

芯生极速 · 智简增效

面向 AI 智能体场景的信创原生全栈安全方案实践

The background features a dark blue gradient with dynamic, glowing light streaks. On the left, multiple blue and cyan streaks radiate outwards from a central point. On the right, several red and magenta streaks radiate outwards from a similar point. These streaks create a sense of motion and depth, framing the central text.

安全与AI共生，对抗中成长

安全能力的三次跃迁

安全技术的发展经历了从规则到学习，再到理解的三个时代，安全大模型的出现标志着安全能力进入了能够“理解意图”的3.0时代。



1.0 时代

规则驱动 + 特征匹配

代表：IDS/IPS、传统杀毒软件

核心逻辑：完全依赖安全专家预先编写的检测规则与病毒特征码库进行匹配

局限性：“知其然不知其所以然”，无法有效应对未知的零日威胁



2.0 时代

机器学习 + 行为分析

代表：UEBA、NDR、XDR

核心逻辑：基于算法建立“正常”行为基线，通过统计学模型检测偏离基线的异常行为

局限性：虽能发现未知威胁，但缺乏深层逻辑推理能力，误报率较高



3.0 时代

大模型 + 智能理解 + 决策

代表：Security LLM、智能体

核心逻辑：利用大模型对海量文本和数据的理解能力，深度理解攻击意图、上下文及逻辑关联

关键转变：从“识别已知特征”全面升级为“理解攻击者意图”，实现主动防御

AI助推黑灰产业，网络攻击门槛下降，安全检测难度抬升

AI驱动攻击自动化



有组织的黑客，通过AI算法动态生成攻击载荷和病毒变种，提升攻击的隐蔽性和成功率。

AI加速漏洞武器化



Mythos模型在主流软件中发现数千个漏洞，包括 FreeBSD 中潜伏 17 年的漏洞。

AI助力社工精准欺骗



通过大语言模型精确伪造音视频和文字，精准钓鱼，提升用户的防范难度。

以 AI 对抗 AI：平衡攻防对抗势力

加速威胁分析能力

加密流量检测

异常行为检测

恶意样本检测

黑客工具检测

DGA域名检测

攻击逃逸对抗

恶意通信检测



提升运维管理效率

威胁狩猎

维保分析

处置建议



告警降噪

综合研判

剧本生产

报告输出

AI赋能攻防实战

渗透测试

代码审计

文件脱壳



情报生产

漏洞挖掘

补丁生成

蜜罐狩猎

“AI + 安全”不是简单叠加，而是共生演化

① AI赋能安全

威胁狩猎、自动化响应，防御效率提升



攻击者被迫升级

② 攻击利用AI

生成钓鱼、对抗样本，攻击进化



暴露AI脆弱

③ AI加固环境

模型加固、防投毒，韧性增强



防御获取新经验

④ 经验反哺AI

攻击样本再训练，AI能力跃升



新一轮攻防



以AI强安全

以安全驱动安全运营
从“感知”到“预判”



