



# 火绒终端安全管理系统V2.0

终端管控与防护进入2.0阶段

2022/07/18

情报驱动

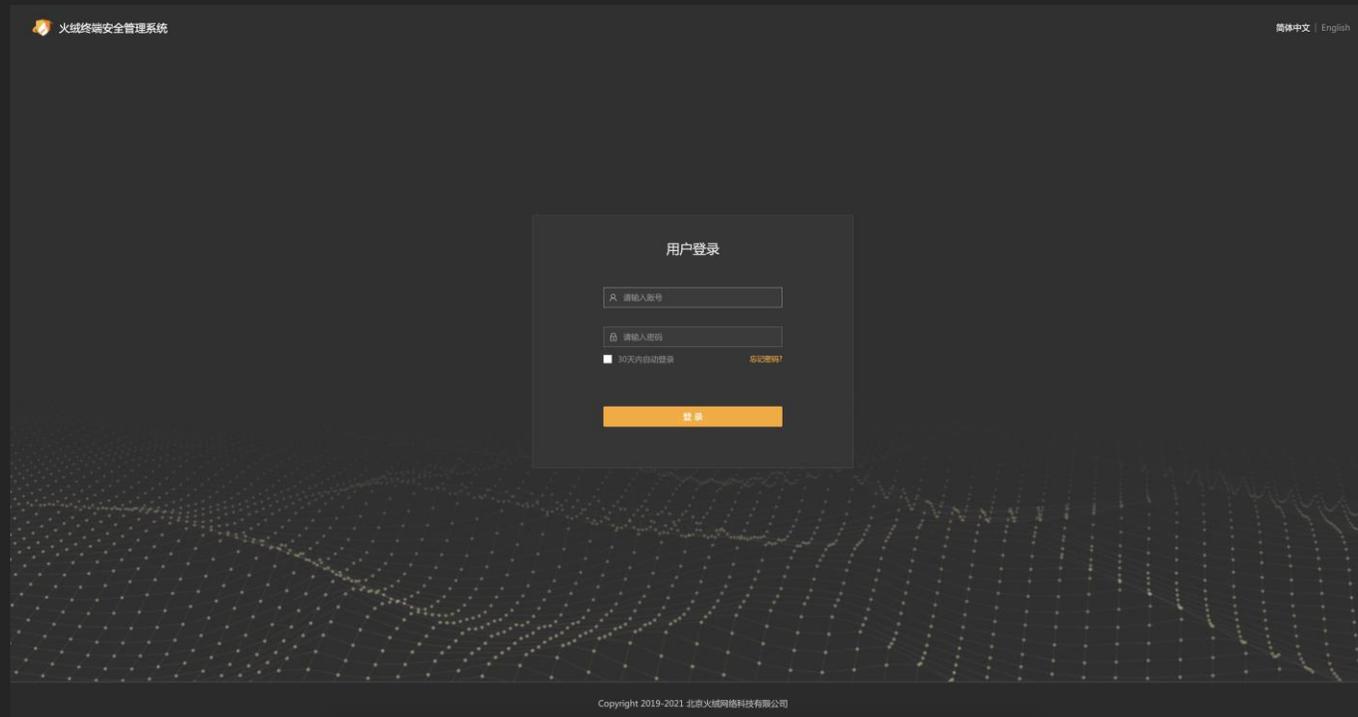
技术革新

免费试用

定制服务

# 火绒终端安全管理系统V2.0

火绒终端安全管理系统V2.0沿袭了1.0版本极致专业的产品品质和核心技术，增加了更多针对企业内外网脆弱点的防护功能，拓展了企业对于终端管理的范围和方式，提升了产品的兼容性、易用性，最终实现更直观地将威胁可视化，让管理轻量化，充分达到保护企业网络财产与信息安全的目的。



