

★完全公开

奇安信天擎终端安全管理系统

产品彩页

V10.0

地址：北京市西城区西直门外南路26号院1号

邮编：100044

1 引言

《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》中明确提出：迎接数字时代，激活数据要素潜能，推进网络强国建设，加快建设数字经济、数字社会、数字政府，以数字化转型整体驱动生产方式、生活方式和治理方式变革。因此，各行各业都在积极地进行数字化转型。

在数字化转型过程中，数据价值越来越重要，商业模式变得越来越开放，技术应用越来越复杂，业务边界越来越宽泛。终端作为数据和业务的最终载体，在发挥着关键作用的同时，也吸引了越来越多黑客的关注，这给终端安全带来了前所未有的挑战：



➤ 终端复杂化

接入内网的终端类型日益丰富，除了 PC、服务器、哑终端，还有各种智能终端；这些终端的产权归属是复杂的，可能属于单位，也可能属于员工、合作伙伴甚至客户；终端上的操作系统也是多样的，除了主流的，还有小众的，甚至老旧的（例如 Win 7/XP 等原厂不提供服务的）。

➤ 监管粗糙化

终端的物理边界消失了，可能出现在任何物理位置，统一纳管越来越困难，对终端上的软硬件资产及其变化、数据流转的监管正变得日益模糊，对不合规行为的判断和监管力度也变得日益单薄。

➤ 隐患多元化

操作系统和主流应用的高危漏洞越来越多，临时补救、补丁验证和修复缓不救急；终端与业务的交互频繁，落在终端上的数据和应用变得越来越多且杂乱，给黑客攻击提供了更多的通道；终端使用者的安全意识参差不齐，很容易被利用，成为黑客攻击的跳板或帮凶。

➤ 攻击整合化

黑客攻击转变为“有组织、分工明确”的团伙作战，呈现协同化、集群化、生态化趋势；新威胁推出的数量和质量不断升级，从而更大概率、更长时间的躲避安全检测，谋取更多的经济利益。

➤ 防御离散化

过去的安全体系建设通常都是被动的，经过长期的“头痛医头 脚痛医脚”，必然导致产品功能堆砌、防护策略失衡、安全孤岛不断等隐患，安全能力升级越来越困难。

➤ 运营盲目化

由于缺少明确的度量、清晰的流程、有效的工具、足够的资源和支持，终端安全运营很难在政企单位内部运转起来，这必然导致终端安全产品能力无法全面发挥出来，安全效果很难得到持续保障。

.....

只有运用“体系化防御、数字化运营”方法，才能准确地识别、保护和监管终端，并确保它们在任何时候都能可信、安全、合规地访问数据和业务，真正构建持续有效的终端安全能力，守住网络安全最后一道防线。

2 部署方案

2.1 级联部署

该方案适用于中控集群模式环境，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和免密登录（支持上级管理员免密登录到下级控制中心）。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。



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。

提供对信创和非信创系统客户端的统一部署及管理功能授权。可管理的国产化系统客户端：中标麒麟（龙芯/海光/鲲鹏）、银河麒麟飞腾、中科方德（海光/兆芯）、统信 UOS（海光/兆芯/龙芯/飞腾/鲲鹏）。可管理的 windows 客户端：WindowsXPSP3(32 位)、Windows7(32/64 位)、Windows10(32/64 位)、WindowsServer2003(32 位)、WindowsServer2008(32/64 位)、WindowsServer2012(64 位)、WindowsServer2016(32/64 位)。可管理的 linux 客户端：CentOS6.0x86_64(及以上)、Redhat6.7x86_64(及以上)、SUSE13.2x86_64

（及以上）、ubuntu14.04.4x86_64（及以上）、Fedora release 23x86_64（及以上）、Linux slackware 14.2（及以上）、凝思磐石 6.0.42 等。

3 功能特性

3.1 防病毒功能

奇安信天擎对终端上的安全威胁具有强大的防御、检测和响应能力，奇安信天擎集成了奇安信自研的多个防护引擎，基于奇安信强大的攻防研究能力及丰富的规则库储备及生产能力，面向政企终端实现精准防护、高效检测和联动响应，为终端的安全运行提供有力保障。

3.1.1 病毒防护

奇安信天擎病毒防护采用客户端、管理中心、云端病毒库相结合的工作模式。为终端、Linux 服务器端、windows 服务器端、国产化服务器端提供防病毒策略管理、下发任务、病毒告警分析、报表等功能

