360 天擎终端安全管理系统

产品白皮书

目录

一. 引言

随着 IT 技术的飞速发展以及互联网的广泛普及，各级政府机构、组织、企事业单位都分别建立了网络信息系统。与此同时各种木马、病毒、0day 漏洞，以及类似 APT 攻击这种新型的攻击手段也日渐增多，传统的病毒防御技术以及安全管理手段已经无法满足现阶段网络安全的需要，主要突出表现在如下几个方面：

1.1、终端木马、病毒问题严重

目前很多企事业单位缺乏必要的企业级安全软件，导致终端木马、病毒泛滥，而且由于终端处于企业局域网内，造成交叉感染现象严重，很难彻底清除某些感染性较强的病毒。这类病毒、木马会导致终端运行效率降低，对文件进行破坏，或者会把一些敏感信息泄露出去。

同时，很多企业网络安全缺乏统一的安全管理，企业内部终端用户安装的安全软件各不相同，参差不齐，导致安全管理员很难做到统一的安全策略下发及执行。

1.2、无法有效应对 APT 攻击的威胁

APT（Advanced Persistent Threat）攻击是一类特定的攻击，为了获取某个组织甚至是国家的重要信息，有针对性的进行的一系列攻击行为的整个过程。APT 攻击利用了多种攻击手段，包括各种最先进的黑客技术和社会工程学方法，一步一步的获取进入组织内部的权限。APT 往往利用组织内部的人员作为攻击跳板。有时候，攻击者会针对被攻击对象编写专门的攻击程序，而非使用一些通用的攻击代码。

此外，APT 攻击具有持续性，有的甚至长达数年。这种持续体现在攻击者不断尝试各种攻击手段，以及在渗透到网络内部后长期蛰伏，不断收集各种信息，直到收集到重要情报。

更加危险的是，这些新型的攻击和威胁主要就针对国家重要的基础设施和单位进行，包括能源、电力、金融、国防等关系到国计民生，或者是国家核心利益的网络基础设施。

同时，很多攻击行为都会利用 0day 漏洞进行网络渗透和攻击。此时由于没有现成的样本，所以传统的基于特征检测的入侵防御系统，以及很多企业的安全控管措施和理念已经很难有效应对 0day 漏洞以及 APT 攻击的威胁了。

1.3、违规终端接入问题严重

企业的内网往往承载着企业重要信息的传递，存储着大量的企业财务、客户、人力资源等信息，这些都是企业需要重点保护的核心资产。但由于很多企业对于终端准入并没有做限制，私人 PC 或外来终端设备可以轻易的接入企业内网获取企业内部信息。尤其在当今网络无边界的趋势之下，通过私设无线路由，手机、Pad 等移动终端也可以轻松的接入企业内网。同时，由于缺乏统一的管控和审计，如果发生企业信息泄露，很难做到追踪溯源。这对于企业数据安全是极大的危害。

1.4、企业终端违规软件难以管控

企业员工在企业终端上私自安装的盗版软件、来源不明的下载软件很可能被黑客植入病毒或木马，用以窃取企业内部信息或导致企业 IT 系统崩溃。另外，很多企业规定员工不得安装某些违规软件，例如聊天软件、P2P 软件等，但却无法进行管控，私装现象严重。并且企业没有量身定制的自定义软件商店，无法保证软件的下载来源可靠。

1.5、终端漏洞不能及时修复

黑客攻击和大部分病毒都会利用到操作系统和一些常用软件的漏洞。而计算机操作人员对操作系统漏洞的补丁修复意识淡薄，很多人根本不知道自己的系统存在漏洞并应及时安装补丁，这为病毒的广泛生存提供了温床，就使网络内的设备安全受到很大的威胁。

如果企业使用单机版的安全软件修复漏洞，就只能靠管理员逐台电脑打补丁，不仅耗费管理员的时间，还大量占用企业网络的带宽和设备资源，企业信息网络的正常运行受到极大的影响。