# 目录 CONTENTS

01

终端管控篇：威胁可预见，敌情先洞察

02

终端防护篇：技术驱动，纵深防护

03

产品优势篇：平台开发完善，产品契合国情

04

企业合作篇：产品覆盖全国用户，技术赋能广大同行

---

01

## 终端管控篇：威胁可预见，敌情先洞察

---

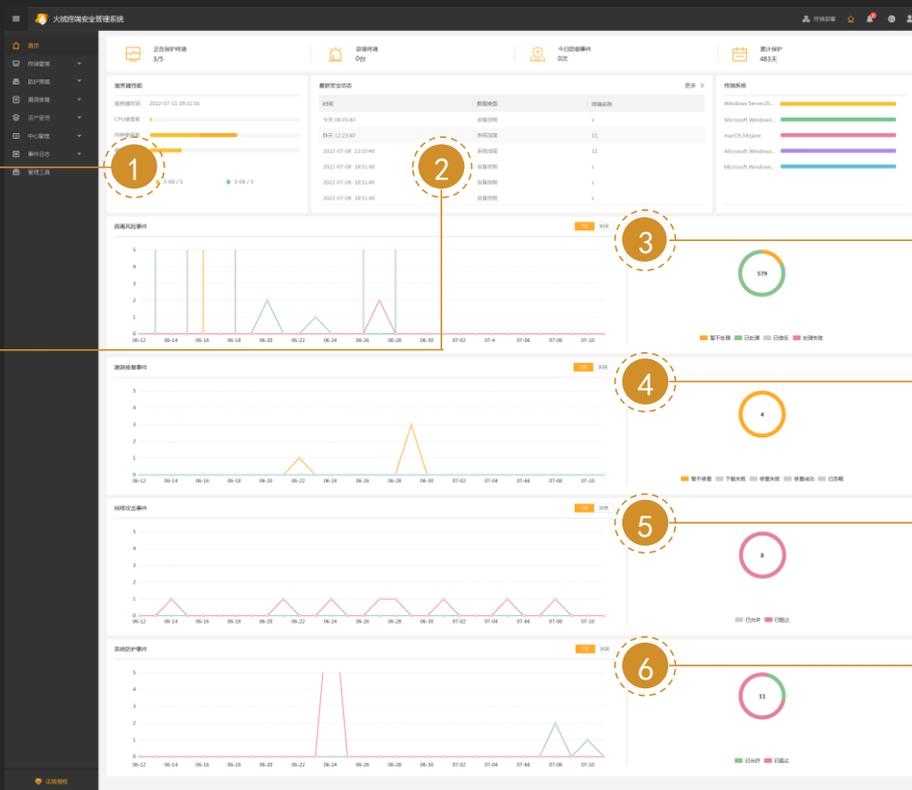
# 可视化中心

## 终端安全数据化，直观呈现威胁信息。

“火绒企业版”将终端处拦截、处理的各类威胁信息呈现在“控制中心”，方便管理员直观了解企业安全状况，并根据显示的信息制定及时、合适的安全策略。

服务器性能及时反馈

安全动态实时更新



病毒风险事件显示

漏洞修复事件显示

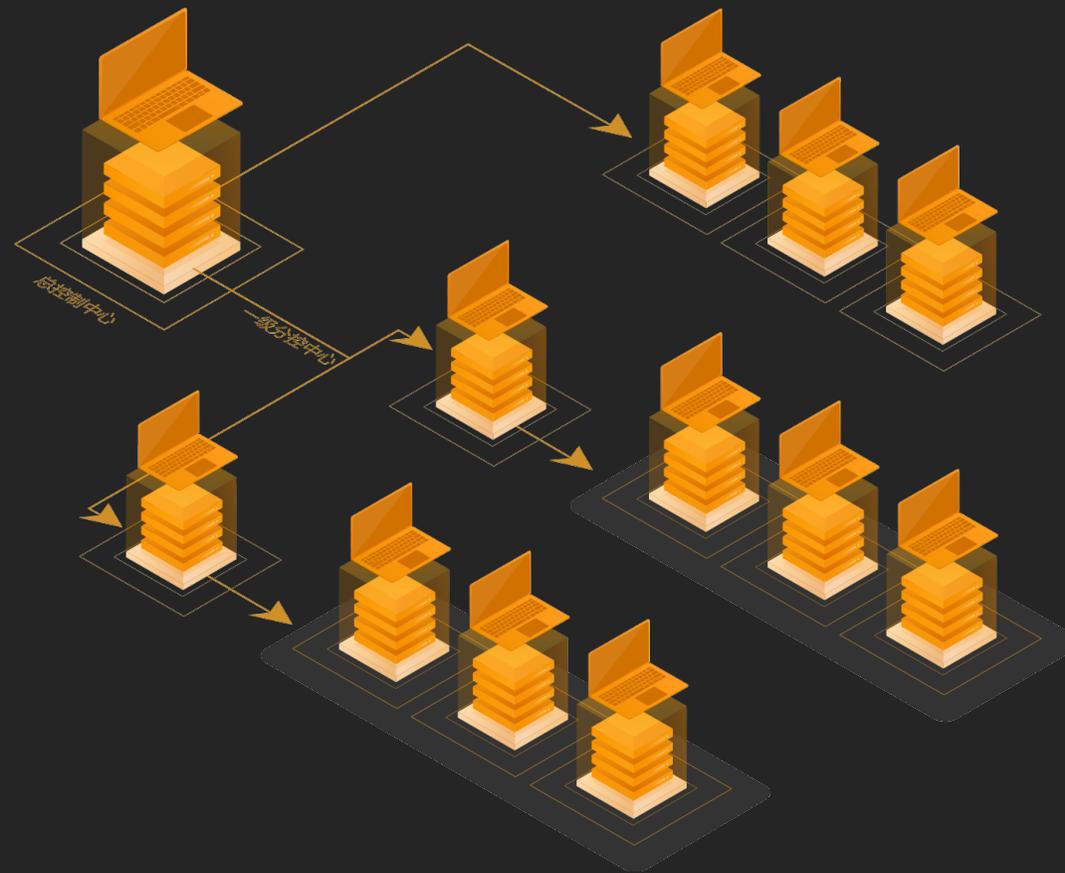
网络攻击事件显示

系统防护事件显示

# 终端管理

## 多级中心

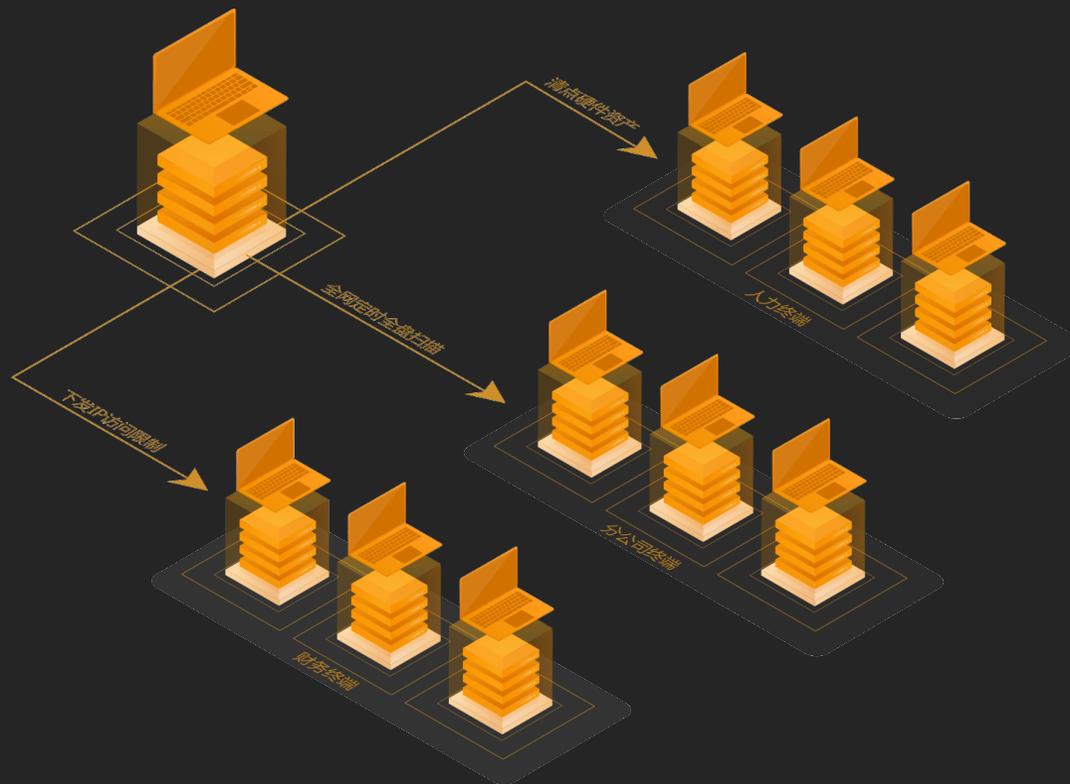
支持多中心管理，解决跨部门、跨地域管理难题，将企业网络有条不紊地纳入严密防控中，确保安全无死角。



# 终端管理

## 定制策略

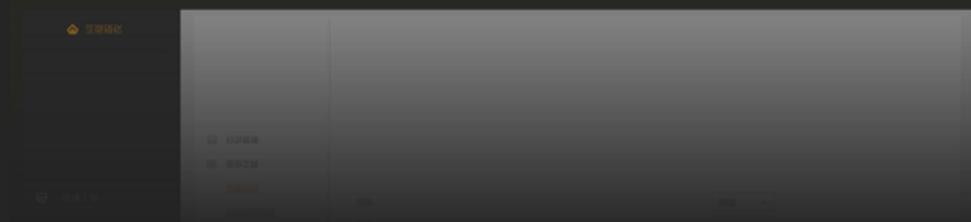
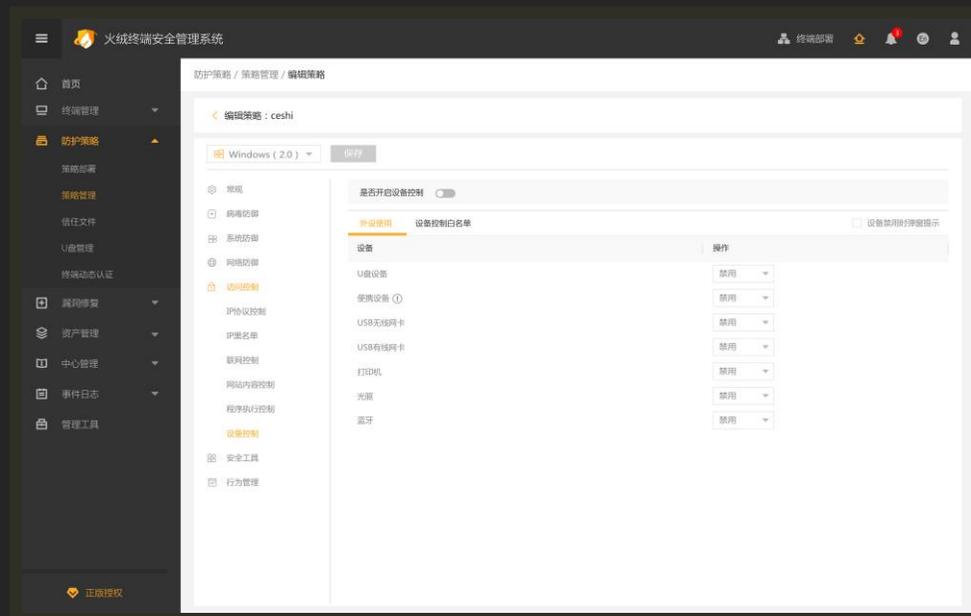
自由分组管理旗下终端，定制、下发【病毒扫描】、【漏洞修复】、【资产管理】等策略，并支持对策略进行“增、删、改、查”等操作。



