火绒安全
HUORONG SECURITY

火绒终端安全管理系统 2.0

技术白皮书

2021/05/20

公　　司：北京火绒网络科技有限公司

地　　址：北京市朝阳区红军营南路 15 号瑞普大厦 D 座 4 层

网　　址：https://www.huorong.cn

电　　话：400-998-3555

版权声明

用户隐私和数据安全声明

1、火绒尊重用户的隐私权、数据所有权，不会上传用户的任何文件、数据等信息。

2、火绒仅在用户中心控制台联网升级的情况下，上传用户许可相关信息（License），用于验证正版授权。

目录

1、概述

欢迎阅读《“火绒终端安全管理系统 2.0”技术白皮书》。为了能够更好的服务于用户，火绒安全特别编写本文件。本文件详细的介绍了 “火绒终端安全管理系统 2.0”的理念策略、核心技术、产品功能等内容，可让用户对本产品有更深入的了解。

Tips:

- 如果您想了解“火绒终端安全管理系统 2.0”的安装需知和部署流程，请参阅《“火绒终端安全管理系统 2.0”安装部署手册》。
- 如果您是初次体验“火绒终端安全管理系统 2.0”，想要快速了解使用方法及操作流程，请参阅《“火绒终端安全管理系统 2.0”使用手册》。
- 如果您想了解“火绒终端安全管理系统 2.0”产品的详细介绍，请参阅《“火绒终端安全管理系统 2.0”产品说明书》。

2、产品

2.1 产品介绍

“火绒终端安全管理系统 2.0”是秉承“情报驱动安全”新理念，全面实施 EDR 运营体系的新一代企事业单位反病毒&终端安全软件。本产品能帮助用户完成终端安全软件的统一部署、全网管控，集强大的终端防护能力和丰富方便的全网管控功能于一体，性能卓越、轻巧干净，可以充分满足企事业单位用户在目前互联网威胁环境下的电脑终端防护需求。

2.2 产品特点

2.2.1 自主知识产权，适合国内用户

自主知识产权和全部核心技术，完全避免产品后门和用户敏感信息外泄等隐患。

自主核心技术，能够更好地开发产品。OEM 引擎需要在外层再次封装,以符合自身产品的需求，增加成本降低效率，无法精细地调整配置，产品效率低、资源占用高。

自主核心技术，能够及时响应本地安全问题，迅速处理国产木马和流氓软件，同时对误报、兼容等问题的沟通、处理时间短。

对国内安全问题的特殊性有深刻认知，除了反病毒、反黑客，更能有效防范商业软件侵权和国内病毒产业链。

“火绒终端安全管理系统 2.0”支持 HTTPS 加密通讯，对控制中心与安全终端交换的信息加密传送，防止数据被窃取和篡改，数据传输更安全。

2.2.2 全网威胁感知，EDR 运营体系

火绒安全秉承“情报驱动安全”的理念——以全面、真实、及时的全网威胁情报和企事业单位安全需求，来驱动技术研发，为单位提供可靠、高效的安全产品和服务。

火绒 EDR（终端、检测和响应）运营体系，基于遍布互联网的数千万“火绒安全软件”用户，这些产品即是截获、处理各种未知威胁的探针，实时感知全网的威胁信息。

通过前端截获、预处理，后端进一步深度分析和处理，火绒 EDR 系统产出强大的威胁情报，据此来升级产品，提供高品质的安全服务。

每一个“火绒终端安全管理系统 2.0”用户，都随时享受着数千万互联网威胁探针（个人用户终端）带来的威胁情报的整体价值，真正做到实时感知、动态防御。

2.2.3 成熟的终端，强悍轻巧干净

火绒终端产品已经有多年运营经验，服务数千万用户，其中大部分是电脑高手，经受了各种复杂环境的考验，产品稳定成熟，运营和服务经验丰富。

独有的基于虚拟沙盒的新一代反病毒引擎，多层次主动防御系统，反病毒、主动防御、防火墙三个模块的深度整合，确保对各种恶意软件的彻底查杀和严密防御。

基于新技术、新理念和 EDR 运营体系，火绒终端产品安装后仅占用 20M 硬盘资源，病毒库 3M 大小，日常内存占用不到 10M，平常使用中，几乎感觉不到火绒终端产品的存在。