要确保及时的修复漏洞，不被木马和病毒利用，同时又要确保合理有效的使用带宽资源，就需要安全软件能够帮助管理员进行统一的漏洞管理和集中修复。

1.6、终端安全状况需要统一管控

如果一个企业缺乏统一的终端安全管理，就无法全面了解和监控企业内网安全状况，一旦终端被感染病毒威胁或遭受恶意入侵，网络管理员很难及时发现并解决问题；某个终端不安全的配置和策略会导致企业网络中出现漏洞，从而成为整个网络安全中的短板。

假如有企业内部员工使用从外部网络中下载的文件，而这些文件又被植入了病毒或木马，黑客就极有可能通过该主机进入企业内部网络，进而通过嗅探、破解密码等方式对内部的关键信息或敏感数据进行收集，或以该主机为“跳板”对内部网络的其他主机进行攻击，影响企业的正常运行，甚至导致企业核心数据外泄。

监控终端面临病毒黑客攻击的状况，及时发现隐患并报警，统一正确配置安全策略，可以极大的提高整个企业网络安全的水平，避免短板出现。

针对以上问题，北京奇虎科技有限公司推出了 “360 天擎终端安全管理系统”（以下简称天擎），来为用户解决终端安全和统一管理等一系列安全需求。

二. 天擎终端安全管理系统介绍

2.1 产品概述

天擎是奇虎 360 面向政府、军队、金融、制造业、医疗、教育等大型企事业单位推出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。

2.1.1 设计理念

- **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，为企业构建立体防护网，确保企业终端安全。

- **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。

2.2 产品架构

天擎系统架构图

天擎终端安全管理系统包括安全控制中心和客户端两层。

第一层：安全控制中心

安全控制中心，是天擎的核心，部署在服务器端，有两大功能：

一方面提供了管理台，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。主要有设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、网络流量管理、终端软件管理、硬件资产管理以及各种报表和查询等。

另一方面，提供了系统运维的基础服务，如：云查杀服务、终端升级服务、数据服务、通讯服务等。

第二层：客户端

客户端部署在需要被保护的服务器或者终端，执行最终的木马病毒查杀、漏洞修复等安全操作。并与安全控制中心通信，提供控制中心管理所需的相关数据信息。

2.3 产品优势

360 天擎终端安全与管理系统的核心价值在于对终端安全的防护与管理。奇虎 360 公司经过多年的投入与积累，沉淀下了多项针对终端安全防御的技术，这些技术在整个安全行业领域内都具有独创性与先进性，多项技术已经达到国际一流水平，并领先其他欧美企业的同类产品。目前 360 杀毒软件是国内唯一包揽 AV-C、AV-TEST、VB100、CheckMark、ICSA、OPSWAT 等各大国际评测“全满贯”的杀毒软件。同时，360 公司的安全技术能力也得到了国内广大用户的认可，目前在个人安全领域 360 安全产品正在为超过 4.65 亿 PC 端用户、4.08 亿移动端用户提供安全防护。在企业安全领域，天擎已累计为国内 50 万家企业、近 800 万终端提供了安全防护及终端管理。

2.3.1 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）**

360 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。

2.3.2 强大的终端安全管理能力

360 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 360 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，360 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。

2.3.3 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，360 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。

2.3.4 顶尖的产品维护服务团队

为了给客户提供有保障的可靠服务，为用户切实解决安全问题，360 打造了一支顶尖的产品与安全服务团队，整个产品与安全服务团队采用金字塔形架构，共分三层：

第一层：产品远程支持、现场问题排查团队，这个团队人数众多，其中一对一服务就多达 400 人，7×24 小时待命，采取电话支持，登门服务等方式，为用户解决产品使用、配置方面的一般性问题。

第二层：技术工程师支持团队，这个团队人数将近 50 人，均为 360 天擎开发的各模块负责人、开发人员组成，这支团队主要对用户现场出现的各种由于产品 Bug 导致的产品问题进行现场代码级排查、定位与解决。

