

火绒终端安全管理系统1.0

火绒企业版

公司介绍

火绒成立于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，并持续对外赋能反病毒引擎等相关自主研发技术。

2012年，火绒推出免费个人产品，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，火绒于2018年正式推出企业版开启商业模式，并在线上线下同时试销，产品覆盖金融、互联网、制造、学校、医疗、公检法等50余类细分行业 and 单位机构。

截至目前，火绒已建立起包含研发、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，火绒团队的规模还在不断扩大中。



产品简介

2018年火绒正式发布首款企业级产品——“火绒终端安全管理系统1.0版”（简称火绒企业版），由“控制中心”和“客户端”构成。该产品拥有高效的终端管理、防御功能，能够通过“控制中心”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，将企业网络纳入严密的防控之中，确保安全无死角，充分满足企事业用户在目前互联网环境下的电脑终端防护需求。



“控制中心”由企业管理员登录后，对安装“客户端”的机器进行各类管控与下发安全策略。



“客户端”统一部署在企业终端与服务服务器上，并根据“控制中心”下发的策略进行具体终端和服务器的安全。

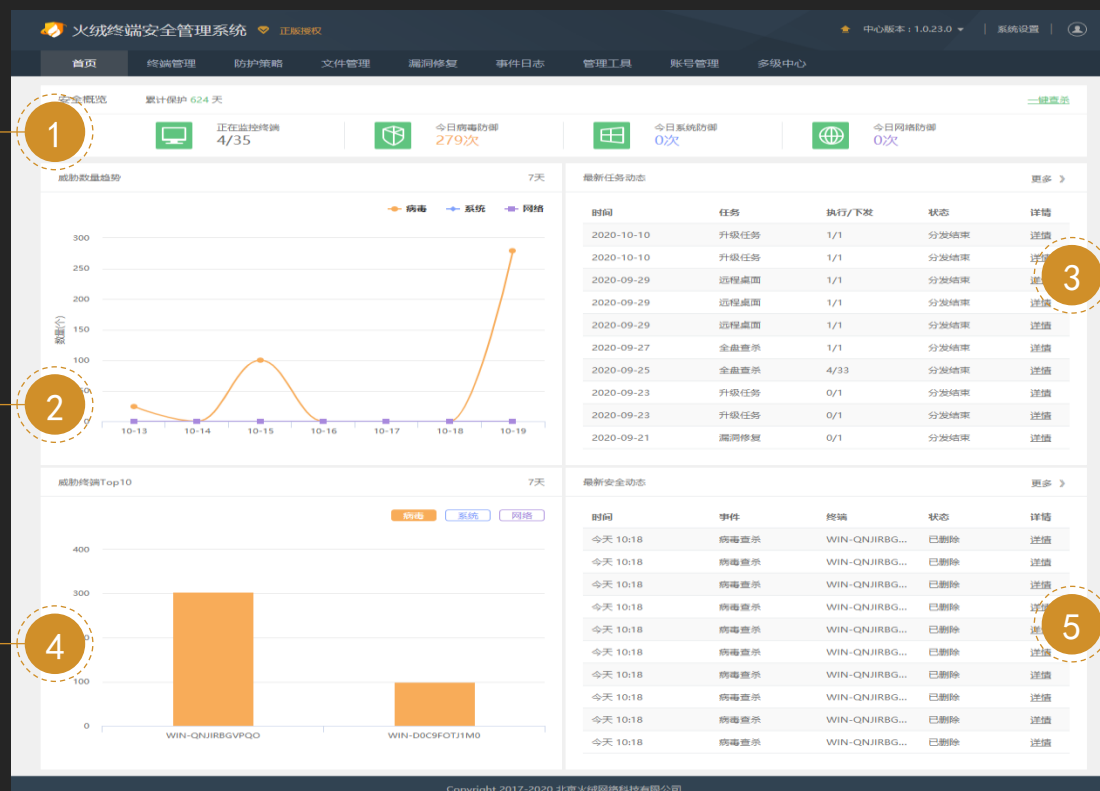
01

终端管理，让安全可控

终端管理

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。



安全概览

显示了监控的终端数量，以及对病毒、网络、系统防御的次数。

威胁数量趋势

曲线图直观展示防御次数变化。

威胁终端TOP10

直接显示定位到被攻击次数最多的终端。

最新任务动态

显示近期由“控制中心”下发的安全策略执行情况。

最新安全动态

显示近期拦截威胁、查杀病毒等信息日志。

终端管理

多级中心

解决企业跨部门、跨地域管理终端难题

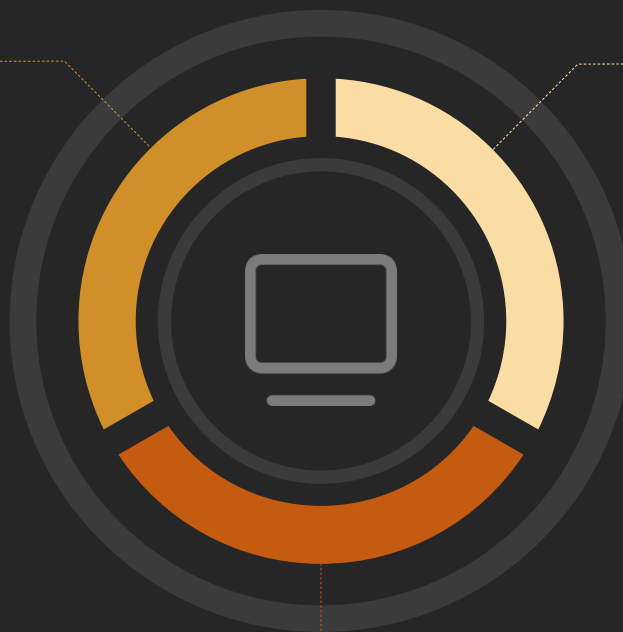
支持管理员通过上级控制中心管理下级控制中心，可帮助机构用户实现多级管理的需求，缓解单控制中心升级、修复漏洞的压力，解决下属单位异地联动、多部门安全管理协同等难题。

远程桌面

关闭有风险的远程端口后

可以协助企业远程办公

远程办公需要开启3389等远程端口，给病毒和黑客入侵的机会。火绒“远程桌面”功能可替代远程端口，完成远程工作，协助管理员远程控制客户端。线上直接帮助员工解决产品设置、病毒查杀、设备故障等各类问题。



U盘管控

给U盘设置白名单和加密，进可防范病毒，出则保护信息。

