火绒终端安全管理系统
1.0 版

解决方案

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”解决方案》。为了能够更好的服务于用户，特别编写本解决方案。本方案是针对目前企事业单位终端安全出现的问题、不足、缺陷、需求等等，提出的整体解决方案。通过本方案可以全面的了解“火绒终端安全管理系统 1.0”产品的理念策略，设计架构及核心技术。专业、有效的保护单位终端设备和数据的安全。

“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用户在目前互联网威胁环境下的电脑终端防护需求。

1.1. 应对策略

“火绒终端安全管理系统 1.0”依靠 EDR（终端、检测和响应）运营体系，以遍布互联网的数百万“火绒安全软件”为基础，实现“情报驱动安全”理念。“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动防御系统（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“火绒终端安全管理系统 1.0”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。

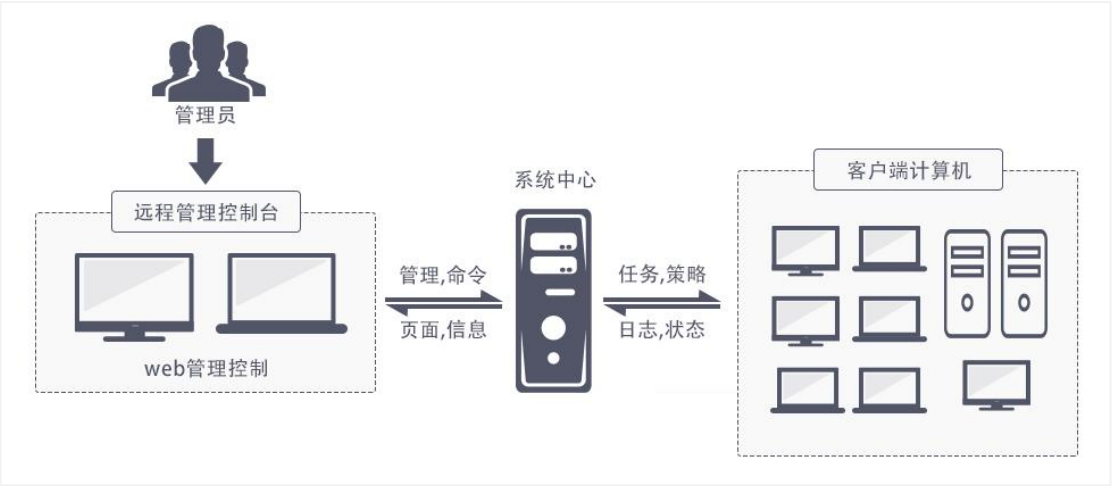
2. 安全理念

“火绒终端安全管理系统 1.0”产品和服务秉承“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. 火绒终端安全管理系统设计