第三层：安全专家服务团队，这个团队人数大约 20 人，均由国内知名的安全研究人员、安全咨询专家组成，可以对用户现场发生的各种攻击行为进行现场应急处理、恢复与加固，并能对用户的安全建设提出合理化建议。

2.4 主要功能

2.4.1 安全趋势监控

支持全网一键体检，帮助管理员发现全网内漏洞、木马、插件、系统危险项、安全配置项、未知文件等的威胁数量和危险终端数量。

支持终端状况展现，帮助管理员对全网不健康终端、亚健康终端、健康终端进行统计。支持安全动态跟踪，帮助管理员了解全网内漏洞补丁的修复状况。

支持威胁趋势分析，帮助管理员全面了解企业内终端危险项、木马、病毒、漏洞、新增文件等的发展趋势。

2.4.2 安全运维管理

支持对终端升级、漏洞修复、木马查杀、插件清理、系统危险项等的全局管理以及分组管理，支持安全策略分组下发，帮助管理员管理复杂的多层次网络以及多部门组织架构。

支持一对一远程协助功能，终端用户可以直接向 360 客服求助，帮助管理员分担支持压力。

支持网络准入管理，禁止没有按要求安装天擎终端安全管理系统、存在安全问题的终端、或者外来非法终端接入企业网络，帮助管理员保证入网终端合规，防止非法终端入侵网络，给企业业务系统造成破坏。

同时，随着病毒的大量出现（360 公司的病毒库已达 60 亿），传统的本地病毒库已经过于庞大，甚至无法在本地加载绝大多数的病毒特征库，这严重地影响了终端性能和病毒检出率。天擎支持公有/私有云查杀技术，帮助管理员解决本地查杀的性能瓶颈，提高病毒检出率，减少误报率和漏报率。

2.4.3 终端流量管理

管理员可以了解各终端的网络流量情况，包括终端的实时网络速度、一段时间的下载上传流量等，同时支持对终端的上传及下载流量限制进行统一管控，帮助管理员管理网络流量，避免非法应用占用大量带宽，保证企业正常业务的平稳运行。

2.4.4 终端软件管理

支持提供适用于企业的自定义软件管家商店，软件商店中的所有软件都会经过严格的安全性测试及加固，企业可以任意添加自身的定制化软件产品，自定义软件黑白名单，终端用户可自由下载运行软件商店中的软件。帮助管理员保证企业内部软件的合规性和安全性。

支持软件的统一分组、定时分发，并可实现自动安装应用以及强制卸载应用，帮助管理员按照企业规定管理终端用户软件的安装。

支持查询全网终端的软件安装情况以及终端进程信息，帮助管理员及时发现违规软件及可疑应用。

2.4.5 硬件资产管理

支持硬件资产查询及展示，可帮助管理员实时查看企业全网终端电脑的硬件配置，包括CPU、内存、主板、硬盘、监视器、光驱、网卡、显卡、USB 接口等，便于掌握硬件资产情况。

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。

支持硬件准入管理，可帮助管理员对终端的 USB 存储设备进行可读写、只读和禁用权限设置，以及对光驱、1394、蓝牙、串口、并口、PCMCIA 卡、手机与平板、VPN 等其他外接设备进行禁用管理。

2.4.6 日志报表查询

支持对终端安全日志、漏洞修复、病毒日志、木马查杀、插件清除、系统危险项，安全配置、流量管理，文件及应用日志等的报表统计。能够从终端、全网、分组等多维度，以及图表、数据等多视图角度进行统计与展现，同进支持报表的导出及打印，帮助管理员对日常安全防护、安全运维工作进行分析评估，以及对安全工作进行总结汇报。

2.4.7 边界联动防御

天擎可以与 360 的边界防护设备——天眼威胁感知系统进行联动，借助 360 天眼的深度检测能力，结合 360 天擎在终端上的精确防御能力，实现对 PC 终端的攻击防御。