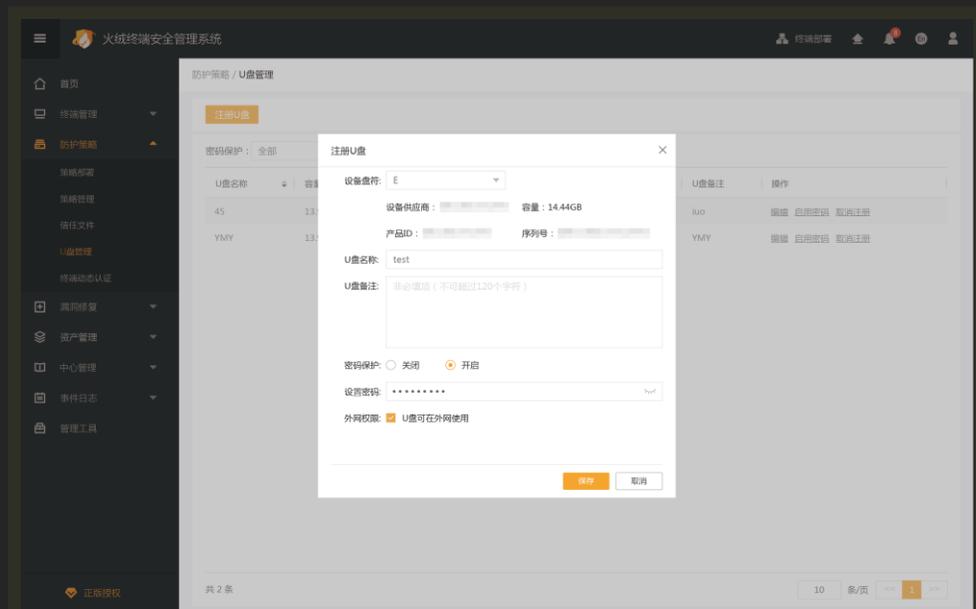
# 设备管理

## 设备管控

可实现对U盘设备、便携设备、USB无线网卡、USB有线网卡、打印机、光驱、蓝牙进行设备的使用与禁用，并支持对U盘设备、便携设备和光驱的只读操作。



# 设备管理



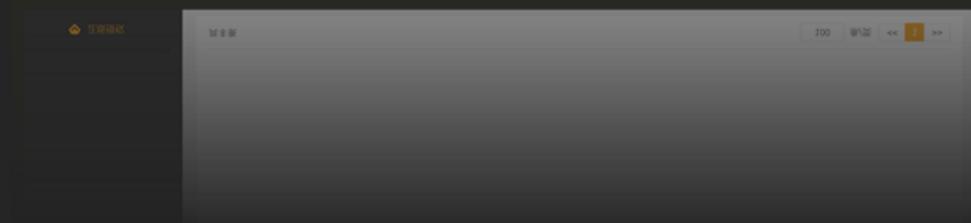
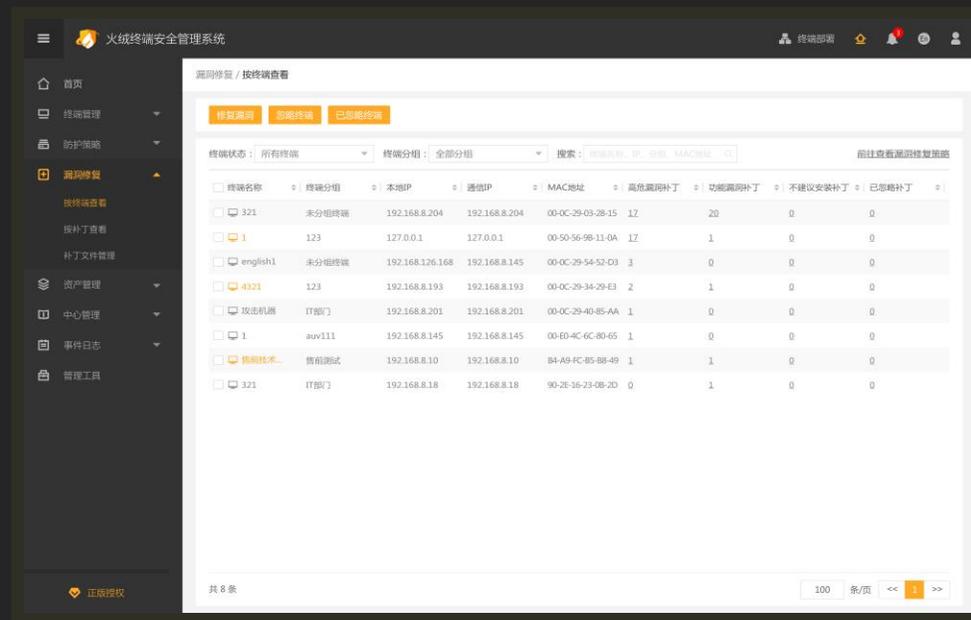
## 注册U盘

