火绒安全

终端安全管理系统1.0版

「关于我们」

Guan Yu Wo Men

火绒是“一个纯粹的安全公司”，“追求本质，以实现真实的安全价值为唯一目的”是我们的价值观。火绒以终端（PC、手机、服务器等）安全作为业务核心，以“冷静、艰苦、长期地专注于核心技术研究”作为立业之本，以“专注于终端安全产品和服务，让人们安全、安静、自由地使用电脑等设备”为业务范围和使命，并通过产品和服务收费实现商业价值。

火绒拥有国内唯一专注终端安全17年的安全团队，经过8年的创业积累和不断探索，研发出领先业界的自主知识产权的反病毒引擎和多项终端防护核心技术，覆盖在终端产品（个人版、企业版）上。

产品介绍

“火绒终端安全管理系统1.0”（火绒企业版）拥有高效的终端管理、防御功能，能够通过“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，拥有直接拦截漏洞攻击的“网络入侵拦截”等强大功能，将企业网络纳入严密的防控之中，确保安全无死角，充分满足政府&企业用户在目前互联网威胁环境下的电脑终端防护需求。

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。

01

安全管理系统

控制中心

信息展示

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。

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。

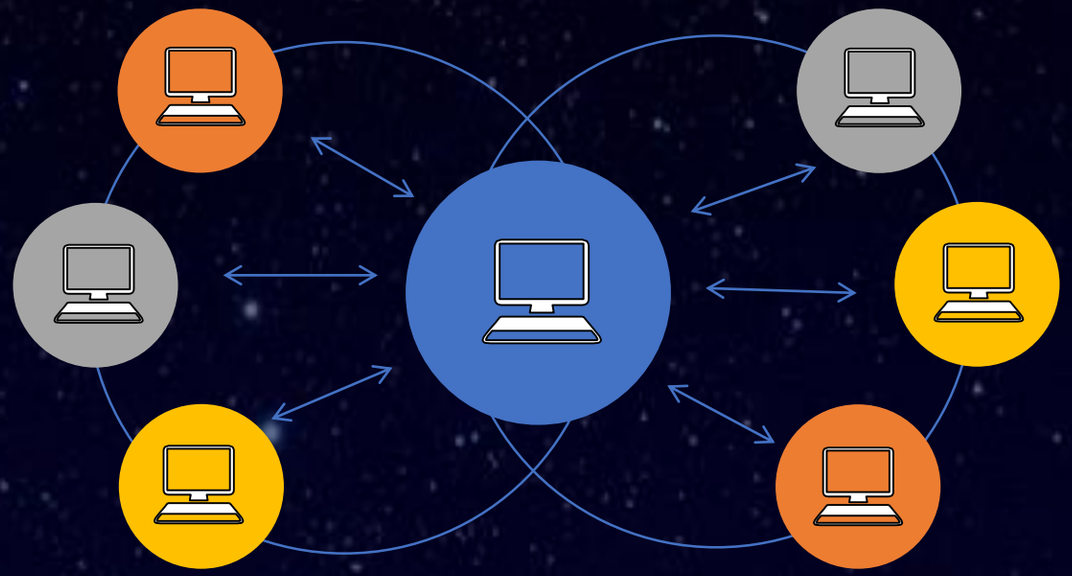
威胁终端TOP10：直接显示定位到被攻击次数最多的终端。

最新安全动态：显示近期拦截威胁、查杀病毒等信息日志。

“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。

多级中心

多级中心



解决企业跨部门、跨地域管理终端难题

（1）功能说明：

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、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。

