火絨安全
Huorong Security

AL-Touch
@the reliable IT Solutions

火絨安全

專業終端安全防護

專注終端安全·守護數位未來

守護個人與企業終端安全，賦能全場景安全防護

香港區代理

AL-TOUCH SOLUTIONS LIMITED 一大方案有限公司

https://www.al-touch.com.hk

目錄

01

公司概況

專注終端安全的覈心力量

自2011年成立以來，火絨安全始終專注於終端安全領域
以冷靜、艱苦、長期的核心技術研究為立業之本
致力於讓用戶安全、安靜、自由地操作終端

公司概述

成立時間
2011

火絨安全正式成立，從第一天起就專注終端安全領域

專注年限
15+

持續反覆運算，個人版與企業版產品經歷多個關鍵反覆運算節點

服務客戶
10K+

覆蓋政企、醫療、製造、金融、教育、能源等多個領域

產品演進時間軸

- **2012** 個人版1.0
- **2013** 個人版 2.0
- **2015** 個人版 3.0
- **2016** 個人版 4.0
- **2018** 企業版1.0
- **2019** 個人版 5.0
- **2021** 企業版2.0
- **2024** 個人版6.0

成立背景
致力於為用戶提供專業、可靠的安全防護解決方案

發展歷程
從個人版1.0到6.0版本，從企業版1.0到V2.0，科技持續陞級

服務範圍
為上萬家客戶提供專業的終端安全防護服務

企業文化與覈心優勢

使命

讓用戶**安全、安靜、自由**地操作終端

價值觀

追求本質，以實現真實安全價值為唯一目的

立業之本

冷靜、艱苦、長期專注核心技術研究

四大覈心優勢

專注純粹

15年科技積累，僅通過產品和服務實現盈利，堅持科技為本的商業模式，在終端安全領域提供專業的產品和專注的服務

自主研發引擎

擁有自主知識產權的反病毒引擎與多層次主動防禦系統，通用脫殼、動態行為查殺、虛擬沙箱三大核心技術

用戶至上

提供專業服務團隊，7×8小時技術支援，快速回應客戶需求，定製化解決方案，根據客戶業務特點量身定製安全性原則

全場景覆蓋

從個人版的輕巧便捷到企業版的全面管控，滿足不同用戶羣體的終端安全防護需求，適配多行業專屬需求

主營業務佈局：四大業務板塊協同發展

個人終端安全產品

面向個人用戶提供終端防護解決方案，核心功能涵蓋病毒查殺、系統防護、網絡防護、訪問控制及實用安全工具

火絨安全軟件 6.0 乾淨 · 輕巧 · 強大

核心技術對外賦能

擁有自主知識產權的反病毒引擎與多層次主動防禦系統，持續對外賦能，助力拓展安全防護領域

OEM合作 技術共享 · 生態共建

企業終端安全產品

全方位縱深防禦與終端統一管控方案，功能集成病毒查殺、終端管理、漏洞修復、資產管理、外設管控等

火絨終端安全管理系統 V2.0 集中管控·多平臺兼容

威脅情報服務

構建火絨威脅情報系統，具備「能發現、能應用、能處理」的核心能力，實現即時響應與動態防禦

威脅情報系統 精準處理 · 動態防禦

四大業務板塊協同發展

構建完整的終端安全防護生態體系

02

核心產品矩陣

個人與企業專屬安全方案

從個人版的輕巧便捷到企業版的全面管控
火絨安全提供差異化的產品解決方案
滿足不同用戶羣體的終端安全防護需求

個人終端安全產品

火絨安全軟件 6.0

核心特點

- 乾淨
- 輕巧
- 強大

增值服務

火絨應用商店

提供一站式管理體驗，用戶可便捷下載、安裝、更新各類應用程式，所有應用均經過安全檢測，杜絕捆綁軟體和惡意插件，讓軟體管理更安全、更高效、更省心

核心功能

病毒查殺

快速掃描、全盤掃描、自定義掃描，全面檢測清除病毒木馬

系統防護

即時監控文件、註冊表、進程等系統關鍵位置，阻止惡意操作

網絡防護

攔截惡意網址、釣魚網站、網絡入侵，保護上網安全

訪問控制

U盤保護、攝像頭防護、程式執行控制，嚴格管控權限

實用安全工具

垃圾清理、啟動項管理、服務管理、hosts文件保護多款實用工具

設計理念

個人版產品專注於個人防護便捷性，追求無廣告、無彈窗、無捆綁的純淨體驗。通過輕量化設計確保系統運行流暢，同時提供強大的安全防護能力，讓每一位個人用戶都能享受到專業級別的終端安全保護

企業終端安全產品：火絨終端安全管理系統V2.0

全方位縱深防禦

構建多層次、立體化的安全防護體系，從網絡邊界到終端設備，從文件掃描到行為監控，實現360度無死角安全防護。結合主動防禦與被動查殺，確保企業終端在任何場景下都能獲得全面保護