可对U盘进行精细化管理。灵活设置U盘名称、U盘备注、开启或关闭密码保护、设置密码和勾选外网权限功能。

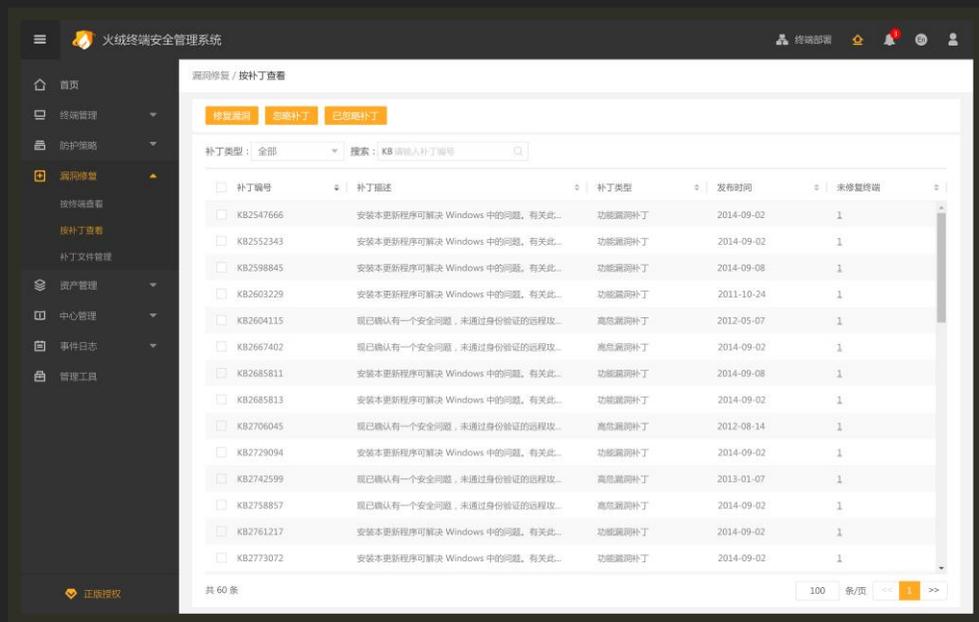
# 漏洞修复

## 漏洞修复（按终端）

可根据终端名称选择进行漏洞修复操作。分组情况、IP地址信息、漏洞补丁分类情况一目了然。



# 漏洞修复



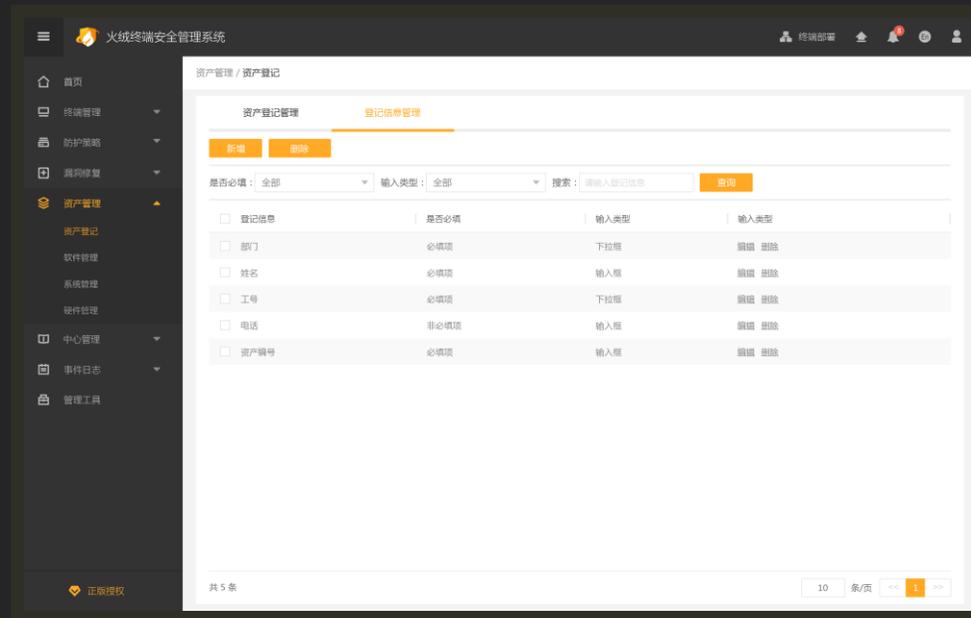
## 漏洞修复（按补丁）

可根据补丁类型或编号检索查询进行漏洞修复操作。补丁描述和发布时间等信息清晰可见。

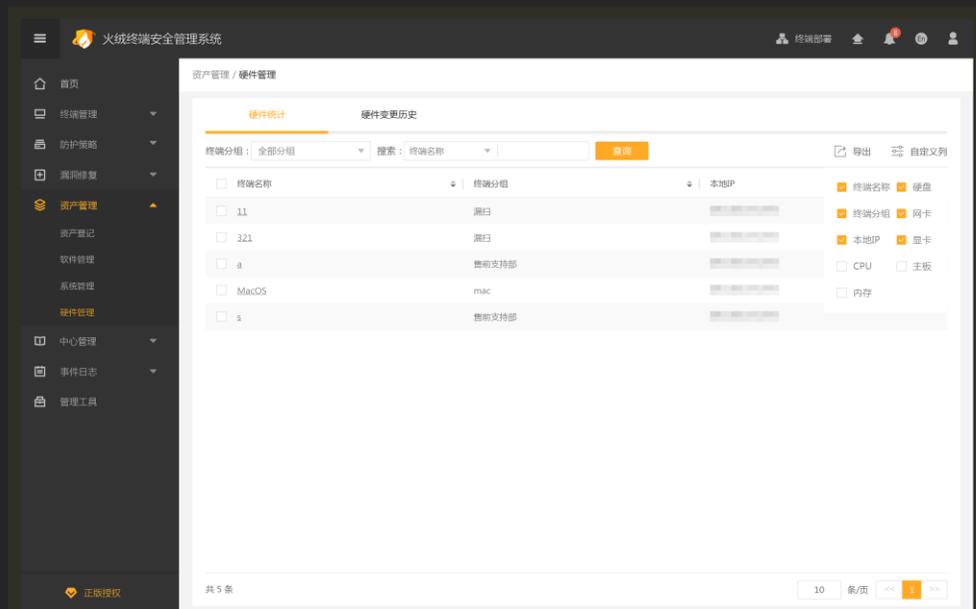
# 资产管理

## 资产登记

简约高效的登记流程。可自定义编辑或删除登记信息，设置必填项或非必填项。



# 资产管理



## 软硬件系统管理

记录和更新终端资产变更情况，包括硬件的变更、新增、遗失等，辅助运维人员对硬件资产进行准确有效的管理和记录，方便财务审计等工作。

# 日志报表

## 日志管理

支持对终端病毒查杀、病毒防御、系统防御、网络防御、访问控制、漏洞修复、行为管理、终端管理、系统管理日志的记录和统计，并可以展现和导出所产生的日志报表。

火绒终端安全管理系统

事件日志 / 访问控制

统计: 按详情 | 终端分组: 全部分组 | 时间: 查询时间 | 搜索: 按终端名 IP 分组 MAC地址 | 导出 | 自定义列 | 检索

时间	终端名称	终端分组	本地IP	通信IP	MAC地址	规则名称	协议	触发动作	远程地址	本地地址	操作进程	处理	
2022-11-15...	1	123	127.0.0.1	127.0.0.1	00-50-56-98...	IP协议控制	TCP	进站	192.168.8.14...	192.168.3.30...	Idle	-	E
2022-11-15...	1	123	127.0.0.1	127.0.0.1	00-50-56-98...	IP协议控制	TCP	进站	192.168.8.10...	192.168.3.30...	Idle	-	E
2022-11-15...	1	123	127.0.0.1	127.0.0.1	00-50-56-98...	IP协议控制	TCP	进站	192.168.8.11...	192.168.3.30...	Idle	-	E
2022-11-15...	1	123	127.0.0.1	127.0.0.1	00-50-56-98...	IP协议控制	TCP	进站	192.168.8.18...	192.168.3.30...	Idle	-	E
2022-11-15...	1	123	127.0.0.1	127.0.0.1	00-50-56-98...	IP协议控制	TCP	进站	192.168.3.58...	192.168.3.30...	Idle	-	E
2022-11-15...	1	123	127.0.0.1	127.0.0.1	00-50-56-98...	IP协议控制	TCP	进站	172.217.160...	192.168.3.30...	C:\Program... C:\Program...	-	E
2022-11-15...	1	123	127.0.0.1	127.0.0.1	00-50-56-98...	IP协议控制	TCP	进站	192.168.8.83...	192.168.3.30...	Idle	-	E
2022-11-15...	1	123	127.0.0.1	127.0.0.1	00-50-56-98...	IP协议控制	TCP	进站	192.168.8.10...	192.168.3.30...	Idle	-	E
2022-11-15...	1	123	127.0.0.1	127.0.0.1	00-50-56-98...	IP协议控制	TCP	进站	192.168.8.10...	192.168.3.30...	Idle	-	E
2022-11-15...	1	123	127.0.0.1	127.0.0.1	00-50-56-98...	IP协议控制	TCP	进站	192.168.8.11...	192.168.3.30...	Idle	-	E
2022-11-15...	1	123	127.0.0.1	127.0.0.1	00-50-56-98...	IP协议控制	TCP	进站	192.168.8.18...	192.168.3.30...	Idle	-	E
2022-11-15...	1	123	127.0.0.1	127.0.0.1	00-50-56-98...	IP协议控制	TCP	进站	192.168.8.14...	192.168.3.30...	System	-	E
2022-11-15...	1	123	127.0.0.1	127.0.0.1	00-50-56-98...	IP协议控制	TCP	进站	192.168.3.58...	192.168.3.30...	Idle	-	E
2022-11-15...	1	123	127.0.0.1	127.0.0.1	00-50-56-98...	IP协议控制	TCP	进站	192.168.8.83...	192.168.3.30...	Idle	-	E

共 63300 条

100 条/页 << 1 2 3 ... 633 >>

终端管理

共 49300 条

100 条/页 << 1 2 3 ... 493 >>

# 日志报表

统计周期内全网病毒  
风险事件累计处理

2677例

系统风险事件  
累计处理

7例

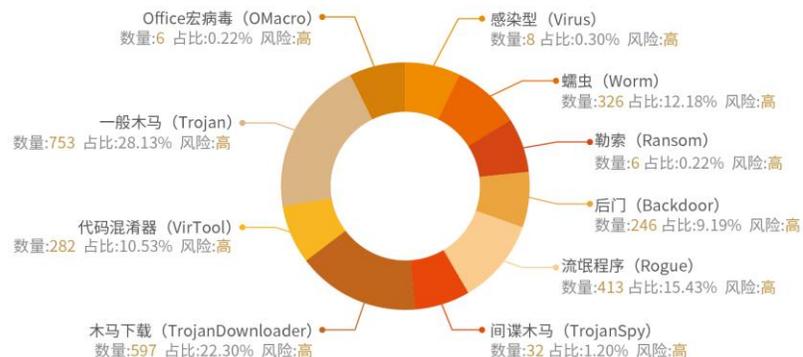
网络风险事件  
累计处理

23例

受影响终端

4台

统计周期内全网累计处理病毒2677例，病毒类型分别是:感染型(Virus)、蠕虫(Worm)、漏洞利用(Exploit)、勒索(Ransom)、后门(Backdoor)、流氓程序(Rogue)、间谍木马(TrojanSpy)、木马下载(TrojanDownloader)、木马释放(TrojanDropper)、代码混淆器(VirTool)、一般木马(Trojan)、Office宏病毒(OMacro)、广告(Adwae)



## 安全分析报告

可对火绒安全防护日志、风险详情等内容进行汇总，并提供分析结果和处理建议，帮助管理员做好后续加固工作。

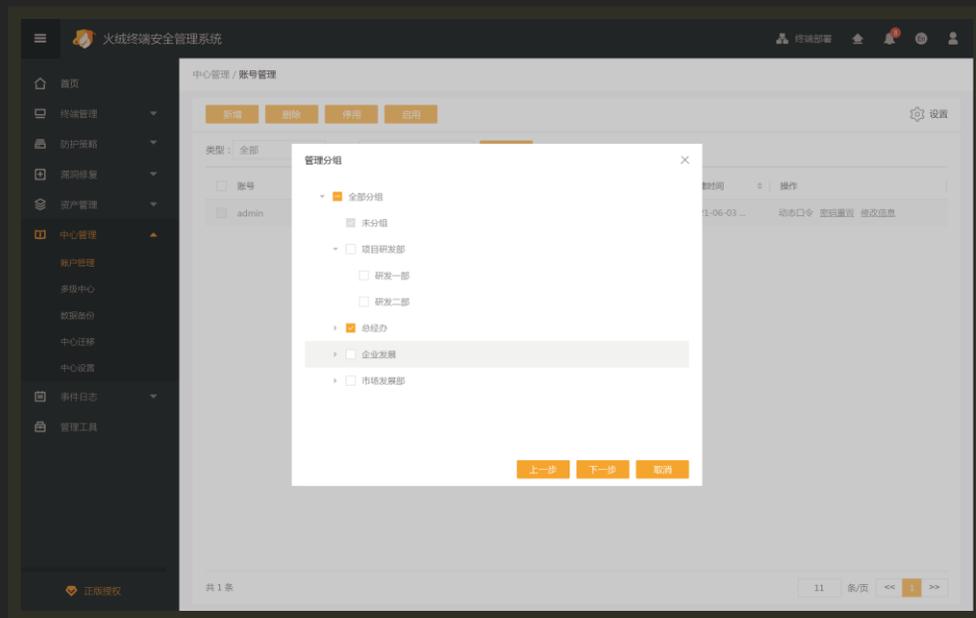
# 中心管理

## 容灾备份

通过设置备用中心，可避免主中心因宕机、断电、软硬件故障等意外突发情况带来的损失。当出现突发情况时，切换备用中心以接管主中心，确保终端安全不受影响。



# 中心管理



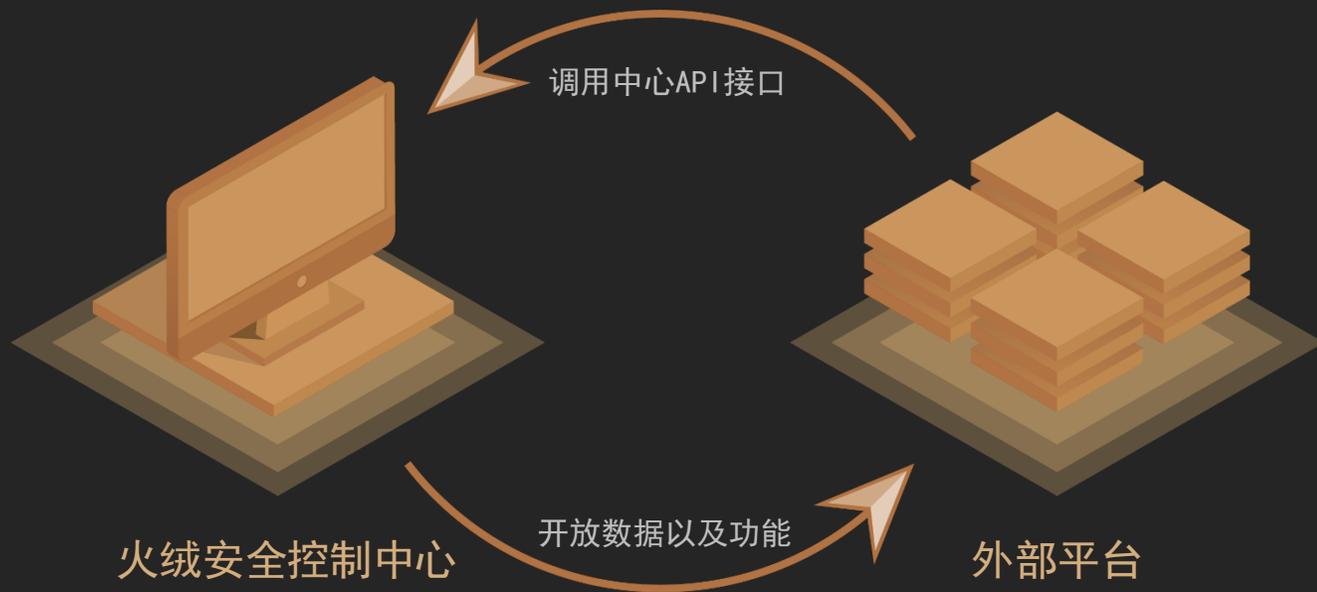
## 账号管理

通过“超级管理员”账户，添加并管理其它管理员，分管控制中心不同模块，减少、优化管理人员工作量。

# 产品联动

## API 接口

通过调用火绒安全预先定义好的API接口，开放与其它产品（如准入系统）进行联动，方便查询部署火绒安全产品的终端的信息，包括终端地址、终端名称、终端版本、分组策略、终端在线状态、病毒库版本等。随着产品完善，后续将逐渐开放更多联动信息和功能。



