★完全公开

奇安信天擎终端安全管理系统
产品白皮书
V10.0

创建时间：2021 年 3 月 29 日
修改时间：2022 年 4 月 22 日

地址：北京市西城区西直门外南路26号院1号

邮编：100044

● 版权声明

● 免责声明

本免责声明（“**本声明**”）适用于奇安信集团（包括但不限于**奇安信科技集团股份有限公司、奇安信网神信息技术（北京）股份有限公司、北京网康科技有限公司**，以及前述主体直接或者间接控制的法律实体）旗下推出的全部产品和/或服务（以下统称“**本产品**”）。**如您使用前述产品，即表示您同意接受本声明的一切内容。如果您不同意接受，请立即停止使用相关产品。**

奇安信集团有权随时自行决定修改、添加或删除本声明的全部或部分内容。**您有责任定期检查免责声明部分的内容**，以了解是否发生了变更。**如您在我们发布变更后继续使用本产品，即表示您接受并同意这些变更。**

1. 您明确理解并同意，**本产品按“现状”提供**，不存在任何形式的明示或暗示保证，并且在适用法律允许的最大范围内，奇安信集团不提供任何明示或暗示的陈述或保证，包括但不限于有关适销性、适用于特定目的以及不侵犯第三方权利的保证。奇安信集团不保证产品中所含的功能将满足您的全部要求，也不保证您对本产品的使用不会中断或出错。**选择本产品来达到预期结果，以及安装、使用本产品并获取结果所带来的所有责任和风险由您承担。**

2. 奇安信集团承诺致力于不断提升产品的质量，本产品是在现有技术水平基础上提供的，但奇安信集团无法保证您使用本产品将完全符合您的期望，包括但不限于不能保证您【通过使用产品能够发现所有的安全漏洞以及能检测到所有的入侵威胁，检测到的入侵威胁不保证完全正确】，**您理解并同意，出现前述不符合您对产品期望的情形不视为奇安信集团违约。**

3. 您明确理解并同意，**您在使用本产品过程中可能发生不可抗力或不可预见的情形，包括但不限于：1)被某些未经许可的个人、团体或机构通过某种渠道获得或篡改；2)因通信繁忙出现延迟，或因其他原因出现中断、停顿或数据不完全、数据错误等情况，从而使交易出现错误、延迟、中断或停顿；3)因地震、火灾、台风及其他各种不可抗力因素引起的停电、网络系统故障、电脑故障等；4)计算机系统可能因存在性能缺陷、质量问题、计算机病毒、硬件故障及其他原因；黑客攻击、计算机病毒侵入或发作等非可归责于奇安信集团的原因；5）政府管制、网络故障、国家政策变化、法律法规之变化等。如发生不可抗力或不可预见的情形，奇安信集团将尽最大努力予以补救，但奇安信集团对于因不可抗力和不可预见的情形造成的各类直接或间接损失，均不承担任何责任。**

4. **对于任何本产品的使用行为，包括但不限于您自身和/或任何第三方的行为，奇安信集团均不承担任何责任。**

5. 对于从**非奇安信集团指定途径以及从非奇安信集团发行的介质上获得的本产品**，奇安信集团无法保证其是否感染计算机病毒、是否隐藏有伪装的特洛伊木马程序或者黑客软件。**使用此类产品，将可能导致不可预测的风险，建议用户不要轻易下载、安装、使用，奇安信集团不承担任何由此产生的一切法律责任。**

6. **上述免责声明适用于因任何性能故障、错误、遗漏、中断、删除、缺陷、操作或传输**

延迟、电脑病毒、通信线路故障、失窃、毁坏、未经授权的访问、篡改或使用（无论是出于违约、侵权、疏忽或任何其他诉因）而导致的任何损害、责任或伤害。

7. 奇安信集团保留在**不发布通知**的情况下随时采取以下行动的权利：**在执行常规或非常规维护、错误纠正或其他更改所必需时，中断或修改本产品的任何组成部分的运行或功能。**

8. 本声明受中华人民共和国法律的约束并依据其解释。

9. 在法律允许的最大范围内，本声明最终解释权归奇安信集团享有。

修订记录

版本	状态	修订理由和内容摘要	修订人	批准人	修订日期
V1.0	C	产品白皮书	熊瑛	熊瑛	2021.3.29
V2.0	M	产品白皮书	熊瑛	熊瑛	2022.4.22

状态：C-创建，A-增加，M-修改，D-删除

目 录

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 终端安全建设的需求与挑战

数字化转型大潮下，终端已不再是单纯的设备，而是组织雇员在数字世界中的代言人。终端用户期望通过多种多样的设备，在任意环境下，通过任意设备，可信、安全、合规地访问业务和数据，以便支撑工作的高效开展。

同时，越来越多用于特定工作场景的泛终端设备出现，如数字摄像机、自助服务终端、联网闸机等，此类终端同样需要可信、安全、合规地接入数字化业务系统，完成其替代人力的工作。

因此，当前运行于 IT 环境中的终端、泛终端设备，已经成为企业、政府或组织机构的“数字化员工”。数字化时代的终端安全建设，则是为了识别、保护和监管这些“数字化员工”，使其可以可信、安全、合规地访问业务和数据。

因此，当前技术环境下，终端安全建设必须回答三个核心问题：

1. 如何准确发现终端资产，识别并标定其数字化身份？
2. 如何对终端进行系统性的防护和监管，并实时感知内外部的安全态势？
3. 如何通过体系化方法，保障持续、有效、快速地识别、防护和监管终端？

然而，传统终端安全体系却存在四大短板，因此无法解决这三个核心问题。

- **单点防护，能力割裂**

终端具有威胁面广、暴露面大的特点，这决定了终端安全建设必须兼顾多项安全能力。在过去，企业通过持续叠加恶意代码防护、漏洞管理、外设管控等安全措施，提升对各类终端的保护强度。

而当前，企业网络已逐渐演变为极其复杂的巨型系统，先前独立建设的各项安全能力，逐渐演变成诸多安全孤岛，很难通过体系化方法来共同解决终端威胁。

- **防控为主，被动响应**

由防病毒、漏洞管理、运维管控组成的“三件套”几乎成为过去终端安全建设的标配，被形象的称为终端安全“老三样”。

然而，它们都是基于“堵漏、设防”被动防护理念设计的，寄希望于通过预设策略“御敌于城池之外”，在攻击整合化的今天，根本无力对抗有组织、目标明确的高级威胁，终端防护安全能力亟需向积极防御迈进。

- **分类纳管，各成体系**

在数字化转型过程中，终端早已不再局限于 Windows PC，运行不同操作系统、采用不同硬件架构的办公终端、业务终端、用户终端、移动终端、泛终端早已出现在 IT 系统中，它们同样需要被保护。

而多数组织仍然将终端安全建设的视角局限在单一类型终端上，并没有对各类终端进行分类防控，防控死角越来越多，大量新兴终端都处在未被纳管的状态。

- **重视建设，粗放运营**

安全产品的部署并不能直接带来安全能力的提升，部署安全产品后仍出现安全问题的案例则比比皆是。

当前多数组织的终端安全体系仍处在单一场景、工具型保障的建设思路上，

缺乏统一的、持续的运营支撑，使得安全措施形同虚设，无法应对最新的安全威胁。

3 数字化终端安全治理安全观

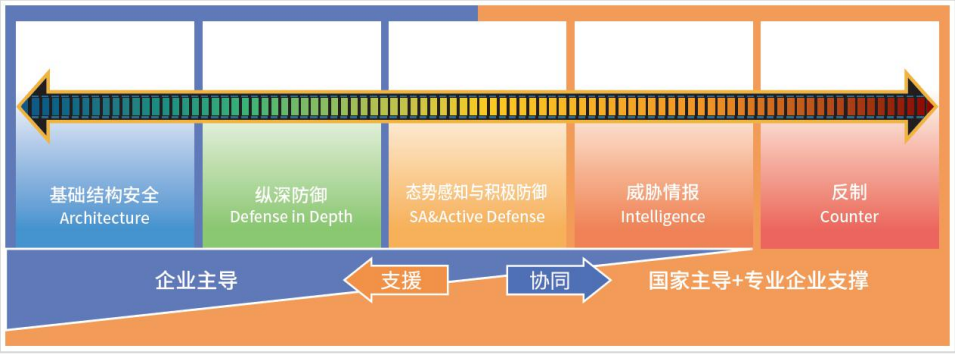
作为一个在数字化时代能够保障业务安全有序运转的机构，应充分考虑组织的管理模式和文化，在确保为终端用户提供良好用户体验的基础上，建设跨数字化终端类别的统一安全管理体系。

应在终端和接入环境上构建面向终端硬件、操作系统、应用软件、数据资源、用户身份、操作行为和末梢网络的一体化安全技术栈；指定和落实标准纳管、分权操作、分级管控、集中分析、全局可视的安全运营目标；充分利用终端的安全能力和数据资源，实现与企业数据安全、系统安全、身份安全、行为安全等其他安全运营目标的有效衔接和深度聚合，进而从容应对组织数字化转型过程的不断变化的边缘侧网络安全风险。