以安全护AI

将安全嵌入AI全生命周期
打造可信AI底座



以AI对抗AI

以对抗促进进化
在实战中淬炼协同能力

新华三AI安全能力图谱



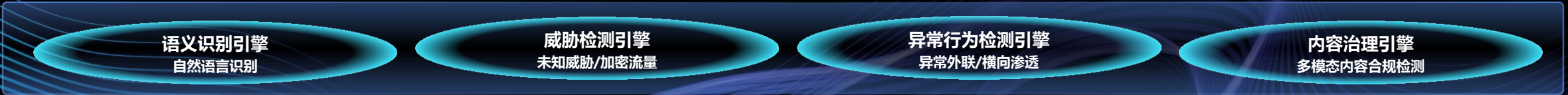
SEC for AI：构建AI内生安全环境，确立AI可信执行体系



AI for SEC：安全管理和安全专项能力提升全面拥抱智能体



AI in SEC：网关产品内置AI引擎，打造AI防护基座





AI in SEC

内置AI，信创网关智能演进

芯片赋能，构筑稳定&极速&全国产的数据中心边界

M9000-CN04 M9000-X06/X10



全国产防火墙
核心器件100%国产化

稳定 全模块冗余架构**99.999%稳定**

成熟 产品头部客户案例**齐全**

性能 吞吐、时延性能优异**1μs**

国产化安全产品的担忧

芯片性能 **低**

➤ 国芯性能**降30%-50%**

芯片稳定性 **差**

➤ 国芯稳定性**不如商芯**

国产化起步 **迟**

➤ 国产化率低，替换进展慢

H3C SecPath M9000国产化系列产品

性能 突破 瓶颈

- 分布式产品性能按板卡数量线性**叠加**
- 性能突破芯片瓶颈，**高吞吐+超低时延**

架构实现 稳定

- 主控模块/业务模块/风扇/电源冗余设计，**故障切换无丢包**
- 平均无故障**提升500%**

多平台带来 安心

- FT 高性能CPU平台
- 海光 高性能CPU平台
- 盛科 高性能交换计算平台
- **16类核心器件全国产**

我们用架构，弥补国产化芯片不足！放心替换商芯！

AI赋能，打造下一代安全检测引擎

新华三AI防火墙内置AI赋能的下一代安全检测引擎，实现本地-云端协同、已知-未知覆盖、性能-深度兼顾、能力自主迭代

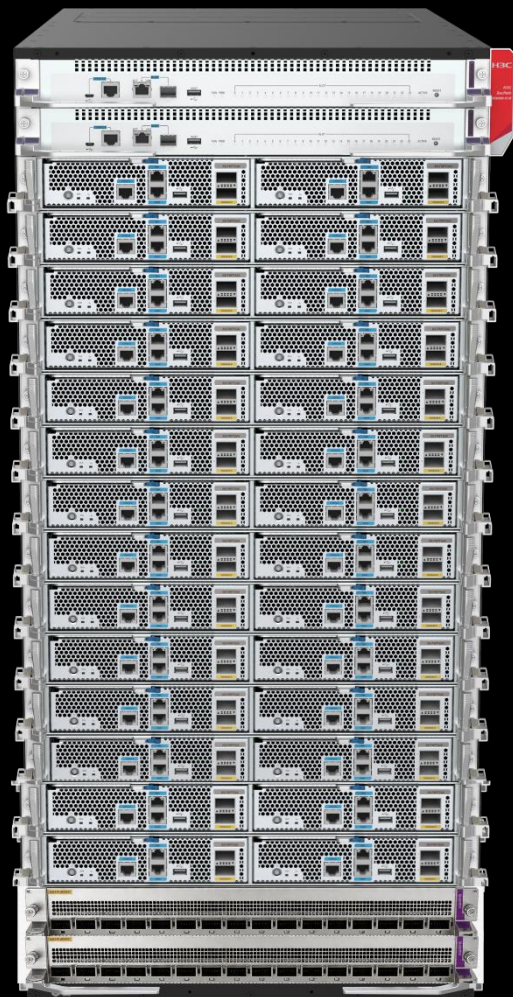


AI 防火墙，内置 AI、识别 AI、保护 AI

单板V，整机**16T**，
业内最高

专用硬件加速，**时延
突破性小于2us**，满
足极速推理时延需求

内置AI运维助手运
维效率极致提升



AI 应用及行为识别：影子AI识别，杜绝 AI 滥用

10000+ AI应用识别，**400+** AI行为特征，精准识别、行为可控；
8000+ AI攻击及漏洞特征，

AI 语义识别，提示词注入防护，屏蔽恶意指令

基于第五代 DPI 引擎开放架构，智能语义分析技术，实现提示词
注入防护，确保智能体意图纯净，准确率**98%+**。

AI 加密流量检测，识别智能体恶意外联及数据传输

独创 “HMM+CNN+主动探测” 组合算法，兼顾性能和效率
识别率**95%+**，误报率空格控制在**0.15%**

发现资产

识别影子AI

识别意图