---

02

## 终端防护篇：技术驱动，纵深防护

---

# 火绒反病毒引擎

## 一. 自主研发，避免掣肘

独有“通用脱壳”、“动态行为查杀”技术，基于“虚拟沙盒”环境，通过行为特征来精准判断，高查杀、低误报。



通用脱壳

火绒安全研发的“通用脱壳”技术可用于戳穿病毒“伪装”，通过启发式逻辑评估待扫描样本，使其在虚拟环境中还原被保护的代码、数据和行为。因此，对比传统反病毒引擎的静态或动态指导脱壳，火绒安全“通用脱壳”可解决病毒使用的自定义壳、代码混淆器在内的所有其他代码级对抗难题。

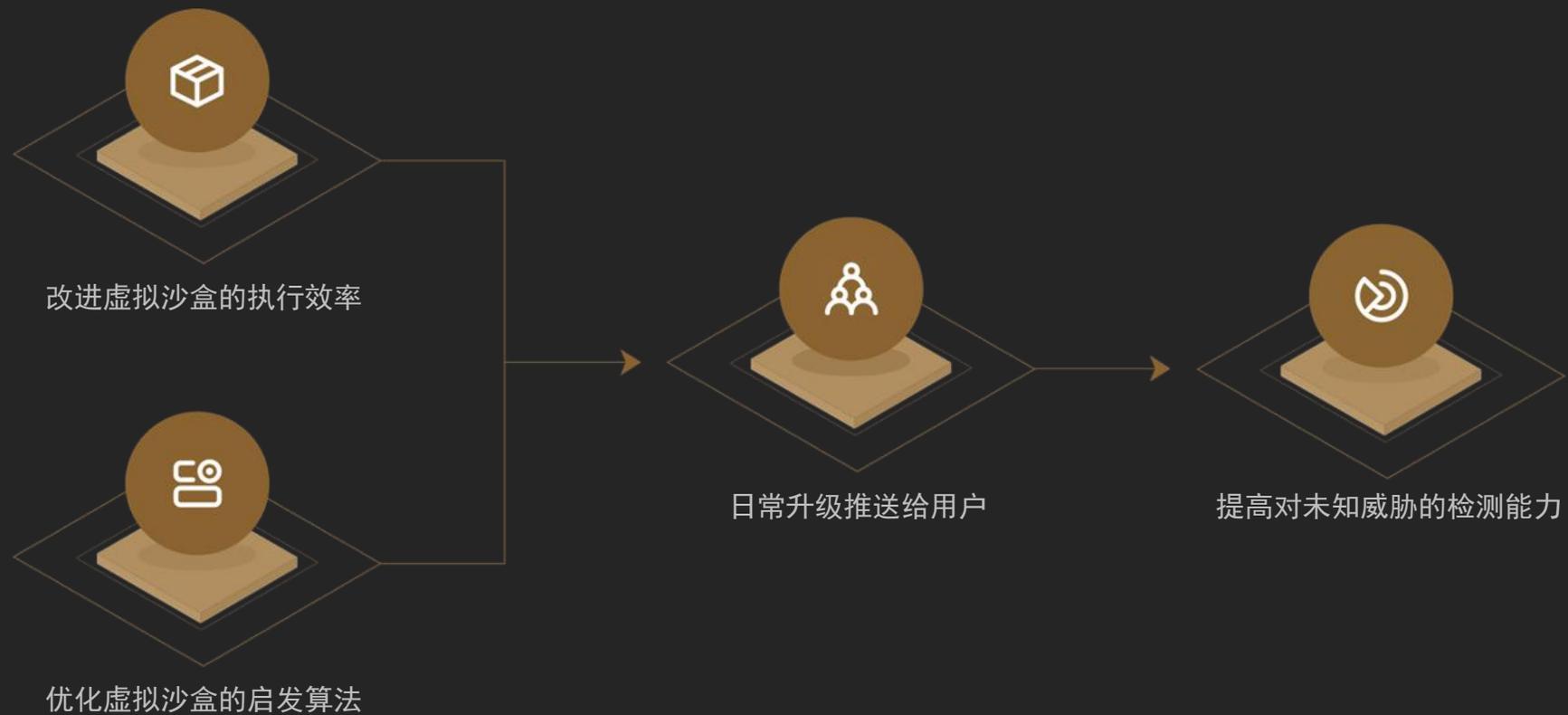


动态行为查杀

火绒反病毒引擎通过跟踪和记录程序或脚本在虚拟环境中的动态行为，配合启发式分析算法对程序的恶意行为进行评估。无论病毒如何修改或混淆特征，只要它的行为与已知的病毒行为模式匹配，就可以直接判定为病毒。因此，和传统的反病毒引擎使用的固定的特征判断病毒的方式相比，火绒引擎可以有效识别已知病毒的新变种和未知病毒。

# 火绒反病毒引擎

## 二. 持续迭代，对抗未知威胁



# 火绒反病毒引擎

## 三. 本地杀毒，不受断网影响

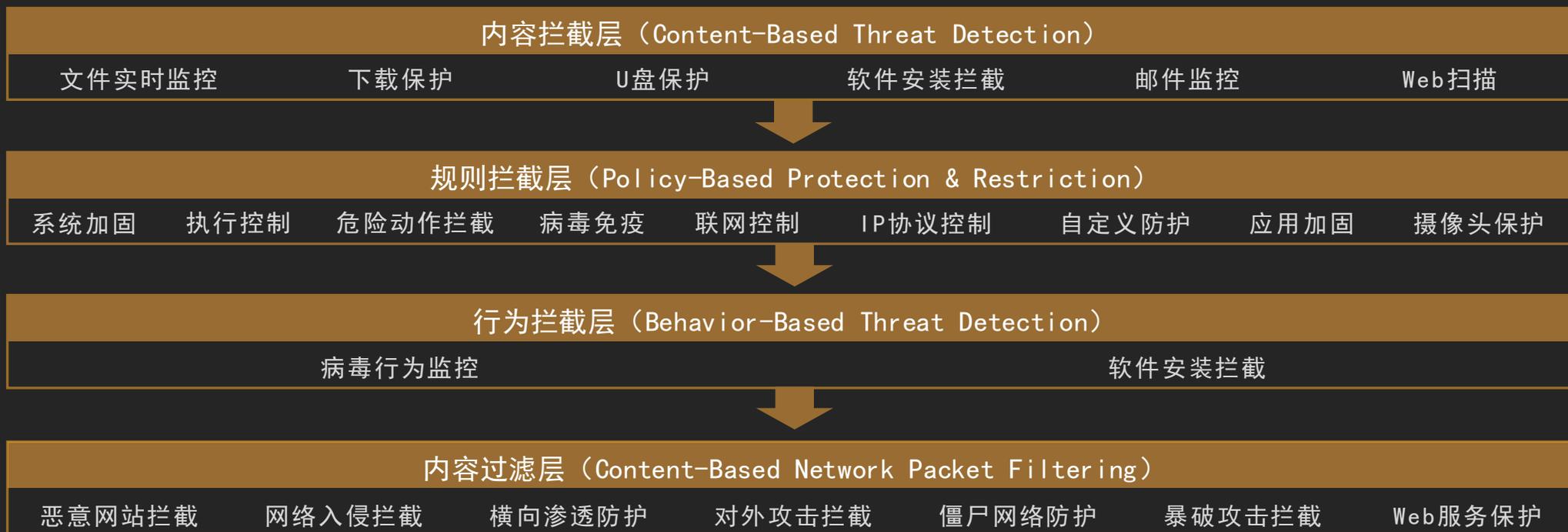


- 1 通过行为特征，第一时间精准识别各类病毒、变种以及新的威胁。
- 2 对感染型病毒、宏病毒等特殊类型病毒能够做到只清除病毒、不损害文件。
- 3 对查杀结果可阐述，能准确指出样本为病毒的依据。
- 4 对查杀结果可控，误报率低，对软件的兼容性好。
- 5 本地杀毒能力强，不受断网环境影响。