概括而言，企业终端安全治理应坚持“体系化防御、数字化运营”的技术理念，通过能力叠加建立纵深防御体系，并使用数字化指标牵引安全运营，以获得实战化的安全防护效能。

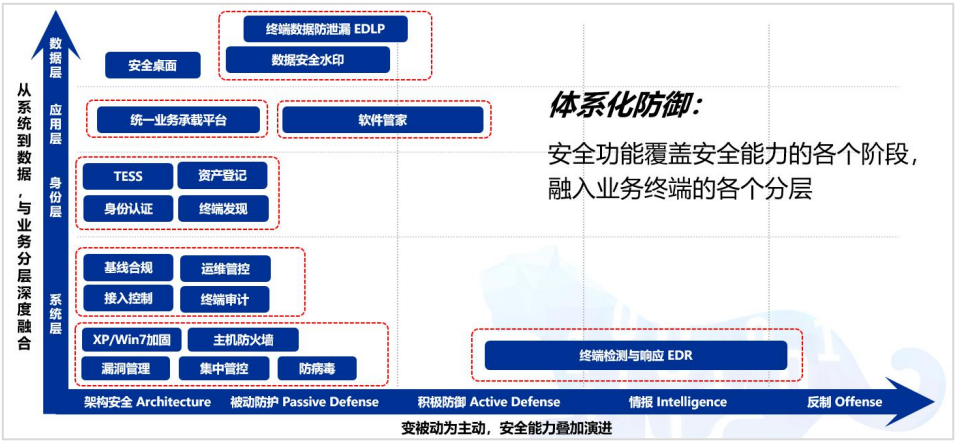
3.1 构建体系化的终端安全防御能力

根据 SANS 滑动标尺模型，网络安全能力体系包含五大类别安全能力，即：基础结构安全（Architecture）、纵深防御（Defense in Depth）、积极防御（SA&Active Defense）、威胁情报（Intelligence）和反制（Counter）。其中，基础结构安全、纵深防御、积极防御、威胁情报这 4 类能力是一个完备的企业级网络空间安全防御体系所需的，而反制能力主要由国家级网络安全防御体系提供。



鉴于企业终端在实际场景中执行业务操作，与之频繁交互的对象通常包括操作系统、用户身份、应用软件及业务数据，因此，可将终端进行逻辑分层，即系统层、身份层、应用层及数据层。

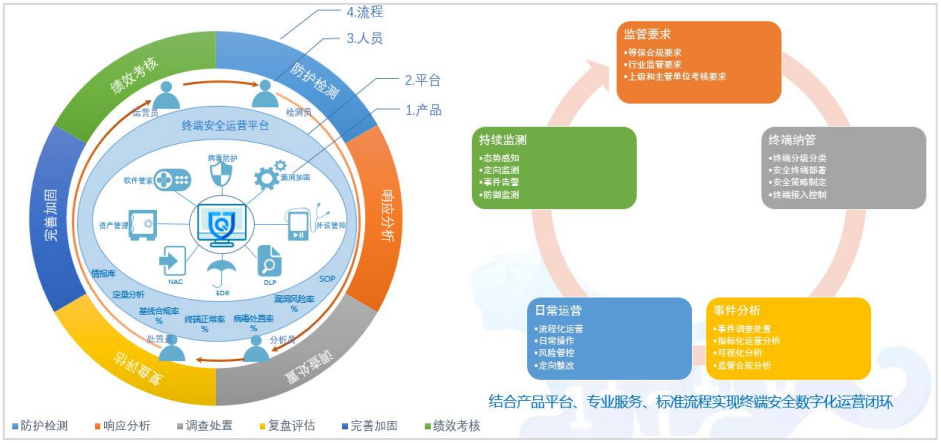
构建体系化终端安全防御，是指将采取的安全措施应覆盖至安全能力的各个阶段，并融入不同终端的各个分层。



3.2 实现数字化的终端安全运营

终端是企业最重要的 IT 基础设施，是“安全的最后一公里”，也是联接物理世界与数字世界的门户，一旦终端出现安全问题，轻则影响员工个人的正常工作，重则会造成企业全网瘫痪或者企业关键信息的外泄，给企业带来巨大的损失。终端安全建设只有动态演进，才能让终端获得持续保障，真正成为助力而不是阻碍业务发展。

终端安全运营，就是为了实现终端安全目标，提出安全解决构想、验证效果、分析问题、诊断问题、协调资源解决问题并持续迭代优化的过程。通过对安全运营过程的统筹管理，满足对终端安全的动态性、持续性和整体性需求。



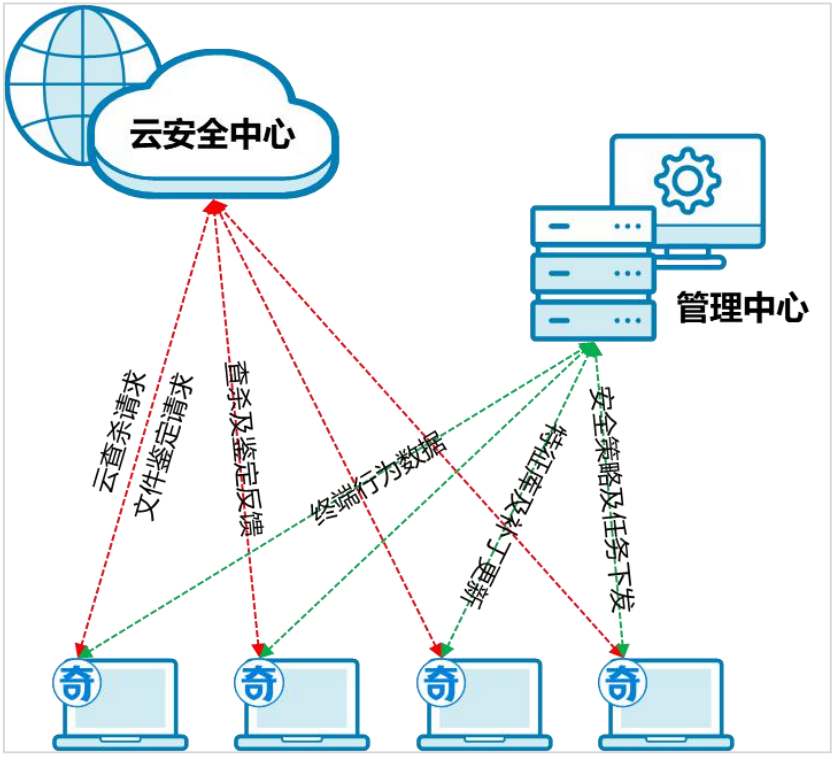
终端安全运营从根本上改变了被动响应单点事件的旧有模式，不再把安全局限在单点的攻防与决战，而是通过平时的积累，建立起一套标准化的流程体系，通过量化的指标对终端安全状况进行实时评定和展示，并基于预设的安全目标不断改进不足，确保终端始终安全。

4 产品架构

奇安信天擎终端安全管理系统 V10.0（以下简称“奇安信天擎”）是一款面向政企客户网络环境的平台化终端安全产品，基于奇安信全新的“川陀”终端集中管控平台构建，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，通过防病毒、漏洞管理、运维管控、基线合规检查、网络准入、终端审计、终端检测与响应（EDR）、终端数据防泄漏等安全功能，为政企单位业务终端提供体系化安全防护能力，并助力客户持续开展基于数字化指标的安全运营。

4.1 基础组件

奇安信天擎由管理中心和客户端程序两大组件构成。管理中心采用 B/S 架构，是管理员进行终端管理、策略下发、终端审计的管理入口；客户端则是一个独立的运行于主机本地的程序，执行管理中心下发的任务和策略，并采集上报安全审计、检测所需的终端行为数据。



➢ **管理中心**

奇安信天擎管理中心采用 B/S 架构，可以通过浏览器访问，对奇安信天擎客户端进行管理和控制，包括分组管理、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，管理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**

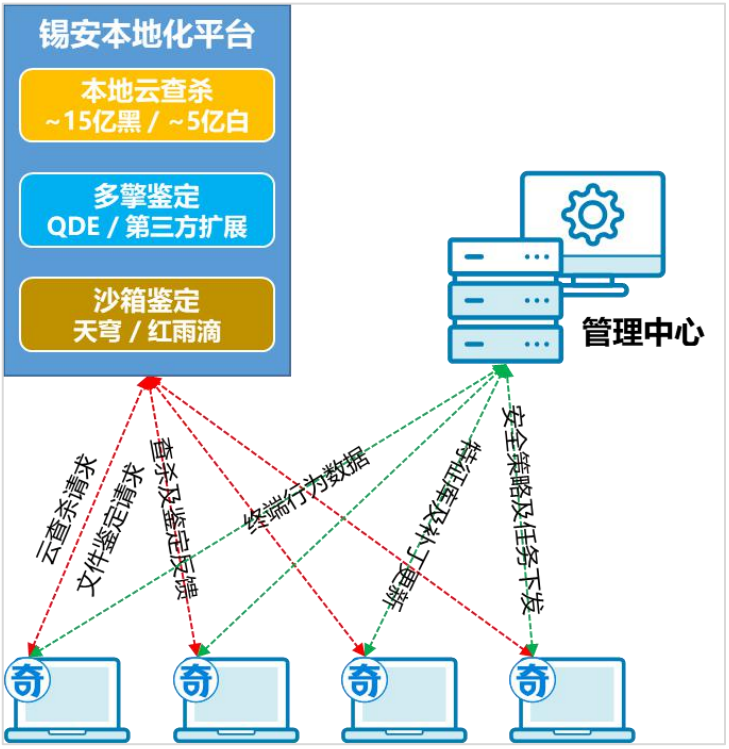
奇安信天擎客户端部署在需要被保护的终端或服务器上，执行木马病毒查杀、漏洞修复、安全防护等安全操作，并与管理中心通信，提供管理中心管理所需的相关安全告警信息。