客户端：部署在终端，内置奇安信自研的多个引擎，实现终端的病毒查杀、防护。

管理中心：作为客户端的集中控制平台，支持管理员根据网络环境配置病毒防护策略，统计病毒报表，下发病毒库升级任务等。

云端病毒库：云端病毒库包含大量的特征、检测规则，可与客户端联动检测并及时返回检测结果，提高检测能力。

此外，病毒防护功能使用的多款病毒引擎，在联网环境和断网环境下均可实现高准确率查杀，并针对终端感染情况生成病毒统计报告，为政企终端病毒防护提供可视化、可量化的参考依据。同时考虑到不同行业客户终端环境的多样性，我们也为老旧、低配置的机器提供了一键切换轻量化的模式。

奇安信天擎的病毒防护功能可执行终端防护、病毒查杀、日常运维等操作：

- **终端防护：**支持对终端配置病毒查杀策略、防护策略、定时扫描、病毒

库更新等策略。

- 病毒查杀：具备快速扫描、全盘扫描、自定义扫描、强力查杀四种模式，支持对蠕虫病毒、恶意软件、广告软件、勒索软件、引导区病毒的查杀。
- 日常运维：支持生成病毒查杀报告、处理病毒误报漏报、建立病毒查杀任务等。

3.1.2 主动防御

主动防御是指对进程的可疑行为进行拦截、阻止其继续操作的防护机制。该功能主要分为系统防护（包括进程防护、注册表防护、驱动防护）、入口防护（包括 U 盘安全防护、邮件防护、下载防护、IM 防护、局域网文件防护、网页安全防护）、网络防护（包括远程登录防护、网络入侵防护、僵尸网络攻击防护、网络攻击防护、ARP 攻击防护）等。

➤ 进程防护

进程防护实时监测活跃进程的各种系统行为（如进程创建、系统注入与挂钩等），当判定为恶意行为时，根据策略进行提示和拦截，避免系统受到各种恶意行为的侵害。

➤ 注册表防护

注册表防护实时监测系统关键注册表的创建、修改和删除行为，当判定为恶意行为时，根据策略进行提示和拦截，以阻止恶意程序试图开机启动、伴生启动或破坏系统的行为。

➤ 驱动防护

驱动防护实时监测系统的驱动安装、加载、卸载等行为，当判定为恶意行为时，根据策略进行提示和拦截，以阻止恶意程序试图躲避安全软件的检测、破坏安全软件或破坏系统的行为。

➤ U 盘安全防护

U 盘防护实时检测系统接入 U 盘的行为，对 U 盘中关键位置的文件进行安

全扫描，根据策略对发现的风险文件进行提示和清理，避免系统受到 U 盘中恶意文件的入侵。

➤ 邮件防护

邮件防护对邮件收发软件收取的电子邮件进行安全检测，防止邮件中内置的恶意程序利用操作系统的漏洞，对系统进行攻击或病毒植入。

➤ 下载防护

下载防护对下载软件、浏览器下载的文件进行安全检测，根据策略对文件的风险进行提示和清理，防止从网络应用下载恶意程序。

➤ IM 防护

IM 防护对即时通讯工具（IM）下载的文件进行安全检测，根据策略对文件的风险进行提示和清理，防止从 IM 下载恶意程序。

➤ 局域网文件防护

局域网文件防护实时检测局域网网络共享文件的拷入、执行行为，当检测文件不安全时，根据策略进行提示和拦截，防止从局域网共享目录下载恶意程序。

➤ 网页安全防护

网页安全防护对浏览器中访问的 URL 和网页内容进行安全扫描，对发现的风险进行提示和拦截。

➤ 勒索软件防护

勒索软件防护实时检测未知风险程序的篡改文件和勒索病毒相关特征行为，避免系统遭受勒索软件的加密等破坏行为。

➤ 远程登录防护

远程登录防护自动阻止远程登录行为，防止黑客远程爆破和拦截恶意的远程登录。

➤ 网络入侵防护

网络入侵防护对流入本机的网络包数据和行为进行检测，根据策略在网络层拦截漏洞攻击、黑客入侵等威胁。

➤ 僵尸网络攻击防护

僵尸网络攻击防护对流出本机的网络包数据和行为进行检测，根据策略在网络层拦截后门攻击、C2 连接等威胁。

➤ 网络攻击防护

网络攻击防护对流出本机的网络包数据和行为进行检测，根据策略在网络层拦截后门攻击、C2 连接等威胁。

➤ ARP 攻击防护

ARP 攻击防护根据策略检测和拦截局域网中的 ARP 欺骗攻击行为。

➤ DNS 防护

检测和保护本机 DNS 的安全性，防止终端 DNS 和 HOSTS 被恶意篡改，该功能需要联接公有云。

3.1.3 主机防火墙

主机防火墙（Host Firewall），在终端上基于网络五元组信息对主机网络的出入站流量进行控制。通过配置和管理防火墙放行或拦截规则，对终端的异常网络请求进行有效控制。此外，可接管 Windows 系统自带的防火墙程序。

