奇安信
新 一 代 网 络 安 全

天擎终端安全管理系统

产品白皮书

V6.0-R7

目录

1. 引言

随着云计算、大数据、人工智能技术的飞速发展，各级政府机构、组织、企业单位等建立了庞大而复杂的网络信息系统。与此同时，政企客户也构建了大量的防御措施，防火墙、入侵检测系统等边界网络安全产品可以解决信息系统一部分安全问题，但计算机终端的信息安全始终是整个网络信息系统安全的一个薄弱环节。

在客户网络中，大量计算机终端未部署有效的终端安全防护系统，造成内部网络木马、病毒、恶意软件肆虐，勒索、挖矿病毒横行；由于系统和软件的漏洞无法避免，以及终端安全管理手段的缺失，计算机对外暴露大量风险点，也给黑客入侵提供了便利；自主知识产权操作系统的缺乏，使得国内广大 XP、Win7 用户在停服后面临前所未有的挑战。除此之外，企事业单位内部网络与终端安全问题还包括：

- **终端病毒、木马问题严重，不能高效有序查杀；**
- **全网被动防御病毒、木马的传播与破坏，无法应对未知威胁；**
- **不能及时发现系统漏洞并进行补丁分发与自动修复；**
- **IT 资产不能精确统计，资产变动情况掌握滞后；**
- **终端单点维护依靠大量人工现场处理；**
- **未经认证的 U 盘、移动硬盘等移动存储介质成为病毒传播的载体；**
- **光驱、网卡、蓝牙、USB 接口、无线等设备成为风险引入的新途径；**
- **终端随意接入网络，入网后未经授权访问核心资源；**
- **非法外联不能及时报警并阻断，导致重要资料数据外传流失；**
- **终端随意私装软件，恶意进程持续消耗有限网络带宽资源；**
- **针对政企客户的定向攻击持续且隐蔽性高，造成严重后果；**

……

针对以上问题，奇安信集团基于终端安全方面多年的技术沉淀和实践经验，不断完善终端安全管理系统和产品解决方案。

2. 产品介绍

2.1 产品概述

天擎终端安全管理系统是面向政府、企业、金融、军队、医疗、教育、制造业等企事业单位推出的集防病毒、终端安全管控、终端准入、终端审计等功能于一体的平台化管理系统。天擎终端安全管理系统，以多引擎复合式查杀能力为创新、以大数据技术为支撑、以多合一终端提供简便部署、以可靠服务为保障，以支持多终端多任务并发处理为核心能力，提供终端防病毒模块、终端补丁管理模块、终端运维管控模块、终端移动存储管理模块、XP 盾甲模块、终端审计模块、终端多网切换模块、终端屏幕水印模块、终端 EDR 模块/产品、终端准入模块、终端软件管家模块等在售的 14 个模块。

2.2 产品理念

针对政企客户终端面临的外部威胁和内部管理痛点，奇安信集团基于“终端安全一体化”产品理念，推出集防病毒、终端安全管控、终端准入、终端审计等功能于一体的平台化管理系统，结合云端统一的大数据和威胁情报，有效发现识别病毒、木马、APT 等各类威胁，通过病毒查杀、补丁修复、终端管控、终端准入、防黑加固等安全能力，为用户构建立体防护体系，同时完美兼容不同操作系统和计算平台，实现多系统统一管理平台、多功能统一管理平台。

2.3 产品架构

天擎系统架构图

天擎终端安全管理系统分为控制中心和终端程序两大部分，客户端部分是一个独立的本地可执行程序，完成管理员下发的任务和策略；控制中心部分采用 B/S 架构，完成管理员的所有管理需求。

在天擎平台上配合使用的组件还包含： NPC 私有云查杀引擎、天擎 NAC 网络安全准入引擎、天擎软件管家 OVA、隔离网升级工具。

- **控制中心**

控制中心是天擎终端安全管理系统的核心，部署在服务器端。

控制中心采用 B/S 架构，管理员可以随时随地的通过浏览器打开访问，对天擎终端进行管理和控制。主要有分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、终端软硬件资产管理等。此外安全控制中心还

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。

- **客户端**

客户端部署在需要被保护的终端或服务器上，执行最终的木马病毒查杀、漏洞修复、安全防护等安全操作。并与安全控制中心通信，提供控制中心管理所需的相关安全告警信息。

另支持离线策略部署；策略部署后，客户端会将策略保存在终端本地，在终端离线场景下，依旧可以持续对终端进行安全防护和管理。

- **NPC 私有云引擎**

NPC 引擎，提供防病毒“私有云”查询能力，具备 PE 文件 MD5 查询功能，提供 MD5 的黑白属性鉴定功能。目前私有云引擎包括黑白样本 12 亿个。

- **NAC 终端准入引擎**

NAC 终端准入引擎，基于天擎控制中心集中统一管理，适应大规模网络环境下的部署，可实现核心区域的准入控制，终端层面的准入控制，接入层边界的准入控制，满足不同网络场景下轻、中、高强度的准入控制需求，引擎具备扩展多种第三方认证源联动认证，支持 AD、LDAP、Email 等多种认证源，实现实名制认证管理，主要解决终端接入的安全合规性要求，用于防止企业网络资源不受非法终端接入所引起的威胁，在有效管理用户和终端接入行为的同时，也保障了终端入网的安全可信，同时达到了规范化地管理计算机终端的目的。

