咨询电话：4006556789

http://neteye.neusoft.com

Neusoft

东软NetEye

因需而变 因御而安

Network Security Professionals

全球领先的网络安全产品及服务供应商

Contents
目录

走进东软

About us

东软价值观

简单、负责、合作、尊重、诚信

东软的历史

从在大学校园教室里开始创业到中国最大的IT解决方案与服务提供商

东软来自于大学。

为了寻求"架设软件研究与应用桥梁"的梦想开始创业。

1991年，东软创立

1996年，成为中国第一家上市的软件公司

2001年，在中国众多的行业领域获得领先的市场份额，向IT解决方案与服务供应商发展

2005年，成为中国最大的离岸软件外包提供商

2008年，东软集团整体上市计划完成

经过28年的努力，

如今，东软已经成为中国最大的IT解决方案与服务提供商。目前拥有近20000名员工在中国建立了8个区域总部，10个软件研发基地，16个软件开发与技术支持中心，在60多个城市建立营销与服务网络，3所东软信息学院。在美国、日本、欧洲、中东、南美设有子公司。

东软的业务

医疗健康与社会保障领域包括： 医疗信息化、临床深化产品、医疗创新业务、医疗大数据、医疗运营及生态价值链管理、医疗保险管理、人力资源和社会保障、医疗设备、健康服务等。

智能汽车互联包括： 汽车电子、智能终端、车载信息安全等自有产品；高级辅助驾驶系统和自动驾驶辅助系统产品线、新能源汽车产品线等。

智慧城市包括： 智慧云城市、智能互联设备、智慧政务系统、物联网链接平台；智慧能源、智慧金融业务、智慧教育、智慧交通等信息化解决方案等。

企业互联及其他包括： 企业信息化、电子商务；网络安全；基于云计算、大数据、物联网的知识资产及产品；业务流程外包（BPO）；IT基础设施建设与服务等。

东软NetEye

作为中国网络安全行业的领导厂商，东软NetEye1996年成立，连续多年保持稳健成长。面对云计算、移动互联网、物联网、大数据、关键基础设施等新技术应用的快速发展和市场需求的不断变化，云安全支付网关、物联网安全、自主可控国产芯片安全网关、160G数据中心防火墙、虚拟安全网关、桌面型无线安全网关、汽车电子安全、预警威胁管控平台等一系列创新产品因需而生，在政府、金融、能源、电信、医疗、交通及大中型企业中得到良好应用。

秉承多年的专业技术经验积累，东软持续为用户提供成熟、先进的网络安全产品以及高效、完善的安全解决方案与服务，努力将东软NetEye打造成为全球领先的网络安全产品及服务供应商。

History

发展沿革

2002-2004

- 东软NetEye北京信息安全实验室成立，承担国家技术创新计划，负责研发基于流过滤技术的防火墙系统；
- 承担国家千兆线速防火墙系统研发项目；
- 成功通过国家联动式信息安全集成系统的产业化示范工程项目验收。

2009-2012

- 承担国家下一代互联网高性能流量深度净化与控制系统及管理型信息安全运维与应急服务研发项目；
- 荣获国家首批信息安全产品自主原创资质、首批风险评估服务一级资质、首批国家信息安全漏洞共享平台（CNVD）技术支撑单位。

2015-2016

- 发布160G数据中心高性能防火墙、云计算安全解决方案、桌面级安全网关等新产品；
- 携手龙芯中科发布首款国家级认证的自主可控千兆防火墙产品，并已获得销售许可证和涉密产品资质；
- 成立车载信息安全产业联盟，发布国内第一款车载信息安全解决方案；
- 东软NetEye防火墙产品通过第二代防火墙安全技术要求测试，获得公安部第二代防火墙销售许可证；
- 成为国家云安全标准、国家智慧城市整体规划标准起草单位。

1996 -2002年 | 2002-2004年 | 2005-2008年 | 2009-2012年 | 2013-2014年 | 2015-2016年 | 2017-2018年

1996 -2002

- 承担国家“九五”公关重点科研项目，率先研发具有信息分析功能的防火墙；
- 发布FW1.0版本防火墙并实现产业化生产；
- 在防火墙领域最早实现状态监测技术；
- 发布安全操作系统NOS、“流过滤”专利技术。

2005-2008

- 荣获中国信息安全认证中心颁发的首批“信息安全服务一级资质”；
- 承担国家基于FPGA芯片的主动式防御千兆线速防火墙系统产业化和入侵防御系统与防拒绝服务产品研发项目；
- 承担国家高性能UTM产品产业化项目和网络威胁防御管理系统、国家电信级防火墙、高性能异常流量分析过滤监控系统产业化研发项目；
- 因在2008年奥运安保中出色的应急安全服务，国家计算机网络应急技术处理协调中心授予“突出贡献奖”。

2013-2014

- 东软NetEye万兆集成安全网关NISG（IPV6版）获得国家网络安全测评信息技术产品安全测评EAL3级证书，成功入选国家发改委下一代互联网网络安全专项UTM类产品目录；
- 连续五年入选国家计算机网络技术处理协调中心“国家级网络安全应急服务支撑单位”。

2017-2018

- 发布东软NetEye业务安全网关；
- 东软智能网联车载信息安全平台系统获中国网络安全产业联盟颁发“2018年网络安全创新产品奖”、获中国信息协会颁发“2017-2018年度新一代信息技术优秀解决方案奖”、东软车载信息安全解决方案S-Car获“中国网络信息安全市场年度创新产品奖”；
- 东软云安全产品获“中国网络信息安全市场年度创新产品奖”；
- 东软NetEye海外市场业绩快速增长并入围国际安全研究机构Frost&Sullivan日本市场新锐品牌；
- 东软连续七届获得CNCERT/CC网络安全应急服务支撑单位（国家级）；
- 参与《国家SM专用设备自主可靠产品》、《汽车电子系统网络安全要求》、《云计算参考架构》、《智慧城市安全体系框架》、《信息安全产品类别与代码》、《北京市卫计委行业信息安全现状研究报告》、《信息安全技术　健康医疗信息安全指南》、汽车信息安全蓝皮书等国家标准及行业标准课题的起草与修订工作。

Partner

并肩同行

SIPO 国家知识产权局
中国移动通信 CHINA MOBILE
中国农业银行 AGRICULTURAL BANK OF CHINA
中国石油
国家保密局 National Administration of State Secrets Protection
中华人民共和国环境保护部 Ministry of Environmental Protection of the People's Republic of China
中国建设银行 China Construction Bank
中华人民共和国工业和信息化部
AIR CHINA 中国国际航空公司
中国人民银行
中国商飞
北京地铁 beijing subway
深圳航空 Shenzhen Airlines
CNCERT/CC 国家互联网应急中心
公安部
中国交通部
CSSC
HUAXIA BANK 华夏银行
中国南方电网 CHINA SOUTHERN POWER GRID
中国电信 CHINA TELECOM
中国联通 CHINA UNICOM
深圳地铁 SHENZHEN METRO
国家信息中心 State Information Center
东北大学 Northeastern University
中国地震局 CHINA EARTHQUAKE ADMINISTRATION
中国铁建
中国科学院 CHINESE ACADEMY OF SCIENCES
中国烟草 CHINA TOBACCO
中国证券监督管理委员会 CHINA SECURITIES REGULATORY COMMISSION
Haier
中投集团
成都国泰制药
阿里云
上海机场集团 SHANGHAI AIRPORT AUTHORITY
CNSG 中盐集团
国家电网公司 STATE GRID CORPORATION OF CHINA
中国电力投资集团公司
北京医院 BEIJING HOSPITAL
1904
五粮液 WU LIANG YE
新华社 XINHUA NEWS AGENCY
步步高
Bank 中国光大银行

东软安全大数据

东软NetEye产品及解决方案分别在政府、航空、金融、能源、交通、医疗、社保、教育及大中型企业中广泛应用，客户遍布全国各地。

为13亿+ 中国人口数据库提供安全防护

为10亿+ 中国医疗患者的安全就诊提供保障

为 5亿+ 航旅用户安全护航

为3亿+ 中国电信用户的安全通信提供保障

为2亿+ 中国金融用户的安全交易提供保障

金融

中国人民银行、中国工商银行、中国农业银行、中国建设银行、招商银行、中国光大银行、华夏银行、商业银行、兴业银行、中国外汇交易中心、中信实业银行、东方证券、民族证券、联合证券、华安基金、华夏基金、华夏保险、深圳联合证券、中国人保、中投、兴业证券、国海证券……

能源

国家电网有限公司、中国南方电网有限责任公司、中国石油天然气集团有限公司、中国石化集团公司、北京电力、辽宁电力、吉林电力、内蒙古电力、西藏电力、江苏电力、浙江电力、湖南电力、山东电力、山西电力、江西电力、安徽电力、广东电网、广西电网、四川电力、云南电网、贵州电网、北京市电力公司电力科学研究院、北海电厂国投北部湾发电有限公司、深圳供电局有限公司、沈阳电业局……

政府

国家发改委、中国证监会、中国公安部、中国海关、农业部、民政部、中国环境保护部、国家广电总局、中国地震局第二监测中心、中央人民政府驻香港特别行政区办公室、国家科委、国家旅游局、国家信息中心、国家知识产权局、中央机构编制委员会办公室、上海公安局、上海安全局、江苏省委机要局、江苏省林业局、辽宁公安厅、吉林省人民政府、吉林省国土资源厅、吉林省监狱管理局、广西省高法、云南省劳动厅、湖北省交通厅、湖南省民政厅、江西省教育厅、安徽省地方税务局、安徽省公安厅交警总队、安徽检察院、福建省委、福建省财政厅、福建省环境信息中心、福建省国家税务局、福建省纪律检查委员会、陕西省人民检察院、浙江省纪律检查委员会、上海宇航系统工程研究所、沈阳市纪律检查委员会、呼和浩特市卫生和计划生育委员会、赤峰市食品药品监督管理局、武汉市公安局、济南市国土资源局、烟台市机要局、烟台市财政局、南昌市政府信息中心、成都市规划信息技术中心、成都市网络新闻信息中心、大庆市环境保护局、大同市国家保密局、宁波市经信委、中共江门市市委、广东省四会市财政局、咸阳市政府信息化办公室、榆林市住房和城市建设局、北海市就业局、苏州审计局、马鞍山市中级人民法院、杭州市中级人民法院、长沙市政法委、长沙市公安局、福州市不动产登记和交易中心……

军队

武警总队、总后营房部、总后司令部、总装司令部、总装驻京单位、总参二部、总参廊坊导弹学院、中央警备局、南海舰队、上海警备区司令部、江苏省军区、新疆武警边防总队、广州军区、南京军区、武汉后方基地、葫芦岛海军基地、战役后勤指挥作业车组、中国人民解放军第某军工厂、安徽军工集团控股有限公司……

教育

中国科学院、北京理工大学、东北大学、大连理工学院、北京航空航天大学、中国医科大学第二临床学院、徐州矿业大学、西安试飞学院、兰州交通大学、福建中医学院、浙江水利水电专科学校、甘肃农大、陕西师范大学、湖南省教育厅、中南大学、河北广播电视大学、安徽农业大学、福州大学……

社保

南京市人力资源和社会保障信息管理中心、广州市人力资源和社会保障信息中心、新疆兵团社保局、衢州市人力资源和社会保障局、长兴县人力资源和社会保障局、天水市人力资源和社会保障局、邢台市人力资源和社会保障局、马鞍山市住房公积金管理中心、湘潭市住房公积金、淮北市住房公积金管理中心、云南省医保中心、郑州医保……

运营商

中国移动通信、中国电信、中国卫通、中国网通、北京电信、辽宁电信、浙江电信、广东电信、福建移动、浙江邮电、长沙电信、济南电信、杭州电信、南宁电信、辽宁联通、安徽联通、南京联通、新疆联通、黑龙江联通、辽宁网通……

企业

阿里云、中电投信息技术有限公司、中国盐业集团有限公司、华能集团、中国广核集团有限公司、大唐集团、中国华电集团公司、华润新能源、北京航空食品有限公司、四川长虹、海尔集团、美菱集团、春兰集团、TCL 集团、跃进集团、一汽集团、LG 集团、步步高集团、五粮液集团、西门子、高路华集团、新华锦集团、安踏(中国)、北汽福田汽车……

医疗

北京医院、中日友好医院、天坛医院、解放军第一零五医院、北京大学首钢医院、上海市仁济医院、上海市第五人民医院、四川省人民医院、山西医科大学附属第二医院、云南省肿瘤医院、陕西省第四人民医院、山东省皮肤病医院、沈阳市第六人民医院、银川市第一人民医院、郑州大学第二附属医院、济南千佛山医院、苏州第一人民医院、石家庄第三人民医院、邯郸市第一医院、浙江省台州医院、泸州医学院附属医院、宜昌市第二人民医院、曙光医院、上海市第一妇婴保健院、上海市闵行区卫计委、重庆开县人民医院、遵义医学院附属医院……

航空

中国国际航空股份有限公司、中国东方航空集团有限公司、南方航空股份有限公司、深圳航空有限责任公司、山东航空股份有限公司、上海航空股份有限公司、厦门航空股份有限公司、济南国际机场、上海市虹桥国际机场公司、厦门机场股份公司、中国商用飞机有限责任公司……

交通

中铁二十局集团有限公司、中国铁路广州局集团、广深铁路股份公司、中国船舶及海洋工程设计研究院、中国船舶重工集团公司第七一一研究所、浙江省交通运输科学研究院、北京地铁、深圳地铁、沈阳地铁、大连地铁、长春地铁……

烟草

浙江烟草、山西烟草、甘肃烟草、辽宁烟草、天津烟草、福建中烟工业公司、厦门烟草工业有限责任公司、龙岩烟草工业有限责任公司、龙岩金叶复烤有限责任公司……

东软 NetEye 防火墙

产品概述

在云计算、物联网空前发展的今天，流量的产生与交互量突飞猛进。此时，高性能、高可靠的防火墙显得尤为必要。东软NetEye防火墙系列产品具有业界领先的高性能、强大的高可靠保障、全面的安全防护功能、灵活的网络适应性等特性，不仅能够为您的各类网络边界提供有力的安全保障，而且能够为对外业务稳定、持续、高效运行保驾护航，是您在构建网络安全体系时的不二之选。

技术亮点

高性能、小空间、低功耗 获得性价比最高的安全保护

160G　80G　5000万

单板三层吞吐性能高达160G。
最高IPS检测能力高达80G。
最高并发5000,0000。

单板接口密度最高可达32口，更节省空间。

160G三层吞吐功率仅为760W，更节能。

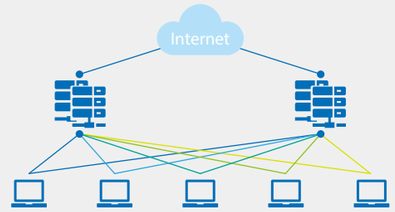
云安全中心联动 大幅提升检测能力，有效应对未知威胁

东软提供强大的云安全中心，允许用户提交可疑文件及URL至云端检测，全面应对未知威胁。

云安全中心通过人工智能手段，综合分析全球在网设备上传的大量数据，形成多种信誉库与特征库。

您可从云端同步信誉库和特征库到本地，大幅度提升设备在本地的检测能力和速度。

电信级高可靠 获得最稳定、持续的保护



HA　设备级、部件级、链路级、接口级逐级高可靠设计，更稳定。

灵活、安全的VPN解决远程连接的安全性问题

IPSec VPN、SSL VPN和GRE VPN三合一，支持多种部署方式，选择更灵活。

自主研发的VPN客户端，支持多种操作系统，方便又安全。

支持多重认证方式，支持国密办加密算法和国际通用加密算法，数据安全无懈可击。

极强的网络适应性 可按照需求随心部署

支持多种方式接入网络，满足绝大多数部署需求。

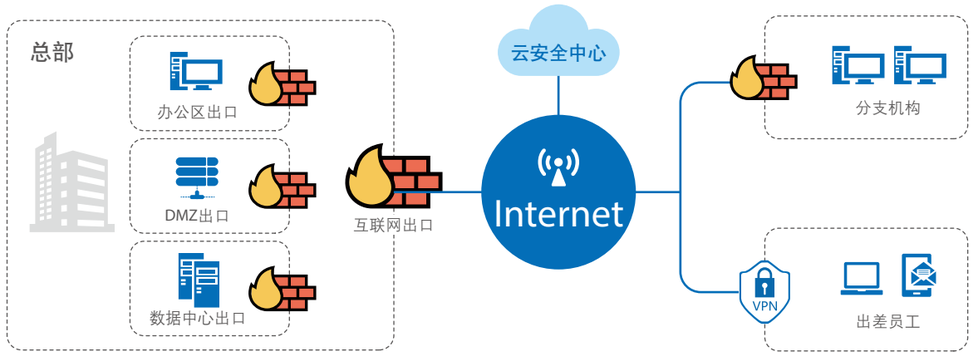
智能的路由选路，丰富而灵活的接口组合，不惧网络环境变化。

IPv6　全面支持IPv6，自如应对IPv6安全挑战。

智能高效管理 减轻管理员负担，降低运维成本

支持智能学习、智能路由、基于智能客户端的监控等一系列功能，极大地减轻了管理员的负担，提升了工作效率，降低了运维成本。

应用场景



东软 NetEye 集成安全网关

产品概述

东软NetEye集成安全网关（NISG）系列产品，是面向应用的智能化第二代防火墙。NISG具备精细的应用识别与控制能力和智能化的带宽管控技术，能够有效管理上网行为，优化用户网络带宽资源，保障用户业务的安全。通过全方位一体化的多项尖端安全技术，NISG可以抵御二层到七层的网络攻击，降低敏感信息泄露的风险，为用户网络排除“内忧外患”。