对于内网用户来说，U盘等外设是病毒传播的一大途径，也是信息泄露的主要“帮手”。火绒“设备控制”与“信任设备”功能可以组成设备白名单，防止病毒通过U盘等外设进入电脑。“信任设备”还具备给U盘加密等保护功能，防止企业重要资料被带出。

终端管理



终端管理

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。



防护策略

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，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。



文件管理

查看所有终端软件情况，并且可以推送下载文件、卸载软件等通知。



事件日志

按特定排序方式以及标签，查看任一时段内发生的全部事件，以分析旗下电脑的安全状况。



管理工具

通过管理工具页面查看日志数据大小并及时清理日志，也可以统一进行软件部署。



账号管理

可以通过“超级管理员”账户，添加、管理“管理员”账户，并设置“管理员”账户的操作模块和权限，令其协助管理控制中心以及终端。



漏洞修复

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。

02

终端防护，自主核心技术

终端防护——反病毒引擎

自主研发新一代反病毒引擎

火绒反病毒引擎是自主研发的新一代本地反病毒引擎，拥有“通用脱壳”、“动态行为查杀”等技术，包含了传统特征扫描、静态、动态启发式扫描。

此外，火绒还在持续不断地改进虚拟沙盒的执行效率和启发算法，通过日常升级推送给用户。这些反病毒引擎技术的及时更新，都会明显提高火绒对网络中未知威胁的检测能力。



终端防护——反病毒引擎



通用脱壳

火绒研发的“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“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，火绒可以有效识别已知病毒的新变种和未知病毒。

终端防护——反病毒引擎

01

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



02

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



03

对查杀结果可阐述，能准确指出样本为病毒的依据



04

本地杀毒能力强，不受断网环境影响



05

对查杀结果可控，误报率低



终端防护——主动防御系统

多层次主动防御系统

国内率先将单步防御和多步恶意监控相结合，监控上百个防御点，从网络防护，到系统保护，再到病毒查杀，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。此外，火绒具备完整的防火墙，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。

