捍卫者主机监控与审计系统

技术白皮书

2017-3-6

目录

第一章 开发背景

计算机网络安全：信息安全即国家安全。没有信息安全，就没有真正意义的国家安全、也就没有真正的政治安全、经济安全、军事安全、文化安全和社会的稳定。随着网络信息化建设的大力推广和广泛应用，人们须要对信息安全有广泛的了解和高度的重视。防止外部的入侵和内部违规、窥探、窃取，已经成为我们必须面对的严重而残酷的现实问题。

据 FBI 和 CSI 在对 484 家公司进行了网络安全专项调查，调查结果显示：超过 85%的安全威胁来自公司内部、有 16%来自内部未授权的存取，有 14%来自专利信息被窃取，有 12%来自内部财务欺骗，而只有 5%是来自黑客的攻击；在损失金额上，由于内部人员泄密导致的损失是黑客所造成损失的 12 倍。

相对与网络边界或外网安全产品而言，内网信息安全产品还没有得到足够的重视，基于内网安全防范产品的和解决内网安全的方案还不够完善。

内网信息安全包括最大威胁是移动存储设备威胁。一个组织可以实现内外网分离切断企业信息的部分外泄途径，但是目前计算机提供了丰富的接口外设，诸如 USB 接口、串口、并口等等，组织内人员可以轻而易举的通过 U 盘，手机等可连接设备偷窃组织内部资料。---这是计算机信息的最大威胁。

因此，为了满足企业及个人对这方面产品的需求，我公司推出了“捍卫者主机监控与审计系统”。

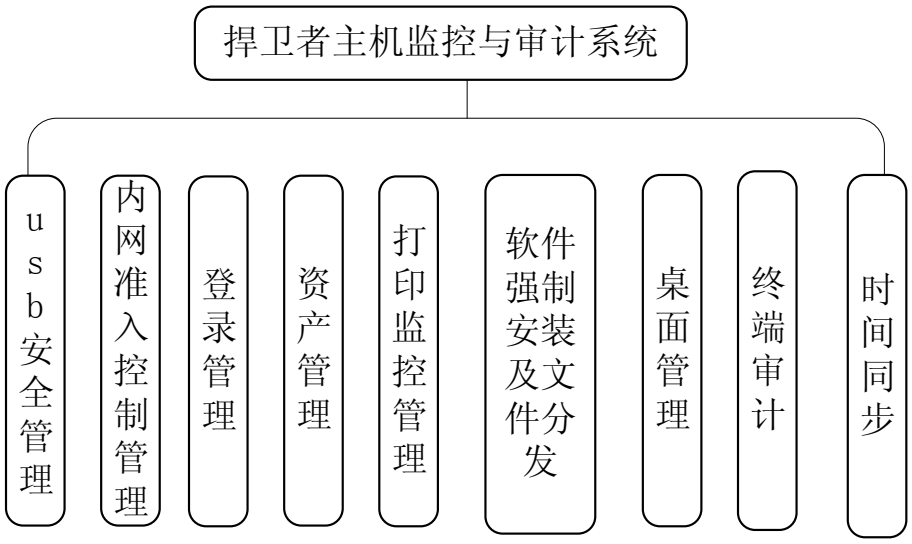
第二章 系统概述

捍卫者主机监控与审计系统是一款覆盖了移动存储介质的使用控制、内网终端的控制、端口设备使用管理、非法外联告警、敏感信息检测、文件共享/打印控制、准接入控制等。通过将所需的功能组件随机融合，即可构成单位特有的综合安全管理平台。

捍卫者主机监控与审计系统采用全新的技术方案，超前兼容所有 Windows 系统，实现深度隐藏。通过加密、认证、鉴别、访问控制、审计等技术手段，做到事前主动防范、事中 监控、事后可审计。基于产品构架设计特性，可满足大型网络系统的跨地域独立部署或分级部署。

第三章 系统结构

捍卫者主机监控与审计系统主要从外设终端主机接入安全、外设设备接入安全、内网准入控制、内网文件安全等方面防信息止内网终端机密外泄。主要由十大功能组成，其系统架构如下：



