新华三集团

北京总部
北京市朝阳区广顺南大街8号院 利星行中心1号楼
邮编:100102

杭州总部
杭州市滨江区长河路466号
邮编:310052

www.h3c.com

Copyright © 2020新华三集团 保留一切权利
免责声明：虽然新华三集团试图在本资料中提供准确的信息，但不保证本资料的内容不含有技术性误差或印刷性错误，
为此新华三集团对本资料中信息的准确性不承担任何责任。新华三集团保留在没有任何通知或提示的情况下对本资料的内容进行修改的权利。
CN-173X30-20200820-BR-DD-V1.0

紫光集团 | H3C
核心企业 | 数字化解决方案领导者

主动安全
智护数字未来

目 录

CONTENTS

新华三网络安全

新华三集团（以下简称“新华三”）在安全领域拥有近二十年的经验积累，拥有1100多项安全领域专利技术，近40大类超400款专业安全产品，覆盖网络安全、云安全、工控安全、数据安全和等级保护等细分领域，具备业界最全面的安全产品和解决方案付能力，可为用户提供可信、可控的全系列网络安全产品及完整的“云-网-边-端”一体化解决方案。

2003

华三成立，发布F100/F1000系列防火墙，正式进入专业安全领域

2004~2007

国内首创全系列SecBlade安全插卡

国内第一台IPS产品发布

SecBlade万兆插卡发布

2008~2010

业界最高端的40G防火墙F5000-A5发布

业界首款全千兆UTM发布

2011~2014

业界最高性能40Gbps SecBlade安全插卡发布

业界最高端M9000分布式综合安全网关发布

2015~2016

新华三大安全解决方案发布

云安全解决方案规模落地

2018

主动安全体系发布

安全云及云墙发布

态势感知2.0发布

2019

全系AI防火墙发布

等保2.0解决方案发布

安管一体机1.0发布

云安全解决方案2.0发布

2020

发布主动安全2.0

安管一体机2.0发布

生态合作战略3.0发布

2021

云安全2.0战略发布

新一代应用交付发布

安全一体机3.0发布

全新一代旗舰M9000-AI-X系列产品发布

零信任解决方案1.0发布

数据安全解决方案2.0发布

工控安全解决方案2.0发布

超融合态势感知一体机发布

新华三网络安全实力

技术实力

1100+
超过1100件
完全自主可控的
网络安全领域专利

1000+
超过1000人的
研发、攻防及服务咨询
专业团队储备

300+
云安全解决方案服务于15个国家部委级、22个省级和300余个地市区县政务云，并且在各行业云市场拥有超过10000个用户实践

400+
超过400款产品，
40+大类信息安全产品
知识产权

市场地位

- 连续多年，中国防火墙、IDP、内容安全市场份额排名前三（IDC）。
- 连续多年入围Gartner防火墙魔力象限，Gartner全球企业网络安全设备市场销售额同比增长率排名第一。
- 防火墙、入侵防御系统、负载均衡等安全产品连续12年入围中国移动、中国电信、中国联通三大运营商，综合市场份额第一。
- 连续12年入围中国工商银行入侵防御系统设备供应商。
- 广泛服务于政府、运营商、金融、企业、教育、教育、能源、大型企业等各行业客户。
- 开放的平台，积极与国际安全组织CVE、微软MAPP、云安全联盟等联合提供最优安全体验，积极跟进前沿安全技术发展趋势，针对新IT时代特点，推出主动安全战略及解决方案。

新华三安全重点参与国家顶层设计

国家网络安全技术主要建设者

新华三主导和参与制定网络安全领域标准二十余项

- GB/T 35279-2017《信息安全技术 云计算安全参考架构》
- GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》
- GB/T 28448-2019《信息安全技术 网络安全等级保护测评要求》
- GB/T20281-2020《信息安全技术 防火墙安全技术要求和测试评价方法》
- 新华三联合国家信息中心发布：政务云等保2.0顶层设计+实施指南

安全机构核心成员

- CNNVD技术支撑单位最高等级证书（一级）
- 中国网络空间安全协会理事会员
- 中国国家信息安全漏洞库CNNVD一级技术支撑单位
- 中国可信计算联盟理事会成员
- 中国互联网协会反网络病毒联盟(ANVA)成员
- 云安全联盟(CSA)理事成员
- 合肥市新一代人工智能产业发展联盟理事单位

CNNVD技术支撑单位
最高等级证书（一级）

国家信息安全漏洞共享平台
CNVD技术组成员

国家信息安全漏洞共享平台
年度突出贡献单位

云安全联盟CSA理事成员

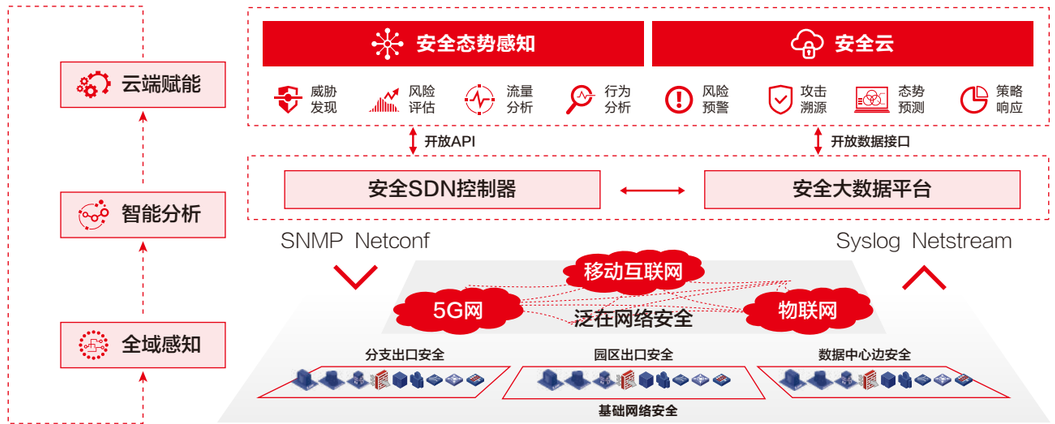
全面的安全产品资质

- 计算机信息系统安全专用产品销售许可证
- 中国国家信息安全产品认证证书
- 网络关键设备和网络安全专用产品安全认证证书
- IT产品信息安全认证证书
- 计算机软件著作权登记证书
- IPv6 Ready Logo 认证证书
- 信息技术产品分级评估证书（EAL）
- 商用密码产品认证证书
- 进网许可证
- 信息技术产品安全测试证书

联合IDC发布技术白皮书

联合专业咨询机构IDC发布技术白皮书，践行市场技术趋势，实现从理论分析到产品落地。

用全局观打造新一代的网络安全主动防御系统



主动安全：主动发现 智能分析 提前预警 及时响应

大安全时代带来全新挑战

近年来网络安全领域颇不平静：勒索病毒肆虐全球150多个国家，更有规模惊人的数据泄露和频繁发生的网络攻击事件。网络安全行业陷入尴尬境地——用户的安全投入不断增加，安全事件的爆发却更加频繁。

可见随着物联网、云计算、大数据等新技术的普及，我们已经进入了网络攻击对象扩大化、攻击方式多样化、攻击常态化和攻击影响更深远的“大安全时代”，传统的网络安全防护理念和体系已无法适应当前的网络安全形势。

传统安全防护的重心在于边界防护——终端防护、网络防护、主机防护等，在不同的区域间通过安全设备构筑了分割孤立的防护体系，彼此之间缺乏信息共享和防护协同，在层出不穷的漏洞和高级攻击手段面前，看似强固的安全防护堡垒成为了摆设。

在大安全时代，我们不可能将一切都控制在边界之内，不可能防护住所有的设备，不可能提前发现和修复所有漏洞。“理念决定行动”，我们的网络安全观已经到了必须革新的时候了。

早在2016年的国际安全技术大会上，安全专家已发出“传统安全防护已失败”的警告，认为未来的防护重点将从预防转向检测与响应。在入侵已经不可避免的情况下，及时检测和快速响应安全威胁，才是降低安全损失的现实选择。

有什么样的安全观，就有什么样的方法论。新华三认为，要成功应对“大安全时代”的网络安全挑战，我们首先需要树立整体与全局的安全观。

树立整体、全局的网络安全观

整体与全局的安全观是指从整体、全局的角度来看待、规划和管理网络安全，而不是仅仅关注单点安全、单个安全防护手段，或单个防护设备。

整体与全局的安全观要求我们在做网络安全体系建设时，考虑全局、完整的安全体系设计，包括前期的咨询、评估、方案部署和后期运维与服务，让安全成为IT解决方案的有机构成，而非后期补丁式的安全防护。

整体与全局的安全观还要求我们扩大安全防护对象：不仅包括传统防护对象——终端与网络，更要注重云端、物联网设备，以及应用的安全防护；不仅防护企业自身系统的安全，更要防护第三方合作伙伴的系统安全。

在安全防护上，我们要跳出单点防护思维，从整体和全局来把控网络安全态势。过去终端防护、网络防护、主机防护等孤岛式工具，犹如九龙治水，各管一摊，彼此缺乏信息共享与协同，无法最大程度发挥安全防护能力。

整体与全局的安全观还需满足等保合规的要求。等级保护是《网络安全法》要求的法律责任。复杂、多样的等保合规要求往往是传统的单个安全厂商无法满足的，需要具有全面安全防护能力的厂商。

在整体安全观下，数据成为威胁攻击的真相之源，成为发现网络攻击的关键。攻击者无论怎样隐藏行踪，总会留下数据痕迹。将终端、边界、云端的流量与日志汇总起来，通过大数据平台分析和威胁情报支持，可以改变过去那种“只见树木、不见森林”的状况，达到对整体网络安全态势的全面掌控，实现对安全攻击的及时响应和处置，最大程度降低安全损失。

所以用户现在更需要一站式的解决方案，能将终端、边界和云端的安全防护融合起来，通过一个整合平台提供全面的安全防护体系，从而让用户将精力用于业务发展上。

新华三主动安全防御系统

作为践行国家网络安全战略的先行者，新华三遵循理念先行、全面防护的战略，立足作为具备最全面安全交付能力的厂商，为用户提供全系列信息安全产品及完整的解决方案，做到从底层信息安全基础设施到顶层应用，可以为用户提供安全可信的新一代主动安全防御系统。

以安全态势感知为核心打造新一代主动防御系统 践行全局网络安全观

新华三认为，只有从被动防护向主动防御转变，通过安全态势感知把原来分散的安全设备、网络设备、服务器、防病毒软件等各IT部件有效组合起来，形成一个能自学习，自演进、预测未知威胁的多维度、多层次主动防御系统，才能真正应对大安全时代的挑战，也是践行整体、全面安全观的最佳方式。

在2016年“4•19”网络安全和信息化工作座谈会上，习近平总书记提出，“要树立正确的网络安全观，全天候全方位感知网络安全态势，增强网络安全防御能力和威慑能力。”网络安全态势感知系统的重要性可见一斑。

根据知名研究机构IDC报告，**网络安全风险态势感知系统将是主动安全防御体系的“指挥中心”，它能帮助用户认清威胁环境的变化，掌控威胁发展趋势，积极主动防御，提升企业安全能力。**

新华三在2017合肥网络安全大会上正式发布了主动防御系统的核心产品——安全态势感知系统，其通过采集全网原始流量数据，结合机器学习和人工智能，对海量异构的安全数据进行挖掘和关联分析，对攻击、威胁、流量、行为、运维和合规等六大态势进行感知，生成全方位的安全全景视图，使用户能够快速准确地掌握网络安全全局态势，及时发现威胁、处理风险，支撑安全决策和应急响应，建立安全预警机制，增强整体安全防护能力。新华三安全态势感知系统可以利用产业联合的集大成者的优势，将各方的日志与告警数据收集起来，同时利用新IT领先厂商的优势，汇集网络和云端流量，为用户呈现“更完整、更全局的”安全态势。

作为复杂的系统性工程，要真正发挥主动防御系统的价值，对于安全厂商和用户都存在较大考验，需要从技术支撑、组织保障、运行维护、外部合作等方面进行协同联动。因此，新华三将主动防御系统视为一种安全服务，包括前期调研、定制开发、部署和后期的响应服务。通过遍布全国的新华三安全专家，可以给用户提供更加及时的安全响应与服务，构筑“预知未来、主动发现、协同防御、智能进化”的安全创新体系。

新华三网络安全生态合作战略

“新基建”大潮下，安全成为数字化基础设施的关键支柱。为了向行业用户提供主动式全方位的安全防御体系，以及持续快速响应的安全服务，新华三于2017年业界率先提出“主动安全”理念，并于同年发起“网络安全创新技术联盟”，号召与推进安全产业内的生态构建，致力为行业用户交付一站式安全解决方案及服务。作为安全产业生态合作的引领者和倡导者，新华三以领先的主动安全理念、出色的安全服务能力，围绕全栈、意图和使能三大关键词，发挥出“领头羊”的核心优势，引领联盟成员数量极速扩充至50余家。在业绩表现上，作为联盟核心成员，新华三安全业务发展迅猛，3年来业绩获得大幅提升，生态合作业绩更是持续翻番，服务星级合作伙伴突破350+家。在2020年上半年，新华三克服疫情的影响，安全产品业务同样实现了高速增长。

