火绒安全
Huorong Security

火绒安全

专业终端安全防护

守护个人与企业终端安全，赋能全场景安全防护

专注终端安全 • 守护数字未来

目录

01

公司概况

专注终端安全的核心力量

自2011年成立以来，火绒安全始终专注于终端安全领域
以冷静、艰苦、长期的核心技术研究为立业之本
致力于让用户安全、安静、自由地操作终端

公司概述

成立时间
2011

火绒安全正式成立，从第一天起就专注终端安全领域

专注年限
15+

持续迭代，个人版与企业版产品经历多个关键迭代节点

服务客户
10K+

覆盖政企、医疗、制造、金融、教育、能源等多个领域

产品演进时间轴

2012	2013	2015	2016	2018	2019	2021	2024
个人版 1.0	个人版 2.0	个人版 3.0	个人版 4.0	企业版1.0	个人版 5.0	企业版2.0	个人版6.0

成立背景
致力于为用户提供专业、可靠的安全防护解决方案

发展历程
从个人版1.0到6.0版本，从企业版1.0到V2.0，技术持续升级

服务范围
为上万家客户提供专业的终端安全防护服务

企业文化与核心优势

使命

让用户**安全、安静、自由**地操作终端

价值观

追求本质，以**实现真实安全价值**为唯一目的

立业之本

冷静、艰苦、长期专注核心技术研究

四大核心优势

专注纯粹

15年技术积累，仅通过产品和服务实现盈利，坚持技术为本的商业模式，在终端安全领域提供专业的产品和专注的服务

自主研发引擎

拥有**自主知识产权**的反病毒引擎与多层次主动防御系统，通用脱壳、动态行为查杀、虚拟沙盒三大核心技术

用户至上

提供**专业服务团队**，7×8小时技术支持，快速响应客户需求，定制化解决方案，根据客户业务特点量身定制安全策略

全场景覆盖

从个人版的**轻巧便捷**到企业版的全面管控，满足不同用户群体的终端安全防护需求，适配多行业专属需求

主营业务布局：四大业务板块协同发展

个人终端安全产品

面向个人用户提供终端防护解决方案，核心功能涵盖病毒查杀、系统防护、网络防护、访问控制及实用安全工具

火绒安全软件 6.0 干净 · 轻巧 · 强大

核心技术对外赋能

拥有自主知识产权的反病毒引擎与多层次主动防御系统，持续对外赋能，助力拓展安全防护领域

OEM合作 技术共享 · 生态共建

企业终端安全产品

全方位纵深防御与终端统一管控方案，功能集成病毒查杀、终端管理、漏洞修复、资产管理、外设管控等

火绒终端安全管理系统 V2.0 集中管控 · 多平台兼容

威胁情报服务

构建火绒威胁情报系统，具备"能发现、能应用、能处理"的核心能力，实现实时响应与动态防御

威胁情报系统 精准处理 · 动态防御

四大业务板块协同发展

构建完整的终端安全防护生态体系

02

核心产品矩阵

个人与企业专属安全方案

从个人版的轻巧便捷到企业版的全面管控
火绒安全提供差异化的产品解决方案
满足不同用户群体的终端安全防护需求

个人终端安全产品

火绒安全软件 6.0

核心特点

- 干净
- 轻巧
- 强大

增值服务

火绒应用商店

提供**一站式管理体验**，用户可便捷下载、安装、更新各类应用程序，所有应用均经过安全检测，杜绝捆绑软件和恶意插件，让软件管理更安全、更高效、更省心

核心功能

病毒查杀

快速扫描、全盘扫描、自定义扫描，全面检测清除病毒木马

系统防护

实时监控文件、注册表、进程等系统关键位置，阻止恶意操作

网络防护

拦截恶意网址、钓鱼网站、网络入侵，保护上网安全

访问控制

U盘保护、摄像头防护、程序执行控制，严格管控权限

实用安全工具

垃圾清理、启动项管理、服务管理、hosts文件保护多款实用工具

设计理念

个人版产品专注于**个人防护便捷性**，追求无广告、无弹窗、无捆绑的纯净体验。通过轻量化设计确保系统运行流畅，同时提供强大的安全防护能力，让每一位个人用户都能享受到专业级别的终端安全保护

企业终端安全产品：火绒终端安全管理系统 V2.0

全方位纵深防御

构建**多层次、立体化**的安全防护体系，从网络边界到终端设备，从文件扫描到行为监控，实现360度无死角安全防护。结合主动防御与被动查杀，确保企业终端在任何场景下都能获得全面保护

终端统一管控

通过**中心化管控平台**，实现数千甚至数万台终端设备的集中管理。管理员可统一配置安全策略、批量部署任务、实时监控终端状态，大幅提升安全管理效率，降低企业运维成本