产品亮点

全方位、一体化安全防护，阻断更多威胁

- 一机多能，集传统防火墙功能与多种安全功能于一身，简化部署，减少投资。
- 全面抵御二至七层攻击威胁，保证关键业务安全。
- 特征库自动升级，防范最新漏洞、蠕虫和垃圾邮件等威胁。

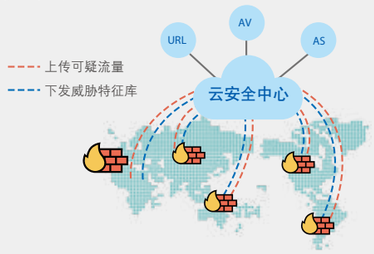
精细的上网行为管控，大大提升工作效率

- 细粒度的应用识别与管控，严格控制与工作无关的应用流量，提高工作效率，防止信息泄露。
- 海量的URL识别与过滤，有效屏蔽风险网站，遵从法律法规。
- 多维度实施精准带宽控制，保障关键业务的可用带宽。

基于 IP地址/端口/服务 用户/应用 页面内容

云安全中心智能联动，有效应对未知威胁

- 将可疑流量上传给云安全中心进行深度检测，可提高对未知威胁的检测能力。
- 将检测结果上传给云安全中心，云安全中心通过大数据和人工智能技术，快速形成信誉库和威胁特征库，统一下发给各安全网关，提升其安全检测能力。



高性能，提升用户访问体验

- 高速数据处理性能，同时容纳大规模在线用户与应用连接；
- 顶级安全检测防护能力，迅速识别阻断攻击威胁。

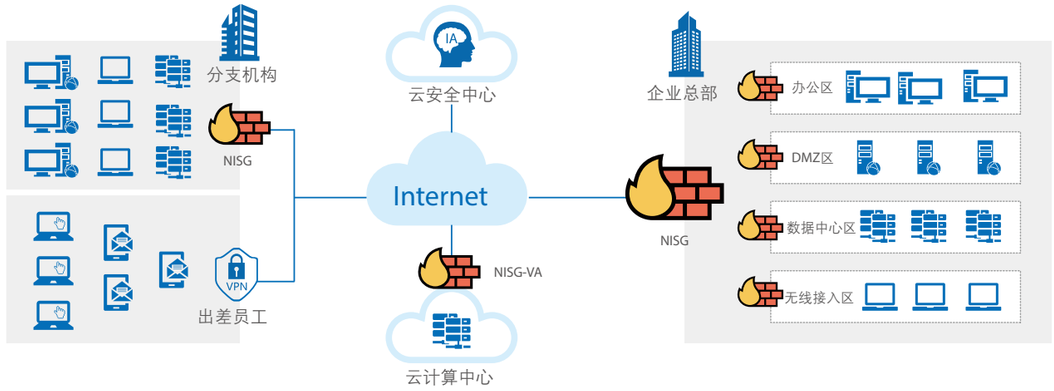
稳定可靠，保障业务持续性

- 软硬件结合的强大灾备处理能力，出现故障瞬间切换流量，提升网络健壮性，保障业务连续性。

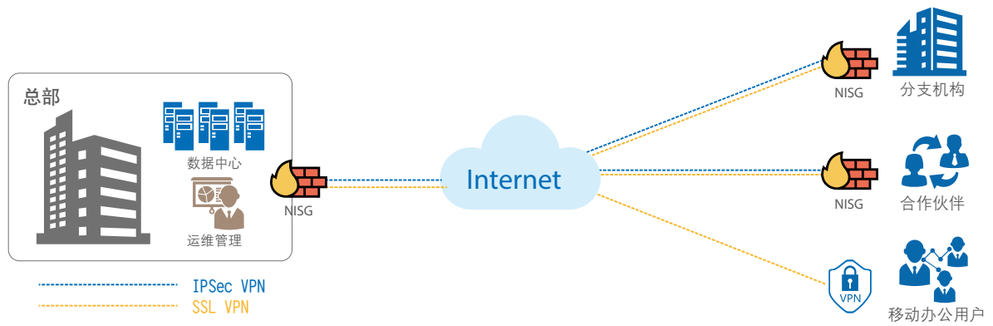
易用，提升安全管理效率

- 智能化的配置管理功能，直观的监控报表界面，配套方便易用的管理工具，大大提升管理效率。

应用场景1



应用场景2



主要特性

• 访问控制	• 智能选路	• 入侵防御	• 应用识别与控制	• SSL检测	• 虚拟系统
• 攻击防御	• 高可用性	• 防病毒	• URL过滤	• 云端协同威胁检测	• QoS
• 策略智能学习	• VPN	• 反垃圾邮件	• 页面过滤	• 集中管理与监控	• IPv6

东软NetEye下一代防火墙——智晟系列

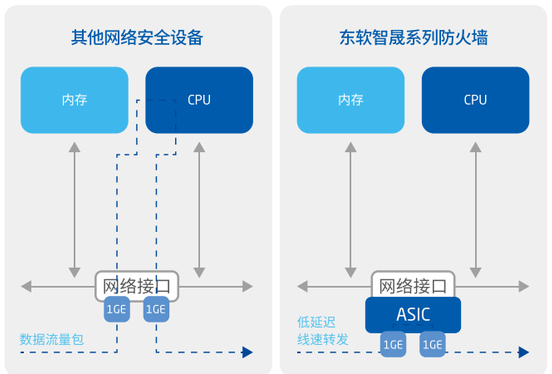
产品概述

东软NetEye下一代防火墙——智晟系列，是面向应用的第二代防火墙，采用国内领先的X86+ASIC芯片硬件架构，突破了传统X86架构在应用层检测方面对CPU性能消耗过高的瓶颈；依托东软自有的智能化“数据并行处理”技术实现对数据包的快速高效转发，保证了设备在大流量环境下的长期稳定运行。东软智晟系列下一代防火墙，具备应用控制、防病毒、IPS入侵防御、DOS防御、URL过滤、Web分类过滤、反垃圾邮件、DLP（数据防泄密）、广域网优化、无线控制与安全、威胁可视化等功能，通过全方位一体化的多项尖端安全技术，为用户保驾护航。

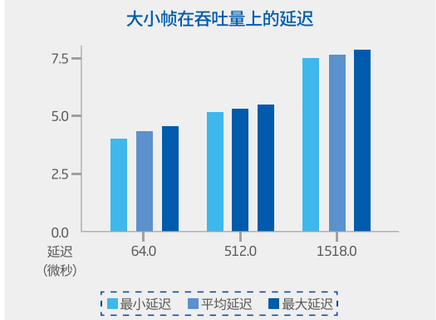
技术亮点

高稳定，低延时——大流量下的安全网管神器

高稳定： 独特的X86+ASIC硬件的设计架构，当新建会话与东软智晟防火墙建立连接后，CPU不再处理相关流量，交由ASIC芯片对数据包做深层次检查及转发，保证设备核心CPU可以长期维持较低的占用率，降低了因为CPU使用率高，而导致设备出现故障的情况，保证了设备在大流量环境下的长期稳定运行。



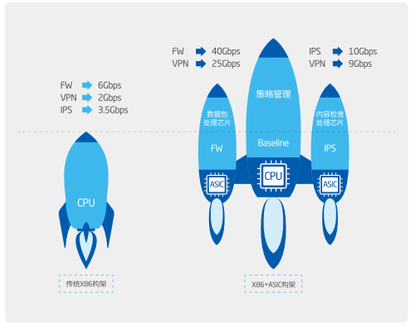
低延时： ASIC芯片对各种网络环境下数据包处理都能实现极低的延迟（均小于8us），极大降低了设备对整体网络性能的损耗。



智晟关键点：具备业内领先的低延迟性线速转发功能

高吞吐——国内领先的X86+ASIC硬件融合技术

东软智晟系列防火墙，采用定制化的X86+ASIC硬件架构，结合东软智能化“数据并行处理”技术，实现对数据包的高效转发，相比采用传统架构的同类产品性能得到极大的提高。



吞吐量对比	Packets	64Byte	128Byte	256Byte	512Byte	1024Byte	1514Byte
	东软智晟	32,820	35,128	35,584	38,700	38,988	35,788
	其他厂商	1,478 ~5,973	1,891 ~10,520	3,594 ~19,710	6,901 ~20,000	11,371 ~20,000	13,270 ~23,356

使用ASIC芯片来处理数据转发，能获得极高的小包吞吐量（包转发率）—接近万兆线速，无需考虑业务量中的大包和小包比例。

智晟关键点：大数据下数据包的快捷转发

应用场景

高校部署图

金融部署图

智慧城市部署图

广电部署图

东软 NetEye 虚拟安全网关

产品概述

云计算和虚拟化技术飞速发展，为企业的数据中心部署提供了一个高效、灵活、低成本的方案。当企业将机密文件和核心业务系统放置在虚拟化环境，尤其是云计算环境中，网络安全产品便成了必不可少的保护企业信息资产的工具。东软NetEye虚拟安全网关（NISG-VA）基于虚拟化技术研发，支持主流虚拟化平台，是拥有强大的安全功能与可靠稳定性的下一代防火墙产品。

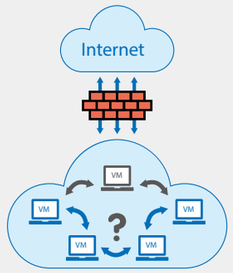
技术亮点

业界领先的虚拟化和云平台安全防护:

NISG-VA支持AWS、阿里云、华为企业云等公有云平台，支持VMware vSphere、OpenStack私有云平台及VMware、KVM、Xen等虚拟化平台。用户可根据其虚拟环境的规模和流量，灵活分配内存和CPU资源。采取快捷、灵活、可伸缩的部署方式，以最简单的步骤、最优的成本定制高可用性防火墙集群。

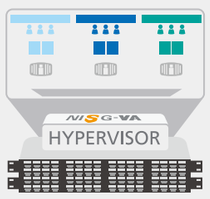
云计算环境中微分段，虚机安全迁移:

针对云计算环境中东西流量难以监控的顽疾，通过与东软云安全系统的集成，可以在大二层网络内部针对虚机部署微分段级别的防护手段，并在此基础上监控任意虚机间的流量，真正做到流量可视化。此外，基于分布式的工作模式，为虚拟化数据中心和云环境提供一张无形的安全防护罩。对于虚机而言，安全如影随形，完美支持虚机迁移（vMotion）。



可扩展的虚拟防火墙:

支持虚拟防火墙功能，每台虚拟防火墙可被看成是完全独立的安全设备。在满足特殊部署要求的同时，降低管理和维护成本，有效地提升用户投资回报率。更加节能环保，引领绿色IT理念。



智能高效的集中管理:

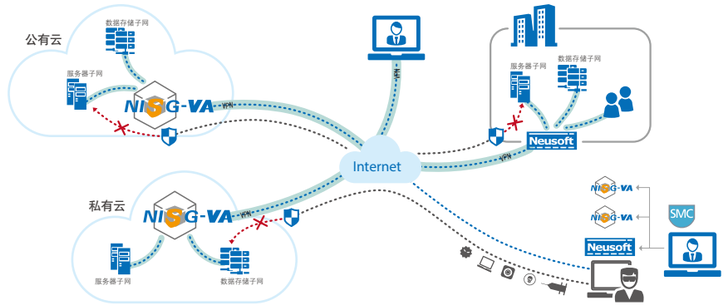
通过自有的防火墙设备集中管理软件，可对大规模虚拟和物理的NISG设备进行统一管理。拥有日志集中审计，规则库统一更新，策略集中下发，统一备份和恢复，流量实时监控，智能报警等功能。

功能特性

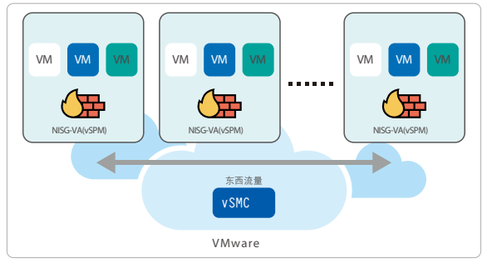
云计算及虚拟化	网络适配	VPN	应用安全	应用识别控制	攻击防御
• 虚拟化环境支持: VMware/KVM/Xen • 公有云应用市场: AWS/ Azure/阿里云/华为云企业 • OpenStack FWaas支持 • NCSS集成	• 桥/路由/NAT混合模式 • 基于策略的NAT/PAT/路由 • 服务器负载均衡 • 链路负载均衡 • IPv6	• IPSec/SSL VPN • VPN冗余网关 • 自有IPSec/SSL VPN客户端 • 网关到网关 • 远程接入	• IPS- 专利引擎 • 超越4000条的IPS特征 • 反垃圾邮件 • URL过滤 • 基于用户、IP、安全域 • VoIP支持	• 带有应用分类的应用识别 • 大于2500个具体应用 • 用户识别 • 内容识别 • QoS支持	• 网络攻击防御 • Dos/DDos防御 • 分片包攻击防御 • 畸形数据包防御 • SYN攻击防御 • IP欺骗攻击防御

应用场景

NISG-VA在支持AWS、阿里云、华为企业云、OpenStack、VMware、KVM、Xen等多种云计算及虚拟化平台的基础上，针对VMware vSphere和OpenStack私有云平台，提供针对性的网络安全解决方案，做更专业的云计算安全。



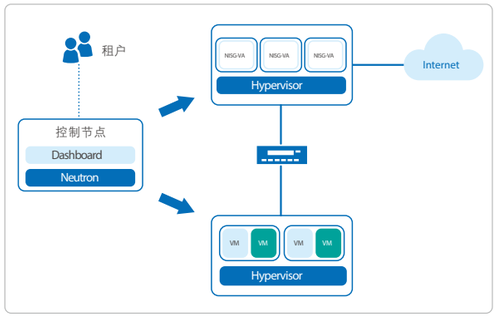
面向私有云的云安全解决方案
东软云安全系统



在东软云安全系统中，虚拟安全管理模块（vSMC）将NISG-VA（需要升级为虚拟安全防护模块 vSPM）部署在VMware vSphere环境中，为VMware提供东西流量控制，并可以实现二层网络内部虚拟机之间的安全隔离，实现微防护。在此基础上，提供虚机级别的流量监控，可以在享受云计算便捷服务的同时消除云安全的最大隐患，为用户配置一副可以洞悉云环境内部的透视镜。

基于OpenStack的云安全解决方案
东软云数据中心FWaaS防火墙解决方案

东软云数据中心FWaaS解决方案将安全控制器、驱动及NISG-VA部署于OpenStack云环境，并与OpenStack进行集成，具有租户隔离、方便管理、弹性扩展的技术特点。