終端統一管控

通過中心化管控平臺，實現數千甚至數萬臺終端設備的集中管理。管理員可統一配置安全策略、批量部署任務、實時監控終端狀態，大幅提升安全管理效率，降低企業運維成本

核心功能矩陣

病毒查殺
本地引擎掃描

終端管理
集中管控

漏洞修復
系統加固

資產管理
硬件軟件統計

外設管控
設備權限控制

行業定製

適配**物流、醫療、金融、製造**等行業專屬需求，提供定製化安全解決方案

規模化部署

支持**中心+客戶端**架構，適配Windows、Linux、macOS等多系統平臺

集中管控

統一策略配置、批量任務部署、實時監控告警，提升管理效率

個人版 vs 企業版・差異對比

面向羣體

個人版

家庭用戶、小型個人工作室，單終端或少量終端使用場景

企業版

中大型企業、機構，大規模內網終端集中防護與管理需求

核心優勢

個人版

輕量化、易操作，滿足個人單機安全防護需求

企業版

集中管控、多平臺兼容、功能豐富，適配企業級規模化管理場景

部署方式

個人版

僅支持Windows系統，單終端安裝客戶端

企業版

支持Windows/macOS/Linux多系統，採用"管理中心+客戶端"架構，支持內網離線部署

功能特性差異

個人版

基礎安全防護 + 部分個性化工具功能

- 病毒查殺、系統防護、網絡防護
- 訪問控制、實用安全工具
- 火絨應用商店一站式管理

企業版

覆蓋個人版核心防護能力，新增企業級專屬管理功能

- 終端概況/安全風險/資產信息集中展示
- 遠程桌面/終端隔離/文件分發
- 漏洞批量修復/軟件黑白名單管控
- 違規外聯檢測/分組管理/LDAP對接

03

網絡安全威脅全景

病毒、攻擊與潛在隱患

從病毒木馬到網絡攻擊，從內部管理到外部威脅
全面剖析當前網絡安全面臨的嚴峻挑戰
揭示企業終端安全防護的關鍵痛點

常見病毒類型

常見病毒類型及危害

挖礦病毒 高發

佔用CPU/GPU資源挖掘加密貨幣，導致**系統卡頓、電費激增、硬件損耗**

感染型病毒 頑固

感染可執行文件和系統組件，導致**系統崩潰、程序無法運行、網絡癱瘓**

勒索病毒 高危

加密重要文件索要贖金，造成**數據無法恢復、業務中斷、鉅額經濟損失**

銀狐病毒 活躍

通過**釣魚郵件傳播，竊取敏感信息、遠程控制**

核心危害

