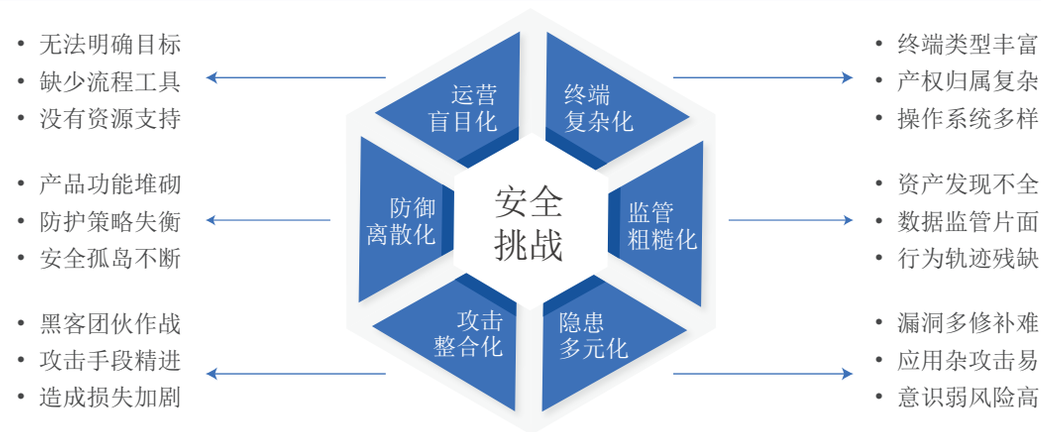
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

奇安信天擎终端安全管理系统

奇安信天擎终端安全管理系统（简称“天擎”）是注重实效的一体化终端安全解决方案，通过“体系化防御、数字化运营”方法，帮助政企客户准确识别、保护和监管终端，并确保这些终端在任何时候都能可信、安全、合规地访问数据和业务。天擎基于奇安信全新的“川陀”终端安全平台构建，集成高性能病毒查杀、漏洞防护、主动防御引擎，深度融合威胁情报、大数据分析和安全可视化等创新技术，通过系统合规与加固、威胁防御与检测、运维管控与审计、终端数据防泄漏、统一管理与运营等功能，帮助政企客户构建持续有效的终端安全能力。

产品价值 PRODUCT VALUE



能力一体，简化管理

采用一体化设计思路，即平台一体化、功能一体化、管理一体化，大幅降低终端安全体系建设、运行、扩展的复杂性。

防御闭环，风险可控

对安全威胁进行闭环防御，即预防、防护、检测、响应，有效防御各种已知、未知安全威胁，大幅降低安全风险。

管控到位，合法合规

对资产、用户、行为、数据等进行全生命周期的精细化管控，确保终端符合内外部的相关要求，真正做到合法合规。

效果清晰，按需提升

提供数字化运营方法、可视化运营工具，实时呈现终端安全效果，针对性分析当前不足，便于按需提升终端安全系数。

产品功能 PRODUCT FUNCTION

系统合规与加固

对操作系统的安全配置、漏洞补丁、软件安装合规性等方面进行检查和修复，通过契合的安全基线核查、有效的漏洞补丁管理、统一的软件管理，及时进行系统加固，达到收缩暴露面、“强身健体”的目的。

威胁防御与检测

集成多个防护引擎，再结合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，实现对可疑行为、已知病毒、未知病毒和各类攻击的实时拦截、高效检测、准确定位、完整溯源，并有效防御针对停服系统的漏洞利用攻击，确保终端始终安全。

终端管控与审计

通过对终端的管控、运维、审计，构建完善的主机管控与行为审计体系，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。

终端数据防泄漏

根据预先定义的策略，实时扫描存储和传输中的数据，评估数据是否违反预先定义的策略，并根据预设自动采取诸如警告、隔离甚至阻断等保护动作；集成资产管理、文件追踪、通道管控等功能，通过资产管控和安全水印等安全措施，实现终端数据防泄漏及泄露追踪。

管理与安全运营

通过管理中心实现全网终端的统一管理及策略、任务的统一下发，同时可利用其配套的安全管理平台实现基于量化指标的数字化安全运营。

产品优势 PRODUCT ADVANTAGE

多擎查杀 准确高效

依托奇安信深厚的攻防技术及安全大数据积累，自主研发的奇安信云安全引擎（QCE）、猫头鹰（QOWL）、海狮人工智能（QDE）及天狗（QTVP）等多个防病毒及主动防御引擎，天擎具备强大且高效的病毒查杀及攻击防御能力，多次高分通过国际权威安全能力测评。

功能一体 集中控制

以奇安信全新的“川陀”终端集中管理平台为技术底座，基于“一体化”理念设计，天擎只需要“一个客户端程序 + 一套管理平台”，即可实现补丁管理、病毒查杀、终端管控、检测与响应、数据防泄漏等各种终端安全能力，是一个功能全面、扩展灵活、兼容性好、资源占用低、运维管理简便的一体化终端安全解决方案。

多维嵌套 精细管控

得益于多年服务大型政企客户的经验，天擎充分理解大规模部署及复杂应用场景下的管理需要，提供策略模板、场景策略、用户策略、分组策略及灵活的用户权限管理等多项功能，让客户能够通过精细化、细粒度的终端管控设置，真正解决特定终端、特定用户、特定场景下的多维管控难题。

端网协同 联防协控

天擎可以与奇安信旗下的天眼新一代威胁感知系统、零信任安全系统、智慧防火墙（NGFW）、互联网控制网关（ICG）等产品实现深度的终端数据共享，为边界安全产品提供多维的访问控制决策支撑；还能接收并执行由天眼新一代威胁感知系统、安全运营中心下发的威胁处置指令，大幅提升攻击事件的响应效率。

指标驱动 实战运行

天擎配有终端安全运营平台（ESOP），将安装率、实名率、正常率、合规率等数字化指标与可视化分析技术相结合，为政企客户提供安全运营效果追踪及决策支撑，并通过持续的漏洞、病毒情报运营，帮助客户更好地对日常终端安全事件进行处置。