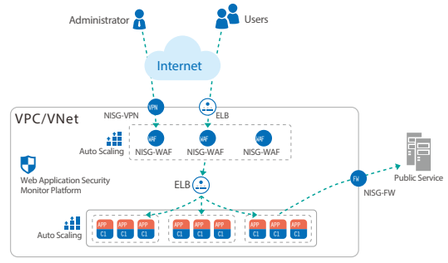


经典案例

OhwYaa SaaS企业社交服务安全防护

在OhwYaa SaaS企业社交服务案例中，OhwYaa在AWS上构建企业社交服务平台并对外提供服务。OhwYaa　SaaS构建企业内的社交网络，促进员工自发自愿的分享经验、共享知识，建立起企业内的自媒体平台。

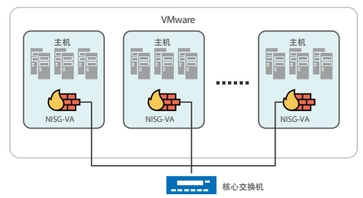
在本项目中，NISG-VPN作为VPN网关方便管理员管理内部服务器资源，NISG-FW作为安全NAT网关使得内部应用可以安全访问第三方资源。通过在AWS云平台上部署NISG-VA，可以解决企业社交服务网络中经常出现的突发业务流量、DDoS攻击和数据泄露等常见问题，为企业社交服务提供了可靠安全防护。



张家口网上审批和电子监察系统"四级平台"系统等级保护

该系统是为了方便老百姓办事，推动政务工作创新，提升政府工作效率。围绕其核心业务系统深入开展的一项信息安全等级保护工作。

项目采用的虚拟化平台是VMware，通过在VMware主机上部署NISG-VA，可为系统提供访问控制、入侵防范、恶意代码防范等网络设备防护。



东软 NetEye 应用交付安全网关

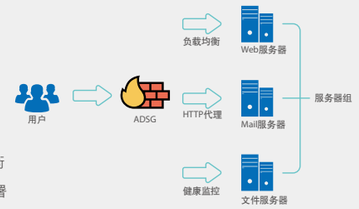
产品概述

随着网站业务访问量的日益增大，如何保证业务高效且安全的交付到客户手中，是企业最关心的问题。东软应用交付安全网关（ADSG）作为业界首创的支持多种环境下使用、具备卓越安全功能的下一代应用交付产品，集多种应用交付与安全功能于一身，包括流量负载均衡、应用加速、基于内容的应用交付、WAF（入侵防御、DDoS 攻击防御、基于自学习功能的主动防御、网页防篡改）等多种先进功能。同时ADSG实现了在传统物理设施、虚拟化以及云计算平台下的多环境部署。支持VMware、Xen、KVM等多种虚拟化平台，支持AWS、阿里云、华为企业云、OpenStack等多种云平台。为用户提供传统环境、虚拟化环境与云计算环境下安全可靠的应用交付解决方案。

技术亮点

基于内容的应用交付

- L4负载均衡
- L7负载均衡
- 链路负载均衡
- 全局负载均衡
- 基于内容加速
- 基于内容的负载均衡
- 完善的HTTP代理部署
- 完善的服务器健康检查

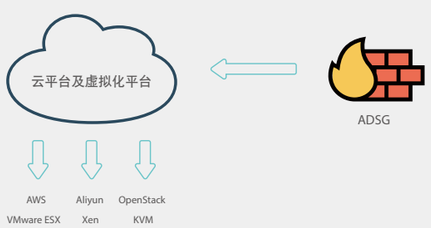


卓越的安全防护

- 基于专利技术IPS
- L7 DDoS攻击防御
- 智能的主动防御
- 细粒度的HTTP访问控制

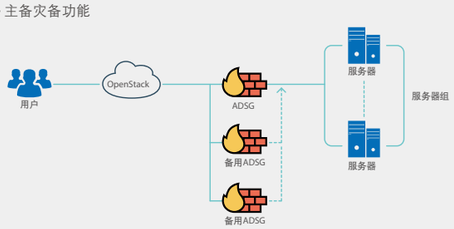
虚拟化及云环境支持

- 公有 / 私有 / 混合云环境部署
- 支持 AWS/ 阿里云 / 华为企业云 /OpenStack 等云平台部署
- 支持 VMware ESX / Xen / KVM 等多种虚拟化平台



OpenStack LBaaS支持

- 替代OpenStack自带负载均衡组件
- 支持OpenStack Kilo/Liberty/Mitaka版本
- 应用交付与安全防护于一身
- 主备灾备功能



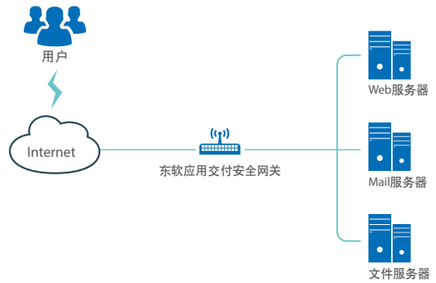
功能特性

服务器负载均衡	应用加速	虚拟化及云环境支持
• L4/L7负载均衡 • 链路负载均衡 • 全局负载均衡 • 多负载均衡算法支持 • 基于内容的负载均衡 • 服务器温暖下线	• TCP单边加速 • 内容缓存 • 内容压缩 • 内容优化	• 支持AWS、Azure、阿里云、华为企业等公有云 • 支持VMware、Xen、KVM虚拟化平台 • 支持OpenStack LBaas

入侵防御	DDoS防御	管理
• 自主专利技术IPS • 协议异常检测 • 智能主动防御 • HTTP访问控制 • 网页防篡改	• SYN Cookie • TCP SYN泛洪 • HTTP访问速率限制 • HTTP请求挑战机制	• 仪表盘 • 日志统计 • 报表功能 • 升级功能

应用场景

ADSG可以安装在物理设备、虚拟化和云计算环境中。服务器端可以是基于物理设备组成的集群、位于云计算平台中的服务器集群以及虚拟化数据中心。ADSG可以在不改变用户原有网络结构的基础上为用户提供高可用性、高可靠性的服务。支持传统环境、虚拟化环境、云环境部署。ADSG的典型拓扑如下:



ADSG接收客户端请求后，根据配置的负载均衡算法分发给真实的后端服务器，然后再将后端服务器的响应流量转发给客户端。

通过部署ADSG不仅可以实现负载均衡功能，还可以实现应用加速、Web安全防护、健康监控等众多功能。为企业网站应用保驾护航，保证业务的连续性，提高用户的满意度。

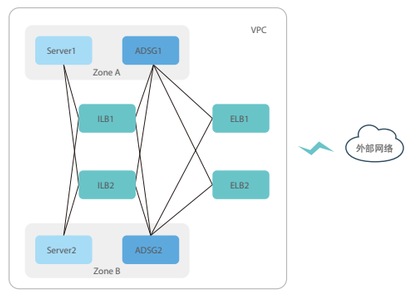
经典案例

索尼（中国）上海技术中心分公司部署 ADSG 案例

索尼（Sony Corporation），是全球知名的大型综合性跨国企业集团 ，AWS 是亚马逊公司旗下云计算服务平台，为全世界范围内的客户提供云计算解决方案。索尼将其本地服务器集群搬迁至 AWS 位于国内的云计算数据中心内。AWS 秉承只提供 IaaS 服务的原则，虽对其云服务基础平台的安全性有着充分的考量，但对于部署其中的具体应用则需要租户自己有针对性部署安全防护设备，索尼选择了东软应用交付网关 ADSG。

在部署方案中，东软 ADSG 部署在 AWS 的外部负载均衡器和内部负载均衡器之间，为网站提供安全防护。在拓扑中，ADSG 通过外部负载均衡器连接外部网络，通过内部负载均衡器连接服务器。ADSG 与用户服务器设施一起分布在两个 AZ 内部，在提升系统整体吞吐量的同时，支持灾备。

基于AWS基础设施的纵深防御部署示意图



在公有云环境中，DDoS、漏洞攻击、口令破解是三种危害大且频繁发生的网络恶意攻击行为。根据国内某公有云厂商年度报告中描述，其公有云平台一年发生了超过 300 亿次 DDoS 攻击，10.2 亿次 Web 攻击，66.3 亿次暴力破解事件。而这其中，面向各类具体互联网服务的应用层攻击占据其中的绝大多数。

东软应用交付安全网关基于专利技术的入侵防御功能可以有效地抵御各类漏洞攻击。通过 ADSG 的部署，结合 AWS 的服务组件，使得网络层及应用层中的 DDoS 攻击得到了有效的缓解。在应对口令破解攻击上，ADSG 自身提供的机器人防御功能可以有效地检测出恶意的口令试探访问，同时不影响系统的正常服务。

东软云安全系统

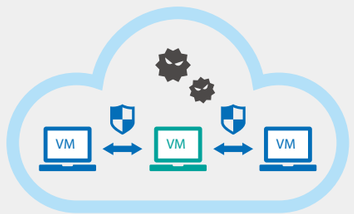
产品概述

东软云安全系统（NCSS）——云启，是针对云计算平台推出的分布式安全产品。通过管理平面与业务平面相分离的模式，帮助用户应对当下面临的云安全问题，有效地解决了用户的安全需求，提升了云计算平台的运营能力。

技术亮点

控制东西向流量，阻断攻击横向蔓延

东软NCSS可将每个虚拟机的流量牵引至虚拟安全防护模块（vSPM）进行威胁检测；发现并阻断东西向的安全威胁；阻止攻击在云平台内部的横向蔓延。



网络拓扑动态展示和流量实时可视化

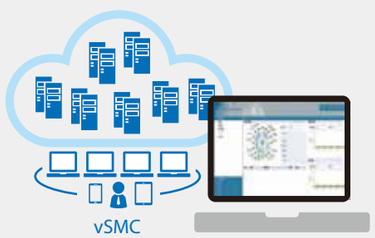
东软NCSS能够直观实时展示虚拟化环境的网络拓扑结构，并能够收集分析虚拟机之间的通信数据，帮助用户掌握云内部的细微变化、流量信息和威胁信息。

云环境特性适应——微隔离及虚机迁移

东软NCSS支持VMware等多种主流云计算平台，并与这些平台无缝融合。适应云平台的弹性扩缩，基于虚机的微隔离。支持云环境内部虚拟机夸物理主机间的迁移，实现动态的实时安全防护。

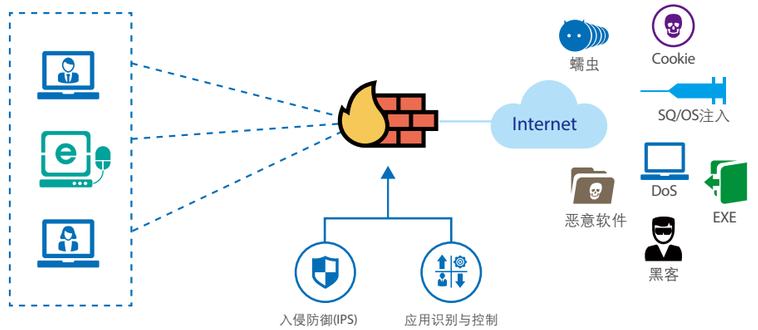
简单高效集中管理

东软NCSS通过虚拟安全管理模块（vSMC）实现集中管理，通过单一管理界面即可完成整个云平台的统一安全部署和管理。



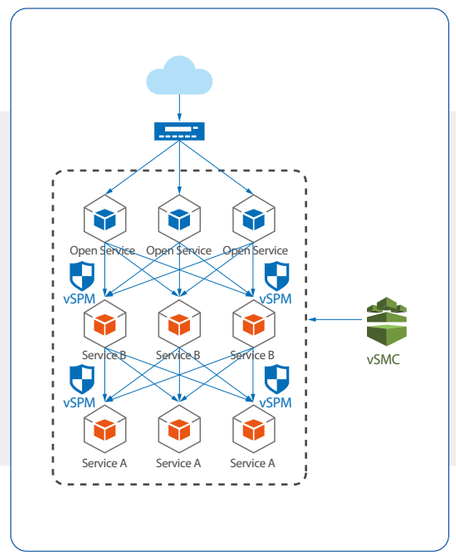
功能特性

DoS/DDoS攻击防御	入侵防御模块(IPS)	可视化
• 能够精确识别和准确防范众多的DoS/DDoS 攻击，进行有效检测和防御 • 实现攻击的智能防范，最大限度地保障用户的网络层及应用层网络安全	• 集成了具有自主知识产权及国际专利技术的东软NEL引擎 • 支持对已知和未知网络及应用层攻击的检测及防御 • 支持超过3000种攻击防御签名 • 支持在线升级	• 支持对接入服务的虚拟机进行全方位的网络监控 • 通过逻辑拓扑的方式展现可视化效果 • 支持虚拟机资产发现，支持对流量、应用、威胁的统计 • 支持系统日志、IPS日志、应用日志
部署模式	**自动化适应**	**虚拟化平台**
• 透明模式部署、无需改变现有的虚拟机配置和网络结构 • 管理平面、业务平面分离，系统统一管理 • 通过虚拟安全防护模块（vSPM）提供安全服务，服务容量可随用户需求增长而扩展 • 用户的虚拟机可被随时加入或者移出安全服务	• 支持云平台资产自动发现 • 支持云内部虚拟机夸主机迁移，动态的实时安全防护 • 支持安全防护模块（vSPM）动态扩容、减容	• 支持VMware vSphere5.1 • 支持VMware vSphere5.5 • 支持VMware vSphere6.0



应用场景

东软NCSS将原来同一网络下不能实现彼此间管控的虚拟机通过虚拟机微隔离、专业的引流技术，在透明模式且不影响用户原有网络拓扑的前提下，彼此隔离开来，进而实现虚拟机之间的流量管控，并且很好的支持了云平台的弹性扩缩、自由迁移等特性，为时下新兴的互联网架构提供了全方位的安全保障。



东软 NetEye 入侵防御系统

产品概述

东软NetEye集成安全网关入侵防御系统（NISG-IPS）是东软具有完全自主知识产权的第二代入侵防御产品，可有效检测并阻断从L2到L7层的入侵威胁，消除企业用户面临的外部和内部安全隐患，从而构筑全方位、多层次的防御体系，为用户业务的正常运行提供强有力的安全保障。

产品亮点

性能安全并重，实力业界领先

- 最高80Gbps的IPS检测能力，突破应用性能瓶颈
- 同时容纳大规模在线用户与高并发连接
- 性能与安全并重，保障用户关键业务高效稳定

主动智能防御，风险可视可控

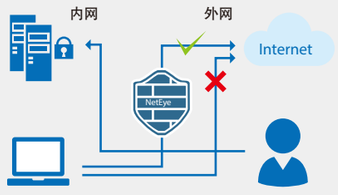
- 智能感知网络环境，自动生成安全策略
- 安全事件自动触发报警并产生日志，实现精准定位与溯源
- 实时监控网络动态，多样化图形方式展示威胁，风险一目了然

立体安全防御，阻断入侵攻击

- 集IPS、AV、AS及应用识别等安全功能于一体，铸就全方位的攻防体系
- 提供多层次防护，从网络层到应用层，阻断DoS/DDoS与SQL注入等数千种攻击
- 基于应用及内容识别的攻击防御，精准高效，安全更可靠