网络安全是数字经济持续健康发展的前提与保障，新华三希望为行业客户提供一站式的解决方案与服务，这就需要自身聚焦主航道，精耕细作主流产品与技术，并加大产业生态的建设，广泛联合生态伙伴的智慧力量，朝着共同支撑客户业务安全应用的目标，打造主动安全体系，助力客户构建安全的数字世界，为此新华三发布生态战略3.0。

1.0时代（~2017）

- 生态体系初步搭建
- 部分领域开启产品级合作

2.0时代（2017~2020）

- 完善生态体系，扩大合作领域
- 伙伴数量与业绩持续翻番

3.0时代（2020~）

- 打破传统合作模式的天花板
- 新华三安全生态战略全面升级

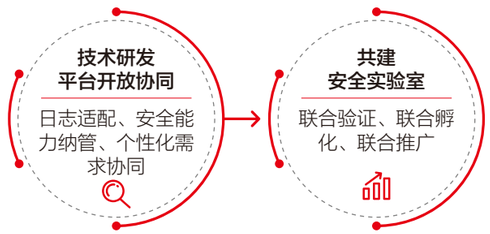
“新华三安全生态合作战略3.0”计划以雄厚产业投资基金为支撑，致力在安全产品技术生态、安全渠道生态、安全服务生态三大领域携手合作伙伴深化合作，并在共享市场侧资源、开放安全软件平台、共建安全联合实验室、大服务体系赋能等方面不断为合作伙伴提供助力，从而拉动生态产品的整体营销与市场规模。

产品技术生态合作

在安全产品技术生态合作上，新华三携手合作伙伴将围绕主动安全体系进行关键产品的合作研发与迭代，聚焦在场景化方案全面扩大产品合作的深度和广度。同时还将提供研发平台的开放协同、创新实验室联合验证等资源，帮助生态伙伴提升整体方案和产品的核心竞争力。

技术生态：提升方案、产品的核心竞争力

围绕主动安全体系，进行关键产品的合作研发与迭代，聚焦场景化方案全面扩大合作深度与广度，提升方案与产品的核心竞争力。



安全渠道生态合作

新华三将联合安全伙伴打造集商业环境、差异化产品、专业服务能力的三维渠道合作生态。通过差异化的产品交付、场景化整体解决方案来实现市场无缝覆盖，集培训/测试/交付一站式服务协助合作伙伴，大幅提升专业化销售能力。此外，新华三预计将投入千万级别的安全拓展基金和安全赋能基金，来奖励优秀合作伙伴并培养专业安全人才，实现互惠共利。

渠道生态：共享市场资源

打造集商业环境、差异化产品与场景化解决方案、专业服务能力三位一体的渠道合作生态。

安全服务生态合作

新华三将对包括精英服务商、专业服务商、培训服务商的各类服务伙伴赋能与认证。通过专业服务商拓展来实现全国规模化安全服务采购；在安全攻防平台、赛事组织上形成战略合作的基础上，加大培训服务商的拓展，进一步完善全方位服务商体系，确保伙伴收益。

安全服务生态：共拓安全服务市场空间

全面打造与完善服务商培训认证体系，共同开拓专业安全服务市场空间与份额。

精英服务商
重点保障安全服务领域的项目收益

专业服务商
实现专业安全服务全国规模化采购

培训服务商
攻防平台、赛事组织战略合作，共享培训机会

产业基金扶持

在技术、渠道与服务等合作维度之外，新华三将对重点合作伙伴提供基金扶持，帮助其改善财务结构，提升公司治理水平，制定发展战略，并助其展开资本运作。

产业基金投资：帮助合作伙伴快速成长

对优质合作伙伴进行产业基金投资，从常规生态合作升级到战略投资层面。

业绩共担
资源共享

帮助改善财务结构
提升公司治理水平

制定发展战略
助力资本运作

基于以上各维度生态合作计划，新华三还构建了国内最完善的安全合作伙伴评级与进阶体系，按照不同合作方向与资源支撑力度分为最佳合作伙伴、杰出合作伙伴和优秀合作伙伴三个梯度。不同的安全合作伙伴面向不同的市场，匹配不同的市场运作方式、技术研发资源及资金扶持力度，最大化驱动生态伙伴的成长与进阶。

新华三的“第一责任人”制

“第一责任人”是新华三在安全生态中的角色定位。

我们希望与合作伙伴开展代码级的合作研发，配备专业团队支撑代码、UI以及日志的适配，对合作伙伴的产品进行全面安全纳管，向客户交付整体的解决方案。在这个过程中，新华三将作为“生态产品质量、安全服务交付以及伙伴认证培训的“第一责任人”，真正实现生态意义上的紧耦合。

——孙松儿

新华三副总裁 安全产品线总裁

基于新华三优质的客户资源、完善的产学研平台及成熟的大服务体系，加入生态计划的合作伙伴将全面提升开发水平与产品质量，扩大市场销售平台，促进供应链管理能力以及高效的体系化交付能力。这些赋能与增值行动，将进一步加强新华三与合作伙伴构建的安全生态，从而为用户打造全面的主动安全防御体系，提供一站式的安全解决方案。

作为国内安全的领军企业，未来，新华三将携安全合作伙伴一同构建与壮大主动安全生态，共享网络安全产业的增长红利，护航新基建，为数字经济提供全方位的安全保障。

新华三网络安全产品

打造国内最强安全产品线

安全态势感知系统

安全态势感知系统

网站安全监测系统

综合日志审计系统

安全管理

超融合态势感知一体机CSAP-X

安全业务管理平台

数据库审计系统D2000系列

运维审计系统A2000系列

安全云管理平台

安全体检

安全控制器

安全运维

安全管理

IAM统一身份管理与安全认证系统

安管一体机X6000系列

EAA加密应用分析系统

边界安全

F1000-AI/F5000-AI/M9000系列

入侵防御
T1000/T5000/T9000系列产品

SecBlade插卡系列
ServerBlade插卡系列

抗DDOS
AFC2000系列

防病毒网关
AVG2000系列

安全隔离产品
GAP2000系列
G9000系列

应用安全

负载均衡
L1000/L5000/M9000-AD系列

上网行为管理
ACG1000系列

WEB应用防火墙
W2000系列

漏洞扫描
SysScan系列

工控安全

ISG-MGT工控
安全管理平台

工控防火墙F3000系列
工控监测审计A3000系列

终端安全

服务器安全
监测系统

终端安全
管理系统

网页防篡改

工控主机
安全卫士

NFV

防火墙

上网行为管理

入侵防御

负载均衡

数据库审计

WEB防火墙

漏洞扫描

运维审计

专业安全服务

安全咨询规划

攻防渗透护网

安全运维服务

用全局观打造新一代的网络安全主动防御系统

新华三安全态势感知系统以安全大数据为基础，对能够引起网络态势发生变化的要素进行获取、理解、评估、呈现以及对未来发展趋势进行预测；从全局视角提升对安全威胁的发现识别、理解分析、响应处置的能力；通过智能分析和联动响应，结合机器学习和人工智能，实现“安全大脑”的闭环决策，以及安全能力的落地实践，真正做到对安全风险威胁的“主动发现、预知未来、协同防御、智能进化”。

产品特性

多样化数据采集

- 支持各种网络设备、安全设备、漏扫设备、主机及应用日志采集，可接入外部威胁情报
- 采用主动、被动技术实时采集网络中的异构海量日志；支持 SYSLOG 协议、HTTP/HTTPS 被动采集、FTP、数据库主动采集、部署代理等多样化日志接入
- 支持海量日志集中存储或分布式存储，满足快速查询的海量日志的要求
- 通过日志范式化和日志分类支持不同厂家日志与系统的快速适配

基于 AI 的智能化威胁分析

- 根据使用场景的不同，主动调整模型算法参数，使安全分析结果更加贴合网络实际情况
- 基于现有安全事件，依托攻防专家经验，关联资产、情报等多维信息，提供“专家级”推理分析
- 引入监督学习、强化学习等 AI 人工智能算法，利用“知识大脑”推理检测已知及未知类型的复杂攻击，全面掌握规模群体性事件的感染路径
- 建立行为基线，通过资产 / 用户的流量、动作等行为的偏离情况，判断各类异常行为

多维度风险预警

- 通过可视化技术的利用，将原本碎片化的威胁告警、异常行为告警、资产管理等数据结构化，形成高维度的可视化视图
- 通过全网威胁情报和大数据分析对入侵事件进行实时检测，提供丰富多样的数据可视化效果，包括 3D 图表、雷达图、拓扑图、热度图等样式
- 以安全大数据为基础，从不同视角和维度进行风险呈现，实现安全事件实时监控与预警

全过程溯源取证

- 针对攻击全过程对攻击者留下的任意线索进行多维拓展，可视化绘制出完整的攻击链条
- 对安全事件进行回溯和调查，主动对攻击过程进行抓包取证，提供完整攻击证据
- 针对 NAT 应用场景，基于 IP 和时间段信息，追溯地址转换关系，并呈现对应的安全事件
- 利用云端丰富的实时威胁情报和本地的网络行为、终端行为、文件信息，覆盖攻击的源头、手段、目标、范围等相关信息，对发现的未知威胁进行快速溯源和定性

自动化编排与响应

- 根据发现的安全事件，自定义安全响应剧本，根据防护需要调整处置步骤
- 响应处置动作类型多样，包括黑名单阻断、访问控制、告警、工单处置、用户下线、主机病毒查杀及隔离等操作
- 不仅可以针对 FW、IPS、WAF、ACG 等常见安全设备进行调度，更可以对交换机、路由、无线 AP 等网络设备进行调度
- 规范处置流程，提升安全管理水平

漏洞全生命周期管理

- 漏洞扫描联动，支持第三方漏扫结果导入
- 通过工单任务实现了漏洞加固任务的下发、审核、复验等功能
- 支持漏洞加固任务处置状态跟踪，对超期未处理任务可进行邮件短信提醒
- 支持人工或工具的方式对漏洞进行复验。并根据验证结果自动同步漏洞当前状态

典型应用场景

安全事件分析、流量及行为分析、威胁场景化分析、

全网资产风险画像分析、响应编排闭环处置、风险大屏可视化

H3C SecCenter CSAP-X 超融合态势感知一体机

H3C SecCenter CSAP-X

H3C SecCenter CSAP-X超融合态势感知一体机产品是经过众多网络安全体系建设实践，自主研发的一款网络安全运营管理综合性一体化安全设备，具有态势感知分析、威胁检测分析、安全设备管理、远程专家会诊、漏洞扫描、终端安全、安全知识大脑深度威胁检测7大功能模块，全面满足安全分析和网络安全运营管理需求。通过一体机设备集成多样功能模块，部署配置简单做到了极简交付；多种功能模块做到了数据打通，无需复杂配置；态势感知平台具备强大的安全分析和可视化呈现能力；同时具备远程专家会诊功能，通过云端协同实现外部安全服务资源的整合，为用户带来快速见效的安全能力，以达到加速检测与响应的目标。

产品特性

省事 – 超融一体

- 多功能融合，方案简单，部署简单，无需改变网络结构。

省时 – 极简配置

- 开箱即用，无需过多复杂配置，快速交付，组件统一监控、统一授权。

省心 – 安全服务

- 内置远程专家会诊系统，平台问题专家远程诊断，快速解决，无需担忧。

合规 – 等保合规

- 围绕等保 2.0 和网络安全法，满足日志存储分析和安全管理中心要求。

典型应用场景

多产品一体化解决方案场景、态势感知分析场景、等保合规要求场景

H3C SecCloud安全云管理平台

新华三OMP安全云管理平台是由新华三自主研发的，面向云计算环境的平台管理类软件，用于集中管理各类软硬件安全产品，实现云安全服务灵活编排，为云平台和云租户提供灵活、高性能的安全能力。产品提供安全服务化、流量编排、策略管理、计量计费、态势呈现等诸多功能，为各类政企用户的云安全保驾护航。

产品特性

云安全集中管理

- 安全资源在云端可见，云平台管理员、租户管理员以及租户根据职责、权限被赋予了不同的管理能力。

安全资源按需申请

- 将软硬件安全资源服务化，形成云端安全的服务目录，包括 FW、LB、WAF、抗 DDos、数据库审计、漏扫、堡垒机、态势感知等。

租户自主化管理

- 租户可对所管设备直接下发关键策略，同时也可登录设备进行全面管理。

安全服务编排能力

- 对安全防护资源具备流量编排能力，完成三层编排。当任意安全服务不可用，可通过编排器自动完成跳过，以保障业务的连续性。

软硬件池化管理

- 管理员可以按需将安全硬件实例化，形成硬件共享资源池，并可将此与 NFV 实例混合，提供软硬混合资源池。

运维 / 运营展示

- 安全资产使用情况的统计、展示、计费等，可提供运营层面的消费报告，安全资产运行状况的展示、系统安全指数等，汇总租户级安全报告。

集成安全服务

- 可在线申请应急响应、安全协维、安全培训、渗透测试等安全服务，形成服务流程化管理。

兼容性管理

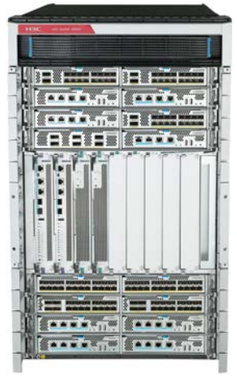
- 可通过单点登录的方式实现与第三方安全产品的对接，做到和用户现有产品的兼容性管理。