4.2 配套系统

为实现特定使用场景下的安全功能，并保障应用效果，奇安信天擎为客户提供了丰富的配套系统，具体包括以下：

➢ **锡安本地化平台**

锡安本地化平台是奇安信天擎在隔离内网场景下的安全能力支撑平台，内置流行恶意文件样本库、人工智能病毒查杀引擎及沙箱，可在无互联网连接的情况下，为奇安信天擎提供接近公有云能力的病毒云查杀、未知文件鉴定服务。



- **NAC 网络安全准入引擎**

NAC 网络安全准入引擎通常以旁路模式部署于用户网络中，其通过与网内交换机进行 802.1X 联动，或利用 TCP/IP 协议自身机制，配合奇安信天擎实现终端入网身份认证、合规检测等安全功能。

当使能“网络准入”功能后，需同步配置该引擎。

- **大数据存储于分析平台**

大数据存储与分析平台用于存储并分析客户端采集的海量行为数据，其基于 ES 架构构建，并配置高性能、大容量存储部件，可为终端审计、终端检测与响应功能提供数据存储及分析服务。

当奇安信天擎使用“终端检测与响应（EDR）”功能，或使用“终端审计”功能且终端数量超过 3000 时，需同步配置该系统。

- **安全 U 盘**

安全 U 盘是采用专用安全芯片的 USB 存储设备，自带用户认证及数据保护程序，并可配合奇安信天擎“移动存储管理”功能实现高强度的 U 盘管控策略。

- **隔离网升级工具**

在隔离内网场景中，奇安信天擎无法连接互联网进行特征库及补丁库等的实时更新，为保证奇安信天擎的正常运行及安全有效性，可通过配置隔离网升级工具实现相关特征库的摆渡更新。

5 功能特性

5.1 系统合规与加固

系统合规与加固是指通过对操作系统的安全配置、漏洞补丁、软件安装合规性等情况进行检查和修复，加固系统自身，收缩暴露面，达到“强身健体”的效果。

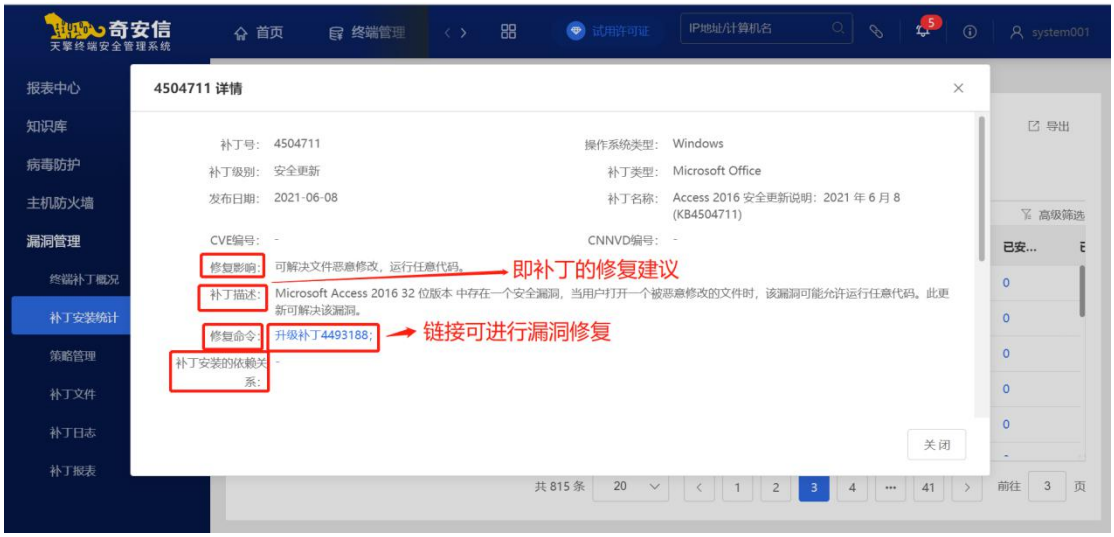
5.1.1 基线核查

基线核查功能通过参考相关的国家标准、行业标准，建立检查模板，对网内终端的基线配置进行检查和量化评估。

奇安信天擎的基线核查功能内置了安全等级保护二级和三级检查模板，还可以根据业务需求自定义检查模板，灵活控制检查标准。

5.1.2 补丁管理

补丁管理功能为企业多网络环境下的补丁安装、统计提供统一、集中的管理。奇安信天擎的管理中心可对装有客户端的终端下发补丁升级指令，收到升级指令的终端会连接部署在公有云的奇安信补丁服务器进行补丁升级。支持对终端系统及组件漏洞的检测及修复，提供包括补丁的修复建议、补丁安装的依赖关系、修复命令、修复影响等信息。



奇安信补丁服务器中的补丁均经过奇安信安全团队的测试，最大限度减小兼容问题。同时，为了进一步应对小概率的补丁兼容性问题，补丁发布升级可基于其自动化的编排能力进行多次分批安装，从而有效控制补丁兼容性问题可能对终端造成的运行风险。对于物理隔离的内部网络，可通过部署内网补丁服务器，利用离线下载工具导入补丁，实现内部网络环境的补丁管理。

5.1.3 软件管理

软件管理功能致力于解决终端软件的安装、授权、版本控制、使用统计等内网软件管理问题。在企业内网环境部署软件管理服务器，通过奇安信天擎的软件管理模块对内网终端进行软件安装管控、版本统计、升级管控、授权管控等操作，实现内网软件的来源可信、管控统一。

通过对软件的统一管理，可避免由于使用未知源带来的软件安全隐患，简化内网软件使用的维护操作，规避软件供应链等因素造成的风险。

5.2 威胁防御与检测

奇安信天擎对终端的安全威胁具有强大的防御、检测和响应能力，集成了奇安信自研的多个防护引擎及部分第三方扩展引擎，并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。

5.2.1 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。

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。

5.2.2 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，该功能需要连公有云。

5.2.3 Windows XP/ Windows 7 系统加固

Windows 7/Windows XP 加固主要解决系统停服后的漏洞利用攻击防护问题，防止针对系统 RCE、浏览器、Office 等应用的漏洞利用攻击。

奇安信天擎集成了采用第三代查杀技术的“天狗引擎”，将系统加固视角转移到检测系统行为的内存指令序列层面，基于内存指令序列检测，将内存指令控制流与可信指令序列特性进行匹配，判断应用程序的操作行为的合法性，评估超低频异常内存指令序列，并对应用程序权限智能控制。

该引擎的运用，改变了针对停服系统漏洞的被动响应模式，根据已知合法操作和已知非法操作，判断系统行为的合法性，阻断非法行为，有效提升针对停服系统漏洞、0Day 漏洞、“后门”等威胁的防御能力。

5.2.4 主机防火墙

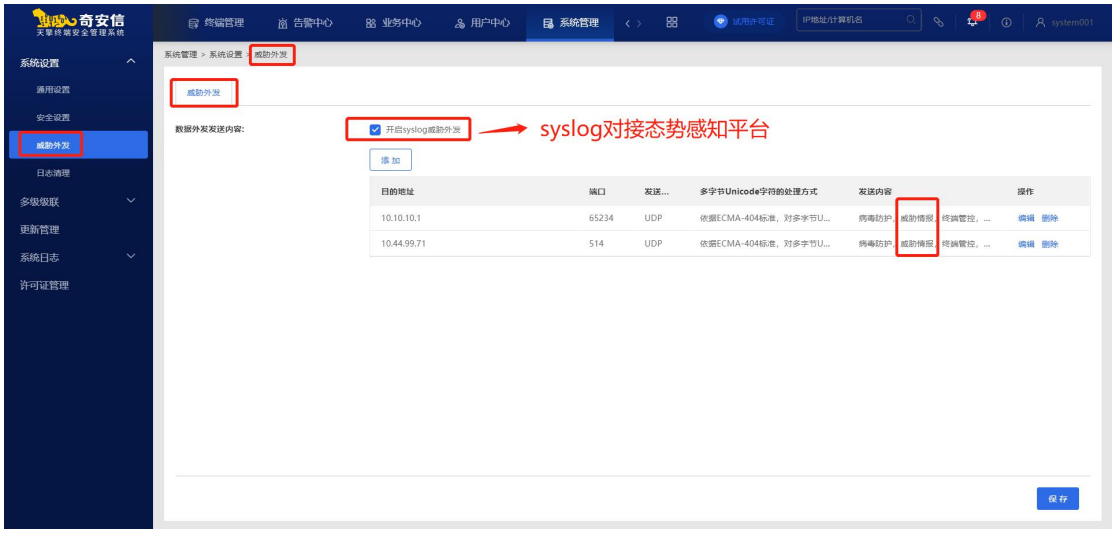
主机防火墙（Host Firewall），在终端上基于网络五元组信息对主机网络的出入站流量进行控制。通过配置和管理防火墙放行或拦截规则，对终端的异常网络请求进行有效控制。此外，可接管 Windows 系统自带的防火墙程序。

