

H3C

数字化解决方案领导者



主动安全护航智慧机场

全球机场网络安全事件回顾

越南河内国际机场



- 2016年5月,越南河内内排国际机场和胡志明市新山一国际机场航班显示屏和广播系统遭到黑客入侵.

美国纽约国际机场



- 2017年2月,美国纽约斯图尔特国际机场的750G内部敏感数据遭泄露,包括各类设备密码和员工社会安全号码.

伊朗马什哈德机场



- 2018年5月,伊朗马什哈德国际机场遭到一群不明身份黑客攻击,机场显示屏遭到黑客劫持,并向伊朗政府发出抗议宣言.

英国布里斯托尔机场



- 2018年9月,英国布里斯托尔国际机场遭勒索病毒攻击,机场航显系统遭干扰,导致机场工作人员被迫使用白板和记号笔工作.

国内网络安全体系建设现状

当前状态



合规防护

被动防护

初级防护

主动安全

经验欠缺组织

在出现安全需求时采用相应的安全措施和行为

- 仅边界控制

被动响应组织

能够处理大多数安全需求，依赖外部提供合规性指导

- 传统被动应对
- 多点不协同
- 缺乏风险监控

合规性组织

已可控制框架应对所有监督管理需求和内部风险评估

- 等保合规驱动
- 安全管理初步有序
- 安全运营流程建设
- 关键业务的积极防御

前瞻性组织

具有完备的安全规程，能够在风险早期进行解决处理

- 关注对风险的提前预警
- 外部情报驱动
- 智能化数据分析
- 运维流程自动化
- 防御体系协同联动

演进到前瞻性组织需要四个转变



时间

事后→事前

实现关口前移和提前预警

静态→动态

通过智能数据分析,实现动态安全防护

关联

效率

手工→自动

实现运维自动化提升运维效率

单点→全面

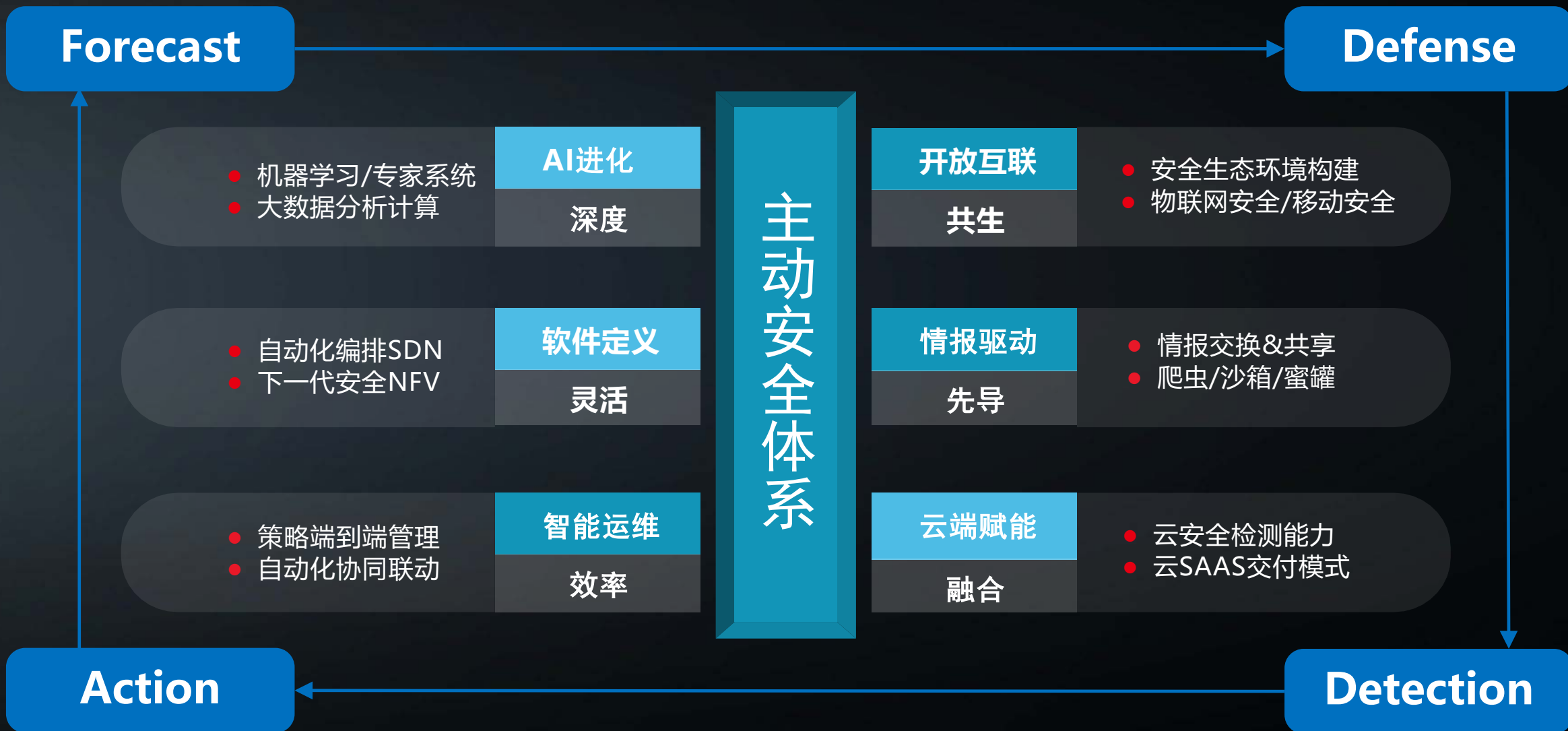
实现协同联动和全面防护

系统

新华三主动安全防御体系架构



四个行为



六大能力



新华三主动安全防御体系目标

预知未来

主动发现

协同防御

智能进化

Thank You!