双向安全管控，防止信息泄漏

- 过滤恶意URL访问与病毒文件下载，免遭病毒木马感染
- 识别钓鱼仿冒网站，防范网络欺诈行为，避免经济损失
- 隐藏替换服务器信息，避免敏感信息外泄



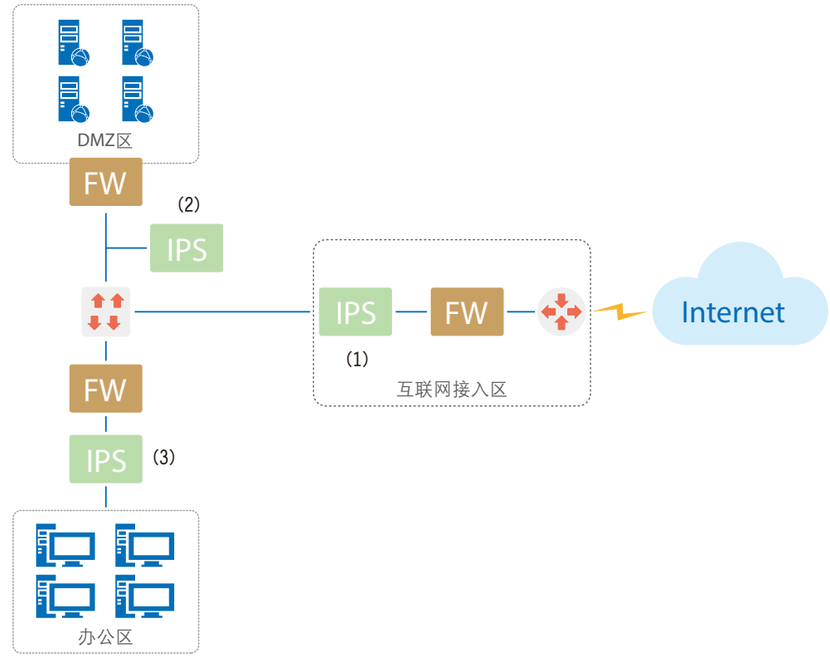
云端安全联动，深度威胁检测

- 与东软云安全平台智能联动，基于大数据与人工智能，检测深入高效
- 查杀文件类型丰富、检测嵌套文件层次深，有效拦截变种病毒和未知病毒
- 对HTTPS加密流量进行深度检测，安全威胁无所遁形

快速定位风险，实时应急响应

- 第一时间知悉重大高危漏洞，及时更新规则，零时差防护
- 实时追踪热点趋势，每周更新特征库，防范最新病毒与攻击
- 提供7*24小时的技术支持，响应服务永不离线

应用场景



场景（1）

NISG-IPS部署在企业互联网接入区，防御L2-L7层的外部入侵攻击。

场景（2）

NISG-IPS部署在企业内部DMZ业务区，针对Web和Mail等各类服务器，提供SQL注入和XSS等入侵攻击检测，与防火墙构成双层防御体系。

场景（3）

NISG-IPS部署在企业内部办公区，防范企业内部攻击，避免病毒木马等蔓延造成网络不可用，规范员工访问行为等。

NISG-IPS有两种部署模式:

1、在线模式：可与防火墙串联，能够检测并阻断威胁攻击，如图（1）和（3）所示。

2、旁路模式：无需改动网络拓扑，NISG-IPS仅对流量进行分析和告警记录。适用于刚开始部署IPS时，收集和了解网络访问和攻击信息，为后续在线部署提供优化配置参考。如图（2）所示。

主要特性

入侵检测（ 应用层）

- CSS/XSS跨站脚本攻击防御
- 跨站请求伪造防御
- 恶意代码攻击防御
- 命令注入攻击防御
- 缓冲区溢出攻击防御

攻击防御（ 网络层）

- DoS/DDoS攻击防御
- ARP攻击防御
- 源路由攻击防御
- 端口和主机扫描防御
- ICMP报文攻击防御
- TCP逃避控制防御

Web安全防护

- SQL/XSS/Shell/LDAP注入攻击防御
- 目录遍历攻击防御
- Web服务器信息泄漏防护
- SSL检测

东软 NetEye 入侵检测系统

产品概述

东软针对网络攻击、违规使用等情况而自主研发的东软NetEye入侵检测系统（IDS）采用深度分析技术对网络进行不间断监控，分析来自网络内部和外部的入侵企图，并进行报警、响应和防范，有效延伸了网络安全防御层次。同时，产品提供强大的网络信息审计功能，可对网络的运行、使用情况进行全面的监控、记录、审计和重放，使用户对网络的运行状况一目了然。

技术亮点

完整的事件特征库

东软NetEyeIDS事件特征库拥有5800+事件特征定义条目，能够广泛覆盖已知网络异常/攻击和应用协议特征，并且通过异常/攻击、应用内容、协议行为、连接会话四个层次深入分析网络流量数据，能够全面掌握网络行为态势。

内容恢复

系统可对常用应用协议（如HTTP、FTP、SMTP、POP3、TELNET、IMAP、DNS等）提供内容恢复功能，能够完全记录通信过程与内容并将其按照应用界面风格进行直观展现。此功能对于分析攻击过程、监控内部网络资源滥用、发现未知攻击等需求极具价值。

多重报警响应方式及实时提醒

系统支持实时报警、记录到数据库、电子邮件报警、SysLog报警、SNMP Trap报警、切断攻击连接等多种报警方式，便于及时通告并触发后续处置流程。

灵活配置及流量展现

系统可为每一个监听接口进行策略设置和监控IP范围设置。当网络具有自身特殊监控要求时，可以针对网络的特殊要求进行策略的设定，定制该网络的策略规则，同时设定监听网络IP范围。

全面的入侵检测，抵御恶意网络流量

检测引擎提供了从网络层到应用层全面的攻击防御功能。针对当前主要的应用层攻击，能够深入到应用的内容层进行检查，及时发现XSS、SQL注入等常见应用层攻击并有效阻断。同时，还能够针对底层有效过滤IP/端口扫描类攻击、DoS/DDoS等异常流量型攻击。

实时安全防护，漏洞修复无时差

作为CVE兼容认证成员，检测引擎拥有规范、全面的漏洞规则库，保障规则匹配效率。同时，作为微软“MAPP”（Microsoft Active Protections Program）成员，检测引擎能够在微软对外公布安全漏洞信息之前提前获取漏洞细节信息，及时更新特征库和升级补丁，第一时间为客户提供安全保护。

功能特性

部署方式

- 镜像模式
- 透明桥接模式(Bypass)
- 802.3
- 802.1q
- PPPoE

检测能力

- 特征匹配
- 异常监测
- 自定义
- 5800+事件特征
- 异常/攻击
- 应用内容
- 协议行为
- 连接会话
- 逐字节解码

内容恢复

- HTTP
- FTP
- SMTP
- POP3
- TELNET
- DNS
- 等主流应用

报警响应方式

- 界面报警
- 记录日志
- Email报警
- SysLog
- SNMP Trap
- 切断连接

信息采集

- 主动扫描判断
- 节点信息统计

特征库管理

- 多种缺省子集模板
- 缺省模板继承、派生

分布式部署

- 任意多层
- 策略集中下发

双引擎与多引擎

- 多重检测
- 并发检测

数据存储

- 本地海量介质
- 事件精简上报
- 自动远程备份
- 日志分类存储

管理安全

- 多角色权限划分
- 细粒度权限分配
- 操作行为记录
- 支持主控设置

日志报表

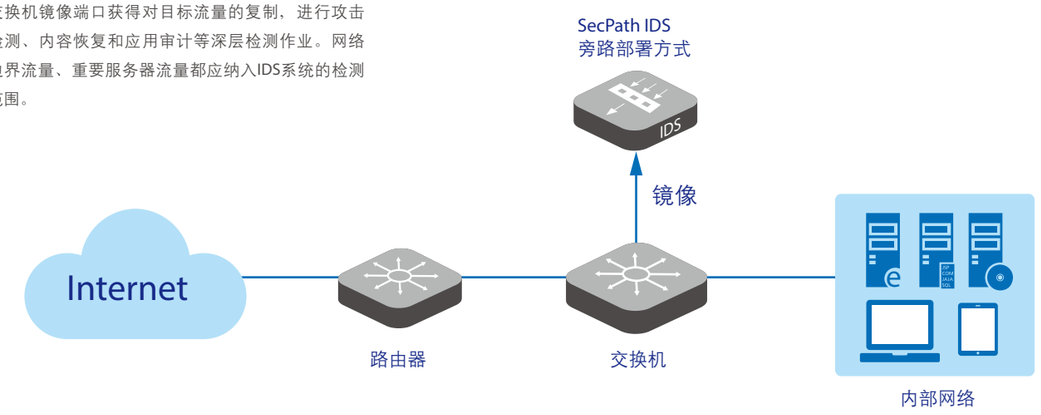
- HTML格式

管理方式

- Web管理

应用场景

东软NetEye IDS典型部署于企业网络核心节点，通过交换机镜像端口获得对目标流量的复制，进行攻击检测、内容恢复和应用审计等深层检测作业。网络边界流量、重要服务器流量都应纳入IDS系统的检测范围。



东软 NetEye 安全运维平台系统

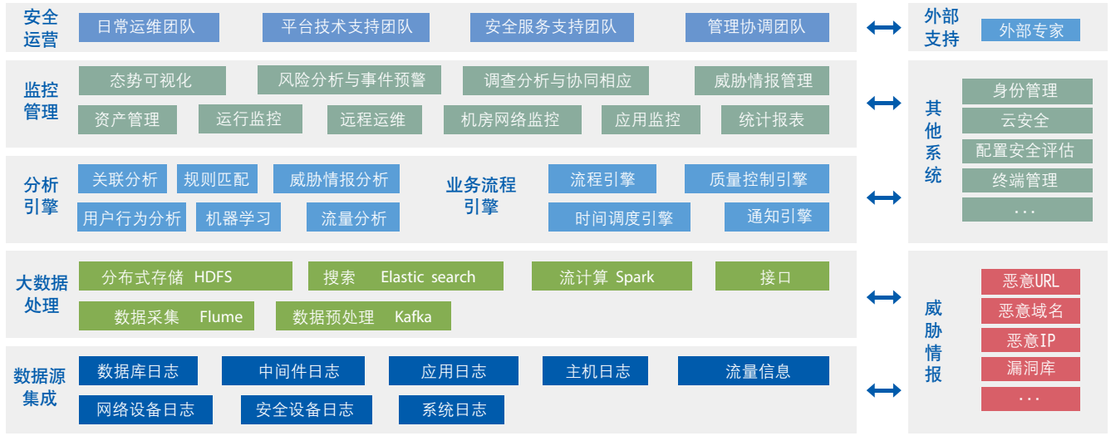
产品概述

东软NetEye下一代安全运营中心（NG-SOC）是根据国家网络安全监管机关发布的《中华人民共和国网络安全法》、《信息安全技术 网络安全等级保护基本要求》等要求，深入分析与研究常见安全漏洞以及流行的攻击技术，将团队攻防研究和安全运维经验以及信息安全等级保护相关标准总结归纳后，研制开发的以IT资产为基础、以业务系统为核心、以用户体验为指引的，应用大数据和机器学习技术，具备大规模数据的实时异常检测和分析、智能化安全分析、用户异常行为分析、安全可视化、风险预警、威胁情报共享和安全态势感知等功能的网络安全综合管理平台。

产品价值

- 统一管理资产的全生命周期静态信息
- 提供集中、远程、自动化运维接口，减轻日常运维负担
- 采用大数据平台架构，实现对海量异构数据的采集\分析\存储\管理
- 提供可视化分析工具，实现安全事件的溯源取证
- 统一监控资产的运行状态，快速定位和解决故障
- 借助可视化工具展现各维度宏观态势，并提供统计报表
- 内置智能分析引擎，快速发现已知威胁，预测未知威胁
- 与其他安全设备协同响应，实现安全事件的实时处理

核心架构与技术优势

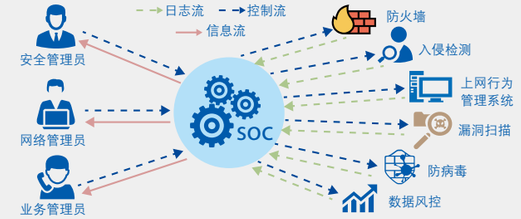


海量信息采集

支持SYSLOG、SNMP/SNMP、TRAP、ICMP、ARP、JDBC/ODBC、TELNET、SSH/HTTP、HTTP、JMX、SOAP、API接口、WMI、WebService、专用Agent端口镜像等数据采集方式；支持近20类设备、数十家厂商、近300余种常见型号设备的日志自动解析。

强大的运维支撑能力

内置流程引擎，支持基于ITIL的日常运维管理；内置知识库，实现安全事件处置经验共享；内置报表模板，提供灵活的安全运维报告。



大数据安全分析

针对海量异构数据，构建智能分析引擎，关联威胁情报、安全设备告警、资产弱点、用户行为、流量异常等信息，预先识别安全风险，报出预警，提高安全告警的处置效率。

可视化展现与分析

利用可视化图表，展现资产信息、运行状态、弱点分布、用户行为、攻击威胁等，满足各角色用户的宏观、中观和微观信息获取需求，实现数据推动决策，创造价值。

自动化响应

针对各类预警事件，迅速定位威胁源和相关资产，通过业务流程引擎，分发安全响应任务，并以微信、短信、邮件等多种方式提醒；通过与其他安全设备联动，可展现、评估、调整安全策略，提升事件响应的效率。

技术亮点

- 采用安全的、成熟的、开放的平台架构，可弹性部署功能模块，涵盖网络管理、安全管理、运维管理等功能，满足日常安全运维、重大活动特保、专项安全报告等各种需求
- 国内第一个成功交付的大数据架构安全管理平台，大于50000EPS处理能力，PB级数据秒级检索
- 10年以上安全运维经验积累沉淀了国内领先的安全管理知识库，内容涵盖安全事件库、安全策略库、预警信息库、漏洞库、关联规则库、处理预案库、案例库等；
- 通过CMMI5认证的专业团队，提供覆盖全国的定制化开发和实施运维服务
- 系统功能丰富易用、界面美观大方，支持多种主题的切换，内置丰富的报表模板，适用于网络管理员、安全管理员、网络主管、安全主管、公司高层等各个层次
- 支持近300种国内外主流网络设备、安全设备、数据库、中间件、存储等的日志高速采集、格式化、关联分析、存储和事件响应
- 内置智能化的安全事件关联分析引擎，提供图形化的、功能强大的关联分析策略建模工具；内置风险计算引擎，实现对全网安全风险的量化分析、安全态势评估和态势预测

东软NetEye业务安全网关——慧眼ElvaEye系列

产品概述

随着互联网业务的快速发展， 业务越来越多，越来越复杂，用户的权益和信息价值越来越高， 面临的业务安全挑战也就越来越大。除了传统的网络黑客入侵攻击以外，新的业务形态带来了新型风险。“东软NetEye业务安全网关——慧眼ElvaEye系列”是对在线业务系统的用户访问数据进行分析、判断用户异常行为、识别未知威胁的业务风险分析产品。该产品通过结合专业的数据采集措施、捕获全流量的行为数据、通过对操作行为还原、异常操作分析并阻止恶意操作。

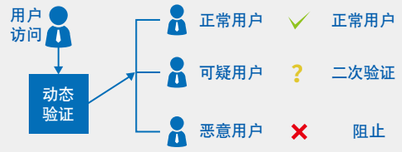
技术亮点

产品四大核心功能：人机验证、设备指纹、行为识别、实时决策，具有易用性强、定位精准、智能学习建模等特点，能高效的解决各类业务安全风险。通过设备指纹技术在客户端进行设备环境布点，采集设备硬件、网络、环境等特征信息，为后续的风险识别提供更多维度的判断依据。同时结合了行为特征识别、访问频率统计、地理位置定位等多项技术，精准判定人机操作，实时有效的拦截垃圾注册、批量登录、刷单等机器行为，并对疑似风险进行二次验证，实现正常用户免打扰，保证用户体验。

人机验证 | 设备指纹 | 行为识别 | 实时风险决策

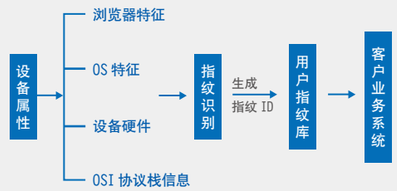
人机验证

当用户访问目标网站时，采用基于“JS挑战”的验证方法，向用户客户端发送特定的、浏览器能解析的应答JS，通过“挑战”的用户会带有一个特定的Cookie值，线上实时模型会依据此Cookie的信息来决定是否放行此请求，未通过挑战的认定为机器行为，进行阻断，通过挑战的认定为正常用户访问行为，进行放行。