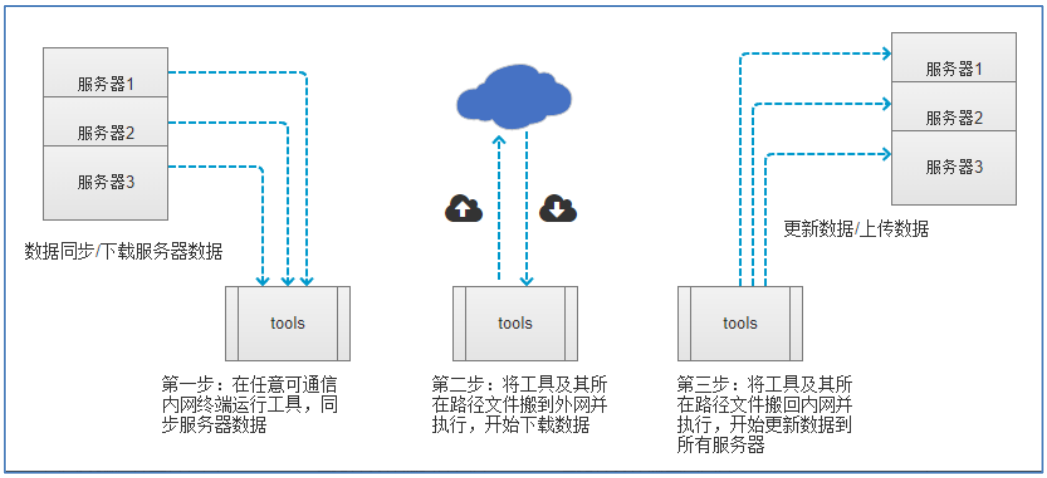
- **软件管家 OVA**

软件管家管理中心主要针对软件进行管理，管理网内的自有软件和供网内终端使用的软件列表，包括上传企业私有软件和下载、软件的安全鉴定、缓存公网软件功能，查看终端软件应用相关的日志报表、基于软件管家中心的管理员操作日志，及基于软件下载限流等功能。

- **隔离网升级工具**

为了保障隔离网用户环境内终端安全，将互联网最新的库文件提供给隔离网用户，每周为隔离网用户提供两次升级病毒库、互联网流行木马库更新，以

此保障隔离网用户不会受到最新病毒变种或木马变种的攻击，降低对企业造成威胁。隔离网工具使用时分为三步，第一步用于同步企业当前版本信息，内网需要下载补丁文件的库信息，以及企业内部灰文件的指纹信息。第二步中会根据第一步同步的信息进行增量下载数据，同时会向云端查询企业内网灰色文件的云端鉴定等级并保存。第三步中将第二步下载的数据更新到服务器，以保障库文件和补丁修复程序都是最新的，同时内部灰色文件也得到鉴定，将在后续防护和扫描中执行最新鉴定结果，以此保障内网安全。



3. 产品功能

3.1 病毒防护

天擎终端安全管理系统支持对蠕虫病毒、恶意软件、广告软件、勒索软件、引导区病毒、BIOS 病毒的查杀，这依赖于人工智能引擎、云查杀引擎、可执行文件的引擎、非可执行文件的引擎等多引擎的协同工作。

防病毒功能的安全防护分为三个方面：扫描，实时防护，主动防御。

扫描：通过客户端程序进行文件扫描，根据客户环境可以使用强大的天擎公有云引擎、私有云或鉴定中心，进行威胁文件的识别。在扫描过程中除了上述云引擎，同时启用 OWL 引擎和智能识别多种格式引擎，具备动态、静态脱壳能力等多引擎的协同工作，全方位扫描文件，不放过一个死角。

实时防护：在文件被访问时对文件进行扫描，及时拦截活动的病毒，对病毒进行免疫，防止系统敏感区域被病毒利用。在发现病毒时会及时通过提示窗口警告用户，迅速处理。

主动防御：全方位立体化阻止病毒、木马和可疑程序入侵。安全中心还会跟踪分析病毒入侵系统的链路，锁定病毒最常利用的目录、文件、注册表位置，阻止病毒利用，免疫流行病毒。目前已经可实现对动态链接库劫持的免疫，以及对流行木马的免疫，免疫点还会根据流行病毒的发展变化而及时增加。

这些功能对云查杀引擎的使用可以根据企业的网络环境自由选择，终端无法连接天擎云的情况下也可以选择通过控制中心或者独立的代理服务器代理到天擎云，企业内部网络和互联网完全隔离的情况下还可以使用专用的私有云安全鉴定中心来保障安全。

防病毒模块共由三部分组成：

终端安全代理软件（天擎客户端）：本地文件安全监控与扫描；

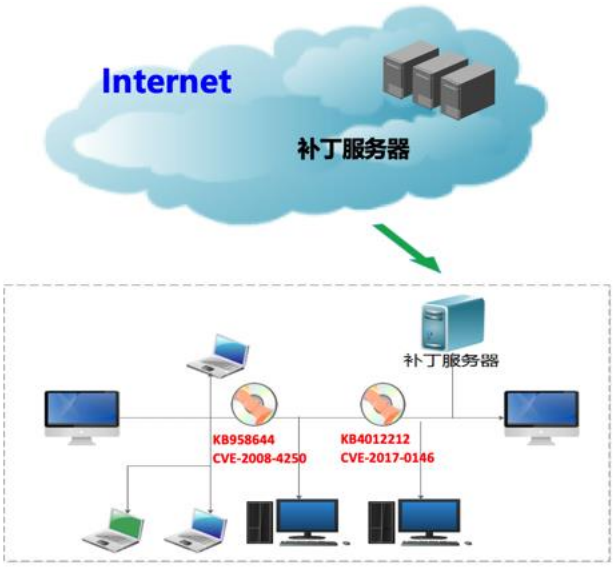
控制中心：管理员统一下发病毒策略，或者查杀任务，对未知文件进行云端查询；

云端库：通过强大的 QCE 引擎进行文件安全性的实时分析，并返回天擎控制中心文件结果。

3.2 补丁管理

天擎终端安全管理系统旨在解决企业多网络环境下的补丁下载与安全问题，提供云端下载和离线下载工具。通过更新补丁来完善软件、修补漏洞，提高软件的健壮性，延长软件的生命周期。

