# 火绒安全亮相中国石油和化工企业网络

2023年2月22-23日，“中国石油和化工企业网络与信息安全技术峰会”在北京召开。会上，来自中国石油、中国石化、中国海油、国家管网等集团网络安全主管与技术专家、科研院所知名专家和学者、网络安全公司代表等共500余位嘉宾参加了大会。火绒安全作为终端安全领域的行业专家受邀出席。


## 网络连接到哪里，网络安全问题就延伸到哪里

石油化工企业产业链条长、覆盖面广，每个板块又拥有各自的业务特点，因此在推进产业数字化转型大背景下，网络安全系统防护是庞杂的，涉及网络安全、终端安全、数据安全、云安全、工业互联网安全等多方面建设。

中国石油化工企业认为：网络连接到哪里，网络安全问题就延伸到哪里；哪里有信息系统，哪里就有网络安全问题。在石油化工行业面临诸多安全风险与挑战中，“ 连接宽泛 ”便是其中一点。智能应用的推广使得网络连接面增大：木桶短板效应凸显，广域网安全不容小觑；连接分布广泛，监测盲点问题突出；终端类型繁多，终端管理难度大。

## 从终端打造企业信息安全的“ 金钟罩 ”

大会上，火绒安全实验室高级研究员发表了《从终端入手，打造企业信息安全的“ 金钟罩 ”》的主题演讲，从企业终端常见安全困境出发，剖析内部环节潜在风险，讲述火绒安全如何为企业打造稳固的终端安全管理防线。


火绒安全看到，大多数企业终端面临三个主要安全困境。一是终端病毒难杀尽。企业在查杀过程中，由于担心文件被清除，即使发现病毒也“ 不敢杀 ”或“ 查杀不彻底 ”，导致病毒四处扩散。二是黑客猖獗，攻击频繁。除了黑客团伙自身规模化外，企业内部脆弱点遍布网络、系统、

应用之中。三是人员和设备难管控。企业内部网络环境复杂、设备类型复杂多样，即便日常所用U盘，都处处存在安全风险。

## 精准查杀

火绒安全产品强大的杀毒能力，源于核心自主研发技术——火绒反病毒引擎。引擎基于独有的高仿真“虚拟沙盒”环境，部署“通用脱壳”和“动态行为查杀”两大技术，可以戳穿病毒的任何“伪装”，有效识别已知病毒的新变种，以及未知病毒，做到高查杀、低误报。

火绒安全对病毒类型和名称的准确识别，可直接帮助管理员对问题精准定性，及时采取有效的针对措施；对于“不敢杀”的感染型病毒、宏病毒做到准确剥离，还原用户原始文件，用户对病毒文件可以“大胆查杀、放心查杀”。

## 纵深防御

单一技术手段不足以在当今网络攻击中赢得胜利，只有综合多种防御技术的解决方案才能在百变的威胁环境中胜出。火绒安全“多层次主动防御系统”贯彻了综合防御的理念，通过组合多种防御技术，在所有可能的威胁入口设计了独特的防御策略，共同有效防御不同类型的恶意威胁。

## 统一部署

企业产品“火绒终端安全管理系统”支持软硬件资产登记、漏洞与补丁管理、多级中心管理、灵活定制分组策略等，实时显示企业全网安全动态、病毒威胁等信息，通过“安全分析报告”辅助管理者随时掌握全部动态。


终端安全作为网络安全综合防护建设的重要一环，火绒安全将持续助力石油化工企业构建完善全方位、立体化的网络安全防护体系，筑牢网络安全防线，增强企业数字化转型中的网络安全保障能力。

本文链接：https://dqcm.net/zixun/167714689910220.html