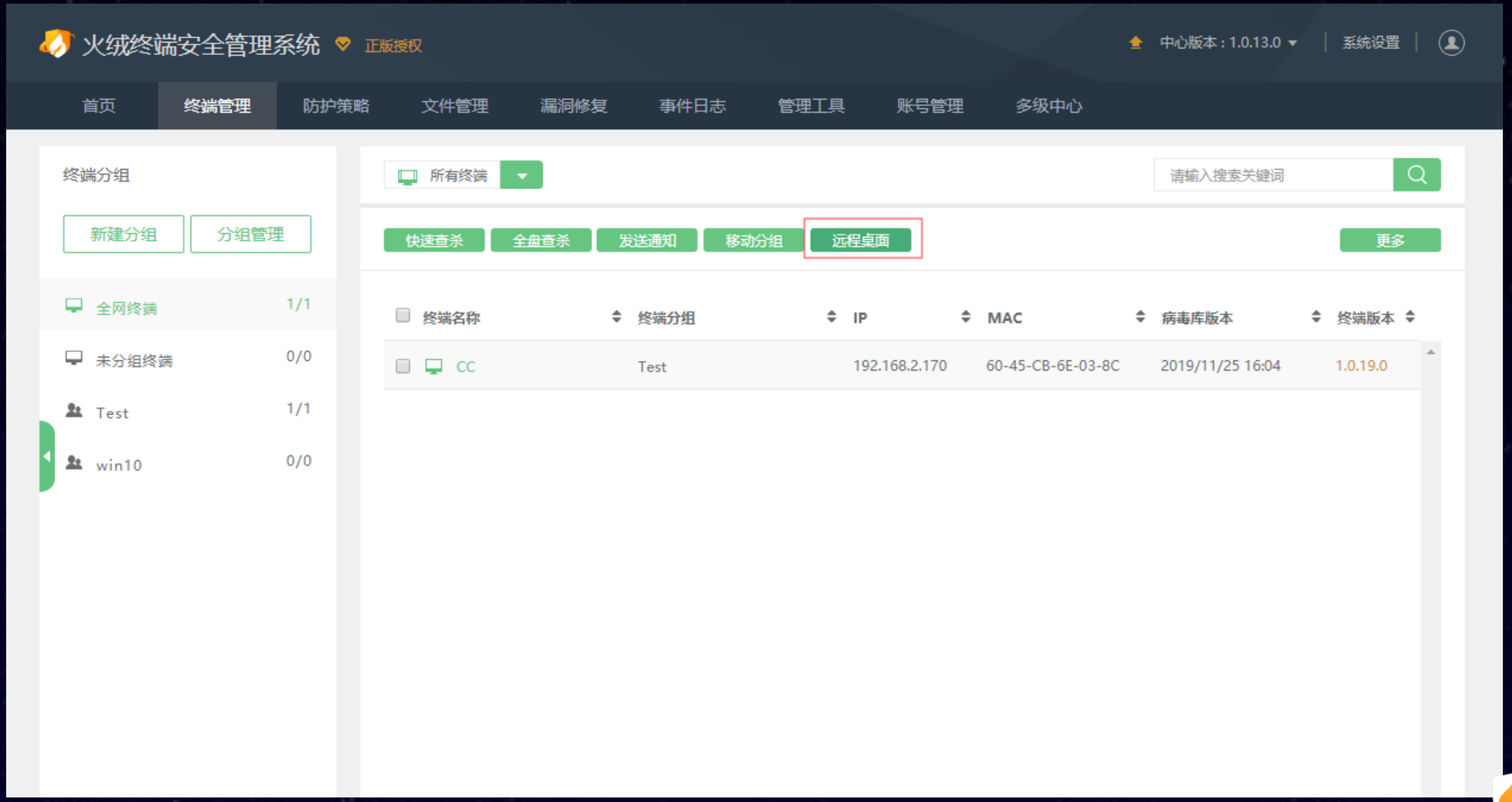
（2）适用用户：

——网络复杂、终端数量庞大的企事业单位。

——子公司、部门分布在异地的企事业单位。

——部门设立复杂，且安全需求高的企事业单位。

远程桌面



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。

（1）功能说明：

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。

（2）适用用户

特别适用于网络环境复杂、部门分散、高涉密类的政企用户。

U盘保护

U盘保护

给U盘设置白名单和加密，进可防范病毒，出则保护信息。

（1）功能说明：

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。