当微软更新补丁后，奇安信会进行专业的补丁安装测试，测试无问题后会上传到云端补丁下载服务器。天擎控制台会通过奇安信的云端补丁下载服务器下载所要更新的补丁，并对需要发布的补丁进行统一下发和安装。支持灰度发布，可进行分多批次安装补丁，先从最小量测试开始，实现补丁影响范围可控。对于物理隔离的内部网络，可以使用离线下载工具下载后通过摆渡设备导入到天擎控制台。



3.3 运维管控

控制中心为管理员提供了终端安全策略管理等多种管理功能，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。

提供统一管理界面对终端上的安全情况做全面的收集与管控。对终端的应用程序、网络防护、违规外联、外设使用、桌面加固等多个维度进行安全管控，提早避免安全事件的发生并对终端尝试的违规动作产生告警信息。

安全模式下管控策略不生效，但可禁用安全模式、或者设置带密码的安全模式，支持对 LDAP 域用户下发管控策略。

3.4 移动存储介质管理

天擎终端安全管理系统，能够实现对移动存储设备的灵活管控，保证终端与移动存储介质进行数据交换和共享过程中的信息安全要求。移动存储管理包括移动存储介质的身份注册、网内终端授权管理、移动介质挂失管理、外出管理和终端设备例外等功能。

移动存储管理解决了用户在安全管控要求下使用移动存储介质，实现数据共享和数据交换的迫切需求。移动存储管理支持分组管理，给予不同的移动存储介质相应的授权使用范围和读写权限，同时支持设备状态的追踪与管理。

3.5 XP 和 WIN7 系统加固

为了彻底解决微软停止 XP 和 Win7 服务带来的安全威胁，根除漏洞因无法修复带来的危害，同时又全面满足各大企业、金融、能源、军队中已经部署的大量应用和对应用运行稳定型、持续性的要求，奇安信采用了多层防护、标本兼治、技术与安全管理策略相结合的整体设计思路，集成了奇安信第三代安全引擎“天狗引擎”，摆脱了对文件、流量、数据、行为等特征的依赖，采用了内存指令控制流检测技术，并与机器学习与人工智能技术深度结合，可从系统的更底层发现漏洞攻击代码的执行，且检测能力不依赖漏洞及攻击代码的特征、与漏洞是否已知无关，面对 0Day 漏洞，亦有着显著的防护效果。

3.6 软件管家

奇安信软件管家系统致力于为政府企业客户快速便捷地建立私有、安全、个性化、场景化的软件应用平台，融合海量软件宝库和云安全系统，快速搭建企业内网软件商店，通过远程安装、卸载、license 管理等方式，全面提升软件

管理能力、软件授权管理能力、防御软件供应链攻击，实现全网软件、软件版本量化管理，对全网终端软件的来源可控、授权可见、版本可知。

3.7 终端审计

随着信息安全技术和理念的发展，安全监控的关注点已经从设备转向对于设备使用者的行为，用户对于设备使用人行为审计和行为控制的需求越来越明显，天擎终端安全管理系统通过技术手段使各种管理条例落地，增强用户的安全和保密意识，保护内部的信息不外泄。所审计的内容只是跟内网安全合规管理相关的信息，不对涉及终端用户的个人隐私信息，达到合规管理的审计的要求。目前可进行审计的内容包括软件使用日志、外设使用日志、开关机日志、系统帐号日志、文件操作日志、文件打印日志、邮件记录日志、安全 U 盘审计、IM 日志等

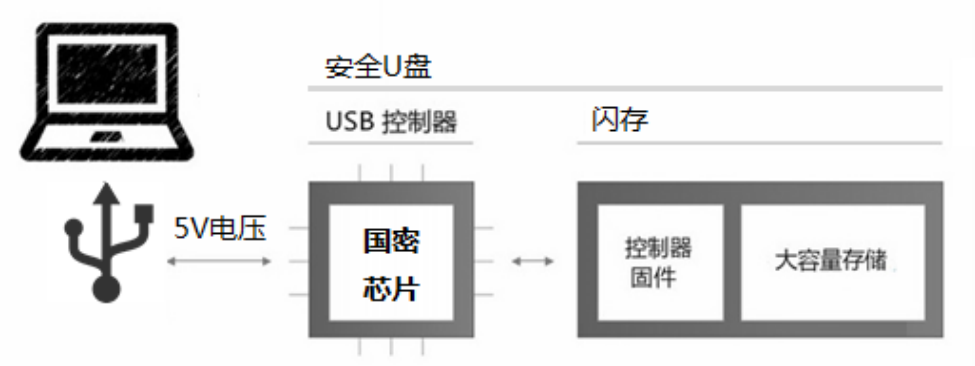
3.8 屏幕水印

屏幕水印功能可以预防拍照截屏方式泄露业务数据，将终端主机启用屏幕水印功能，屏幕水印会始终保持最前端展示，不管启用何种软件，均可正常显示水印信息。屏幕浮水印可以将水印文字、显示计算机名、显示用户名、IP 地址、MAC 地址等数据以半透明的方式呈现在屏幕上，屏幕水印功能虽不能终止

业务终端泄露业务敏感数据，但是对拍照等方式泄露涉税数据形成有效的震慑，直接降低了以拍照方式泄露涉税数据的风险。

3.9 安全 U 盘

天擎安全 U 盘是采用安全固件进行加密的移动存储介质，有效解决了木马摆渡、病毒传播、U 盘交叉使用和 U 盘文件使用缺乏审计等方面的安全问题，通过定制安全芯片的应用大大提高了 U 盘的安全特性，配合移动介质存储管理模块保证即使 U 盘丢失也依然可以有效保护 U 盘内的加密文件，从各个方面减少了因 U 盘使用而为企业内网带来的安全隐患。



3.10 多网切换

在某些特殊客户场景下，例如医保药店、政务大厅、电子政务外网等，为了满足业务需要均会存在一机多网使用的情况，一台终端同时接入多张相互隔离的网络，这样的业务场景会对终端的管理及信息安全的保护带来极大的风险。为了即满足各政企用户在此特殊场景的业务，又保证终端安全管理的政策及安全需求，经过对客户场景详细的调研与交流后，我们推出了多网切换功能。