随着火绒工程师在处理安全事件的运营过程中，根据获取到的最新安全情报，会不断丰富更多的防护项目，帮助企业和个人在攻击的早期阶段抵御复杂威胁，保障主机安全和业务的正常运行。



终端防护——主动防御系统

灵活的网络管理

火绒具备完整的防火墙，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。

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进行拦截，无需人工干预。

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”，可以在无需重启服务或中断业务的情况下，保护存在漏洞的操作系统或者程序免受黑客攻击。



全面的系统加固

火绒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。

应用加固防护技术

对受保护的常见进程行为进行监控，防止黑客利用应用程序中的没有修复的漏洞或零日漏洞对用户主机发起攻击。

RDP弱口令渗透防护

通过登录终端进行二次验证，以及设置远程访问的IP白名单，阻止终端密码泄漏后遭遇攻击的风险。尤其对常利用RDP弱口令入侵的勒索病毒防御效果显著。

03

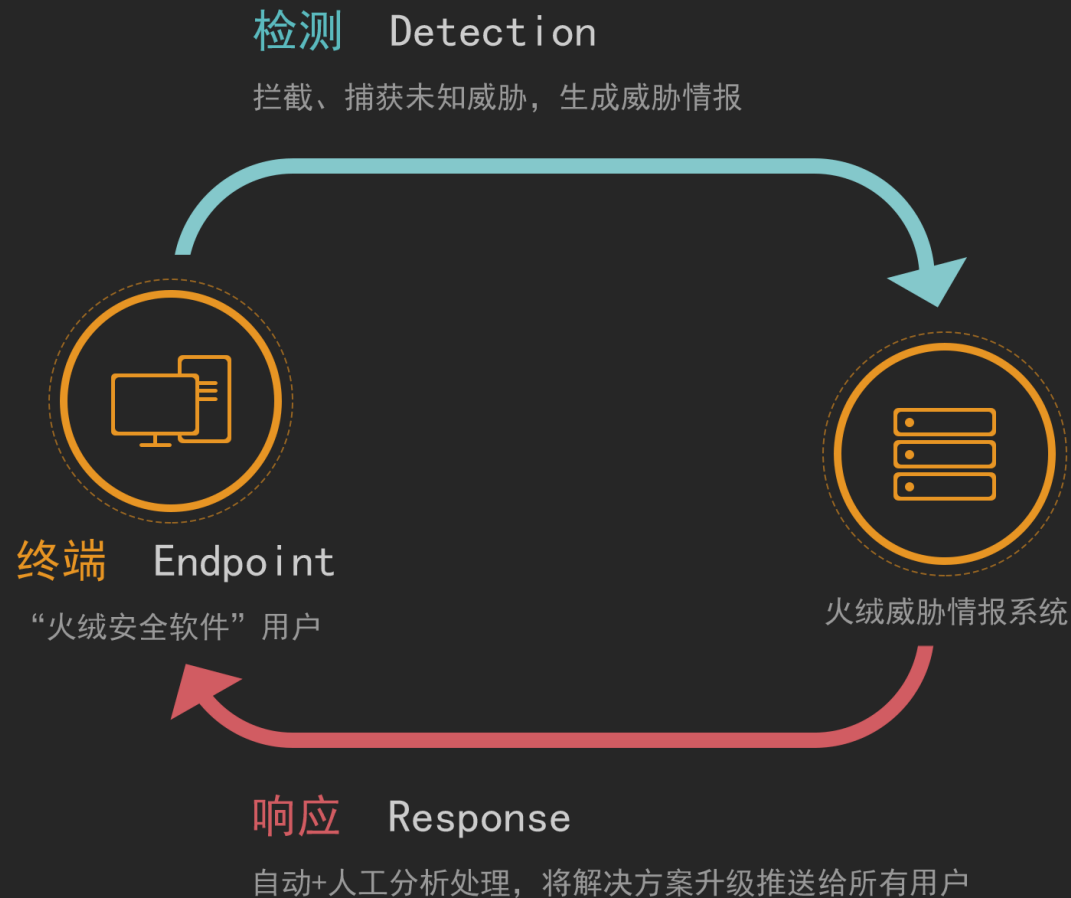
三大优势，体验产品和服务

三大优势——EDR运营体系

1 以遍布互联网的数千万“火绒安全软件”终端作为支撑体系的基石，即Endpoint。

2 火绒在给用户电脑进行防护的同时，还会对截获到的各类威胁进行初步检测、分析，即Detection。