秉承安全厂商的基本操守，火绒终端产品没有任何捆绑、弹窗、侵占资源等行为，并强力狙杀各种流氓软件、商业软件的侵权行为，确保电脑系统干净清爽，就像每天都在使用新电脑。

2.2.4 高效的控制中心，可靠、易用

“火绒终端安全管理系统 2.0”拥有强大、高效的终端管理功能，统一部署、集中管理，将企事业单位网络纳入严密的防控之中，确保安全无死角，每个终端的安全防御状况都能轻松掌握。

基于对用户的深刻理解，“火绒终端安全管理系统 2.0”的控制中心设计合理，拥有友好的界面、人性化的统计报表，安全管理信息和日志一目了然，能极大的提高安全管理效率。

控制中心提供了基于 Web 服务架构的可移动控制平台，管理员无需安装额外的控制软件，就可以在任意一台电脑通过 Web 浏览器访问控制台远程操作控制中心，轻松实现对整个网络的管理。

“火绒终端安全管理系统 2.0”支持域脚本安装等安装方式，可以短时间在网络内部署众多客户端，简单快速的完成整个网络反病毒体系的部署。

3、理念和策略

3.1 理念：“情报驱动安全”

“火绒终端安全管理系统 2.0”和服务秉承“情报驱动安全”的理念——以全面、真实、及时的互联网威胁情报为基础，来驱动技术研发和产品开发，并建立相应的安全服务运营体系。实时感知、精准处理、动态防御，为用户提供可靠、及时、成本合理的安全防护。

3.2 策略：EDR 运营体系

实现“情报驱动安全”的核心，是部署实施 EDR（终端、检测和响应）运营体系。火绒 EDR 体系以遍布互联网的数千万“火绒安全软件”（个人版）终端为基础。“火绒安全软件”在保护用户安全的同时，又是截获、处理各种未知威胁的探针，这些威胁信息在用户电脑上完成初步分析和处理，然后回传给火绒后台系统，进一步分析和处理。

EDR 终端探针的有效运行，依赖“火绒安全软件”的新一代反病毒引擎和多层次主机防御系统（HIPS）这 2 个核心模块，它们在保护用户终端安全的同时，在系统中设置多层、

严密的威胁感知点，实时感知、预处理各种威胁信息，然后返送给火绒“终端威胁情报系统”。

通过前端截获、预处理，以及后端的进一步深度分析和处理，火绒 EDR 系统产出强大的威胁情报，据此来升级病毒库、各种威胁样本库，进而不断改进产品。每个火绒的终端用户，都是感知威胁的探针，同时也享受着所有客户终端产生的威胁情报的整体价值。

综上所述，每个“火绒终端安全管理系统 2.0”的用户，都享受着数千万火绒产品终端和 EDR 系统所产生的威胁情报的价值。

4、核心技术

4.1 自主知识产权的新一代反病毒引擎

自主产权的火绒反病毒引擎，历经多年艰辛打磨成熟，基于独特的“虚拟沙盒”技术，可以深度解析各类恶意代码的本质特征，有效地解决加密和混淆等代码级恶意对抗。同时，该引擎还能够实时感知静态的代码级威胁信息，以及动态的文件级威胁行为信息，是终端威胁探针的主要功能模块。

火绒引擎具有强大的通用扫描、通用脱壳和代码行为分析能力，以及轻量化设计、支持多种平台和丰富的文件格式，具有较高的解码、检出和代码修复能力。因此火绒产品拥有误报率超低、查杀速度快、体积和资源占用小等特点。

4.2 多层次主动防御系统

火绒主动防御系统率先将单步防御和多步恶意监控相结合，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。同时还能实时感知动态的系统级威胁行为信息，是终端威胁探针的重要组成部分。

该防御系统在文件、注册表、进程、网络这四个维度均设计了全面的防护规则，有效地针对操作系统的脆弱点进行防护。单步防御模块还开放了自定义规则功能，允许用户自行编写防护规则，制订适合自身需求的防御、隐私保护规则。

5、系统架构

火绒终端安全管理系统采用了业界主流的 B/S 开发模式，由控制中心、升级服务、客户端、服务器端四个模块组成了防病毒体系，能够有效拦截和清除目前泛滥的各种网络病毒，并提供强大的管理功能。