現代網絡攻擊採用多技術組合形成攻擊鏈，偵察→入侵→橫向移動→數據竊取，具有隱蔽性強、破壞力大、持續時間長的特點，傳統單點防護難以有效應對

常見病毒類型及典型攻擊手段

典型網絡攻擊手段解析

惡意軟件攻擊

惡意軟件又稱“流氓軟件”，指在未明確提示用戶或未經用戶許可的情況下，在用戶計算機或其他終端上安裝運行

暴破攻擊

針對於密碼的破譯方法，將密碼進行逐個推算直到找出真正的密碼

釣魚攻擊

僞造可信機構郵件、網站，誘騙用戶泄露**賬號密碼、銀行卡信息、驗證碼**

殭屍網絡

將大量主機感染bot程序（殭屍程序）病毒，從而在控制者和被感染主機之間所形成的一個可一對多控制的網絡

攻擊特徵

現代網絡攻擊採用**多技術組合形成攻擊鏈**，偵察→入侵→橫向移動→數據竊取，具有**隱蔽性強、破壞力大、持續時間長**的特點，傳統單點防護難以有效應對

企業環境核心安全隱患與威脅態勢

企業環境核心安全隱患

內部管理隱患

- **人員安全意識薄弱**：缺乏安全培訓，易中招釣魚攻擊
- **權限管控混亂**：多人共用賬號，離職未註銷

技術防護隱患

- **邊界設備防護不足**：防火牆規則配置寬鬆
- **終端體系龐大難管控**：設備數量多，缺乏統一管理

威脅態勢洞察

終端攻擊趨勢

木馬病毒	**佔比最高**
勒索病毒	**破壞性強**
挖礦病毒	**持續高發**

重點威脅：銀狐病毒、LummaStealer病毒持續活躍，通過釣魚郵件、惡意鏈接傳播

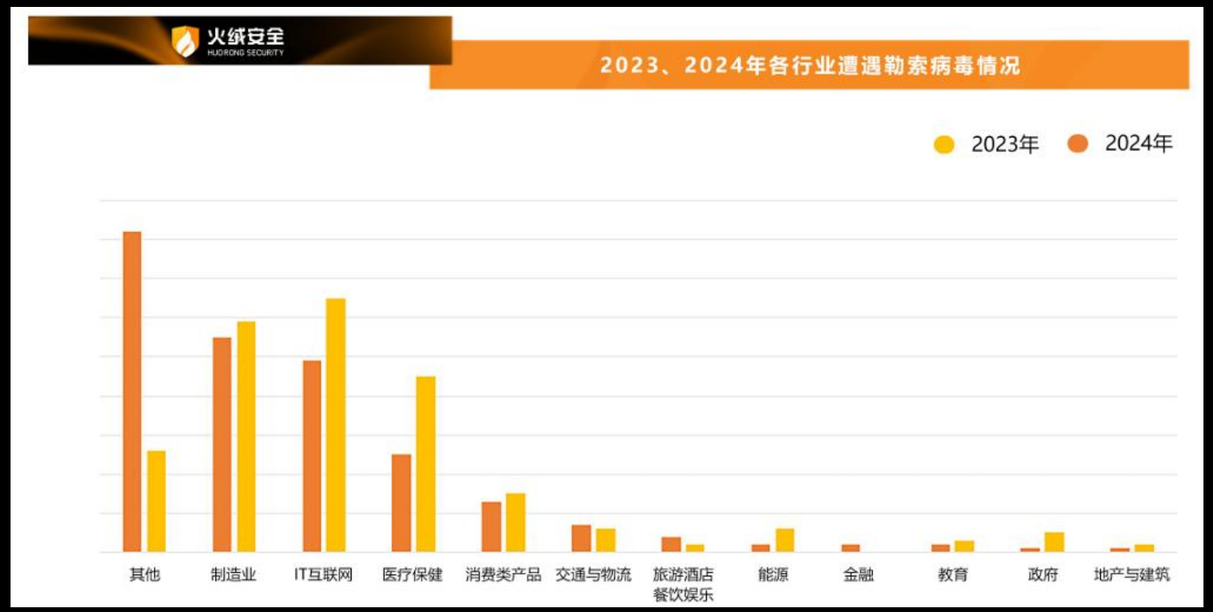
漏洞風險態勢

系統漏洞
系統漏洞被頻繁利用，**及時補丁更新**至關重要

攻擊趨勢：漏洞利用工具包氾濫，攻擊者通過自動化工具批量掃描、攻擊目標系統

威脅態勢洞察與真實案例

威脅態勢數據



真實威脅事件案例

企業核心系統入侵

某某車輛公司遭遇網絡攻擊，被迫關閉全球IT基礎設施，暫停部分工廠生產

內部人員與權限濫用

某某銀行盜竊案：黑客以920美元賄賂IT員工獲取企業憑證，盜走1.4億美元

定向攻擊與數據竊取

境外組織利用弱密碼入侵多所中學廣播系統，企圖篡改內容傳播有害信息

勒索軟件關聯

某某開發商遭勒索攻擊，超1萬用戶個人信息泄露

安全啓示

