火绒安全
www.huorong.cn

“火绒终端安全管理系统1.0版”

企业简介

企业定位

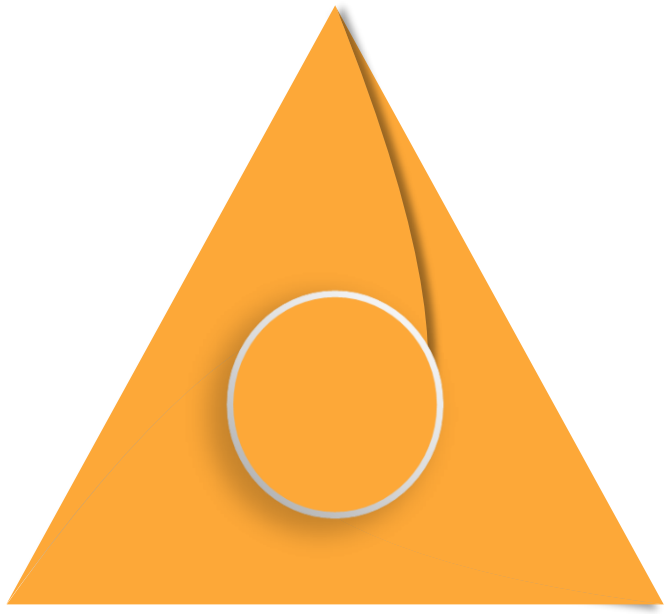
一个纯粹、专注的终端安全公司，自主研发终端安全核心技术和产品。

立业之本

冷静、艰苦、长期地专注于核心技术研究。

商业模式

通过产品和服务直接收费。



产品和服务

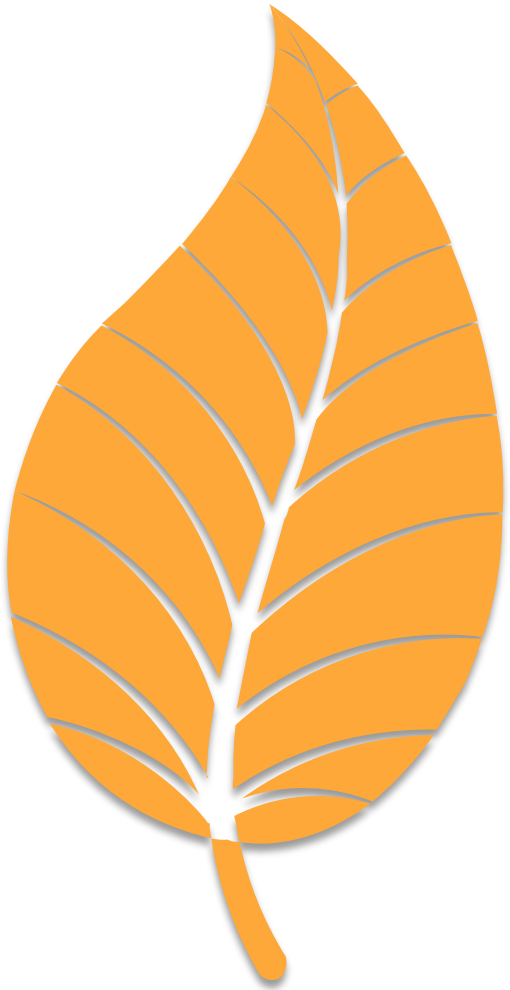
成立于2011年的火绒，拥有自主产权的新一代反病毒引擎等全套终端安全技术，并向联想、天融信、绿盟、深信服等行业伙伴输出反病毒引擎等技术。

2012年，火绒推出个人版产品“火绒安全软件”，目前已拥有300万忠实用户，其中大部分是网管技术人员等电脑高手。

2018年5月30日，火绒发布“火绒终端安全管理系统1.0”，正式进军to B安全市场。

火绒未来还将陆续推出Linux、Android、Mac等平台的产品，以及“企业威胁情报平台”和安全咨询等服务。

理念与策略



策略：EDR体系产生威胁情报

实现“情报驱动安全”的核心，是部署实施EDR（终端、检测和响应）运营体系。火绒EDR体系以遍布互联网的数百万“火绒安全软件”为基础。在保护用户安全的同时，“火绒安全软件”又是截获、处理各种未知威胁的探针，这些威胁信息在用户电脑上完成初步分析和处理，然后回传给火绒后台系统，进一步分析和处理。

理念：情报驱动安全

火绒所有产品和服务都秉承“情报驱动安全”的理念——以真实、全面、及时的互联网威胁情报为基础，来驱动技术研发和产品开发，并建立相应的安全服务运营体系。实时感知、精准处理、动态防御，为用户提供可靠 、及时、成本合理的安全防护。

理念与策略

技术支撑策略

“火绒安全软件”拥有数百万用户，遍布整个互联网。火绒产品经受了各种复杂环境的考验，产品稳定成熟，为火绒EDR运营体系和“火绒威胁情报系统”提供了强大支撑。

“火绒安全软件”拥有的新一代反病毒引擎和多层次主动防御系统（HIPS）这2个核心模块，它们在保护用户终端安全的同时，在系统中设置多层、严密的威胁感知点，实时感知、预处理各种威胁信息，然后返送给火绒“终端威胁情报系统”。

策略放大技术

通过前端截获、预处理，以及后端的进一步深度分析和处理，火绒EDR系统产出强大的威胁情报，据此来升级病毒库，和各种威胁样本库，以及改进产品。每个火绒个人版用户，都是感知威胁的探针，同时也享受着所有客户终端产生的威胁情报的整体价值。