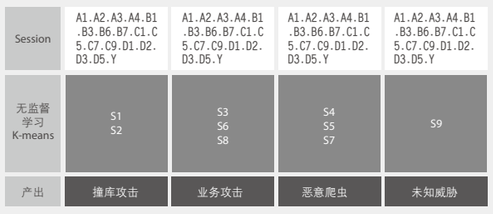
设备指纹

设备指纹采用在网站端集成JS脚本来采集终端设备的硬件、网络、浏览器等非敏感设备的特征信息，然后提交服务端，通过特定的Hash算法为每一个终端设备生成一个全球唯一的设备指纹标识写入用户Cookie，设备指纹伴随在会话的整个生命周期，进而实现对访客的服务鉴权、行为跟踪等。
设备指纹作为风险控制的关键技术之一，将其作为风险识别的重要维度数据，可以精准识别用户身份，能有效解决社保、公积金、医保等多个行业的互联网恶意查询、欺诈等风险问题。



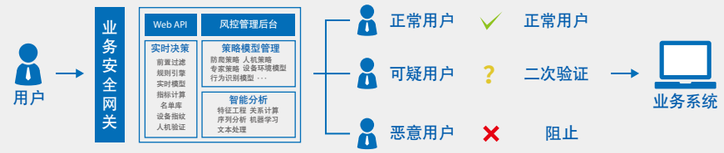
行为识别

行为识别的核心就是给互联网用户画像，采用非监督式和监督式学习相结合的方式打造了一套基于多层动态模型的风险评分体系和决策系统。从而将设计聚焦在真正用户的动机和行为上。



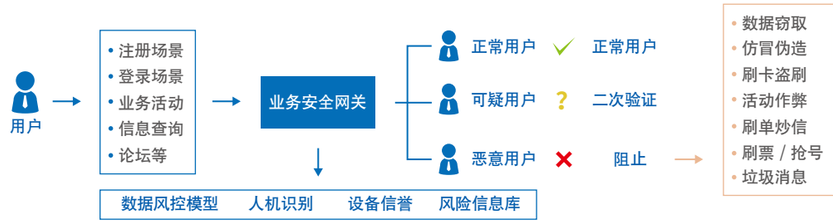
实时风险决策

实时风险决策是基于设备指纹、规则引擎、指标策略、风险数据、机器学习等多项技术的业务风险防控模块，帮助用户快速建立自有的业务安全体系，解决仿冒、盗用、欺诈、作弊、垃圾、爬虫等各类风险。
支持包括实时决策、近线分析、离线挖掘的多层次决策分析。能够作出毫秒级响应，利用策略和实时计算，同步识别风险，直接阻断恶意风险或通过二次验证确认疑似风险。



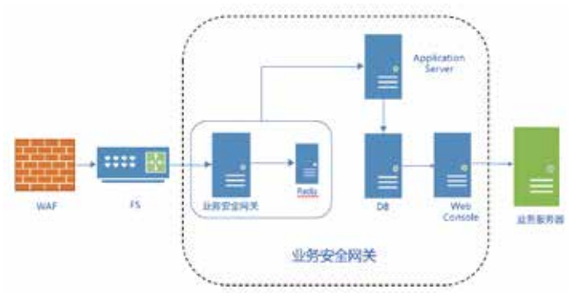
应用场景

- 场景一：信息查询场景，人社公积金系统、企业工商信息查询、政府和企事业单位以及在互联网提供查询服务、交互服务的大型网站平台等。（社保信息恶意查询、公积金信息恶意查询、企业信息恶意查询）
- 场景二：活动/促销场景，P2P金融理财、高回报理财产品、活动促销、抽奖等。（薅羊毛、恶意下单，订单欺诈、盗号盗卡，洗钱，恶意下单，恶意提现）
- 场景三：注册/登录场景，电商行业、民航业、恶意注册、点击欺诈、低价机票、热门机票、占座、恶意注册等。（撞库盗号，账号分享，批量注册、盗播盗看，广告屏蔽，刷量作弊）



部署模式

业务安全网关为保证业务系统正常运行，做到实时阻断恶意请求，需采用串联方式部署：通常部署在服务器之前F5（负载均衡）之后。
使用F5负载均衡设备将访问流量分发到业务安全网关，业务安全网关对访问流量进行过滤后，将恶意访问直接拒绝，正常访问透传到业务服务器。能够实现专业、实时对抗各种业务层面的攻击行为，智能区分人机，同时保证正常用户体验顺畅无影响。



功能特性

- 适用于分析B/S信息系统和移动应用
- 交付周期短，基础部署服务周期为1周
- 技术专家、数据专家、业务专家进行多维度异常行为识别和风险分析
- 通过专业软件对网络全流量数据进行采集，易于实施，不依赖日志记录的完整性
- 通过智能学习建立行为基线，逐渐形成风险模型
- 通过对HTTP及HTTPS全流量的分析，还原异常行为
- 提供专业风险分析报告，专家建议。

东软 NetEye VPN 网关

产品概述

东软NetEye VPN 网关是专业的VPN设备，采用标准SSL、TLS 协议，同时支持IPSec VPN、SSLVPN两种VPN，非插卡或防火墙带VPN模块设备。可提供远程的安全接入，配置简单快捷。兼容性好，利用浏览器内嵌SSL协议，可适用于任何终端及主流操作系统。运用SSL加密和逻辑隔离的特性为客户的核心数据实现安全防泄密。是解决远程用户访问公司敏感数据最简单最安全的技术。

技术亮点

更安全：提供细致的权限划分、高效的数据加密机制、丰富多样的身份认证手段、全面的单点接入安全检查、完整的日志审计，全面保护组织信息安全。

更精细：提供基于URL授权的细粒度访问权限控制。提供多种认证安全机制，可采用多种机制组合的方式进行认证。根据安全级别，提供多种加密算法进行选择。

更好用：适用于任何终端及主流操作系统。使用内容压缩技术全面提高远程接入访问的办公效率。

更轻松：可助您轻松使用笔记本、桌面PC、智能手机、Pad等移动终端设备实现安全、便捷的远程接入内网，在降低运营成本的同时大幅提高企业的生产效率。

功能特性

• SSL VPN • IPSec VPN • 防火墙 • SSO 单点登录 • LDAP 动态目录

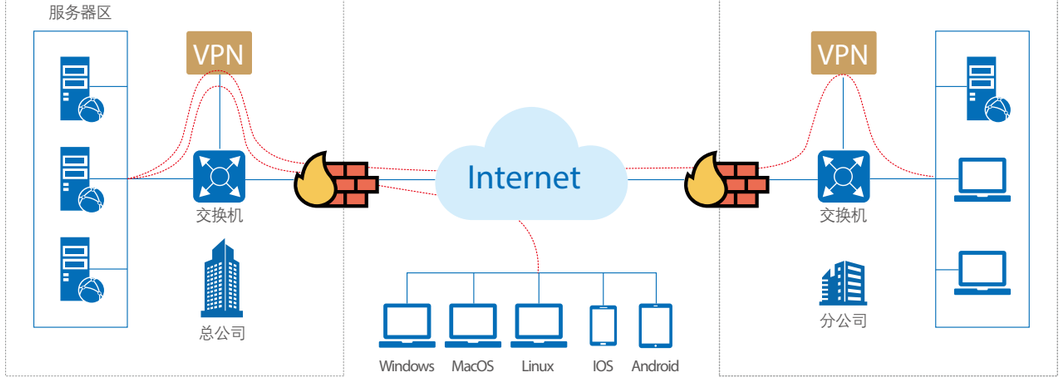
特性列表

SSL VPN	IPSec VPN	防火墙	认证方式	系统管理
Portal 模式	网关到网关远程访问	IP 包过滤	本地认证	WebUI
支持协议Http、Https、FTP、SSH、Telnet、RDP	支持IKEv2，兼容IKEv1	SNAT	RADIUS	管理员角色与权限划分
SSO 单点登陆	3DES/AES加密	DNAT	LDAP	免费软件升级
主从账号绑定	失效对端口检测(DPD)	路由	AD	日志审计管理
内容压缩/缓存	完美向前保密(DH组):1,2,5	攻击防御	eDirecory	对象管理（用户组、资源组）
支持验证码登录	抗重放攻击	IP-mac绑定	OTP令牌环认证	配置自动备份同步
隧道模式	基于域名的VPN		USB KEY认证	双机热备
全网访问	预共享密钥/证书		证书（自带CA中心）	
客户端支持：Windows、MacOS、IOS、Android、Linux	SM3、SM4国密算法			
LDAP动态组/安全组				

设备配置表

型号	接口	尺寸	电源	环境	支持客户端
NVPN5K	USB 2.0接口*2 10/100M自适应口*1 10/100/1000M自适应口*5 Console口 *1	4.45 cm (1U) 44 cm 30 cm	交流单电源	工作环境温度: 0- 40℃ 工作环境湿度: 5-95%, 不凝结 存储运输温度: -40℃~+70℃	1-500
NVPN6K	USB 2.0接口*2 10/100/1000M自适应口*6 Console口 *1 扩展槽 *1	4.5 cm (1U) 45 cm 44 cm	交流单电源/ 交流冗余电源 可选		1-4000
NVPN7K	USB 2.0接口*2 10/100/1000M自适应口*10 Console口 *1 扩展槽 *3	8.8 cm (2U) 43.2 cm 56 cm			4000以上

应用场景

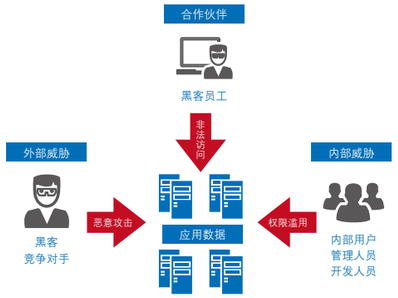


东软 NetEye 数据库审计系统

产品概述

高效的数据安全平台

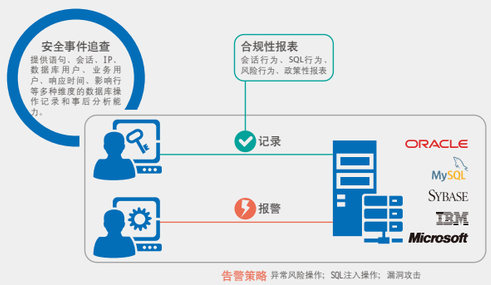
在传统网络安全体系基础之上，数据库内部和周边SQL活动的监视及安全控制是至关重要的“下一步”建设目标。东软NetEye数据库审计系统（DBA）是用户核心信息资产——数据库系统的最后一道防线，是数据安全解决方案的重要产品依托。该系统能够对链路上的SQL数据流进行采集、分析、识别、屏蔽、替换、阻断、授权、身份验证和身份识别等操作，把相关行为、相关内容进行归档存储，形成高效的监视审计机制，并对违规操作进行报警甚至拦截，同时提供全面的合规性报告。一方面，东软NetEye数据库审计系统能够汇总并分析数据库SQL通信以形成审计记录，另一方面还可检测发现异常访问并进行报警。甚至在合理的策略配置和模块支持下，东软DBA系统还能够对严重违规SQL 流量进行拦截阻断，防止其损害数据库。



技术亮点

详尽的数据库审计能力

实时监控业务系统和管理员对业务数据库的所有访问，根据多种安全策略判定访问操作的风险等级，并根据风险等级采取对应的报警策略，从而实现完全独立于数据库的审计功能。系统能够有效识别数据库访问行为，完整记录并形成审计数据，最终通过合规性报告、检测警报等形式通告管理者，是合规性建设及调查取证的重要工具。

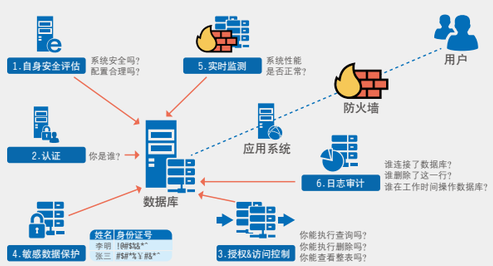


强有力的违规拦截与防御

东软 DBA 数据库审计系统支持专业的数据库防火墙扩展模块，该模块能检查将要进入数据库的 SQL 语句，并根据管理策略采取允许、记录、替换、阻止或者警报等处理手段。防火墙可提供完全独立的授权检查，按照 IP、用户、时间、命令进行针对性的权限控制，同时还可防御数据库 SQL 注入、缓冲区溢出等高危行为。

完善的数据安全解决方案

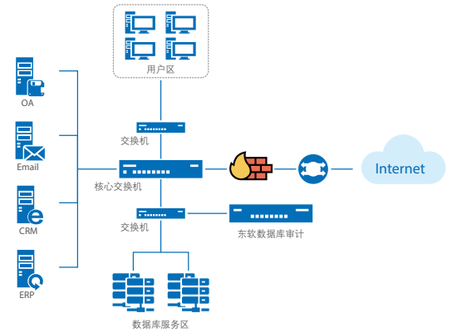
系统单一硬件即可按需提供全部的数据安全功能包，实现完整的数据安全解决方案，如数据库审计、数据库防火墙、数据库风险扫描、数据库透明加密、数据库脱敏、数据库状态监控、关联分析、合规报表等，能够针对数据安全流程节点提供对应的保护机制。



应用场景

完善的数据安全解决方案

系统单一硬件即可按需提供全部的数据安全功能包，实现完整的数据安全解决方案，如数据库审计、数据库防火墙、数据库风险扫描、数据库透明加密、数据库脱敏、数据库状态监控、关联分析、合规报表等，能够针对数据安全流程节点提供对应的保护机制。



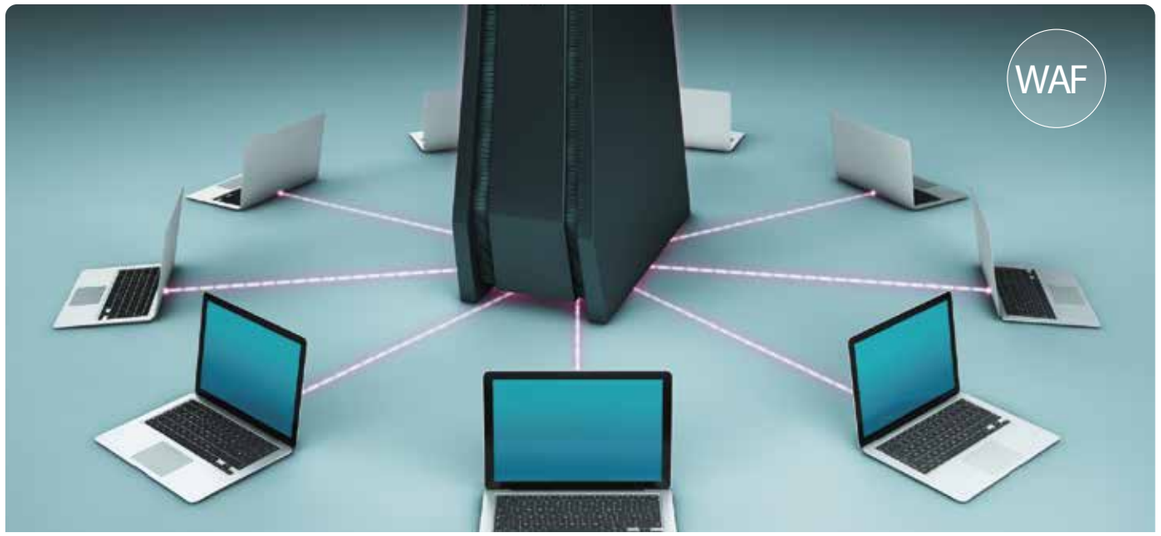
支持数据安全分析平台

数据安全分析平台能够对多台分布式的NDBA设备提供集中分析服务。系统基于大数据技术架构，采用关联分析、行为分析、机器学习、日志还原、可视化技术等多种手段，并结合用户资产、敏感数据、组织架构等基础信息，构建数据安全态势分析平台，提供海量日志存储分析、安全态势分析、安全设备管理、业务状态展现、安全事件追溯取证、安全策略联动等功能。

- 海量日志存储分析：实现PB级别的分布式日志存储，千亿规模日志检索秒级响应
- 智能学习：基于机器学习机制，生成用户行为画像，提升安全态势感知能力
- 关联分析：与网络安全、运维、应用等安全事件深度联动
- 实时预警：威胁事件实时分析、秒级预警、安全事件取证溯源