從個人用戶到大型企業，從內部管理到外部攻擊，安全威脅無處不在。只有建立**全面的安全防護體系**，提升安全意識，纔能有效應對日益複雜的網絡安全挑戰

04

技術防護

技術、功能與策略保障

火絨核心防護技術

自主研發反病毒引擎三大核心技術

通用脫殼

深度解析**加殼、混淆、加密**的惡意代碼，還原病毒真實面目，確保查殺無遺漏

動態行爲查殺

基於**病毒行爲特徵**進行檢測，即使病毒變種也能精準識別，有效應對未知威脅

虛擬沙盒

在**隔離環境**中運行可疑程序，分析其行爲邏輯，判斷是否爲惡意軟件

高查殺率

低誤報率

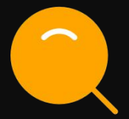
斷網可用

不損文件

火絨EDR體系

體系基石 · 終端

以數千萬“火絨安全軟件”終端爲基石，是數據採集源與策略執行者。



智能感知 · 檢測

實時防護並初步分析各類威脅，精準識別已知和未知風險。

協同處置 · 響應

專家深度分析，將解決方案快速下發至所有終端，形成閉環。

構建“終端-檢測-響應”的動態閉環，持續保護用戶安全

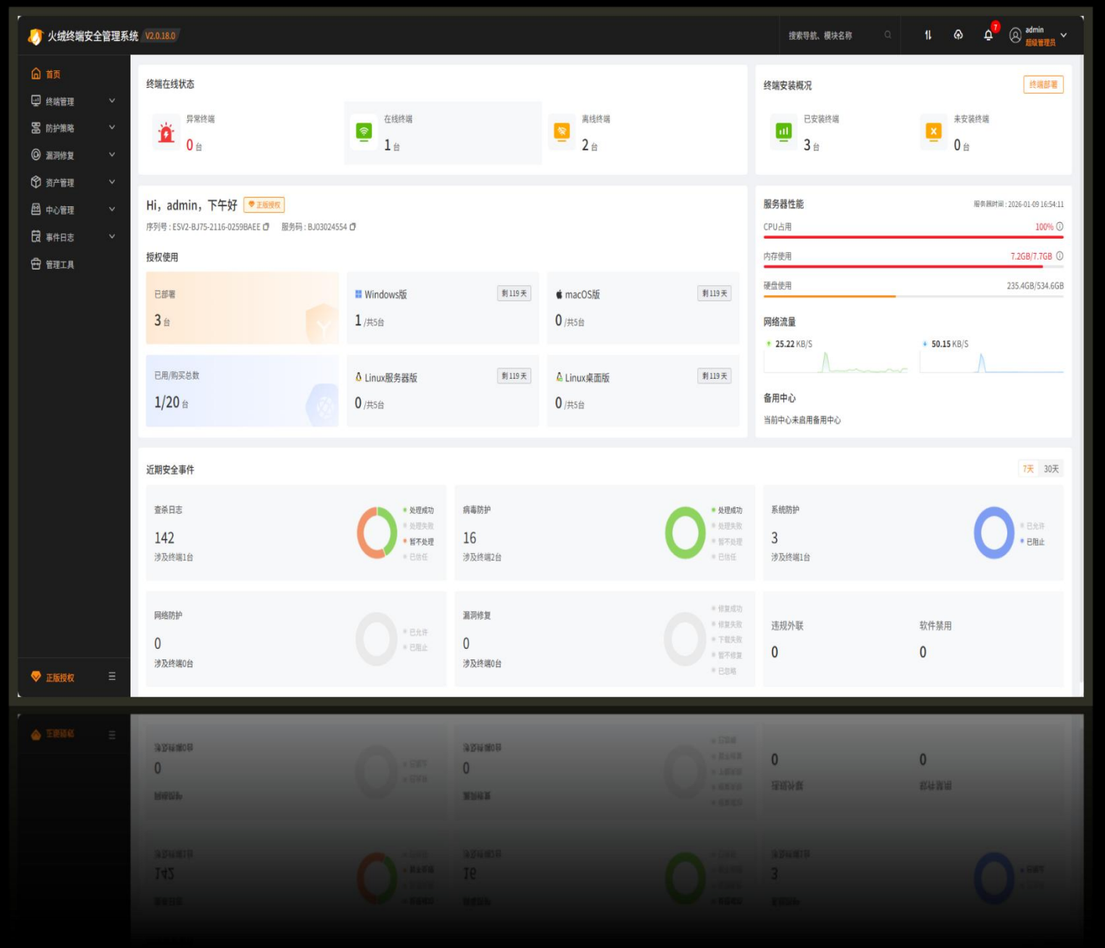
企業版本功能-可視化控制中心

可視化控制中心

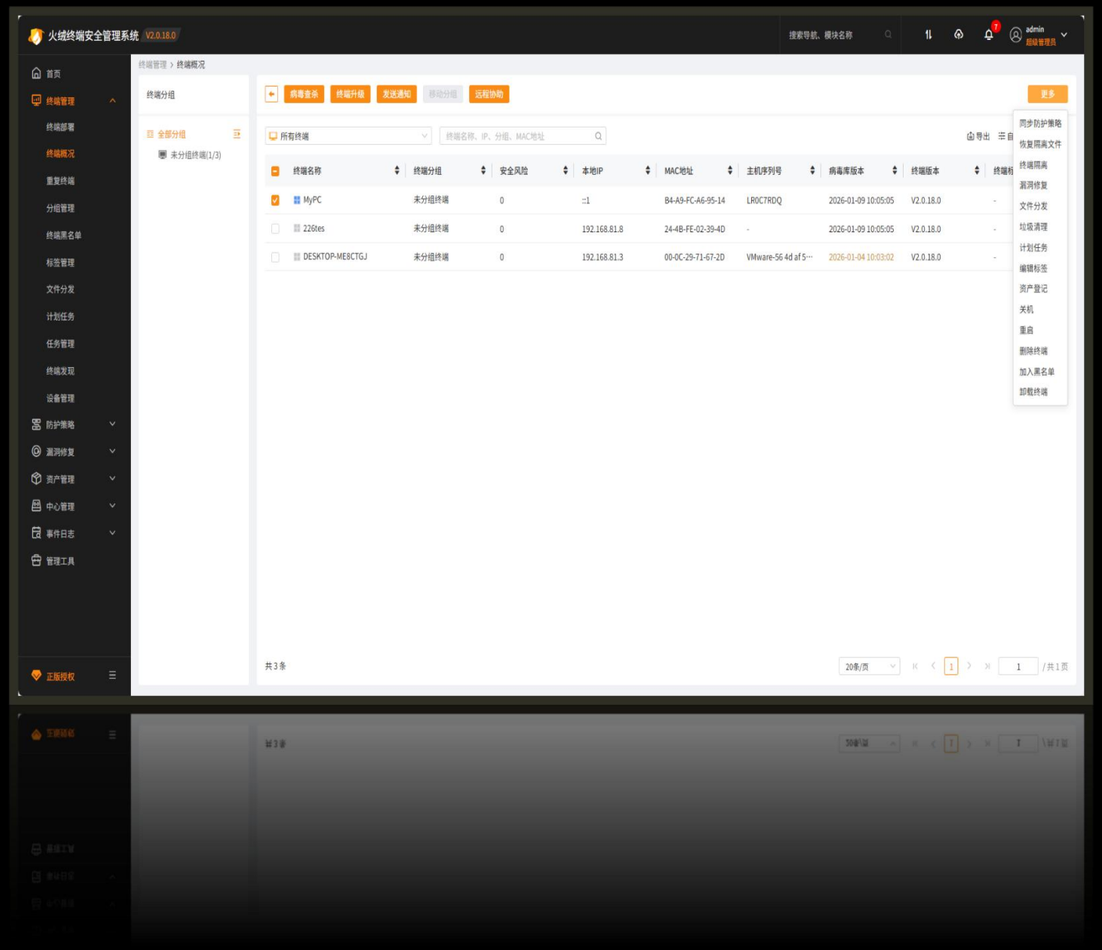
直觀呈現各類安全信息，反映服務器性能，方便管理員快速及時地掌握企業的安全全貌。

核心展示模塊

終端狀態:在線/離線終端數量及佔比。
安裝概況:終端安裝覆蓋率統計。
安全事件:近7天及30天內各防護模塊事件數量及處理情況。
服務器性能:實時監控服務器運行狀態。



企業版本功能-終端管理



終端全生命週期管理

核心功能概覽

提供全面的終端全生命週期管理，幫助管理員實現終端的統一部署、管控、維護與監控，確保企業終端安全與合規。

子功能模塊

- **終端部署**：支持自助安裝、安裝包安裝、域部署三種方式。
- **終端概況**：可執行病毒查殺、終端升級、遠程協助等操作，並支持篩選、導出、搜索。
- **終端詳情**：查看終端多類信息並支持相關操作下發。
- **高級管理**：重複終端處理、分組管理 (含組織架構同步)、終端黑名單、標籤管理。
- **任務與分發**：文件分發、計劃任務。
- **設備發現與管理**：終端發現、設備管理 (設備申請審批、信任設備管理)。