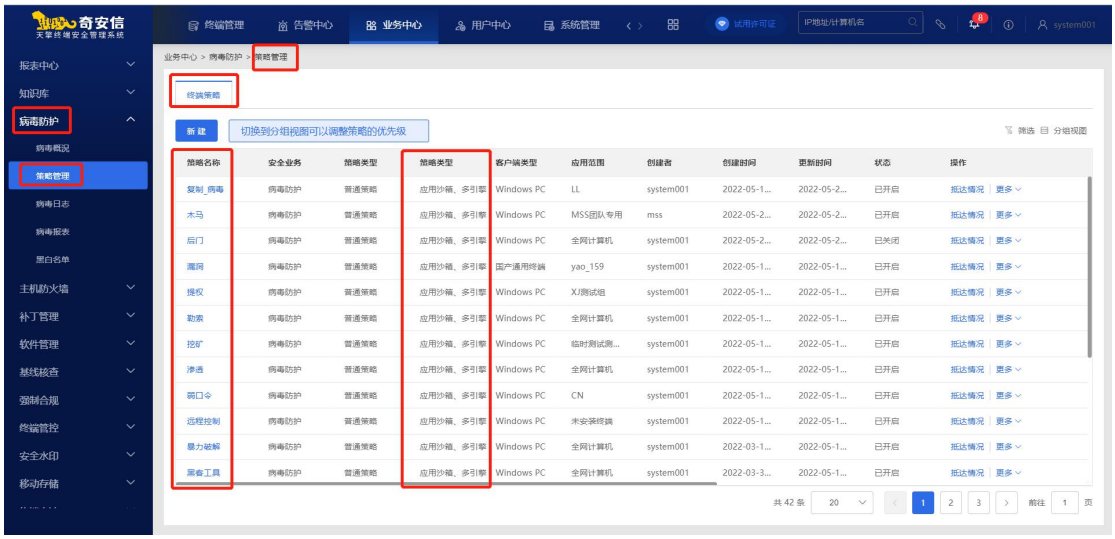
5.2.5 终端检测与响应

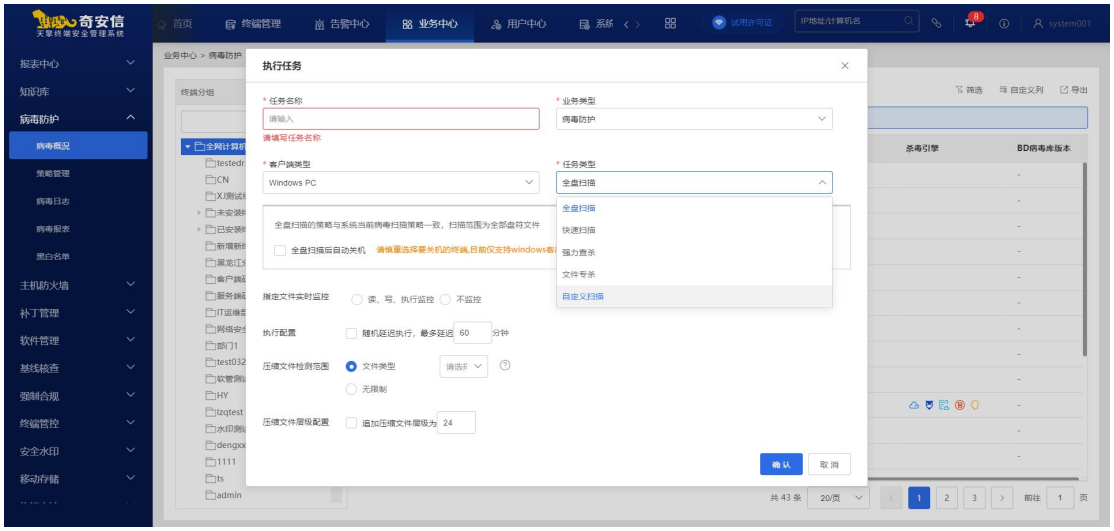
终端检测与响应（EDR）分为高级版和基础版两个版本；

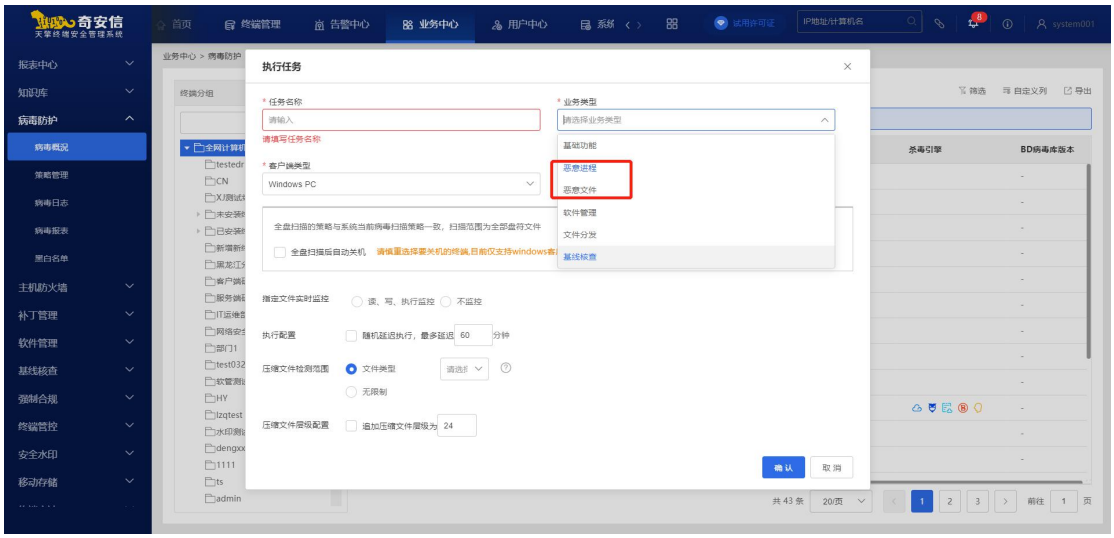
高级版能够对终端的系统级行为数据进行全量采集，并基于 IOC / IOA 等手段对其进行深度检测，及时告警可疑的恶意攻击或主机失陷，支持对接态势感知

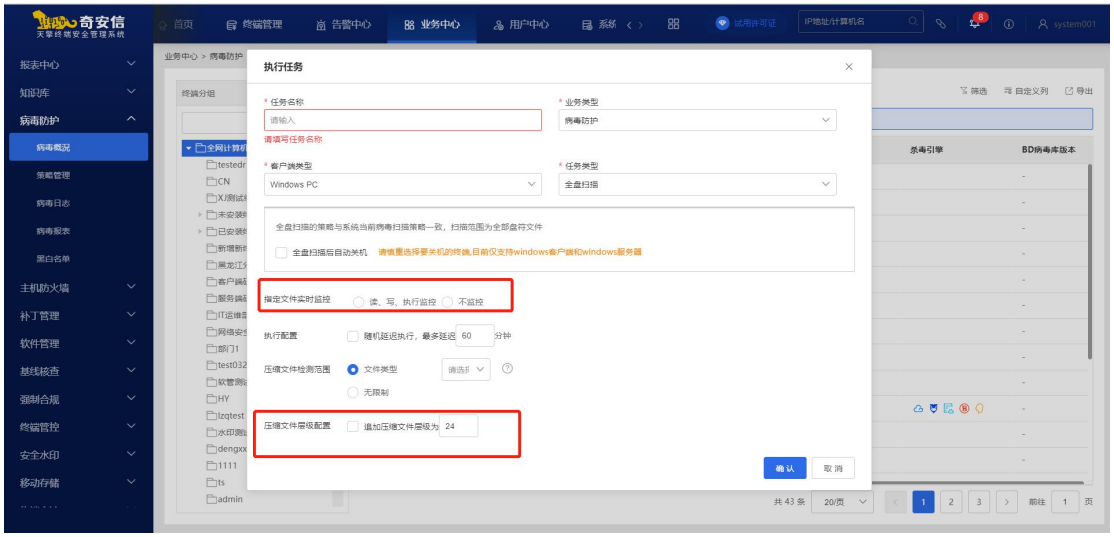
平台多维威胁情报，内置应用沙箱和多引擎等技术，检测范围包括但不限于病毒、木马、后门、漏洞、提权、勒索、挖矿、渗透、弱口令、远程控制、暴力破解、黑客工具等风险，提供快速扫描、全盘扫描、自定义扫描多种方式对恶意进程和恶意文件进行扫描，支持实时监控指定文件的读、写和执行，支持对 zip、rar、jar、cab、7z 等常见压缩文件的扫描检测，支持对压缩文件层级进行策略配置。






执行任务
* 任务名称
请输入
请填写任务名称
* 业务类型
病毒防护
* 客户端类型
Windows PC
* 任务类型
全盘扫描
全盘扫描
快速扫描
强力查杀
文件专杀
自定义扫描
全盘扫描的策略与系统当前病毒扫描策略一致，扫描范围为全部盘符文件
全盘扫描后自动关机
指定文件实时监控
读、写、执行监控
不监控
执行配置
随机延迟执行，最多延迟 60 分钟
压缩文件检测范围
文件类型
无限制
压缩文件层级配置
追加压缩文件层级为 24
确认
取消


