火绒安全
HUORONG SECURITY

# 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

2024/12/2

情报驱动　技术革新　免费试用　定制服务

# 目录 CONTENTS

# 01 公司介绍

# 公司介绍


**企业公司简介**

## 火绒安全

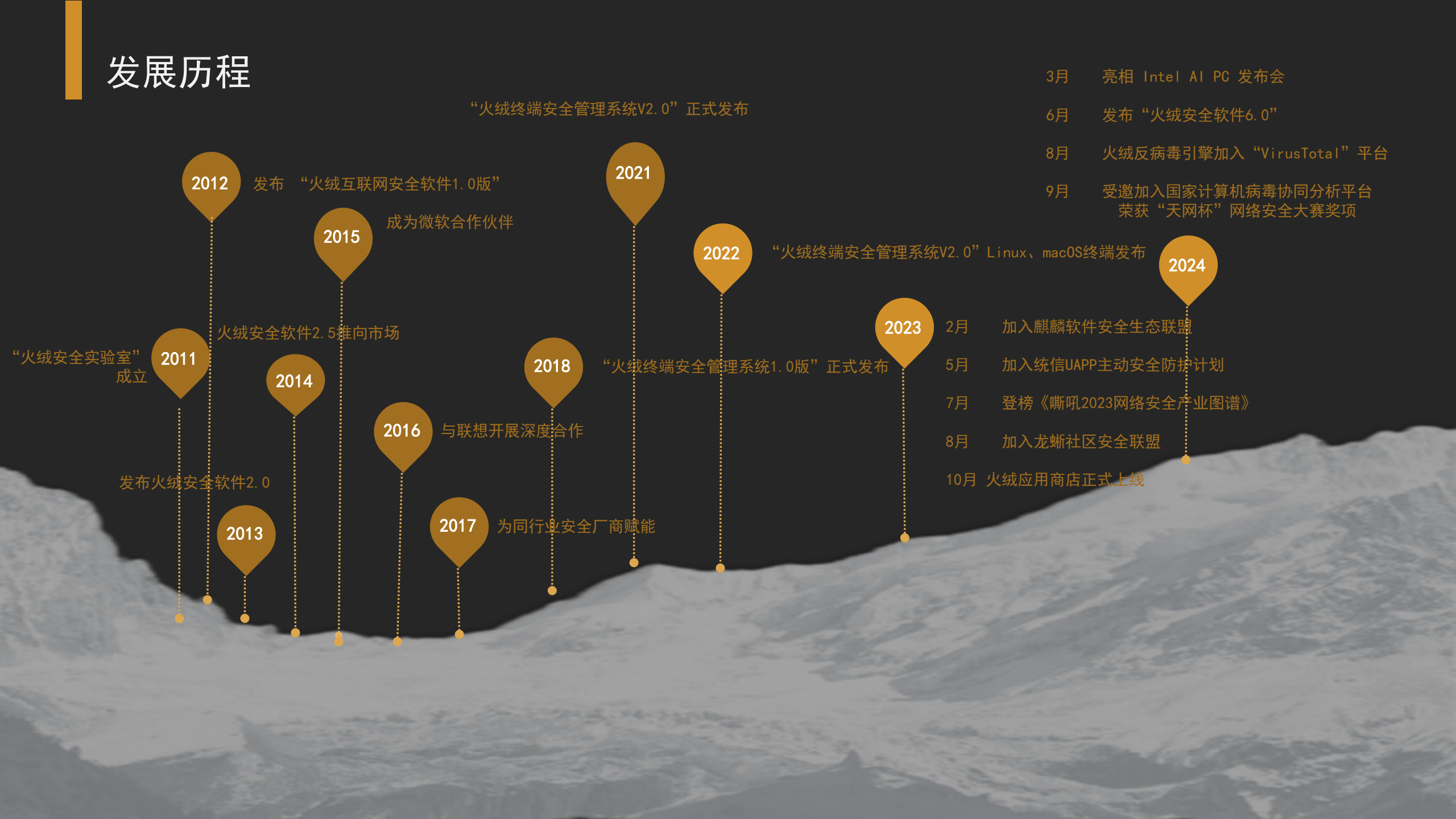
HUORONG SECURITY

火绒安全成立于2011年9月，是一家专注、纯粹的安全公司，致力于在终端安全领域，为用户提供专业的产品和专注的服务，产品功能涵盖“恶意代码防护”、“系统防护”、“网络防护”、“身份鉴别”、“资产管控”、“入侵防范”等，并持续对外合作反病毒引擎等相关自主研发技术。

2012年，火绒安全推出免费个人产品，凭借“专业、干净、轻巧”的特点收获良好的用户口碑；经过6年技术打磨和经验沉淀后，火绒安全于2018年正式推出企业版产品，并在线上线下同时试销，仅两年就有上万家企业用户参与试用购买，覆盖金融、医疗、公检法等50余类细分行业和单位机构

截至目前，火绒安全已建立起包含研发、产品、测试、运营、市场、商务在内的完整团队，具备健全的企业架构，可向用户提供成熟的终端安全产品和配套的安全服务。随着业务和产品的拓展，火绒安全团队的规模还在不断扩大中。

# 发展历程


2011
“火绒安全实验室”成立
2012
发布 “火绒互联网安全软件1.0版”
2013
发布火绒安全软件2.0
2014
火绒安全软件2.5推向市场
2015
成为微软合作伙伴
2016
与联想开展深度合作
2017
为同行业安全厂商赋能
2018
“火绒终端安全管理系统V2.0”正式发布
2021
“火绒终端安全管理系统1.0版”正式发布
2022
“火绒终端安全管理系统V2.0”Linux、macOS终端发布
2023
2月 加入麒麟软件安全生态联盟
5月 加入统信UAPP主动安全防护计划
7月 登榜《嘶吼2023网络安全产业图谱》
8月 加入龙蜥社区安全联盟
10月 火绒应用商店正式上线
2024
3月 亮相 Intel AI PC 发布会
6月 发布“火绒安全软件6.0”
8月 火绒反病毒引擎加入“VirusTotal”平台
9月 受邀加入国家计算机病毒协同分析平台
荣获“天网杯”网络安全大赛奖项

# 企业文化

一个纯粹、专注的终端安全技术公司。

## 使命

让用户安全、安静、自由地操作终端

## 价值观

追求本质，以实现真实的安全价值为唯一目的

## 立业之本

冷静、艰苦、长期地专注于核心技术研究

## 业务核心

在终端安全领域，提供专业的产品和专注的服务

## 商业模式

仅通过产品和服务实现盈利

# 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

军工业

交通

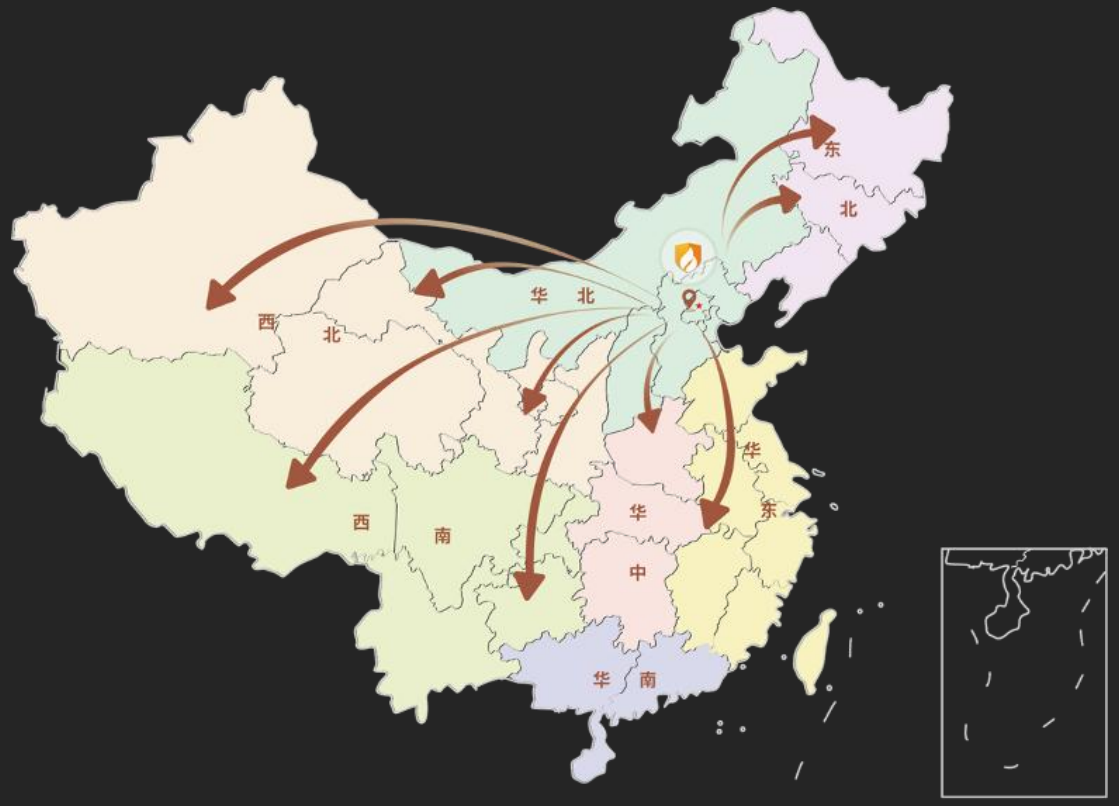
能源

# 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
得物
小红书
唯品会
品牌特卖
Jin Jiang International
锦江国际
叮当快药
酒仙网
www.Jiuxian.com
Joyoung 九阳
慈铭体检
CIMING CHECKUP
只为健康
山东港口
SHANDONG PORT GROUP
烟台港
Yantai Port
京客隆
ZTO
中通快递
ZTO EXPRESS
YTO express
圆通速递
百世
BEST LOGISTICS
喜马拉雅
桂林银行
GUILIN BANK
HONDA
红蜻蜓鞋业
華潤
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
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

# 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

# 技术合作

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，还与广大合作伙伴技术合作。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。