理念与策略

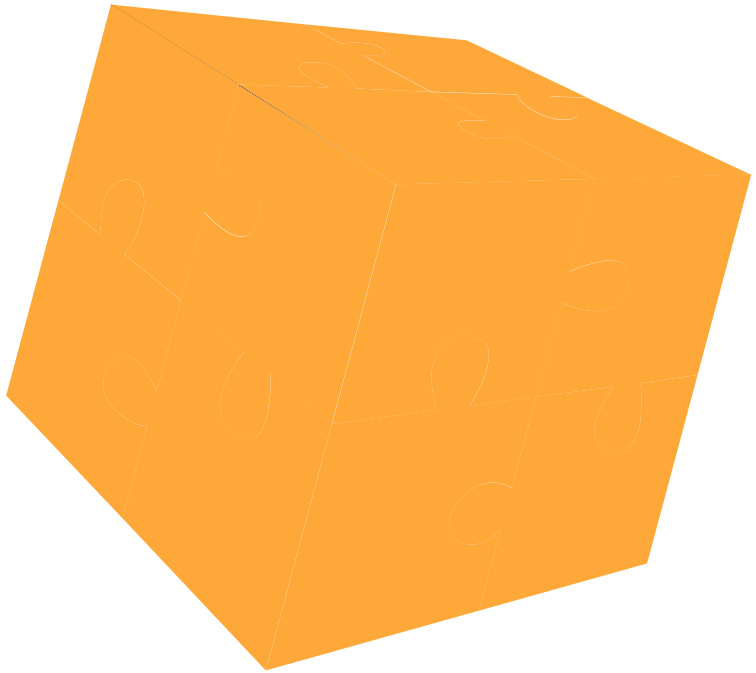
每个部署“火绒终端安全管理系统1.0”的政、企用户，都享受着300万火绒个人产品和EDR运营系统所产生的互联网威胁情报的价值的总和。

产品优势

1、自主知识产权，适合国内用户

自主知识产权和全部核心技术，完全避免产品后门和用户敏感信息外泄等隐患。

能够更好地开发产品。OEM引擎需要在外层再次封装,以符合自身产品的需求，增加成本降低效率，无法精细地调整配置，产品效率低、资源占用高。



能够及时响应本地安全问题，迅速处理国产木马和流氓软件，同时对误报、兼容等问题的沟通、处理时间短。

能够对国内安全问题的特殊性有深刻认知，除了反病毒、反黑客，更能有效防范商业软件侵权和国内病毒产业链。

产品优势

2、成熟的终端，强悍、轻巧

05

火绒终端产品安装后仅占用20M硬盘资源，病毒库3M大小，日常内存占用不到10M，平常使用中，几乎感觉不到火绒终端产品的存在。

04

国内唯一将反病毒引擎、主动防御系统、网络防火墙深度融合在一起的终端安全产品。三个模块协同运行，可以有效帮助机构用户抵御勒索等恶性病毒、黑客渗透等高等级威胁，并一举解内网用户多年来漏洞防御困难、本地病毒屡杀不绝等难题。

03

强大的防火墙。内嵌的“漏洞攻击拦截”技术，可识别不安全的网络数据通过漏洞发起的攻击，比如去年肆虐全球的“想哭wannacry”勒索病毒，甚至还可以记录攻击发起者的IP，方便进行攻击溯源，与“漏洞修补功能”构成双重保护。

02

多层次主动防御系统（HIPS）。拥有上百个防御点，率先将单步防御和多步恶意监控相结合，不依赖白名单，消除了信任漏洞。在文件、注册表、进程、网络这四个维度均设计了全面的防护规则，有效地针对操作系统的脆弱点进行防护。

01

国内唯一拥有“通用脱壳”能力的新一代反病毒引擎。通过行为特征来精准判别各种电脑病毒和威胁代码，无需国内常见的“云查杀”，也不用庞大的“白名单”库规避误杀，完全本地杀毒，不受断网环境影响，非常适用于内外网隔离的政府、军方、央企、公检法等机构用户。

产品优势

3、高效的管理中心，可靠、易用

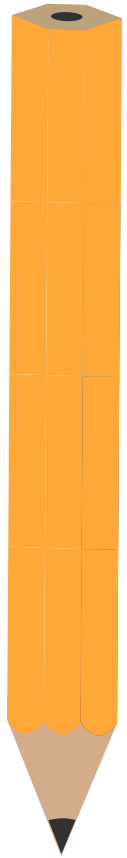
“火绒终端安全管理系统1.0”拥有强大、高效的终端管理功能，统一部署、集中管理，将企业网络纳入严密的防控之中，确保安全无死角，每个终端的安全防御状况都能轻松掌握。

基于对企业用户的深刻理解，“火绒终端安全管理系统1.0”的管理中心设计合理，拥有友好的界面、人性化的统计报表，安全管理信息和日志一目了然，能极大的提高安全管理效率。