典型应用场景

公有云、私有云、专有云等云场景

安徽省政务云、四川省政务云、江西省交通厅、紫光云、河南大象融媒

H3C SecPath M9000系列 多业务安全网关



H3C SecPath M9000系列多业务安全网关是新华三结合云计算、5G、物联网、IPv6、大数据及高性能计算的发展趋势，针对云计算数据中心、运营商CGN、大型企业及园区网出口等市场推出的新一代高性能多业务安全网关。同时，是新华三结合云计算、5G、物联网、IPv6、大数据及高性能计算的发展趋势，针对云计算数据中心、运营商CGN、大型企业及园区网出口等市场推出的新一代高性能多业务安全网关。

H3C SecPath M9000系列采用高性能多核CPU+AI计算芯片的芯架构，在AI人工智能算法的加持下，全面支持AI网络内容安全审计、AI加密应用识别、攻击防范……全面支持攻击防范、异常流量清洗、未知威胁检测、服务器异常外联检测、敏感数据保护、web应用安全防护、访问控制、安全域划分、黑名单、流量监控、邮件过滤、网页过滤、应用层过滤等功能，能够有效的保证网络的安全；深度业务安全检测可更细致的为web服务器提供保护；支持多种VPN业务，满足多种高性能VPN接入的需求；支持业界最丰富的NAT特性，满足各大运营商的NAT需求；全面支持IPv4/IPv6双协议栈。

目前在线部署数千台，为各行各业保驾护航。

型号：

■ M9000-AI-E8　■ M9000-AI-E16　■ M9006　■ M9010　■ M9014

■ M9008-S　■ M9012-S　■ M9010-GM

产品特性

高性能的软硬件处理平台

采用控制、业务、数据相分离的全分布式架构，控制引擎、交换引擎、业务引擎及接口单元硬件分离，解耦合系统关键部件，提高系统可靠性；独立的硬件交换引擎，支撑高性能安全业务无阻塞处理及转发。

电信级设备高可靠性

采用新华三自主知识产权的软、硬件平台，设备主要部件均采用冗余设计并支持热插拔，支持 ISSU 不中断业务方式升级，提供业界最高的可靠性。

支持 SCF（安全集群框架）

支持多框集群，实现零落管理和弹性扩展。全面突破机框的限制，在简化管理和部署的基础上同时实现了安全业务和安全性能的弹性扩展。

支持安全 ONE 平台 (SOP)

采用创新的基于容器的虚拟化技术实现了真正意义上的虚拟设备，支持对系统静态及动态的资源进行细粒度的划分，不同虚拟设备间实现操作系统级的隔离。

典型应用场景和用户

城域网 NAT444、大型数据中心安全、校园网出口

四川移动、江苏移动、广州联通、广西政务云、郑州市政务云、中粮集团、安徽农金、重庆银行、南开大学、陕西师范大学

H3C SecBlade安全插卡系列

H3C SecBlade FW防火墙模块/SecBlade IPS入侵防御系统模块/SecBlade ADE应用交付模块/SecBlade NS流量分析模块；丰富的安全模块种类、顶级的安全业务处理、多安全特性集成、复杂网络协议适配、全面支持各类型网络主机平台。

型号： ■ SecBlade

H3C SecPath F1000/F5000系列 AI防火墙

伴随Web2.0时代的到来并结合当前安全与网络深入融合的技术趋势，新华三针对各类运营商、企业数据中心、园区网、广域网等场景推出AI系列高性能防火墙，即H3C SecPath F1000/F5000 系列AI防火墙。它能够支持多维一体化安全防护，可从用户、应用、时间、五元组等多个维度，对流量展开IPS、Anti-Virus、DLP等一体化安全访问控制，能够有效的保证网络的安全。同时采用新华三最新的SCF、SOP虚拟化技术，结合SDN实现动态、按需调度防火墙资源，让网络安全感知与攻击防护知行合一。结合AI算法，AI防火墙能够识别更多威胁，适应日益复杂的安全态势。

型号：

■ F1000-AI-10　■ F1000-AI-25　■ F1000-AI-35　■ F1000-AI-55　■ F1000-AI-65

■ F1000-AI-75　■ F1000-AI-60　■ F1000-AI-70　■ F1000-AI-90　■ F5000-AI-20

■ F5000-AI-40

产品特性

H3C SCF 集群 &SOP 虚拟化技术实现防火墙资源池，防火墙资源按需调用，重新定义安全产品部署架构。

H3C SMP 安全业务管理平台，与 NGFW 紧密关联，实时感知威胁并且能调度防火墙资源防护。

全面支持 SDN Overlay 网络，改变复杂部署模式，用软件量身定制的安全即服务 (SAAS)。

多种高性能 VPN，无缝对接 iOS、Android，紧密联动 H3C BYOD 方案，移动办公一触即得。

典型应用场景和用户

政务云、公有云、私有云等各类云数据中心，运营商、大企业等数据中心、大中型企业核心安全、出口安全、教育三通两平台，铁路局及公检法职能机构广域网核心 + 分支出口安全、商贸连锁等

中国农业银行总行、重庆城商银行、交通银行、中国邮政、东北证券、人民网、公安部、贵州高法、国美电器、宝钢集团、中国石化、中国南方航空、新兴际华集团、浙江移动、陕西移动、广告移动、安徽移动、四川移动、华数传媒

H3C SecPath T1000/T5000/T9000系列 入侵防御系统

作为业界领先的IPS产品，H3C SecPath T系列产品部署在客户网络的关键路径上，通过对流经该关键路径上的网络数据流进行2到7层的深度分析，能精确、实时地识别并阻断或限制黑客、蠕虫、病毒、木马、DoS/DDoS、扫描、间谍软件、协议异常、网络钓鱼、P2P、IM、网游等网络攻击或网络滥用。同时，H3C SecPath T系列产品还具有强大、实用的带宽管理和URL过滤功能。并能实现基于用户、应用、时间、安全状态等多维度的策略控制功能。

在虚拟化和可靠性方面，支持多设备集群及1:N虚拟化。更好地适应云计算的要求的弹性扩展能力。

■ H3C SecPath T9014

■ H3C SecPath T5080

■ H3C SecPath T1000-AI-90

■ H3C SecPath T9000-E8

产品特性

高性能

■ 全系列采用 64 位多核高性能处理器，高端采用机框式设备，单业务卡最高 40G 处理能力。

高可靠

■ 机框式设备采用控制、业务分离的分布式架构，主控1+1冗余,电源模块M+N备份,所有单元均支持热插拔。

典型应用场景和用户

各种网络的 4~7 层应用安全防护

工商银行、中国银行、农业银行、交通银行、中国电信、中国邮政、中国移动、中国联通

财政部、科技部、国家专利局、国家海洋局、中国科学院、中国铁路总公司

H3C SecPath ACG1000/AK系列 应用控制网关

H3C SecPath ACG1000是以全网行为管理为理念的安全业务网关产品，支持对网络社区言论、P2P带宽滥用、IM文件泄密、网络游戏/炒股等行为进行精细化识别和控制。产品支持联动终端行为管理系统和BA行为感知系统，配合智能应用识别、机器学习算法、TB级数据分析技术，实现全网用户行为画像、业务访问风险画像、多场景感知画像的分析。基于云、网、端的产品能力，ACG1000产品可以提供业界最全面、最完善的全网行为管理方案。

型号：

■ ACG1000-BE　■ ACG1000-SE　■ ACG1000-ME　■ ACG1000-AE

■ ACG1000-XE1　■ ACG1000-AK230　■ ACG1000-AK250　■ ACG1000-AK280

产品特性

融合丰富特性

■ 支持上网行为管理、实名认证、网络审计、智能流控、防私接、智能应用选路、应用缓存等多种安全功能。

全网行为管控

■ 支持对接入网络人员进行实名认证，对终端类型及进程做访问权限控制，可记录内网访问行为、互联网访问行为，实现全局可视和管控闭环。

智能行为感知

■ 在全网行为检测的数据基础上，充分利用机器学习算法实现对人员网络访问行为的智能分析，支持全网行为感知分析、校园贷/裸贷感知分析、员工离职倾向感知分析、员工涉黄 / 涉毒 / 涉赌等多种行为分析引擎，帮助用户实现风险预知和网络行为可视化呈现。

典型应用场景和用户

商贸/酒店连锁、金融网点、企业总分互联、互联网+教育出口、IPV6改造、无线非经

银泰广场、万达广场、万达集团、新华联集团、华润万家、中央电视台、中国南方航空、湖南大学、天津教育城域网、浙江农信、渤海银行

H3C SecPath EAA 加密应用分析系统

H3C SecPath EAA 加密应用分析系统拥有强大的加密流量应用识别能力，本产品部署在流量汇聚出口，结合深度学习、AI关联、自动建模、恶意证书库、全球资产指纹库等完成的多项加密流量识别技术，能对加密VPN（含隧道、翻墙）和国内外加密应用（含协议）精准识别，并对行为进行审计。在国家、产业、学术界多个层面，均可以为网络管理和网络空间安全管控提供有效技术支撑。

H3C SecCenter X6000系列 安管一体机

H3C SecCenter X6000系列安管一体机产品是由新华三技术有限公司在多年的安全研究沉淀、等保建设服务实践经验和对等级保护2.0标准的权威理解的基础上，自主研发的一款用于等保2.0建设或者信息系统安全管理区 域建设的综合性的安全管理平台，具有漏洞扫描、日志审计、运维审计、数据库审计、终端杀毒等功能模块，全面满足网络安全等级保护2.0中安全管理中心的系统管理、审计管理、安全管理、集中管控的要求。

■ H3C SecCenter X6010

■ H3C SecCenter X6020

产品特性

突出“一体化”，丰富应用功能，简化部署，便于快速上线。

集、简配置

业务信息集中展示，应用策略集中管理，提供常用配置模板，提升部署速度和易用性，实现快速上线。

一体管理

“一个”设备，通过重构统一管理平台，统一 UI，统一运维，多种应用模块化设计，实现真正的“一体机”。

合规可视

围绕等保 2.0，提供差异化产品，实现等保、关保全面合规；对各组件日志进行关联分析，并进行大屏分析展示。

典型应用场景和用户

党政行业：政府、法院、 检察院等

教育行业：高教、普教、 教育局等

财税民生：国土局、社保局 公积金中心、测绘院等

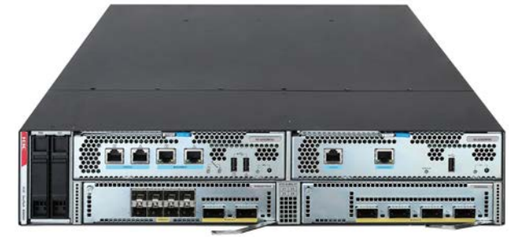
医疗健康：医院、妇幼保健院、 卫健委等

企业：国企、上市企业、制造企业等

H3C SecPath L1000/L5000/M9000-AD系列 应用交付产品

新华三应用交付产品支持完备的链路负载均衡、服务器负载均衡和全局负载均衡功能，支持丰富的健康检测方式和高效的调度算法，可以帮助政府、运营商、金融、企业等用户提升出口多链路、服务器集群和数据中心级的资源利用率，保障业务连续性。

新华三应用交付产品已经适配主流的网络解决方案和安全解决方案，如云数据中心网络解决方案、IPv6网站改造解决方案、SSL加解密解决场景、智能DNS解决方案、双活数据中心解决方案等，可以满足各类业务场景中对于链路优化、应用优化和应用安全的需求。



■ M9000-AD系列

■ L5000系列

■ L1000系列

产品特性

丰富灵活的应用交付特性

- TCP 连接复用 /TCP 双边加速 /TCP 协议栈优化
- SSL 硬件加解密，支持 SSL 卸载和 SSL 代理
- HTTP 压缩 / WebCache/ 数据库读写分离等

业界最全的安全防护特性

- 支持全量 IPS、AV、WAF 防护功能
- 支持泛洪攻击防范、单包攻击防范
- 支持地址扫描、端口扫描等攻击防范

IPv4 无缝迁移至 IPv6

- 完备的 IPv6 协议栈，支持通过 IPv6 地址对设备进行管理
- 链路负载、智能 DNS、DNS 透明代理、服务器负载、应用优化、应用安全等业务 100% 兼容 IPv6 环境
- 支持 IPv6 的 X-forward-for /TCP Option 字段插入，满足溯源要求
- 支持 IPv6 天窗改造

云网安一体化

- 支持东西向安全服务链的引流和纳管
- 支持通过紧耦合和松耦合两种模式对南北向安全服务链的引流和纳管
- 支持基于 VRF/Context/vSystem 等多种虚拟化技术满足不同场景的虚拟化需求
- 支持通过 SDN 安全控制器对业务进行灵活编排