核心功能矩阵

病毒查杀
本地引擎扫描

终端管理
集中管控

漏洞修复
系统加固

资产管理
硬件软件统计

外设管控
设备权限控制

行业定制

适配**物流、医疗、金融、制造**等行业专属需求，提供定制化安全解决方案

规模化部署

支持**中心+客户端**架构，适配Windows、Linux等多系统平台

集中管控

统一策略配置、批量任务部署、实时监控告警，提升管理效率

个人版 vs 企业版 · 差异对比

面向群体

个人版

家庭用户、小型个人工作室，单终端或少量终端使用场景

企业版

中大型企业、机构，大规模内网终端集中防护与管理需求

核心优势

个人版

轻量化、易操作，满足个人单机安全防护需求

企业版

集中管控、多平台兼容、功能丰富，适配企业级规模化管理场景

部署方式

个人版

仅支持Windows系统，单终端安装客户端

企业版

支持Windows/macOS/Linux多系统，采用"管理中心+客户端"架构，支持内网离线部署

功能特性差异

个人版

基础安全防护 + 部分个性化工具功能

- 病毒查杀、系统防护、网络防护
- 访问控制、实用安全工具
- 火绒应用商店一站式管理

企业版

覆盖个人版核心防护能力，新增企业级专属管理功能

- 终端概况/安全风险/资产信息集中展示
- 远程桌面/终端隔离/文件分发
- 漏洞批量修复/软件黑白名单管控
- 违规外联检测/分组管理/LDAP对接

03

网络安全威胁全景

病毒、攻击与潜在隐患

从病毒木马到网络攻击，从内部管理到外部威胁
全面剖析当前网络安全面临的严峻挑战
揭示企业终端安全防护的关键痛点

常见病毒类型

常见病毒类型及危害

挖矿病毒 高发

占用CPU/GPU资源挖掘加密货币，导致**系统卡顿、电费激增、硬件损耗**

感染型病毒 顽固

感染可执行文件和系统组件，导致**系统崩溃、程序无法运行、网络瘫痪**

勒索病毒 高危

加密重要文件索要赎金，造成**数据无法恢复、业务中断、巨额经济损失**

银狐病毒 活跃

通过**钓鱼邮件传播，窃取敏感信息、远程控制**

核心危害

现代网络攻击采用多技术组合形成攻击链，侦察→入侵→横向移动→数据窃取，具有隐蔽性强、破坏力大、持续时间长的特点，传统单点防护难以有效应对