该模块可通过终端访问控制的方式实现对同一终端上不能同时访问多张互相隔离的网络实际使用场景，解决终端由于同时访问多个网络而带来的安全隐

患，亦帮助用户达到了安全合规的要求。其相比常见的硬件隔离方式，减少了对于用户硬件及网络变更的成本，大大提高了部署和使用上的便利性。

3.11 终端准入（配合 NAC 引擎使用）

终端强制合规、安检合规需要配合 NAC 准入引擎一起使用，主要解决终端接入的安全合规性要求，用于防止企业网络资源不受非法终端接入，在有效管理用户和终端接入行为的同时，也保障了终端入网的安全可信，同时达到了规范化地管理计算机终端的目的。

基于天擎控制中心集中统一管理，适应大规模网络环境下的部署，可实现核心区域的准入控制，终端层面的准入控制，接入层边界的准入控制，满足不同网络场景下轻、中、高强度的准入控制需求，具备扩展多种第三方认证源联动认证，支持 AD、LDAP、Email 等多种认证源，实现实名制认证管理， 产品具备从访客管理、用户注册、认证授权、安全检查、隔离修复、访问控制 “一站式”的入网管理流程，并支持多种认证技术，多因素认证方式，多条件认证绑定机制，支持混合认证模式，多层防护体系，适应复杂网络环境的部署，满足企业内部终端准入控制需求，从而使内部网络管理变得安全、透明、可控，达到信息安全管理要求。

3.12 终端威胁检测与响应

在企业终端安全领域，企业用户不但能接触到面向企业个人的安全威胁，同时还有可能接触到面向企业资产的安全威胁。由于企业资产的价值是远高于

企业个人的，所以攻击者愿意付出更多的攻击成本来实施安全威胁。这些成本往往包括一个团队，使用鱼叉攻击、社会工程学攻击等定向攻击的方式，甚至还有可能使用 0day 漏洞来提升攻击的强度，确保最终威胁实施的成功和隐蔽。同时，由于企业的安全大数据相对封闭，导致安全厂商无法第一时间帮助企业用户处理安全威胁。而企业的安全运维能力往往不足，最终导致面向企业资产的安全威胁的响应速度严重不足，甚至在企业内潜伏多年，无法发现。

为了提升面向企业资产的高级威胁响应速度，天擎推出 EDR 模块。通过 EDR，奇安信能够把自身云端终端安全大数据处理能力，前置到企业用户中。这些处理能力不光包括大数据存储，查询的能力，还包括大数据分析的思路和方法。通过云端威胁情报的向企业用户推送，企业用户在威胁情报中知识的引导下，学习企业内发现的已知威胁，积累威胁分析的经验。EDR 系统在威胁情报中知识的引导下，可以发现新的潜在未知威胁，供管理员分析与调查。最终，通过一套标准的未知威胁响应的业务流程，能够让对未知威胁的单次响应，快速落地为对已知威胁的持续拦截。最终成功缩短未知威胁的响应时间。

3.13 终端发现

终端管理的前提条件是需要知道管理的对象有哪些，随着智能终端的快速推广，IT 消费化的潮流越来越明显，越来越多的企业员工希望使用移动设备访问公司邮件、企业内网等资源，同时希望使用自己的移动设备进行工作。BYOD（Bring Your Own Device）作为 IT 消费化的一个重要表现形式，对原有的企业网络接入管理产生了严重的冲击，与此同时，IoT 万物互联理念的兴起，让更多的非人触设备接入网络，比如交通摄像头，温度传感器，网络打印机，VoIP 等，这些设备更加剧了传统管理体系与新兴安全形势的冲突，加大了管理难度。

处于安全考虑，企业 IT 管理员需要根据不同的用户终端类型，定义不同的安全策略。如何高效、准确识别终端类型，则成为每一个 BYOD，IoT 解决方案提供商必须解决的问题。天擎终端安全管理系统利用终端发现模块发现并识别

政企业务范围内的一切 IP 终端，可视化统筹企业终端资产，快速定位终端信息及安全状态。

3.14 第三方集成

天擎终端安全管理系统具备很丰富的管理能力和数据采集能力，天擎可开放基础框架和数据能力给第三方合作伙伴，第三方合作伙伴可以利用天擎开放的强大终端管控能力，成熟稳定的通信、升级能力，丰富的终端数据接口，为天擎用户提供更贴近业务的功能，为天擎用户更好的服务。

4. 产品优势

天擎终端安全管理系统的核心价值在于对终端安全的防护与管理。奇安信自身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得到了国内广大用户的认可，在企业安全领域，天擎终端安全管理系统已累计为国内 7 千家企事业单位、超过 3300 万终端提供了安全防护及终端管理。

4.1 终端安全一体化

- 功能一体化：国内首家集终端防病毒和安全管控于一体的终端安全管理系统；
- 平台一体化：完美兼容各类终端及服务器 Windows、Linux、国产操作系统、MacOS X，同时支持云桌面和服务器虚拟化；
- 数据一体化：利用云端大数据和威胁情报，增强本地威胁防御，有效感知本地安全态势；

4.2 病毒防御多维化

- 多引擎技术：拥有领先的云查杀引擎、OWL 引擎、主防引擎、人工智能引擎，有效查杀已知和未知病毒
- 立体化主防：具备隔离防护、5 层入口防护、7 层系统防护及 8 层应用防护等主动防御技术
- 智能自学习：通过海量病毒样本数据自学习，人工智能引擎无需频繁更新特征库、病毒检出率仍远超传统查杀引擎
- “非白即黑”安全策略：具备及时发现和抵御未知威胁的能力，并可以扩展 EDR 模块，有效抵御 APT 攻击