完备的基础网络能力

依靠公司网络技术的积累和 Comware 统一平台的能力，新华三应用交付产品具备完备的基础网络能力

- 支持 ARP、VLAN、MSTP 等二层网络协议
- 支持 TCP/IP 协议、IPv4 及 IPv6 静动态路由协议
- 支持 ALG、IPv6 隧道、VxLAN 隧道等技术

典型应用场景和用户

链路负载均衡场景、服务器负载均衡场景、全局负载均衡场景、IPv6/SSL网站改造场景

中国人民银行、国家税务总局、北京环球国际影城、北京邮电大学、云南省医保云、三大运营商、国家人口库、中国质检总局、人民网、中国民航信息集团、国家电网、中石化、华润集团、新兴际华集团等

H3C SecPath VMSG系列 虚拟安全产品

H3C VMSG (Virtual Multi-service Security Gateway) 虚拟安全产品，包括vFW和vLB。VMSG产品支持多种虚拟平台，基于专业的H3C Comware V7平台，监控和保护虚拟环境的安全，为虚拟化数据中心和云计算网络带来全面的安全防护。

在安全功能方面，vFW为用户提供了全面的安全防范体系和远程安全接入能力，支持攻击检测和防御、安全域策略，采用ASPF (Application Specific Packet Filter) 应用状态检测技术，提供多种智能分析和管理手段；vLB开创性地实现了负载分担、安全与网络的深度融合，具有强大的网络、负载均衡、2~7层安全防护等功能；用户还可以根据自己的需要灵活扩展业务接口和性能，以适应各种复杂的组网环境。

产品特性

部署场景突破业务能力突破

- 得益于虚拟化的天然优势，解决了物理设备在云计算多租户网络中的部署难题，实现企业在公有云中部署网络设备的求，有效拓展网络设备的部署场景。

设备性能突破

- 通过为虚拟设备增加虚拟资源的方式来提升设备性能，不受物理设备的硬件限制，使得按需扩容成为现实。

业务能力突破

- 发挥虚拟设备的计算能力，配合物理设备组网，卸载物理设备的控制平面业务（如：路由计算、密钥管理等），虚实结合、优势互补，有效提升整网规模和性能。

典型应用场景和用户

数据中心、公有云、私有云、混合云

湖北地税数据中心安全项目、腾讯公有云VPC网关项目、北京电视台数据中心安全项目、中国电信集团、国家电网公司、北京邮电大学、黑龙江大学、中南财经政法大学、河南师范大学、四川省政务云、内蒙古地税、黑龙江省人社厅

H3C SecPath AFC2000系列 异常流量清洗

H3C SecPath AFC2000异常流量清洗系统基于嵌入式系统设计，基于自主研发的高效防护算法，创造性的将算法实现在协议栈最底层，使整个运算代价大大降低。同时，产品采用全新一代多核处理器硬件平台，整机采用主动探测防护。用于抵抗各类拒绝服务网络攻击，例如：SYN-flood、UDP-flood、DNS-flood、CC攻击等类型攻击，广泛应用于IDC机房，政府、事业单位，大型企业，为客户解决拒绝服务类的攻击防护问题，保证重要网络环境的安全和完整性。

型号：

- M9000 AFC 模块
- AFC2020-G2
- AFC2040-G2
- AFC2100-G2
- AFC2200-G2
- AFC2400-G2
- AFC2100-D-G2

H3C SecPath GAP2000系列安全隔离与信息交换系统

H3C SecPath GAP2000安全隔离与信息交换系统是H3C利用自身的技术优势和在安全体系结构方面的研究成果，经过长期研发，推出的一种全新的、高效的、安全的网间隔离产品。

在安全功能方面，H3C SecPath GAP2000可在确保用户内外网TCP/IP协议彻底阻断的情况下，提供HTTP、SMTP、POP3、FTP、ORACLE、FileSync、视频等应用级检测通道。在屏蔽会话层以下网络威胁的前提下，对内外网交互数据进行严格的访问控制和日志审计。

型号：

- GAP2000-AE
- GAP2000-BE
- GAP2000-SE

H3C SecPath W2000系列 Web应用防火墙

Web应用防火墙(Web Application Firewall，简称：WAF)代表了一类新兴的信息安全技术，用以解决诸如防火墙一类传统设备束手无策的Web应用安全问题。与传统防火墙不同，WAF工作在应用层，因此对Web应用防护具有先天的技术优势。WAF会对所有Web流量（包括客户端请求流量和服务器返回的数据流量）进行深度内容检测和验证，确保其安全性与合法性，对非法的请求予以实时阻断，从而对各类网站进行有效防护。

型号：

- W2000-AK415
- W2000-AK445
- W2040-G2
- W2000-AK425
- W2010-G2
- W2080-G2
- W2000-AK435
- W2020-G2
- W2200-G2

H3C SecCenter IAM统一身份管理与安全认证系统

H3C SecCenter IAM统一身份管理与安全认证系统，实现应用帐号的统一管理、统一认证、单点登录和权限管理，以企业用户、B/S 系统为整合目标，实现统一认证、统一授权和访问控制。集成强身份认证、会话审计、集中管理功能的一体化。可对企业内部用户应用访问、管理员维护等各类操作进行访问控制。统一的身份管理系统，统一的用户权限管理，统一的安全策略，使得身份认证的过程更加标准化，安全性方面更加靠。集中式的身份和权限管理，使得用户身份维护更加同步，减少用户认证系统的维护成本。

H3C SecPath A2000系列 运维审计系统

H3C SecPath运维审计系统为用户提供了全面的运维管理体系和运维能力，支持资产管理、用户管理、双因子认证、命令阻断、访问控制、自动改密、审计等功能，能够有效的保障运维过程的安全。在协议方面，运维审计系统全面支持SSH/TELNET/RDP（远程桌面）/SFTP/VNC，并可通过应用中心技术扩展支持VMware/XEN等虚拟机管理、Oracle等数据库管理、HTTP/HTTPS管理等。

型号：

- AK602
- AK615
- AK625
- AK630
- A2025-G
- A2100-G
- A2105-G
- A2200-G
- A2210-G

H3C SecPath D2000系列 数据库审计产品

数据库审计技术能够实时记录网络上的数据库活动，对数据库操作进行细粒度审计的合规性管理，对数据库遭受到的风险行为进行告警，对攻击行为进行阻断。它通过对用户访问数据库行为的记录、分析和汇报，用来帮助用户事后生成合规报告、事故追根溯源，同时加强内外部数据库网络行为记录，提高数据资产安全。

型号：

- D2010-G
- D2020-G
- D2030-G
- D2050-G

H3C SecPath SysScan系列 漏洞扫描系统

H3C SecPath SysScan漏洞扫描产品是一款综合漏洞扫描产品，可对主流操作系统、WEB站点/应用、数据库系统、网络设备、各种常见应用等目标进行深入扫描，发现可被黑客利用的安全漏洞、脆弱性和弱口令等安全问题，并提供详尽、专业的安全建议和修补方案，能够有效降低安全管理人员的工作难度和工作量。

型号：

- SysScan-AE
- SysScan-ME
- SysScan-SE
- SysScan-Cloud
- SysScan-AK810

H3C SecCenter综合日志审计平台

综合日志审计平台具备高性能日志采集能力，提供了强大的分析功能，能够对大量分散设备的异构日志进行统一管理、集中存储、统计分析、快速查询，透过事件的表象真实地还原事件背后的信息，能对全网范围内的网络安全事件进行集中的统计分析。为用户提供真正可信赖的事件追责依据的同时，满足等级保护和网络安全法要求。

- H3C SecCenter CSAP-SA

型号：

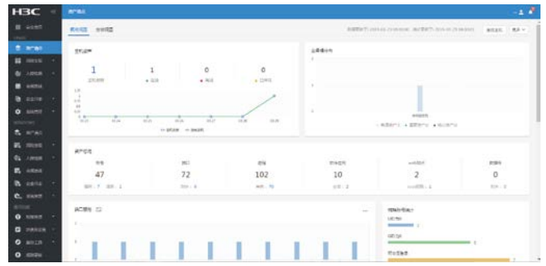
- H3C SecCenter CSAP-SA
- H3C SecCenter CSAP-SA-V
- H3C SecCenter CSAP-SA-AK640
- H3C SecCenter CSAP-SA-AK645

H3C SecCenter安全业务管理平台

安全业务管理平台能够对我司防火墙、入侵防御安全设备、视频安全网关进行统一管理，为部署于各关键位置的安全设备提供集中的安全策略管理与控制，并能直观的为实时事件监控和综合分析攻击等各种安全事件提供丰富的统计报告，方便用户随时了解网络安全状况。提供实时监控、综合分析、策略下发以及威胁日志审计等功能。

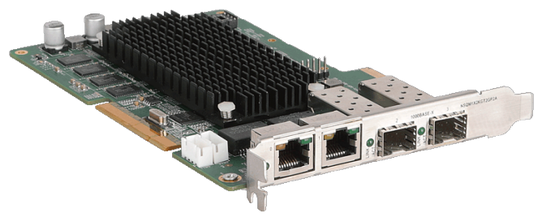
H3C SecPath服务器安全监测系统

H3C服务器安全监测系统由Agent，Server，Web三部分构成，是一款专注于服务端主机的安全防护，提供持续的安全监控、分析和快速响应能力，能够在公有云、私有云、混合云、物理机、虚拟机等各种业务环境下实现安全的统一策略管理和快速的入侵响应能力。



H3C SecPath F1000-ServerBlade服务器安全智能模块

服务器安全智能模块是集成AV、FW、IPS、WAF4个主要功能模块的一款服务器标准尺寸的安全插卡，可对单台物理服务器提供更精细化的安全策略，为服务器安全提供更完善的保护。



型号：

- H3C SecPath F1000-ServerBlade-S
- H3C SecPath F1000-ServerBlade-A

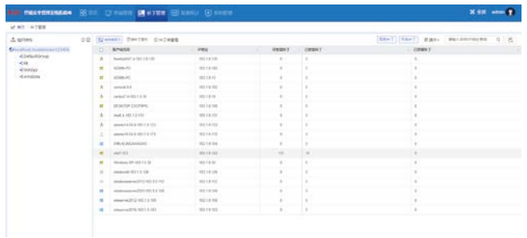
H3C SecPath AVG2000防病毒网关

H3C SecPath AVG2000系列防病毒网关产品是针对近年来恶意代码威胁快速演变而设计的一款革新的网关级过滤设备，可全面高效防范恶意代码威胁的传播、动态式攻击、异常通讯，可全面的、综合的覆盖恶意代码威胁的各个阶段，使其无处循形，适用于等级保护、企业内控等信息安全规范，全面保障数据库的完整性、保密性和可用性。

型号： ■ AVG2000-B ■ AVG2000-S ■ AVG2000-A

H3C SecCenter终端安全管理系统

H3C终端安全管理系统产品集恶意代码防护、桌面管理、终端威胁检测与响应（EDR）于一体的全新一代终端安全管理系统，彻底解决终端安全威胁全生命周期的管理，包括事前预警防范、事中应急处置、事后追责溯源，完成终端安全威胁闭环。



型号： ■ ESM ■ ESM-AV

H3C SecPath G9000系列 多级安全互联交换平台

H3C SecPath G9000 多级安全互联交换平台，是新华三技术有限公司利用自身的技术优势和在安全体系结构方面的 研究成果，经过长期研发，推出的一种全新的、高效的、安全的网间隔离产品。

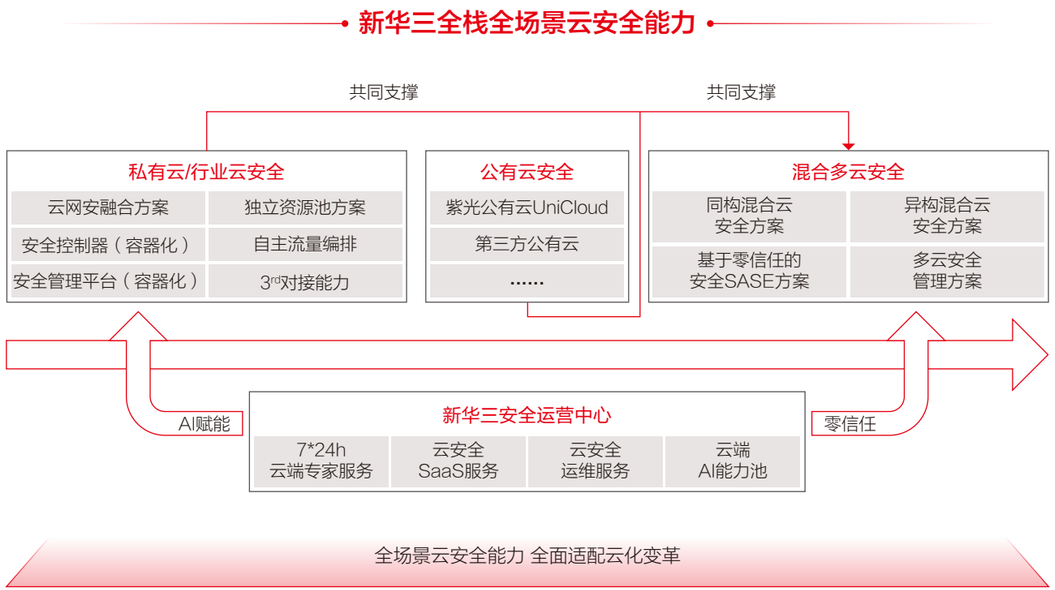
在安全功能方面，H3C SecPath G9000 可在确保用户内外网 TCP/IP 协议彻底阻断的情况下，提供 HTTP、SMTP、POP3、FTP、ORACLE、GB/28181-SIP 等应用级检测通道。在屏蔽会话层以下网络威胁的前提下，对内外网交互数据进行严格的访问控制和日志审计。