3 将终端检测、分析后的可疑信息在“火绒终端威胁情报系统”聚合，由火绒工程师深度分析，制定出解决方案反馈至终端，提升终端安全性能，即Response。



三大优势——EDR运营体系

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



三大优势——成熟稳定的产品性能

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。

01

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。

02

03

适配广

支持微软系统、Linux服务器与主流国产操作系统，并支持与其它平台系统进行联动，开放接口传输数据。

04

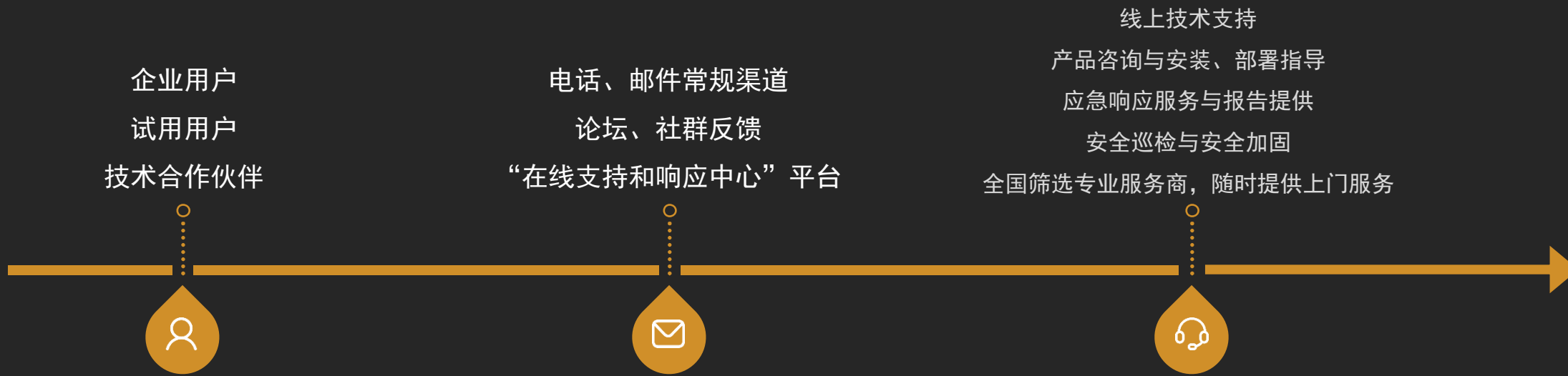
占用小

占用空间小、配置要求低，轻巧干净，不拖慢电脑速度。

三大优势——完善的服务体系

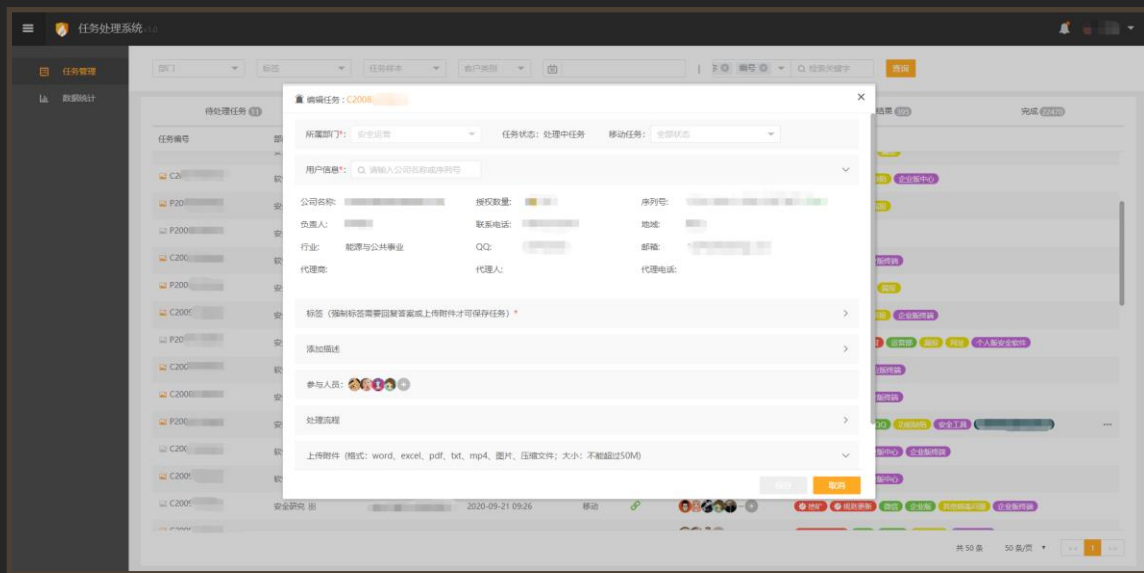
企业服务分钟级快速响应

火绒建立一套完整的、专业的服务平台和流程，通过集中统一收纳用户、代理商、技术合作伙伴等企业需求，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。



三大优势——完善的服务体系

用户服务平台和系统



完善的任务处理系统



企业级快速响应服务中心

三大优势——完善的服务体系

用户服务平台和系统



主流自媒体平台运营



官方论坛解决问题

04

服务用户与合作商

服务企业

企业用户