防御提示注入

检测威胁

异常及风险行为

新华三防火墙能力平替国外厂商，支持4阶18步平滑替换流程，全配置自动翻译

访问控制以及传输加密场景：能力全面平替国外厂商

核心功能1：安全策略

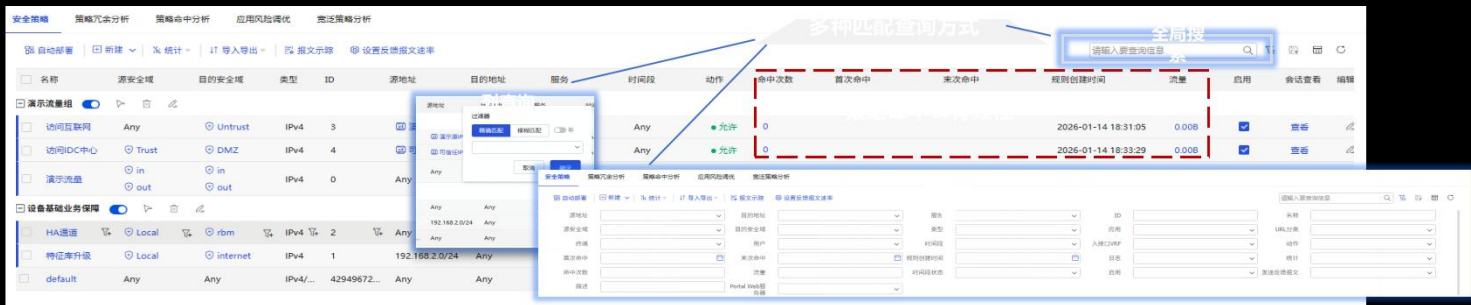
- 策略条目数量同档次高于国外厂商，容量替换无忧
- 匹配条件支持范围相同，支持五元组、应用等条件，动作支持日志、长回话、生效时间等，功能替换无忧
- 命令配置逻辑相近，翻译关系明确

国外厂商策略配置

```
FortiGate-200G-DUT (3) # show
config firewall policy
edit 9
    set name "usetest"
    set uuid 4a24c4c8-f1fa-51f0-f51f-ec98b8ca1ebc
    set srcintf "port17"
    set dstintf "port18"
    set action accept
    set srcaddr "t1"
    set dstaddr "t2"
    set service "HTTP"
next
end
```

H3C策略配置

```
FortiGate-200G-DUT (3) # []
RBM_MIRROR_P[DOT-security-policy-ip-13-usetest]show this
rule 13 name usetest
action pass
source-zone port17
destination-zone port18
source-ip t1
destination-ip t2
service http
return
```



主要涉及款型：F5000-AI系列、F1000-AI系列

内网边界&区域隔离防火墙

主要涉及款型：F5000-AI系列、M9000系列

核心功能2：NAT策略

- 国外厂商：同一个NAT翻译关系可使用两种方式替换，推荐使用全局NAT方式。我司支持全局NAT配置方式，并支持3万+NAT策略，容量无忧。
- 支持源NAT、目的NAT、双向NAT、NAT64、NAT46，创景替换无忧，场景翻译无忧

核心功能3：VPN加密传输

- 支持Tunnel方式以及策略方式配置IPSEC，可平替国外厂商IPSEC功能，加密套件以及算法基本与国外厂商一致
- 标准IPSEC协议，可对接飞塔、思科、PA、华为、山石、深信服等厂商。

应用以及风险检测场景：安全功能丰富替换国外厂商无忧

核心功能1：IPS、WEB等行为风险检测

- 本地2万+ IPS支持，URL云端亿评级库，流引擎能力与国外厂商持平
- 云端AI情报中心，支持IP、域名、URL、文件hash等实时更新，对0-day漏洞攻击拦截
- 本地威胁分析中心，分析展示内网风险主机以及攻击溯源