型号：

- G9010
- G9020

新华三网络安全解决方案

新华三全栈全场景云安全能力助力云化变革



私有/行业云安全：云安协同 网安智联。

面向私有云、专有云和行业云的解决方案，新华三采用1+2+N的模式：1+2就是一个统一的平台，两种部署模式，配合着N类安全服务资源，从而达到一种安全一体化的效果。一个统一的安全管理平台可以通过紧偶合的方式跟第三方云平台或者新华三的云平台紧密衔接，衔接分为三层：从界面上进行统一，引流调度上实现统一，再从安全资源和计算资源实现一个统一，这就是云、网、安的统一融合能力。针对第三方，新华三在逐步推进跟运营商的云平台去做对接，把新华三全套的安全服务能力提供给合作伙伴，一同来运营这个统一的云平台。这一切离不开安全的自动化部署能力，安全自动化部署依靠新华三安全控制器来实现。

公有云安全：构造公有云原生安全体系。

公有云方面，新华三成功借助紫光集团的紫光云平台，实现进军公有云领域的一个重大突破。紫光公云上的整体安全服务的架构、技术路线以及服务目录的提供都是由新华三统一生成，我们也在逐步探索配合着其他第三方公有云去实现整体安全服务的交付。

混合多云安全：同构/异构多云安全一体化服务。

同构场景方面，新华三整体发布云安全战略2.0，把紫光公有云平台和紫鸾私有化平台打成一体，实现远端的公有云和近端的私有云在整体底层架构的统一，通过统一的云平台实现对于身份识别、内容识别、数据加密的一些需求，以及过等保等各类安全服务，实现统一的一体化服务。针对于异构场景，新华三正在逐步以第一责任人的身份吸纳更多的合作厂商，把各家擅长的能力交给各家去实现，新华三统一输出一体化引流调度或一体化服务交付。

云安全运营中心：云化安全一站式服务中心。

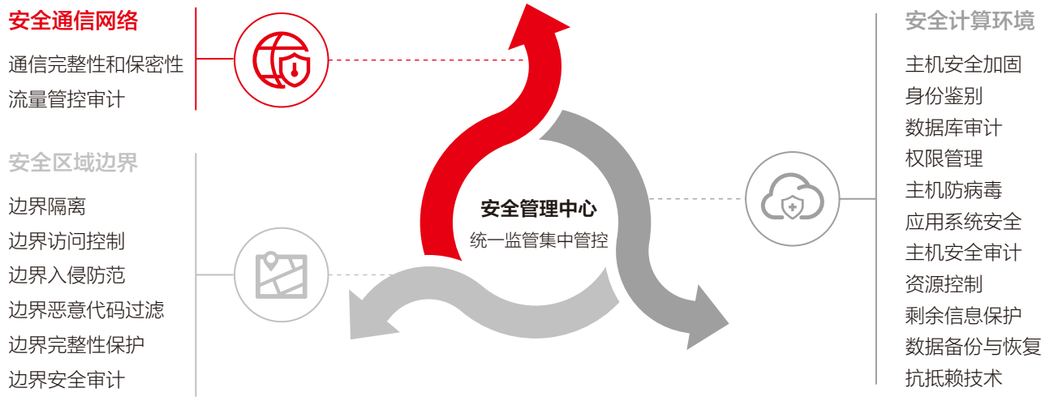
目前新华三云上安全运营中心实现两个云化：1）安全产品的云化；2）安全服务的云化。在这种大环境下，新华三实现融合统一赋能的能力，比如云SaaS化服务，实现云的安全能力随时随地取用。整体云安全运营中心作为一个能力的云端补充，为新华三私有云的解决方案、混合云的解决方案注入了有利的新鲜血液。

云安全零信任接入：全面身份管控，无界安全访问。

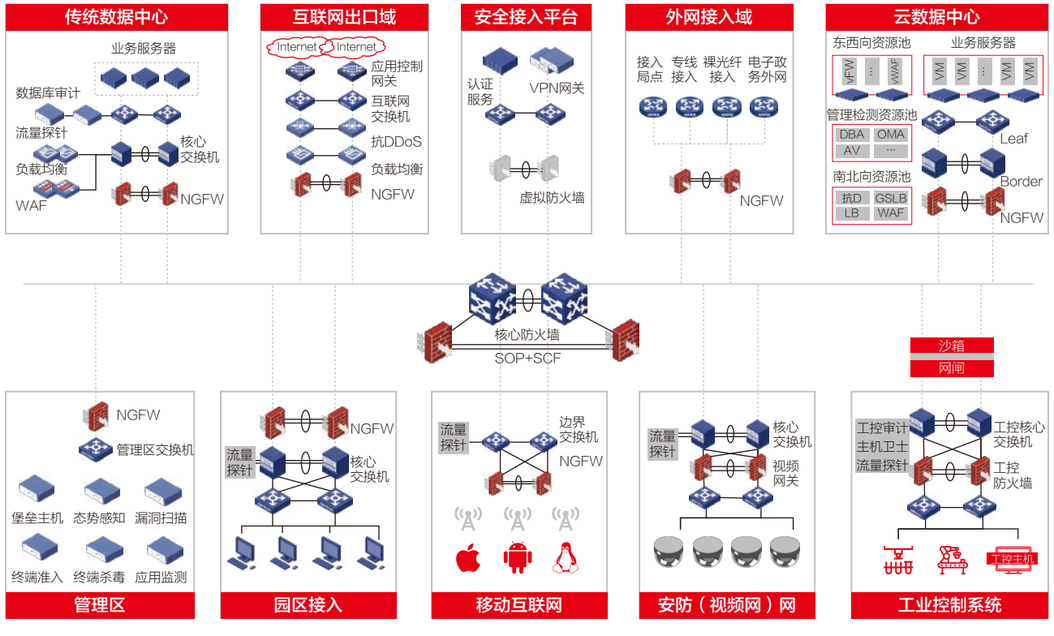
零信任近年来成为国内外非常火热的词语，新华三把零信任作为一种统一身份的管理，统一持续的云原生的能力注入到刚才提到的所有的解决方案当中。不论是通过旁挂或者部署，都是在将身份永不信任以及持续验证的过程去部署到整个云环境当中，真正实现无界安全访问。

新华三网络安全等级保护解决方案

等级保护设计思路 —— 一个中心三重防护



等级保护技术规划指导



安全通信网络层面

双链路设备冗余	网络架构	应提供通信线路，关键网络设备和关键计算设备的**硬件冗余**，保证系统的可用性。
HTTPS，VPN	通信传输	应采用密码技术保证通信过程种**数据的保密性**。
可信计算	可信验证	在应用程序的关键执行环节进行**动态可信验证**。

安全区域边界层面

AC，NGFW	边界防护	应限制无线网络的使用，保证无线网络通过受控的边界设备接入内部网络。
NGFW，DLP	访问控制	应对进出网络的数据流实现**基于应用协议和应用内容的访问控制**。
沙箱 反垃圾邮件系统	入侵防范	应在关键网络节点处**对垃圾邮件进行检测和防护**，并维护垃圾邮件防护机制的升级和更新。
ACG，流量探针	安全审计	应能对远程访问的用户行为，访问互联网的用户行为等**单独进行行为审计和数据分析**。
可信计算	可信验证	在应用程序的关键执行环节进行**动态可信验证**。

安全计算环境层面

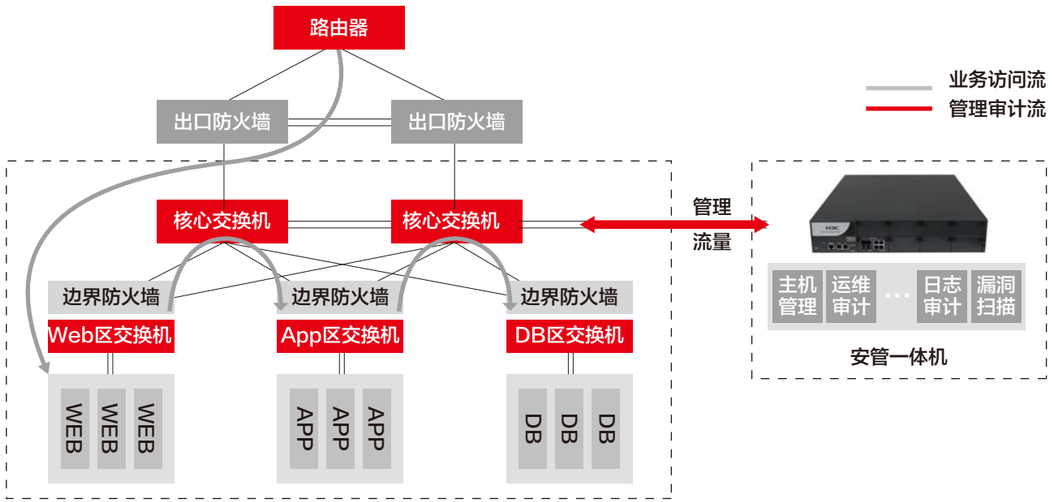
堡垒机	身份鉴别	应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。
主机加固	访问控制	访问控制的粒度应达到主体为**用户级或进程级，客体为文件、数据库表级**。
终端防病毒，沙箱	恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为，并将其有效阻断。
VPN，加密机	数据保密性	应采用密码技术保证重要数据在传输/存储过程中的保密性，包括但不限于鉴别数据、重要业务数据和重要个人信息等。
数据实时备份 业务高可用架构	数据备份恢复	应提供异地实时备份功能，利用通信网络将重要数据实时备份至备份场地。

安全管理中心层面

安全设备纳管	安全管理	应通过**安全管理员对系统中的安全策略进行配置**。
安全管理区建设 FW	集中管控	划分**单独的安全管理区域，并建立安全的信息传输路径**。
SOC 日志审计系统	集中管控	应对网络链路、安全设备、网络设备和服务器等的运行 状况进行**集中监测**； 审计记录留存时间符合法律要求。
主机加固 态势感知系统	集中管控	应对**安全策略、恶意代码、补丁升级**等安全相关事项进行**集中管理**；并对各类安全事件进行**识别、报警和分析**。

新华三“等保+”解决方案

“等保+”解决方案架构

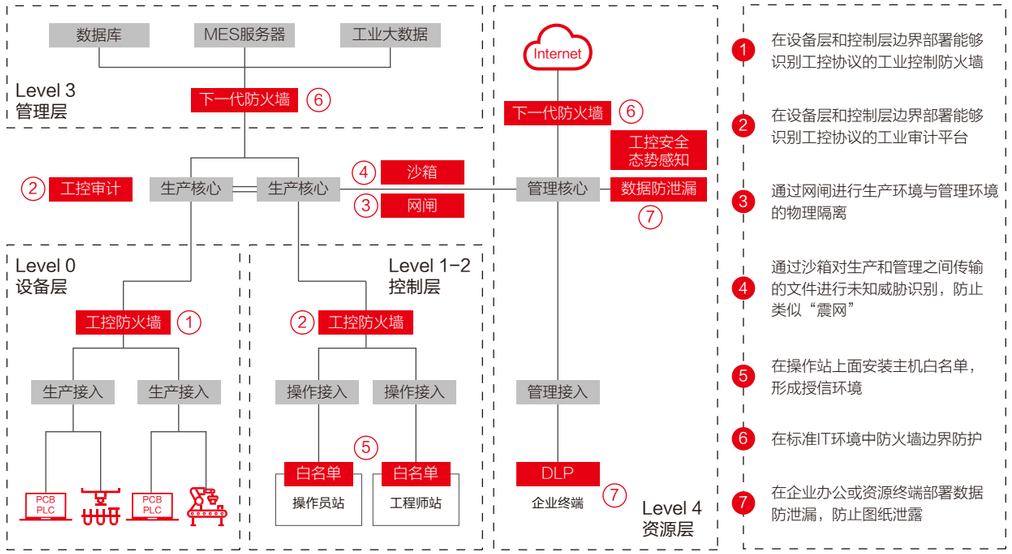


工控安全与网络安全侧重点不同

- 在不利条件下维护生产系统功能正常可用
- 确保信息实时下发传递
- 防范外部、内部的网络攻击
- 保护工控系统免受病毒等恶意代码的侵袭
- 避免工控系统遭受有意无意的违规操作
- 安全事件发生后能迅速定位找出问题根源

- 在不利条件下保证不出现信息泄露
- 保护信息资产的完整性
- 信息传递实时性要求不高
- 防范外部、内部的网络攻击
- 保护信息系统免受病毒等恶意代码的侵袭
- 安全事件发生后能迅速定位找出问题根源