第四章 系统介绍

4.1 USB 安全管理

捍卫者主机监控与审计系统--usb 安全管理为终端计算机使用移动存储设备提供了完整的安全解决方案。实现了对 U 盘、移动移动硬盘、SD 卡等移动存储设备的有效管理客户和控制。既保证了移动存储设备的安全使用，又避免了移动存储设备随意使用造成的信息外泄风险。

USB 安全管理系统提供计算机端口的安全管理、移动存储设备的授权使用、内部安全 U 盘使用。

计算机端口安全管理，主要对 usb 端口和其他非常用端口进行安全管理。对 usb 端口设置：禁用、只读、开放三种模式，三种模式可以灵活使用，还可以对 usb 端口权限设置临时开放或只读，一定时间后自动禁用。其他非常用外设端口（如：光驱、本地连接、无线网卡、手机同步、蓝牙等）设置：禁用、开放模式。

移动存储设备授权使用，在终端计算机端口禁用/只读管控状态下，usb 安全管理系统对指定的移动存储设备授权，授权后的移动存储设备得到权限，可以在认证的计算机上使用，为经过授权认证的移动存储设备则是不可以使用的。

内部安全 U 盘使用，此为我公司研发的专属 U 盘，通过

特殊加密技术，实现专属 U 盘可以在内部安全使用，在外部专属 U 盘不可以使用的效果。

多年来捍卫者主机监控与审计系统--usb 安全管理功能应用在医疗、事业单位、金融等各行业中，并不断完善和更新，在外设端口准入安全方面是国内最为完整的安全产品。

4.2 准入控制管理

捍卫者主机监控与审计系统—准入控制管理，是解决企业内部终端计算机非法访问外网或外部终端，外部终端非法访问内部网络或内部计算机终端的最完善的解决方案。采用底层安全控制技术，有效的隔离内部终端计算机访问非法网络和非法终端，屏蔽外部终端或外部网络。同时还阻止内部终端通过私改 MAC 和 IP 非法访问外部终端或网络。

捍卫者主机监控与审计—准入控制管理的主要功能：

通过网络准入机制，建立可信网络，为企业建立可信的网络环境；

可信网络内部终端通过认证，可以相互正常通信；非认证终端部不可访问可信终端；

建立网络访问控制机制，可信终端未经允许，不可访问非认证网络或终端；

捍卫者主机监控与审计—准入控制管理低成本实现内外网软件隔离和内网准入信息安全防护，防止外部终端因为非法

接入、内部终端非法外联导致泄密。为企业内网安全提供又一安全解决方案。

4.3 登录管理管理

捍卫者主机监控与审计—登录管理，主要是通过特殊电子钥匙 USB KEY(简称 Ukey)实现对终端计算机的系统访问控制。在没有插入电子钥匙 Ukey 的终端计算机上不能登陆操作系统，插入电子钥匙 Ukey 状态下终端计算机正常操作，拔出后锁定计算机系统。

捍卫者主机监控与审计—登录管理为每个终端加了一道安全系统锁，为企业终端又提供了一重安全保障。

4.4 软件强制安装及文件分发

捍卫者主机监控与审计系统—软件强制安装及文件分发功能，提供软件分发、安装等远程功能，以及对一些常用软件的远程安装，可以使企业更好的管理网内计算机，防止病毒的入侵，提高计算机自身的安全性。对于统一安装的软件，系统会自动检查终端机是否安装或卸载了指定安装程序，并强制安装。

4.5 桌面管理

捍卫者主机监控与审计系统—桌面管理，提供远程终端监控

功，企业管理员可以实时监控终端运行状态，包括应用程序、桌面情况、内存使用情况、使用状态等。对于不符合规定的行为，可通过锁定、关机、重庆、结束进程等终止其行为或截屏进行及时取证。本系统可以对多台终端进行监控，可同时监控 9 屏；对终端可监、可控，操控灵活。