常见病毒类型及典型攻击手段

典型网络攻击手段解析

恶意软件攻击

恶意软件又称“流氓软件”，指在未明确提示用户或未经用户许可的情况下，在用户计算机或其他终端上安装运行

暴破攻击

针对于密码的破译方法，将密码进行逐个推算直到找出真正的密码

钓鱼攻击

伪造可信机构邮件、网站，诱骗用户泄露**账号密码、银行卡信息、验证码**

僵尸网络

将大量主机感染bot程序（僵尸程序）病毒，从而在控制者和被感染主机之间所形成的一个可一对多控制的网络

攻击特征

现代网络攻击采用**多技术组合形成攻击链**，侦察→入侵→横向移动→数据窃取，具有**隐蔽性强、破坏力大、持续时间长**的特点，传统单点防护难以有效应对

企业环境核心安全隐患与威胁态势

企业环境三大核心安全隐患

内部管理隐患

- **人员安全意识薄弱**：缺乏安全培训，易中招钓鱼攻击
- **权限管控混乱**：多人共用账号，离职未注销

技术防护隐患

- **边界设备防护不足**：防火墙规则配置宽松
- **终端体系庞大难管控**：设备数量多，缺乏统一管理

威胁态势洞察

终端攻击趋势

木马病毒	占比最高
勒索病毒	破坏性强
挖矿病毒	持续高发

重点威胁：银狐病毒、LummaStealer病毒持续活跃，通过钓鱼邮件、恶意链接传播

漏洞风险态势

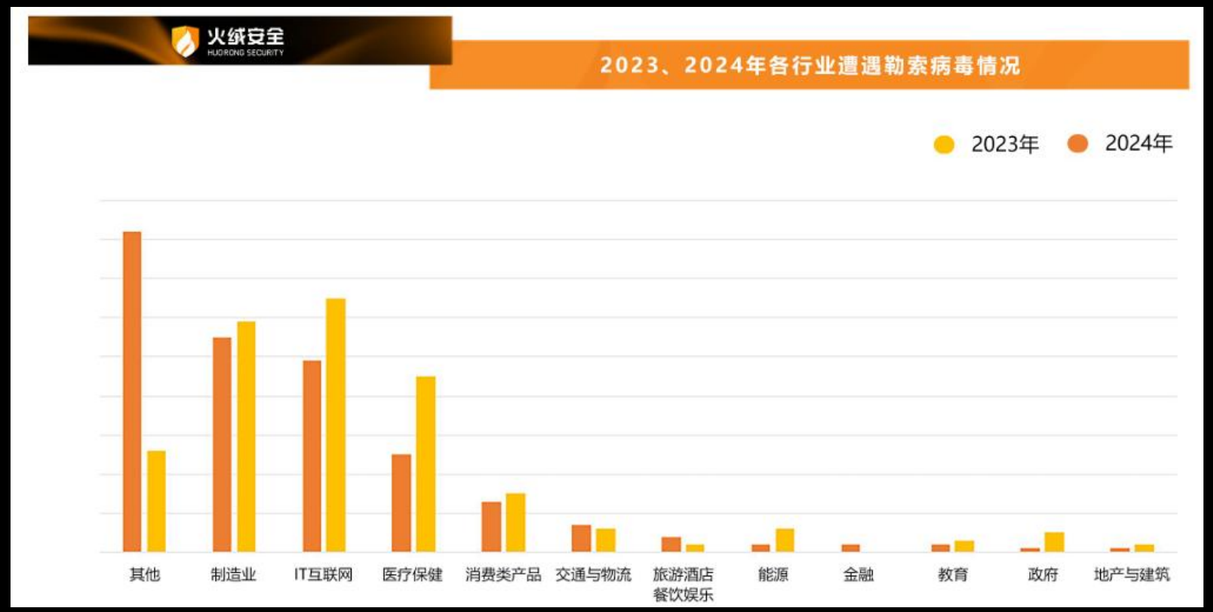
系统漏洞

系统漏洞被频繁利用，**及时补丁更新**至关重要

攻击趋势：漏洞利用工具包泛滥，攻击者通过自动化工具批量扫描、攻击目标系统

威胁态势洞察与真实案例

威胁态势数据



真实威胁事件案例

企业核心系统入侵

某某车辆公司遭遇网络攻击，被迫关闭全球IT基础设施，暂停部分工厂生产

内部人员与权限滥用

某某银行盗窃案：黑客以920美元贿赂IT员工获取企业凭证，盗走1.4亿美元

定向攻击与数据窃取

境外组织利用弱密码入侵多所中学广播系统，企图篡改内容传播有害信息

勒索软件关联

某某开发商遭勒索攻击，超1万用户个人信息泄露

安全启示

从个人用户到大型企业，从内部管理到外部攻击，安全威胁无处不在。只有建立**全面的安全防护体系**，提升安全意识，才能有效应对日益复杂的网络安全挑战