工业控制系统等保解决方案

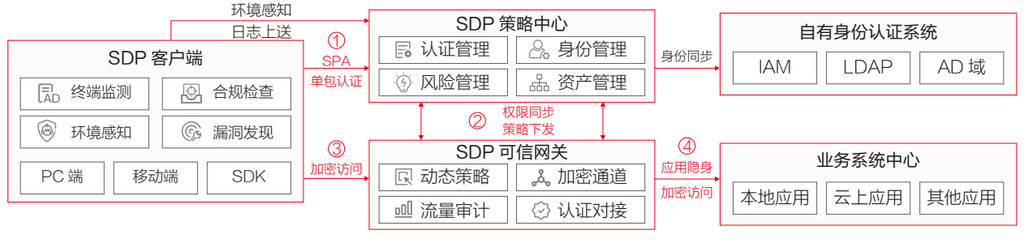


新华三等保2.0全景架构

新华三零信任解决方案

当今愈发复杂的网络架构、多样化的业务系统、交叉流动的业务数据的安全现状，使得业务系统和数据的边界逐渐模糊，非黑即白的一次性授权方式、粗放的权限粒度控制、非自动的威胁响应能力、内部数据不可控的泄露。传统安全机制失效背后的根本原因是信任，随着内网基础设施愈发复杂和流经网络流量的种类增加，同时随着云大物移技术的发展和混合云的大规模部署落地，企业用户无法确立明确的网络边界。

新华三零信任解决方案主体从 SDP（软件定义边界）的技术方向进行研究和演进，主体由 SDP 客户端、SDP 可信网关、SDP 策略中心组成。结合对零信任的研究及实践，通过对用户的统一安全接入及动态权限管理，实现了身份、终端、应用系统的安全可信。



基于 SDP 架构的零信任解决方案架构图

新华三零信任解决方案具备如下五大核心能力：

动态权限管控

通过用户风险、终端风险、UEBA 等信息，同时利用动态防火墙技术快速建立安全防御策略、准入策略，从而动态地调整安全访问策略。

应用服务隐藏

SDP 网关默认关闭所有端口，攻击方端口嗅探和漏洞扫描等信息探测搜集手段不会得到任何响应，可防止 SDP 网关被扫描及渗透，杜绝后端的应用资源被暴露。

细粒度访问控制

可支持基于应用、功能、身份、接口等，最小化原则进行访问控制授权，即使获取了某台服务器的权限，也无法对其他服务器进行横向渗透。

一体化可信网关

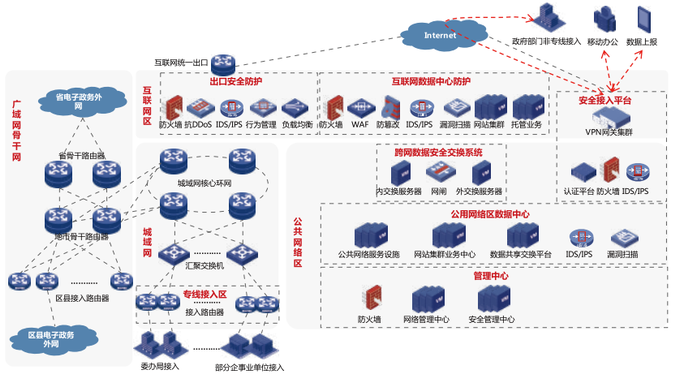
全系列电信级可信网关设备，提供稳定性和高可用性能力，具备深度安全检测及应用安全检测能力，同时支持应用交付算法，最精准的满足负载分担能力。

威胁协同处置

深度融合全网的身份管理、资产管理、权限管理、威胁管理数据，根据用户的威胁情况，自动化编排协同，形成闭环处置。

新华三零信任安全解决方案基于持续性分析检测、动态授权、最小化原则零信任安全的核心思想，利用自身在云、网络、安全、大数据、AI 方面的技术积累，贯彻“永不信任，始终验证”的原则，通过对身份进行统一管理，实现了设备、用户、应用等实体的全面身份化，建立企业全新的身份边界。

电子政务外网安全解决方案



国家电子政务外网（简称政务外网）是按照中办发〔2002〕17 号文件和〔2006〕18 号文件要求建设的我国电子政务重要公共基础设施，是服务于各级党委、人大、政府、政协、法院和检察院等政务部门，满足其经济调节、市场监管、社会管理和公共服务等方面需要的政务公用网络。政务外网支持跨地区、跨部门的业务应用、信息共享和业务协同，以及不需在政务内网上运行的业务。政务外网由中央政务外网和地方政务外网组成，与互联网逻辑隔离。

截至2013年末，政务外网骨干网已经覆盖100%的省（区、市）和新疆生产建设兵团，93.7% 的地（市），80.6% 的县以及 33.2% 的乡镇；横向连接了 85 个中央政务部门和相关单位，全国范围接入的政务部门及相关单位约 9.8 万多个，接入终端已达 147 万多台。庞大的电子政务外网必然需要与更符合电子政务业务的安全建设。

新华三电子政务外网安全防护解决方案，为国家电子政务外网提供可靠的技术架构，其包括以下几部分：

广域网骨干网

通过 MPLSVPN 对不同的业务或信息系统进行隔离，同时在骨干网的关键节点部署 H3C 防火墙安全插卡，实现防火墙的灵活扩展，同时各级广域网部署 H3C 安全态势感知系统，实现对广域网的统一安全运维和安全事件分析。

互联网接入区

提供 L2-L7 层完善的互联网出口链路安全防护，对互联网的流量进行强访问控制与清洗，同时记录审计每一条走向互联网的流量；新华三完善的安全产品解决方案为互联网数据中心提供全方位的安全防护，同时为互联网区与其它区域的安全接入提供网闸解决方案，实现跨区访问的强隔离。

公用网络区

对于移动办公用户及政府部门非专线接入的用户，提供 VPN 安全接入解决方案，保障数据不被篡改，同时在公用网络提供数据中心级完善的安全防护方案，保障落地数据的安全。在公用网络的管理中心部署 H3C 安全态势感知系统，实现全网的安全事件分析和流量行为分析。

专线接入区

各委办局用户单位安全对接区域位于用户单位局域网与省直电子政务外网城域网之间，由一台边界安全网关组成，主要实现路由、NAT 转换、安全隔离、入侵防御（可选）、防病毒（可选）和接入认证功能。用户单位安全对接区边界网关通过虚拟化技术，虚拟出四台虚拟边界设备，分别承载局域网整体对接区、外网专用终端接入区、外网业务 DMZ 区、专网对接区（预留）。同时部署一套身份认证及鉴权系统，实现用户接入认证、身份管理，一套安全业务管理中心，实现边界安全网关统一管理及策略下发，安全事件分析展示及告警，NAT 日志审计及溯源等。

凭借在电子政务外网十三年的项目建设经验积累，新华三对于电子政务网的业务发展及面临的安全威胁有着更深的理解，同时一直积极参与国家相关安全标准的制定，对政策的解读也更加深刻。整体方案的设计严格遵循国家相关标准，能够达到等级保护三级的安全防护要求，保障电子政务外网安全建设的合规性。同时，新华三完善的安全产品解决方案，能够为电子政务外网提供 L2-L7 层的安全防护，实现持续的安全监测，可视化的安全服务，全网的安全态势感知，为电子政务网的安全发展提供坚实的技术支撑。

网站安全解决方案

针对社保查询、考生成绩查询、公积金查询等相关涉及个人信息的查询系统网站时，这些资料都属于特殊资料，而且带有涉密性质的资料，需要社会大众通过相关门户网站提供个人信息进行定向查询。另外各类互联网网站在提供服务时都需用户进行注册，在用户注册信息中包含了手机号码、地址、邮件、银行卡号等信息。这些个人信息在黑色产业链中如同矿场一样成为资源。黑客通过技术手段入侵各类网站系统，窃取个人信息资料，从而谋取经济利益。

从内容篡改造成的影响来看，一类是政府类门户网站造成的首页内容恶意篡改，从而影响政府形象，另一类是篡改关键信息内容，从而谋取相关利益。广西“黑客”曾篡改考生成绩，并从中获利 17 万余元。在教育行业，此类报考志愿篡改等安全事件一直层出不穷。

新华三网站安全整体解决方案以黑客入侵过程为视角，针对黑客入侵的每个关键步骤分别制定了“网站安全状态评估、网站入侵安全防护、网站流量审计分析、网站安全加固修复”四个方位进行一体化的安全防护。

在网站安全状态评估阶段，新华三通过渗透测试服务可以真实模拟用户网站系统的脆弱性，可以在保障网站业务正常和客户授权的前提下，提前预知网站的安全状态，通过专业的渗透测试报告可以清晰了解网站系统中存在哪些可入侵的方式、入侵后扩展的范围，以及核心数据有遭破话的可能，从而以最接近实战的方式进行有效的防护修复。

在网站安全入侵防护阶段，新华三通过设置七道安全防线，拦截黑客恶意攻击，可以有效抵御 DDoS、漏扫探测、病毒、后门上传、木马、漏洞利用攻击、SQL 注入、跨站脚本攻击等网络层和应用层的攻击行为，并且为网站服务器配置独立的网页防篡改软件，贴身防护网站文件目录，禁止非法恶意篡改行为。通过设置合理的安全域，将网站服务器与内网核心数据库物理分开，利用安全隔离与信息交换系统可保障在物理隔离的基础上进行部分必要信息的交换。最后在运维管控防线中，严格的对运维人员的操作进行管控，避免内部人员的恶意操作或误操作。

在网站流量审计分析阶段，新华三通过 WEB 应用防火墙及运维审计系统、数据库审计系统审计网站的日常业务流量和运维流量。通过细粒度的报文解析能力和记录方式将业务用户和运维用户的每一个请求流量、响应流量都能完整的记录下来，从而通过设置合规策略对异常访问和异常行为进行告警提示，可以在黑客入侵过程中起到提示管理员的作用，并且在安全事件发生之后，结合其他审计日志，可以对安全事件进行追踪溯源，找出关键线索。

在网站安全加固修复阶段，新华三通过安全加固服务为用户的网站系统及其他相关设备进行策略优化，对在安全事件发生过程中体现出来的网站系统防护薄弱点进行修补。一方面可以通过添加相应防护能力的安全防护设备，另一方面在网络设备、安全设备、服务器上进行策略的优化，并且清理黑客攻击过程中植入的恶意代码、木马和后门，避免再受攻击。

新华三网站安全整体解决方案是由专业安全服务、安全软件与安全硬件相结合进行防护，从网页文件到网站系统，再到硬件服务器。网站整体解决方案是由内到外，层层进行有效防护。

校园网出口安全解决方案

高校校园网一直以来都是践行互联网发展的技术前沿，教学、科研、办公等工作与生活对于校园网平台的依赖性越来越强，然而高校校园网作为承载整个校园内部学生、老师的信息流通、资源共享的平台，校园网出口作为校园网络平台的“门户”，承载着与互联网的信息交流、内网安全防护的重要作用。

目前互联网化时代校园出口现状：互联网访问集中在运营商、教育网出口，拥堵严重，用户数多、流量较大、应用多、并发连接数高、吞吐量大，这些特点导致传统防火墙出现性能瓶颈。

随着校园网络拓扑的改变和黑客攻击手段的变化，原有校园网络也会存在很多安全隐患及威胁。网络安全建设是一个长期投入的过程，是一个不断完善各种规章制度和加强管理的过程。因此，需要根据校园现在的实际需要和安全级别，来规划校园网络安全措施和方法。

基于校园网出口安全防护需求，H3C M9000 安全多业务网关产品为校园网出口提供以下安全防护：

- 全面支持攻击防范、抗 DDoS、访问控制、安全域划分、黑名单、流量监控、邮件过滤、网页过滤、应用层过滤等功能，能够有效的保证网络的安全。
- 采用 UAAE 应用状态识别引擎，可对连接状态过程和异常命令进行检测。
- 支持基于用户、地址、服务、应用、时间等多维度管理，支持带宽限流、带宽保证、新建连接数、并发连接数等多种形式的带宽管理。
- 支持多种链路负载均衡手段：支持出方向基于内置 ISP 地址库的智能选路、链路质量的智能探测及基于应用的精细化选路、DNS 透明代理，从访问层智能解决出口带宽拥堵问题。入方向访问校园资源时提供基于最优链路质量的 DNS 响应
- 支持业界最丰富的 NAT 特性，满足各大运营商的 NAT 需求。
- 支持多种 VPN 业务，如 L2TP VPN、GRE VPN、IPSec VPN、SSL VPN、MPLS VPN 等，满足多种高性能 VPN 接入的需求。
- 提供丰富的路由能力，支持静态路由、RIP/OSPF/ BGP/ISIS 路由策略及策略路由；全面支持 IPv4/IPv6 双协议栈。

该方案具备以下优势：

- 100G 平台安全防护能力，提供千万级 NAT 能力及日志溯源，满足互联网安全防护及安全审计需求
- 丰富的负载均衡手段，及时更新的内置 ISP 地址表、一键式多出口选路、DNS 透明代理综合方案完美实现出口负载的需求
- 单模块集成多业务处理，统一解决了 IPS、应用审计、带宽管理的综合性安全需求，简化管理及日志收集
- 采用分布式架构设计，具有超强的业务、接口扩展能力，匹配不断增长的带宽需求能力要求
- 支持容器级、设备级的虚拟化技术，可以实现安全设备的集群和虚拟化，简化管理，应用灵活