执行任务
* 任务名称
请输入
请填写任务名称
* 业务类型
请选择业务类型
基础功能
恶意进程
恶意文件
软件管理
文件分发
基线核查
* 客户端类型
Windows PC
全盘扫描的策略与系统当前病毒扫描策略一致，扫描范围为全部盘符文件
全盘扫描后自动关机
指定文件实时监控
读、写、执行监控
不监控
执行配置
随机延迟执行，最多延迟 60 分钟
压缩文件检测范围
文件类型
无限制
压缩文件层级配置
追加压缩文件层级为 24
确认
取消


执行任务
* 任务名称
请输入
请填写任务名称
* 业务类型
病毒防护
* 客户端类型
Windows PC
* 任务类型
全盘扫描
全盘扫描的策略与系统当前病毒扫描策略一致，扫描范围为全部盘符文件
全盘扫描后自动关机
指定文件实时监控
读、写、执行监控
不监控
执行配置
随机延迟执行，最多延迟 60 分钟
压缩文件检测范围
文件类型
无限制
压缩文件层级配置
追加压缩文件层级为 24
确认
取消

同时，EDR 基于大数据存储分析平台，可对采集到的全量数据建立内在关联，并通过可视化界面帮助管理者对告警信息进行研判，并对威胁事件进行深入的回溯分析。

基础版结合云端威胁情报大数据，专注于对已知威胁事件的深度溯源，确保用户能够从源头彻底清除威胁。

EDR 高级版和基础版同时兼顾终端调查、威胁事件风险性评估的能力，可对已确定的威胁执行面向进程、网络、主机的隔离、阻断等处置操作，也支持与奇安信旗下天眼产品的联动处置。

5.3 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。

5.3.1 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，支持主动扫描未安装客户端的终端，对终端进行探测管理。

- **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

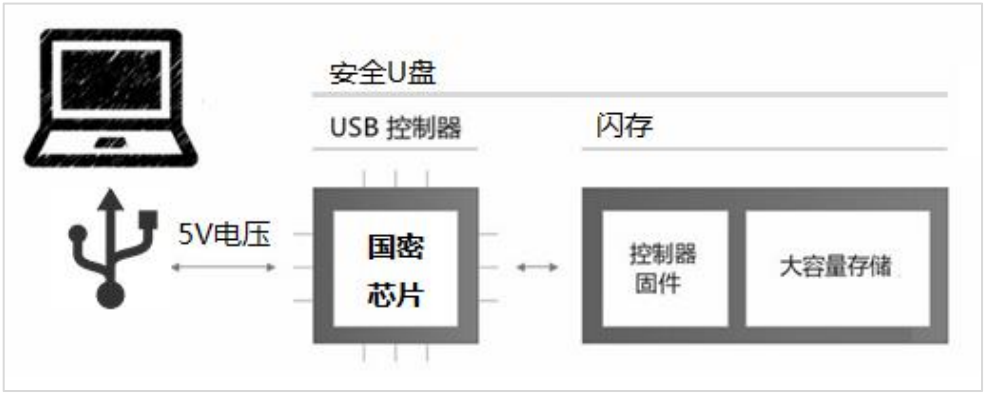
光驱进行管控；对 USB 存储设备，存储卡，冗余硬盘，打印机，扫描仪，磁带机，键盘，鼠标，红外，蓝牙，摄像头，手机/平板,移动数据网卡，MODEM 设备，ISDN 设备，ADSL 设备进行管控，控制方式为禁用和允许两种方式。

- **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。

- **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。



- **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。为避免客户端上报服务器日志过多，给服务器带来较大压力，还可按需设置日志最大上报限制。

- **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。

5.3.2 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

5.3.3 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。

➢ **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。

5.4 终端数据防泄漏

终端数据防泄漏能够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。此外，该功能还集成了文件追踪功能，通过资产管控和安全水印等安全措施，实现数据防泄漏及泄露追踪。

5.4.1 通道管控

基于预设策略，对数据传输的网络通道、设备通道或应用程序通道进行监控，若传输内容匹配预设的敏感信息特征，则可执行审计、审批或阻断的操作。

支持的通道管控网络通道包括 **HTTP/HTPTS/FTP/SMTP/共享目录等**，数据通道包括 **USB、CD-RO、蓝牙、打印等，**应用程序通道包括常用的 IM 类软件、邮件客户端、网盘客户端等。

5.4.2 安全水印

针对打印、拍照、截屏等场景提供安全水印功能，通过数字水印的输出，可直接、间接识别出泄露身份信息，实现泄露溯源。

- **打印水印**

在软件打印的时候获取打印操作行为，将水印信息以明文或二维码的方式附加到打印内容里，送到打印机进行打印输出。

- **屏幕水印**

屏幕水印采用屏幕浮水印技术，使水印信息呈现在屏幕最外层，通过截图、拍照方式获取的图片结果会附带相应的水印信息。

- **截屏水印**

通过截屏操作获取的图片，会自动附带终端信息、截屏时间和用户信息。使用过程中屏幕无任何水印信息展示，图片泄漏后，将图片导入系统，即可溯源用户、时间及终端信息。

5.5 管理与安全运营

奇安信天擎可通过其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。

5.5.1 统一管理

奇安信天擎支持对终端资产进行集中、统一的管理，在建立资产与用户、角色关联分组后，通过可视化的任务配置，对终端进行管理操作，同时支持集中处理告警信息。

- **资产管理**

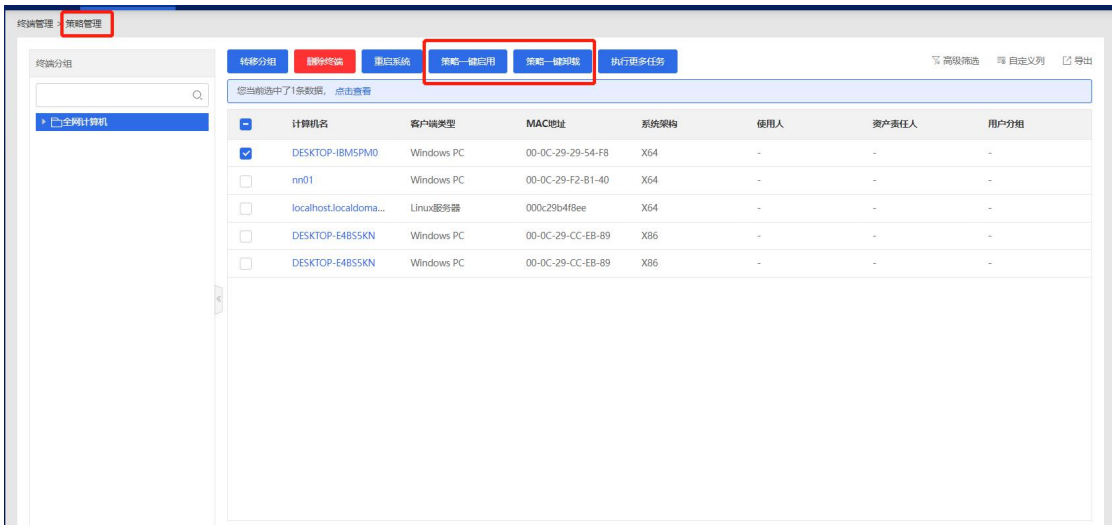
通过终端发现功能，解决庞大网络环境中客户端安装管理、以及对终端资产的信息统计和资产安全管理问题。当终端安装客户端后，客户端会主动连接管理中心，并通过内置插件进行终端信息扫描，将终端的基础 IT 信息和接入信息报送至管理中心，管理中心可对已发现的终端进行分组、责任人关联等操作。终端发现功能为管理员对新入网终端的资产统计分类提供了便利。

- **用户管理**

灵活的用户权限角色创建及分组配置，支持超级管理员、普通管理员、审计管理员三种权限。并通过角色的划分实现用户权限的差异配置。用户导入方式支持通过第三方服务器进行导入，简化创建操作。

- **策略管理**

奇安信天擎将终端安全管理各维度的策略集中进行管理，方便管理员统一配置各维度策略。奇安信天擎支持终端管控、安全水印、终端数据安全等多方位安全运维角度的管控配置相关策略，支持通过管理平台对客户端的统一启用和卸载，满足客户端安全策略的统一配置和下发。