产品优势

4、尊重用户隐私，保护企业数据安全

秉承安全厂商的基本操守，火绒产品没有任何捆绑、弹窗、侵占资源等行为，并强力狙杀各种流氓软件、商业软件的侵权行为，确保电脑系统干净清爽。



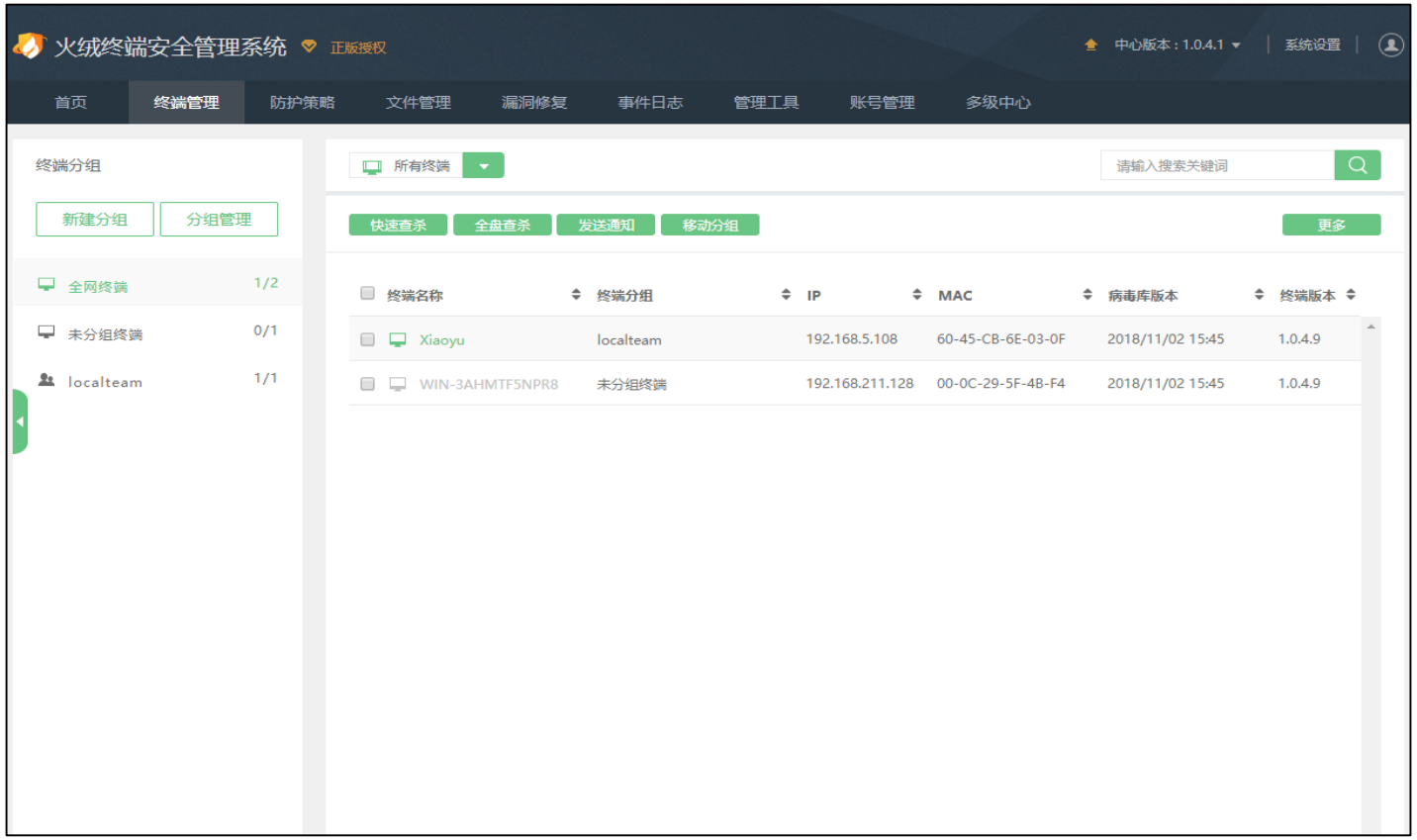
针对政府、企业等机构用户，火绒独家承诺：“**尊重用户的隐私权、数据所有权，不会上传用户的任何文件、数据等信息。**”