智能VPN解决方案

如何让日常的外出员工（如市场人员、运营人员、外地办事分支等）通过 Internet 安全的接入公司的内网，访问 CRM、ERP、OA 等重要的内部业务办公系统，而且保证网络的安全、稳定、高速，是企业经常面临的问题。

国内几大运营商之间的网络带宽存在瓶颈，给 VPN 的发展带来了挑战。在部署大规模 VPN 网络时，分布在不同运营商网络的用户在使用 VPN 时，存在延时大、带宽小的问题。需要一种通过多线路智能选择技术，当分布在不同运营商网络的 VPN 客户端访问总部时，会自动选择速度最快的线路连接到总部网络，避免了跨运营商的网络互访存在的延迟过高问题。

对于一些安全级别有要求的公司（如金融系统企业）或者全球布局的公司，要求外地员工和分支机构通过多种链路方式接入总部，而且需要高效的身份认证与流量可视化能力。

通过 H3C 智能 VPN 解决方案，可实现：员工在家或者出差办公时，连接公司内网（Intranet），为避免上网速度太慢，不是所有流量都通过公司网络转发，因此配置外网黑名单，默认所有请求都由外网（Internet）转发，黑名单的 IP 和域名由 VPN 转发，这样分流互不影响。

具体实现方式如下:

- 针对总部和分支机构的网络出口，部署高性能 H3C VPN 设备，针对使用人数、分支数目以及客户需求，对 VPN 设备进行选型。
- 设备在开启 SCF 虚拟化技术之后，将 VPN 设备虚拟化成一个统一的 VPN 资源池，根据分支和用户的使用需求再进行资源分配。SCF 的部署方式全面突破了机框的限制，在简化管理和部署的基础上同时实现了安全业务和安全性能的弹性扩展，可以实现业务流量经过一组 SCF 系统的自动负载分担和冗余备份。

SCF 组中每台设备都称为成员设备。成员设备按照功能不同，分为两种角色：

1. 主用设备（简称为主设备）：负责管理整个 SCF 系统。
2. 从属设备（简称为从设备）：作为主设备的备份设备运行。当主设备故障时，系统会自动在从设备中选举一个接替原主设备工作。

- 每个分支的业务专网，设置 2 条及以上 VPN 隧道，实现 VPN 双链路互联，保证链路的通畅稳定。

方案价值

提供多线路最优选路 VPN 功能。通过“智能自动选择”功能。如果总部是多线路，各分支节点在与总部构建 VPN 隧道时，总部设备能分析判断客户机的外网访问请求，客户端也会选择最优化的线路，使用户无论在哪里浏览网站或接入公司内网，都能获得最快速度。

提升中心节点的出口带宽和网络稳定性。如果某一条 VPN 线路中断，基于策略的 VPN 协议将客户端切换到无故障线路上，几乎没有任何延迟，可以最大程度地减少费用和故障切换时间。既保证了数据安全无间断的传输，又有效地实现了数据在各条线路上的分流，同时保证大量客户端都能正常访问总部应用服务器。

可按需要对 VPN 及上网流量进行比率或定量调控，保证多线路接入带宽不一致的时候，按照带宽比例将流量合理分配到多线路上。

新华三专业安全服务

新华三安全服务团队具有网络安全、云安全、移动安全、大数据安全、工控安全、可信计算及物联安全在内的服务能力，依据国家政策及行业标准结合云安全、安全设备、主机、网络、存储、数据库等专业技术为客户提供顾问式、管家式的一体化安全服务，凭借丰富的安全咨询和技术实践经验，帮助客户规划安全架构、评估风险态势、加固防护，建设安全开发和运维应急体系，满足合规要求，有效保障客户关键系统安全高可用性。

用户名单：云上北疆等保2.0、云安全保障体系咨询服务、太平洋保险安全体系建设服务、合肥市数据资源局网络安全攻防大赛、英大传媒高级安全协维服务、华润电力网络安全保障服务、辽港集团安全咨询规划服务

新华三安全服务工作汇报-能力集

风险评估

安全评估类
- 安全风险评估
- 新系统上线评估
- 等保差距评估
- 电子银行评估
- 安全管理评估

安全检测类
- APP安全检测
- 漏洞监测
- 基线核查
- 渗透测试
- 代码审计
- 安全众测
- 利剑-全流量威胁分析工具
- 利保-重保服务工具
- 利视-安全视频漏扫服务工具

规划设计

规划设计类
- 安全战略规划
- 管理体系设计
- 等保体系设计
- 云安全架构设计
- IAM统一身份管理

合规咨询类
- 等保合规咨询
- 开发生命周期咨询
- ISO27001合规咨询
- 云安全合规咨询
- SOX合规咨询
- 业务连续性咨询
- 信息安全治理咨询
- 利规-等保全流程服务工具

工程实施

安全加固类
- 系统集成服务
- 安全加固
- 等保整改
- 安全设备策略维护
- 利策-安全策略管理服务工具

运行维护

基础协维类
- 安全预警
- 安全设备维护
- 安全设备日志分析
- 漏洞监测
- 基线核查
- 病毒分析与查杀
- 安全事件应急响应
- 重大时刻安全保障
- 安全加固

高级协维类
- 渗透测试
- 安全监测服务
- 应急预案与演练
- 管理体系建设

平台运维类
- 网站安全防护
- 云WAF服务
- 云DDoS防御
- SAAS化云安全运维服务

教育培训

规划设计类
- 安全产品培训
- 安全技术培训
- 安全管理培训
- 客户定制化培训
- 安全攻防比赛组织
- 安全实训平台服务

新华三重点安全服务方案介绍——传统服务方案全面升级

新重大时刻安全保障服务解决方案

新华三安全服务团队通过引入利剑 – 全流量威胁分析工具箱、利保 – 重保服务工具箱、资产探测、狩猎平台、众测平台等先进的服务工具平台，有效提升重保工作的覆盖面和有效性，同时针对重保工作的特殊性，形成以区域为中心交付团队，从而确保人力资源的充足储备及服务的及时性。

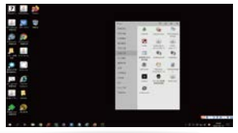
准备阶段	自查整改	预演阶段	正式护网	项目总结
团队组建 人员组织与分工 明确工作职责 细化工作流程 召开工作启动会	**资产梳理** 关键资产梳理 互联网暴露信息评估 老旧资产排查 网络架构分析	**演练团队组建** 架构、角色、职能明确 演练流程明确 演练流程应急机制宣贯 应急处置培训与演练	**告警监控** 态感平台监控 各类安全设备日志分析 主机侧攻击行为验证 对攻击行为制定策略 业务系统检测 网络流量检测	**成果总结** 根据演练结果总结当前安全状况 分析安全问题根源 安全技术 安全管理 风险控制 成果和经验总结 制定改进计划（人、制度、技术） 经验分享培训 贯穿始终的技能培训
方案编制 护网防护工作方案 预演方案 安全专项应急预案	**风险排查** 高危账号、弱口令排查 渗透测试 漏洞基线核查 主机安全检查 应用系统安全检查 运维终端安全检查	**内部演练开展** 内网攻防演练 互联网攻防演练 应急响应、分析溯源	**应急处置** 阻断 IP 调整安全策略 专家研判	
安全培训 护网防护工作方案 预演方案 全员 – 安全意识培训 信息技术人员 – 应急响应培训 安全专业人员 – 实战化防护 专业能力培训 (HWBP)	**防护落地** 运维策略优化 安全设备与工具部署 安全策略调优 漏洞基线修复 安全风险复测	**多工具联合分析** **安全防护：**防火墙、IPS、WAF、HIDS **安全监测：**态势感知、利剑、威胁情报、数据库审计、蜜罐 **演练复盘** 优化安全设备及策略 持续日常测试 处理预演遗漏问题 增补安全加固	**攻击还原** 利用利剑、蜜罐、还原攻击过程 分析脆弱点，实时优化加固 每日、每周工作报告	

重大时刻安全保障服务配套工具平台

利剑
iSec全流量威胁分析工具箱

利保
iSec重保服务工具箱

资产探测工具



众测平台

新安全运维服务解决方案

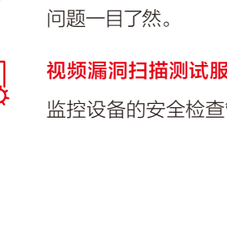
新华三安全服务团队在驻场安全运维的基础上，依托云技术，推出远程安全运维服务，包括远程设备运维、网站监测、云抗 DDoS、云 WAF 等，及时发现用户的网络及业务安全风险，推进安全智能运维的规划。

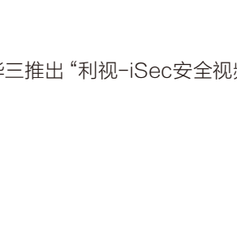
另外，针对云数据中心的业务特色，新华三打造专业化的云中心安全运维服务，从而应对云数据中心平台及租户的安全运维工作需要。

驻场安全运维：驻场方式，及时有效的协助用户开展安全能力建设，安全策略规划，安全设备运维，安全流程优化等工作

\+

远程安全运维：利剑、网站监测、云抗 D、云 WAF，及时发现用户的网络及业务安全风险，推进安全智能运维的规划，依托云技术，提供远程运维服务。





安全合规建设	重大时刻保障
日志分析监控	安全设备维护
安全加固	病毒分析 / 安全漏洞检测
应急响应	安全基线检查

- 安全监控服务
- 安全应急处置服务
- 安全运营服务
- 安全事件分析服务
- 专家诊断服务

业务分布

传统数据中心运维：

英大传媒、天津大学、智芯微电子、江西交通厅、合肥信息中心、合肥市公安、四川移动、诚泰保险、贵州纪委等。

云中心运维：

国家政务云、河北移动政务云、大庆政务云、淄博政务云；成都政务云等。

远程运维：

四川大数据中心、河北医科大学、湖南理工、合肥信息中心等。

新安全测试服务方案

新华三安全服务团队，在原有安全测试方案的基础上，结合多年深耕客户一线的丰富经验，总结并创新，推出一系列全新的安全测试方案，拓宽了新华三安全测试服务能力面。

渗透测试：依托新华三的情报和技术资源，融合新华三原厂渗透工程师、第三方众测人才，融合远程和现场服务，融合人工与自动化工具箱，优势互补，重新定义了渗透测试。

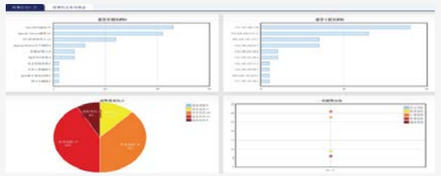
APP合规安全测试：依据国家监管侧相关法律法规，可针对评估点对App个人信息采集行为逐条对应分析，合规问题一目了然。

视频漏洞扫描测试服务方案：新华三推出“利视-iSec安全视频漏扫服务工具箱”（简称: 利视），可实现对视频监控设备的安全检查管理。

新范围

APP合规安全测试

视频漏扫

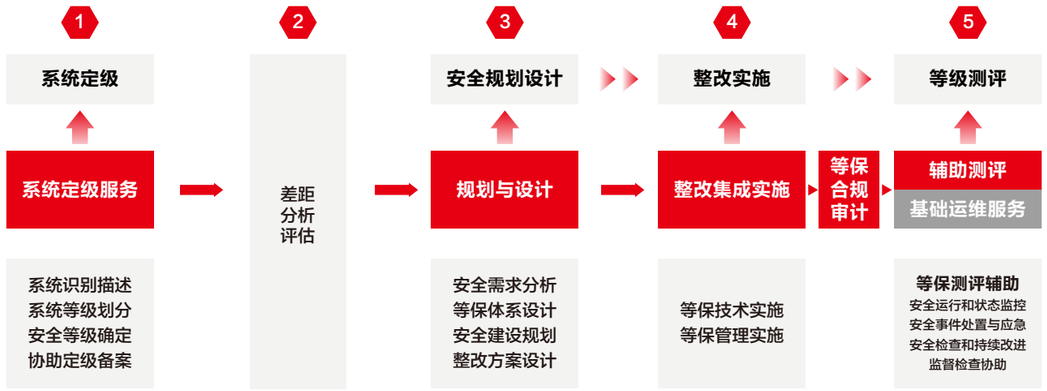


新模式

众测模式

新安全等级保护服务解决方案

新华三安全服务团队通过引入利规-iSec等级保护全流程服务工具箱，不再以获得等级保护认证证书为服务结束标志，而是基于等级保护2.0基本要求，覆盖系统调研建设，等保建设整改，安全运维管理，等保系统测评，系统废除废止全过程的等级保护安全服务工作，实现业务系统等保全生命周期的合规管理。



利规-iSec等级保护全流程服务工具箱

是一款可以对等保工作进行全生命周期管理的工具，可实时掌握等保工作开展状态，顺利通过等保测评，可用于系统调研、差距分析、建设整改、等保自测评分及等保运维管理阶段。

新华三重点安全服务方案介绍——新型服务模式不断破冰

安全集成服务方案

针对多厂商、多产品等复杂型的安全项目，新华三提供总体集成服务，通过组织协同多个友商，真正承担起安全总集角色，包括项目建设、日常运维、安全检查等安全工作，从而提升项目交付质量，确保按照设计完成建设，实现预期效果目标。