# 多层次主动防御系统

## 一. 构建充分防护纵深

火绒安全产品率先将单步防御和多步恶意监控相结合，监控百个防御点（包含防火墙），有效阻止各种恶意程序对系统的攻击和篡改，保护终端脆弱点。



火绒纵深防护体系

# 多层次主动防御系统

## 二. 多层次主动防御系统



### 01. 灵活的网络管理

火绒安全产品具备完整的防火墙，可以从“协议”、“来源”、“应用程序”三个维度对终端的网络连接进行全面预防。

### 02. 僵尸网络防护规则

通过对网络通讯数据进行扫描，识别主机存在的Botnet、RAT和后门程序与黑客间的恶意通信并进行拦截，无需人工干预。



# 多层次主动防御系统

## 03. 漏洞攻击防护技术

对严重的蠕虫级漏洞、Web服务漏洞，提前创建“虚拟补丁”，保护存在漏洞的操作系统或者程序免受黑客攻击。

## 04. RDP弱口令渗透防护

通过二次验证与IP白名单设置，阻止终端密码泄漏后遭遇攻击的风险。尤其对利用RDP弱口令入侵的勒索病毒防御效果显著。

 功能消息

网络入侵拦截 1分钟前  
受到【192.168.5.25】的网络攻击，已阻止

清除所有通知

 功能消息

爆破攻击防护 1分钟前  
受到【192.168.3.177】的网络攻击，已阻止

清除所有通知

# 多层次主动防御系统

## 05. 应用加固防护技术

对受保护的进程行为进行监控，防止黑客利用应用程序中未修复的漏洞或零日漏洞对主机发起攻击。



## 06. 全面的系统加固

对系统的防护包括文件防护、注册表防护、敏感动作防护三大项共86个防护点。



# 绘制威胁情报系统，执行EDR防护策略

## 一. 威胁情报系统

火绒威胁情报系统实时报告互联网中存在的威胁

每一个用户、终端都将享受“情报驱动安全”带来的防护

2,490,660

当日病毒防御事件

1,387,113

当日终端防御事件

5,909,756

当日网络防御事件

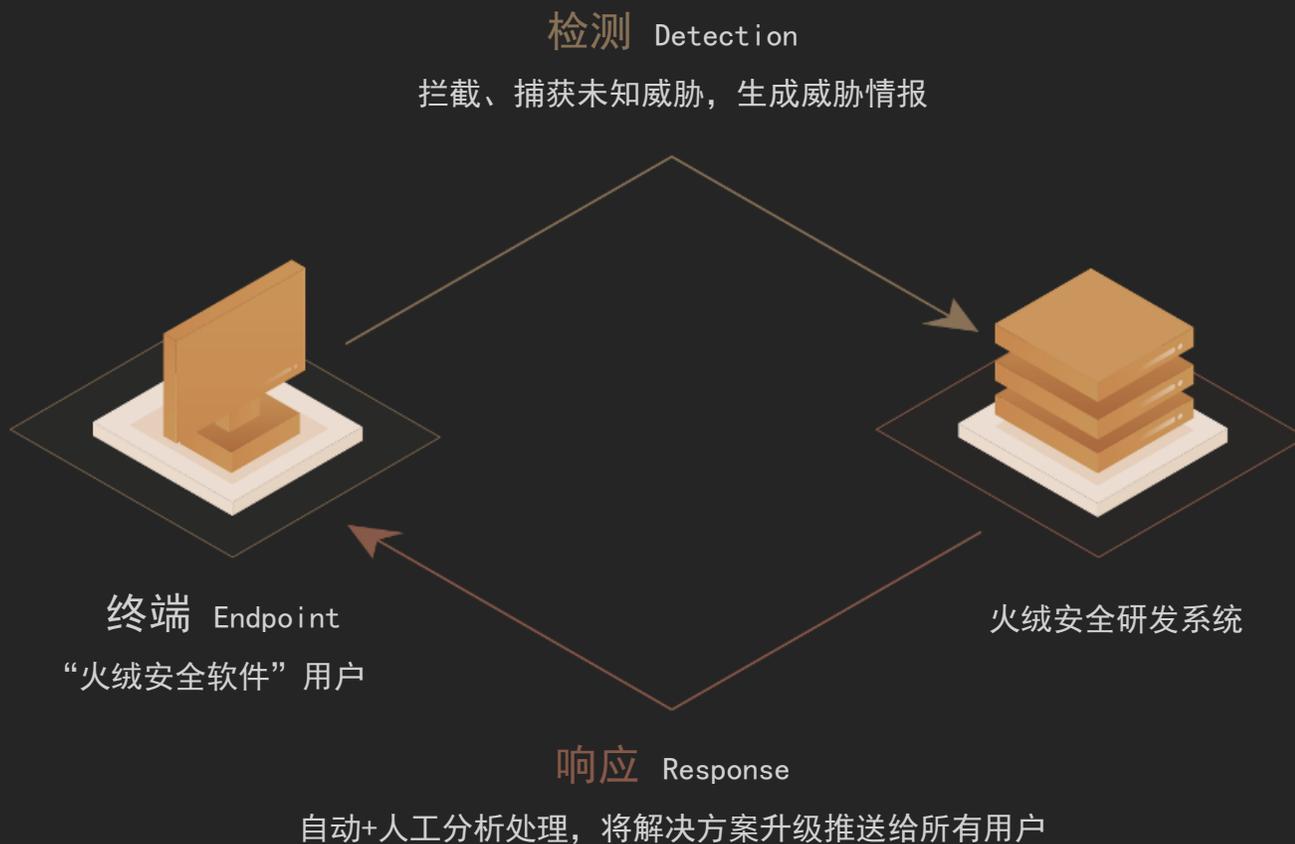


# 绘制威胁情报系统，执行EDR防护策略

## 二. EDR防护策略

终端捕获威胁信息后，在安全情报系统响应，经过分析处理后升级

解决方案，再反馈给所有火绒终端。



---

03

产品优势篇：平台开发完善，产品契合国情

---

# 成熟稳定的产品性能



## 兼容好

对政企机构使用的特殊软件有较强的兼容性，不影响正常办公。



## 本土化

能迅速处理、拦截国内常见流行的蠕虫、挖矿、勒索等病毒和流氓侵权行为。



## 占用小

占用空间小、配置要求低，轻巧干净，不拖慢电脑速度。



## 适配广

支持微软系统、Linux主流系统和macOS系统，并支持国产芯片及系统。

# 火绒企业版2.0系统适配图

Linux系统			Windows系统				macOS系统
 <b>Linux服务器版终端</b>	 <b>Linux桌面版终端</b>	 <b>Linux版控制中心</b>	 <b>Windows版终端</b>	 <b>Windows版控制中心</b>	 <b>WindowsServer版终端</b>	 <b>WindowsServer版控制中心</b>	 <b>macOS版终端</b>
<b>支持系统：</b> <ul style="list-style-type: none"><li>CentOS</li><li>Ubuntu</li><li>SUSE</li><li>统信UOS</li><li>银河麒麟</li><li>中标麒麟</li><li>中科红旗</li><li>优麒麟</li><li>深度</li><li>龙芯 (Loongnix) 等发行版</li></ul>	<b>支持系统：</b> <ul style="list-style-type: none"><li>Ubuntu</li><li>SUSE</li><li>统信UOS</li><li>银河麒麟</li><li>中科红旗</li><li>优麒麟</li><li>深度</li><li>龙芯 (Loongnix) 等发行版</li></ul>	<b>支持系统：</b> <ul style="list-style-type: none"><li>Ubuntu 16.04</li><li>Ubuntu 22.04</li><li>CentOS 7</li><li>CentOS 8</li><li>RedHat6.1</li><li>openSUSE 15</li><li>UOS-20 (统信)</li><li>Kylin-v10-sp1 (麒麟) 等发行版</li></ul>	<b>支持系统：</b> <ul style="list-style-type: none"><li>Windows XP (SP3)</li><li>Windows Vista</li><li>Windows 7</li><li>Windows 8</li><li>Windows 8.1</li><li>Windows 10</li><li>Windows 11</li></ul>	<b>支持系统：</b> <ul style="list-style-type: none"><li>Windows 7</li><li>Windows 8</li><li>Windows 8.1</li><li>Windows 10</li><li>Windows 11</li></ul>	<b>支持系统：</b> <ul style="list-style-type: none"><li>Windows Server 2003 (SP1)</li><li>Windows Server 2008</li><li>Windows Server 2012</li><li>Windows Server 2016</li><li>Windows Server 2019</li><li>Windows Server 2022</li></ul>	<b>支持系统：</b> <ul style="list-style-type: none"><li>Windows Server 2008 (R2)</li><li>Windows Server 2012</li><li>Windows Server 2016</li><li>Windows Server 2019</li><li>Windows Server 2022</li></ul>	<b>支持系统：</b> <ul style="list-style-type: none"><li>macOS10.13及以上版本</li></ul>
<b>备注：</b> <ul style="list-style-type: none"><li>x86_64 (glibc 2.12及以上版本)、MIPS64、AArch64 (glibc 2.17 及以上版本)、LoongArch64 (glibc 2.28 及以上版本)</li></ul> <b>支持CPU：</b> <ul style="list-style-type: none"><li>支持Intel/AMD/飞腾/鲲鹏/兆芯/海光/龙芯等CPU</li></ul>		<b>备注：</b> <ul style="list-style-type: none"><li>x86_64 (glibc 2.12及以上版本)、AArch64 (glibc 2.17 及以上版本)</li></ul> <b>支持CPU：</b> <ul style="list-style-type: none"><li>支持Intel/AMD/飞腾/鲲鹏/兆芯/海光等CPU</li></ul>	<b>支持CPU：</b> <ul style="list-style-type: none"><li>Intel</li><li>AMD</li></ul>				<b>支持CPU：</b> <ul style="list-style-type: none"><li>Intel</li><li>M1</li></ul>