企業版本功能-防護策略

核心功能概覽

支持自定義安全策略配置，幫助企業構建多層次、可定製的終端安全防護體系。

子功能模塊

策略管理

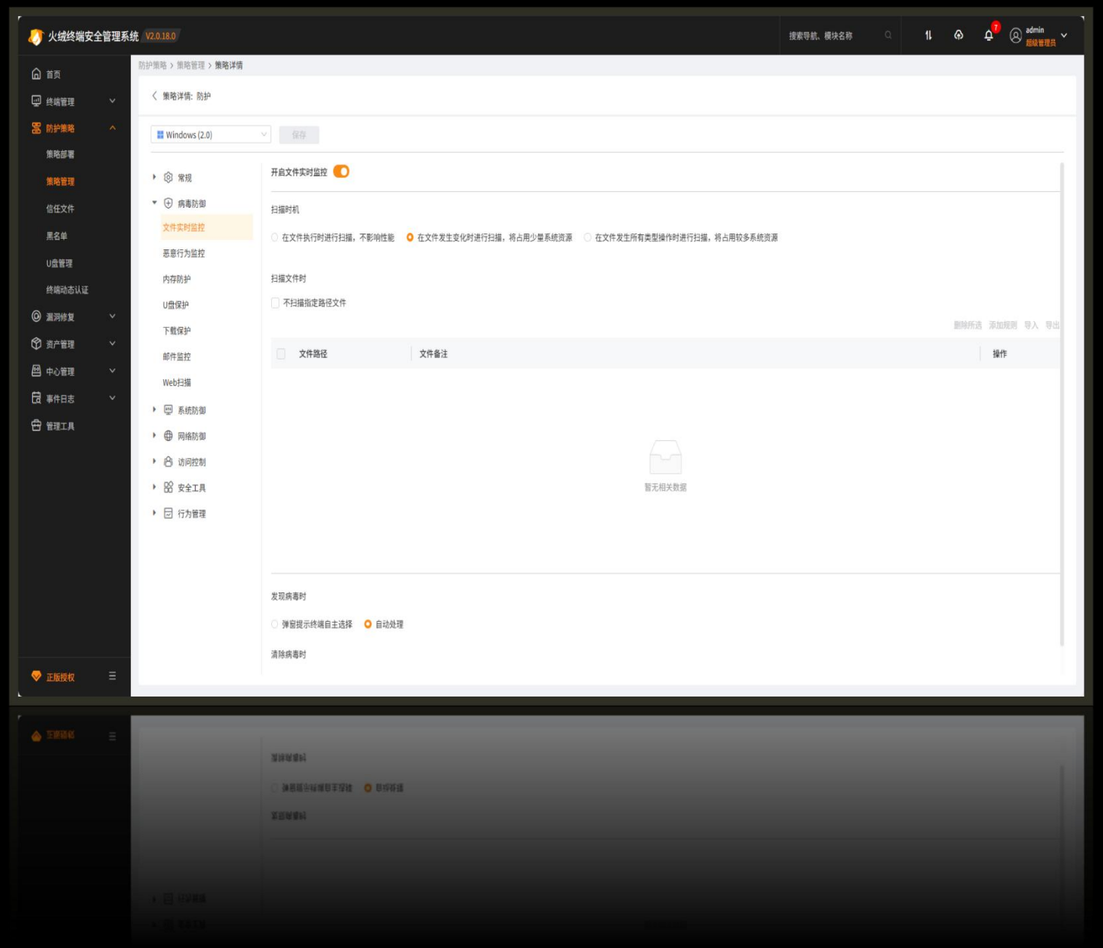
策略部署、分組策略、終端策略

安全管控

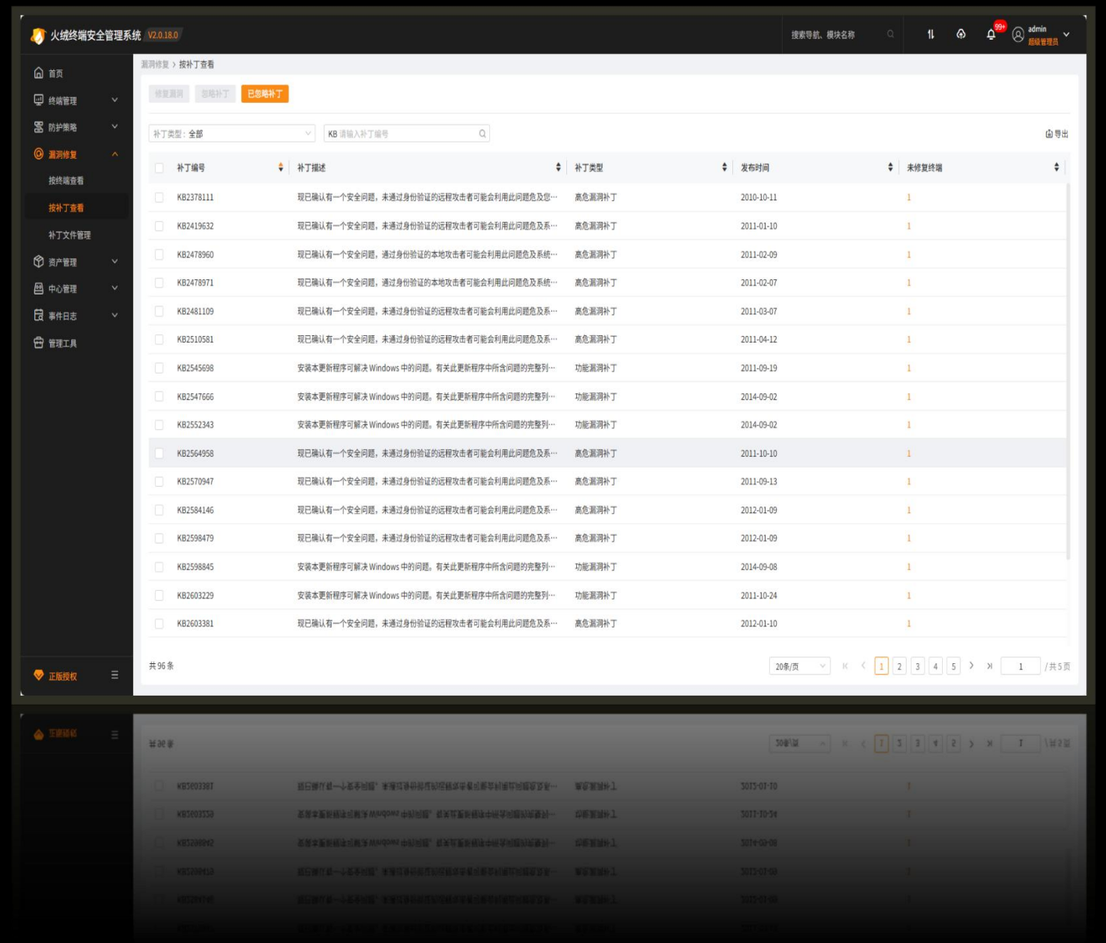
信任文件、黑名單、U盤管理、動態認證

五大防護區域

- 病毒防禦
- 系統防禦
- 網絡防禦
- 訪問控制
- 行爲管理



企業版本功能-漏洞修復



漏洞修復

精準操作

根據終端名稱、分組、IP選擇特定終端修復。

清晰概覽

終端狀態、漏洞分類一目瞭然。

高效檢索

支持按補丁類型或編號快速查詢。

補丁文件管理

集中緩存

補丁緩存在中心服務器，提升分發效率。

分發共享

客戶端從中心獲取，節省網絡帶寬。

企業版本功能-資產管理

資產管理

資產登記