Lenovo

安恒信息 DAS-security 安全中国

北信源VRV 信息安全管理

DP tech

杰思安全 MAJORSEC

天融信 TOPSEC

Venus 启明星辰 领航信息安全

天际友盟 TianJi Partners

Microsoft

02

# 产品介绍

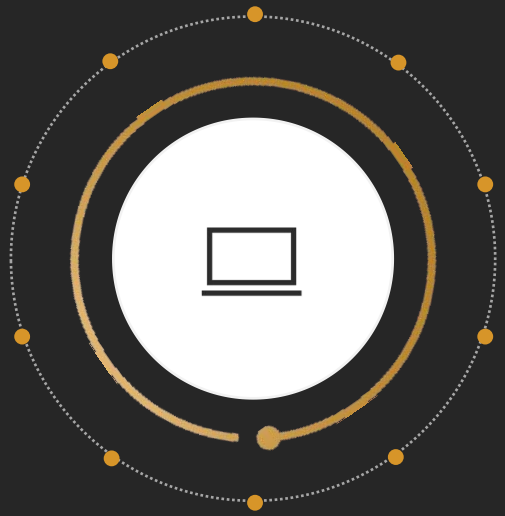
# 常见终端安全管理问题

终端成为安全威胁的主要来源，是火绒安全软件的主要服务对象，所以要保护终端用户的系统安全，我们需要分析企业终端用户真正面临的威胁是什么。

网络内病毒泛滥，如何彻底清除和预防？

如何有效规避病毒、网络及系统层面的风险？

如何统一网络内终端安全配置？



如何限制某此软件安装、执行和使用？

U盘如何有效限制使用？

网络内终端安装有哪些软件？

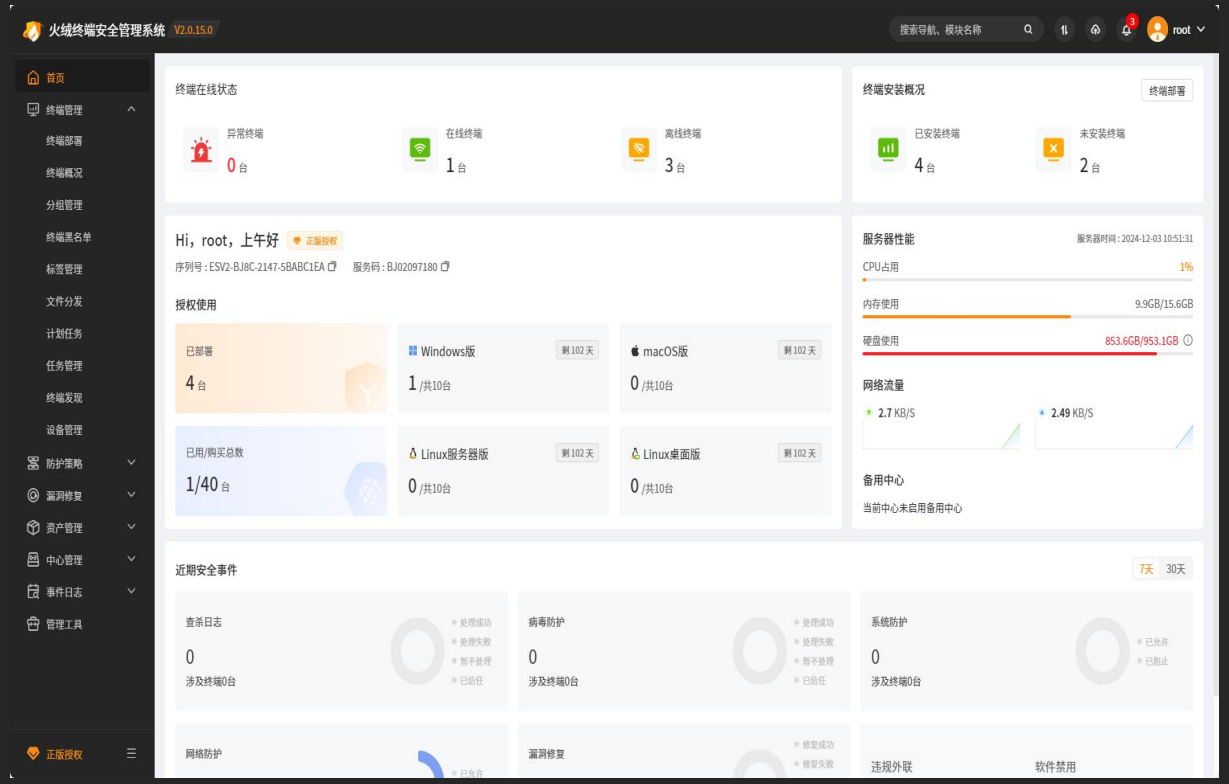
办公电脑经常有广告弹窗怎么办？

终端设备是谁在使用？

操作系统漏洞如何统一管理和修复？

终端遇到问题时，如何快速响应和处理？

# 火绒中心




## 火绒终端安全管理系统中心

火绒终端安全管理系统分为控制中心和安全终端两部分，用户需要分别部署后，通过控制中心实现对网内终端统一管理和安全策略部署。控制中心整体采用B/S架构，用户可通过浏览器访问中心服务器IP地址及端口访问控制中心，实现对网内终端进行安全策略统一部署、任务下发、安全终端管理、安全日志分析等操作，总览全网安全态势。

# 火绒客户端


## 火绒客户端

火绒客户端通过浏览器访问中心服务器IP地址和部署端口访问部署界面，下载火绒客户端也就是火绒终端安全管理系统的执行端，可执行用户在管理中心下发的查杀任务以及按照管理中心配置的安全策略自动防护终端机器环境，并持续与控制中心保持通讯，传递安全日志。