04

技术防护

技术、功能与策略保障

火绒核心防护技术

自主研发反病毒引擎三大核心技术

通用脱壳

深度解析**加壳、混淆、加密**的恶意代码，还原病毒真实面目，确保查杀无遗漏

动态行为查杀

基于**病毒行为特征**进行检测，即使病毒变种也能精准识别，有效应对未知威胁

虚拟沙盒

在**隔离环境**中运行可疑程序，分析其行为逻辑，判断是否为恶意软件

高查杀率

低误报率

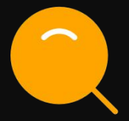
断网可用

不损文件

火绒EDR体系

体系基石 · 终端

以数千万“火绒安全软件”终端为基石，是数据采集源与策略执行者。



智能感知 · 检测

实时防护并初步分析各类威胁，精准识别已知和未知风险。

协同处置 · 响应

专家深度分析，将解决方案快速下发至所有终端，形成闭环。

构建“终端-检测-响应”的动态闭环，持续保护用户安全

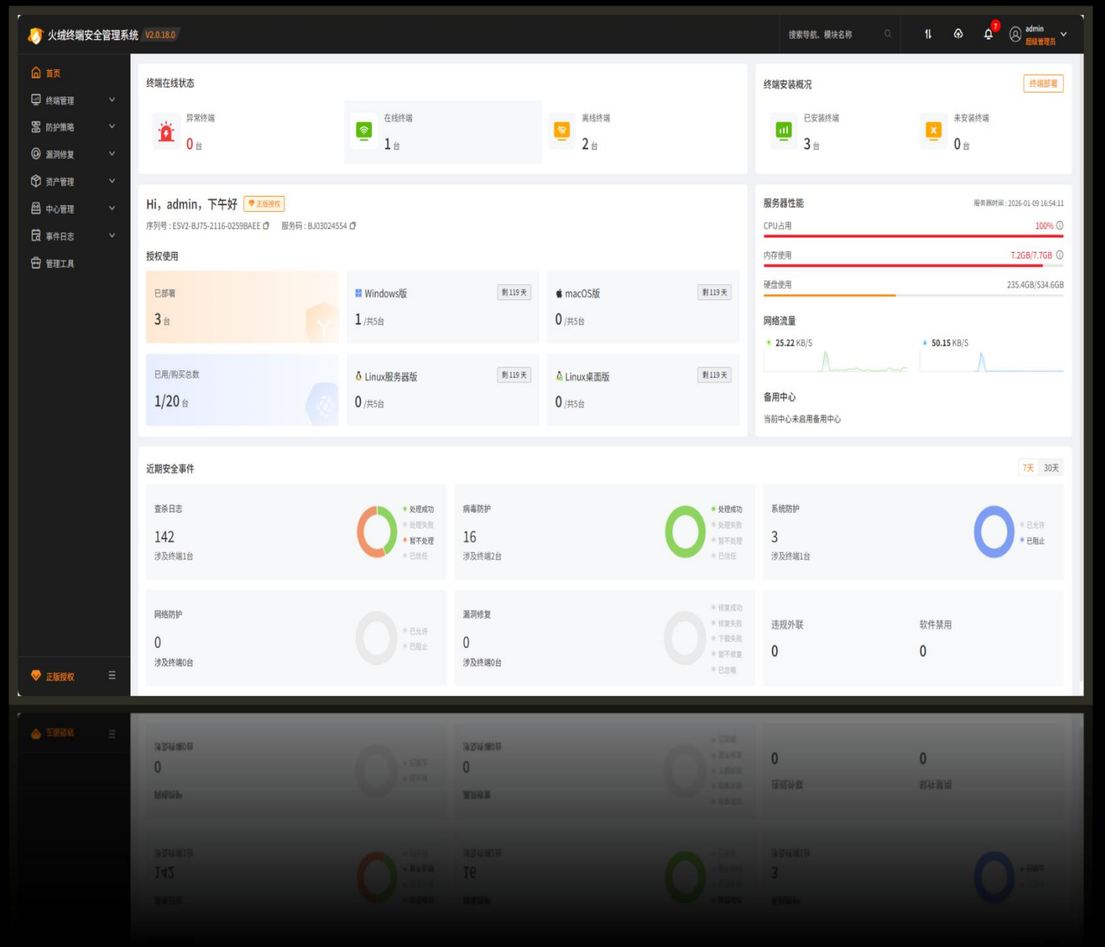
企业版本功能-可视化控制中心

可视化控制中心

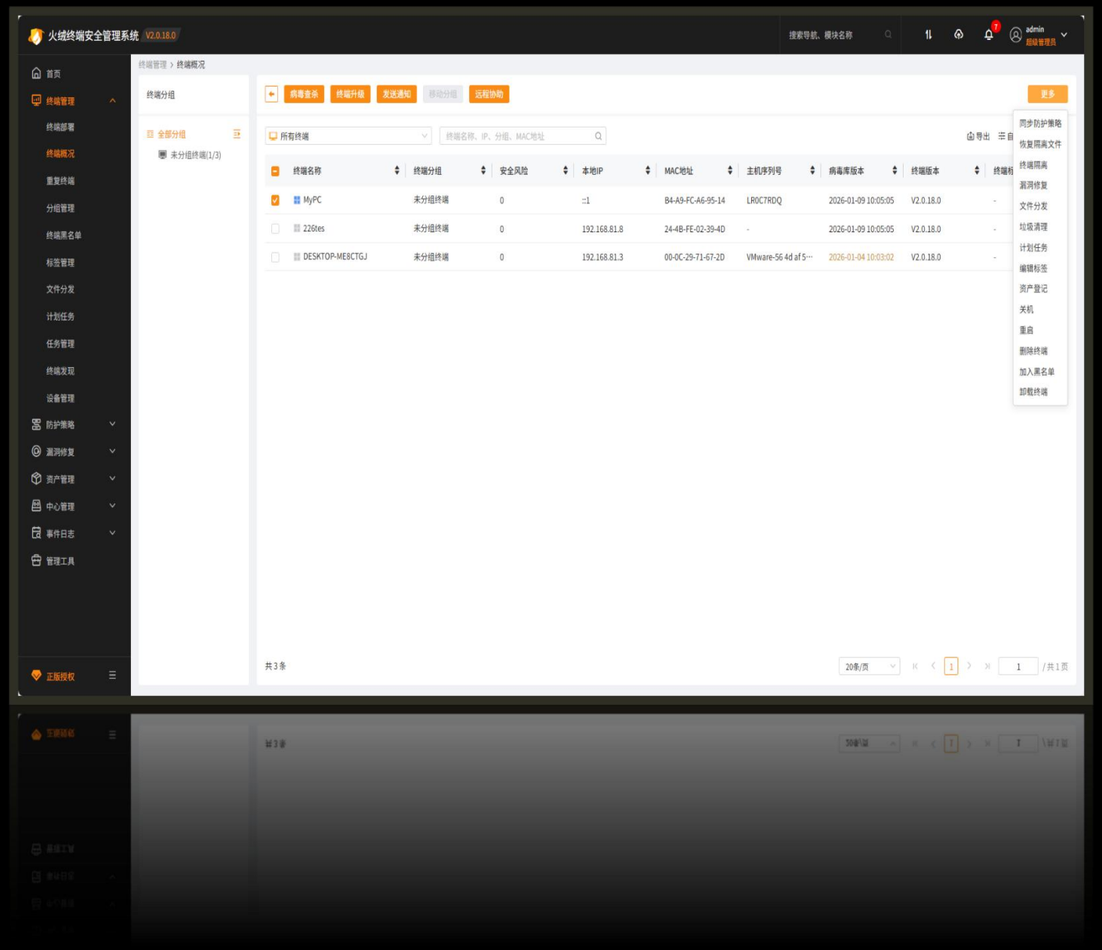
直观呈现各类安全信息，反映服务器性能，方便管理员快速及时地掌握企业的安全全貌。

核心展示模块

终端状态:在线/离线终端数量及占比。
安装概况:终端安装覆盖率统计。
安全事件:近7天及30天内各防护模块事件数量及处理情况。
服务器性能:实时监控服务器运行状态。



企业版本功能-终端管理



终端全生命周期管理

核心功能概览

提供全面的终端全生命周期管理，帮助管理员实现终端的统一部署、管控、维护与监控，确保企业终端安全与合规。

子功能模块

- **终端部署**：支持自助安装、安装包安装、域部署三种方式。
- **终端概况**：可执行病毒查杀、终端升级、远程协助等操作，并支持筛选、导出、搜索。
- **终端详情**：查看终端多类信息并支持相关操作下发。
- **高级管理**：重复终端处理、分组管理 (含组织架构同步)、终端黑名单、标签管理。
- **任务与分发**：文件分发、计划任务。
- **设备发现与管理**：终端发现、设备管理 (设备申请审批、信任设备管理)。