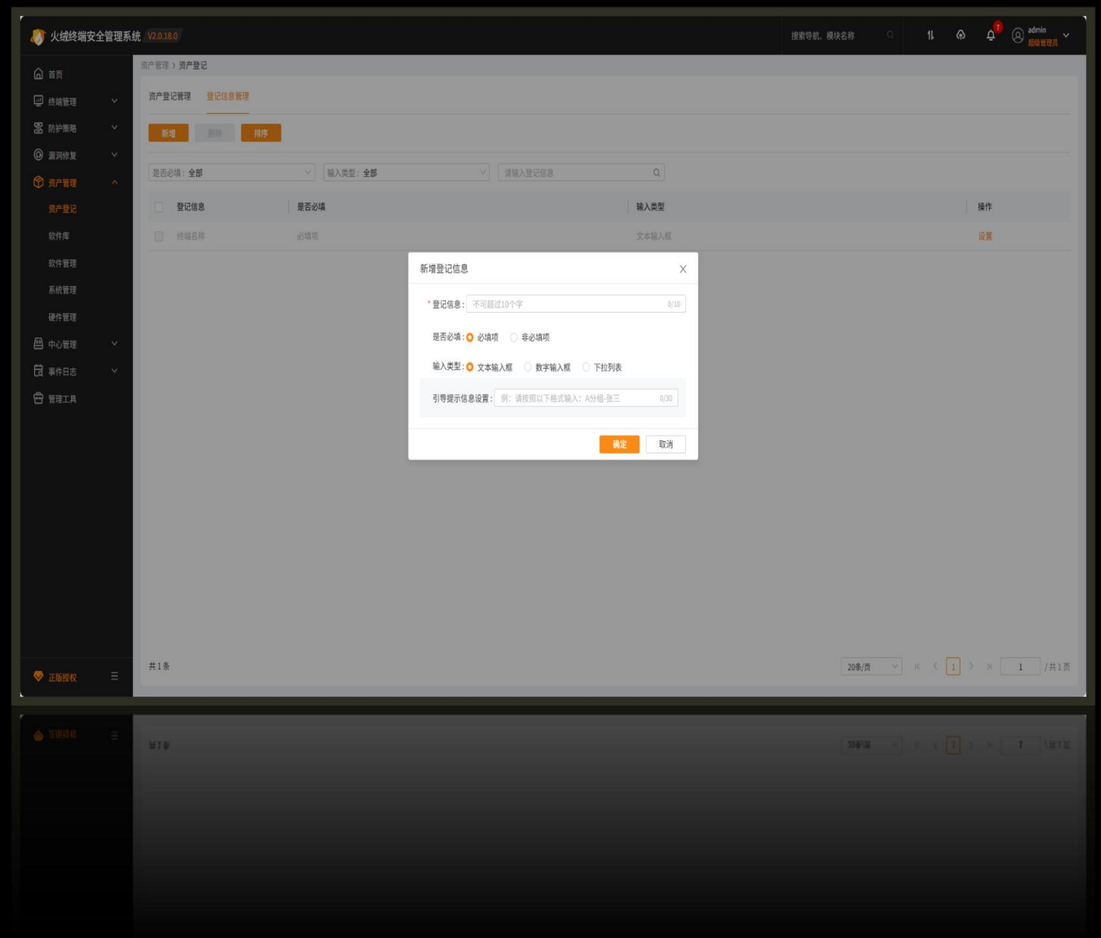
提供簡約高效的登記流程，支持自定義字段、設置必填項，滿足企業個性化需求。

軟硬件系統管理

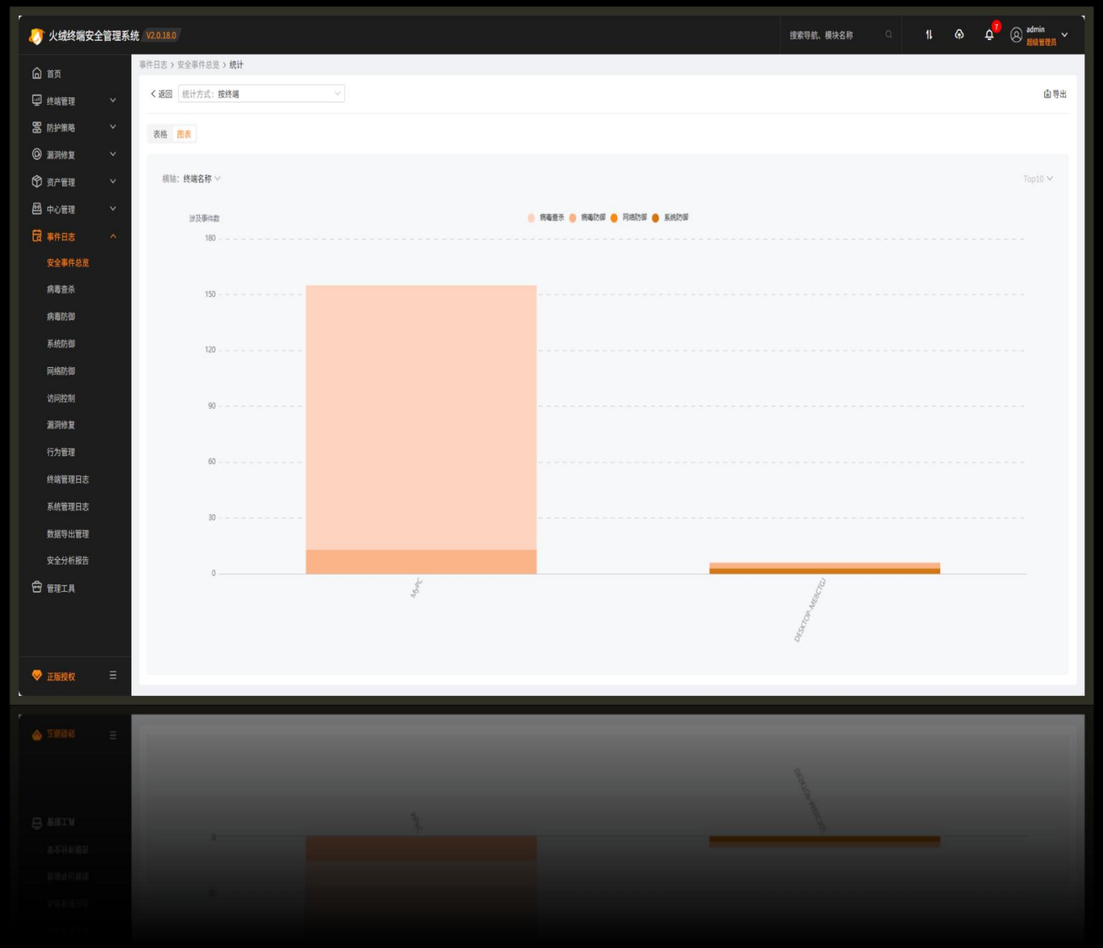
詳細記錄資產變更，輔助運維管理與財務審計，確保資產信息準確可追溯。

軟件庫

管理本地與雲軟件庫，聯動策略限制下載，構建企業私有應用商店。



企業版本功能-日誌報表



日誌管理

- **全面記錄：**記錄終端病毒查殺、防禦、漏洞修復等所有安全操作日誌。
- **報表導出：**直觀展現並導出各類日誌報表，滿足審計與合規要求。

安全分析報告

- **智能彙總：**自動對防護日誌、風險詳情等內容進行彙總分析。
- **專業建議：**提供詳細分析結果與處理建議，持續提升企業安全水位。

企業版本功能-產品聯動

產品聯動

開放API接口

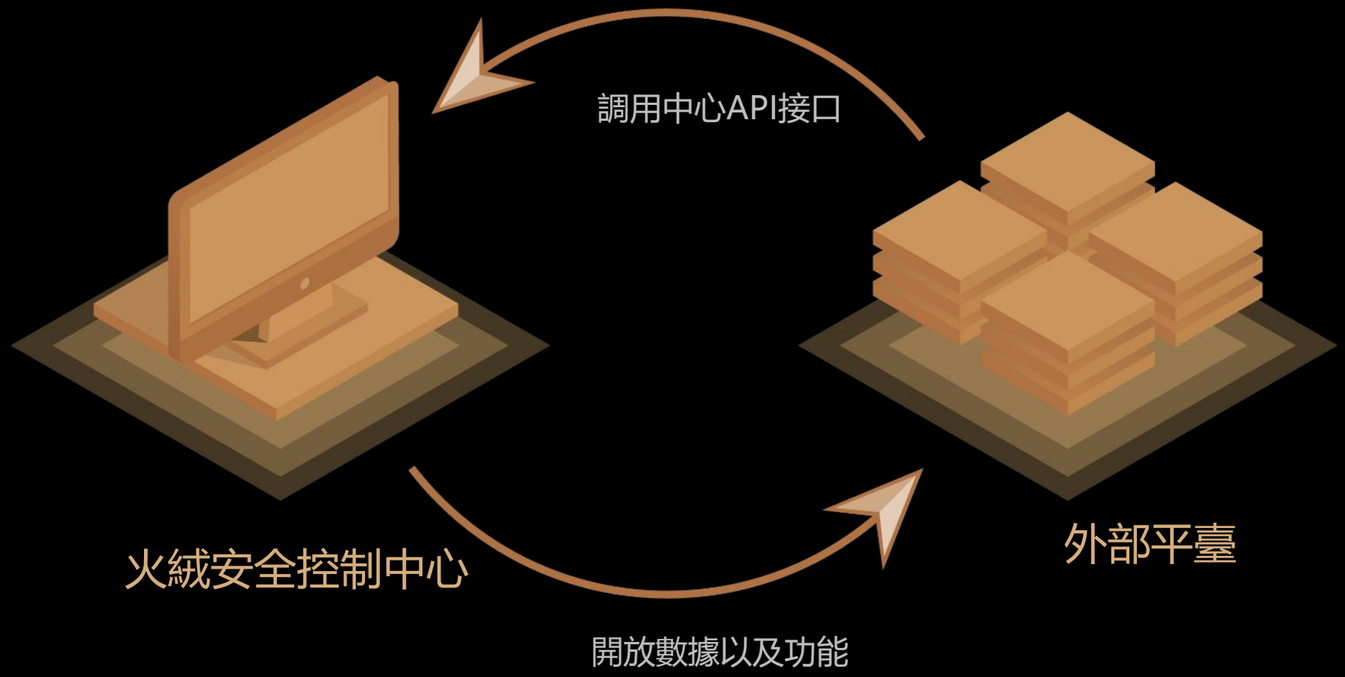
與准入系統等產品靈活聯動，打破信息孤島，構建一體化安全生態。

豐富的查詢信息

- 修改終端分組
- 查看終端信息
- 查看未修復漏洞
- 創建查殺、隔離、通知任務
- 查詢軟件信息

持續的功能擴展

持續開放更多聯動能力，滿足企業日益增長的集成需求。



火絨終端安全管控與防護

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

API接口

全員安全意識提升與賬號權限規範化管理

全員安全意識提升

基礎安全普及

病毒識別能力

識別**釣魚郵件、惡意鏈接、可疑附件**，不隨意下載未知來源文件

三不原則

不點擊、不下載、不轉發可疑內容，第一時間報告IT部門

高風險崗位專項教育

- **財務崗位**：識別冒充領導詐騙、資金轉賬覈實流程
- **IT崗位**：漏洞識別、應急響應、安全配置規範
- **採購崗位**：供應商郵件驗證、支付賬戶確認流程