（2）适用用户

——政企内网用户，防范U盘等外设带入病毒。

——高涉密政府机构，对内部数据有高防范要求的企业。

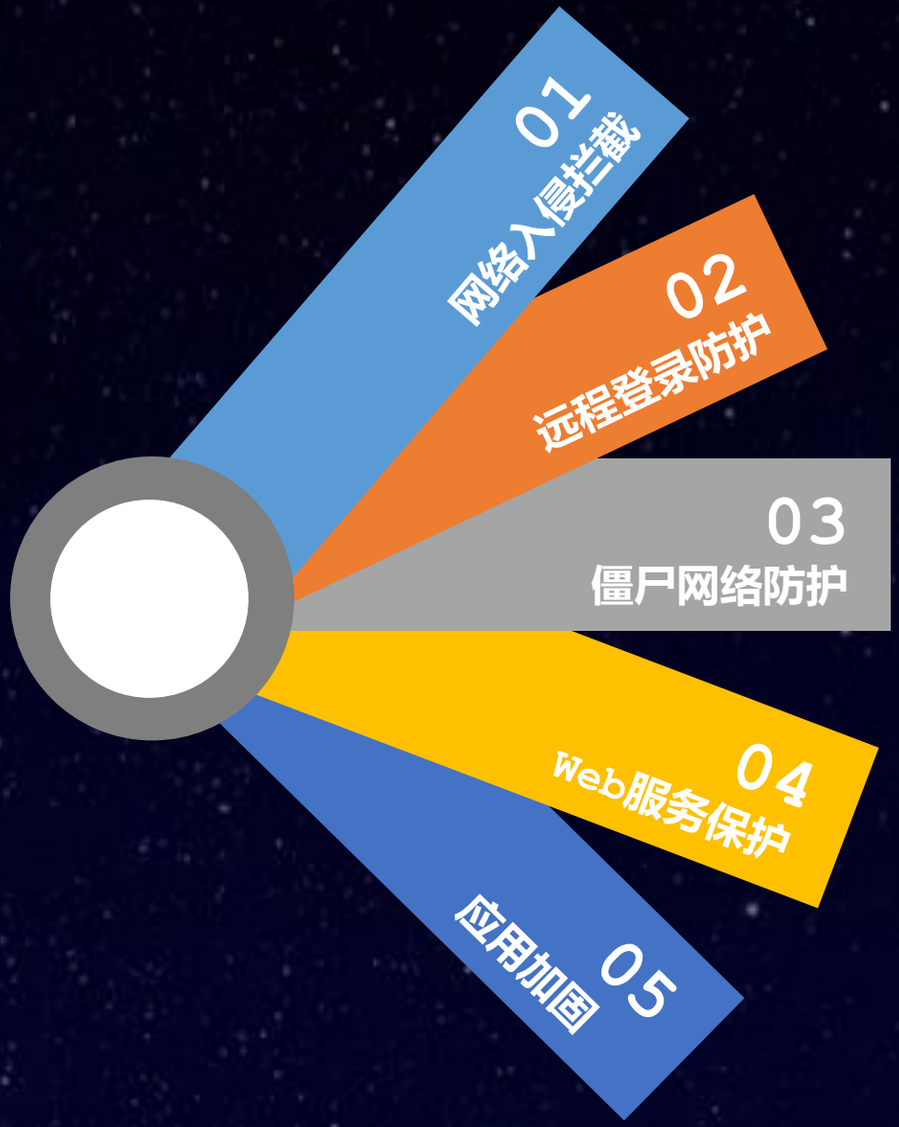
——需要对U盘等外设进行有效管理的办公网络

02

硬核防御功能

及时保护企业安全薄弱点

硬核防御功能



网络入侵拦截

顶尖漏洞防御技术，无论系统是否打补丁，都可以阻止勒索病毒、黑客攻击等高危威胁的入侵，并精准锁定攻击源头

远程登录防护

针对弱口令账号的有效防御手段，阻止黑客通过暴力猜密码入侵电脑

僵尸网络防护

避免电脑被黑客控制攻击其它设备，造成更大规模的影响

Web服务保护

拦截针对Web服务器的的漏洞攻击，保护服务器脆弱点

应用加固

火绒为常见软件提供安全加固，阻止应用遭遇攻击后，被利用下载病毒等

03

技术全面

深度融合“反病毒+主动防御+网络防火墙”