企业版本功能-防护策略

核心功能概览

支持自定义安全策略配置，帮助企业构建多层次、可定制的终端安全防护体系。

子功能模块

策略管理

策略部署、分组策略、终端策略

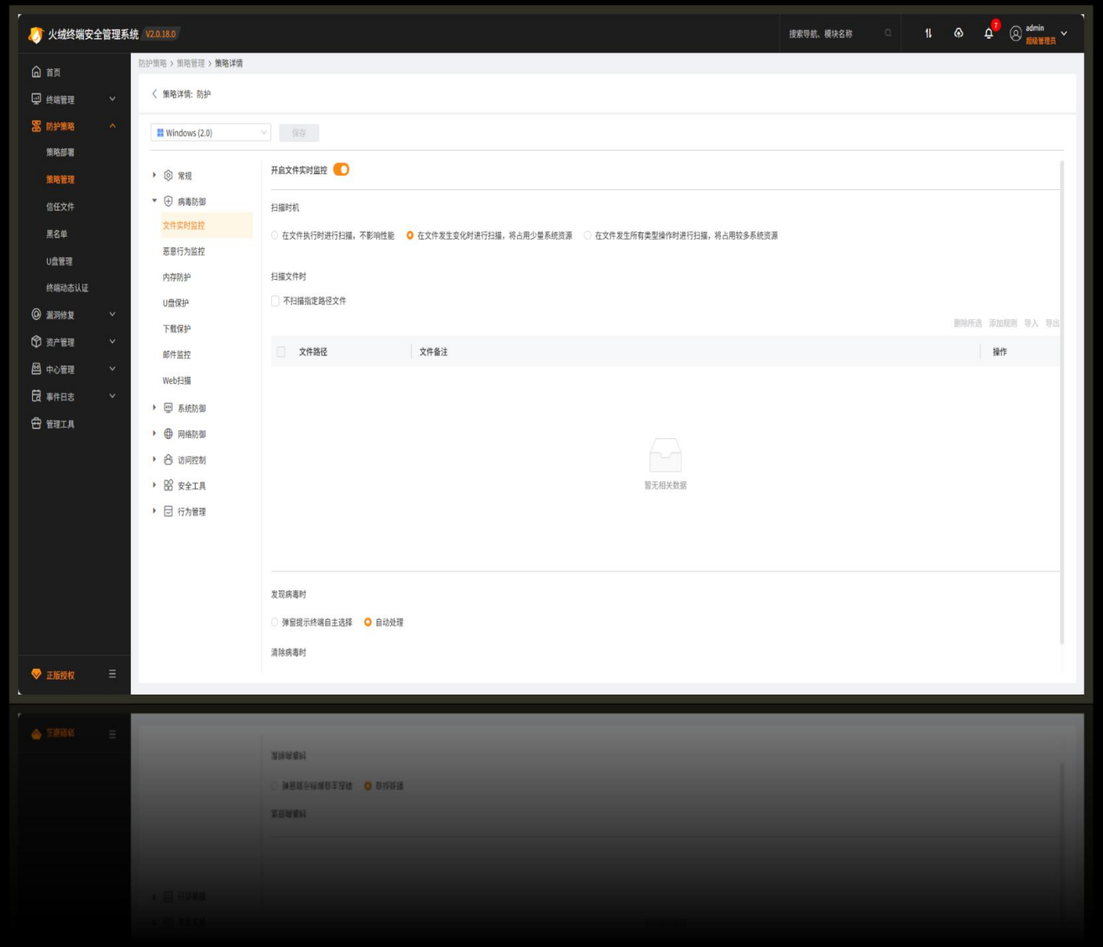
安全管控

信任文件、黑名单、U盘管理、动态认证

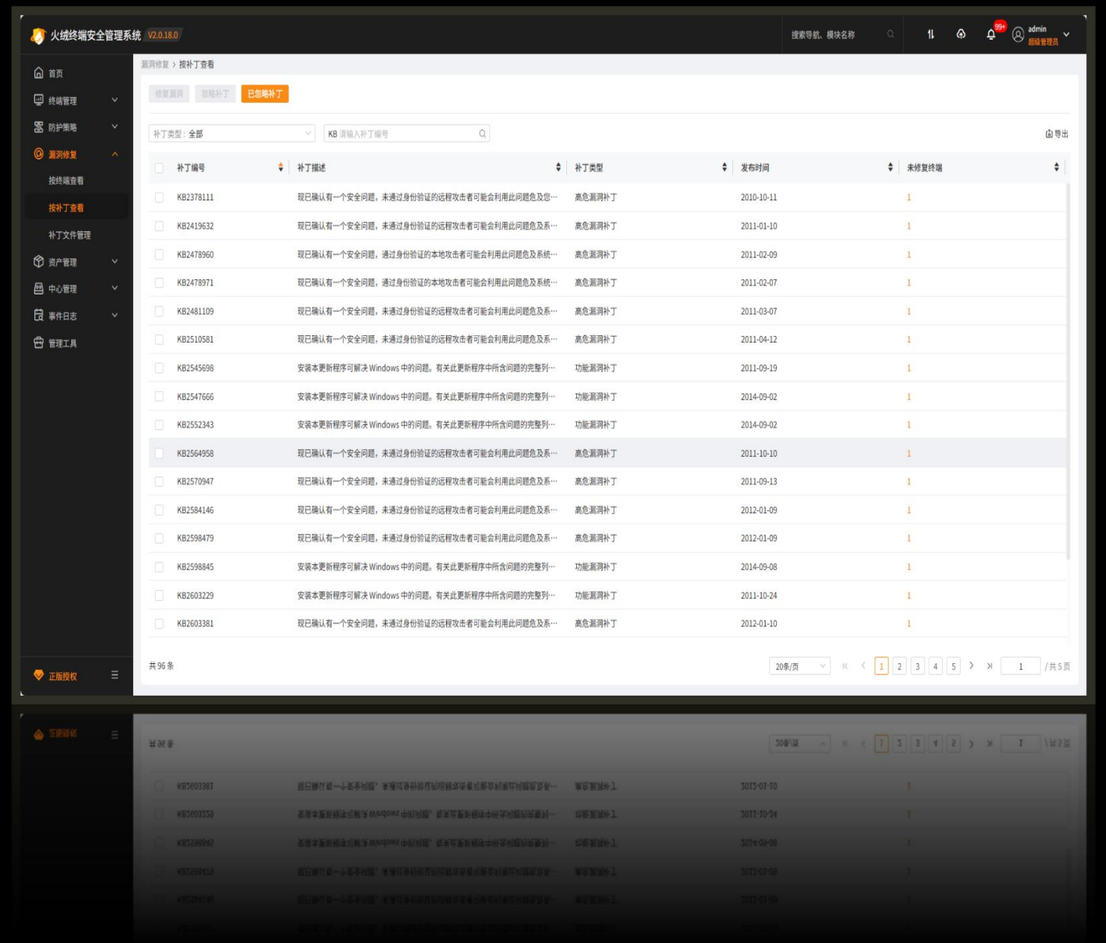
六大防护区域

病毒防御　　系统防御　　网络防御

访问控制　　行为管理



企业版本功能-漏洞修复



漏洞修复

精准操作

根据终端名称、分组、IP选择特定终端修复。

清晰概览

终端状态、漏洞分类一目了然。

高效检索

支持按补丁类型或编号快速查询。