賬號與權限規範化管理

賬號生命週期管控

- **一人一號**：禁止賬號共享，確保操作可追溯
- **實名綁定**：賬號與真實身份關聯，責任到人
- **離職註銷**：員工離職時立即禁用賬號，防止權限濫用

權限最小化原則

- **按需授權**：根據崗位需求分配最小必要權限
- **第三方權限嚴格限制**：外部人員權限定期審查

多因素認證（MFA）

對**核心系統強制啓用MFA**，即使密碼泄露，攻擊者也難以登錄。支持短信驗證碼、動態令牌、生物識別等多種認證方式，大幅提升賬號安全性

外部文件安全管理與場景化培訓演練

外部文件與郵件安全管理

郵件過濾與審覈

部署**企業級郵件網關**，攔截惡意附件、釣魚鏈接、垃圾郵件。對包含可執行文件、宏文檔的郵件進行隔離審覈，確保郵件安全

外部文件掃描

強制安全檢測後再使用U盤、移動硬盤等外部存儲設備。建立文件掃描流程，所有外部文件必須經過殺毒檢測，確保安全後方可使用

軟件下載管控

搭建**官方軟件庫**，提供經安全檢測的正版軟件。禁止從第三方網站下載軟件，杜絕捆綁軟件、惡意插件風險

場景化培訓與演練

模擬攻擊演練

釣魚郵件演練
定期發送模擬釣魚郵件，測試員工識別能力，對點擊用戶提供針對性培訓

弱口令暴破演練
模擬黑客暴破攻擊，檢測弱口令賬號，強制用戶修改高強度密碼

案例化培訓

結合**真實安全事件案例**進行深度剖析，讓員工瞭解攻擊手法、危害後果、防範措施。通過身邊案例強化安全意識，提升培訓效果

考覈與監督閉環

安全意識納入績效

- 基礎知識測試
- 演練表現評估
- 安全事件考覈

反饋機制

- 安全舉報通道
- 定期覆盤優化

05

成功案例

實力見證與行業認可

從互聯網巨頭到政府機構

從金融機構到能源企業

火絨安全憑藉專業技術與優質服務贏得廣泛信賴

跨行業客戶覆蓋與技術合作生態

商業用戶案例

- **京東金融**- 金融科技
- **拼多多**-電商平臺
- **中通快遞**-運輸平臺
- **桂林銀行**-金融機構

爲大型互聯網企業和金融機構提供終端安全防護與管控解決方案，保障核心業務系統穩定運行

政企事業單位

- **北京醫院**-醫療機構
- **浙江大學**- 教育機構
- **中國鐵建**- 交通基建
- **中國能建**- 能源企業

覆蓋政府、教育、醫療、交通、能源等關鍵基礎設施領域，爲國家級機構提供高安全級別的終端防護

技術合作生態

- **Lenovo**-硬件廠商
- **Microsoft**- 操作系統
- **啓明星辰**- 安全廠商
- **天融信**-網絡安全

核心技術對外賦能，與行業領先企業建立OEM合作關係，共築行業安全防線，實現互利共贏

客戶價值

火絨安全憑藉**專業技術、優質服務和定製化解決方案**，贏得了衆多行業領先客戶的信賴。從互聯網巨頭到政府機構，從金融機構到能源企業，火絨安全爲不同行業的客戶提供量身定製的終端安全防護方案，保障核心業務系統穩定運行，確保用戶數據和業務連續性

06

總結與展望

構建更全面的終端安全防護生態

立足技術優勢，深化產品服務
拓展生態合作，升級安全價值
持續守護數字時代的終端安全

核心優勢與未來發展方向

核心優勢總結

技術優勢

- **自主研發反病毒引擎**，通用脫殼、動態行爲查殺、虛擬沙盒三大核心技術
- **主動防禦系統**，四層縱深防護功能矩陣，全方位攔截威脅
- **持續技術迭代**，15年專注終端安全領域，緊跟威脅演進

產品優勢

- **全場景覆蓋**，個人版與企業版產品滿足不同用戶需求
- **功能全面且精準**，病毒查殺、系統防護、網絡防護、資產管理等
- **行業定製能力**，適配物流、醫療、金融等行業專屬需求

服務優勢

- **專業服務團隊**，7×8小時技術支持，快速響應客戶需求
- **定製化解決方案**，根據客戶業務特點量身定製安全策略
- **持續賦能客戶**，安全培訓、威脅情報、最佳實踐分享

未來展望

技術迭代

持續深耕**反病毒引擎與主動防禦**核心技術，引入AI/ML技術提升威脅檢測能力，應對AI驅動的新型網絡威脅，保持技術領先優勢

生態拓展

深化**行業合作**，擴大技術賦能範圍，與更多安全廠商、硬件廠商、系統集成商建立OEM合作關係，共築產業安全生態

價值升級

從**終端安全**向**全場景安全防護**演進，構建覆蓋雲、管、端的立體化安全防護體系，守護數字時代的用戶安全

使命願景

繼續踐行**"讓用戶安全、安靜、自由地操作終端"**的使命，堅持核心技術自主研發，以更專業的產品、更優質的服務，爲個人和企業用戶提供全方位的終端安全防護，守護數字時代的安全底線

火絨安全
Huorong Security

AL-Touch
@the reliable IT Solutions

火絨安全國際版

讓終端安全更簡單、更可靠

官方網站
www.huorong.cn

客服熱線
852-2333 2399

香港區代理

AL-TOUCH SOLUTIONS LIMITED 一大方案有限公司
https://www.al-touch.com.hk