

360 终端安全用户案例

神华集团

© 2016 360 企业安全集团

■ 版权声明

本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明外，所有版权均属 **360 企业安全集团** 所有，受到有关产权及版权法保护。任何个人、机构未经 **360 企业安全集团** 的书面授权许可，不得以任何方式复制或引用本文的任何片断。

1. 神华集团

摘要：神华集团作为国际领先的综合性大型能源企业，拥有众多分公司、子公司，甚至多级子公司，如何做好终端安全的统一管理一直以来都是神华集团信息安全的工作重点之一。360 天擎终端安全管理系统为神华集团提供了国际领先的未知威胁检测能力，博古通今的病毒防御能力、高效可控的终端管理能力，助力神华集团全网终端统一安全管理，全面提升了神华集团信息安全建设水平。

近年来，神华集团信息化建设快速推进，新的系统和 IT 基础设施不断上线，IT 系统的种类和规模日益扩大。但与此同时，互联网上各种木马、病毒、0day 漏洞，以及类似 APT 攻击这种新型的攻击手段也日渐增多，病毒的制造技术也在不断发展和更新，传统的单纯依靠病毒特征的病毒防御技术以及安全管理手段已经无法满足现阶段计算机安全的需要。因此，神华集团急需构建全新的终端安全管理系统，以应对当前严峻的信息安全形势。

构建一体化防病毒及终端管理系统

神华集团各下属单位网络基本为自建且自行运维，但同时又与总部互联互通，总部对下属单位没有管理权，因此，需要建神华集团统一防病毒体系、统一计算机安全管理体系，以提高整个企业网络安全的水平，避免短板出现。在整个体系中需要包含终端病毒防护以及终端管理。

360 天擎终端安全管理系统实现了病毒查杀、病毒库更新、病毒防控等基本安全策略的统一分发和管理。各下属单位可根据自身需求，在集团安全基线的基础上自定义本单位的防病毒策略。通过统一防病毒体系，实现全集团计算机病毒的可视化管理，掌握计算机病毒在集团内部的动态，及时响应上级单位的有关防毒策略、补丁策略等。

与此同时，360 天擎终端安全管理系统实现了非法外联管控、补丁检测与防护、XP 系统安全防护、软硬件管控、准入控制等，并及时、有效地管理和处置各种违反集团公司终端安全策略的事件；通过统一安全管理体系，结合企业组织架构模型，可持续改进日常安全运维流程、提高信息安全管理水平，整体提高神华集团的计算机安全管理水平。

神华集团整体终端安全管理系统的构建具备以下特点：

➤ 技术先进性

系统所采用的技术应具有先进性，符合当前技术和管理发展的方向，具有国际 PCT 专利的防病毒引擎更是为神华集团提供了全球领先的病毒防御能力。

➤ **系统稳定性**

系统具备长期、稳定运行的能力，并具有良好的兼容性，在一定程度事件或灾难发生时，仍能保证防病毒及安全管理系统不间断运行。即使网络终端，亦不影响安全防御能力。

➤ **整体安全性**

系统建设采用全面的安全防范技术和措施，能够保障平台信息和数据安全，能够保障系统的长期、稳定、可靠运行。

➤ **平台标准化**

系统采用符合国际、国家标准的软件、应用，遵循有关技术规范体制，系统具有灵活的互联能力。

➤ **系统扩展性**

系统充分考虑了神华集团未来业务和技术发展的需要，具有功能扩展的灵活性和跨平台的可移植性，在有扩展需要时，能够快速、平稳地实现应用规模的扩展和技术升级。

通过部署 360 天擎终端安全管理系统，神华集团成功构建了统一的终端安全管理体系，满足了神华集团安全性、合规性以及全集团统一管理的需求。360 天擎使用国际领先的病毒防御技术，辅以高效可控的终端管理手段，全方位解决神华集团内网终端安全管理建设，助力神华集团提升整体安全防御能力。