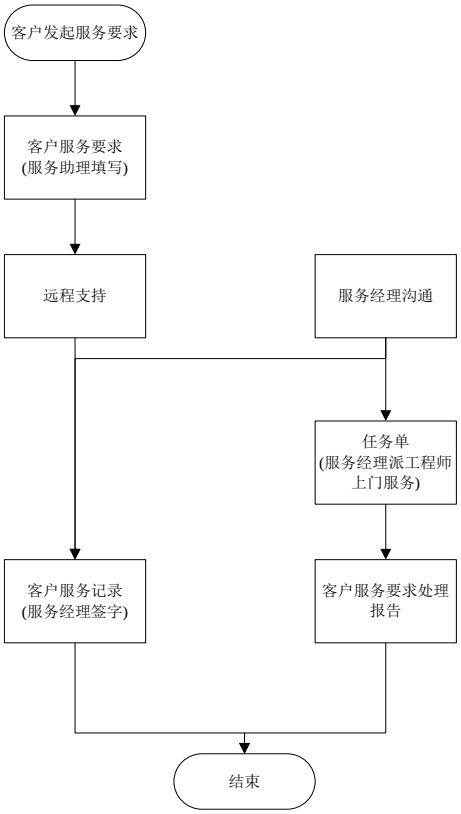
电话支援服务：如客户有任何有关于合约中所涵盖的系统技术问题，可随时

（7×24 小时）拨打 360 的服务电话，360 工程师将通过电话协助客户及时解决难题。

备机服务：当发生特别故障，致使维修时间超过客户可接受程度时，我们可以根据实际业务需求提供能支撑客户系统运行的备用设备，以保证客户的生产不受影响。

6.4 售后服务流程

工作程序：



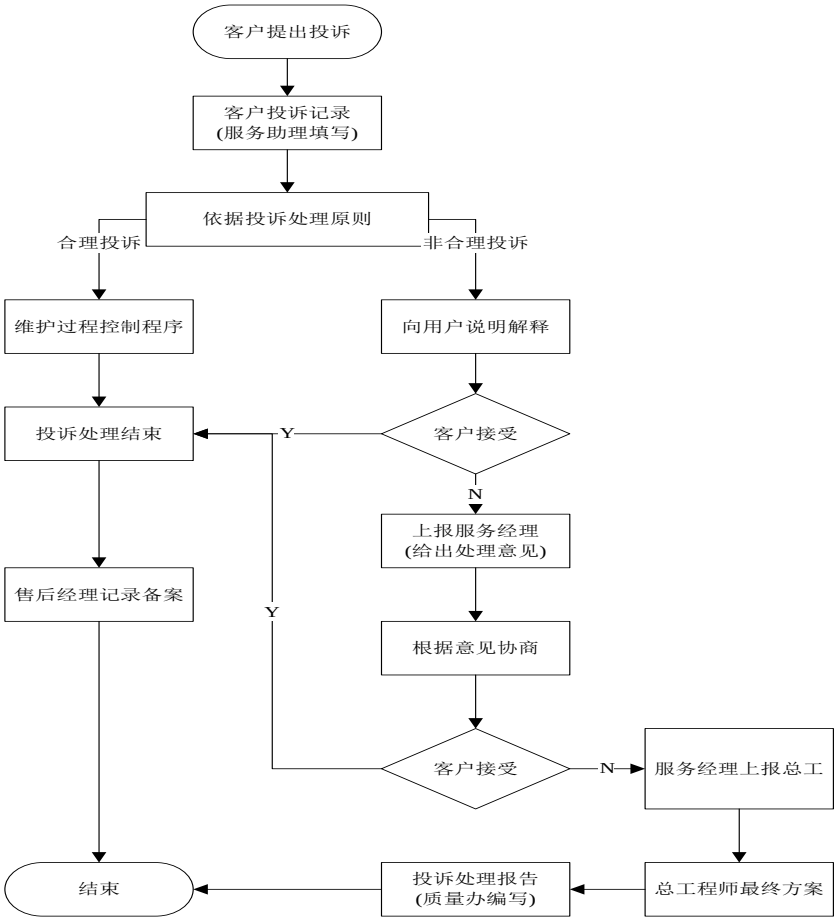
客户服务请求处理程序

在接到客户的服务请求后，应在《客户维护请求记录》上详细记录客户系统发生的问题、时间、严重性。如是一般问题，能够在电话中解决的要及时解决，或通过 Email 或远程登录访问服务解决，解决完毕应及时向售后服务经理汇报，由售后服务经理在《客户维护请求记录》上签字确认；如不能解决则与售后服务

经理或该项目经理沟通，再不能解决则填写《维护任务单》，由工程服务部指派工程师采取上门维护予以解决，具体过程执行《维护过程控制程序》。

以上工作将在二个工作日内完成。

客户投诉意见处理程序



在接到用户投诉的半个工作日内与客户及有关负责部门进行沟通，明确客户投诉的重点和要求，详细了解事情的经过，作好《客户投诉记录》，并安抚客户，向客户说明公司会尽快调查处理，并主动与客户联系。