# 严格的职业操守



尊重  
用户隐私

火绒安全秉承安全厂商的基本操守，保证产品没有任何捆绑、弹窗、侵占资源等行为，并强力阻挡和狙杀各种流氓软件、商业软件的侵权行为，确保系统干净清爽。



保护企业  
数据安全

针对政府、商业企业等机构用户，火绒安全独家承诺：“尊重用户的隐私权、数据所有权，不会上传用户的任何文件、数据信息”。

# 全面适配国产化

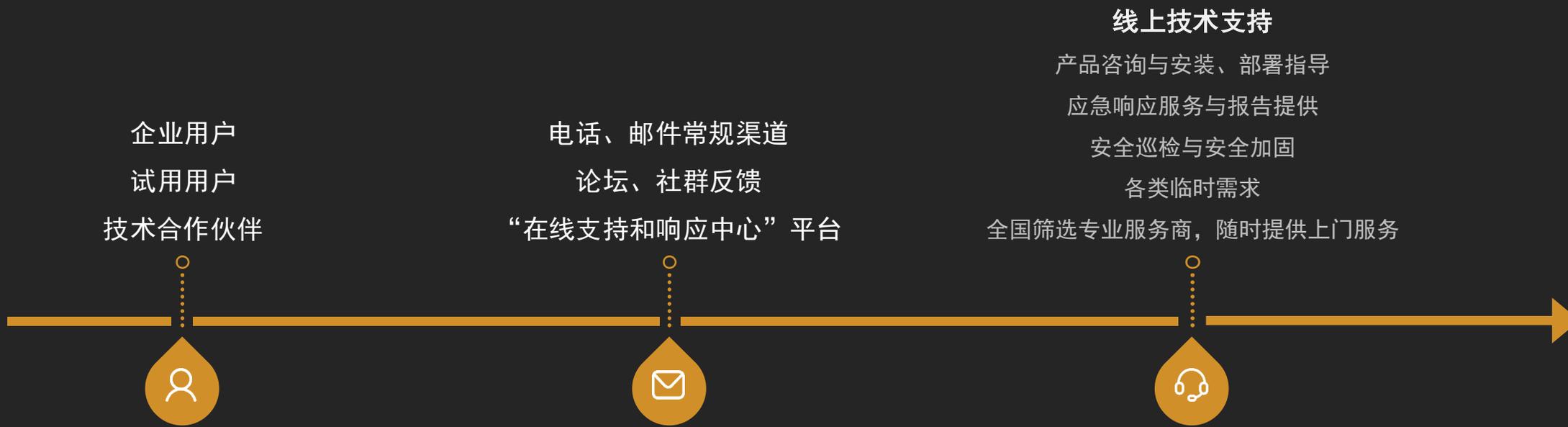
一直以来，火绒安全都在国产化服务的道路上不断稳步前行，包括产品和自主研发的反病毒引擎技术模块也早已完成对主流国产CPU芯片和操作系统的支持。



# 企业服务分钟级响应

## 一. 科学严谨的服务流程

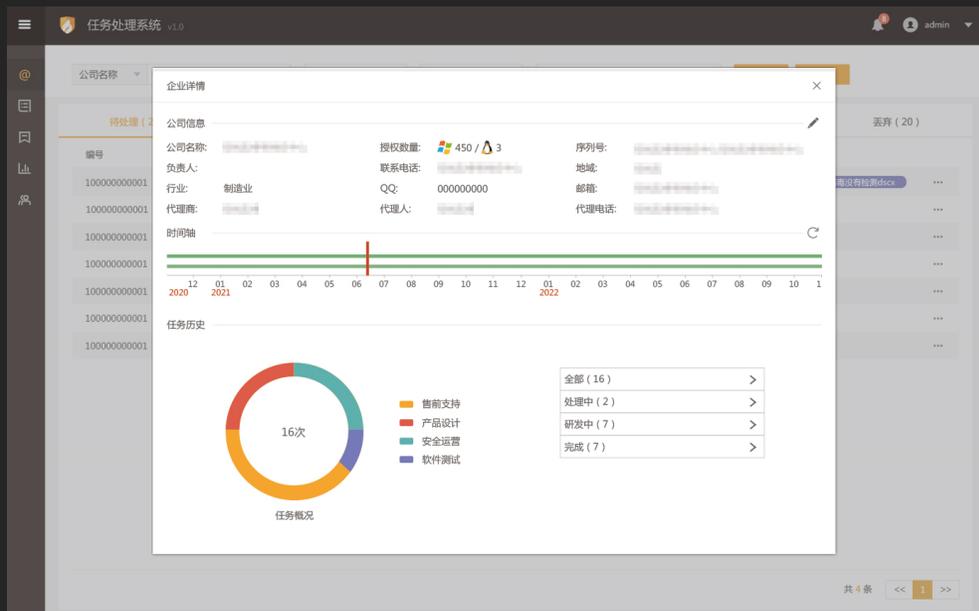
火绒安全建立了一套完整、专业的服务平台和流程，通过集中收集用户、代理商、技术合作伙伴的需求，分拣派发给反病毒研究、产品开发、产品测试、售前和售后服务等相关部门，及时匹配专业的工程师评估、解决。



# 企业服务分钟级响应

## 二. 完善齐全的服务平台

### 用户服务平台和系统



任务处理系统

The screenshot shows an '在线支持与响应中心' (Online Support and Response Center) form. The service hours are listed as '每日9:30-18:30'. The form includes the following fields:

- \* 问题分类:** Radio buttons for 使用指导, 问题与BUG, 功能建议, 购买咨询.
- \* 问题标题:** Text input field with placeholder '请填写您的标题'.
- \* 问题描述:** Text area with placeholder '请填写您的问题描述'.
- 上传附件:** A button labeled '上传附件' with a note '(可上传5个附件,每个附件大小不得超过8M)'. A '提交' (Submit) button is located to the right.

在线支持和响应中心

---

04

企业合作篇：产品覆盖全国用户，技术赋能广大同行

---

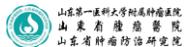
# 市场覆盖



50多细分行业 | 数万家单位 | 覆盖全国 | 延伸海外

# 事业单位 (部分)

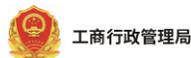
## 医疗



## 国有企业



## 政府



## 教育



嘉兴市海盐县教育局

## 军工业



## 交通



## 能源



# 商业用户（部分）

 京东金融  
京东数科旗下

 拼多多  
拼着买·才便宜





 唯品会  
品牌特卖

 锦江国际  
Jin Jiang International

 叮当  
快药

 酒仙网  
www.Jiuxian.com

 Joyoung 九阳

 慈铭体检  
CIMING CHECKUP  
只一方健康

 山东港口 | 烟台港  
SHANDONG PORT GROUP | Yantai Port

 京客隆

 ZTO  
中通快递  
ZTO EXPRESS

 YTO  
圆通速递  
express

 百世  
BEST LOGISTICS

 喜马拉雅

 桂林银行  
GUILIN BANK



 红牛  
红牛功能饮料

 华文  
与您携手 改变生活

 保德利  
BAODELI

 美年大健康  
Health 100

 Quanta Computer  
广达集团

 Glodon  
广联达

 GDS 万国数据

 JACK 杰克  
杰克缝纫机

 RAVO  
宁波瑞孚工业集团有限公司

 SONGZ  
松芝股份

 通和股份  
TONHE FLUID

 万乘金融服务集团  
Wansun Financial Services Group

 易程股份  
EASYWAY | 行之易 享其程  
Easyway Easy journey

 电魂  
ELECTRONIC SOUL

 中控 · SUPCON

 张小泉  
ZHANG XIAO QUAN

# 行业安全方案

## 一. 医疗行业

### 问题与挑战

医疗行业在信息化建设不断提升的过程中，大部分设备没有进行及时的统一更换，导致各科室机器、系统冗杂。正常运转业务时，空闲时间较短，导致无法定期对内网终端进行安全检测。发生一定的风险时，不能够及时了解安全事件的源头，无法对安全事件进行溯源以及追责。



### 解决方案

“火绒终端安全管理系统”，通过提供病毒防御、系统防御、网络防御、访问控制、资产管理、漏洞修复等功能，为医疗企业实现全网终端的安全防护和管理，构建全网一体化防病毒系统，避免其数据和财产的损失。