# 核心安全防御

不依赖白名单，消除了信任漏洞，自上而下地在所有可能的威胁入口设计独特的防御策略，共同有效地防御不同类型的恶意威胁。

**终端动态认证**

二次验证阻断RDP弱口令入侵

**网络入侵拦截**

拦截系统高危漏洞攻击

**横向渗透防护**

阻止黑客入侵网络的后续渗透行为

**僵尸网络防护**

切断黑客与后门病毒的联系


**恶意网址拦截**

拦截钓鱼、盗号等危险网站

**流氓软件拦截**

及时提醒软件安装行为

**应用加固**

保护正常应用程序不被恶意利用

**邮件监控**

检测邮件及附件安全性

# 终端管控

通过控制中心向终端派发安全策略、规范外接设备使用、提供远程桌面服务、进行异地终端管理等，解决企业常见管理难题，并实时监控终端安全。

**文件分发**

实现其他程序的批量安装

**远程桌面**

高效、快速响应桌面运维

**外设管理**

有效管理外设的使用范围及状态

**补丁管理**

制定统一漏洞修复策略

**资产登记**

有效对全网终端资产进行管理

**软件管理**

实现全网软件的统计和管理

**系统管理**

了解全网操作系统使用及占比信息

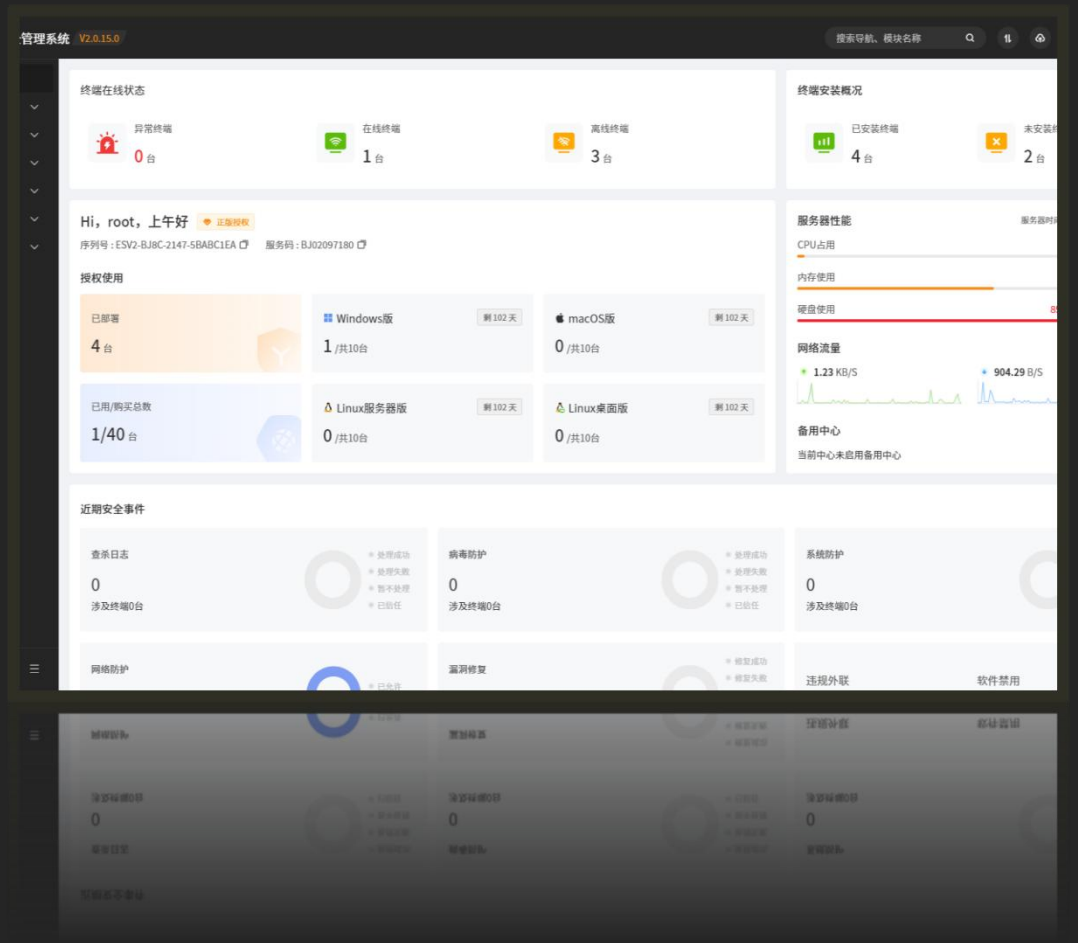
**硬件管理**

了解全网硬件系统详细信息