自2018年企业版推出以后，已有上万家机构单位在试用“火绒企业版”，用户涵盖政府、公检法、央企、学校、医院、金融等各行业，均反映良好，安装、使用简单，运行稳定，从未发生任何重大产品故障。企业用户可直接通过火绒官网申请，免费试用“火绒企业版”3个月，且享受与付费用户同等服务。

商业用户

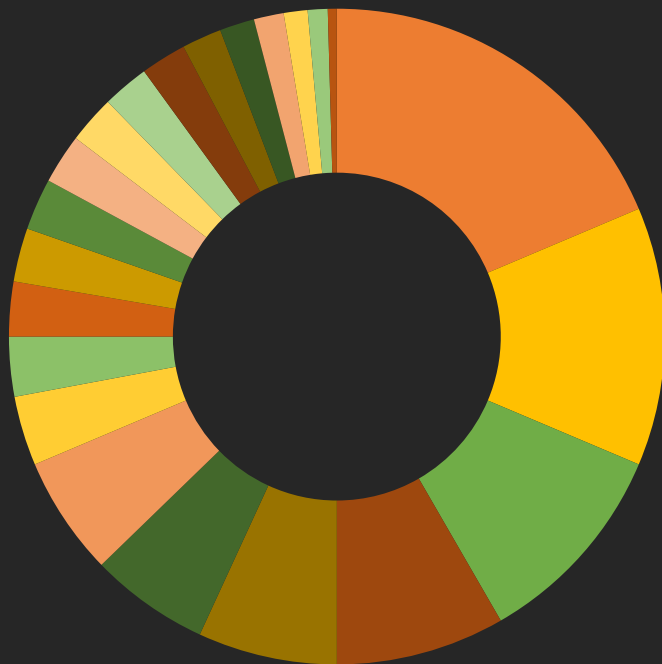


政企单位



服务企业

火绒企业版服务50多类细分行业

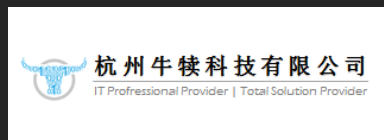


- 计算机与电子
- 制造业
- 其他
- 医疗保健
- 教育
- 政府
- 软件与网络
- 地产与建筑
- 零售
- 能源与公共事业
- 金融服务
- 交通物流
- 专业服务
- 农业与矿业
- 消费类产品
- 媒体与娱乐
- 游戏
- 旅游与酒店
- 批发与分销
- 非营利性组织
- 电信
- 生命科学

合作伙伴

服务商

为了更好的服务广大企业用户，火绒开启与代理商合作模式。目前，火绒已经完成全国代理、服务体系搭建。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。



合作伙伴

技术赋能

一直以来，火绒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，维护广大用户的终端安全。



05

企业常见问题与解决方案

企业常见问题与解决方案

1 电力公司局域网内病毒屡杀不绝

● 事件背景

某电力公司员工终端数量众多，且多为Windows7甚至XP等老旧系统，近期还发现有大量的病毒在网络中流窜，管理员使用同类产品杀毒后，仍旧不见好转，病毒仍然在疯狂传播。