产品主要功能

1、病毒查杀。检测电脑终端是否存在病毒、木马等威胁，并进行高效处理。

产品主要功能

2、终端管理。管理员自由分组管理旗下终端，并对旗下终端进行扫描病毒、发送消息等多种操控。

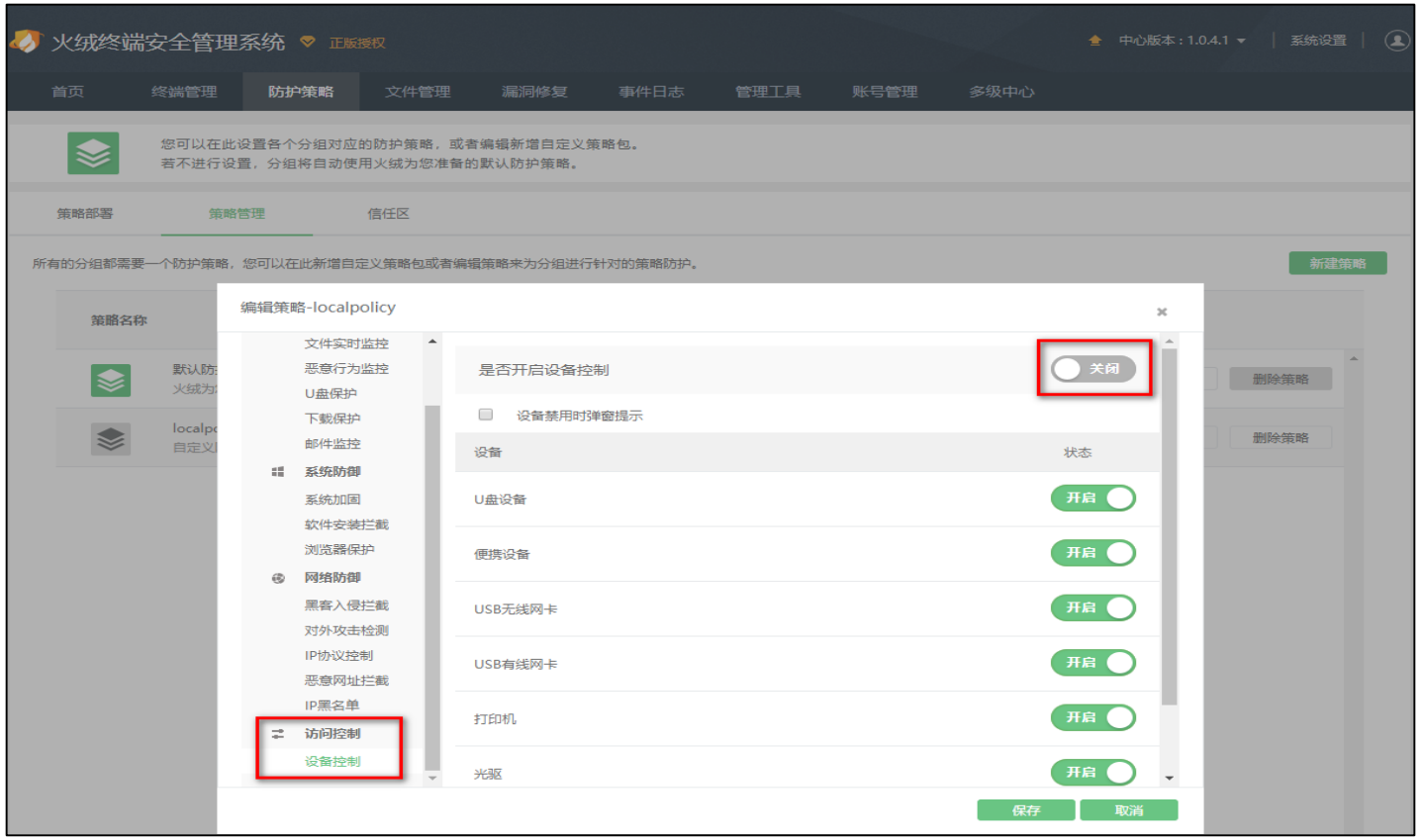


产品主要功能

3、防护策略管理。 管理员查看终端防护策略现状，并设置相应的防护策略，使终端能够自动处理威胁事件。便于调控终端防护中心模块中病毒防御、网络防御、系统防御下的所有项目，帮助旗下终端更好的进行文件实时监控、恶意行为监控、U盘保护等。

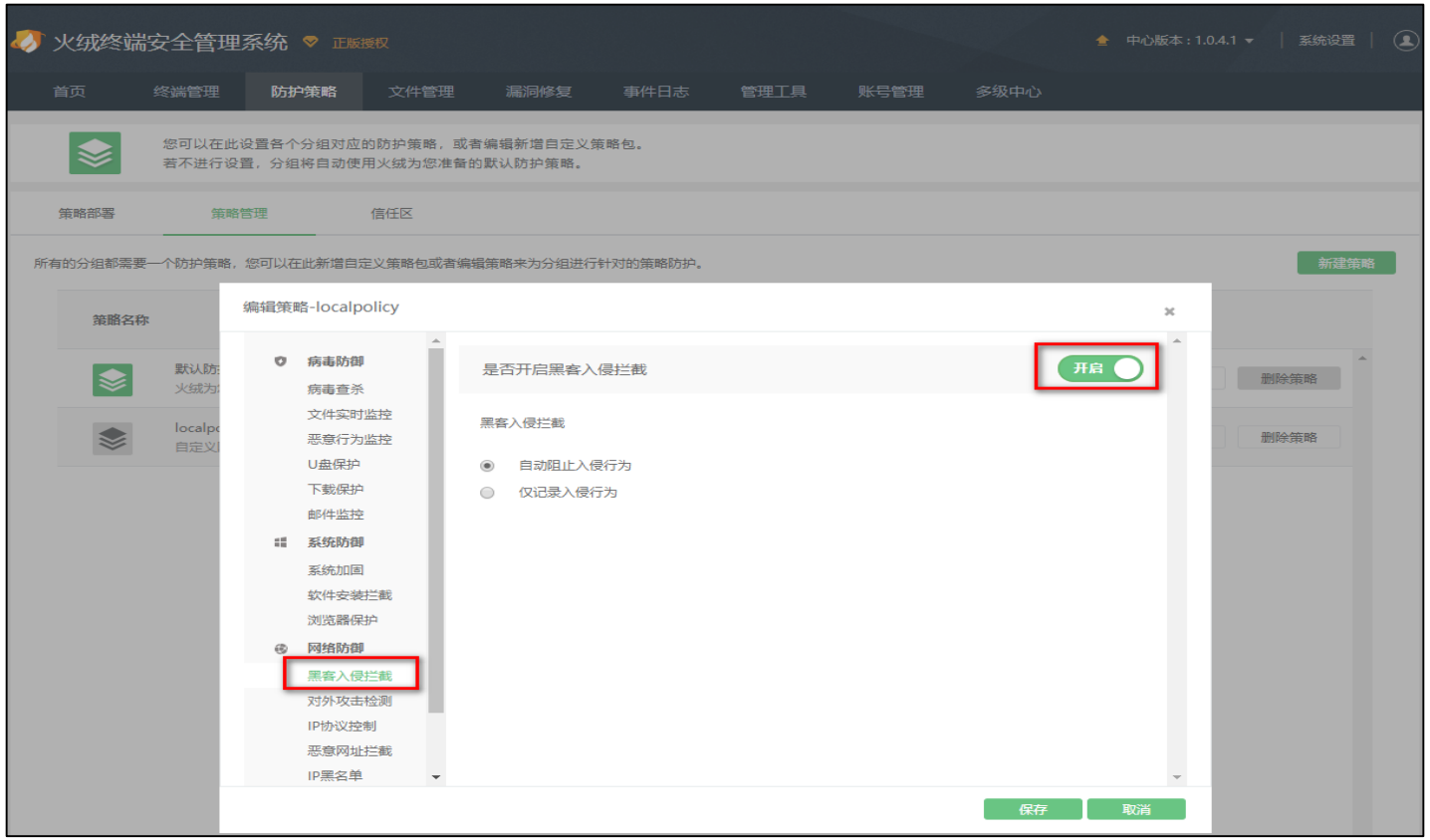
产品主要功能

3-1、防护策略管理——设备控制。管理员可通过“防护策略”—“设备控制”功能，进一步加强对外接设备的安全防范和管理，防范病毒传播，保障重要资料不被外泄。该功能支持管理员任意选择、设置相关终端，禁用U盘、便携设备、USB有线及无线网卡等各种外接设备。