4.6 资产管理

捍卫者主机监控与审计系统—资产管理，针对 IT 设备管理特点量身打造，不同于传统的资产管理。主要是收集内网计算机的软件、硬件信息，可以查看网内计算机的软件、硬件状态等信息系，若软、硬件资产产生异动及时报警。

4.7 打印机监控管理

捍卫者主机监控与审计系统—打印监控管理提供安全的终端打印环境，对计算机进行打印设定，监控打印机的使用，记录终端打印记录，防止非授权的信息被打印，从而防止了内部资料从打印机外泄。

本系统详细记录每次打印事件的终端 IP、主机名、用户名、打印机名、打印时间、打印文档、打印页数、日志上报时间和记录时间等信息，且可以设定按时间、关键字、IP 等多种查询方式，并可以备份打印的内容以便留存取证。

4.8 终端审计

捍卫者主机监控与审计—终端审计主要提供对终端计算机系统用户、用户组、系统日志、网络共享设置等信息的记录，通过查看记录，对终端记录进行分析，及时发现安全不足等问题。在审计的基础上，本系统还增加了对非法进程的管理，通过黑白名单方式对终端计算机非法运行进程进行控制，防止客户端运行非法进程或在工作时间运行与工作无关的程序，从而对客户端进行有效控制。

4.9 时间同步

捍卫者主机监控与审计—时间同步提供统一管理时间方式，提供工作效率，同时也避免了因时间差异而导致的信息交互歧义等问题造成的损失和争议。

主要功能是管理终端向终端时间同步，使终端处于统一时间上管理，终端计算机不能私自修改系统时间，如果终端私自更改时间，时间会自动变回与管理终端同步。

第五章 系统特色

捍卫者主机监控与审计系统为企业内网安全提供的是一套最为完整的终端安全解决方，集外设端口准入控制、内网准入控制、终端准入控制为一体。具有其独特的产品优势，系统特色如下：

1. 可以管理 USB 端口及光驱、软驱、红外、蓝牙等各种外设，对

USB 存储设备及光驱可以设定开放、只读、禁用三种状态，并且不影响 USB 键盘、鼠标及 ukey 的使用。

2. 可以记录 USB 存储设备的插拔使用日志以及在 USB 端口开放时文件的拷贝日志。
3. 同时支持在线/离线策略，对移动存储设备可以分域分部门授权做到移动盘与计算机一对一、一对多绑定使用，未注册 U 盘遵循 USB 移动存储设备端口设置。
4. 可以授权移动存储设备几天、几次后失效，若需使用需经管理员重新授权。
5. 可以远程临时设定移动存储设备端口的开放，超时自动禁用。
6. 配合指定加密 U 盘，可以实现 U 盘在非法环境内无法直接看到加密区，需要专用工具切换密区进行查看，在授权匹配的合法环境中可以直接查看加密区，并且记录插拔及文件拷贝日志。
7. 可以收集计算机软硬件资产信息，并在有异动时产生报警。
8. 进程管理，采用黑白名单机制，非法进程无法运行。
9. 可以对区域内计算机进行认证，实现可信域方式的计算机管理，可信计算机间可以相互访问，外来计算机无法访问可信域内计算机，可信域内终端也无法访问 3G/4G/WIFI 等私接外部网络。并能记录合法、非法计算机访问日志，可信域终端连接外网产生告警。
10. 在可信域中可以设定指定的外网出口，或临时接入 IP，并可以限制各种网络协议：http、ftp、netbios 等。