自主知识产权的新一代反病毒引擎

国内领先支持通用脱壳、拥有动态行为查杀能力的反病毒引擎，本地查杀能力强，不受断网环境影响，无需“白名单”；反病毒混淆能力强，病毒检测准确。

对查杀结果可阐述

能准确指出样本为病毒的依据

高查杀、低误杀，对软件的兼容性好

对查杀结果可控

多层次主动防御系统 监控上百个防御点

具备全面的“系统加固”，监控终端上百个防御点，阻止各种恶意程序对系统的攻击和篡改，从病毒查杀，到漏洞防御，邮件防护，恶意网址防护，再到商业流氓软件、弹窗拦截等等。

内容过滤

对文件、程序等内容进行安全扫描，排查威胁

行为分析

对文件、程序等行为进行安全分析，阻止作恶

规则拦截

对程序、系统等设置严格的防御规则，拦截任何违反规则的行为

强大的防火墙

从三个层面提供保护：拦截恶意网址、 IP规则拦截、黑客入侵拦截。

04

三大优势

体验火绒

先进的EDR策略

1

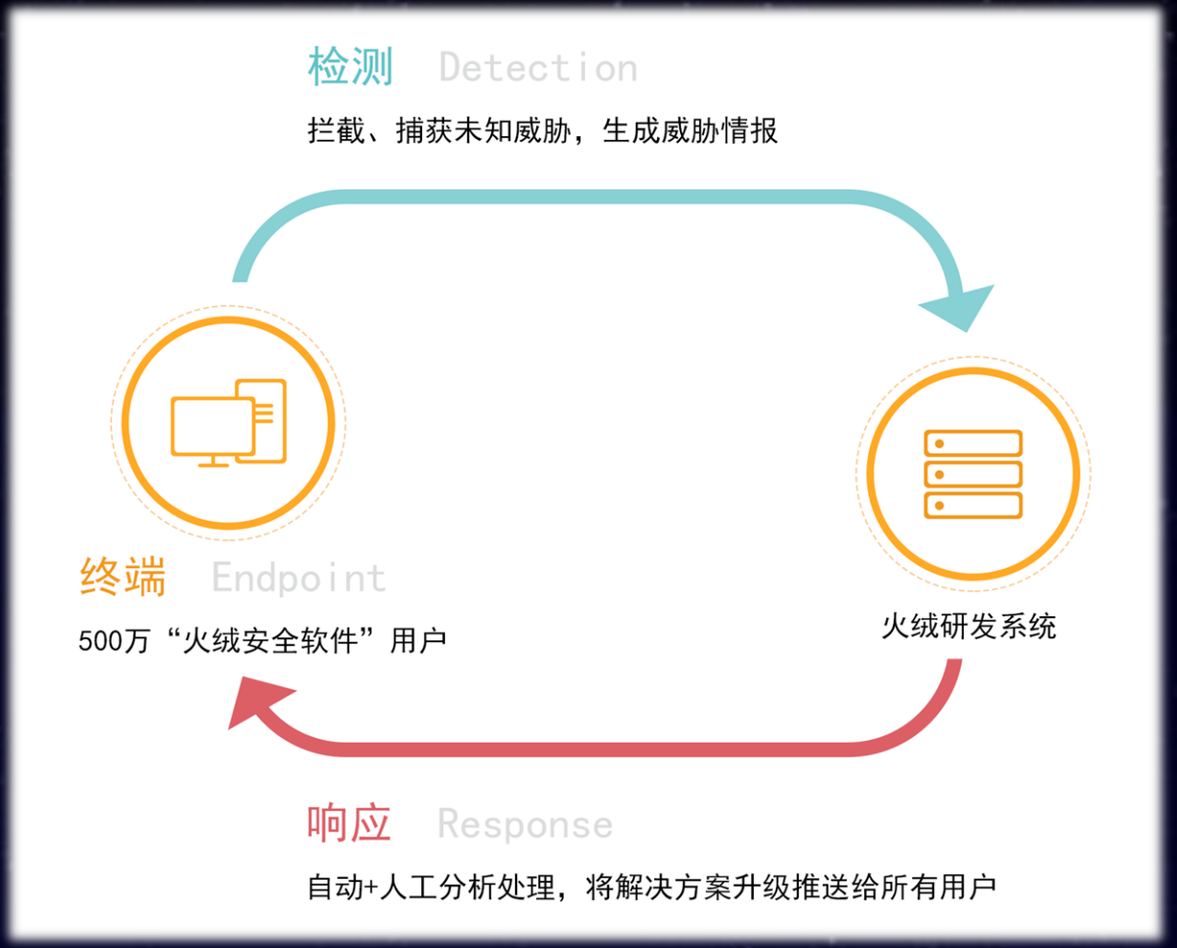
第一步，以遍布互联网的数百万“火绒安全软件”终端作为支撑体系的基石，即**终端**(Endpoint)。