3.2 终端管控与审计

基于运维管控、终端审计功能，奇安信天擎能帮客户构建完善的主机管控与行为审计体系，可实现对终端的外接设备、移动存储设备、系统行为、网络行为、应用进程等多层次的管控与审计。

3.2.1 终端管控

终端管控功能主要对终端进行安全管理以及维护。其主要能力包括外设管理、

移动存储、进程管理、能耗管理、网络访问管控、非法外联检测等，可基于策略模板对终端执行细粒度的分组管控。

➤ 外设管控

对 1394、串口、并口、PCMCIA、USB 接口进行管控；对内置光驱和外置光驱进行管控；对 USB 存储设备，存储卡，冗余硬盘，打印机，扫描仪，磁带机，键盘，鼠标，红外，蓝牙，摄像头，手机/平板,移动数据网卡，MODEM 设备，ISDN 设备，ADSL 设备进行管控，控制方式为禁用和允许两种方式

➤ 网络管控

网络管控提供网卡地址控制、热点创建控制、DNS 地址设置（非地址绑定）、Wi-Fi 连接控制，并支持 IPV6 地址禁止，禁止终端同时连接多个无线信号（多无线网卡环境）。网络管控支持检测当前终端是否存在有线无线共用场景，如存在则自动断开无线连接，通过设置可信 Wi-Fi 列表控制终端能连接的无线 SSID，其他无线信号不可连接，同时也支持网络连接及网络流量的查看。

➤ 违规外联

通过配合公网服务器探测终端本地的互联网出口地址，判断终端是否存在违规外联情况，并可以在探测到互联网出口时执行断网或锁屏等措施，保证终端网络安全，且终端在断网状态下只能连接管理中心，断网状态重启恢复。锁屏时，可以使用策略预置密码进行解锁。关机措施时，支持 1 分钟的缓冲，可以对终端操作文件进行保存和整理。

➤ 进程管理

终端不能运行黑名单中的进程，系统目录和奇安信天擎目录进程默认例外；终端运行的进程自动上报至管理中心，管理员可自定义设置进程组，也可按照规则（进程名、公司名称等）进行自动分组；终端只能运行白名单中的进程，系统目录和奇安信天擎目录进程默认例外；终端必须运行的进程，对指定进程的进程保护，防止终端关键进程被误杀。

➤ 远程协助

远程协助功能支持以远程桌面访问的形式对终端进行远程协助，以便管理员高效开展终端运维工作。

➤ 能耗管理

能耗管理功能支持不同规则、不同节能类型的管控及告警，为管理员提供灵活的运维管控策略。

支持 CPU、内存、磁盘使用监控和告警，可设置 CPU、内存、磁盘使用的阈值，帮助管理员发现存在资源使用异常的终端。

➤ 桌面加固

对操作系统常用设置进行集中配置管理，可支持 `internet` 属性中的信任站点进行统一配置添加，对 `internet` 属性中的代理服务进行代理禁用或统一管控代理配置；支持自定义桌面和屏保，禁止修改计算机名、禁止开启文件共享和禁止使用注册表编辑器，禁止终端从安全模式启动或设置安全模式登录密码。