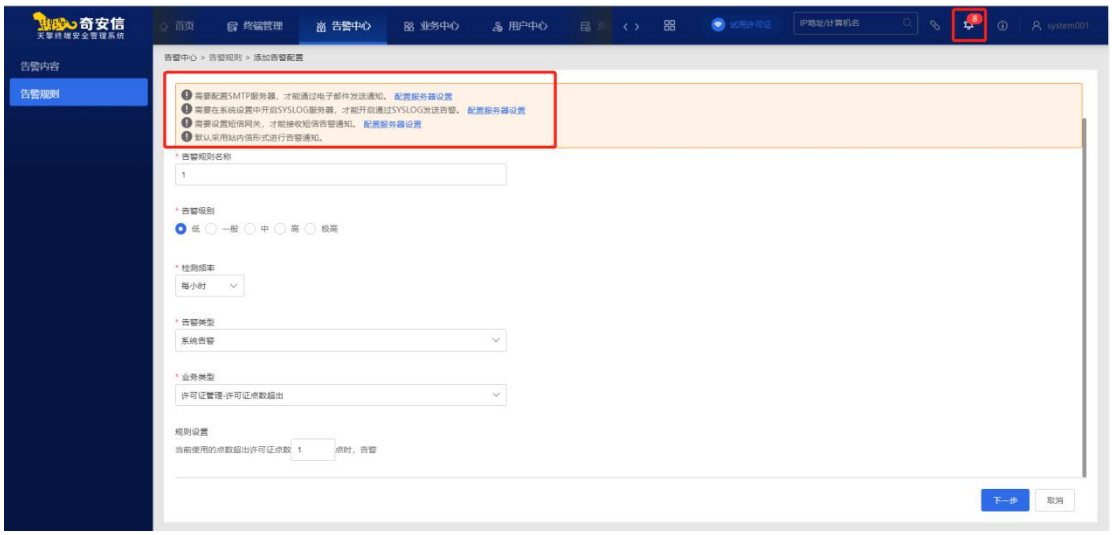
- **任务管理**

奇安信天擎对终端的集中管控以任务的形式实现，管理员可通过任务管理模块，配置周期任务、单次任务，以及管理任务的执行周期及执行范围，进行可视可控的任务管理。

- **告警中心**

奇安信天擎支持统一处置终端安全的告警信息，告警的产生基于不同策略的

配置及终端行为的监测，告警中心可详细展示告警的事件类型、风险级别、告警源等要素，方便管理员及时查看及处置，告警方式多样，支持邮件、SYSLOG、短信、站内信形式的告警通知。



➢ **统计报表**

奇安信天擎支持将丰富详细的终端信息转化为统计报表，报表输出包括但不限于终端的名称、地址、漏洞、恶意文件、恶意进程等多维度的，报表格式包括但不限于 word、pdf、html、xls 等格式，统计报表支持管理员自定义创建相关统计模板，报表生成后支持通过邮件的方式及时报送，为管理员提供数字化、可视化、可量化的终端安全运营依据。

5.5.2 安全运营

奇安信天擎用户可部署其配套的终端安全运营平台（ESOP），助力安全运营开展。该平台基于对企业终端安全状况的数字化指标定义，并利用终端安全管理系统运行数据的分析结果，以可视化手段全面展示终端安全运营效果，从而为管理者提供终端安全运营状态感知和安全决策的支撑。

该系统可从资产、漏洞修补、病毒防护、终端管控等维度全面揭示终端安全威胁情况，帮助客户构建终端安全的“指挥中心”。

➢ **终端安全运营概况**

可直接根据安全要求定义可量化的终端安全指标，包括安装率、正常率、实名率、基线合规率、病毒扫描执行率、病毒处置成功率、病毒风险终端比率、漏洞风险终端比率等，支持展示但不限于病毒、木马、后门、进程、漏洞、勒索、挖矿、弱口令等风险的全网风险展示，并对上述指标进行实时统计，并以可视化方式呈现网内特定终端的安全状况。

➢ **安装部署及资产概况**

可对奇安信天擎的安装进度、目标、分组安装情况，以及安装部署趋势、终端类型、操作系统分布、终端安装卸载事件、终端升级事件等数据进行统计及可视化展示。对终端的操作系统、软件、端口、账户、启动项、计划任务等信息的统一清点。对终端的所属责任人、责任人联系方式、资产位置等信息的统一登记。同时，对全网终端的操作系统版本、操作系统激活、未激活操作系统排行、资产未登记部门排行、软件安装、资产登记趋势、计算机品牌、CPU、内存、硬盘等资产数据进行统计展示。

➢ **漏洞修补概况及分析**

可支持全部漏洞以及高危漏洞的筛选，以方便针对重点漏洞进行数据统计；支持云端数据更新，以便第一时间了解最新漏洞，及时制定对应的安全决策准备；支持级联与分组的双视图切换，从不同管理维度查看漏洞全貌；可利用云端漏洞威胁情报，结合内网终端数据，对指定漏洞进行完整性安全分析。

➢ **病毒防护概况及分析**

可实现病毒仍感染次数、感染次数、中毒终端分布、仍感染终端比率排行、查杀趋势等统计数据的展示。同时，可针对特定病毒，查看内网终端的感染情况。支持追溯展示病毒在内网的感染历史与趋势。病毒事件分析大屏支持各分组仍感染终端分布及仍感染终端比率排行，精准定位当前感染分布；支持级联与分组的双视图切换，从不同管理维度查看病毒全貌。

➢ **终端管控概况及分析**

可对违反终端管控策略的告警信息进行统计集分析，包括分组告警、终端告警统计、告警趋势统计、远程统计、告警终端 Top5、策略部署统计等。针对违规外联事件，统计信息包括违规外联终端比率、违规外联时长、外联趋势、外联终端分布、外联次数、外联设备接入类型、违规出口统计等。

5.5.3 数据开放平台（ODP）

奇安信天擎内置终端安全管理系统数据开放平台（简称 ODP），可对外提供应用编程接口（简称 API）数据服务，第三方软件或者平台可通过调用 ODP 接口获取终端安全管理系统里的终端信息，实现奇安信天擎与第三方管理平台的集成与数据协同。

ODP 接口提供的数据信息包含终端和分组信息、防病毒信息、漏洞信息、终端管控信息、终端发现信息、软硬件资产信息等。

6 核心优势

➢ **多擎查杀，精准高效**

奇安信天擎内置云查杀（QCE）、猫头鹰（QOWL）、海狮人工智能（QDE）及天狗等多款防病毒及主动防御引擎。基于奇安信深厚的攻防技术及安全大数据储备，各引擎具备领先的病毒查杀及攻击防御能力。其中，云查杀引擎收录流行样本特征超 200 亿，覆盖政企网络环境流行样本；猫头鹰本地查杀引擎可支持识别 50 余种文件格式，针对各类文件具有丰富的典型特征提取能力，确保样本特征精度；采用第三代查杀技术的天狗引擎则可基于内存指令序列检测实现 0Day 漏洞、后门攻击的防护。在多安全引擎的共同加持及协同运行下，奇安信天擎具备极强的恶意代码及漏洞攻击防护能力，并多次高分通过国际权威安全能力测评。

此外，奇安信天擎客户端基于奇安信最新的“川陀”平台进行了重构，其病毒扫描速度及效能得到了大幅提升：相较上一版本，奇安信天擎客户端在快速扫描、自定义扫描等不同模式下的效能优化比率均大于 70%，达到行业领先水平。

➢ **功能一体，集中控制**

奇安信天擎是国内“终端安全一体化”理念的开创者和践行者，其功能覆盖架构安全、被动防护、主动防御等各个安全能力阶段，深度集成了补丁管理、病毒查杀、终端管控、检测与响应、数据防泄漏等多项功能，并通过奇安信天擎管理中心对上述功能实现统一配置及运行监控，真正实现了通过一个客户端程序、一套管理平台全面解决各类终端的安全问题。

相较同类产品，采用一体化设计的奇安信天擎具有功能全面、扩展灵活、兼容性好、资源占用低、运维管理简便等技术优势。

➢ **多维嵌套，精细管控**

基于奇安信天擎多年服务于大型政企客户的经验，其面向大规模部署及复杂场景的管理特性得以持续打磨和提升。

通过策略模板、场景策略、用户策略、分组策略及灵活的用户权限管理等功能，奇安信天擎可为特定终端、特定用户在特定场景下设定多维管控策略，实现精细化、细粒度的终端管控，满足政企客户日益复杂的终端管控需求。

➢ **端网协同，联防协控**

终端是一切恶意攻击的“着陆点”，而网络边界是恶意攻击要突破的第一道防线，作为安全防护体系部署的重要阵地，部署于终端与网络边界的安全措施应实现数据共享、协同防御及联动处置。

奇安信天擎可与奇安信旗下的零信任系统、下一代防火墙（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，实现端网协同防控。

此外，奇安信天擎可基于标准接口，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，实现网络侧及终端侧的协同处置，大幅提升攻击事件的响应效率。

- **指标驱动，实战运行**

奇安信天擎致力于为客户提供“实战化”的终端安全防护效果，其配套的终端安全运营平台（ESOP）作为客户开展常态化运营的保障工具，创造性的将安装率、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，为用户提供安全运营效果追踪及决策支撑。