# 可视化控制中心

## 可视化控制中心

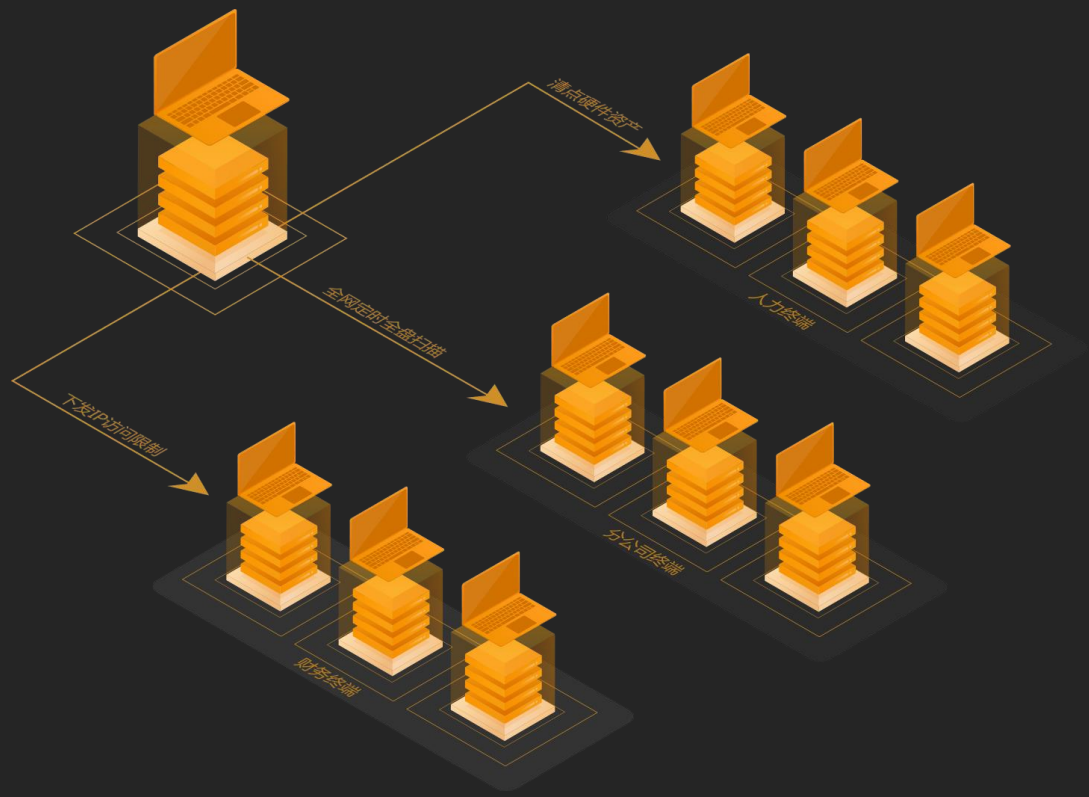
直观呈现各类威胁信息，反馈服务器性能，方便管理员制定及时、合适的安全策略



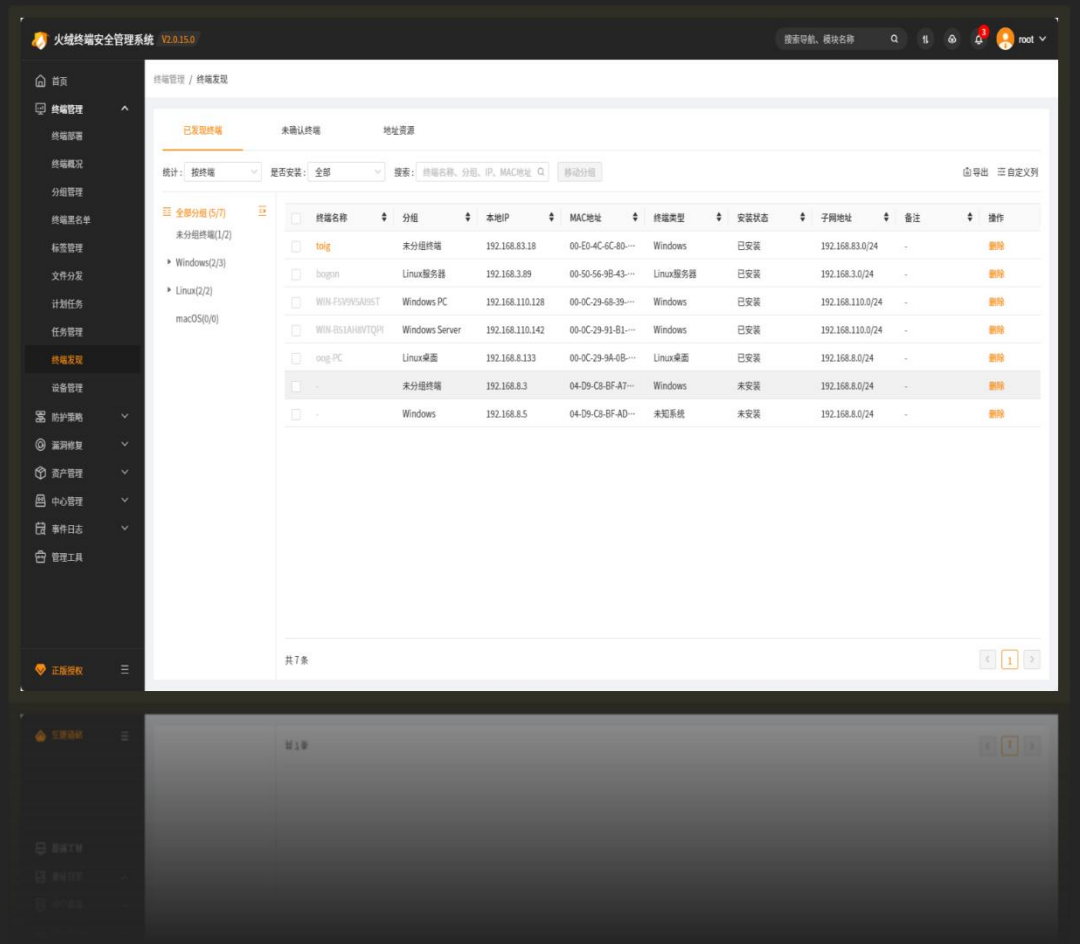
# 防护策略

## 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。



# 终端发现



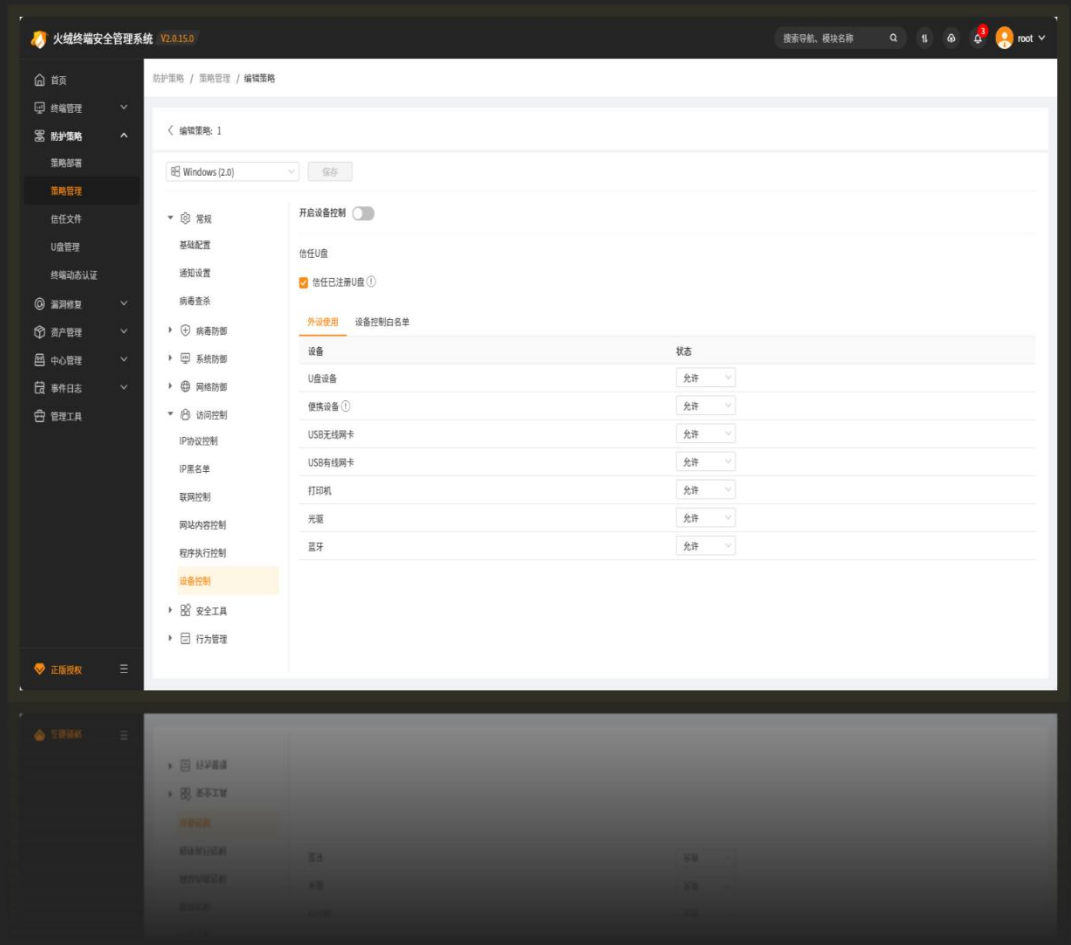

## 终端发现

帮助管理员发现需要安装但没有安装火绒安全终端的计算机，以免出现漏管漏控的情况

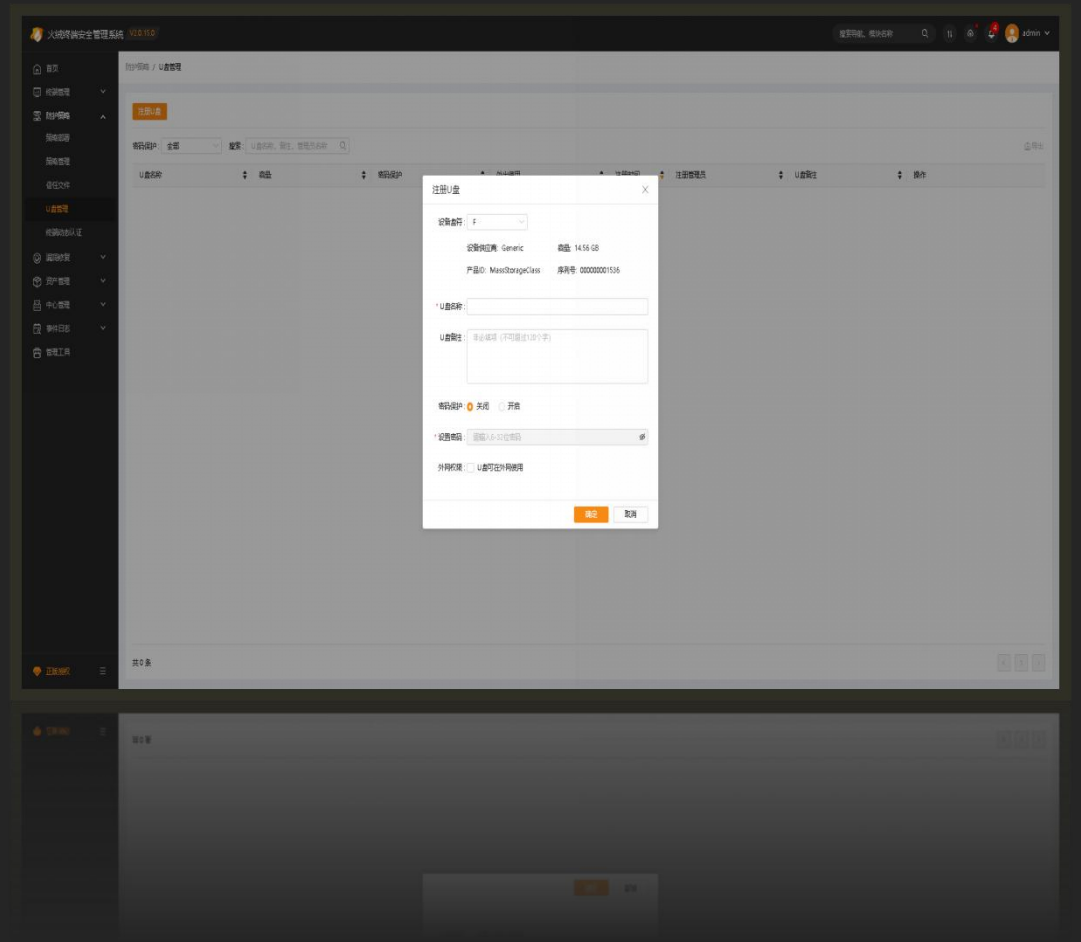
# 设备管理

## 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。

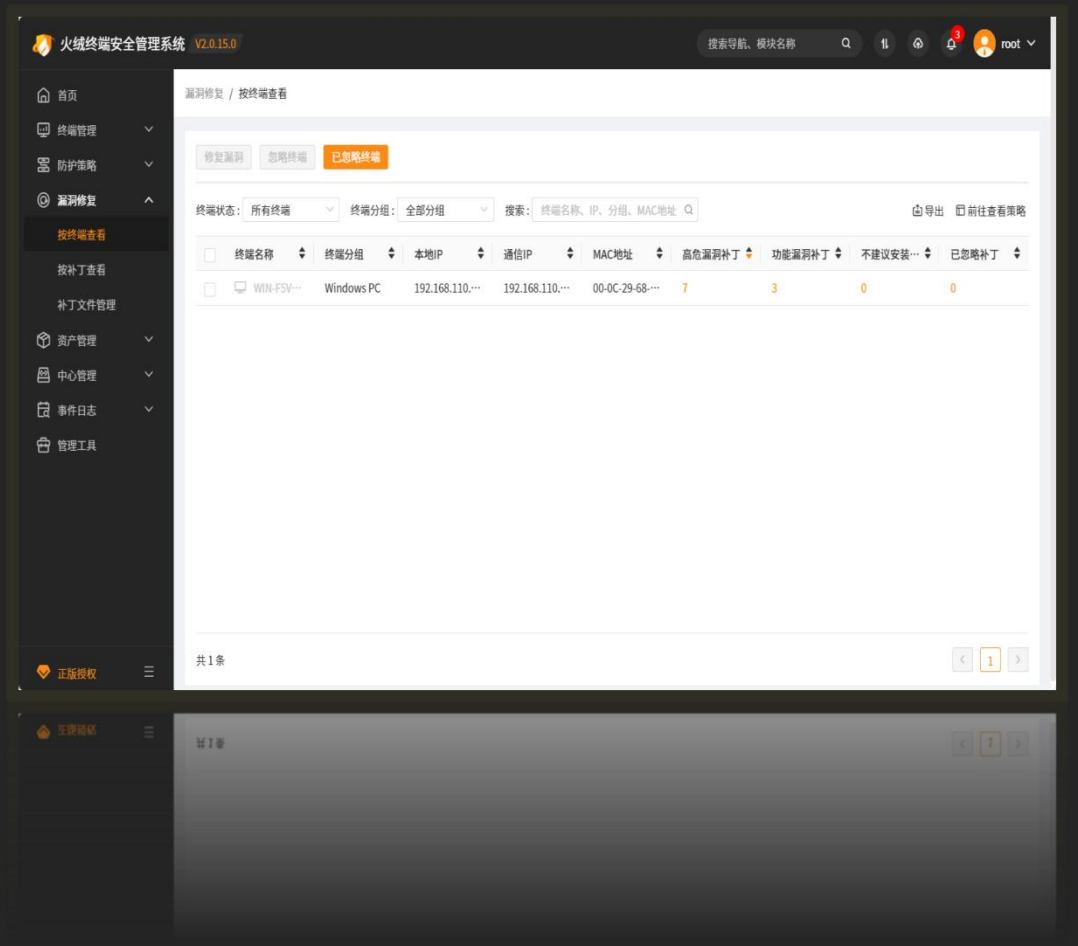
# 漏洞修复

## 漏洞修复（按终端）

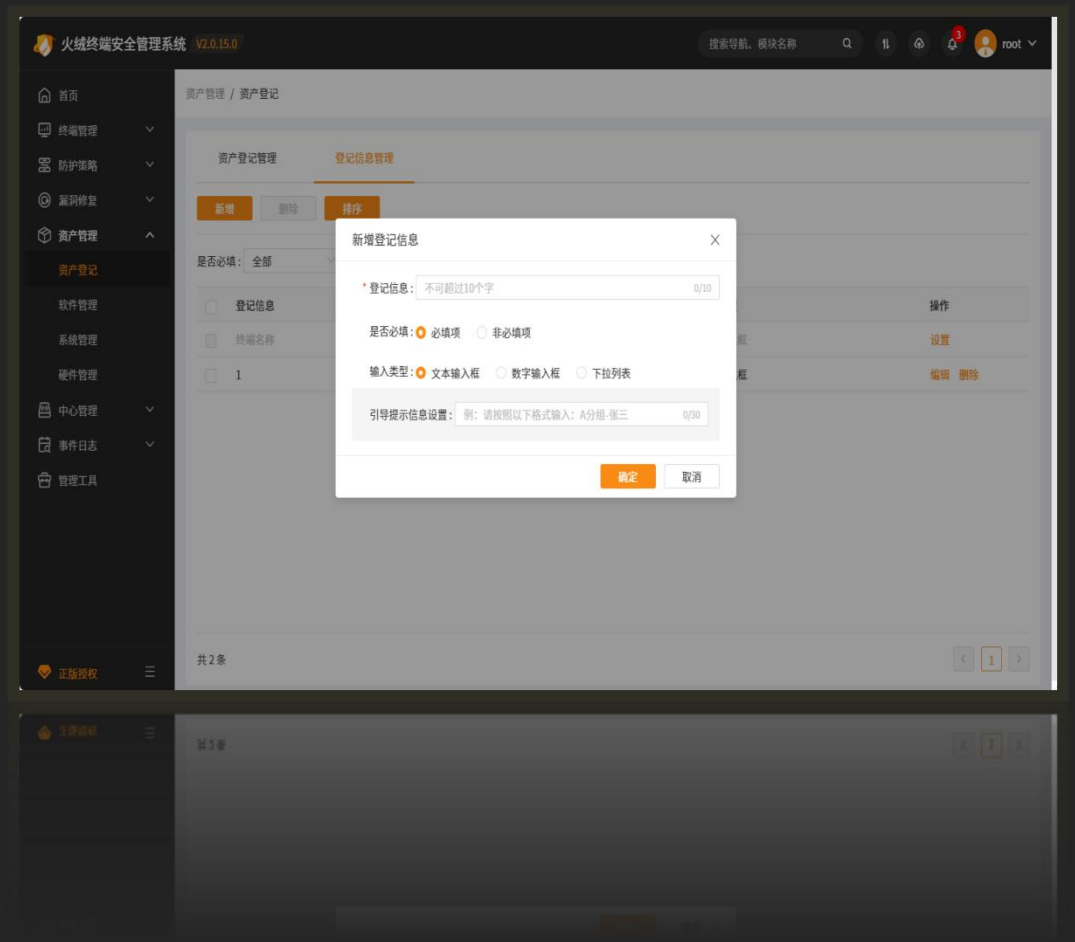
可根据终端名称选择进行漏洞修复操作。分组情况、IP地址信息、漏洞补丁分类情况一目了然。

