火绒终端安全管理系统
1.0 版

技术白皮书

版权声明

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 B 座 1201 室

网　　址：http://www.huorong.cn

技术支持：010-84905882

目录

1 概述

欢迎阅读《“火绒终端安全管理系统 1.0”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 1.0”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 1.0”的安装需知和部署流程，请参阅《“火绒终端安全管理系统 1.0”安装部署手册》。
- 如果您是初次体验“火绒终端安全管理系统 1.0”，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 1.0”使用手册》。
- 如果您想了解“火绒终端安全管理系统 1.0”产品的详细介绍，请参阅《“火绒终端安全管理系统 1.0”产品说明书》。

2 产品

2.1 产品介绍

“火绒终端安全管理系统 1.0”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 1.0”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百万“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 1.0”用户，都随时享受着数百万互联网威胁探针（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 4 年运营经验，服务数百万用户，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 1.0”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 1.0”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 1.0”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 1.0”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百万“火绒安全软件”终端为基础。“火绒终端安全管理系统 1.0”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 1.0”的用户，都享受着数百万火绒产品终端和 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 6 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。

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终端管理

在该模块，管理员可以了解所有终端的安全情况以及信息，对终端进行统一的管理防护。并且可以对指定终端下达快速查杀、全盘查杀、终端升级等安全防护任务。

6.1.2文件管理

在该模块，管理员可以查看所有终端的软件安装情况，并可以要求终端卸载软件；而且，该模块还为管理员提供了文件下发功能，管理员通过该模块，可以向指定终端推送安装某些软件或许下发某些文件。

6.1.3策略管理

在该模块，管理员可以查看所有终端分组采用的策略情况，以及为指定的终端分组进行策略的部署。

6.1.4漏洞管理

在该模块，管理员可以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。

6.2 客户端功能

6.2.1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。

6.2.2恶意行为分析

开启恶意行为监控功能，通过监控程序运行过程中是否存在恶意操作来判断程序是否安全，从而可以作为传统特征查杀的补充，极大提升电脑反病毒能力。

6.2.3邮件监控

开启邮件监控后，在邮件收发的过程中，对邮件进行快速扫描，及时发现风险，保护邮件安全。

6.2.4黑客入侵拦截

开启黑客入侵拦截后，软件将检测您通过网络传输的数据包中是否包含敏感入侵信息，从而一定程度上避免您的电脑遭到黑客入侵。

7 技术参数

7.1 服务端配置要求

硬件要求：

CPU: 1GHz 及以上(32 位或 64 位处理器）

内存: 1GB 及以上（32 位）或 2GB 及以上（64 位）

操作系统要求：

Windows 7；Windows 8；Windows 8.1； Windows 10；

Windows Server 2008；Windows Server 2012；Windows Server 2016；

7.2 客户端配置要求

操作系统要求：

Windows XP SP2 以上；Windows Vista；Windows 7；Windows 8；Windows 8.1；

Windows 10;