核心功能2：文件内容风险检测

- 具备防病毒流引擎和文件引擎，提供转发模式优先和病毒检测率优先两个模式，能力与国外厂商基本持平。
- 支持基于文件类型和文件敏感内容过滤，支持邮件、主流传输协议

核心功能3：其他安全能力

- 邮件过滤：标题内容过滤、附件内容检测；
- 智能DNS：支持DNS过滤以及选路
- HTTPS&邮件协议加密流量解密检测
- 带宽限速

配置逻辑相同：一体化安全策略，策略下引用防护策略



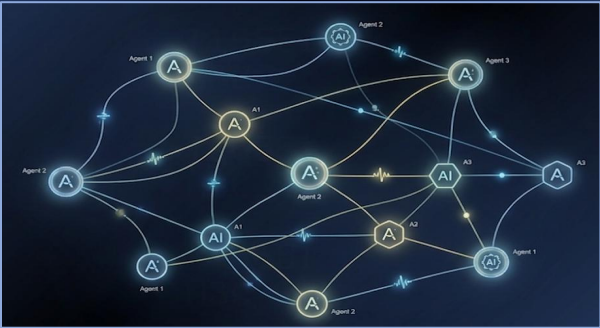
AI for SEC

智启安全，构建主动防御新生态

Agentic SOC智能体安全运营大脑，以Agent对抗Agent

聚焦智能体风险运营，以决策推进自主、以协同重塑生态、以进化驱动成长，重构智能安全运营范式。

自决策：事件自主研判、狩猎和处置



事件研判降噪

概率性推理，确认事件置信度，降噪率95 %

未知威胁狩猎

假设性推理，找证据，发现未知威胁

自主响应决策

自主规划响应处置，无剧本，防止威胁蔓延

自协同：多智能体协同运营



智能体协同

预置30+成熟安全智能体自主运营，事件调查/专项分析

工具协同

自主对接设备、外部系统等

人机协同

低危操作，机器做，人审计；高危操作，机器建议，人执行

自进化：安全能力持续进化



在网数据喂养

安全云能力中心，收集全网数据，驱动模型迭代更新。

在线经验学习

本地安全运营经验沉淀为私域知识库图谱，越用越聪明。

Skill能力拓展

开放平台支持运营技能在线扩展。



日志接入智能体



告警降噪智能体



事件研判智能体



报告生成智能体



响应联动智能体



通报溯源智能体



漏洞挖掘智能体



邮件安全智能体



渗透测试智能体



内容安全智能体



情报生产智能体



代码审计智能体



文件安全智能体



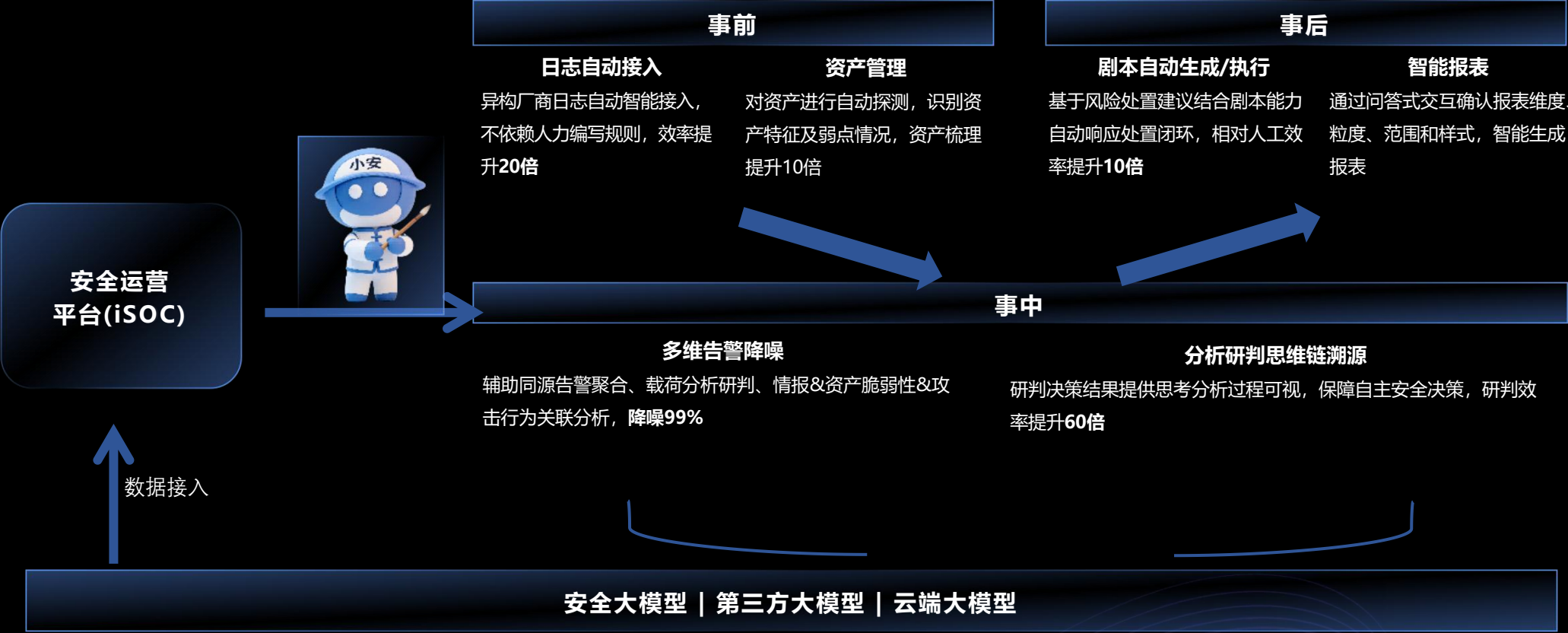