2

第二步，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**检测**（Detection）。

3

第三步，将威胁信息在“火绒终端威胁情报系统”聚合，由火绒工程师深度分析，制定解决方案，再在终端上响应（比如升级病毒库），即**响应**（Response）。



先进的EDR策略

成熟稳定的产品性能

1

深谙国内安全特殊性，能迅速处理国产流行病毒，有效防范商业软件侵权行为。

2

兼容性好，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。

3

尊重用户的隐私权、数据所有权，不会上传用户的任何文件、数据等信息。

4

全面支持微软系统，同时还支持Linux服务器。

完善的服务

1

首家建成“在线支持和响应中心”，保证客户提交问题后，30分钟内回复。

2

专业服务团队对接，病毒、开发、测试、销售等多部门配合解决问题。

3

一对一建立客户档案，全程记录、跟踪，直到解决问题。

4

筛选专业的服务商，目前已遍布全国主要区域，可随时随地提供服务。

05

安全方案

典型案例

电力公司局域网内病毒屡杀不绝

1

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，近期还发现又大量的病毒在网络中流窜，管理员使用技术手段艰难清除后，仍旧不见好转，病毒仍然在疯狂传播。

2

技术分析

- 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。
- 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。

3

解决方案

- 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。
- “漏洞攻击拦截”功能找到存在漏洞的的IP地址，修复漏洞并全盘查杀病毒。

公安部门预防外设传播病毒

1

事件背景

某公安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。

2

技术分析

通过日志发现病毒来自U盘、执法记录仪等外设，然后通过共享文件夹在整个网络中交叉感染。

3

解决方案

- 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。
- 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。

企业弱密码暴破防御

1

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。

2

技术分析

该企业遭遇典型的“黑客入侵+勒索病毒”攻击，黑客通过弱口令暴破方式，获取系统登录密码，关闭企业防御系统，并成功植入勒索病毒。

3

解决方案

开启“远程登录防护”，对短时间内多次错误输入密码的行为进行拦截，阻止暴破。

06

典型服务企业与合作商

典型服务企业与合作商

企业大事记


Start
2011年09月
“火绒安全实验室”成立
2012年08月
火绒发布第一款产品，专供安全专业人士使用的“火绒剑-互联网安全分析工具”
2012年12月
火绒发布针对PC个人市场的主打产品“火绒互联网安全软件1.0”，后改名为“火绒安全软件”
2013年10月
发布“火绒安全软件2.0”
2014年07月
发布“火绒安全软件2.5”，并正式推向市场
2015年09月
加入微软VIA（Virus Information Alliance），10月加入微软MVI（Microsoft Virus Initiative），成为微软的安全合作伙伴
2015年11月
发布“火绒安全软件3.0”
2016年01月
和联想展开深度技术合作
2016年10月
发布“火绒安全软件4.0”
2017年05月
和绿盟、深信服等企业进行深度技术合作
2017年05月
完成首轮Pre A融资，并和天融信成为战略合作伙伴
2017年10月
首款企业级产品“火绒终端安全管理系统1.0”打造完毕
2018年03月
火绒宣布“关停流量业务”
2018年05月
火绒终端安全管理系统1.0”正式发布
2019年05月
发布“火绒安全软件5.0”

THANK YOU

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B座1202室
Room 1202, Tower B, Ruipu Building, No. 15 Hongijunying South Road,Chaoyang District,
Beijing. China