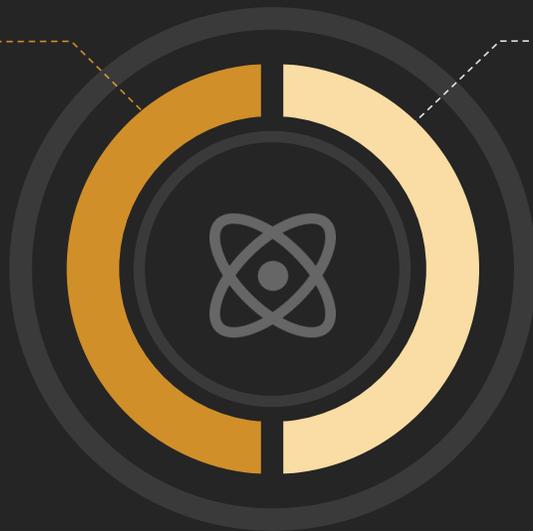
- ★ 在威胁检测上，深度洞察发现，精准有效查杀；
- ★ 在情报响应上，敌情预先感知，延伸纵深防护；
- ★ 在统筹管控上，资产统一管理，设备统一设防；
- ★ 在边界延伸上，通过合作+赋能，构筑泛安全边界。

# 行业安全方案

## 二. 互联网行业

### 问题与挑战

日常下载办公软件容易出现病毒隐患。黑灰色利益链迅速发展，恶意的网站带有钓鱼、欺诈行为、下载者木马。外设的私自乱用容易引起病毒横向传播。不少企业缺少主动防御系统，可攻击的入口多，导致内网瘫痪。



### 解决方案

对于互联网行业企业内部终端受到的威胁，火绒安全通过布局总体安全策略，除了常规的威胁检测和网络防御外，还将从风险评估、安全意识培训、预警通告、安全巡检、安全加固等角度保障企业安全。

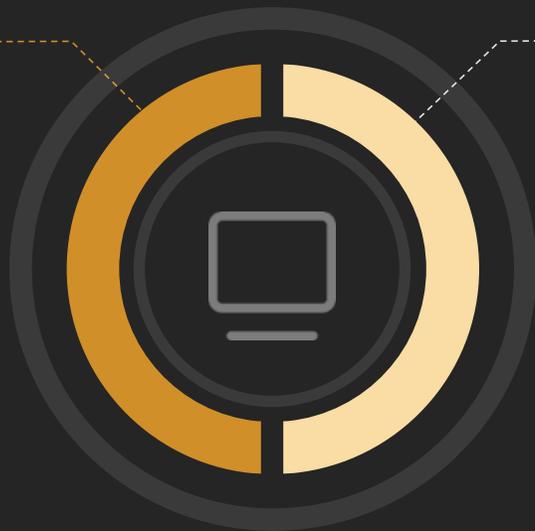
- ★ 风险评估：以企业终端设施为轴，对系统防护、应用软件、漏洞和数据进行深度扫描和检测。
- ★ 安全巡检：以企业安全设备为托，对防护状态、补丁管理、病毒查杀等结果出具分析报告。
- ★ 加固建议：以威胁入侵缺口为点，通过多层防护，如应用加固、动态认证功能堵截。

# 行业安全方案

## 三. 科技行业

### 问题与挑战

在发展过程中，企业的大部分设备没有及时进行统一更换，在资产管理上遇到难题，如无法找到员工对应的机器、无法统计操作系统占比、无法了解到员工装的软件是否符合规范等。老旧的设备、系统在运行防病毒软件时可能会占用过多的资源，导致影响正常业务。



### 解决方案

科技行业的安全防护是一项大规模的防御性工作，而终端作为易被攻击的脆弱点，更需要重点对待。“火绒终端安全管理系统”从网络、系统、病毒三个层面，配合定制化的管控策略，可针对不同类型的威胁，做出积极的应对。

- ★ 通过威胁检测层面，以EDR运营体系为基础，快速感知、处理潜在的安全隐患和威胁。
- ★ 通过网络防护层面，利用内容过滤、行为判断、规则加固，构建一体化防御体系。
- ★ 通过管控管理层面，设置对外拦截策略和对内准入规定，让威胁无法内外串联扩大影响。

# 服务商

为了更好地服务广大企业用户，火绒安全开启与代理商合作模式。相比于分销、推广等销售能力，我们期待前来合作的伙伴厂商拥有更好的技术服务能力和意识；我们也会提供给大家专业的培训、指导，期待您的加入。



火绒安全已签订上千家合作供应商

在全国范围内提供优质服务

# 技术赋能

一直以来，火绒安全不仅将反病毒引擎等具备自主知识产权的技术用于自身产品，还向广大合作伙伴技术赋能。截至目前，火绒安全已经成为国内成熟的反病毒引擎提供商。

我们希望，通过产品与技术输出的形式，结合规范化的商业模式，来加强与友商、相关安全机构的合作，以此拓宽和延伸终端防护领域，覆盖更大的服务范畴，守护广大用户的终端安全。



安恒信息  
DAS-security 安全中国



杰思安全  
MAJORSEC



天融信  
TOPSEC



北信源 VRV<sup>®</sup>  
信息安全管理



启明星辰  
领航信息安全



天际友盟  
TianJi Partners



中控 · SUPCON

# 火绒终端安全管控与防护

## 中心/系统运维

- 账号管理
- 中心设置
- 日志管理
- 中心升级
- 中心地址管理
- 通知设置
- 邮件预警
- 服务器带宽设置
- 中心迁移

## 资产管理

- 资产登记管理
- 资产登记信息管理
- 软件管理
- 系统管理
- 硬件统计
- 硬件变更历史

## 访问控制

- IP协议控制
- IP黑名单
- 程序执行控制
- 设备控制
- 网站内容控制
- 联网控制

## 日志报表

- 病毒查杀日志
- 病毒防御日志
- 系统防御日志
- 网络防御日志
- 访问控制日志
- 漏洞修复日志
- 终端管理日志
- 系统管理日志
- 安全分析报告
- Syslog安全日志
- Syslog升级日志
- Syslog漏洞日志

## 级联部署

- 多级中心
- 中心策略同步

## 病毒防御

- 文件实时监控
- 恶意行为监控
- U盘保护
- 下载保护
- 邮件监控
- Web扫描

## 口令验证

- 管理员密码校验
- 中心动态认证
- 终端动态认证
- 高权限操作动态认证

## 设备管控

- U盘设备
- 便携设备
- USB无线网卡
- USB有线网卡
- 打印机
- 光驱
- 蓝牙
- 设备白名单
- 信任U盘

## 数据可视化概览

- 病毒查杀事件可视化
- 漏洞修复事件可视化
- 网络攻击事件可视化
- 系统防护事件可视化
- 服务器性能可视化
- 操作系统占比可视化

## EDR运营体系

- 终端 (Endpoint) 探测威胁
- 检测 (Detection) 处理威胁
- 响应 (Response) 解决威胁

## 灾备机制

- 备用中心
- 数据备份与恢复

## 行为管控

- 违规外联
- 软件禁用

## API接口

## 环境体系

- C/S-B/S架构
- Windows全系列
- Linux主流发行厂商
- 国产操作系统

## HIPS防御系统

- 系统加固
- 恶意网址拦截

## 系统防御

- 软件安装拦截
- 摄像头防护
- 浏览器保护
- 应用加固

## 网络防御

- 网络入侵拦截
- 对外攻击拦截
- 僵尸网络防护
- 爆破攻击防护
- 远程登录防护
- WEB服务保护
- 横向渗透防护

## 核心技术

- 自研新一代反病毒引擎
- 通用脱壳技术
- 动态行为查杀
- 静态扫描
- 动态启发式扫描
- 多层次主动防御系统

## 威胁情报

- 火绒威胁情报系统
- 数千万终端探针
- 本地威胁情报分析

## 安全工具

- 漏洞修复
- 系统修复
- 弹窗拦截
- 垃圾清理
- 文件粉碎
- 启动项管理
- 断网修复
- 网络流量

## 终端运维

- 终端任务一键下发
- 终端树状分组管理
- 自定义终端展示信息
- 终端数据一键导出
- 自定义终端标签
- 多规则终端检索引擎
- 终端远程支持
- LDAP组织架构导入
- 计划任务
- 漏洞修复
- 终端隔离
- IP绑定设置
- 隔离文件恢复
- 文件分发
- 垃圾清理
- 终端标签管理
- 终端发现

## 服务体系

- 7\*24小时应急响应
- 多渠道问题反馈
- 分钟级服务反馈
- 企业专享服务平台
- 问题跟踪系统
- 线上技术支持
- 应急响应服务
- 专属安检报告
- 定制安全巡检
- 专业上门服务

## 中心定制

- 支持Logo定制
- 支持模块定制

# THANK YOU

我们坚持在终端安全领域，提供专业的产品和专注的服务



火绒安全

北京火绒网络科技有限公司

Beijing Huorong Network Technology Co., Ltd.

北京市朝阳区红军营南路15号院瑞普大厦D座4层

Floor #4, Tower D, Ruipu Building, No. 15 Hongijunying South Road, Chaoyang District, Beijing. China