同时，通过持续的漏洞、病毒情报运营，ESOP 针对特定的漏洞及病毒事件可提供影响分析、防护措施、处置方法等信息，指引用户对日常的事件进行处置。

7 用户价值

- **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，按需提升终端安全管理成熟度。

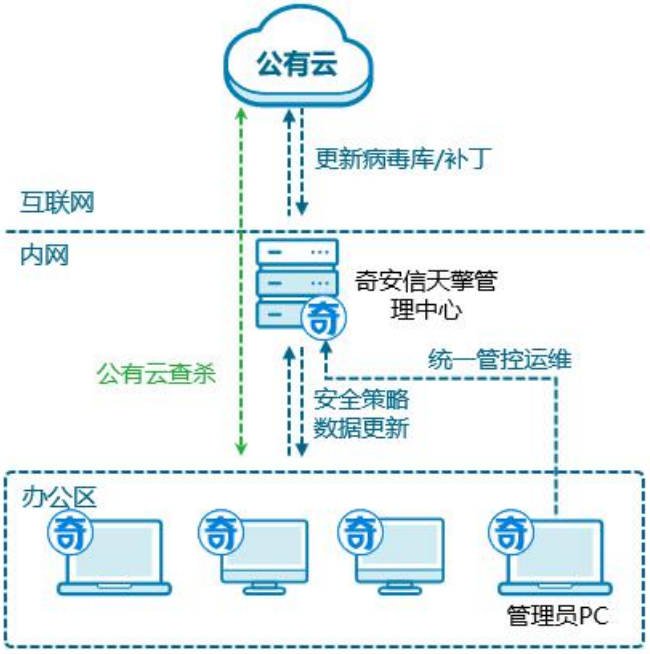
8 部署方案

8.1 互联网络部署方案

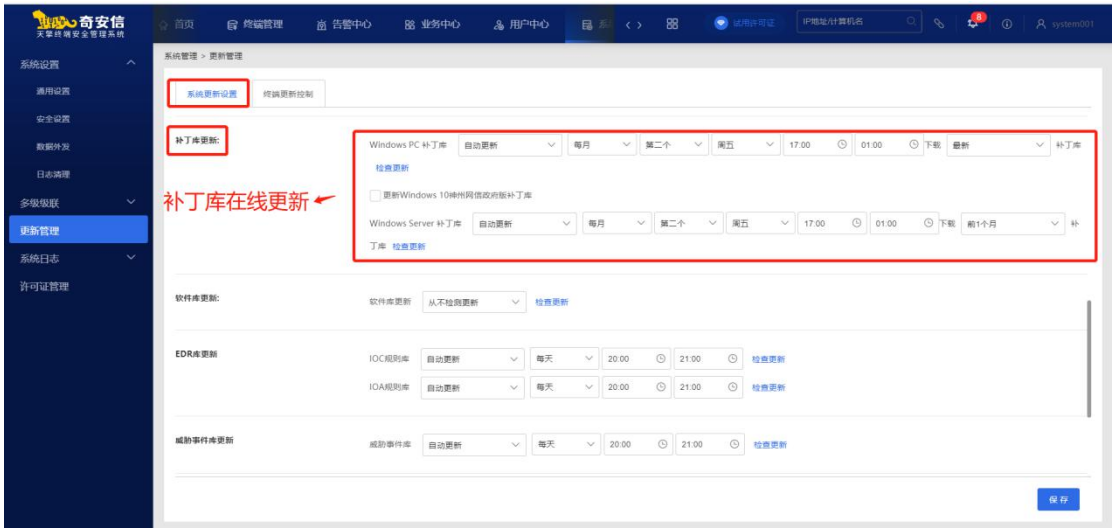
➢ **方案特点**

本方案适用于能够连接互联网环境的客户，客户网络中部署奇安信天擎服务端（具体配置要求请参考《部署安装手册》），办公终端安装奇安信天擎客户端，通过管理中心对办公终端做统一的安全防护和管理。

➢ **部署示意图**



在网络内部署奇安信天擎（管理中心），通过在线安装或者离线安装包的方式安装奇安信天擎客户端。管理中心支持管理平台、客户端、病毒库、补丁库通过互联网连接到云端的升级服务器进行在线升级、更新，然后客户端通过管理中心统一进行升级、更新及策略下发，可以极大地节省企业总出口带宽，同时对于物理隔离的内部网络，可通过部署内网升级服务器，利用离线下载工具导入进行对管理平台、客户端、病毒库、补丁库，实现内部网络环境的升级管理。



客户端会根据管理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。可以设定终端是从管理中心更新病毒、补丁库，还是从互联网更新。

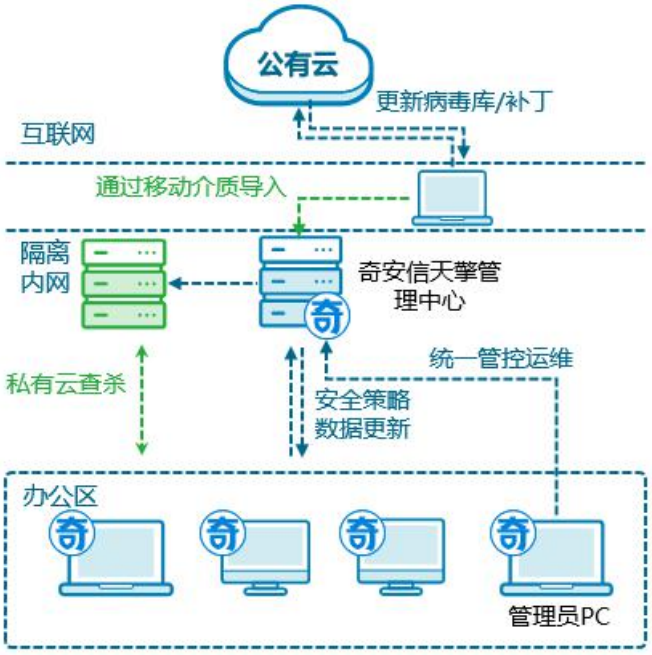
终端可连接云端进行云查杀，极大地提高终端病毒的查杀能力。

8.2 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客户，网络中部署一套奇安信天擎服务端（具体配置要求请参考《部署安装手册》），网内中的终端安装奇安信天擎客户端，通过管理中心进行统一的安全防护和管理，管理中心的病毒、补丁等更新程序通过离线升级工具进行升级。

➢ **部署示意图**



在客户网络中部署奇安信天擎管理中心，通过在线安装或者离线安装包的方式安装终端客户端，客户端会根据管理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。

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；然后使用移动存储介质更新到内网的管理中心，用户的终端连接到内网管理中心进行自动升级和漏洞修复。

8.3 部署环境要求

8.3.1 操作系统要求

天擎终端安全管理系统安全管理中心 Windows 安装包支持的操作系统包括：

1、 Windows Server 2012 64 位，Windows Server 2016 64 位；

2、 CentOS 7.2-7.6 64 位；

8.3.2 安装目录要求

Windows 版系统默认安装路径为 C:\Program Files (x86)\qianxin\Tianqing Endpoint Security，您可以根据实际情况修改对应的安装路径（建议安装路径设置 为非系统盘，且所在盘符剩余空间大于 70GB）。

8.3.3 单机本地化部署版服务器要求

天擎终端安全管理系统安全管理中心支持部署在硬件服务器和虚拟化服务器上，在对安全管理中心进行安装时需要提前根据如下要求准备对应的服务器环境，授权到期后不影响管理平台的正常使用，建议的服务器配置为：

管理的终端数量	服务器配置
1000	CPU ：最低 8 核2.4Ghz； 内存容量：最低 16GB ； 硬盘：最低 500GB，推荐 1TB，IOPS 在2W 以上的磁盘； 推荐操作系统：Windows Server 2012/2016 64 位； 网卡：千兆单网卡；
5000	CPU ：最低 16 核 2.4Ghz； 内存容量：最低 32GB ； 硬盘：最低 1TB，推荐 SSD 或IOPS 在2W 以上的磁盘； 推荐操作系统：Windows Server 2012/2016 64 位； 网卡：千兆单网卡；

8.3.4 集群版本地化部署服务器要求

天擎 v10 在 CentOS 7.2 以上的环境上进行过大量的测试，同时也是手册操作系统的最佳实践，因此建议使用手册要求的操作系统来部署天擎 v10。操作系统可运行在物理服务器以及 VMware、KVM、XEN 主流虚拟化环境上，授权到期后不影响管理平台的正常使用。

对于集群版最低配置服务器要求如下：

终端点数	资源配置A套餐	数量	备注
10000	CPU：16C，2.40GHz及以上	4台	1，不同的硬件资源、业务模块所支撑的点数会有差异（表中所列配置参数不包含DER、DLP和审计业务） 2，部署在物理环境或者虚拟化环境均可 3，存储预估是基于业务生成的日志数据且存储180天 4，磁盘建议：IOPS值：20000；吞吐量：160MB/s
	内存：32GB		
	磁盘：系统盘100GB，数据盘：1500GB		
	网卡：千兆网卡		
	操作系统：CentOS7.2 ~ CentOS7.6		
	资源配置B套餐	**数量**	
	CPU：8C，2.40GHz及以上	6台	
	内存：16GB		
	磁盘：系统盘100GB，数据盘：1000GB		
	网卡：千兆网卡		
	操作系统：CentOS7.2 ~ CentOS7.6		

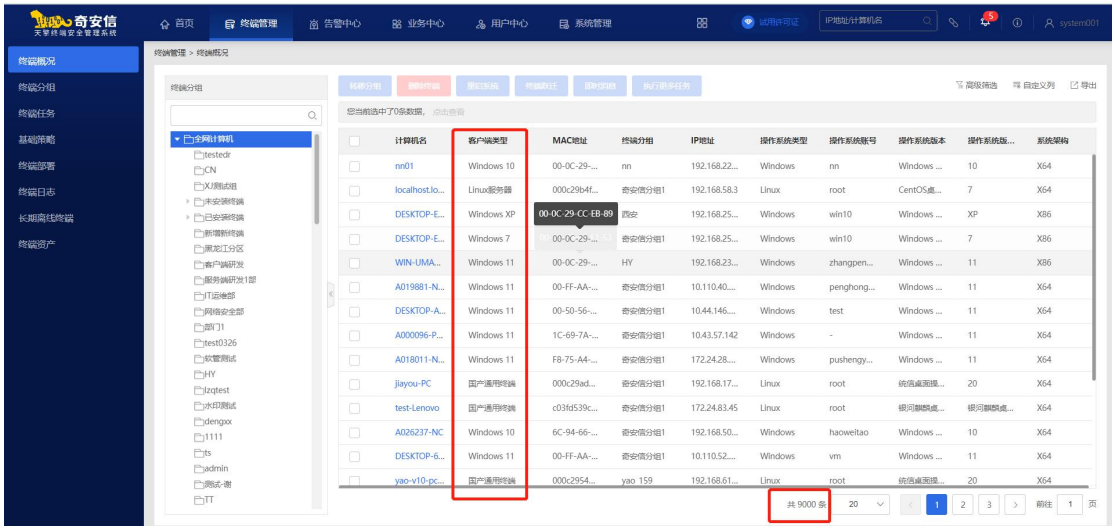
8.3.5 终端支持的操作系统类型

天擎终端安全管理客户端支持部署在如下操作系统类型上，支持终端授权数量 3000 点以上，客户端支持 Windows XP/Windows 7/Windows 10/Windows 11 等，详细信息如下表：