➤ 外发管控

终端外发文件时，可针对规则进行阻断，确保外发数据的安全，从而实现在不影响外发通道连接的基础上阻断数据外发，满足用户合规管控的需求。

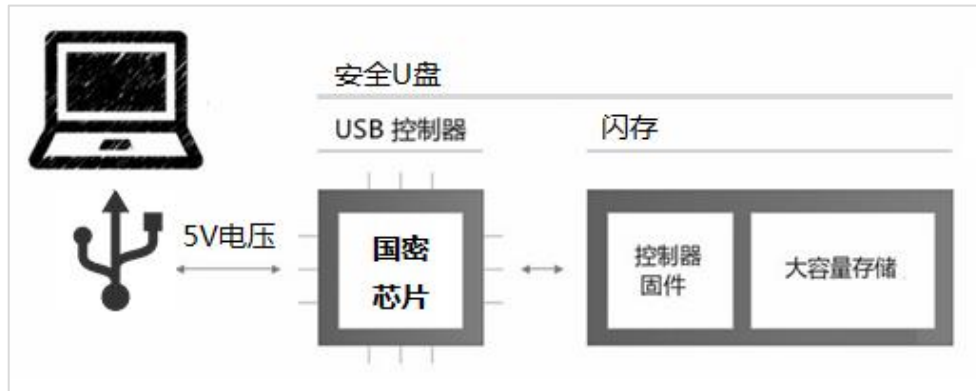
3.2.2 移动存储管理

移动存储介质管理模块解决 U 盘、移动硬盘等移动存储介质的使用合规问题，细化移动存储介质的使用权限，减轻病毒传播、数据泄露等风险。奇安信天擎的移动存储管理模块主要功能是针对移动存储介质的注册、授权的安全管理，实现按不同使用要求授予不同的权限，同时对移动介质进行状态管理，方便管理员进行集中管控。主要分为设备注册、设备分类授权、设备 ID 授权、挂失管理、外出管理、终端申请、漫游管理，移动存储例外，安全 U 盘（自带文件审计）几大控制功能。通过移动存储介质管理模块，管理员可集中管控内网终端的移动存储介质使用规则，规避移动存储介质带来的安全风险。

3.2.3 安全 U 盘

安全 U 盘是采用安全固件进行加密的移动存储介质，解决 U 盘存储控制权

的问题。安全 U 盘的存储操作由内置的控制软件进行控制，当 U 盘接入计算机后，U 盘与计算机的数据交换只能通过 U 盘内置的专用软件进行，极大减轻了 U 盘传播病毒的可能性。配合奇安信天擎的移动介质存储管理模块，管理员可对移动存储介质的读写、标签等进行细分授权和审计。



3.2.4 弹窗防护

终端启用弹窗防护功能可有效拦截第三方软件弹出的暴力、色情、游戏类的广告，避免日常工作或教学过程中出现软件弹窗受到影响。弹窗防护功能可对非主流第三方软件广告弹窗进行无差别拦截，终端用户可通过客户端自动抓取非主流第三方软件弹窗规则并上报拦截，管理员可在管理中心进行上报弹窗的运营和发布。

- 弹窗拦截规则自由制定，实时拦截
- 统一下发拦截策略，终端用户可自由调整
- 管理控制台实时统计拦截日志，按需检索

3.2.5 终端审计

奇安信天擎支持对终端进行行为审计和文件审计；

➤ 行为审计

■ 打印审计

对文件的打印行为进行审计，包括全量打印审计、指定打印审计。同时支持

打印类型的选择：网络打印、虚拟打印、本地打印及共享打印。

■ IM 审计

对 IM 类软件（QQ、微信、企业微信、钉钉）即时通讯消息进行审计。

■ 网站访问审计

对终端访问网站的行为进行审计。

■ 邮件审计

对终端收发邮件的行为进行审计。

■ 系统账号审计

对终端系统账号的登录、注销、锁屏和解锁操作行为进行审计。

➤ 文件审计

■ 文件流转审计

文件流转审计能力主要实现终端上所有文件的外发和读写审计，可通过文件的唯一 ID 对文件进行全流程跟踪，对文件流转进行行为审计。按照文档类型，在流转时可归档到文件服务器，并对文件流转和本地操作行为进行记录和审计，便于事后进行追溯。

文件流转分析能力通过对本地文件的新建、移动、复制、读写、删除、重命名通过指定的上传时间和流转通道（HTTP/HTTPS/FTP/SMTP/共享目录/移动存储/光盘刻录/QQ/微信/企业微信/钉钉）的控制，对文件进行详细的审计，实现文档的全流程跟踪和防护。

3.2.6 安全空间

奇安信天擎提供了创建安全空间的能力，通过管理员赋予权限可有安全空间的使用权，安全空间内的一切操作将会被严格保护。安全空间内数据默认保存在空间内，不允许外出。管理员可以通过策略中对空间内部分通道进行授权，允许数据外出。目前已支持的授权有剪切板、文件导出、防截屏、屏幕水印、打印控

制、打印水印、samba 共享、无痕模式、链接自适应等。

3.3 联动处置

3.3.1 防火墙及防毒墙联动

可与网络出口的防火墙、防病毒网关联动，实现高危终端的精准阻断封锁，实现病毒查杀以及终端精细管控。提供多域部署，部署位置不限于用户域、数据域、视频传输网和互联网等。实现对用户域、数据域、视频传输网和互联网的客户端进行管控。

3.3.2 宏病毒联合防护

支持 OA 系统在线文档宏病毒联合防护能力，能有效阻止和清除在线预览带有威胁的文档，可限制 OA 在线文档对本地宏模块的加载，防止 WPS 办公软件异常弹窗。在不影响正常文档编辑的前提下，能主动防御并清除终端上的异常文档进程，可阻止和清除 OA 系统上传的潜在威胁文档。



北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

让冬奥更安全 让世界更精彩