3.1. 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。

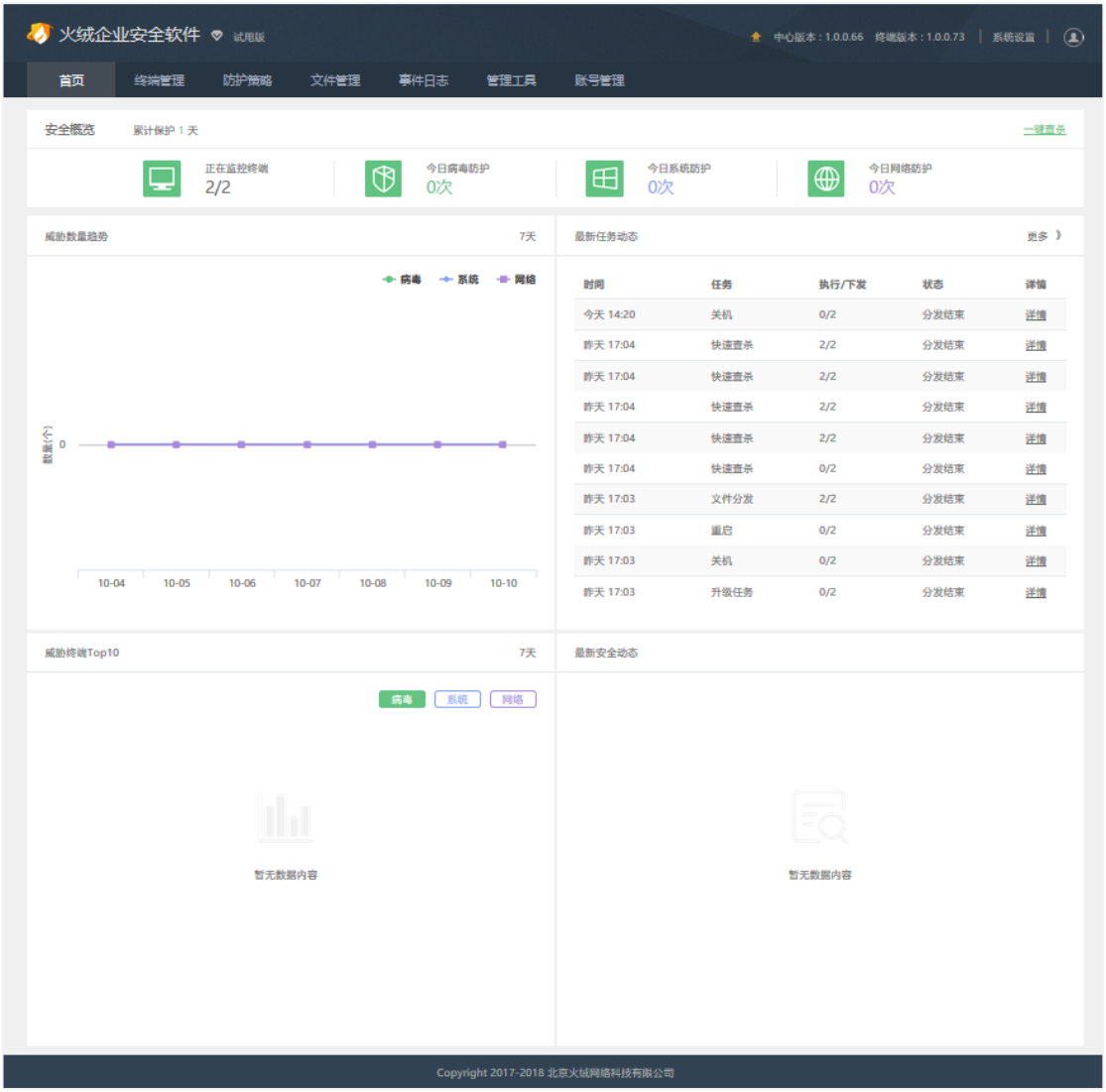


3.1.1 系统中心

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。

3.1.2 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。



3.1.3 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。

3.1.4 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。

3.2. 设计实现

火绒终端安全管理系统主要从服务端功能以及客户端功能进行统一管控。

3.2.1 服务端功能

3.2.1.1 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。

3.2.1.2 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。

3.2.1.3 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。

3.2.1.4 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。

3.2.2 客户端功能

3.2.2.1 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。

3.2.2.1 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。

3.2.2.1 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。

3.2.2.1 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。

4. 火绒终端安全管理系统的技术特点

4.1 自主研发反病毒引擎

拥有自主知识产权的新一代反病毒引擎，可以通过高效的虚拟沙盒、通用壳等技术，深度解析病毒本质特征，在全面查杀病毒、木马和流氓软件的同时，保持超低误报率，为用户提供最全面、立体的安全防护。

4.2 高效的防御监控功能

HIPS 模块将单步防御和多步监控相结合，自上而下地在所有可能的威胁入口设计了独特的防御策略，拦截各种危险行为和恶意网址，且不依赖白名单，消除信任漏洞，不卡机，资源占用低。

4.3 有效阻断灰色软件

软件安装拦截能够有效阻断流氓软件安装。

4.4 Web 管理平台

控制台使用 Web 交互方式，界面友好、直观，符合用户的使用与操作习惯，无需任何培训即能轻易应用自如。管理员无需安装额外的控制软件，只要在任意一台装有浏览器的计算机上，即可轻松实现对整个网络的管理。

4.5 简便的安装部署

支持域脚本安装等方式，在较短的时间内完成网络内部署众多客户端的安装作业，简单快速的实现整个网络反病毒体系的部署。

4.6 高安全性通讯

支持 HTTPS 加密通讯，数据传输更安全。

附：公司简介

火绒成立于 2011 年，长期专注于终端安全领域，潜心研发引擎等底层技术，秉承“情报驱动安全”理念，率先构建完成 EDR（终端、检测和响应）运营体系，逐渐开始领跑终端安全领域。火绒安全 2012 年发布的“火绒安全软件”是一款免费个人电脑安全软件，经过数年口碑相传，积累了以技术人员、专业人士、意见领袖为主的数百万用户。被认为是最纯粹的安全软件，以功能强悍、无流氓行为、占用资源少赢得了良好的口碑。“火绒终端安全管理系统 1.0”是火绒推出的第一款商业化产品，标志着火绒正式进军企业级市场。