天眼威胁感知系统在检测出网络攻击行为之后，一方面会采用页面报警、邮件报警的方式对攻击行为进行实时报警，同时，天眼威胁感知系统还会将报警信息实时发送给部署在终端之上的天擎终端安全管理系统进行有效联动。天擎在接收到报警信息之后，会及时根据报警信息所提供的文件名称、五元组信息对攻击行为进行及时的隔离与阻断，实现“边界发现、终端防御”的深度发现与防御效果。

最后，天擎会将对攻击和文件的阻断与隔离结果实时反馈给天眼威胁感知系统，天眼威胁感知系统在接收到天擎终端安全与管理系统的反馈结果之后，修改天眼威胁感知系统的报警信息，加入“处理结果”更新防护规则，同时将本次攻击防御的处理结果分享给网内其它控制中心和终端，以提高全网的安全防护能力，完成对一次攻击及其报警的闭环防御流程。

2.5 典型部署

2.5.1 小型企业解决方案

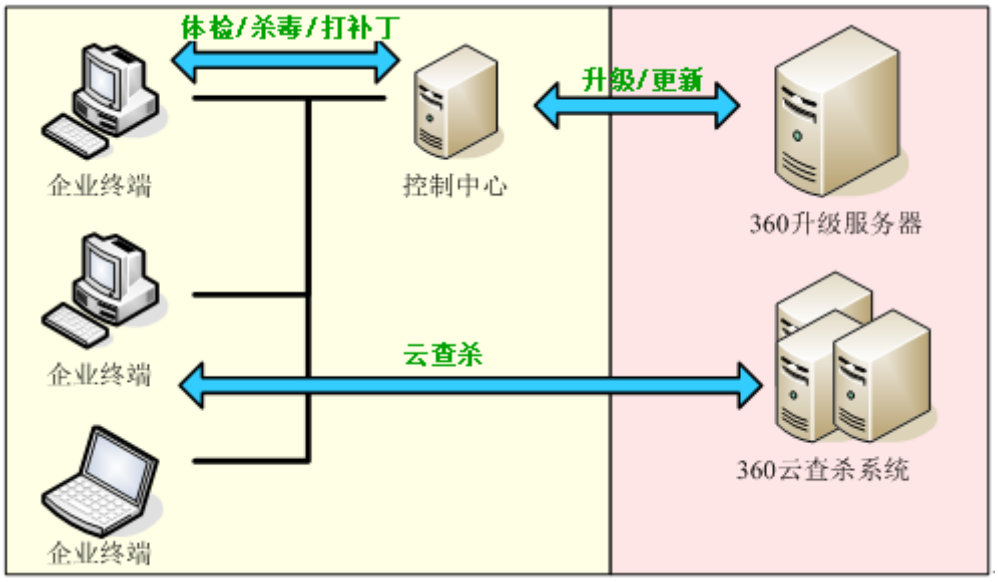
- **企业特点**

企业终端数较少，从几台到几十台不等，没有专职的网管或者安全管理员。网络方面管理体现为快捷方便，终端可以直接连接互联网，带宽有限。

- **管理目标**

无人值守，简单易用。

- **部署方案**



在企业内部部署天擎控制中心和终端，天擎终端通过控制中心连接到 360 的升级服务器进行升级、更新等，控制中心具有缓存功能，同样的数据文件只会下载一次，可以极大的节省企业总出口带宽。天擎终端根据控制中心制定的安全策略，进行体检、杀毒和修复漏洞等安全操作。进行杀毒扫描时，天擎终端可以直接连接 360 的云查杀系统，进行云查杀。

