

## 网络保护一体机



### 产品概述

恩创网络保护一体机专为HW行动中的防守方企业用户打造，HW行动期间，部署在电力、交通、市政、新闻广电、石油石化、电信运营、烟草、智能制造等行业用户的网络出口或关键网络节点处，精准检测攻击行为、洞察攻击手段及方法、动态关联攻击意图，有效破除HW行动中的“战争迷雾”；不仅能帮助企业用户快速定位攻击源头、排查失陷及应急处置；同时也是一款“应试利器”，支撑企业用户在攻击检测、分析上报、溯源取证方面取得高分，顺利通过“HW大考”。

### 产品特点

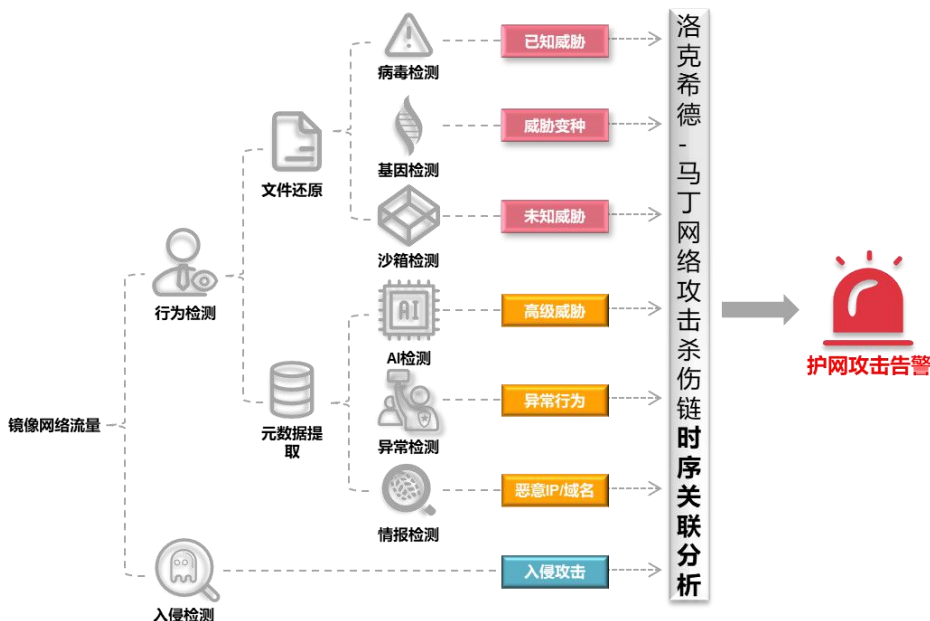
#### 七大产品一体HW

恩创网络保护一体机集成了威胁情报、行为检测、入侵检测、病毒检测、沙箱等7款产品，以方案级的产品架构，系统性的解决HW行动中“攻击检测难”、“分析上报难”、“溯源取证难”的问题。