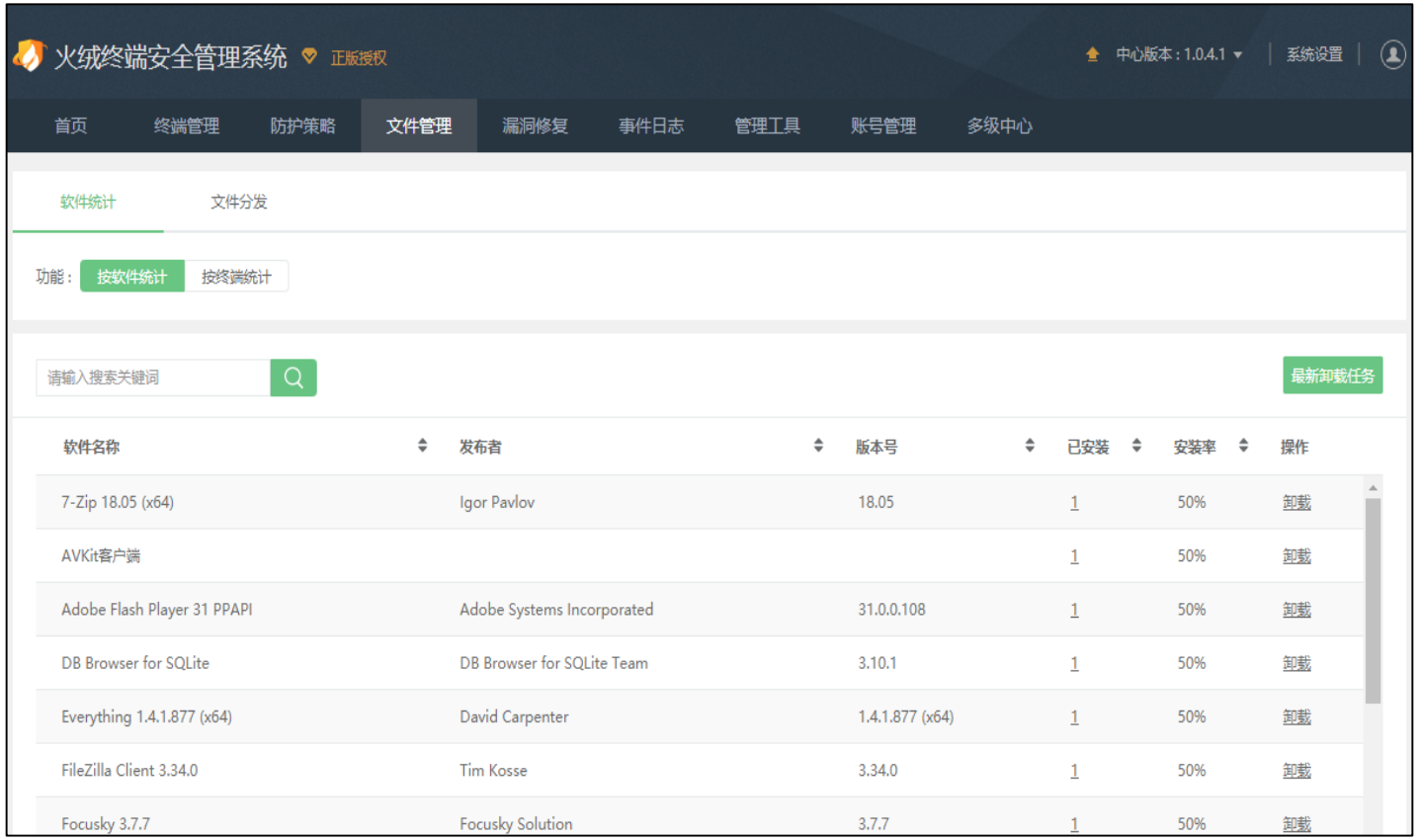
产品主要功能

3-2、防护策略管理——漏洞攻击拦截。 该功能镶嵌在“黑客入侵拦截”模块中，可从网络数据层面分析并识别漏洞攻击模型（譬如：永恒之蓝的SMB协议漏洞），在攻击数据进入系统漏洞之前进行拦截，从而在系统没有打漏洞补丁的情况，完成安全热补，阻止勒索软件、黑客渗透程序等高危威胁的入侵，并记录攻击发起者IP地址信息，方便进行攻击溯源。