- **部署过程**

1、安装天擎控制中心。

2、部署天擎终端。

3、设置安全策略。

4、坐享企业安全。

2.5.2 中型企业解决方案（可联接互联网环境）

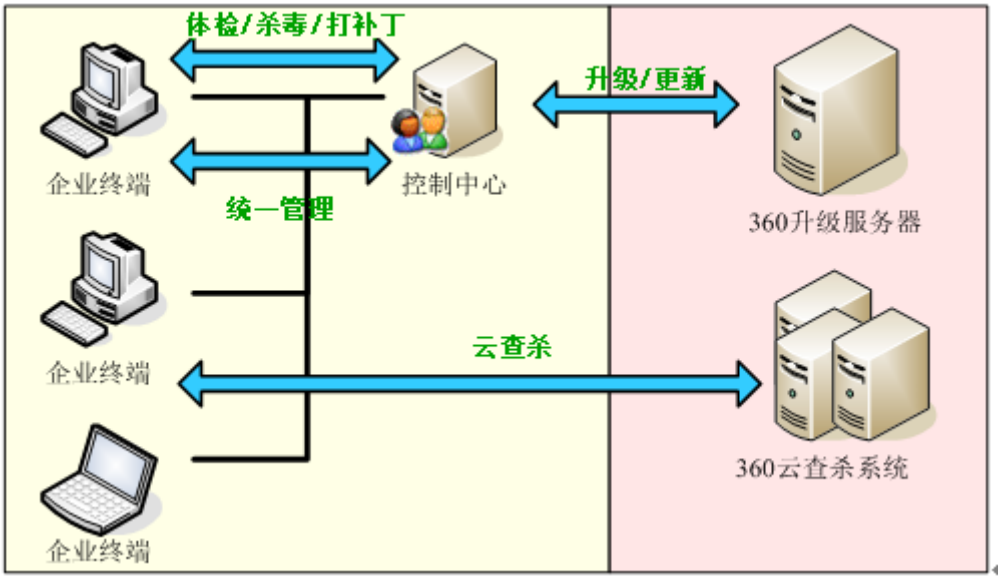
- **企业特点**

企业终端数规模从几十台到几百台不等，网络管理由于业务需求，允许终端上网。所有终端都集中在一个局域网内，有专门的网络管理员或者安全管理员。

- **管理目标**

方便管理，确保安全。

➢ **部署方案**



在企业内部部署天擎控制中心和终端，天擎终端通过控制中心连接到 360 的升级服务器进行升级、更新等，控制中心具有缓存功能，同样的数据文件只会下载一次，可以极大的节省企业总出口带宽。天擎终端根据控制中心制定的安全策略，进行体检、杀毒和修复漏洞等安全操作。进行杀毒扫描时，天擎终端可以直接连接 360 的云查杀系统，进行云查杀。