4.3 安全管控智能化

- 资产管理：自动识别全网终端资产信息，实时监控系统状态并告警，保障业务连续性
- 安全策略管理：通过非法外联、外设管理、进程控制、主机防火墙、桌面安全加固等多元化方式，提升终端安全等级
- 漏洞补丁管理：对全网终端漏洞进行扫描并关联，简化补丁运维，实现补丁自动验证，减少人为参与提高效率，降低补丁部署风险。
- 网络安全准入：支持旁路应用准入、802.1x 准入及其它多种准入技术，对不满足安全性检查的终端不予接入网络，并引导到修复区进行安全修复
- 审计管理：全网文件安全审计，外设使用审计，多级管理，多种报警方式，实现高效的全网管控

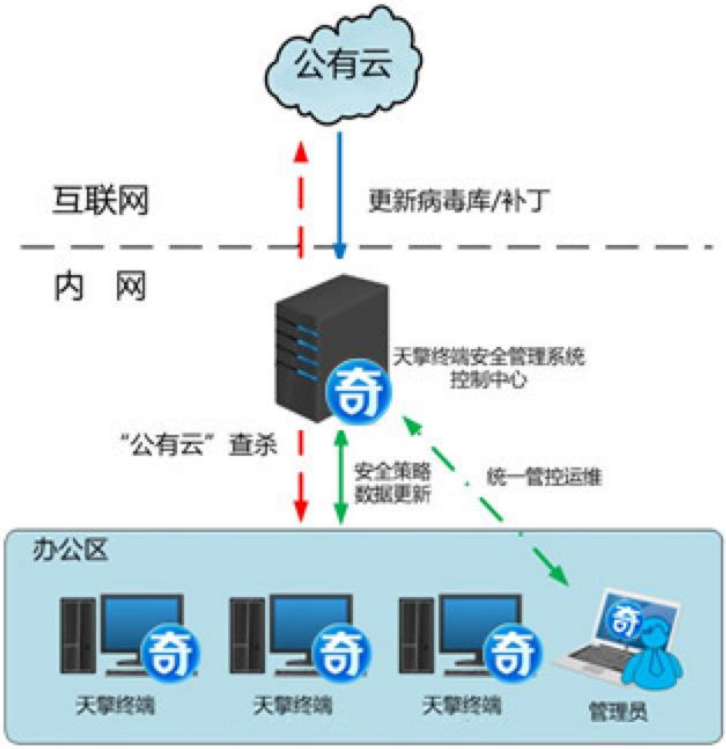
5. 典型部署

5.1 互联网络部署方案

➢ **方案特点**

本方案适用于能够连接互联网环境的用户，用户网络中部署天擎终端安全管理系统服务端（控制中心），办公终端安装天擎终端安全管理系统客户端，通过控制中心对办公终端做统一的安全防护和管理。

➢ **部署示意图**



在网络内部署天擎终端安全管理系统（控制中心），通过在线安装或者离线安装包的方式安装终端客户端。控制中心通过互联网连接到云端的升级服务器进行升级、更新，然后客户端通过控制中心统一进行升级、更新及策略下发，可以极大的节省企业总出口带宽。

客户端会根据控制中心下发的安全策略，进行体检、杀毒和漏洞修复等安全操作。可以设定终端是从控制中心更新病毒、补丁库，还是从互联网更新。

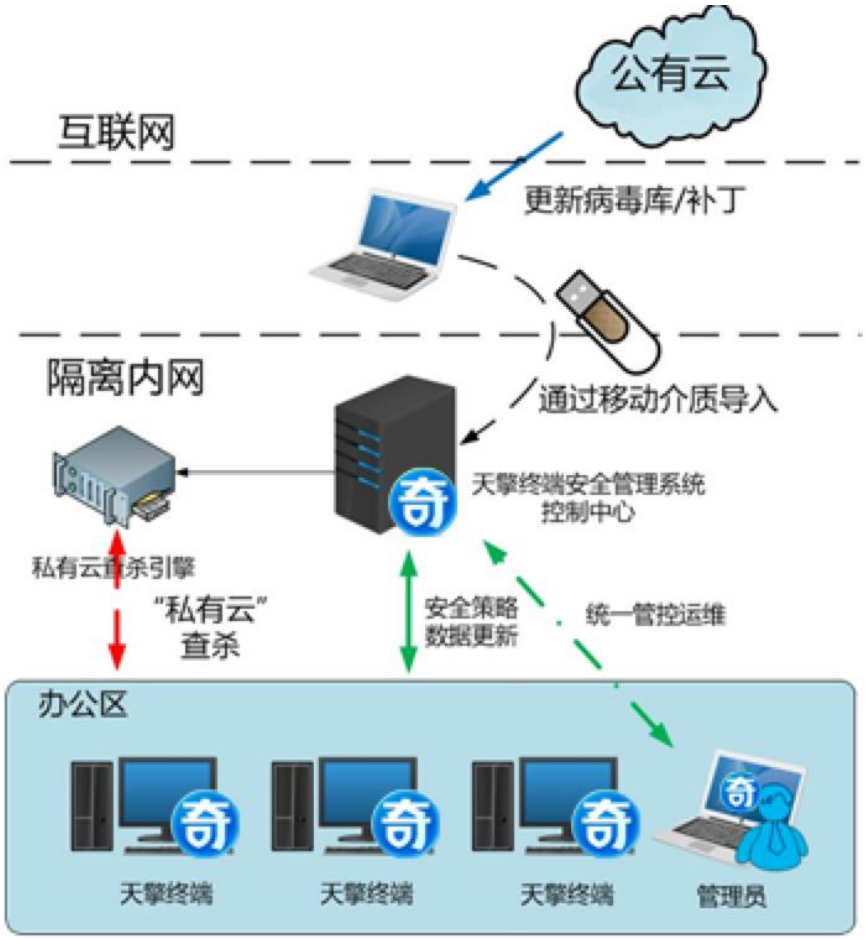
终端可连接云端进行云查杀，极大的提高终端病毒的查杀能力。

5.2 隔离网络部署方案

- **方案特点**

该方案适用于无法连接互联网环境的用户，网络中部署一套天擎终端安全管理系统（控制中心），网内中的终端安装天擎终端安全管理系统客户端，通过控制中心进行统一的安全防护和管理，控制中心的病毒、补丁等更新程序通过离线升级工具进行升级。