补丁文件管理

集中缓存

补丁缓存在中心服务器，提升分发效率。

分发共享

客户端从中心获取，节省网络带宽。

企业版本功能-资产管理

资产管理

资产登记

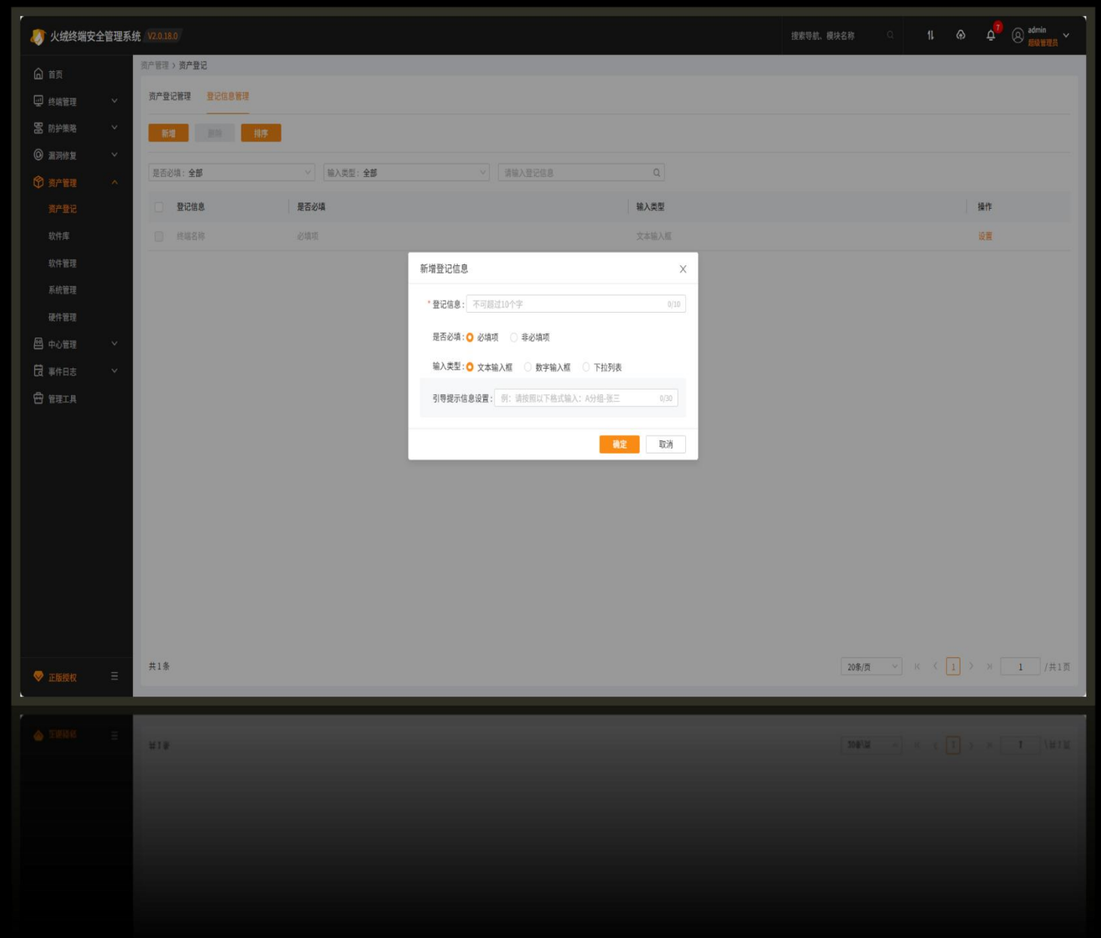
提供简约高效的登记流程，支持自定义字段、设置必填项，满足企业个性化需求。

软硬件系统管理

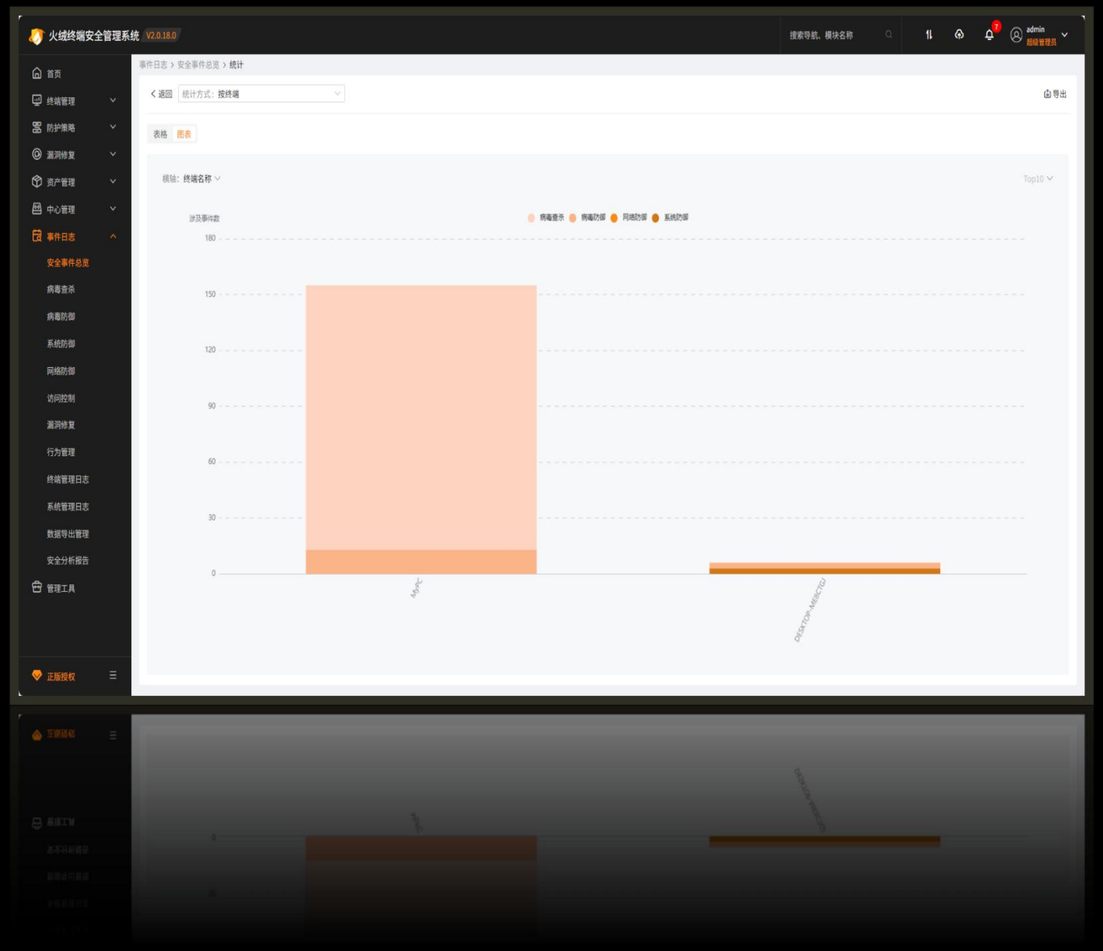
详细记录资产变更，辅助运维管理与财务审计，确保资产信息准确可追溯。

软件库

管理本地与云软件库，联动策略限制下载，构建企业私有应用商店。



企业版本功能-日志报表



日志管理

- **全面记录：**记录终端病毒查杀、防御、漏洞修复等所有安全操作日志。