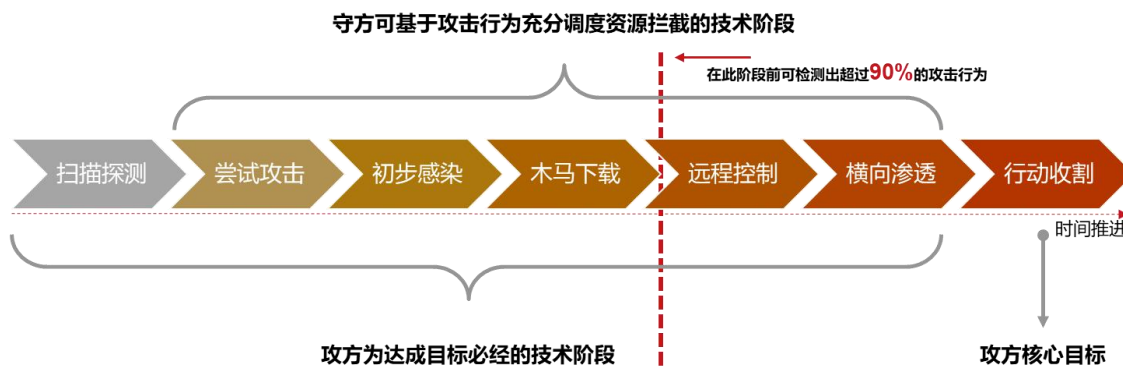
## 多引擎交叉检测威胁

网络保护一体机具备恶意文件、恶意行为、入侵行为的综合检测能力，可有效检测已知威胁、威胁变种、未知威胁等多种威胁类型，基于网络攻击杀伤链进行深度关联分析，可有效发现隐匿的HW高级攻击行为。



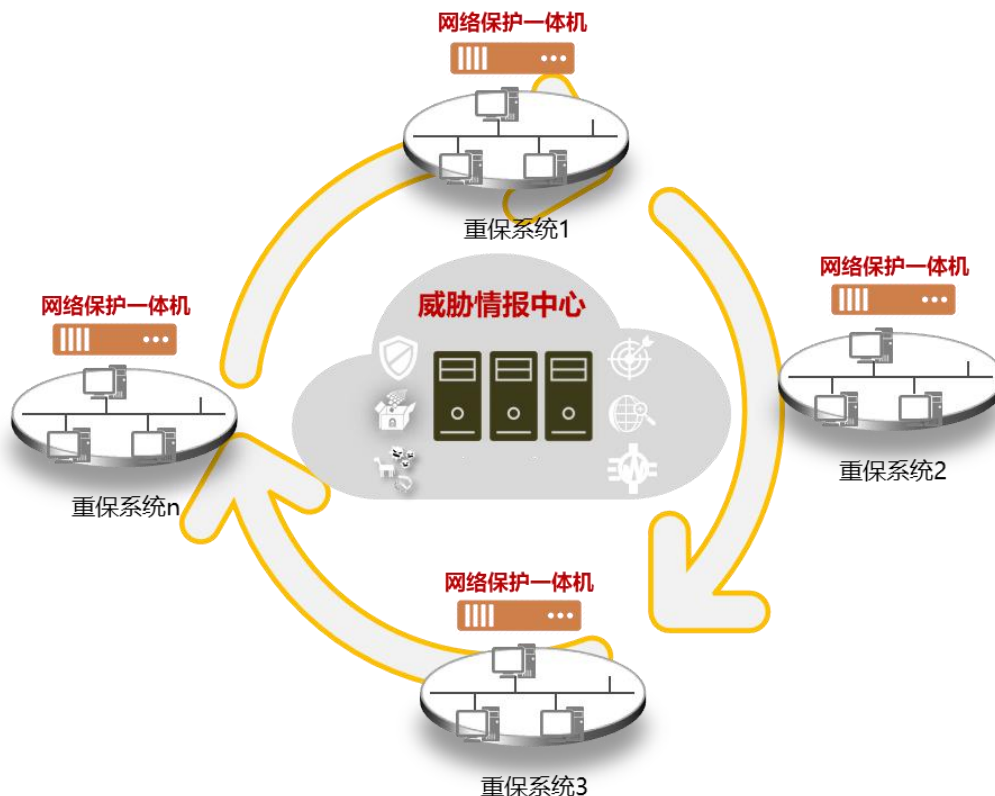
## 高效精准的攻击发现

得益于多产品交叉的检测机制及全局视角的动态关联，网络保护一体机可在木马植入/木马下载阶段检测出超过90%的攻击渗透行为，有效防范攻方最具威胁的“控制、窃取”活动；防守方如不能在第一时间对攻击进行封堵，导致主机失陷，基于HW行动积分制，也可以依赖网络保护一体机的攻击发现进行上报，结合威胁处置获得双倍积分。