有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。

➢ **部署过程**

1、 安装天擎控制中心。

2、 部署天擎终端。

3、 定时登录控制中心，查看各终端安全情况。

4、 下发统一杀毒、修复漏洞等策略，确保终端安全。

2.5.3 中型企业解决方案（隔离网环境）

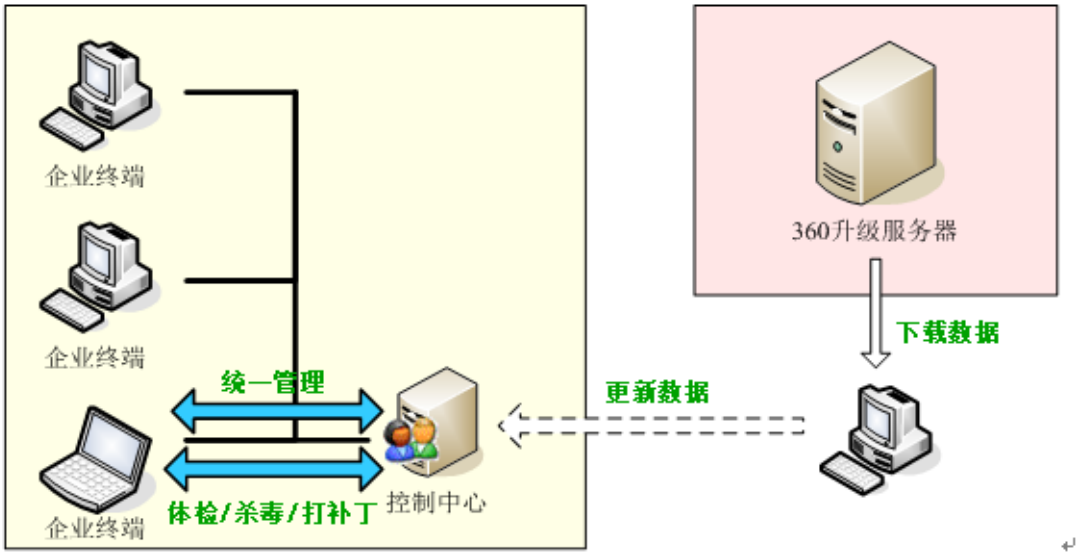
➢ **企业特点**

企业终端数规模从几十台到几百台不等，网络管理比较严格，不允许终端连接互联网。所有终端都集中在一个局域网内，有专门的网络管理员或者安全管理员。

➢ **管理目标**

方便管理，确保安全。

- **部署方案**



在企业内部部署天擎控制中心和终端，天擎终端根据控制中心制定的安全策略，进行体检、杀毒和修复漏洞等安全操作。

使用隔离网工具，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。

有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。

- **部署过程**

1、安装天擎控制中心。

2、部署天擎终端。

3、定时登录控制中心，查看各终端安全情况。

4、发统一杀毒、修复漏洞等策略，确保终端安全。

5、定期使用隔离网工具下载数据，并更新到控制中心。

2.5.4 大型企业解决方案

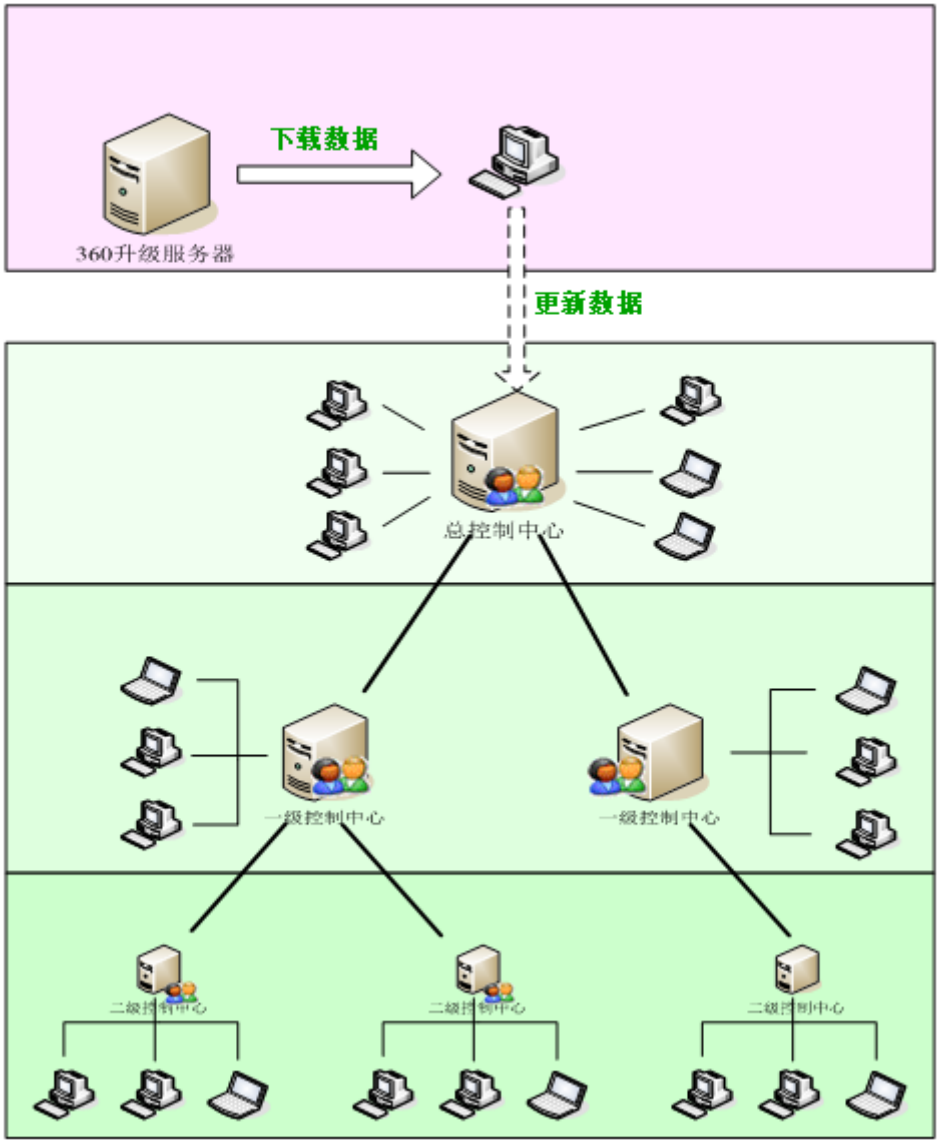
- **企业特点**

企业规模很大，一般会有几千、几万甚至几十万的终端，网络管理严格，不允许终端上网。终端分散在不同的区域，区域内部通过千兆或者百兆的局域网连接，区域和区域之间通过十兆级别的专线连接。每个区域都会配有的管理员。

- **管理目标**

专属服务，无限扩展。

- **部署方案**



在企业的核心区域，部署天擎总控制中心，在每个分区域，部署天擎分控制中心。分控制中心的上级指向到邻近自己的上级控制中心，以方便管理和节省网络带宽。每个区域的终

端，都指向自己区域的控制中心，并从控制中心接收管理指令，上报安全数据，进行病毒库、木马库升级和修复漏洞等。

使用隔离网工具，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，更新到总控制中心，各分控制中心会从总控制中心下载需要的升级文件和补丁文件，各区域的终端会从本区域的控制中心进行升级和下载补丁文件修复漏洞。

- **部署过程**

1、 安装部署规划，包括控制中心的分布，推广计划等。

2、 安装天擎总控制中心。