功能特性

功能模块	
系统管理	对本身进行配置，可以对系统用户的三权分立、操作权限等进行配置
策略管理	对目标数据库服务器资产的添加、授权、策略制定、告警设置等配置功能
检索系统	系统可实现多种组合方式查询检索，目前主要实现一级检索
告警系统	系统有多种告警方式，如Syslog、短信、邮件、FTP、SNMP等方式
报表系统	系统内置多种报表模板，有DPA、SOX、等保、通用统计等多种报表
备份系统	系统可实现对审计日志的自动备份、手动备份、FTP异地备份及还原备份数据
数据库审计	持续监控和分析对数据库服务器的所有请求，实时识别针对系统和敏感数据的攻击和危险操作，实现实时的监制、报警、和智能审计
数据库防火墙	对访问数据库的请求进行过滤，持续保障访问的合规性
数据库状态监控	实时监控数据库运行状态，在状态异常时进行预警，防止业务瘫痪，保障业务系统的可用性
数据库风险扫描	全面扫描数据库与宿主操作系统的漏洞并告警，分析数据库与宿主操作系统的配置风险并提出整改方案



东软 NetEye Web 应用防护系统

产品概述

当Web应用越来越为丰富的同时，Web服务器以其强大的计算能力、处理性能及蕴含的较高价值逐渐成为主要攻击目标。而在防火墙、IPS/UTM市场规模逐渐增长的同时，Web安全事件却反而呈现增多的趋势，SQL注入、网页篡改、网页挂马等频繁发生。究其原因，是防火墙、IPS/UTM在防护机制或检测深度方面无法满足日益复杂的Web安全防护需求。东软以多年的Web安全研究经验和成果为核心，针对Web应用的安全问题开发出了东软NetEye Web应用防护系统，从防护机制和防护深度方面解决了传统安全防护网关对Web应用防护效果不佳的问题，使得Web应用的安全性有了质的提高。

技术亮点

精细化Web安全防护

防护系统能防护7大类Web攻击威胁。

精细化的规则配置，发挥最大的安全防护功能，有效应对OWASP Top10定义的威胁及其变种。

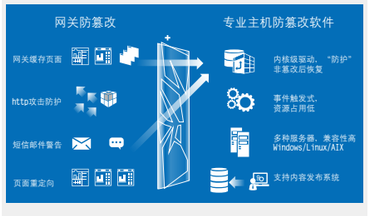
完整网页防篡改解决方案
网关防篡改+主机防篡改

除具备普通WAF的防篡改功能之外,更具备独有的专业级主机防篡改方案。

基于文件夹驱动级保护技术，采用事件触发机制，确保系统资源不被浪费。同时防篡改软件可以与WAF联动，阻断Web威胁。

采用文件级驱动保护技术后，用户每次访问每个受保护网页时，Web服务器在发送之前都进行完整性检查，保证网页的真实性。

软件兼容Windows2000/xp/2003/2008(64位)，Linux/BSD等多种操作系统。



全面的立体防护

提供Web漏洞扫描等事前告警功能，提醒客户为Web服务器进行升级，做好充分的安全防护;

上线后，提供全方位的Web攻击防护、网页挂马防护、网页篡改防护等功能，同时提供抗DDOS攻击功能，确保网站的正常运转;

提供一系列的Web页面加速、负载均衡等功能，提高Web服务器的性能；特有的网页防篡改软件和WAF配合，可以为Web服务器安全又添加一层保障。

旁路阻断

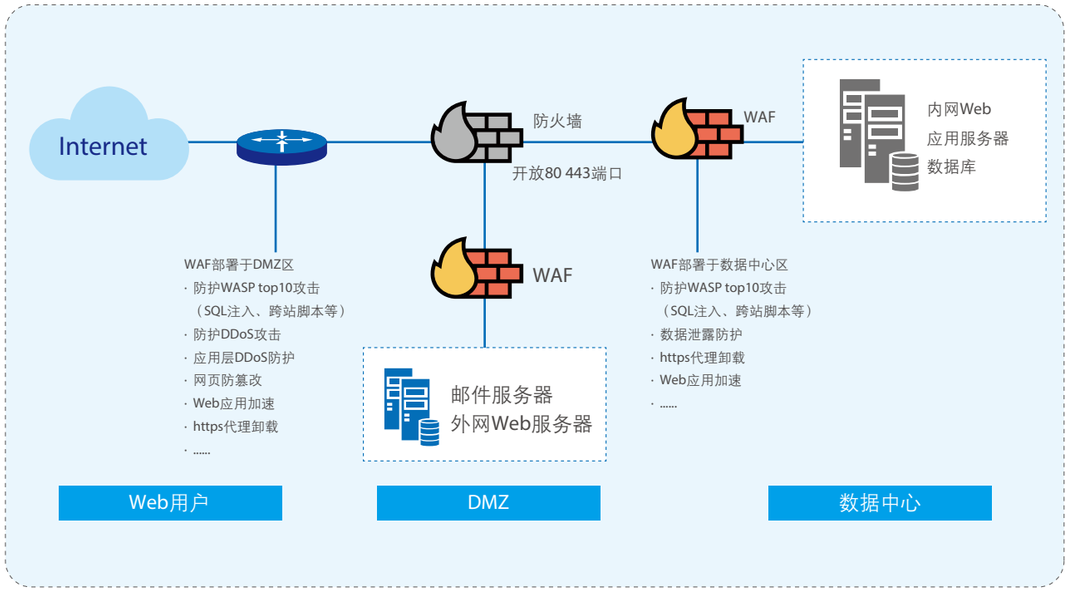
在原有的IPS镜像检测基础上，实现了回注阻断攻击的请求。真正的规避开了单点故障问题，完美的保证了Web系统的正常运行。

安全情报中心

内置威胁情报管理中心，同国际主流数据源、国内情报源进行对接，获取威胁情报。通过情报中心，可以基于实时更新的问题IP、黑链进行动态防护，并通过多样化的图表进行数据展示。更加准确的进行防护与溯源。

应用场景

支持旁路模式、旁路阻断、透明部署、路由部署、反向代理等模式，在透明代理模式下，用户无需改动自己的网络拓扑，Web应用防火墙能自动适应网络结构，捕获Web流量，进行安全检测、过滤、防护等安全功能。



功能特性

- Web安全
- 防信息泄露
- 应用交付
- DDOS防护
- 网络层防火墙
- Web安全扫描
- 网页防篡改
- 安全情报中心
- 系统管理
- 多角色用户管理
- 系统诊断
- 多种部署模式
- 双操作系统
- 网络管理
- 黑白名单
- 系统状态检测
- 双机部署
- 日志/告警
- 手动/自动升级

东软 NetEye 统一身份管理系统

产品概述

东软NetEye统一身份管理系统（NABH）为高端行业用户解决IT运维管理和IT内控外审的问题而设计。它将众多管理员账号（主账号）和设备的账号（从账号）进行统一管理，建立统一的权限影射关系，呈现统一的运维管理门户。在管理员进行运维操作的同时，东软NetEye统一身份管理系统会对其操作行为进行访问控制，对全程运维行为进行记录、分析和展现，帮助用户规范运维管理流程，提高运维效率，完善责任认定体系。

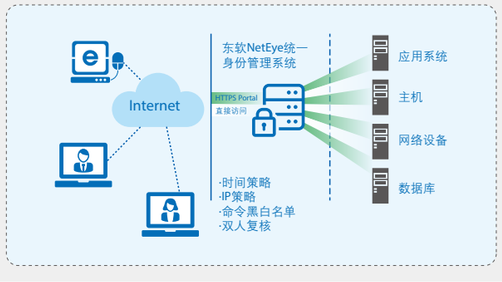
技术亮点

多种协议、设备支持，单点登录提高运维效率

东软NetEye统一身份管理系统全面支持主流的运维协议Telnet、SSH、FTP/SFTP等，可以对每个字符进行详细审计和过滤控制。同时实现了多平台的多种图形终端操作的审计，如RDP、XWindow、VNC等方式图形终端操作。各种操作系统、主流数据库、网络设备、Web应用系统及中间件皆可以通过东软NetEye统一身份管理系统来实现命令级的运维审计，对于CS/BS类应用协议，东软开放登录流程编辑工具，可实现大多数应用协议密码代填无需定制，在东软NetEye统一身份管理系统进行全部设备托管后即可通过单点登录进行密码代填，大大提高运维效率。

精细的访问控制，有效降低操作风险

东软NetEye统一身份管理系统可以根据时间、IP、命令黑白名单、用户组、服务器组、角色等对运维管理员进行精细的实时访问控制。同时支持双人复核授权流程，外包运维人员登录设备和输入关键命令时，需要高权限运维人员复合才能进行，此功能特别适用于有运维外包的大型企业。



准确的操作还原，便捷的事后取证

东软NetEye统一身份管理系统采用操作还原技术将操作流程自动的展现，能够监控用户的每一次行为，并判定该行为是否对企业内部网络安全造成危害。操作还原功能有效地降低了恶意操作的可能性。

更多价值展现

- 一次登录，全网畅通，有效提高工作效率
- 多因素认证手段，有效提高整体运维安全性
- 细粒度访问控制功能保证权限最小化原则实施
- 实时审计/录像回放有效控制操作风险
- 双人复核管理流程，有效监控代维人员
- 符合IT内控审计要求，确保法律法规遵从

功能特性

支持协议

- SSH
- Telnet
- FTP
- SFTP
- RDP
- VNC
- Xwindows
- 私有协议

支持设备

- Windows
- Linux
- Unix
- AIX
- Cisco
- Huawei
- H3C

账号管理

- 主帐号管理功能
- 从帐号管理功能
- 组织机构管理
- 账号批量管理
- LDAP/AD域导入

认证管理

- 单点登录SSO
- LDAP
- AD
- RADIUS
- MAC地址
- 证书
- 内置OTP令牌
- USBKey
- 双因子认证

平台功能

- 平台自管理功能
- 系统备份
- 双机热备
- 平台角色管理
- 与东软4A联动

授权管理

- 命令策略管理
- 时间策略管理
- 密码策略管理
- IP访问策略
- 访问锁定策略
- 实时监控策略
- 双人复核管理
- 电子密码保管箱

审计管理

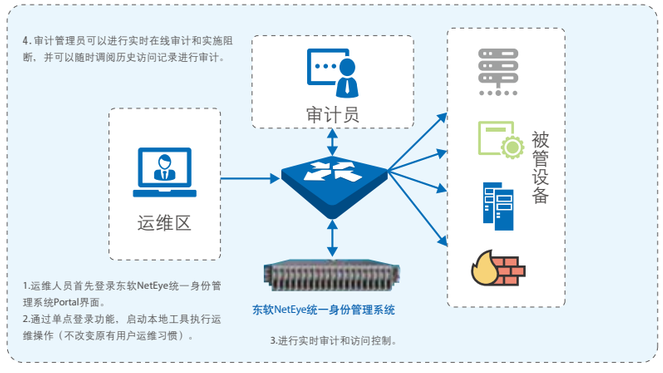
- 协议审计
- 审计报表
- 日志回放
- 日志查询
- RDP图像字符识别
- 数据库SQL语句识别

部署方式

- 旁路模式
- 网关模式
- 支持HA
- 支持分布式部署
- 集群部署

应用场景

东软NetEye统一身份管理系统采用“物理旁路，逻辑串联”的模式，不改变网络拓扑结构，无需在终端安装客户端软件，不改变管理员、运维人员的操作习惯，不影响正常业务运行。用户从portal页面单点登录，东软NetEye统一身份管理系统进行协议代理，代替用户连接到运维设备，进行实施的访问控制和审计记录。审计人员可以实时审计或者事后进行录像回放查看操作记录。



东软 NetEye 网络审计系统

产品概述

东软NetEye网络审计系统（ESM）采用先进的协议识别和智能关联技术，通过对网络数据的采集、分析和识别，实时动态的监测网络行为、通信内容和网络流量，发现并捕获各种敏感信息、违规网络行为，全面记录网络系统中的各种会话和事件，实现对网络信息的智能关联分析和安全评估。

技术亮点

行为审计

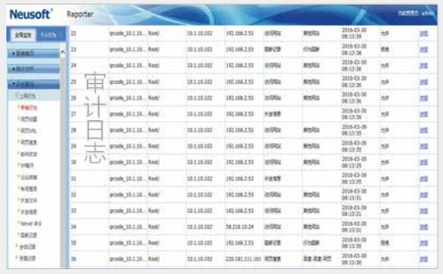
东软NetEye网络审计系统能够全面详实地记录多种网络行为，并根据国家有关法规规定保存至少180天，便于回溯以及审计和分析。

流量审计

- 接口流量统计（实时流量/速率、历史数据分析）
- 用户流量统计（趋势分析、细分流量、URL细分、多链路使用对比、总流量、上行/下行、峰值/平均）
- 用户组流量统计（总流量、上行/下行、峰值/平均）
- 应用流量统计（趋势分析、用户排名、多链路分析）
- URL流量统计（趋势分析、用户排名、多链路分析）
- 支持实时和历史数据的分析与统计
- 审计结果以饼状图或柱状图形式展现
- 审计数据保存至少180天以上
- 支持FTP形式的外部备份，提供手动备份和自动备份方式

内容审计

针对互联网上流行的可还原协议，东软NetEye网络审计系统能够在记录网络内流经监听出口的各种网络行为产生的具体内容，包括正文、文件等信息，并根据国家有关法规规定保存至少180天，以便进行事后的审计和分析。



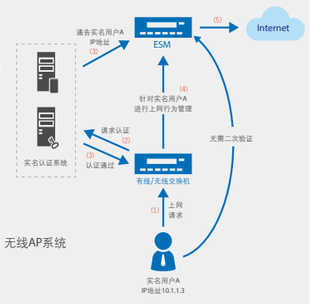
实名审计

功能特点

- 用户管理简便，实名账号自动学习
- 认证过程友好，无需二次认证
- 支持有线+无线的接入上网场景
- 实名制上网行为管理与审计

系统支持

- 锐捷SAM认证计费系统
- H3C IMC智能管理中心平台
- 城市热点认证计费系统
- 符合中国移动portal2.0规范的BAS、无线AP系统



适用场景

- 教育网学生上网实名制审计
- 运营商WLAN接入实名制审计
- 非经营性公共上网场所WIFI接入
- 酒店上网实名管理审计（定制）
- 其它需要使用实名制上网审计的场所

功能特性

7层应用协议识别

- 自动识别和智能分类
- P2P下载软件
- 网络流媒体软件
- Web视频
- HTTP应用
- 网络电话
- 网络游戏
- 股票交易
- 网上银行
- 支持根据特征码自定义7层服务

用户管理

- 建立组织结构
- 上网策略
- 支持本地数据库、POP3、AD、LDAP或RADIUS等认证
- 自动创建未创建账户
- IP、MAC、IP+MAC、VLAN绑定
- NetbIOS协议扫描
- 域单点登录
- 临时账号申请

行为统计

- 上网行为管理与审计
- 即插即用
- 网页关键字过滤
- 网页URL过滤
- 文件传输类型过滤
- 邮件过滤
- IM即时通讯的过滤
- 网页标题记录
- 发贴记录、网页评论记录
- 在搜索引擎上的搜索记录
- URL访问记录
- 网页文件上传
- 下载记录
- 邮件内容审计
- 邮件附件审计
- IM即时通讯软件内容审计
- FTP的上传和下载记录，包括用户名和文件名

防火墙功能

- 支持防火墙包过滤功能
- NAT地址转换功能
- 端口地址转换（PAT）
- 一对一静态地址
- 端口地址映射
- 基于状态的包过滤
- GRE隧道
- DDos攻击
- ARP防欺骗

负载均衡

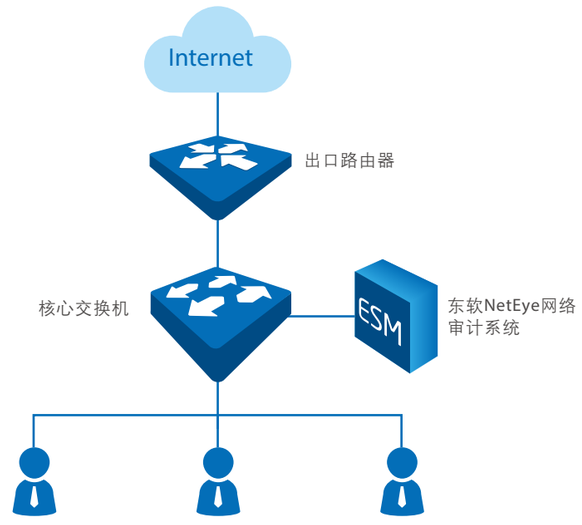
- 支持4出口以上的多链路负载均衡
- 多负载均衡算法
- 智能DNS，对内部服务器负载均衡
- 认证管理