数据安全智能体



等保合规智能体

.....

AI赋能安全运营：打破数据孤岛的主动降噪和协同研判



日志数据、协议元数据、原始报文数据、漏洞数据、威胁情报数据、IT资产信息数据、用户身份数据.....

流量探针

NDR

EDR

防火墙

漏扫

4A系统

资产探针

3rd威胁情报平台



SEC for AI

安全筑基，筑牢AI发展新屏障

AI时代下的安全防护体系演进

Agentic AI
主动感知/规划/决策/执行
关注目标达成

智能体建设



应用安全

身份权限

应用风险

大模型建设



模型安全

算法

数据

Gen AI
被动响应指令
可生成原创内容

底座建设



算力安全

基础设施

主机容器

- **智能体身份** → 智能体身份动静态赋权，打造信任链
- **业务代理** → 代理大模型、MCP、智能体，业务无改造接入
- **防算力滥用** → 精细化token限速，有效管理资源
- **智能体行为画像** → 智能体异常行为监控与分析
- **Skills安全** → skills安全审计，避免恶意文件与外联行为

- **提示词注入** → 安全围栏，基于自然语义发现恶意/嵌套诱导
- **敏感数据外泄** → 审计输出内容，对敏感信息进行撤回
- **数据投毒** → 识别训练语料中的恶意内容，及时阻拦

- **数据泄漏** → 对数据外发行为进行审计，敏感数据及时阻断
- **终端安全** → 容器安全监测、智能体行为管控、高危skills告警
- **默认配置风险** → 端口隔离，配置加固
- **底座防攻击** → ICT 底座及基础设施安全防护

智能体态势感知

Agentic SOC

经典态势感知

新华三智能体安全解决方案



AI安全网关，智能体安全管控中枢

以AI网关为核心，融合身份权限控制、内容安全与数据安全防护，构建智能体全生命周期的零信任安全闭环



THANKS