## 漏洞修复（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。

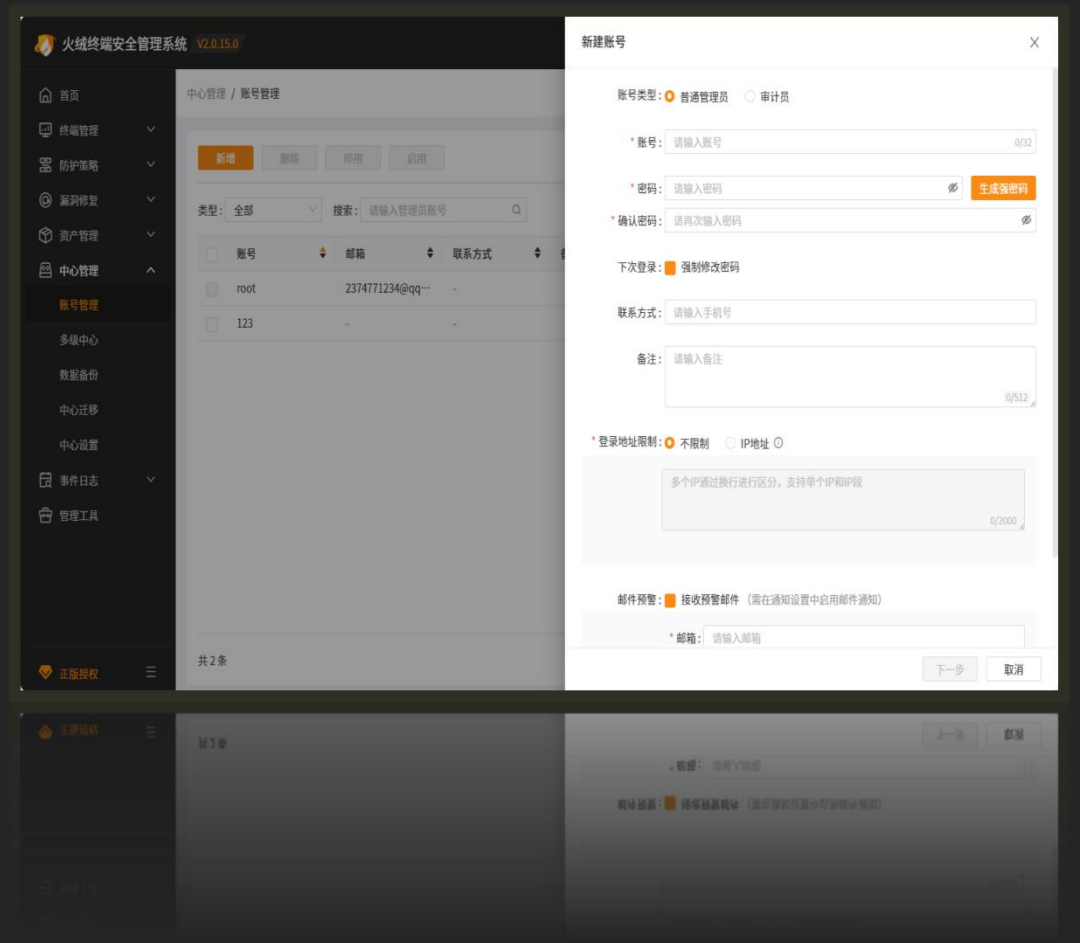
## 软硬件系统管理

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。

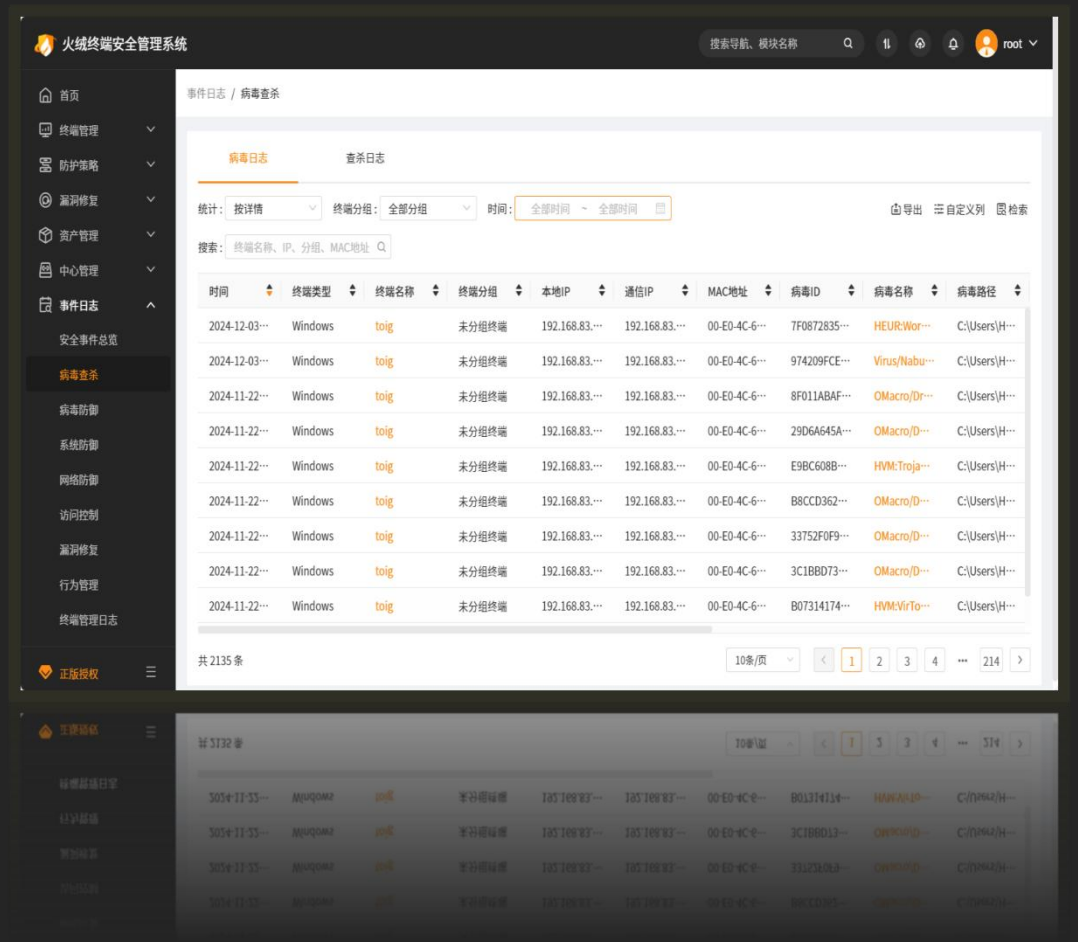
# 中心管理

## 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。



# 日志报表




## 日志管理

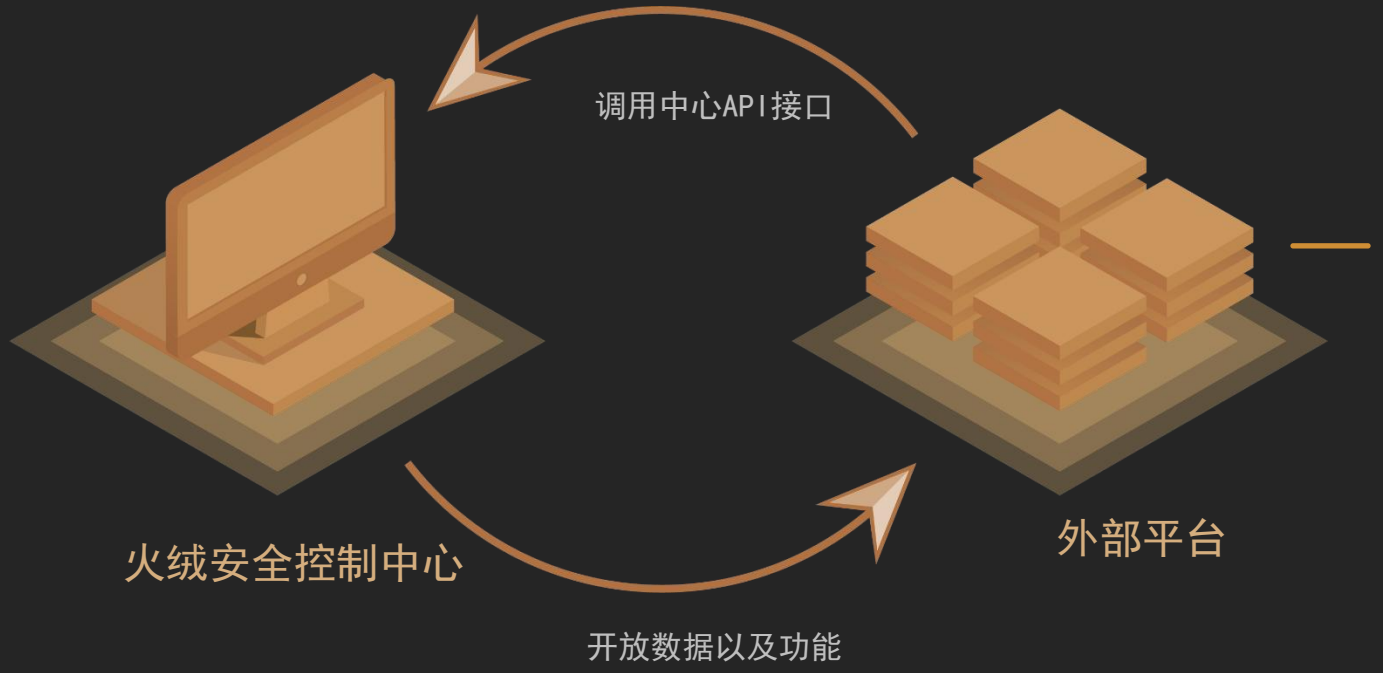
支持对终端病毒查杀、病毒防御、系统防御、网络防御、访问控制、漏洞修复、终端管理、系统管理日志的记录和统计，并可以展现和导出所产生的日志报表。