流量控制

- 线路宽带设置
- 基于用户、协议、服务、URL的带宽阻断、限制和保障
- 单用户会话数限制
- 应用限额策略

应用场景

东软NetEye网络审计系统支持旁路、路由、网桥三种部署模式。



旁路模式（经典部署）

东软 NetEye 安全评估与监控系统

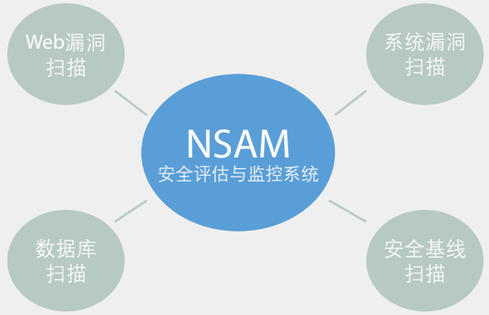
产品概述

东软NetEye安全评估与监控系统（NSAM）通过本地检测技术与远程检测技术相结合，对网站进行全面的、深入的、彻底的风险评估，综合性的规则库（本地漏洞库、ActiveX库、网页木马库、网站代码审计规则库等）以及业界最为领先的智能化爬虫技术及SQL注入状态检测技术，检查系统中存在的弱点和漏洞，使得相比国内外同类产品智能化程度更高、速度更快、结果更准确，做到防患于未然。

技术亮点

综合性扫描监控系统

集主机漏洞扫描、Web扫描、数据库扫描和基线扫描于一体的专业一体化扫描系统。
事前对系统、网站的安全进行评估，让您充分了解网络和业务的安全现状，及时发现问题、及时处理问题，并提供相应的解决方案。



全方位多层次检测网站安全漏洞

对网站安全状况做出最全面的评估，包括：系统补丁、危险插件、代码审计、恶意网站、网页木马、SQL注入、跨站注入、管理入口以及敏感信息等等。以强有力的安全攻防团队为支撑，深入研究分析最新安全漏洞，及时更新漏洞库。

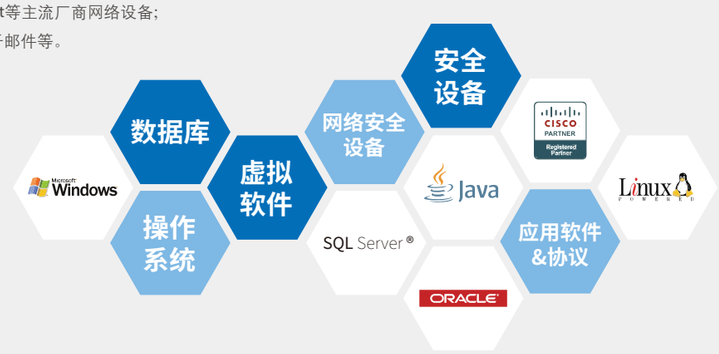
A1:Injection	A2:Cross Site Scripting(XSS)	A3:Broken Authentication and Session Management	A4:Insecure Direct Object References
A5:Cross Site Request Forgery (CSRF)	A6:Security Misconfiguration	A7:Failure to Restrict URL Access	A8:Unvalidated Redirecets and Forwards
	A9:Insecure Cryptographic Storage	A10:Insufficient Transport Layer Protection	

基于状态扫描的SQL注入扫描技术

采用自主创新的状态检测来判断，针对某一链接输入不同的参数，通过对网站反馈的结果使用向量比较算法进行比对判断，从而确定该链接是否为注入点，不依赖于特定的数据库类型、设置以及CGI语言的种类，对于注入点检测全面，不会产生漏报现象。

全方位的网络对象支持

网络主机：服务器、客户机、网络打印机等；
操作系统：Microsoft Windows 9X/NT/2000/XP/2003、Sun Solaris、HP Unix、IBM AIX、IRIX、Linux、BSD等；
网络设备：Cisco、3Com、Checkpoint等主流厂商网络设备；
应用系统：数据库、Web、FTP、电子邮件等。



多年积累的丰富的网码特征库

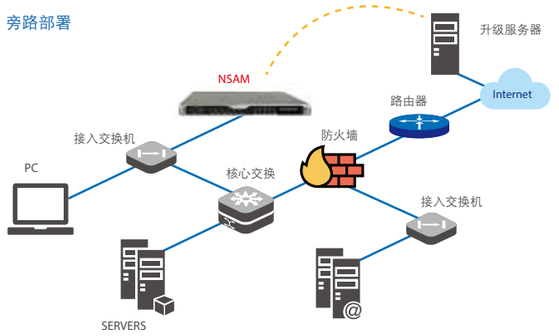
采用了研究团队多年积累的丰富网码特征库，不仅包括网码代码特征而且包括挂码网站的列表。
双重检测手段保障网码检测较低的漏报率和误报率，同时我们保证每周至少一次的特征库升级。

强有力的扫描效率保证

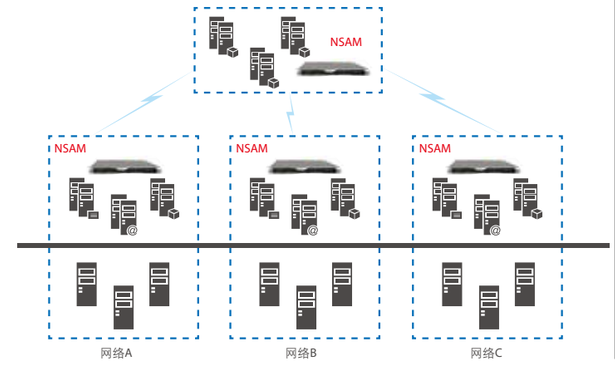
综合运用预探测、渐进式、多线程的扫描技术，能够快速发现目标网络中的存活主机
根据渐进式探测结果选择适合的扫描策略，启动多个线程进行并发扫描，从而保证了扫描任务可以迅速完成。

应用场景

旁路部署



分布式部署



功能特性

- 系统扫描
- Web扫描
- 数据库扫描
- 基线扫描
- 弱密码检测
- 扫描策略
- 安全域
- 资产自动发现
- 系统诊断
- 安全登录
- 报表分析
- 扫描结果展示
- 自动/手动升级
- 审计/告警

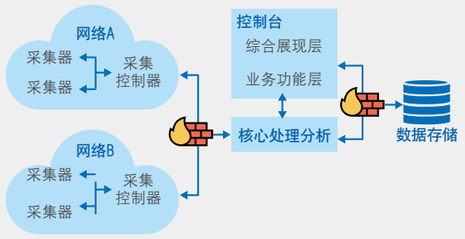
东软 NetEye 日志审计系统

产品概述

随着信息安全的不断发展，信息系统的多样化导致日志数量巨大、日志格式多样、用户无法进行重点分析、难以挖掘各类日志之间的关联关系等问题，为解决此类问题东软结合在网络安全领域多年的理论和实践经验特推出面向政府、企业和各类组织的日志审计系统，东软NetEye日志审计系统（SOC-LA）支持多种日志采集方式、日志支持种类多、扩展灵活，可智能关联各类日志信息，能够为用户从纷繁复杂的日志中萃取出具有价值的部分。

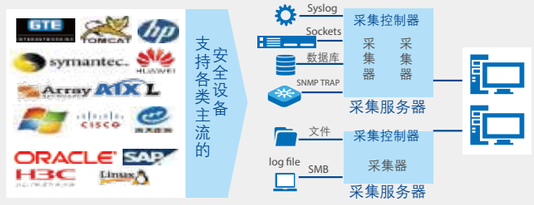
技术亮点

日志审计系统分为数据存储、管理控制（控制台）、核心处理分析和采集控制四大组件群，组网 、平滑扩展。



支持多种日志采集方式

包括Syslog、SNMP、trap、数据库、本地文件、控制台标准输出、TCP Socket等，同时扩展灵活，对于非主流的日志格式可快速自定义规则进行解析。

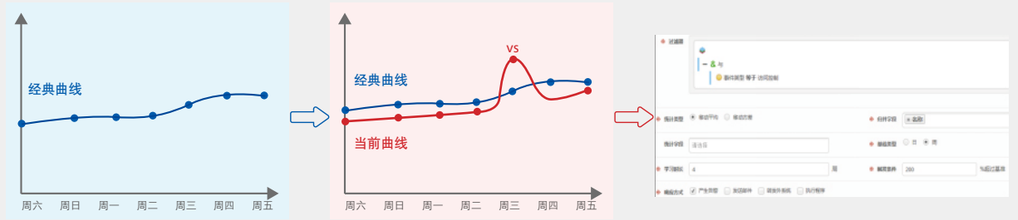


强大的二次分析能力

系统内置了大量审计策略模板，涵盖了常见的、对企业非常实用的审计策略模板，同时能够方便的自定义审计人员、行为对象、审计类型、审计策略等基本配置，提供强大的日志关联分析能力。

自学习的基线建模分析

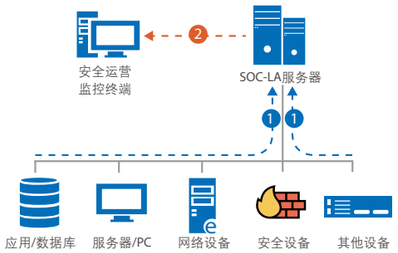
基于统计的关联，通过分析记录日基线和周基线的自动生成基线数据，并以此基线建模，判断信息系统中的安全事件。



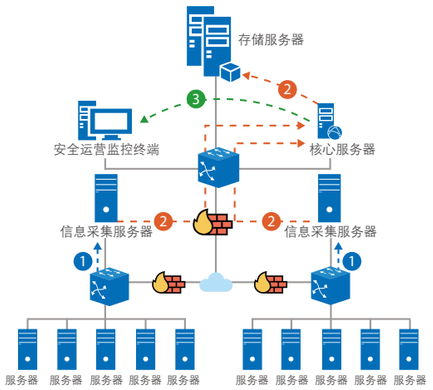
应用场景

根据用户网络规模的不同，东软NetEye日志审计系统支持单机部署和分布式部署两种方式——

单机部署：主要适用于网络结构较为简单的中小型企业。



分布式部署：主要适用于网络架构较复杂、需要跨网络区域运营的大中型企业。



功能特性

全面日志采集

全面支持对各种主流日志进行采集，同时支持对非主流日志的定制化采集。

便捷资产管理

自动发现企业网络中的设备，可便捷的定义所关注的设备为资产，从而进行持续的管理。

事件挖掘分析

对海量原始日志的分析挖掘，并与相关日志进行横向及纵向关联分析，发现异常安全问题。

审计与报表

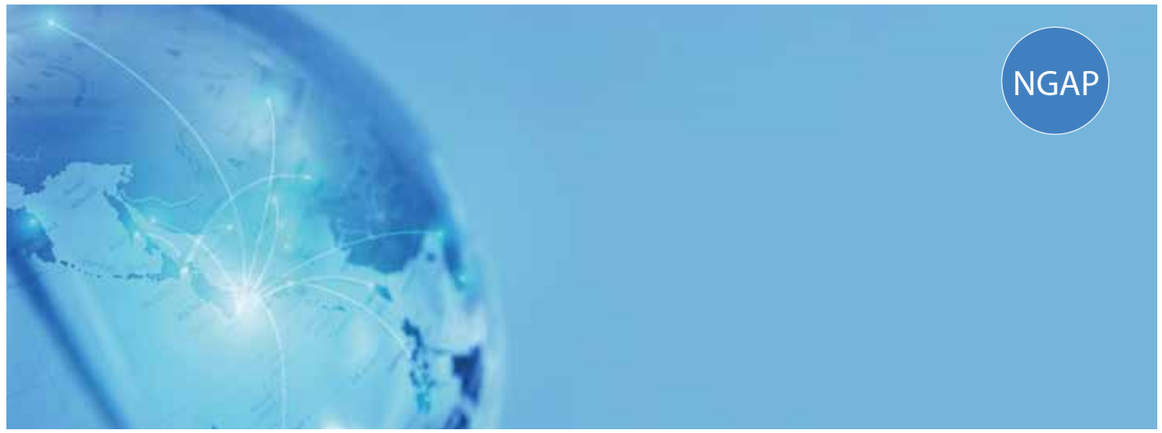
自定义审计对象、审计策略，从而满足不同行业用户日志分析、审计合规的需求。系统内置了各类实用的安全审计模板。

实时监控

实时滚动展示当前接收到的日志，显示内容可根据需要来定制过滤。

告警监控

以用户业务为视角，对收集到日志中的异常安全事件及审计违规情况进行集中告警展示，便于集中运维和审计管理。



东软 NetEye 安全隔离与信息传输系统

● 产品概述

东软NetEye安全隔离与信息传输系统（NGAP）由内、外网处理单元和安全数据交换单元组成，是使用带有多种控制功能的固态开关读写介质连接两个独立主机系统的信息安全设备。东软NetEye安全隔离与信息传输系统所连接的两个独立主机系统之间，不存在通信的物理连接、逻辑连接、信息传输命令、信息传输协议，不存在依据协议的信息包转发，只有数据文件的无协议摆渡。从而在保证在内外网隔离的情况下，实现可靠、高效的安全数据交换，而所有这些复杂的操作均由隔离系统自动完成，用户只需依据自身业务特点定制合适的安全策略即可实现内外网络进行安全数据通信，在保障用户信息系统安全性的同时，最大限度保证用户使用的便捷性。

● 产品优势

- **部署灵活：** 支持3种工作模式：透明模式、代理模式、路由模式，可适用各种网络环境的变化要求。
- **双重隔离：** 支持物理层及协议的双重隔离。
- **严格控制：** 可控制各种业务模块、动作、协议及各种参数。
- **审计功能：** 日志默认存储在设备中。并且支持通过标准SYSLOG的日志格式发送到远端日志服务器，为日志审计提供了很好的数据支撑和方便性。
- **管理安全：** HTTPS登录方式，是以安全为目标的HTTP通道，简单讲是HTTP的安全版。
- **应用广泛：** 支持最全及最常用的应用协议模块，有HTTP/DNS/POP3/SMTP/H323/SQLSERVER/ORA CLE/MYSQL/DB2/SSL 及自定义等多种协议。
- **性能高效：** 采用多核多线程运行操作系统及高效的数据定位算法，来保证低延迟，数据的准确性、高效性。

采用专用的安全通道进行内外网信息交换，业务数据通过物理隔离、协议隔离、内容隔离等措施使外网网络数据及有害数据信息无法进入高安全域内。

硬件结构上采用专用网络安全主板设计，进一步提高了设备的可靠性，可在超负荷的环境下长期稳定运行。双机热备的部署可使系统抗灾难性损坏时的可靠性成倍提高。

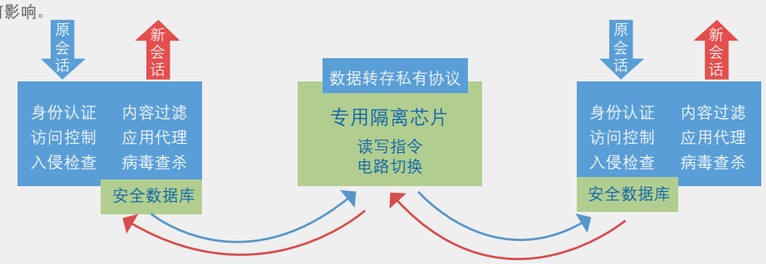
外网处理单元采用复杂对称多处理（RSNP)技术，在东软NetEye安全隔离与信息传输系统内集成多个处理模块，成倍提高处理能力使系统具有很高的性能。东软NetEye安全隔离与信息传输系统系统延迟小于1ms。