- **报表导出：**直观展现并导出各类日志报表，满足审计与合规要求。

安全分析报告

- **智能汇总：**自动对防护日志、风险详情等内容进行汇总分析。
- **专业建议：**提供详细分析结果与处理建议，持续提升企业安全水位。

企业版本功能-产品联动

产品联动

开放API接口

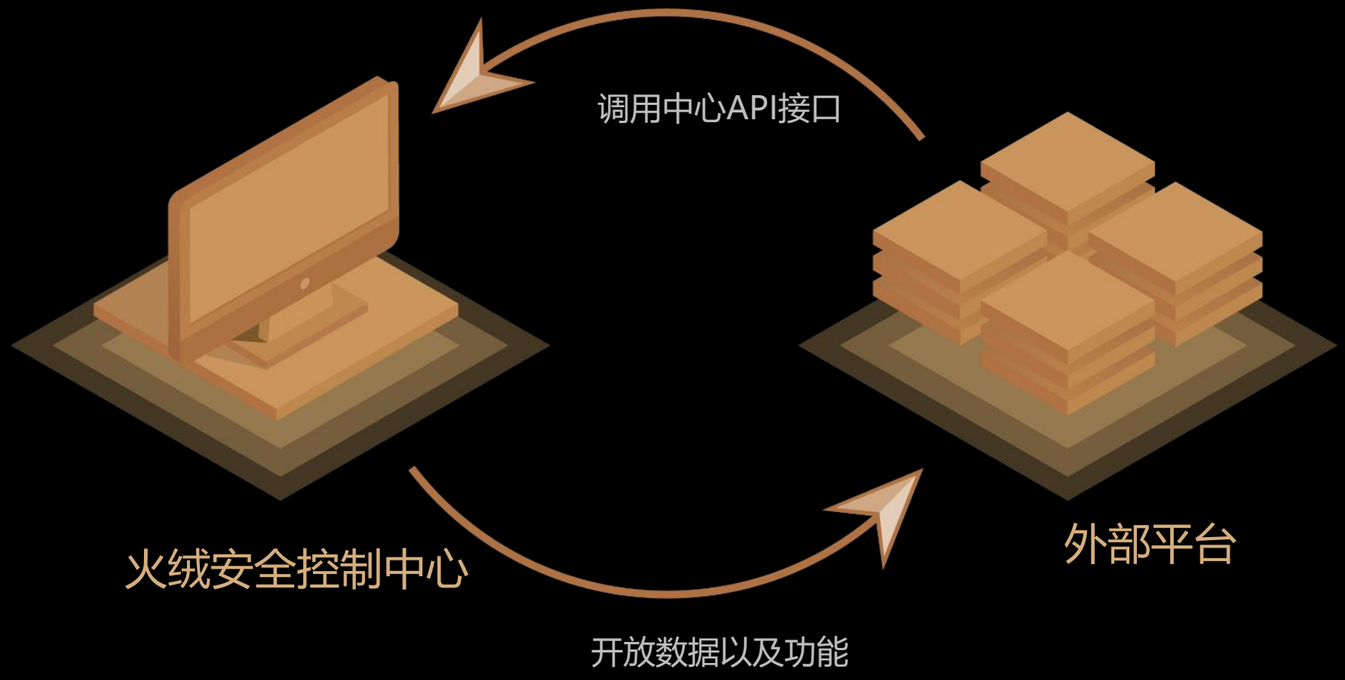
与准入系统等产品灵活联动，打破信息孤岛，构建一体化安全生态。

丰富的查询信息

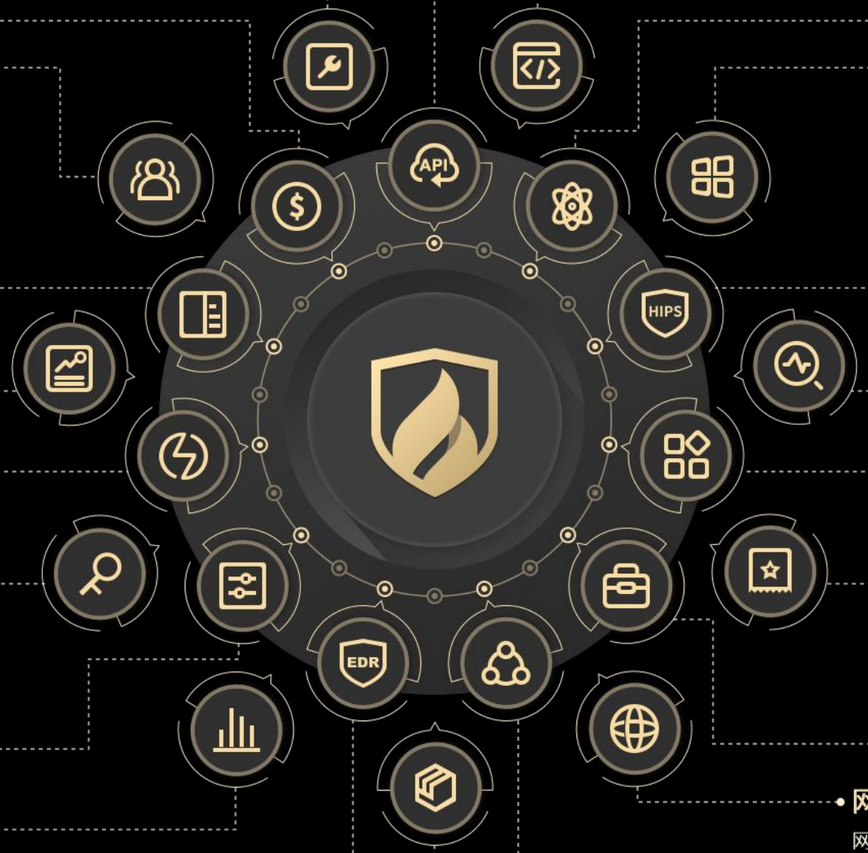
- 终端地址与名称
- 终端版本信息
- 分组策略配置
- 终端在线状态
- 病毒库版本