- **部署示意图**



在用户网络中部署天擎终端安全管理系统控制中心，通过在线安装或者离线安装包的方式安装终端客户端，客户端会根据控制中心下发的安全策略，进行体检、杀毒和漏洞修复等安全操作。

部署私有云查杀引擎，保证能和控制中心网络连通即可。提高内网查杀能力，帮助用户快速、精准定位查杀威胁较高的恶意样本。

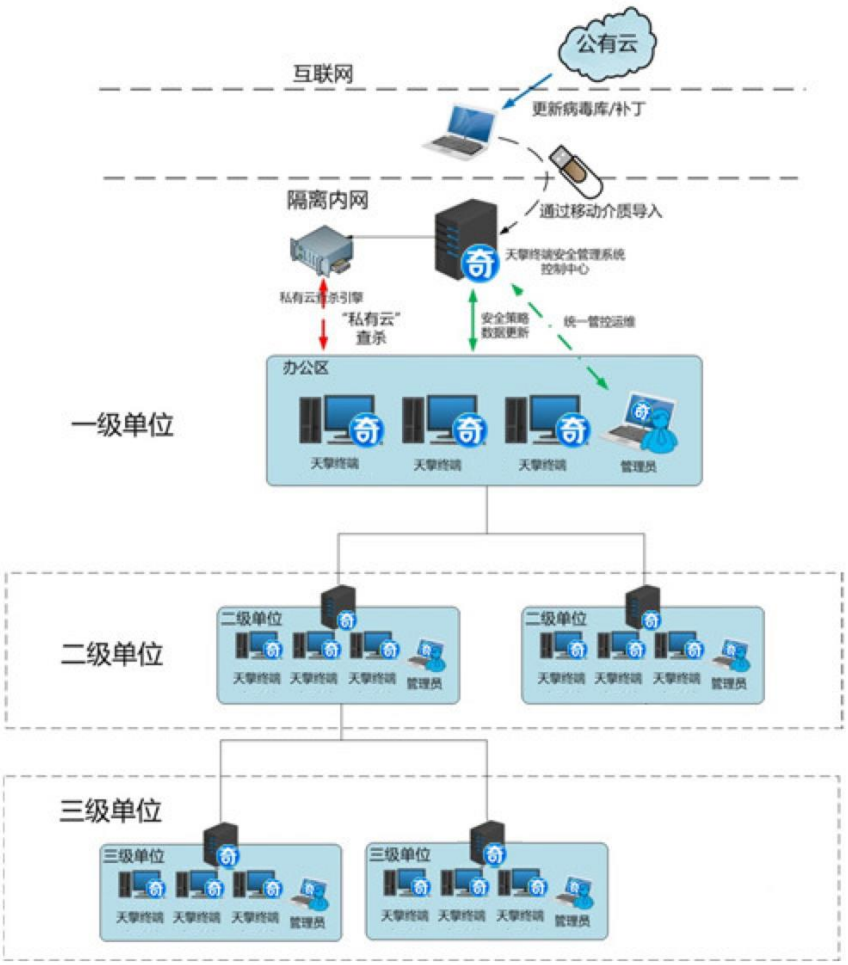
在有互联网的环境中使用隔离网更新工具，定期从云端相关服务器下载病毒、木马库、补丁库；然后使用移动呢存储介质更新到内网的控制中心，用户的终端连接到内网控制中心进行自动升级和漏洞修复。

5.3 级联部署方案（大型网络环境）

- **方案特点**

该方案适用于大型用户（总部-多分支机构）环境，用户网络中部署多套天擎终端安全管理系统（控制中心），通过在线安装或者离线安装包的方式安装终端客户端，多套控制中心可以分级级联管理。如在用户网络中一级总控中心的病毒/补丁等更新通过离线升级工具升级，二级、三级分控中心通过一级总控中心进行级联更新，下级分控中心可以向上级控制中心上报告警信息。

- **部署示意图**



在一级单位部署总控制中心，在每个分支机构部署二级、三级分控制中心。分控制中心指向到所属的上级控制中心，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、木马库升级和漏洞修复。

隔离网环境更新：使用离线更新工具，定期从云端服务器下载病毒库、木马库、补丁文件等，更新到总控制中心，各分控制中心会从上级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。

互联网环境更新：总控制中心从互联网跟新病毒库、木马库和补丁文件，各分控制中心会从上级控制中心下载需要的升级文件和补丁文件。各级控制中

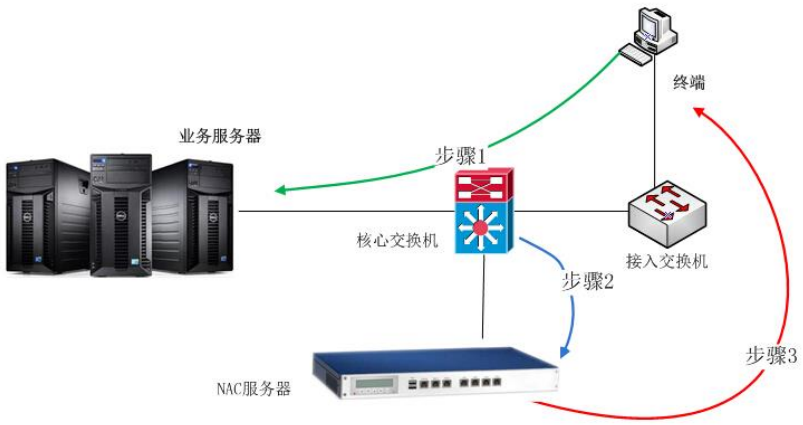
心也可以直接从互联网下载需要的升级文件和补丁文件，客户端也可以直接从互联网下载需要的升级文件和补丁文件，来减轻上级控制中心出口带宽压力。