系统支持透明、代理、路由三种工作模式，可适应各种网络环境变化的部署要求，基于GUI的人性化管理方式更方便管理员的配置管理。

高安全性的系统架构

东软NetEye安全隔离与信息传输系统以独有的“摆渡+代理”技术为核心，内、外网双主机系统+专有安全通道为基础安全架构，为用户构建一套高安全性的软硬件系统。

东软NetEye安全隔离与信息传输系统采用专用的安全操作系统，完全剥离TCP/IP协议，各种TCP/IP结构异常的网络攻击不会对安全操作系统造成任何影响。

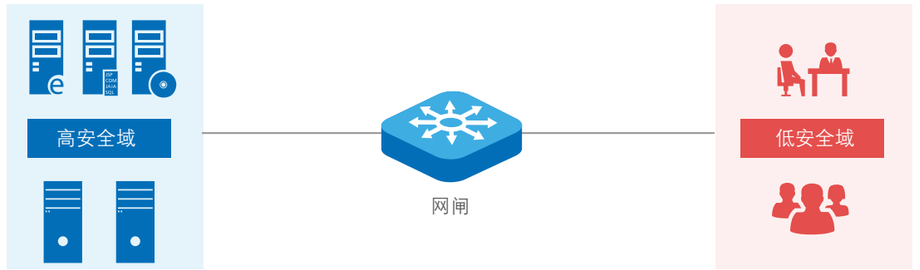


● 功能特性

功能	管理	易用性
• 安全隔离	• 用户管理	• 升级
• 协议隔离	• 管理员账户	• Web升级
• 应用隔离	• 认证账户	• 易用性
• 内容隔离	• 管理功能	• 备份
• 风险隔离	• 权限分配	• 诊断工具
• 信息交换	• 策略定制功能	• 高可靠性
• Web信息交换	• 日志功能	
• 文件信息交换	• 审计功能	
• 邮件信息交换	• 网络设置	
• 数据库信息交换	• 接口设置	
• 视频信息交换		
• DCS工控信息交换		
• 特殊定制信息交换		
• 双重安全防护机制		
• 文件内容控制		

● 功能特性

此部署方式适用于部分需要等级保护部门或网络中存在两种保护级别网络的企业或公司。



东软 NetEye 上网行为管理系统

产品概述

东软NetEye上网行为管理系统（NIBC）拥有丰富的上网行为管理、审计以及专业的流控功能，致力于帮助互联网用户控制和管理对互联网的使用，包括对网页访问过滤、网络应用控制、带宽流量管理、信息收发审计、用户行为分析。通过优化上网管理，有效提高企业内部IT资源的使用安全，帮助企业提高生产力，提升网络资源利用率，降低法律风险。

技术亮点

实名审计

功能特点

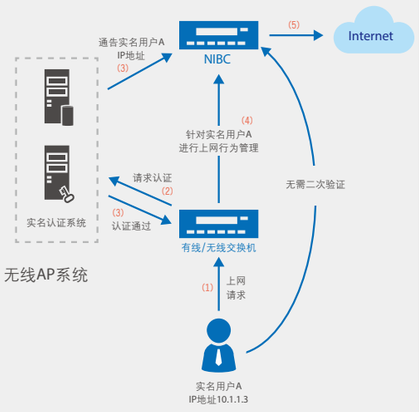
- 用户管理简便，实名账号自动学习
- 认证过程友好，无需二次认证
- 支持有线+无线的接入上网场景
- 实名制上网行为管理与审计

系统支持

- 锐捷SAM认证计费系统
- H3C IMC智能管理中心平台
- 城市热点认证计费系统
- 符合中国移动portal2.0规范的BAS、无线AP系统

适用场景

- 教育网学生上网实名制审计
- 运营商WLAN接入实名制审计
- 酒店上网实名管理审计（定制）
- 非经营性公共上网场所WIFI接入
- 其它需要使用实名制上网审计的场所



WIFI热点管理

WIFI（NAT模式）管控策略

- 可检测出WIFI热点的IP地址
- 通过防共享功能阻断WIFI热点
- 通过限制IP地址阻断非法WIFI
- 对合法WIFI的IP允许放行并审计
- 不能识别WIFI下接入的移动终端

WIFI（非NAT模式）管控策略

- 识别终端IP地址
- 识别终端品牌和操作系统
- 阻断非法终端/启动事件告警
- 合法终端可加入信任列表并审计
- 不能识别WIFI的IP地址

微信认证

产品提供的快速微信认证和实名审计功能，通过采集线下用户的微信号将线下用户转移至线上，从而减少广告成本，提升营销效率，支持点一点、扫一扫、连一连等多种微信认证方式，适用于酒店、商超、旅游景区、机场等公共场所。

个人行为审计

一个能够允许内网用户访问互联网的系统也必须及时关注具体用户对网络资源的使用情况，东软产品所提供报表中心不但可以从全局角度分析网络运行情况，还可以针对具体人的上网流量及行为进行全方位的记录，将统计数据从宏观到微观、整体到局部、层次分明的展现给管理者，帮助管理者在全局与细节上均能准确掌控网络的活动情况。

终端准入控制

终端准入控制主要对接入的终端进行主机健康检查和网络接入认证，在终端满足特定条件时，才准许使用网络资源，随着网络应用的普及和云计算的兴起，网络准入控制对保证网络边界完整，进行访问控制将起到非常重要的作用。

临时账号

随着移动互联网的普及，各种移动终端都会接入网络中，接入场景不光只是办公区域。还有访客接待区、会议室、公共教学区等等，东软NetEye上网行为管理系统可以针对不同场景接入的用户提供不同的身份认证方式，既保证用户身份的合法性，也让认证过程更快捷，从而降低用户的网络管理成本。

终端上网提醒

通过定期将HTTP流量重定向到指定的公告页面地址，从而把公告信息通过浏览器传递给终端用户，支持的终端系统包括：Windows、Android、IOS、Linux。

精细的流量管理

流控（QOS）是目前客户使用率最高的功能之一，但在一些特殊条件下（翻墙上网、私改IP、私接WIFI），会出现流控失效、非业务流量长期占用出口带宽而不被发现的情况，此时需要网络管理者手动添加规则封堵流量，配置繁琐维护成本高。东软NetEye上网行为管理系统提供的流量黑名单可以基于“流量”、“流速”、“时长”给用户设置流量配额。当配额耗尽后，系统会根据策略将用户的非业务应用加入到流控惩罚通道中，同时帮助管理员快速准确定位肆意占有网络资源的源头，减少后期人工维护成本。

功能特性

部署模式

- 透明模式
- 路由模式
- 旁路模式
- 混合模式

网络功能

- 静态/策略路由
- NAT
- PPPOE
- DDNS
- DHCP Server
- PPTP、GRE、IPSec VPN

冗余机制

- 双机热备
- 链路汇聚
- 多链路授权
- Bypass

流量控制

- 多线路带宽控制
- 最大/保证带宽
- 基于用户/应用7级流量通道
- 用户会话数限制
- 时间段控制

WIFI管理

- 无线热点发现
- 无线终端审计

用户管理

- IP/MAC/主机名绑定
- LDAP/Radius/POP3认证
- 微信/二维码/短信认证
- AD/PPPOE/WEB单点登录
- 临时账号申请
- USBKey免审计

上网行为管理

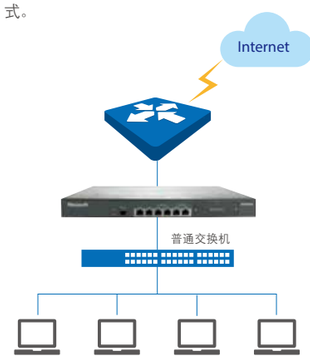
- 自动识别和智能分类
- P2P下载软件
- 网络流媒体软件
- Web视频
- HTTP应用
- 网络电话
- 网络游戏
- 股票交易
- 网上银行
- 根据特征码自定义7层服务

行为审计及报表

- 上网行为审计
- 流量审计
- IM/Mail/论坛/会话审计
- 多样化数据排名
- 内置/外置报表中心
- 应用限额策略

应用场景

东软NetEye上网行为管理系统支持多种部署模式：网桥模式、路由模式、旁路模式。



路由/透明模式（典型部署）

Service

服务保障

东软NetEye不仅设计研发具有自主知识产权的信息安全产品，并且凭借优秀、诚信的服务能力和高效、可靠的质量控制管理方法，为各行业组织提供覆盖信息系统全生命周期的全方位安全管家式服务。

安全体系建设顾问咨询服务

信息安全保障体系的建设需要遵循好的思路框架来构建，东软依据ISO27001、信息安全等级保护、SOX、IT内控等国际、国内优秀的信息安全体系标准，为各行业客户提供标准政策合规性咨询服务，制订合适的安全策略、措施和方案，确保组织机构具有完成其使命的信息安全保障能力。

安全风险评估服务

东软采用公认的ISO 27001、GB/T 20984-2007信息安全风险评估规范（中国国家标准）以及国家信息安全等级保护指南等安全标准进行风险评估工作；针对资产重要程度提供不同频率和方式的安全评估，帮助用户了解自身网络系统客观真实的安全现状，规划适合自己网络系统环境的安全策略，从而全面完整的解决可能存在的各种风险隐患。

渗透测试服务

渗透测试是为了证明网络防御按照预期计划正常运行而提供的一种机制，模拟黑客攻击行为通过远程或本地方式对信息系统进行非破坏性的入侵测试。渗透测试可以发现逻辑性更强、更深层次的漏洞，并直观反映漏洞的潜在危害，了解信息系统的真实安全状况，为信息系统的安全配置与管理提供指导建议。

等保合规咨询服务

信息系统安全等级保护作为国家信息安全保障的基本制度、策略和方法，目前已经在全国各行业大力推广，东软作为信息安全等级保护标准的践行者，帮助客户根据等级保护标准，落实具体防范措施。结合行业特点，为各行业用户提供从咨询规划、网络安全产品、网络安全服务到集成交付的整体解决方案。

安全加固服务

东软NetEye安全加固服务参照国际权威系统加固配置标准，并结合等级保护国家政策及行业规范，根据客户业务系统的安全等级划分和具体要求，对相应信息系统制定和实施不同策略的安全加固和配置优化，为系统及应用平台建立起一套适应性更强的安全保障基线，并以此作为保证客户信息系统安全的起点。

安全培训服务

东软拥有CISP国家级信息安全专业认证培训机构最高级资质，拥有多名CIWCI国际认证讲师。东软凭借在网络信息安全领域多年的产品研发、服务实施的经验积累，成功总结、规划和设计出一系列适合国内实际情况的信息安全培训课程，可以为各类组织的各层次人员提供全方位、高质量的个性化、系统化的专业培训服务。

应急响应服务

东软多年来一直协助国家层面提供重大互联网安全事故的处理工作，并于2004年成为首批国家级公共互联网应急处理服务技术支撑单位，为国家及各行业客户处理了包括大规模病毒爆发、网络入侵事件、拒绝服务攻击、主机或网络异常事件等上百项重大紧急安全事件。多年来，东软所处理的各项重大安全事故应急服务得到了客户的高度评价和广泛认可。

安全运维服务

东软作为“全球最佳表现IT服务提供商10强”，可以为各行业客户提供量身定制的日常安全运维服务，包括日常安全巡检监控服务、安全设备维护服务、安全预警通告服务、7*24小时应急响应服务、敏感时期的现场值守服务等，帮助客户从日常繁杂的IT运维工作中解脱出来。

覆盖全国的本地化服务能力

东软NetEye在北京、上海、广州、武汉、西安、成都、沈阳、济南设立8个大区服务中心，本地化服务覆盖范围达到国内40多个核心城市。同时，开通400-655-6789全国免费服务热线，随时随地响应客户的各类服务需求。

涉密信息系统分级保护

涉密信息系统分级保护是国家信息安全等级保护的重要组成部分，是等级保护在涉密领域的具体体现。东软网络安全具备行业领先的涉密集成及产品资质，依托遍布全国30余省的本地化交付体系，具备丰富的分级保护项目集成、产品实施及服务运维经验。以信息系统分级保护政策、规范为准则，结合涉密信息系统特点，落实具体防范措施，为用户提供卓有成效的定制化的整体解决方案。

Technology

技术能力

国家密码管理局

商用密码产品生产定点单位证书
商用密码产品技术鉴定证书
商用密码产品销售许可证

工业和信息化部省软件认定办公室

软件产品登记证书

国家保密局

涉密信息系统集成证书（系统集成/软件开发/运行维护）（甲级）

中国信息安全认证中心

中国国家信息安全产品认证证书
信息安全服务资质认证证书 应急处理资质
信息安全风险评估服务资质
信息系统安全集成服务资质
信息安全服务资质认证证书

中国人民解放军信息安全测评认证中心

军用信息安全产品认证证书

国家计算机网络技术处理协调中心

国家级网络安全应急服务支撑单位

国家版权局

产品著作权登记证书

中国信息安全测评中心

国家信息安全认证产品认证证书EAL3+级
国家信息安全测评信息技术产品自主原创测评证书
国家信息安全测评信息安全服务资质证书（安全开发类）
国家信息安全测评信息安全服务资质证书（安全工程类）
国家信息安全测评授权培训机构（注册信息安全人员培训机构）

国家计算机网络技术处理协调中心

涉密信息系统产品检测证书

中华人民共和国公安部

计算机信息系统安全专用产品销售许可证
信息安全等级保护安全建设服务机构

NetEye
1996

Approval

行业认可

2018

- 获安全可靠技术和产业联盟颁发“安全可靠事业的奋进者”称号
- 东软智能网联车载信息安全平台系统获中国网络安全产业联盟颁发“2018年网络安全创新产品奖”
- 东软车载集成安全网关获中国信息协会颁发“2017-2018年度新一代信息技术优秀解决方案奖”
- 东软获专用信息设备应用示范基地颁发“最佳合作企业奖”、“最佳突击攻关奖”
- 2018年信息安全与对抗技术竞赛（全国赛区）一等奖
- 第二届“强网杯”全国网络安全挑战赛线上赛优秀奖

2017

- 国家计算机网络与信息安全管理中心西藏分中心
- 2016-2017中国网络信息安全市场年度创新产品-东软车载安全解决方案S-Car
- 连续七届CNCERT/CC网络安全应急服务支撑单位（国家级）
- 2017年度安全可靠优秀解决方案商
- 中国IT市场年会中国新兴产业创新典范企业
- 东软NetEye集成网关NISG获得中国IT市场年会年度影响力产品奖
- 东软云安全获得中国IT市场年会年度创新产品奖

2016

- 国家计算机网络应急技术处理协调中心北京分中心
- 中国农业银行内蒙古分行
- 安徽省人民检察院
- 中国防火墙产品市场“年度成功企业”
- 2016年度“最佳网站类安全产品”奖
- 2016年度中国软件行业优秀产品奖
- 2015-2016中国防火墙产品市场年度成功企业
- 第二十届中国国际软件博览会金奖

2015

- 山东省农行科技与产品管理部
- 国家电子政务外网管理中心
- 中国建设银行安徽省分行
- 巴彦淖尔市人民检察院
- 嘉兴市人民检察院
- 烟台市人民检察院
- 烟台市牟平区人民检察院
- 软博会创新奖-高性能下一代防火墙
- 2015十佳安全方案商
- 第十九届软博会创新奖-高性能下一代防火墙
- 2015方案商峰会十佳安全方案商
- 第二届世界互联网大会信息安全设备供应商

2014

- 国家计算机网络应急技术处理协调中心
- 山东省农行科技与产品管理部
- 江苏省烟草公司信息中心
- 烟台市牟平区人民检察院
- 2013-2014中国防火墙市场年度成功企业
- 2014十佳安全方案商
- 第十八届软博会东软NetEye统一身份管控系统 V2.0
- 2013-2014中国防火墙市场年度成功企业
- 2014方案商峰会十佳安全方案商

2013

- 中国农业银行黑龙江省分行
- 山东省农行科技与产品管理部
- 海南省国土环境资源信息中心
- 中国农业银行内蒙古分行
- 2012中国IT商业伙伴冠军调查评选安全产品备件储备满意度第一名
- 2012年海南省CIO可信赖的信息安全服务商
- 2012年度中国最佳IT供应商
- 中国软件渠道满意度优秀企业

NetEye

因需而变 因御而安

全球领先的网络安全产品及服务供应商