5.1 系统中心

系统中心提供了基于 WEB 方式的本地控制台。系统中心对已注册的客户端进行分组管理，可以向客户端发出指令、配置选项并提供集中的日志操作。

5.2 控制台

控制台是控制中心的可移动控制平台（基于 Web 服务架构），管理员可以通过 WEB 浏览器（IE7.0 以上）访问控制台对控制中心进行远程管理。

5.3 客户端

客户端是面向网络中的客户机而设计的病毒防护执行端，它提供了实时监控、全面查杀、病毒隔离、邮件防护及漏洞扫描等多种功能,针对可能来自软盘、光盘、网络共享及邮件、网络下载等各种途径的病毒入侵，实现全方位的病毒防护。当发现病毒时，客户端将病毒信息反馈给系统中心。客户端还能接收并执行系统中心发出的指令，按系统中心设定的策略配置选项。客户端通过系统中心指定的服务器升级，升级过程无需人工参与。当前客户端支持 Windows 操作系统与 Linux 操作系统。

5.4 升级服务

升级服务模块负责升级文件的更新与传递，客户端、控制台、系统中心均通过升级服务模块进行升级。

6、主要功能介绍

6.1 服务端功能

6.1.1 首页

该模块提供了对正在保护终端总数量和在线终端数量的统计，通过相关展示了解到企业安全情况以及信息，其中包含异常终端数量、今日防护事件次数、累计保护总天数、控制中心服务器性能、最新安全动态、终端系统统计。管理员可以通过页面展示的安全概览曲线图了解最近 7 日或 30 日的病毒风险事件统计、漏洞修复事件统计、网络攻击事件统计、系统防护事件统计等内容。方便管理员实时查看，及时对相关存在的风险进行了解和处理。

6.1.2 终端管理

管理员可通过该模块对下属已安装火绒企业版客户端的设备进行分组的创建，并对已经在控制中心管理下的客户端进行相关的任务的派发，包含病毒查杀、终端升级、发送通知、移动分组、远程桌面、同步防护策略、恢复隔离文件、终端隔离、漏洞修复、文件分发、垃圾清理、计划任务、编辑标签、资产管理、关机、重启、删除终端、加入黑名单等操作。

管理员也可通过终端管理模块中的计划任务，对相关分组或未分组的终端进行计划任务的创建，包含计划任务的类型、任务频率、执行任务类型等设置。

6.1.3 防护策略

管理员可在策略部署中查看和配置部署的防御策略，并在策略管理中对分组策略进行新建和修改，策略内容包含常规、病毒防御、系统防御、网络防御、访问控制、安全工具等。

管理员可通过信任文件模块对相关需要信任的项目进行添加信任，添加信任方式包含文件路径、文件校验和和网址等。

U 盘管理模块可针对受限制的 U 盘进行注册，通过注册的方式允许该 U 盘在环境下使用，并在注册时可对 U 盘进行访问密码设置、以及是否允许在外网使用等设置。通过此功能可有效避免病毒利用 U 盘等传输介质进行的传播，以及企业内部可能出现的信息泄露等问题。

管理员可通过终端动态认证功能配置终端的二次登录认证，该功能可有效阻止由于客户端遭到密码泄露、弱口令爆破、撞库等黑客破解行为带来的危害，达到对下属客户端保护的目的。

6.1.4 漏洞修复

该模块可以收集和统计被保护的客户端针已扫描出的高危漏洞和功能性漏洞，管理员可从控制中心对下属客户端执行统一的漏洞修复策略任务的下发，支持按终端查看和按补丁查看等方式，同时管理员可在该功能模块统一配置漏洞扫描的时机、补丁安装的先手顺序、补丁下载方式的优先级，以及补丁的缓存机制。避免威胁利用已有的漏洞进行渗透的危险。

6.1.5 资产管理

管理员可通过资产管理模块对下属管理的终端进行资产信息登记和录入的工作。

管理员通过软件统计功能了解下属管理终端所有已安装软件的明细，该功能可有效展示具体软件的安装情况，以及安装率。管理员可针对列表中出现的违规软件进行卸载操作的通知下发，及时通知下属客户端对相关软件的删除工作，该功能支持按软件统计和按终端统计等方式的查看。