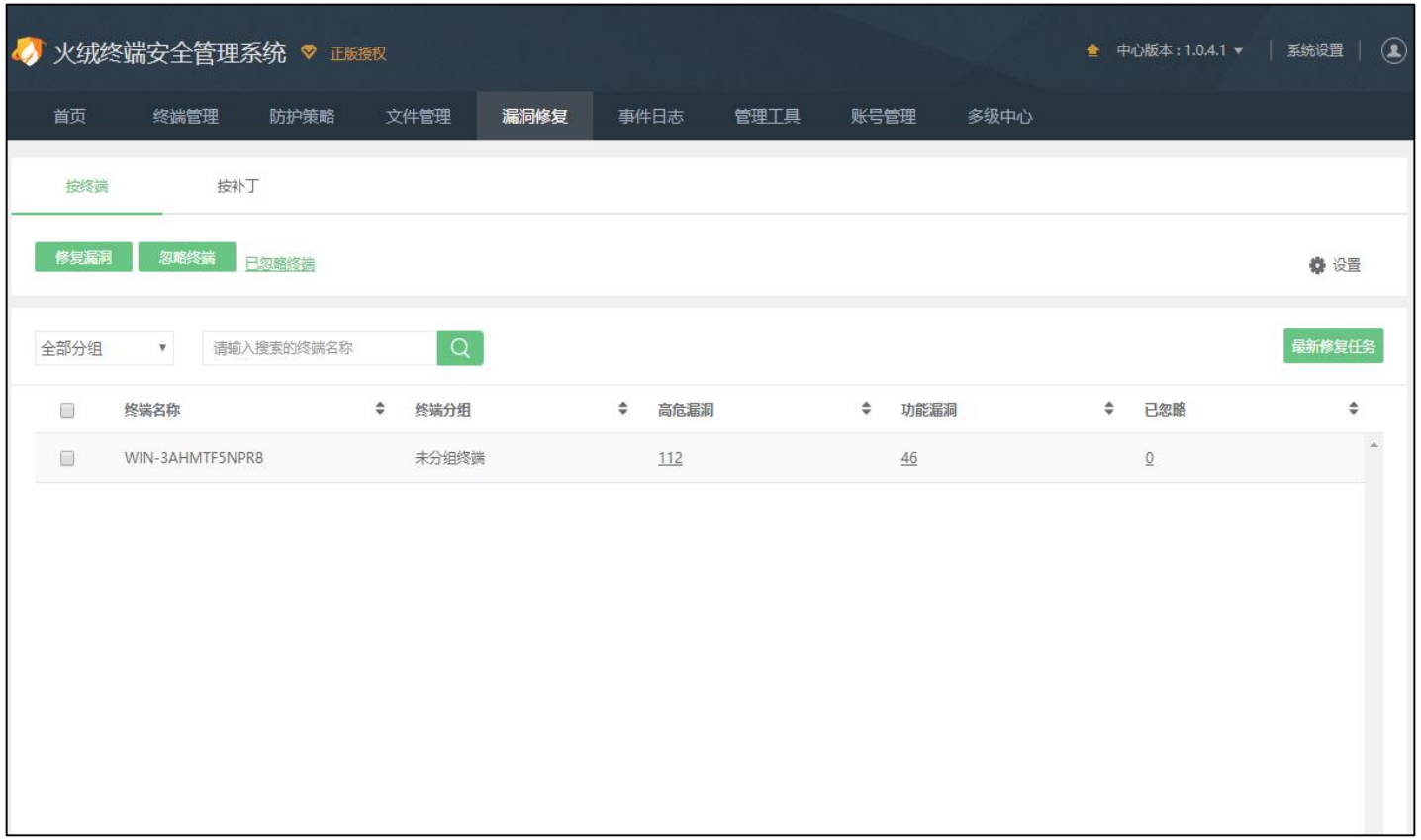
产品主要功能

4、文件管理。管理员可查看所有终端软件情况，并发送、推送、强制卸载终端的软件。



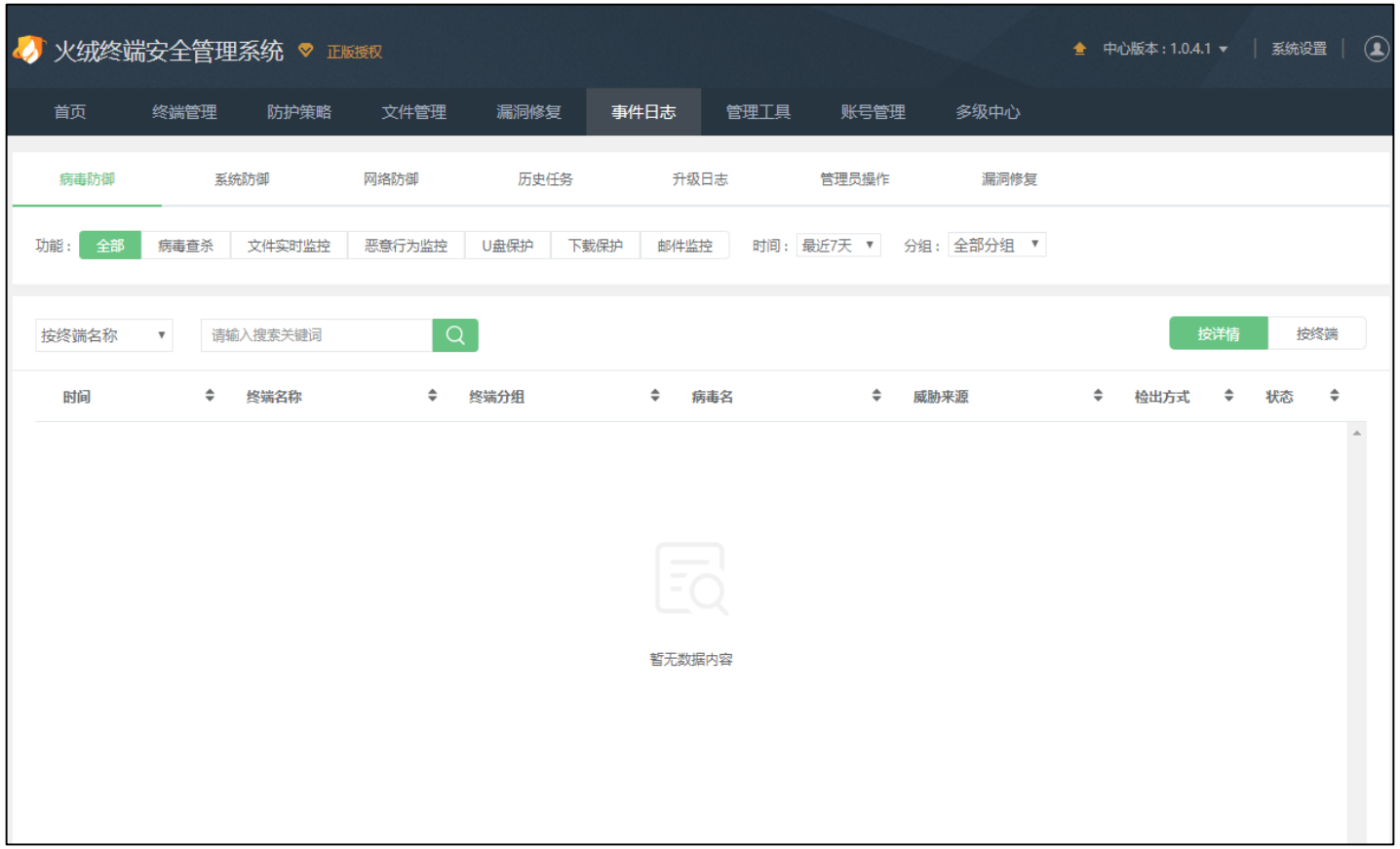
产品主要功能

5、漏洞修复。 管理员可以查看所有终端的漏洞情况，包括高危漏洞、功能漏洞以及忽略漏洞，对终端进行统一的漏洞扫描以及修复任务，保障终端安全。



产品主要功能

6、事件日志。管理员按特定排序方式以及标签，查看任一时段内查看发生的全部事件，以分析旗下电脑的安全状况。

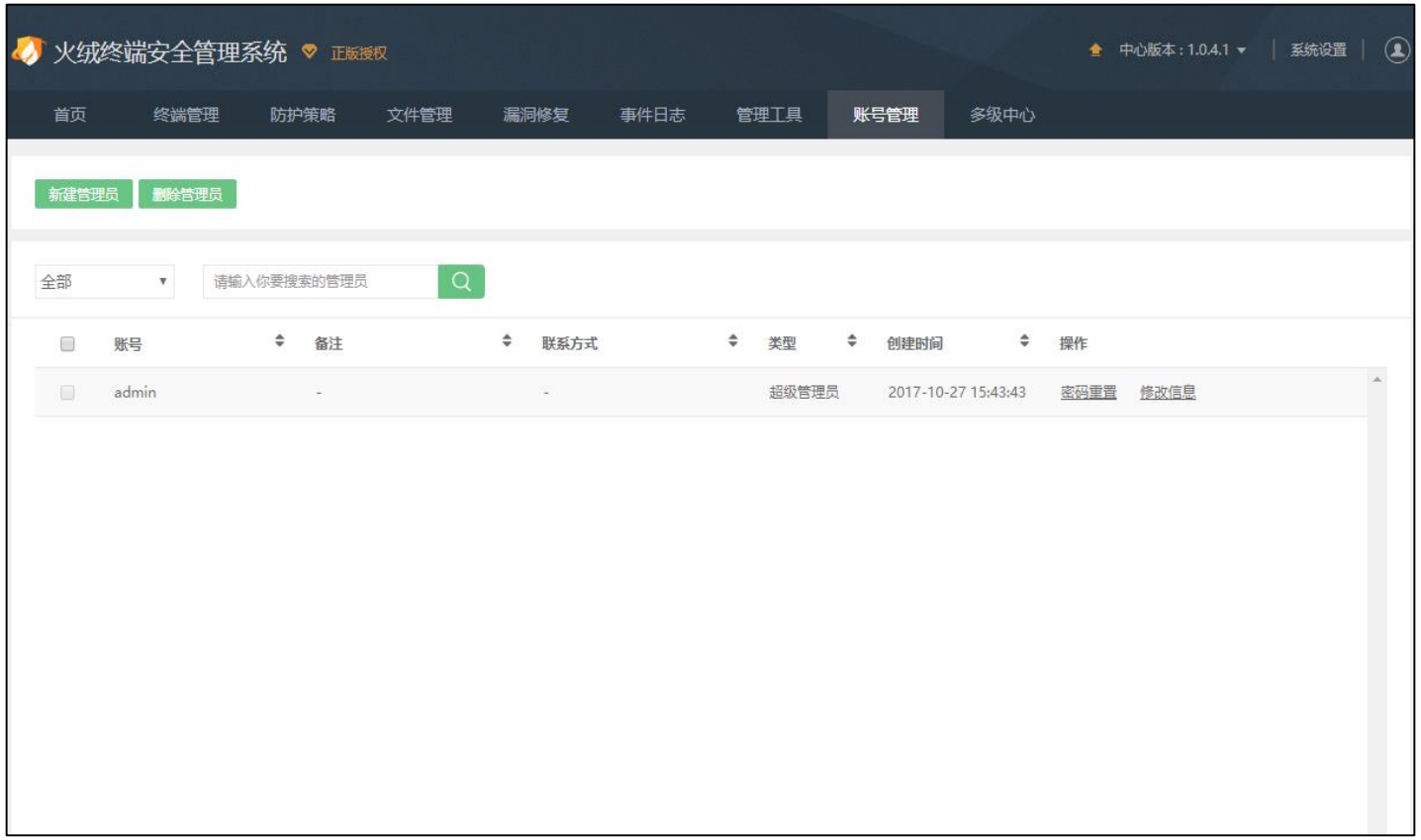


产品主要功能

7、管理工具。管理员可通过管理工具页面日志数据大小并及时清理日志，也可以统一进行软件部署。

产品主要功能

8、账号管理。可以通过“超级管理员”账户，添加、管理“管理员”账户，给其他“管理员”授权操作模块的权限，令其协助管理控制中心以及终端。



产品主要功能

9、多级中心。针对跨地域的超大型政企单位，以及需要严格分级管理的单位实现多级管理的需求，缓解单控制中心升级、打补丁压力，解决下属单位异地联动、多部门安全管理协同等管理难题。

欢迎试用

到2018年5月30日正式发布为止，已有上千家政府、企业单位试用了“火绒企业版”。安装、使用简单，运行稳定，从未发生任何重大产品故障。

火绒官网持续开放试用申请，机构用户可以获得授权，免费试用“火绒终端安全管理系统1.0版”3个月。

真实案例——“火绒企业版”解决的客户问题

- 多种勒索病毒同时在网内流窜
- 员工私自下载不合规软件致使病毒入群四处扩散
- U盘等外设传播病毒，屡杀不止
- 内外网安全糟糕，每日被攻击上千次
- 大型公司终端数过多，统一管控、规范管理成难题