持续的功能扩展

持续开放更多联动能力，满足企业日益增长的集成需求。



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

API接口

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

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

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

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

全员安全意识提升与账号权限规范化管理

全员安全意识提升

基础安全普及

病毒识别能力

识别**钓鱼邮件、恶意链接、可疑附件**，不随意下载未知来源文件

三不原则

不点击、不下载、不转发可疑内容，第一时间报告IT部门

高风险岗位专项教育

- **财务岗位**：识别冒充领导诈骗、资金转账核实流程
- **IT岗位**：漏洞识别、应急响应、安全配置规范
- **采购岗位**：供应商邮件验证、支付账户确认流程

账号与权限规范化管理

账号生命周期管控

- **一人一号**：禁止账号共享，确保操作可追溯
- **实名绑定**：账号与真实身份关联，责任到人
- **离职注销**：员工离职时立即禁用账号，防止权限滥用

权限最小化原则

- **按需授权**：根据岗位需求分配最小必要权限
- **第三方权限严格限制**：外部人员权限定期审查

多因素认证（MFA）

对**核心系统强制启用MFA**，即使密码泄露，攻击者也难以登录。支持短信验证码、动态令牌、生物识别等多种认证方式，大幅提升账号安全性

外部文件安全管理与场景化培训演练

外部文件与邮件安全管理

邮件过滤与审核

部署**企业级邮件网关**，拦截恶意附件、钓鱼链接、垃圾邮件。对包含可执行文件、宏文档的邮件进行隔离审核，确保邮件安全

外部文件扫描

强制安全检测后再使用U盘、移动硬盘等外部存储设备。建立文件扫描流程，所有外部文件必须经过杀毒检测，确保安全后方可使用

软件下载管控

搭建**官方软件库**，提供经安全检测的正版软件。禁止从第三方网站下载软件，杜绝捆绑软件、恶意插件风险

场景化培训与演练

模拟攻击演练

钓鱼邮件演练
定期发送模拟钓鱼邮件，测试员工识别能力，对点击用户提供针对性培训

弱口令暴破演练
模拟黑客暴破攻击，检测弱口令账号，强制用户修改高强度密码

案例化培训

结合**真实安全事件案例**进行深度剖析，让员工了解攻击手法、危害后果、防范措施。通过身边案例强化安全意识，提升培训效果

考核与监督闭环

安全意识纳入绩效

- 基础知识测试
- 演练表现评估
- 安全事件考核

反馈机制

- 安全举报通道
- 定期复盘优化

05

成功案例

实力见证与行业认可

从互联网巨头到政府机构

从金融机构到能源企业

火绒安全凭借专业技术与优质服务赢得广泛信赖

跨行业客户覆盖与技术合作生态

商业用户案例

- **京东金融** - 金融科技
- **拼多多** - 电商平台
- **唯品会** - 品牌特卖
- **桂林银行** - 金融机构

为大型互联网企业和金融机构提供终端安全防护与管控解决方案，保障核心业务系统稳定运行

政企事业单位

- **北京医院** - 医疗机构
- **浙江大学** - 教育机构
- **中国铁建** - 交通基建
- **国家电网** - 能源企业

覆盖政府、教育、医疗、交通、能源等关键基础设施领域，为国家级机构提供高安全级别的终端防护

技术合作生态

- **Lenovo** - 硬件厂商
- **Microsoft** - 操作系统
- **启明星辰** - 安全厂商
- **天融信** - 网络安全

核心技术对外赋能，与行业领先企业建立OEM合作关系，共筑行业安全防线，实现互利共赢

客户价值

火绒安全凭借**专业技术、优质服务和定制化解决方案**，赢得了众多行业领先客户的信赖。从互联网巨头到政府机构，从金融机构到能源企业，火绒安全为不同行业的客户提供量身定制的终端安全防护方案，保障核心业务系统稳定运行，确保用户数据和业务连续性

06

总结与展望

构建更全面的终端安全防护生态

立足技术优势，深化产品服务
拓展生态合作，升级安全价值
持续守护数字时代的终端安全

核心优势与未来发展方向

核心优势总结

技术优势

- **自主研发反病毒引擎**，通用脱壳、动态行为查杀、虚拟沙盒三大核心技术
- **主动防御系统**，四层纵深防护功能矩阵，全方位拦截威胁
- **持续技术迭代**，13年专注终端安全领域，紧跟威胁演进

产品优势

- **全场景覆盖**，个人版与企业版产品满足不同用户需求
- **功能全面且精准**，病毒查杀、系统防护、网络防护、资产管理等
- **行业定制能力**，适配物流、医疗、金融等行业专属需求

服务优势

- **专业服务团队**，7×8小时技术支持，快速响应客户需求
- **定制化解决方案**，根据客户业务特点量身定制安全策略
- **持续赋能客户**，安全培训、威胁情报、最佳实践分享

未来展望

技术迭代

持续深耕**反病毒引擎与主动防御**核心技术，引入AI/ML技术提升威胁检测能力，应对AI驱动的新型网络威胁，保持技术领先优势

生态拓展

深化**行业合作**，扩大技术赋能范围，与更多安全厂商、硬件厂商、系统集成商建立OEM合作关系，共筑产业安全生态

价值升级

从**终端安全**向**全场景安全防护**演进，构建覆盖云、管、端的立体化安全防护体系，守护数字时代的用户安全

使命愿景

继续践行**"让用户安全、安静、自由地操作终端"**的使命，坚持核心技术自主研发，以更专业的产品、更优质的服务，为个人和企业用户提供全方位的终端安全防护，守护数字时代的安全底线

火绒安全
Huorong Security

火绒安全

让终端安全更简单、更可靠

官方网站
www.huorong.cn

客服热线
400-998-3555