系统管理模块可收集下属客户端的系统统计信息，包含操作系统版本、安装时间、激活状态、终端名称、终端分组、本地 IP，系统占比可按照已收集的信息展示相关的系统占比情况。

硬件管理模块针对下属硬件信息进行统计和收集，包含终端名称、终端分组、本地 IP、CPU、内存、硬盘、网卡、显卡、主板等，并可在硬件变更历史查看。

6.1.6 中心管理

管理员可在账号管理模块中添加相关普通管理员或审计员，针对不同的角色分配相应的权限划分，包含终端管理、防护策略、漏洞修复、资产管理、事件日志、管理工具等。

管理员可通过多级中心解决针对跨地域的超大型政企单位，以及需要严格分级管理的单位需求等问题。

管理员可通过数据备份功能配置自动备份或手动备份及导入备份的操作。

管理员可通过中心迁移功能对控制中心进行迁移工作。

管理员可通过中心设置配置相关设置选项，包含终端管理员设置、中心升级、中心地址管理、通知设置、通用设置等。

6.1.7 事件日志

管理员可通过事件日志查看相关的病毒查杀、病毒防御、系统防御、网络防御、访问控制、漏洞修复、终端管理日志、系统管理日志、数据导出管理等日志信息内容，同时提供相关日志信息的导出、自定义列及检索功能。

6.1.8 管理工具

该模块提供了管理员相关的管理工具，包含域部署工具、离线升级工具、中心迁移工具、移动存储注册工具、火绒安全 U 盘程序、专杀工具、SHA-2 代码签名补丁修复工具、Windows 终端、Linux 终端等工具的下载。

6.2 客户端功能

6.2.1 Windows 终端

1、病毒查杀

病毒查杀分为快速查杀、全盘查杀、自定义查杀等多种方式，可以由终端用户自己发起查杀；也可以由管理员从控制中心发起，并且支持修改查杀配置。

2、防护中心

可通过查看防护中心了解被保护功能和防护的状态以及开启项，包含病毒防护（文件实时监控）、系统防御（系统加固、应用加固、软件安装拦截、摄像头保护、浏览器保护）、网络防御（网络入侵拦截、横向渗透防护、对外攻击拦截、僵尸网络防护、Web 服务保护、暴破攻击防护、远程登录防护、恶意网址拦截）。

3、访问控制

可通过查看访问控制了解相关计算机内应用程序与设备使用的管控情况，包含 IP 协议

控制、IP 黑名单、联网控制、网站内容控制、程序执行控制、设备控制。

4、安全工具

客户端用户可查看和使用管理员相关已开启或允许使用的漏洞修复功能、系统修复功能等各项扩展工具，包含漏洞修复、系统修复、弹窗拦截、启动项管理、垃圾清理、文件粉碎、右键管理、断网修复、流浪监控等。

6.2.2 Linux 终端

病毒扫描

病毒扫描由管理员从控制中心发起，扫描完成后结果自动上传至中心。

7、技术参数

7.1 服务端配置要求

- 硬件要求：
- Windows 版本（暂不支持 Linux/Unix/Mac 版本）：
  - Windows XP（SP3）、Windows Vista、Windows 7、Windows 8、Windows 8.1、Windows 10
  - Windows Server 2003（SP1 及以上） /2008/2012/2016
- 包含 32 位以及 64 位
- 内存：至少 2GB
- 硬盘：建议 60GB 以上
- 网卡：具备以太网兼容网卡，支持 TCP/IP 协议
- IE 支持：支持 IE8 及以上
- 是否支持虚拟机：支持

7.2 客户端配置要求

7.2.1 Windows 终端

- 系统版本：支持版本与服务端相同
- 内存：至少 1GB
- 硬盘：建议 40GB 以上
- 网卡：具备以太网兼容网卡，支持 TCP/IP 协议
- 是否支持虚拟机：支持

7.2.2 Linux 终端

- 系统版本：支持 CentOS、Ubuntu、SUSE、Deepin 等发行版，仅支持 64 位
- GNU libc：2.12 及以上
- 内存：至少 1GB
- 硬盘：建议 40GB 以上
- 网卡：具备以太网兼容网卡，支持 TCP/IP 协议
- 是否支持虚拟机：支持