# 日志报表

## 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。

# 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。

# 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

## 级联部署
多级中心
中心策略同步

## 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

## 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

## 中心定制
支持Logo定制
支持模块定制

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

## 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
右键管理
断网修复
网络流量

## 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

## 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

## 系统防御
软件安装拦截
摄像头防护
浏览器保护
应用加固

## HIPS防御系统
系统加固
恶意网址拦截

## 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

## 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

## 环境体系
C/S-B/S架构
Windows全系列
Linux主流系统
Mac操作系统
国产操作系统

# 03 优势介绍

# 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

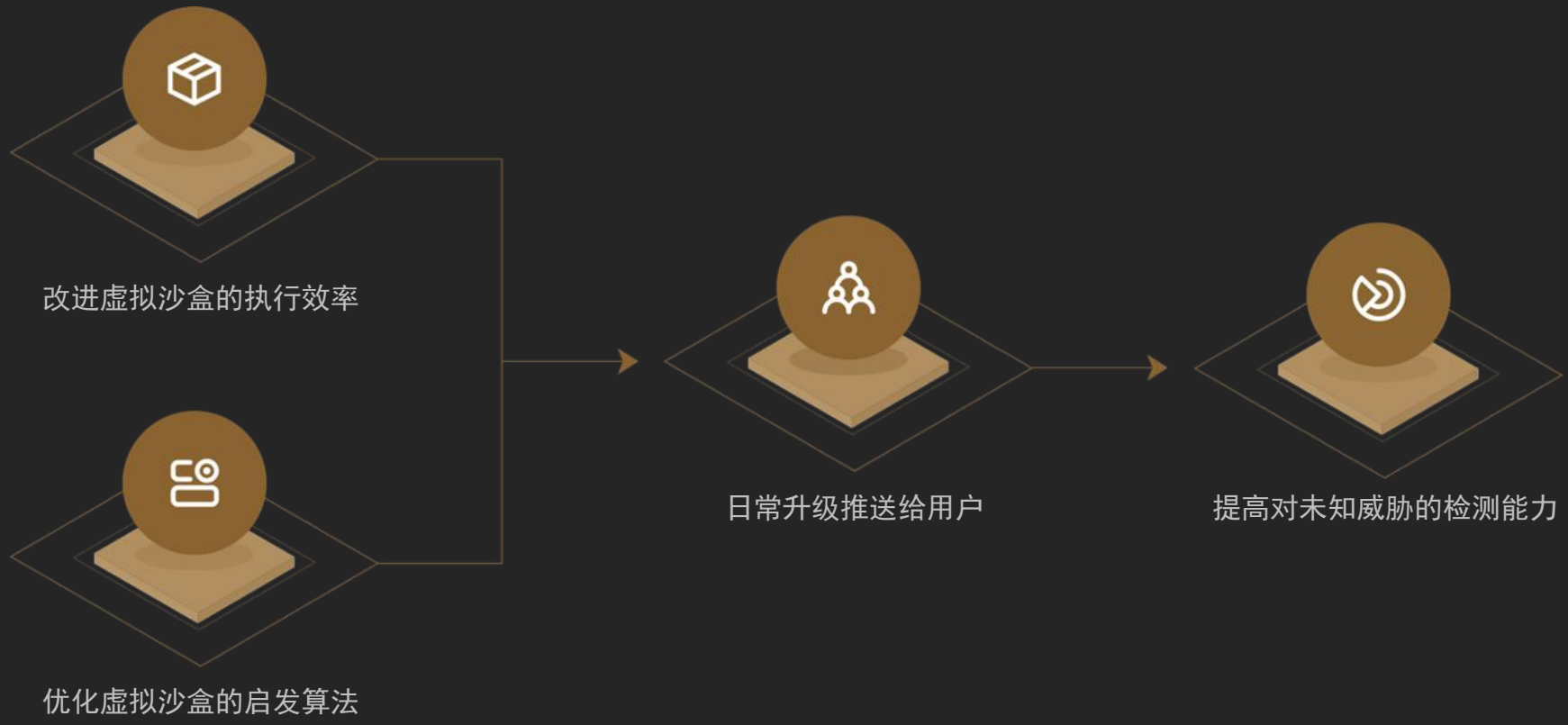
火绒安全研发的“通用脱壳”技术可用于戳穿病毒“伪装”，通过启发式逻辑评估待扫描样本，使其在虚拟环境中还原被保护的代码、数据和行为。因此，对比传统反病毒引擎的静态或动态指导脱壳，火绒安全“通用脱壳”可解决病毒使用的自定义壳、代码混淆器在内的所有其他代码级对抗难题。

### 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。

# 威胁情报

## 海量情报驱动安全

专注、纯粹的终端安全技术公司，深受广大用户企业的认可和信赖。

757,333

当日病毒防御

875,925

当日终端防御

415,995

当日网络防御

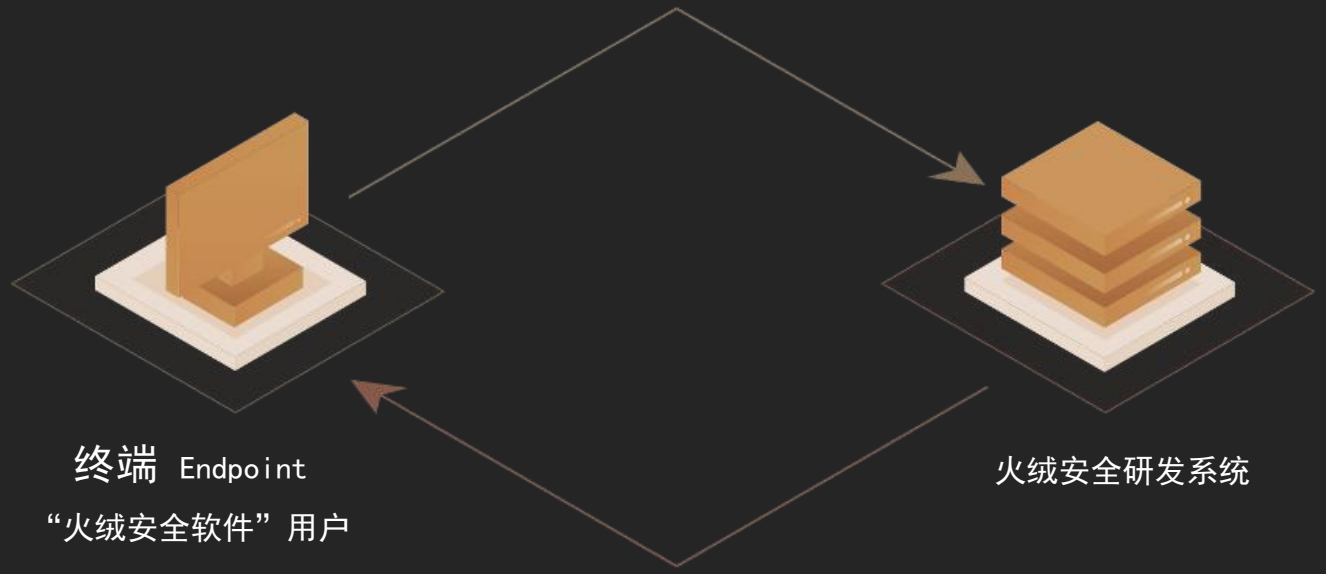
461,885

当日广告弹窗拦截

# 绘制威胁情报系统，执行EDR防护策略

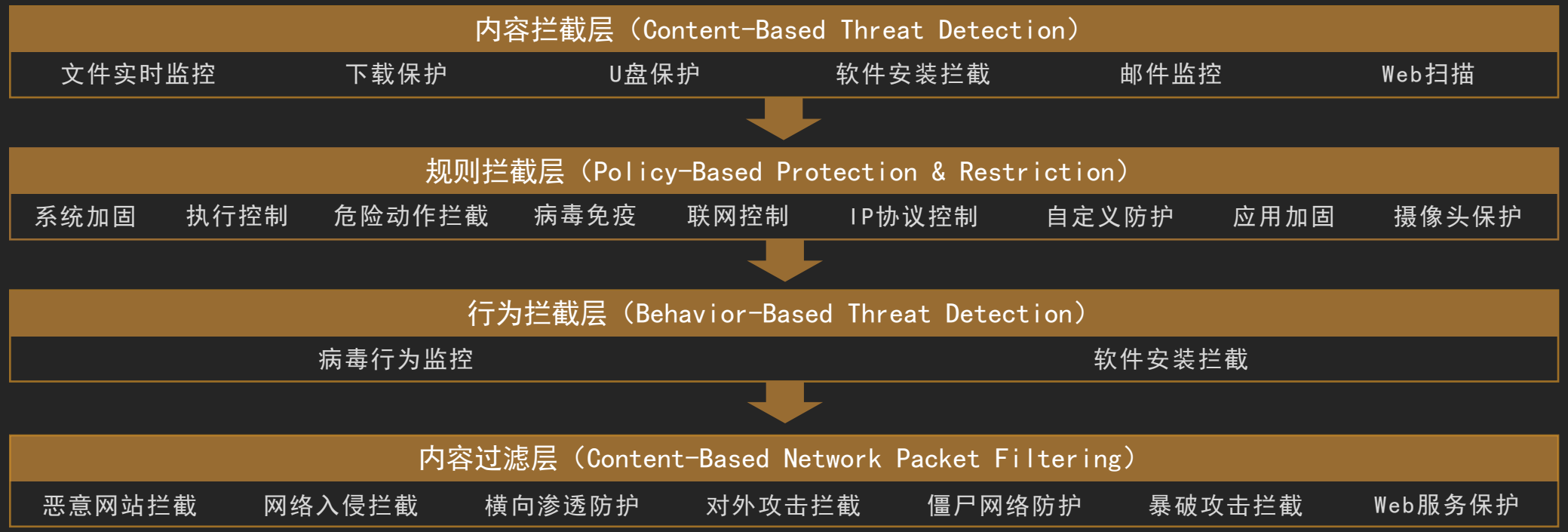
## EDR防护策略

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。



# 多层次主动防御系统

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

# 企业服务分钟级响应

## 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。

企业用户
试用用户
技术合作伙伴

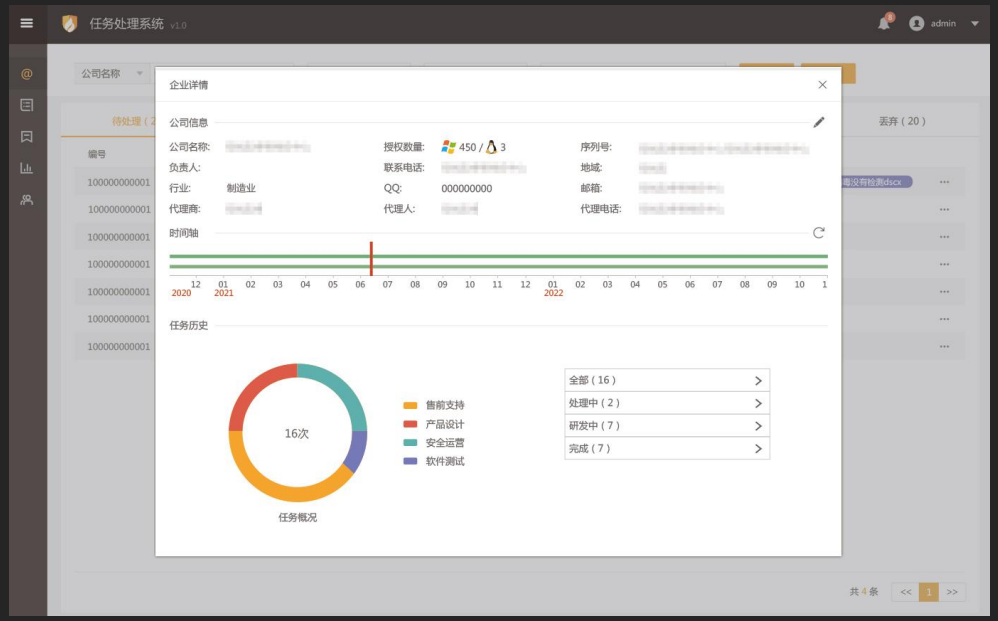
电话、邮件常规渠道
论坛、社群反馈
“在线支持和响应中心”平台

**线上技术支持**
产品咨询与安装、部署指导
应急响应服务与报告提供
安全巡检与安全加固
各类临时需求
全国筛选专业服务商，随时提供上门服务

# 企业服务分钟级响应

## 完善齐全的服务平台

用户服务平台和系统




任务处理系统


在线支持和响应中心

# 04 产品部署

# 火绒企业版2.0系统适配图

## Linux服务器版

支持系统：

- CentOS
- Ubuntu
- SUSE
- 统信UOS
- 银河麒麟
- 中标麒麟
- 中科红旗
- 优麒麟
- 深度
- EulerOS
- 龙芯（Loongnix）等发行版