## 一 “点” 情报，全网设防

网络保护一体机可实现跨地域、跨行业、跨系统的情报信息共享，做到一处情报，处处设防。



## 全网攻击杀伤链动态关联

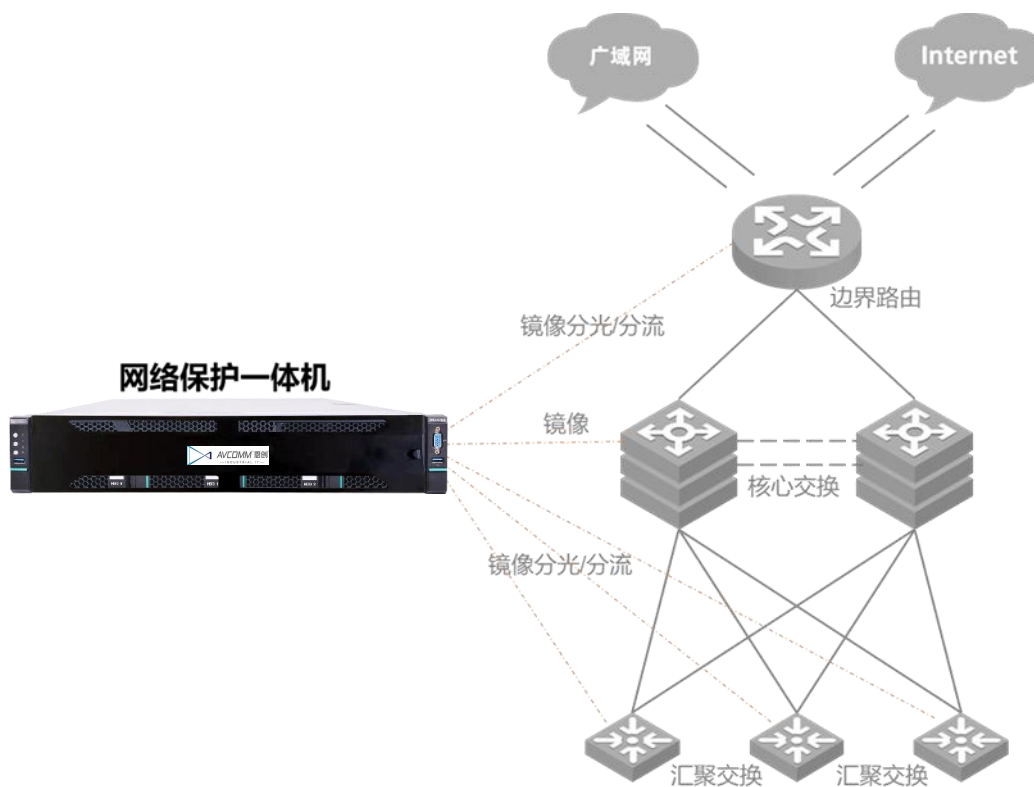
网络保护一体机可将全网攻击杀伤链动态展示，提供防护资源调度决策支撑，针对攻击行为进行“围追堵截”。



## 硬件指标

指标项	NG8200	NG8300	NG8500
存储	250G SSD+4TB企业级HDD	250G SSD+8TB企业级HDD	250G SSD+3*4TB企业级HDD
业务接口	2*千兆RJ45	2*千兆RJ45	2*千兆RJ45+2*万兆SFP
管理接口	1* RJ45	1* RJ45	1* RJ45
串口	1*Console	1*Console	1*Console
USB接口	2*USB前, 4*USB后	2*USB前, 4*USB后	2*USB前, 4*USB后
输入电流	2路100-230V AC	2路100-230V AC	2路100-230V AC
平均功率	550W	550W	550W
宽*深*高	436*665*88 mm	436*665*88 mm	436*665*88 mm
部署类型	2U、机架式部署		
工作环境	温度: 5°C ~ 45°C; 湿度: 20% ~ 90% (非凝结)		
储存环境	温度: -10°C ~ 70°C; 湿度: 5% ~ 95% (非凝结)		

产品部署



- HW行动期间，部署在企业网络出口等边界处可实现边界流量中高级攻击的检测
- HW行动期间，部署在企业网络核心交换处，可实现核心节点流量中高级攻击的检测
- HW行动期间，将边界路由、核心交换、汇聚交换的网络流量通过分光汇集至网络保护一体机，可实现全网高级攻击的检测