3、 部署核心区域天擎终端。

4、 根据推广计划，逐步在各区域部署分控制中心和终端。

5、 定时登录控制中心，查看各终端安全情况。

6、 定期使用隔离网工具下载数据，并更新到控制中心。

三. 产品价值

3.1 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，中国自己的国际一流杀毒软件和终端安全管理系统，能够帮助政府部门、涉密单位、以及关系国计民生的大型企业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。

3.2 解决安全问题，安全不只合规

天擎系统正稳定可靠运行于 360 公司自身网络中，每天接受大量网络攻击的实战检验，能够真正帮助企业发现网络攻击、解决安全问题，使安全再也不仅仅是合规，使企业的安全投入物有所值。

3.3 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，极大的提高了企业安全管理的效率，使企业安全管理信息和日志再也不会如天书般难懂。

3.4 灵活扩展能力，持续安全升级

天擎具备灵活的升级方案、可扩展的多级管理平台、集群化虚拟化的部署方式，以及支持对 XP 系统漏洞的持续挖掘和修复，可以帮助企业安全系统平滑升级，保护企业安全投资。

四. 服务支持

联系方式	服务内容	支持时间
电话支持	4008 136 360	7X24 小时响应
邮件支持	qiyeban-kefu@360.cn	24 小时内回复
QQ 支持	4008136360	24 小时内回复
求助中心	http://help.360.cn/	24 小时内回复
论坛支持	http://bbs.360.cn/5500002.html	24 小时内回复
微博支持	http://weibo.com/360wgb	24 小时内回复
飞信支持	18923391322	24 小时内回复
远程桌面	通过远程协助解决	24 小时内回复

如需更多专属服务或本地化服务请联系：010-5854 2764

五. 总结

天擎终端安全管理系统是奇虎 360 面向政府、军队、金融、制造业、医疗、教育等大型企事业单位推出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。天擎秉承信息收集、立体防护、集中管控的设计理念，具备完善的终端防御体系，强大的终端安全管理能力，良好的用户体验与易用性，顶尖的产品维护服务团队。能够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功能，为客户带来终端安全防护和管理的真正价值。