在处理过程中，依据《投诉处理原则》判断客户要求是否合理，若客户提出的要求正常合理，则按《维护过程控制程序》执行。

当客户提出的要求不合理或不符合公司规定时，服务助理（热线员）需向客户说明公司对此类问题正常处理程序，讲解公司服务政策，与客户协商，寻求其它解决办法。

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

经协商，客户接受服务助理（热线员）的解决方案，则投诉处理工作可结案，按公司有关规定进行办理，并报售后服务经理，记录备案。

协商后客户对所提的处理方案不接受，服务助理（热线员）则上报售后服务经理。

工程服务部经理接到服务助理（热线员）报来的《客户投诉记录》后，根据具体情况提出处理意见，并形成处理方案。

服务助理（热线员）将处理方案与客户进行协商，若客户同意，则将处理结果报售后服务经理备案，处理过程执行《维护过程控制程序》。

若客户对处理方案不接受，则由服务助理（热线员）通知售后服务经理并上报公司领导。

以上工作必须在二个工作日内完成。

公司领导在接到未结案的重大投诉后，要对事情经过和处理意见和过程详细了解并拿出最终处理方案与客户协商，原则上按此处理，不再提出新的处理意见。

工程服务部服务助理应将处理结果记录在案，上述工作必须在三个工作日内完成，质量办公室对上述工作进行抽检并形成《投诉处理总结报告》。

客户满意度调查

质量办公室根据服务工作的要求制定《客户满意度调查表》。

质量办公室每年六月和十二月组织向有关用户发出《客户满意度调查表》或电话询问。

收回调查表后，由质量办公室进行汇总分析后编写《客户满意度调查分析报告》作为管理评审输入之一。

必要时每年年终由管理者代表组织售后服务部，质量办公室对用户进行回访，并形成回访报告。

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

6.5 顾客档案管理-服务管理系统

360 设有专业的服务管理系统，能自动跟踪处理并记录技术服务的全过程，确保客户得到及时有效的服务，服务管理系统可处理以下内容：

客户信息

客户的系统硬件系统配置及网络环境记录

客户的应用系统架构体系和应用功能记录

服务事件记录（一个事件 CASE 从开始 Open 到结束 Close 的全过程）

客户投诉及处理记录

客户满意度调查记录及统计

客户回访记录

客户建议

6.6 服务响应时间

故障级别	故障现象	响应速度	到达现场时间	执行响应人
一级	由于硬件或系统软件的原因造成系统停机，整个系统处于瘫痪状态，不能正常运行对客户的业务运作造成严影响。	1 小时	4 小时	资深工程师
二级	现有系统的性能严重降级，或由于系统性能失常严重影响客户部分业务运作。	2 小时	8 小时	资深工程师
三级	系统部分设备或者软件出现故障，系统的性能受损，但大部分业务运作仍可正常工作。	4 小时	12 小时	工程师

故障级别	故障现象	响应速度	到达现场时间	执行响应人
四级	客户需要硬件、软件产品功能、安装或配置方面的信息或支援。对客户的业务运作几乎没有影响或根本没有影响。	8 小时	24 小时	工程师

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

第七章 效益分析

7.1 安全源自实践，安全不只合规

天擎稳定可靠的运行于 360 公司自身网络中，每天接受大量网络攻击的实战检验；天擎采用的双杀毒引擎、云查杀引擎、恶意 URL 检测引擎、QVM-II 人工智能引擎及“非白即黑”策略等技术均来自于超过 5 亿 360 用户终端安全防御的最佳实践，这些技术的组合应用能够真正帮助 XXX 发现网络攻击、解决计算机安全问题，使安全再也不仅仅是合规，使 XXX 的安全投入物有所值。

7.2 持续安全升级，力助系统过渡

目前 XXX 仍有大量 XP 系统的计算机，天擎支持对 XP 系统漏洞的持续挖掘和修复，具备 XP 系统多项安全加固功能，可以帮助 XXX 安全度过操作系统的升级、替换期。

7.3 强大管理能力，提高运维效率

天擎具有丰富的管理功能，友好的用户界面，人性化的统计报表，极大的提高了 XXX 计算机安全管理的效率，使 XXX 轻松完成跨区域的计算机管理及运维工作。

7.4 自主知识产权，杜绝后门隐患

天擎具有完全自主的知识产权，是中国自己的国际一流杀毒软件和终端安全管理系统，能够帮助 XXX 对网络进行安全管控和安全加固，杜绝安全后门隐患，响应国家信息安全国产化政策及号召。

北京朝阳区酒仙桥路 6 号院 2 号楼 邮编: 100015
电话: +86 10 5682 2690 传真: +86 10 5682 2000

第八章 产品配置清单

序号	名称	项目说明	数量
1	360 天擎终端安全管理系统	包括：服务器管理端系统、管理控制台、客户端系统； 提供满足 XXX 系统 800 个客户端的应用；	1 套
2	360 私有云平台	包括：天擎私有云平台（专有硬件），标准 1U 上架设备	1 台
3	5*8 小时服务	提供原厂 5*8 小时服务响应 可疑病毒威胁检测 专用病毒码制作	1 年
4	技术服务包	系统实施服务 应用培训服务	1 项
		定期巡检 紧急上门支持 软件版本升级和人工服务	1 年