Neusoft东软®

东软 NetEye 终端安全管理系统（EDR）

下一代终端安全解决方案

概述

终端安全往往被理解为杀毒软件，于是公司企业从终端安全厂商那里买来软件，然后让 IT 运营员工负责照管这些杀毒软件——任务完成，终端安全！

但刚刚过去的几年里，这一情况发生了很大改变。因为出现了针对性攻击、无文件恶意软件和勒索软件，传统基于签名特征来防护的产品难以发挥作用，取而代之需要以威胁预防、检测和响应上的新技术来满足不断变化的企业安全需求。

东软 NetEye 适时推出面向泛终端安全防护产品——东软 NetEye 终端安全管理系统（东软 EDR），帮助用户解决多形态 IT 资产一体化安全防护需求。

泛 IT、多云的安全问题

- **多种形态 IT 资产并存**

  传统硬件、虚拟化、私有云、公有云及多云并存。

- **统一运维及一体化安全部署的需求**

  IT 分布在不同的地理位置，需要集中统一运维。对于安全而言，同样需要安全策略集中下发，全网统一管理。

产品价值

东软 NetEye 终端安全管理系统以 PPDR 安全模型动态安全体系为基础，以 AI 大数据技术为支撑、通过云网端联动协同、 威胁情报共享、多层级响应机制， 帮助用户快速处置终端安全问题，构建下一代终端安全系统，能够精确检测已知病毒木马、未知恶意威胁，有效防御 APT 攻击，勒索病毒，并提供终端资产管理、漏洞补丁管理、安全运维管控、软件管控等多功能。

- 终端资产统一盘点

终端资产的全面盘点，包含业务服务器的终端和用户 PC 的终端，虚拟机，云端服务器，工控机，云桌面等。盘点每台终端设备的名称、IP 地址、MAC 地址、所属组织、责任人、资产编号、资产位置等。每一台的终端上的资产信息清晰，每一个安全事件责任到人，使得安全管理能落实到位。

- 多维度恶意软件检测

传统的终端防病毒检测技术使用特征匹配，使得病毒特征库越来越大，运行所占资源也越来越多。东软终端安全产品使用多维度轻量级的多特征检测技术，包含 AI 技术引擎、行为引擎、云查引擎、全网信誉库等，检测更智能、更精准，响应更快速，资源占用更低消耗。

- 勒索病毒防御

通过加密文件索要赎金的勒索病毒攻击方式越来越流行，东软终端能够非常精准的识别不同的勒索软件家族，并通过专业分析识别出种种勒索病毒感染行为和加密特征，对最新的勒索软件进行有效的查杀，防止用户感染最新

的勒索软件。

- 微隔离技术

传统的安全设备无法管控东西向流量，内网威胁传播路径无法可视化，东软终端安全产品提供基于代理形式的微隔离方案，使得端点安全可视可控，精细化微隔离，简单落地，高效运维大大降低威胁影响范围。

- 多产品安全协同

该产品能与东软安全网关，东软安全运营管理平台，东软日志审计系统，上网行为管理等产品进行产品进行协同联动响应，关联在线数安全设备的反馈威胁情报数据，智能分析精准研判，超越传统的黑白名单和静态特征库，为已知未知威胁检测提供有力支持。

技术原理

- 多维度智能检测

终端上的安全检测是核心的技术，传统的病毒检测技术使用特征匹配，使得病毒特征库越来越大，运行所占资源也越来越多。EDR 产品使用多维度轻量级的无特征检测技术，包含 AI 技术引擎、行为引擎、云查引擎、全网信誉库等，检测更智能、更精准，响应更快速，资源占用更低消耗。。

- 云查杀

针对最新未知的文件，使用微特征的技术，进行云端查询。云端的安全运营中心，使用大数据分析平台，多引擎扩展的检测技术，秒级响应未知文件的检测结果 。

- 无文件攻击检测

传统网络攻击者利用恶意软件访问受害者的电脑（通常会利用软件漏洞或诱骗这种方法的问题在于易被反病毒解决方案检测。随着攻防形势的变化，越来越多的黑客利用 PowerShell 或 WMI 等无文件攻击方式进行恶意活

动，占比逐年升高。 针对无文件攻击，涉及反射 DLL 注入 、Exploit 攻击内存利用、PowerShell 脚本命令执行东软 EDR 产品通过增强型对内存扫描技术和行为监控来检测无文件攻击行为，及时发现这类的攻击。

➢ 基于微隔离技术东西流量访问控制

微隔离方案提出了一种基于安全域应用角色之间的流量访问控制的系统解决方法，提供全面基于主机应用角色之间的访问控制，做到东西流量的可控和可视化，集中统一管理服务器的访问控制策略。基于 EDR 轻量级主机 Agent 实现的微隔离实现，不受虚拟化平台的影响，不受物理机器和虚拟机器的影响。

利用应用角色之间的主机流量访问控制的技术，提供对业务安全域之间、业务安全域内不同应用角色之间、业务安全域内相同应用角色之间的访问控制策略配置，提供简单可视化的安全访问策略配置，提高了安全管理的效率。

➢ 技术参数

指标型号	NESM3000
机箱规格	1U
标配接口	6 千兆电口；1 个扩展槽位；2 个 USB 接口；
电源	交流单电源
存储介质	1T 硬盘；8G 内存
支持终端数量	不低于 20 个
支持系统	Windows 操作系统　linux 操作系统

沈阳东软系统集成工程有限公司

服务电话：400-655-6789

E-mail：servicedesk@neusoft.com