5.4 终端强制合规（NAC）旁路部署方案

➢ **方案特点**

未安装客户端的用户或未认证用户，在访问核心网络中受保护区域时，访问连接会被阻断，HTTP 请求被重定向到客户端下载页面或 Portal 认证页面。终端认证通过或安装客户端后，用户可以正常访问相关服务。下次登录时只要不卸载客户端，就可以正常访问相关服务。

➢ **部署示意图**



➢ **入网流程**

NAC 采用旁路部署，对端网络设备配置端口镜像，NAC 做流量分析。同时配置阻断口，当终端不合法时发送阻断包，阻断终端入网，终端无法访问业务服务器。

◆ 天擎终端安全管理系统打点联动方案

功能：只有安装天擎终端安全管理系统客户端的 PC 才有权限访问受保护服务器。

1. 用户访问受保护服务器时重定向到客户端下载页面。

2. 下载并安装天擎终端安全管理系统客户端，之后用户 PC 可正常访问受保护服务器。

◆ Web Portal 认证+安装天擎终端安全管理系统客户端

功能：合法用户经过 portal 认证或用户注册，下载并安装天擎终端安全管理系统客户端后才能访问受保护服务器（注册用户需经管理员审批确认或自动审批确认）

1. 客户 PC 访问受保护服务器，重定向到认证/注册页面。

2. 注册用户填写用户真实信息并提交管理员确认身份合法。

3. 经管理员确认后，用户再次访问受保护服务器，重定向到下载天擎客户端页面，安装客户端之后用户可正常访问受保护服务器。

◆ Web Portal 认证方案

功能：合法用户经过 portal 认证或用户注册，可直接访问受保护服务器（注册用户需经管理员审批确认或自动审批确认）

1. 用户访问受保护服务器，重定向到认证页面，具有合法身份用户认证成功后可以直接访问受保护服务器。

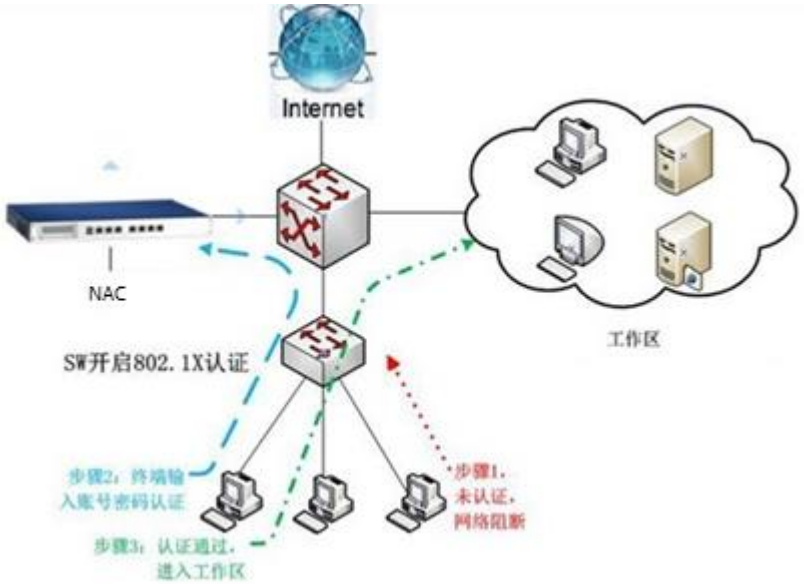
2. 注册用户填写用户真实信息并提交，管理员确认后并认证可以访问受保护服务器。

5.5 终端强制合规（NAC）802.1x 部署方案

➢ **方案特点**

802.1X 认证是通过标准 802.1x 协议，在网络接入层做接入认证、根据认证授权情况确定是否能访问网络，并进行合规性检查，根据检查结果下发网络访问权限，802.1X 认证可提供端口级的强准入认证方案，并支持认证授权、安全检查、隔离修复、访问控制“一站式”的入网控制。

➢ **部署示意图**



- **入网流程**

NAC 接入到用户网络中，保证在网络中 IP 可达即可。

在用户交换机中配置 802.1x 功能，把认证服务器地址指向 NAC，NAC 接收来自终端的认证请求，并将认证结果下发给交换机，确定是否放行。当终端安装了天擎认证小助手后，入网前会弹出认证界面，输入用户名口令后，如果认证成功，可以正常网络访问。

设置了合规性检查策略，则进行合规性检查。检查通过，就进入正常业务网络；否则进入修复区，在修复中的终端只可以访问修复服务器；处在修复区的终端，如果修复完成后，可以正常访问工作区网络。

5.6 配置建议

控制中心配置要求

管理终端数	服务器配置要求
1000	CPU：最低 8 核 2.4Ghz； 内存容量：最低 8GB ； 硬盘：最低 1TB； 操作系统：Windows Server 2008 R264 位，简体中文版； 网卡：千兆单网卡；
5000	CPU：最低 16 核 2.4Ghz 内存容量：最低 16GB； 硬盘空间：最低 1TB；操作系统：Windows Server 2008 R264 位，简体中文版； 网卡：千兆单网卡；
10000	拆分部署模式，需使用 linux 版本
管理浏览器	chrome43.0 及以上版本 推荐奇安信可信浏览器

客户端配置要求

类型	操作系统	CPU	内存	硬盘	备注
Windows 终端	Windows XP Windows Vista Windows 7 Windows 8 Windows 10	双核 2.0GHZ	1G	>20G	最低配置
Mac	OS X	苹果 PC 标准配置			
服务器	Windows Server 2003 SP2 Windows Server	双核 3.0GHZ	4G	>20G	最低配置

	2008 Windows Server 2012 Windows Server 2016 中标麒麟 Deepin				

6. 产品价值

6.1 自主产权，杜绝隐患

天擎终端安全管理系统具有完全自主的知识产权，拥有国家背景的一流企业级终端安全管理系统，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。