备注：

- 目前仅支持64位
- x86_64、aarch64、mips64el架构需要GNU libc 2.17及以上版本/loongarch64架构需要GNU libc2.28及以上版本
- 支持Intel / AMD / 飞腾 / 鲲鹏 / 兆芯 / 海光 / 龙芯等CPU

## Linux桌面版

支持系统：

- Ubuntu
- SUSE
- 统信UOS
- 银河麒麟
- 中科红旗
- 优麒麟
- 深度
- 龙芯（Loongnix）等发行版

备注：

- 目前仅支持64位
- x86_64、aarch64、mips64el架构需要GNU libc 2.17及以上版本/loongarch64架构需要GNU libc2.28及以上版本
- 支持Intel / AMD / 飞腾 / 鲲鹏 / 兆芯 / 海光 / 龙芯等CPU

## Windows版

支持系统：

- Windows XP (SP3)
- Windows Vista
- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows 11
- 神州网信 Windows 10

支持CPU：

- Intel
- AMD

## Windows Server版

支持系统：

- Windows Server 2003(SP1)
- Windows Server 2008
- Windows Server 2012
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

支持CPU：

- Intel
- AMD

## macOS系统

支持系统：

- macOS 10.13及以上版本

支持CPU：

- Intel
- M1

# 产品部署架构

全面了解火绒系统的部署架构及端口信息。

火绒服务器（病毒库及组件更新、授权激活）

| 域名 | 端口 |
| --- | --- |
| update.huorong.cn<br>down4.huorong.cn<br>down5.huorong.cn<br>www.huorong.cn | 80、443 |

微软服务器（补丁）

| 域名 | 端口 |
| --- | --- |
| download.windowsupdate.com<br>download.microsoft.com | 80、443 |

如控制中心不能联网，则需要使用离线升级工具完成授权激活及相关更新

**控制中心（服务端）**

| 8080 | 6080 | 5901 | 5500 |
| --- | --- | --- | --- |
| 控制中心管理端口 | 客户端部署/通讯端口 | 中心远程端口 | 终端远程端口 |

tcp双向通信

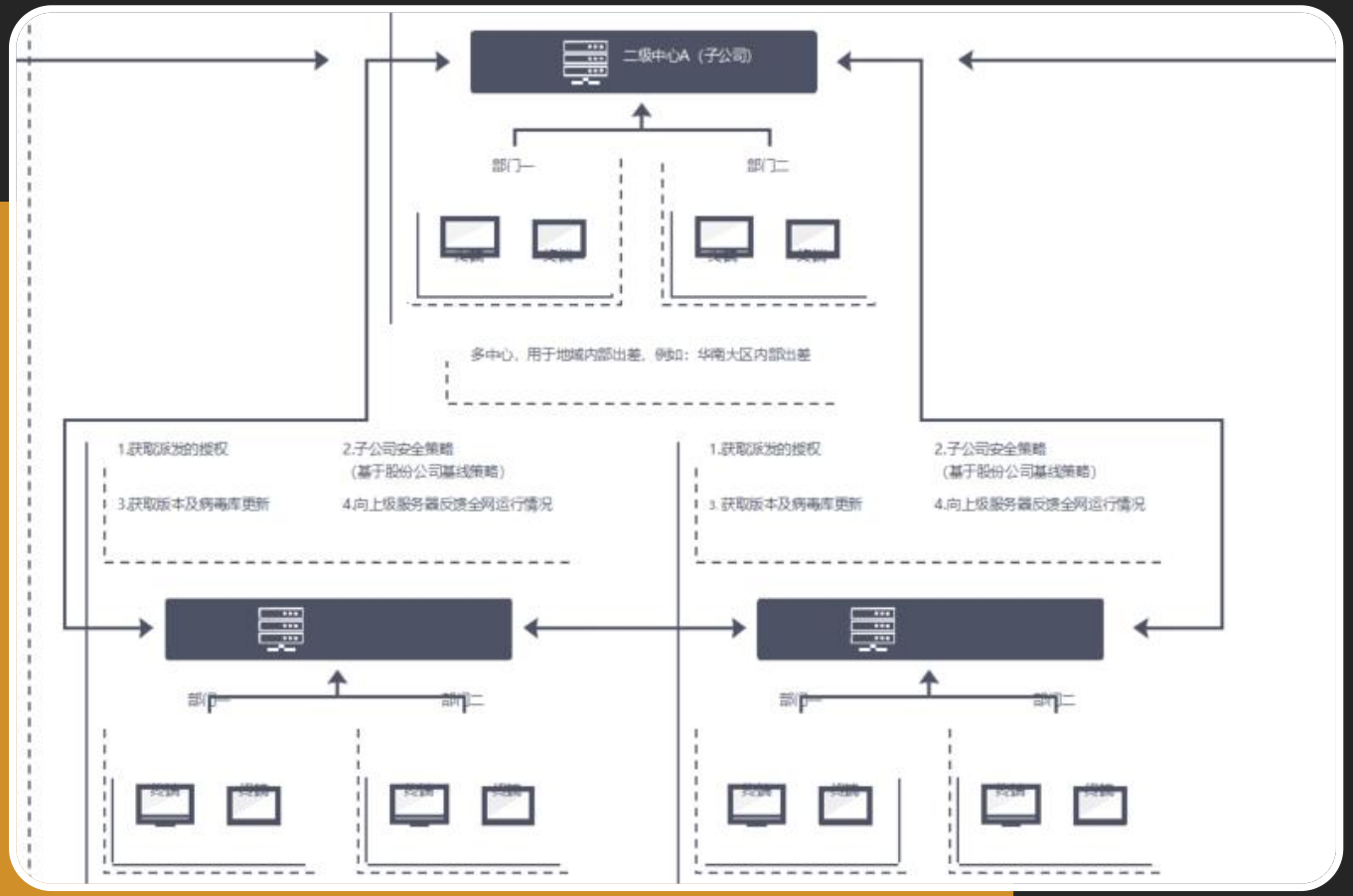
下发IP访问控制　定时全网扫描　清点软硬件资产　下发漏洞修复　桌面管理

客户端　客户端　客户端　客户端(发起远程)　客户端(被远程)

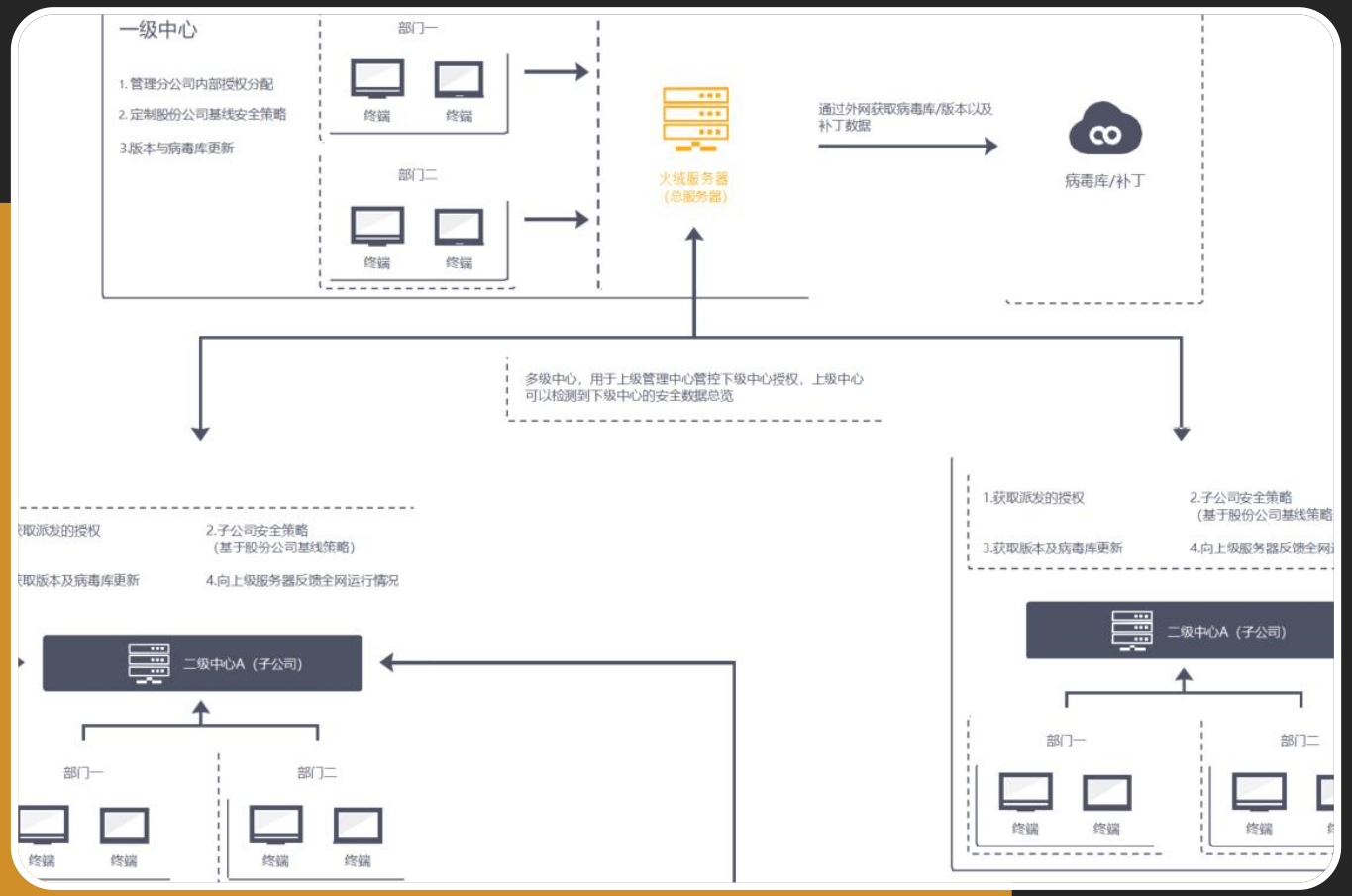
# 多中心部署

## 多中心

对于有分公司的企业，部分员工工作时需要总公司和分公司之间来回处理业务，如果只在总公司安装一个控制中心的话会导致员工去分公司时终端无法统一管控出现安全问题，为了解决这一问题，火绒提供了中心地址管理功能模块，当员工无法连接当前中心时，终端会尝试连接对应的控制中心，以确保后续可以继续被管控。