湖北某企业在试用“火绒企业版”期间，发现网络中有两种勒索病毒在流窜：一个是GlobeImposter勒索病毒，通过未安装安全软件的电脑入侵，加密共享文件夹，导致同一局域网中共享文件夹内文件均被加密；另一个是Wannacry想哭勒索病毒，通过“永恒之蓝”漏洞在局域网中无线扩散，屡杀不止，时刻威胁信息、财产安全。

真实案例——“火绒企业版”解决的客户问题

- 多种勒索病毒同时在网内流窜
- 员工私自下载不合规软件致使病毒入群四处扩散
- U盘等外设传播病毒，屡杀不止
- 内外网安全糟糕，每日被攻击上千次
- 大型公司终端数过多，统一管控、规范管理成难题

江西某电力企业部分员工私自下载不合格软件，导致病毒入侵，并在企业内网络不断扩散。包括挖矿病毒、CAD病毒、锁首木马等，甚至安装的某个人版安全软件都捆绑了锁首木马。通过安装部署“火绒企业版”，最终在三个月内共拦截、清除病毒木马攻击20000余次，拦截恶意网址约13000多次，结果触目惊心。

真实案例——“火绒企业版”解决的客户问题

多种勒索病毒同时在网内流窜

员工私自下载不合规软件致使病毒入群四处扩散

U盘等外设传播病毒，屡杀不止

内外网安全糟糕，每日被攻击上千次

大型公司终端数过多，统一管控、规范管理成难题

北京某公安部门网络频繁遭受木马病毒攻击，导致电脑运行缓慢，严重影响办公。今年5月试用“火绒企业版”后发现网络中的病毒均来自U盘、执法记录仪等外设，然后通过共享文件夹在整个网络中交叉感染。部署“火绒企业版”当天，拦截清除的病毒日志高达40页，最多一天拦截清除病毒1000多次，可见当时网络环境十分复杂，病毒感染传播非常广泛。

真实案例——“火绒企业版”解决的客户问题

多种勒索病毒同时在网内流窜

员工私自下载不合规软件致使病毒入群四处扩散

U盘等外设传播病毒，屡杀不止

内外网安全糟糕，每日被攻击上千次

大型公司终端数过多，统一管控、规范管理成难题

国内某上市电商企业数千台终端分别连接内、外网：连接外网的终端因员工私自下载不合格软件，导致被静默安装流氓软件；内网终端由于系统老旧，存在供病毒传播的未修复漏洞，是一个典型的互联网电商企业所面临的安全难题。在安装部署“火绒企业版”后，内、外网的的攻击次数已经由每日上千次下降到个位数。

真实案例——“火绒企业版”解决的客户问题

多种勒索病毒同时在网内流窜

员工私自下载不合规软件致使病毒入群四处扩散

U盘等外设传播病毒，屡杀不止

内外网安全糟糕，每日被攻击上千次

大型公司终端数过多，统一管控、规范管理成难题

深圳某大型金融公司终端使用量高达5000余台，给管理带来诸多不便：员工随意下载不合格的软件、使用带毒U盘，导致病毒泛滥；公司网管也无法统一制定防护策略，维护网络安全。通过部署“火绒企业版” 的“多级中心”功能，给5000台终端划分级别管理，并设置相应的防护策略，比如对不合格软件的进行卸载，制定病毒查杀任务，设置浏览器首页等，达到对大量终端统一、规范管理的目的。

客户案例（部分）

政府类客户		
政府	山东省地震局	重庆市九龙坡区保险局
	郴州市汝城县财政局	武汉市黄陂区国土资源局
	襄阳市经济与信息化委员会	丰县国土资源局
公检法	成都市青白江区司法局	开封市祥符区法院
	曲靖市公安局交警支队	赣州市信丰县人民法院
	漳州市公安局芗城分局	广东省广州市南粤公证处
医院	呼和浩特120急救中心	邯钢医院
	龙胜各族自治县妇幼保健医院	南京医科大学眼科医院
	望城区人民医院	临沧市双江自治县人民医院
	宿州市立医院	沙洋县人民医院
学校	对外经济贸易大学	台州科技职业学院
央企	深圳地铁	中铁十一局集团有限公司

客户案例（部分）

企业类客户		
IT&互联网	上海寻梦—拼多多	安徽舜德信息技术有限公司
	哈尔滨科盛网络科技有限公司	鞍山市四方信息技术有限公司
	哈尔滨鼎创科技有限公司	江西博微新技术有限公司
	北京黑鸢智能安防科技有限公司	天津益阳煜赢网络科技有限公司
	苏州易维迅福州服务站	金亿锡电子有限公司
制造业	洛阳涧光特种装备股份有限公司	新奥维工业自动化（上海）有限公司
	浙江松原汽车安全系统股份有限公司	浙江恒诚鞋业有限公司
	宝鸡保德利电气设备有限责任公司	芜湖通和汽车管路系统股份有限公司
	马鞍山飞马智科	深圳市凯发科技有限公司
金融	万乘深圳有限公司	山西三立期货经济有限公司
	微贷（杭州）金融信息服务有限公司	

客户案例（部分）

企业类客户		
医疗保健	宁波慈铭体检	上海嘉越医药科技有限公司
	鹏瑞利国际医疗健康中心	甘肃新仁和医药有限公司
能源与公共事业	长春国信供热工程有限公司	山东京博控股股份有限公司
	杭州佳和电气股份有限公司	南通天生港发电有限公司
	乐昌市自来水有限公司	成都市新都区自来水公司
批发与分销	温州早晨电子有限公司	上海泉澳网络工程有限公司
	威海味岛食品有限公司	烟台坤泰汽车内饰件有限公司
零售	携手服饰	上海松江好饰家家居市场经营管理有限公司

专注、纯粹，才会更安全