11. 支持 IP 和 MAC 绑定，私自修改 IP 或 MAC 都会导致断网，并产生告警。
12. 对移动设备拷入与拷出任何文件有详细的审计功能，可以详细记录源文件名、计算机 ID 等。
13. 打印监控，可以记录所有打印机打印的操作，包括打印 IP、文件名、打印页数等。
14. 可以对所有客户端的应用程序日志、系统信息、网络监控、共享设置进行查看，并可以远程限制共享。
15. 全面日志审计功能，包括断网日志、插盘日志、客户端上线日志等，统计分析功能并可以 excel 报表导出。
16. 服务器对客户端进行时间同步、并且防止客户端私自修改系统时间。
17. 服务器对客户端可以进行上线控制，客户端非正常时间上线有告警提示。
18. 同时具备 windows 密码+硬件 Ukey 登陆计算机控制模式，并且 UKEY 可以分计算机唯一 key 和可信域全局 key。
19. 通过服务器可以对客户端进行远程升级、卸载等维护，卸载必须有密码控制。
20. 可以统一对客户端机下发文件，可以自由制定文件下发路径，并设置是否自动运行，对于要下发的软件可以进行安装，并自动扫描客户端是否安装了指定软件并强制安装。
21. 可以对客户端远程进行锁定、关机、结束、唤醒等操作。

22. 国内少数获得公安部和保密局认证销售许可产品。

23. 客户端异常或是破解在服务器的安全信息里面显示相关状态，进行报警。

24. 客户端遵循 windows 操作规范，不改变用户使用习惯。

25. 切换用户和切换安全模式都认证之前的软件设置。

26. 全面的日志审计功能(包括外携盘日志、断网日志等)。

27. 网络版直接推送安装、服务器级联。

第六章 部署方式

捍卫者终端安全与访问控制系统提供单机版和网络版两种部署方式

单机版：单机版安装在终端计算机上，直接在每台终端计算机上进行安全策略部署。单机版适用于中小企业，单独管理方便，安全性价比高。

网络版：网络版分服务器端和客户端，服务端安装在管理终端上，客户端安装在终端主机上，管理终端通过服务器控制平台对安全主机进行安全策略部署。网络版支持大中型局域网络、跨区局域网络

第七章 售后服务

公司一直秉承“**创新技术理念，打破行业格局**”的宗旨，在内网安全领域不断研究和创新，为用户打造完整的内网安全解决方案及服务。公司拥有精湛的技术研发团队和技术实施维护团队。为用户提供安全的售后维护保障。

- 售后服务团队

产品实施组：负责产品的现场具体实施，现场安装、调试、产品使用培训

售后技术组：分线上及线下维护。线上免费提供电话和远程维护，24 小时内响应；线下技术上门调试维护（跟进区域收取相应上门服务费等费用）

第八章 公司简介

河北易泰通软件科技有限公司是一家专注于内网信息安全的高科技创新企业。公司先期筹备于深圳，经过初期技术预研，在2007年石家庄正式注册成立河北易泰通软件科技有限公司，公司先后在山东、天津、深圳、广州、上海、吉林、辽宁、黑龙江、陕西、河南、四川、重庆、浙江、内蒙古等省份发展代理加盟商300 余家，并不断的拓宽产品销售渠道，改善经营条件，扩大经营规模。

公司旗下以捍卫者品牌为主的一系列信息安全产品获得 10 多项自主知识产权，在申技术专利一项，并获得“科技部中小企业创新扶植基金”。“捍卫者主机监控与审计系统”成功通过国家最新保密局标准检测，获得“涉密信息系统规范检测证书”。目前，捍卫者产品已经行销全国所有省份自治区，捍卫者品牌已经在业内享有较高知名度。

公司拥有技术精深的研发队伍，拥有经验丰富而又富有活力的咨询及项目实施队伍。注册商标“捍卫者”品牌系列软件以其优良独特的加密控制技术，有效地防止企业内部信息外泄风险，现已被广泛应用到政府、医疗、电力、科研、军事、设计、影视、银行等诸多领域。