# 多公司部署



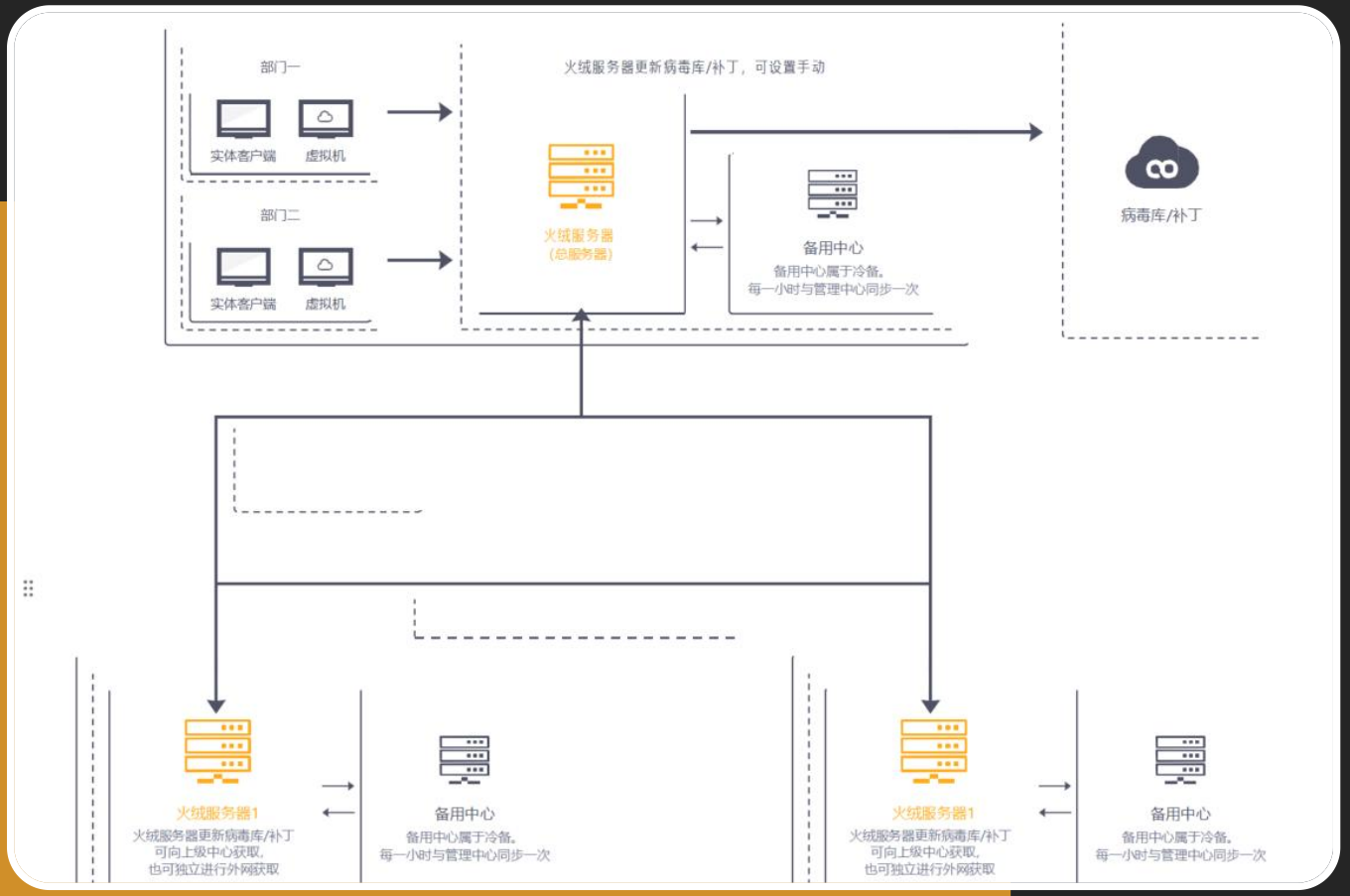

## 多级中心

"多级中心"支持管理员通过上级控制中心管理下级控制中心，可帮助用户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。

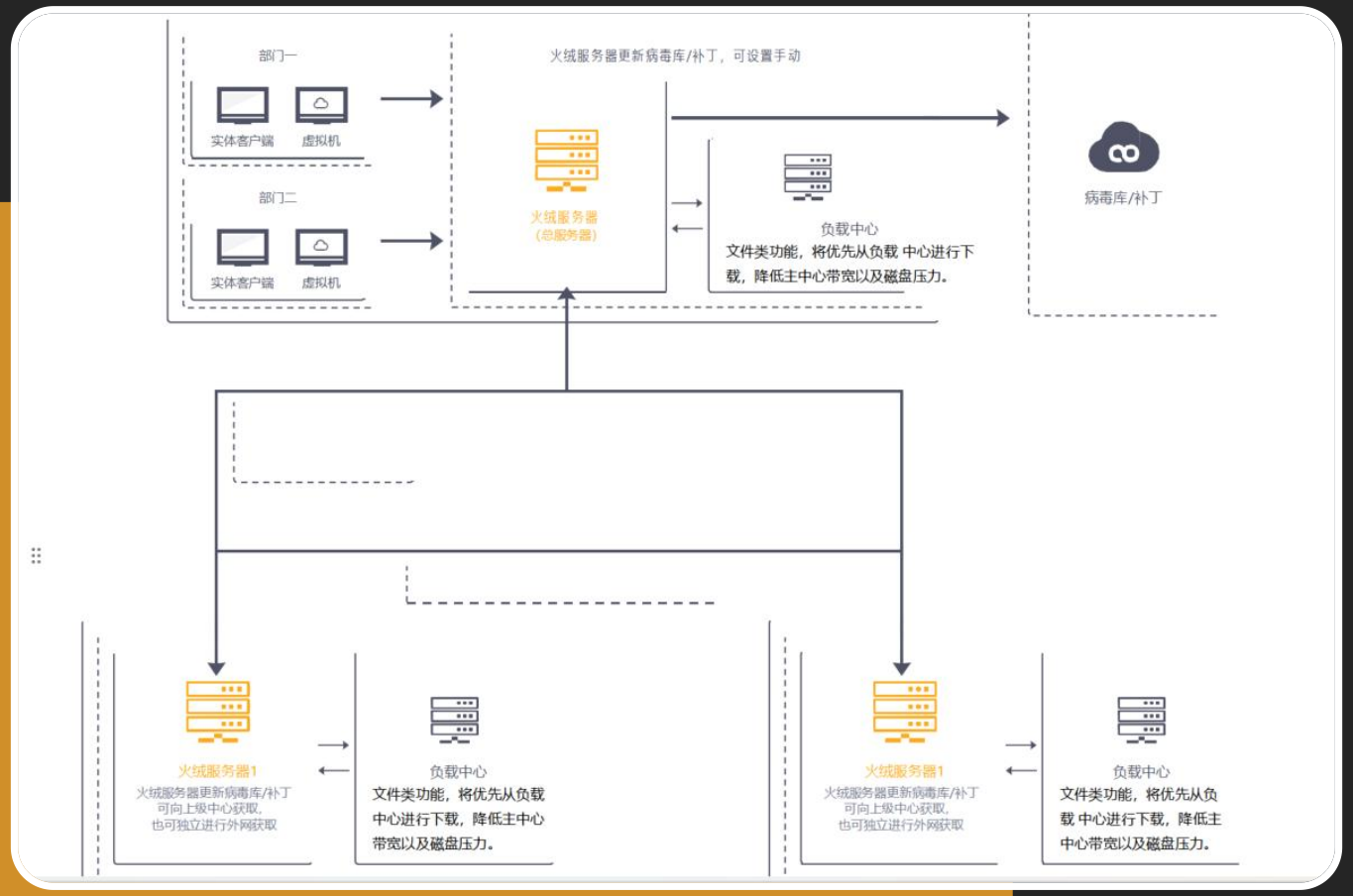
# 公司灾备部署

## 备用中心

中心支持容灾备份功能，当主中心计算机遭受如宕机、断电、硬件/软件故障等意外情况或人为操作错误导致主中心计算机无法正常使用时，备用中心将顶替宕机的主中心且同步数据



# 公司负载部署




## 负载中心

在单一业务中心的环境下，由于单控制中心的处理能力有限，在中型或大型网络环境中，大量的客户端可能会导致整体系统性能下降。部署并完成注册后，文件类功能，如：文件分发、终端升级、补丁文件终端将优先从负载中心进行下载，降低主中心带宽以及磁盘压力。

# 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

扫描二维码　了解更多产品介绍和安全资讯

北京火绒网络科技有限公司
Beijing Huorong Network Technology Co., Ltd.
北京市朝阳区北苑路北京文化创意大厦B座9层
9th Floor, Block B, Beijing Cultural and Creative Building, Beiyuan Road, Chaoyang District, Beijing