优化一：集成商能力优化

新华三作为集成商具备以下能力：大项目管理能力、安全体系咨询及顶层设计能力、安全服务能力（攻防、运维、培训等）

“2+1”转型：两优化+一创新

优化二：项目建设内容优化

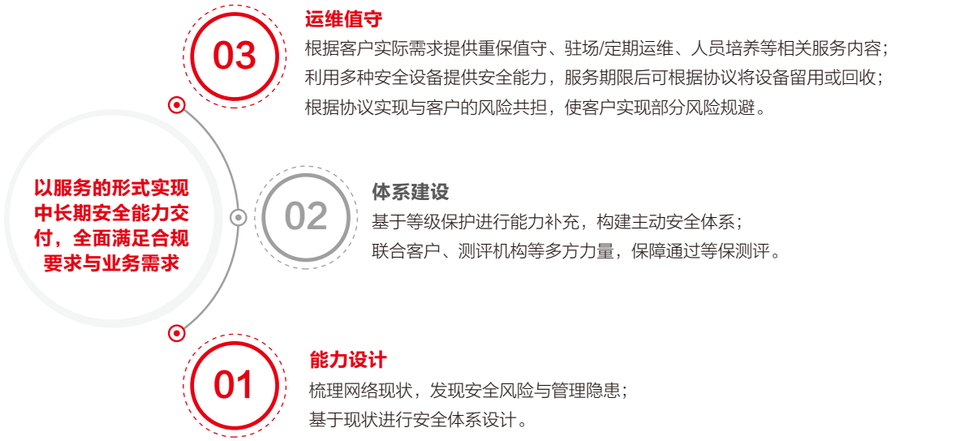
加强了对实际业务风险识别、组织架构、安全技术发展趋势、安全合规需求的调研与评估，项目建设验收点不以系统上线为标准，战线拉长到1年甚至更长时间的运维期结束为项目结束标志。

创新一：安全工作模式创新

新华三以日常所面临的安全工作作为项目交付内容，真正承担起安全总集角色，包括项目建设、日常运维、安全检查等安全工作，所有安全工作统一由新华三向甲方汇报。

安全托管服务方案

新华三为用户统一提供从产品、管理制度到专业服务人员三个方面的支持，从而全面支撑用户信息安全工作的开展，为用户信息安全工作开展效果负责。此服务的关键在于以承接安全工作为交付目标、以安全工作成效为验收标准、以精细化罚则为担当体现。



工具自动化服务方案

新华三安全服务团队近几年在攻防演练、安全事件应急处置等安全服务工作开展的同时，通过经验积累、知识沉淀以及实战校验，以“敢战，能战、可赢”为目标，打造了一系列单兵作战装备，为用户提供攻击分析、安全测试、应急处置、合规管理、策略管理和重保防护等功能，配合安全服务专家，使服务模式趋于自动化、平台化，从而提升安全服务的效能与覆盖面。

利剑-iSec全流量威胁分析工具箱

是一款全方位、多维度高级威胁检测工具，实现APT攻击以及内部违规行为的有效检测，
融合多种网络安全要素实时评估网络的安全攻击态势，保护核心资产。

利用全网流量侦测高级威胁，针对安全事件进行预警、响应和控制。
可实现威胁溯源、攻击取证、恶意代码分析、资产发现梳理、建立行为基线、呈现安全态势、远程专家会诊等功能。

重大时刻保障 | 日常安全评估 | 应急响应 | 攻防演练

利策-iSec安全策略管理工具箱

是一款防火墙策略的全生命周期管理工具，可实现全网不同厂商安全策略集中可视化管理，可节约90%策略排查时间，减少20-30%无用的策略变更。

安全策略管理

- 提高配置的准确性
- 确保策略的改变不带来新风险
- 满足策略最小授权原则
- 减少被攻击的安全隐患
- 周期性采集记录变更
- 定期生成报表发送

策略管理集中化：实现策略自动采集，对设备接口、zone、地址、服务、策略、nat等进行展示，支持策略全局检索、变更对比跟踪。

策略梳理最优化：检测隐藏、冗余、过期、空策列、 可合并的策略等，实现策略优化分析，对策略进行针对性收敛。

策略配置合规化：依据行业安全配置标准或自定义安全规范进行安全配置检查，暴露安全策略中不合规项，便捷优化，满足等保、合规要求。

策略运维自动化：支持路径查询、策略规划、策略生成、策略下发，下发验证回退全生命周期自动运维。

开局 | 日常安全运维 | 重大时刻保障 | 合规检查

利视-iSec安全视频漏扫服务工具箱

是一款专业视频类设备安全威胁检测工具，支持手工录入设备，识别准确率达到95%以上，有效降低视频网络的安全风险。

资产摸底	设备资产识别；设备资产的集中管理；设备资产自动归类	弱口令检测	默认口令；简单口令
资产状态监测	重要资产离线监测；非法接入违规行为识别；异常替换行为识别；网络流量异常监测	漏洞检测	视频监控设备漏洞检测；视频应用漏洞检测；网络设备漏洞检测；操作系统漏洞检测
资产网络定位	IP地址使用审计；网络资产定位；网络接入审计	边界完整性检测	非法外联检测；违规内联检测
通报预警	结果查询统计；事件通知联动；报表报告导出	考核评定	统计分析与趋势对比；检测结果考核评定

视频网络安全自查 | 视频网络安全监管

利保-iSec重保服务工具箱

是一款实现自动化模拟黑客攻击的渗透测试工具，提供一键式渗透测试的全新自查整改体验，
具备6大渗透能力，摸清系统安全的薄弱环节。

资产挖掘探测
依托智能爬虫技术和指纹识别算法，识别广泛类别的IT资产，包括IP、域名、主机、操作系统、应用程序、WEB、插件、网络设备等。

风险量化展示
基于获得数据、权限等实际攻击成果的风险评价，自动生成攻击链图、攻击全景等可视化的黑客剧本及攻击过程。

漏洞检查扫描
具有丰富的漏洞库及安全事件数据知识，各种风险模型及专家知识，提供强大的漏洞挖掘能力。

高级持续攻击（APT）
对目标系统进行长期的，可由多类触发事件自动唤醒的持续的漏洞检查，可触发因素包括知识更新，资产变化，漏洞知识迭代等。

验证渗透利用
利用智能沙箱技术，模拟攻击环境，进行漏洞真实性验证，内置丰富的攻击组件，可支持外网、内网和本地攻击；再后攻击阶段，基于特征字典及逆行数据搜索，收集进一步攻击的支撑数据。

知识积累
对新发现的漏洞或行业漏洞等，可根据系统规则自行编写组件逐步形成属于自己的漏洞组件库。

重大时刻保障 | 攻防演练 | 日常运维

利规-iSec等级保护全流程服务工具箱

是一款可以对等保工作进行全生命周期管理的工具，可实时掌握等保工作开展状态，顺利通过等保测评。

全周期：
利规可支持涵盖等保测评前自查，测评中得分计算，定级备案后系统日常等保状态监控等阶段，从而实现了等保工作全生命周期覆盖。

自动化：
自动识别并采集设备资产信息、自动化的设备安全配置核查、先进的无损扫描技术、自动输出检查报告计算分数。

效率高：
可通过利规快速开展等保合规性评测工作，快速进行合规差距分析，有利于快速开展自评或对下级单位的评测工作。

特点 → 功能

知识库：
拥有内置等级保护管理制度，流程，报表记录，规范化等级保护工作。

智能化：
拥有指标评分算法，智能预测测评结果，自动导出报告，计算分数，智能化等级保护工作。

可视化：
拥有等级保护资产，工作，状态可视化能力，量化资产工作及状态，清晰化等级保护工作。

流程化：
拥有大数据处理能力，能够支撑等保工作运转监控，安全状态监控，资产状态监控，人员工作执行监控。拥有全流程事务通知体系，上传下达，记录留存。
拥有协同管理体系，协同合作，提高效率。

系统调研 | 差距分析 | 建设整改 | 等保自测评分 | 等保运维管理

安全SaaS云服务方案

随着云时代的到来，传统的安全服务模式已无法应对复杂的网络安全挑战，新华三安全服务团队，凭借对国际国内安全市场发展形势敏锐的洞察力，依托于对网络安全市场深耕多年的服务经验，打造安全运营中心，为用户提供安全防护、安全监控、安全测试、安全培训以及安全合规的全面安全SaaS云服务。

功能名称	功能模块	功能内容
云端监测	云监测+本地利剑	云端安全监控、威胁预警、脆弱性分析、攻击态势、链路加测、行为画像、攻击取证、策略优化
云端防护	云WAF+云抗D+云漏扫	云端安全防护、web应用保障、网页防篡改、流量清洗、抗Ddos攻击、抗CC攻击、事前漏洞预警、针对性整改建议
云端专家	7*24小时专家服务	安全值守、责任到人、应急响应、重要保障、安全支撑分秒必争

“云”化产品丰富多样，云端监测及防护功能可选择范围广

“云”端专家响应迅速，事件预警响应速度及时主动

“云”方托管省时省力，用户省去部署时间、空间和财力，安全服务灵活便捷

“云”侧报告质量优良，运行流程专家级保障，产品服务最优化呈现

多 快 省 好

云端监测洞察秋毫 安全防护万夫莫敌

全面的安全服务资质

新华三参与国家信息安全顶层设计，是国家信息安全标准委员会标准牵头编写单位，等级保护 2.0 标准起草单位，作为中国网络空间安全协会理事会员，入选 CNVD（China National Vulnerability Database 即国家信息安全漏洞共享平台）技术组成员单位，同时也是国家信息安全漏洞库 CNNVD 一级支撑单位。

具备安全工程类二级、网络安全风险评估二级、网络安全应急响应一级、信息安全风险评估一级、信息安全应急响应一级、信息系统安全集成一级、等级保护建设资质，还拥有 CMMI5、ISO9001/TL9000 质量体系证书，信息安全管理体系（ISO27001）、信息技术服务管理体系 (ISO20000) 和业务连续性管理体系 (ISO22301) 等资质证书。


ISO27001


TL9000


ISO20000


ISO9001


ISO22301


等保建设能力证书


风险评估服务资质


安全集成服务资质


应急处理服务资质


CMMI5

专业安全服务优势

新华三具备丰富的行业实战经验、全面的安全服务资质、强大的安全服务团队以及成熟的服务交付流程，为客户提供基于行业最佳实践的安全专业服务，保障客户业务的持续稳定运营。

◆ 丰富的行业实战经验

新华三在安全领域拥有超过15年的服务案例积累，结合自身云计算、大数据和大互联的优势，提供最契合客户业务的服务体验。曾为北京奥运会、上海世博会、世界互联网大会、十九大、APEC 峰会、杭州 G20 等重大活动提供安全保障，具备丰富的行业实战经验。并且在“永恒之黑”漏洞、BlueKeep 漏洞、DTLMiner 变种挖矿病毒等重大漏洞爆发的时候，表现出色，获得用户的一致好评。

◆ 强大的安全服务团队

新华三服务团队采用总部安全服务专家 + 区域安全服务工程师的模式，拥有上百名安全服务专家及工程师，涵盖网络安全、云安全、移动安全、应用安全、大数据安全、工控安全、可信计算及物联安全等各领域有丰富实战经验和资质的专家（CISP、CISSP、CISA、CISAW、H3CIE、C-CCSK、ITILV3、ISO27001、PMP、MCSA、DBA 等认证），依托丰富的项目交付经验和技术积累，为客户提供安全规划咨询、安全风险评估、安全研究、安全集成、安全加固、安全攻防等全生命周期的安全服务。

◆ 成熟严谨的服务交付流程

新华三坚持以总部专家对项目进行交付，并在全国各代表处设置安全服务人员，总部专家保证了项目的交付质量，区域服务工程师能够对用户的需求进行及时响应。

新华三交付管理平台对安全服务交付每一个环节制定了专业严谨的服务规范及实施流程，包括项目启动、方案编制、现场评估、风险分析、整改建议、报告撰写、验收准备等几个阶段，以客户满意度为最终目标，可保障高质量的交付实施，丰富的安全咨询与规划经验，业内最完善的售后服务质量保障体系，为客户提 供更高标准的服务。

重大项目保障

基于十多年的信息安全实践经验，新华三信息安全全力满足各大行业在新IT与新经济时代的安全需求，广泛服务于政府、金融、企业、教育、运营商等各大行业，成功保障重大国事会议活动的信息安全。

- 2008 北京奥运会
- 2009 国庆阅兵
- 2010 上海世博会
- 2014 南京青奥会
- 2014 北京APEC
- 2014 巴西世界杯
- 2016 G20杭州峰会
- 2017 金砖国家峰会
- 2018 珠港澳大桥
- 2018 中非合作论坛
- 2018 第14届世界短池游泳竞标赛
- 2019 上海进口博览会
- 2019 北京世园会
- 2019 山西青运会重保
- 2019 国庆阅兵
- 2015-2019 乌镇世界互联网大会
- 2020 国家政务云春节重保
- 2020 火神山/雷神山医院
- 2020 两会重保（合肥信息中心）