6.2 安全问题，不止合规

天擎终端安全管理系统正稳定可靠运行于国内 7 千家企事业单位内网中，累计防护超过 4000 万终端。拥有接受大量网络攻击的实战经验，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。

6.3 强大管理，提高效率

天擎终端安全管理系统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。

6.4 灵活扩展，持续安全

天擎终端安全管理系统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 和 WIN7 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。

6.5 数据驱动，协同防御

天擎终端安全管理系统拥有海量的云端安全大数据，我们将这些数据进行分析利用以配合本地部署的终端安全管理系统提升用户内网威胁防御能力，帮用户检测出传统手段无法检测出的威胁，最终定位本地威胁，使用户具备及时发现和抵御未知威胁的能力，满足国家信息安全发展要求。

同时天擎还可以与奇安信智慧防火墙、天眼威胁检测进行协同联动。与防火墙配合实现终端的准入与准出，与天眼配合阻断威胁的源头，有效防护攻击。从而达到全方位全天候感知网络威胁，实现高效的内网安全防护。

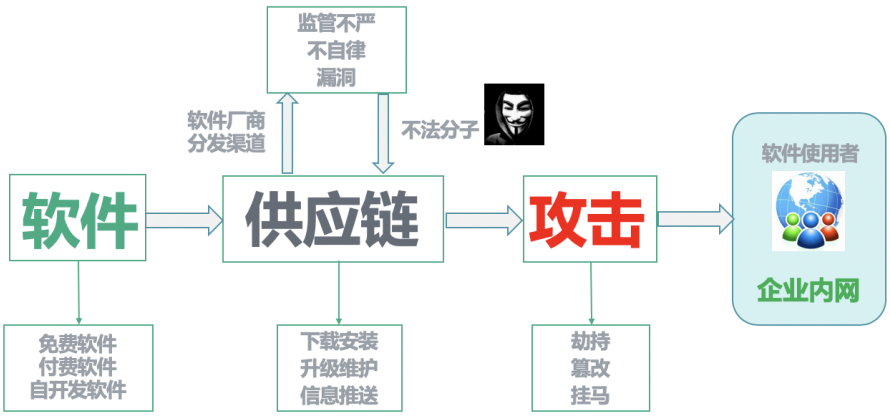
7. 应用场景

7.1 勒索病毒防护场景

奇安信持续给政企用户提供多重的专业化终端安全防护——例如勒索病毒场景，在此种场景下需要终端具备勒索病毒的查杀防护能力、漏洞修复能力、以及 RDP 爆破防护机制。针对于此种场景，天擎采用三重攻击防护以及三重勒索防护来解决。

- 三重攻击防护。
  - 专项的漏洞入侵防护，防止勒索病毒利用系统漏洞攻入。
  - 远程桌面的暴力破解防护，防止黑客漏洞入侵成功后对远程桌面进行暴力破解。
  - 杀软恶意退出防护，防止黑客拿到终端权限后，恶意退出杀软进行投毒。
- 三重勒索防护。
  - 文件系统防护（FD），通过云查杀、人工智能查杀引擎，实时检测文件的执行、生成和重命名等行为，发现可疑文件时及时提示或拦截。
  - 勒索病毒免疫，通过内核对象抢占欺骗勒索软件，迫使其退出。
  - 进程防护（AD），系统目录放入 Office 等文本文档做诱饵。发现有修改文档行为，拦截关联进程。

7.2 软件供应链安全防护场景



天擎终端安全管理系统针对于软件供应链安全防护场景，可通过软件管家模块提升软件安全管理，来解决软件供应链场景下的终端安全防护。

◆ 提升软件安全管理

- 提升操作系统和办公软件正版化率，降低盗版软件知识产权被告风险。
- 控制软件版本，软件版本不统一导致低版本软件存在于某些终端，这些终端称为网络中被攻击的信息点。
- 确保软件下载源的唯一性，避免恶意篡改的软件进入内网。
- 利用软件管家自动升级，某些软件强制升级功能，加强软件的统一管理。

7.3 业务网终端的合规管理

天擎终端安全管理系统一体化终端安全解决方案，针对业务网终端的合规管理场景，通过准入与多网切换，屏幕水印，多中心注册，来解决一机多网场景下的终端安全防护。

- 准入与多网切换，通过准入强制终端安装天擎客户端，通过客户多的多网切换功能来控制用访问互联网的时候，不能访问业务网；访问业务网的时候，不能访问互联网。
- 屏幕水印，屏幕水印有效震慑屏幕拍照行为，从而降低数据外泄风险。

- 多中心注册，实现内外网均可以使用注册 U 盘，但是无法使用未注册 U 盘，同时一个 U 盘可以在两个中心注册。

7.4 高级威胁防护场景

天擎终端安全管理系统一体化终端安全解决方案，针对高级威胁防护场景，通过终端安全响应系统（EDR），来解决高级威胁防护场景下的终端安全防护。

- 主动威胁检测，实时接收大数据威胁情报、鉴定中心等告警线索信息，在大数据分析平台中主动检索、匹配 IOC 告警、定位符合条件的威胁终端。另外，也可以通过自学习建立终端安全基线，识别异常行为，触发威胁检测流程。
- 终端威胁追踪，针对威胁告警的线索，安全管理员通过数据平台提供的数据聚合筛选、日志检索、终端进程树还原等手段，在全网内追踪威胁来源、载体、行为，还原威胁的真实目的。
- 威胁应急响应，针对终端威胁的类型以及扩散的程度提供不同等级的响应手段，如进程隔离、进程删除、样本加黑、防火墙联动阻断、网络隔离等，通过将单次响应固化成全局策略，实现安全基线提高，以持续拦截威胁。
- 安全状况全面评估，针对于威胁终端进行全面的安全评估，结合终端背景数据，对于终端的安全漏洞、威胁的攻击步骤进行分析评估，发现整个攻击链与终端沦陷的根本原因以及影响范围。