系统类型	操作系统	是否支持
Windows 个人版	Windows xp 32 位 sp2 及以上版本	支持
	Windows vista 32 位版本	支持
	Windows 7 (32 位、64 位)	支持
	Windows 8 (32 位、64 位)	支持
	Windows8.1（32 位、64 位）	支持

	Windows10 (32 位、64 位) th1、th2、RS1、RS2、RS3、RS4 和RS5 版本版本	支持
	Windows11 (32 位、64 位)	支持
Windows 服务器版	Windows 2003 server SP2(32 位、64 位)	支持
	Windows 2008 server(32 位、 64 位)及 R2(32 位、 64 位)	支持
	Windows 2012 server 及 R2	支持
	Windows2016	支持
	Windows2019	支持
Linux 服务器版（64 位）	Ubuntu(10、12、14)	支持
	Redhat(5.x、6.x、7.0、7.2)	支持
	SuSe(11 sp3、12)	支持
	SLES10-sp2/4-x64	支持
	SLE-12-Server-DVD-x86_64-GM	支持
	ESXi 5.5/6.0	支持
	H3CV2.0 D0219	支持
	XEN server 6.5	支持
	CentOS(5.x、6.x、7.0、7.2)	支持
国产操作系统	Kylin-4.0-1E-server_x86_64 Kylin-4.0.2-server_x86_64 Kylin-4.0-1E-server_x86_64 UniKylin-Desktop-334-x64	支持

	NeoKylin-DesktopV7-x86_64 NeoKylin-DesktopV6-x86_64 NeoKylin-AS-x86_64 V6.4 NeoKylin-AS-x86_64 V7U2 NeoKylin-AS-x86_64 V5.4 NeoKylin-Desktop-4.0-x86(32bit)	支持
	NeoKylin_desktop-v6_mips （ 3A900 、 3B1500） NeoKylin-AS-4.0-mips(3A1000,3B1500) NeoKylin_desktop-v7_mips (3B1500 、 3A2000) NeoKylin advanced server v6 update5_64_mips(3A1000) Deepin15-desktop-mips32 （ 3B1500 ） Deepin-mips64-15.1-server （ 3A2000 ） Deepin-mips32 15.1.1 桌面版(3A2000) iSoft-Desttop-v5-mips64el (3A2000)	支持
	飞腾 1500 银河麒麟 server-4.0.2-sp1	



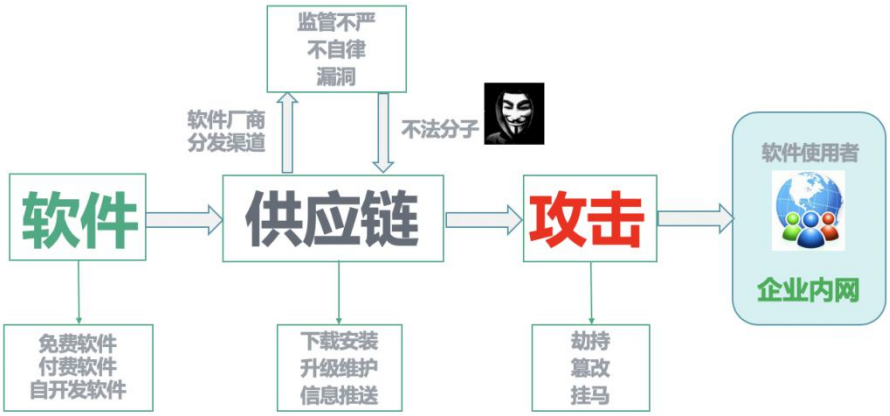
9 应用场景

9.1 勒索病毒防护场景

奇安信持续给政企用户提供专业化的终端安全防护——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，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，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。

9.2 软件供应链安全防护场景



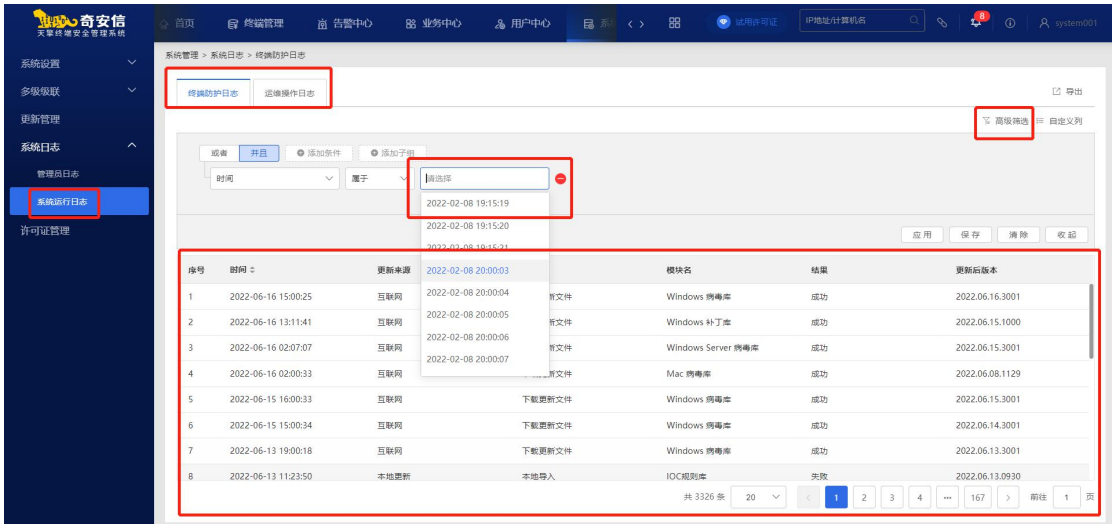
奇安信天擎终端安全管理系统针对于软件供应链安全防护场景，可通过软件管家模块提升软件安全管理，来解决软件供应链场景下的终端安全防护。

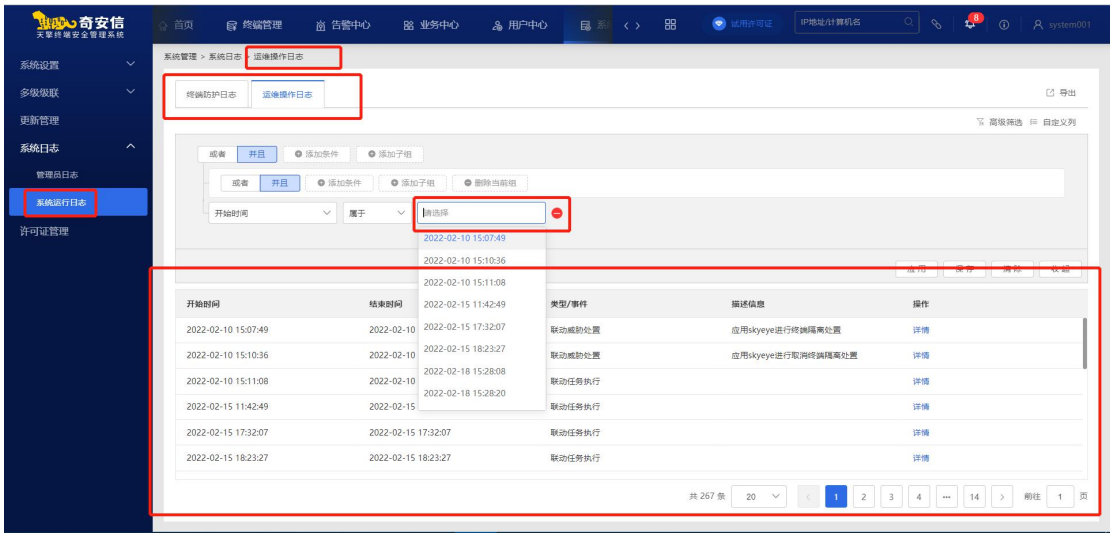
- 控制软件版本，软件版本不统一导致低版本软件存在于某些终端，这些终端称为网络中被攻击的信息点。
- 确保软件下载源的唯一性，避免恶意篡改的软件进入内网。
- 利用软件管家自动升级，某些软件强制升级功能，加强软件的统一管理。

9.3 高级威胁防护场景

奇安信天擎终端安全管理系统是一体化的终端安全解决方案，针对高级威胁防护场景，通过终端检测与响应（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，日志管理提供终端防护日志和运维操作日志的记录与检索，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。