● 技术分析

1. 员工终端数量多，有员工私自下载不合格的商业软件，导致病毒入侵。
2. 系统老旧，多残留漏洞，病毒可通过漏洞在局域网中横向传播，屡杀不绝。

● 解决方案

1. 通过“终端管理”功能及时对终端上的有害软件进行了统一卸载，全盘查杀。
2. “漏洞攻击拦截”功能找到存在漏洞的IP地址，修复漏洞并全盘查杀病毒。



终端防护——反病毒引擎

2 外设传播病毒

● 事件背景

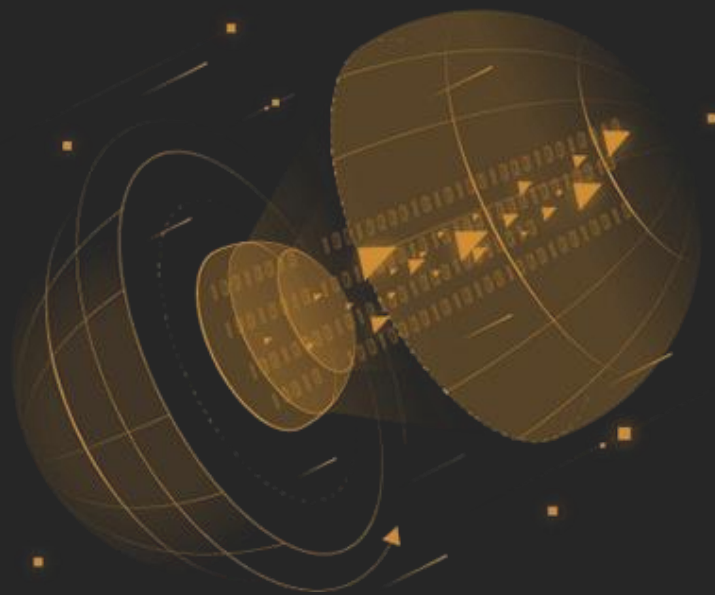
某企事业单位部门网络频繁遭遇木马病毒攻击，导致电脑运行缓慢，严重影响办公。

● 技术分析

工程师通过现场查看，发现用户网络内存在多种“蠕虫病毒”，且没有进行过处理查杀。导致病毒通过U盘、执法记录仪等可移动设备、共享目录、系统漏洞多种方式，在整个单位内网内大肆传播。

● 解决方案

1. 开启“U盘保护”功能，可更精确的针对U盘携带的病毒进行查杀。
2. 开启“设备控制”功能支持管理员禁用U盘等各种外接设备，进一步加强对外接设备的安全防范和管理。
3. “漏洞攻击拦截”功能对全网终端进行漏洞修复，并全盘查杀病毒。



终端防护——反病毒引擎

3 企业RDP弱口令爆破防御

- 事件背景

某企业在升级企业安全系统后，依旧屡次遭遇勒索病毒攻击，公司财产、资料损失惨重。

- 技术分析

该企业遭遇典型的“黑客入侵+勒索病毒”攻击，黑客通过弱口令爆破方式，获取系统登录密码，关闭企业防御系统，对企业内安全环境进行破坏，并成功植入勒索病毒。

- 解决方案

1. 开启“远程登录防护”功能，通过“白名单”的方式，只允许信任IP进行远程桌面。

2. 开启“终端动态认证”功能，通过二次验证的方式，预防RDP爆破后带来的风险。



06

企业大事记

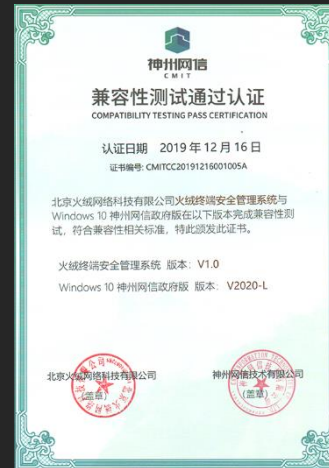
企业大事记



07

资质认证

资质认证





END

专注、纯粹才会更安全



微博



微信

企业官网: <https://www.huorong.cn>

客服电话: 400-998-3555

公司地址: 北京市朝阳区红军营南路15号瑞普大厦D座4层