第九章 公司资质

涉密信息系统
产品检测证书

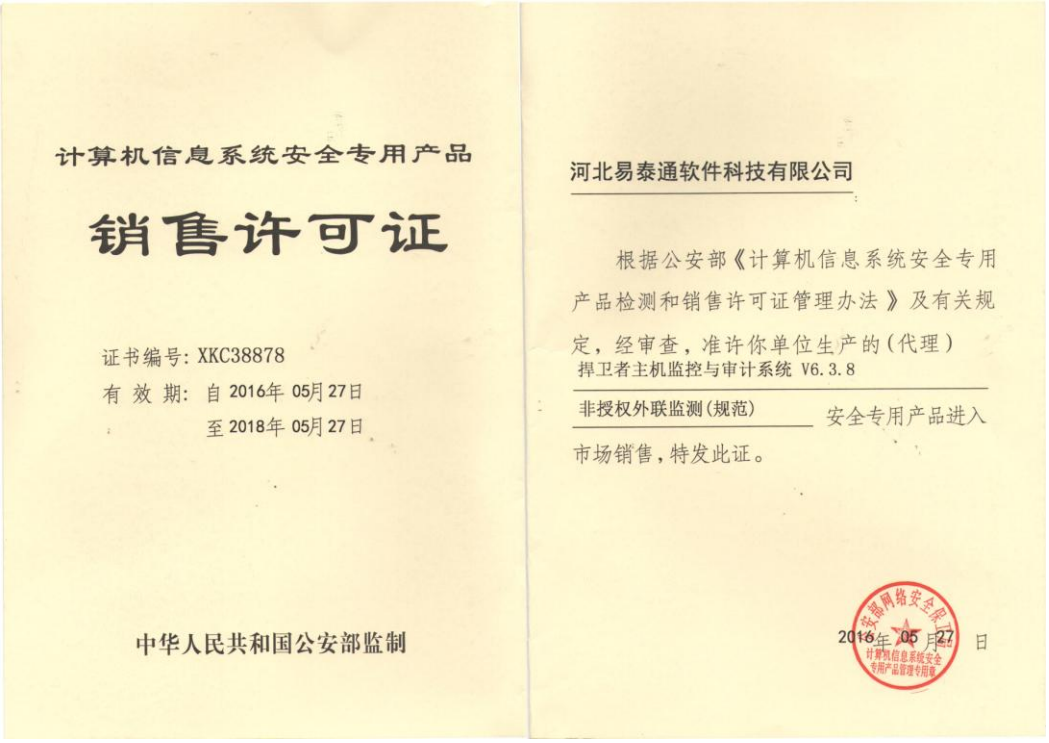
编号：国保测 2015C03924

兹证明：河北易泰通软件科技有限公司
研制生产的捍卫者主机监控与审计系统 V5.0.0
经国家保密科技测评中心检测，符合国家保密标准 BMB15-2011《涉及国家秘密的信息系统安全监控与审计产品技术要求》中主机监控与审计基本型产品的要求

本证书有效期自 2015 年 5 月 13 日至 2018 年 5 月 12 日

批准人：　　国家保密科技测评中心

使用证书复印件应由产品研制生产单位加盖公章　　证书信息核查：WWW.NSSTEC.ORG.CN



计算机信息系统安全专用产品

销售许可证

证书编号：XKC38878
有 效 期：自 2016年 05月27日
至 2018年 05月27日

中华人民共和国公安部监制

河北易泰通软件科技有限公司

根据公安部《计算机信息系统安全专用产品检测和销售许可证管理办法》及有关规定，经审查，准许你单位生产的（代理）捍卫者主机监控与审计系统 V6.3.8 非授权外联监测（规范）安全专用产品进入市场销售，特发此证。

2016年 05月27日


第 8470833 号
商标注册证
捍卫者
核定服务项目(第 38 类)
信息传送；计算机终端通讯；计算机辅助信息与图像传输；计算机辅助信息和图像传送（截止）
注 册 人
注册地址
注册有效期限
局长签发
许瑞表
商标局
河北省科学技术成果
证书
软件企业认定证书
经审核，
符合《进一步鼓励软件产业和集成电路产业发展的若干政策》和《软件企业认定管理办法》的有关规定，认定为软件企业，特发此证。
证书编号：
发证机关：
计算机软件著作权登记证书
中华人民共和国国家版权局
计算机软件著作权登记证书

第十章 联系方式

河北易泰通软件科技有限公司，总部位于河北省石家庄市，公司联系方式：

产品咨询热线电话：4001146628

产品线上咨询 QQ： 2979925250

产品官方网站链接：www.hanweizhe.net

产品技术支持热线：18132161875