OWASP
Open Web Application Security Project

企业漏洞管理与持续化追踪建设浅析

爱加密 魏超

目录

CONTENT

OWASP
Open Web Application Security Project

企业面临的安全挑战

1. 安全信息数据孤岛

外部漏洞情报，内部信息系统和设备的日志、网络流量和业务数据中都存在大量的安全信息，但是各自隔离，无法有效整合实现关联分析。

2. 安全态势难以评估

工具平台各自独立，安全人员须投入大量的工作精力关注各类告警，但安全态势无法整体直观的呈现。决策缺乏有效依据。

3. 层出不穷的安全漏洞

应用漏洞越来越严重，安全事件频发、各类攻击手段层出不穷，如勒索软件、APT、DDoS，难以快速准确定位、分析和取证。

4. 日趋复杂的安全保障需求

互联网金融业务蓬勃发展，信息系统复杂度越来越高。来自内部和第三方合作单位的的安全漏洞不容忽视。

5. 安全能力局限性

网络安全基础较为薄弱，管控机制须不断完善，安全人员的数量和技术能力略显不足。能调动的外部技术资源相对受限。

6. 监管合规

网络安全法的实施，对日志存储，信息安全事件处理，安全态势感知等方面均提出相关要求

。

OWASP
Open Web Application Security Project

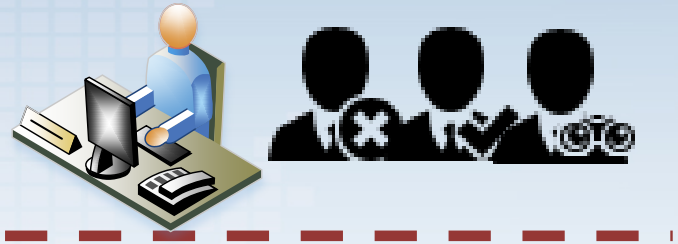
复杂的网络安全架构

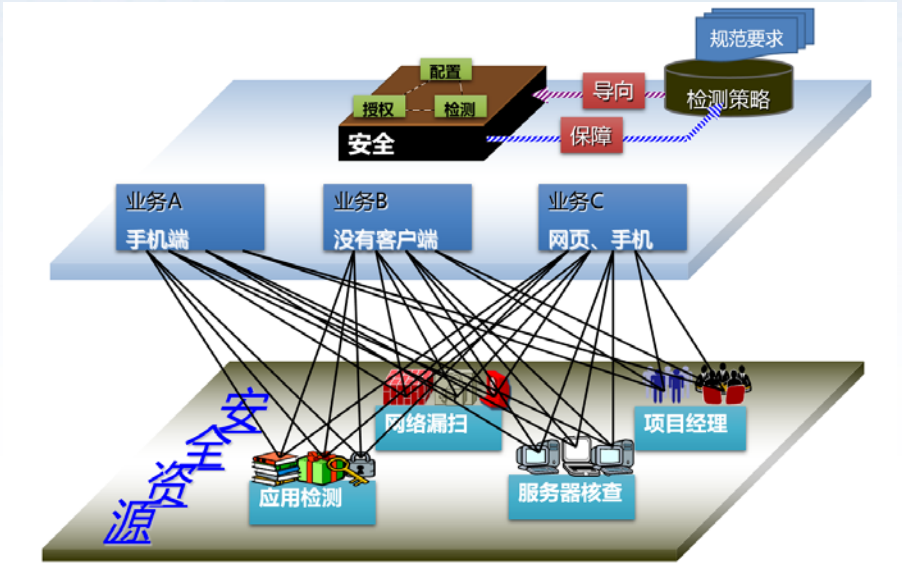
新业务爆发带来的安全压力

- 快速版本更新带来的工作压力
- 技术人力投入的局限
- 一些安全工具的安全误报率高

  （重复、无用及错误！）
- 缺乏整体评估的安全保障

线上业务增多
安全压力增多





OWASP
Open Web Application Security Project

不同维度下的风险边界

来自安全的风险

- 物联网风险
- 病毒木马
- 劫持攻击
- 注入攻击
- 调试攻击
- 框架攻击
- 网络攻击
- 云安全风险
- 其他攻击

来自业务场景的风险

- 交易欺诈
- 虚假营销
- 刷单刷量
- 其他场景

来自自身的开发风险

- 性能下降
- 响应迟缓
- 功耗增加
- 程序崩溃
- 其他缺陷
- 体验缺失

来自运营场景的风险

- 转化率下降
- 留存率下降
- 无效推广
- 运营策略缺失
- 其他场景

目录

CONTENT

OWASP
Open Web Application Security Project

新形式下企业安全需求分析

管理范围

安全管理的范围涉及移动业务各个层面资源调度和使用，在系统初始考虑到相应的安全资源配置与安全设计。

业务发展

市场环境与业务需求带来的安全风险需设计相对应的防范策略，在安全与业务中寻求企业的平衡点，保障业务的核心竞争力。

技术发展

不同技术平台的业务实现方式和安全评估，同时需结合虚拟化、云计算等行业技术发展带来的安全需求变革。

合规意识

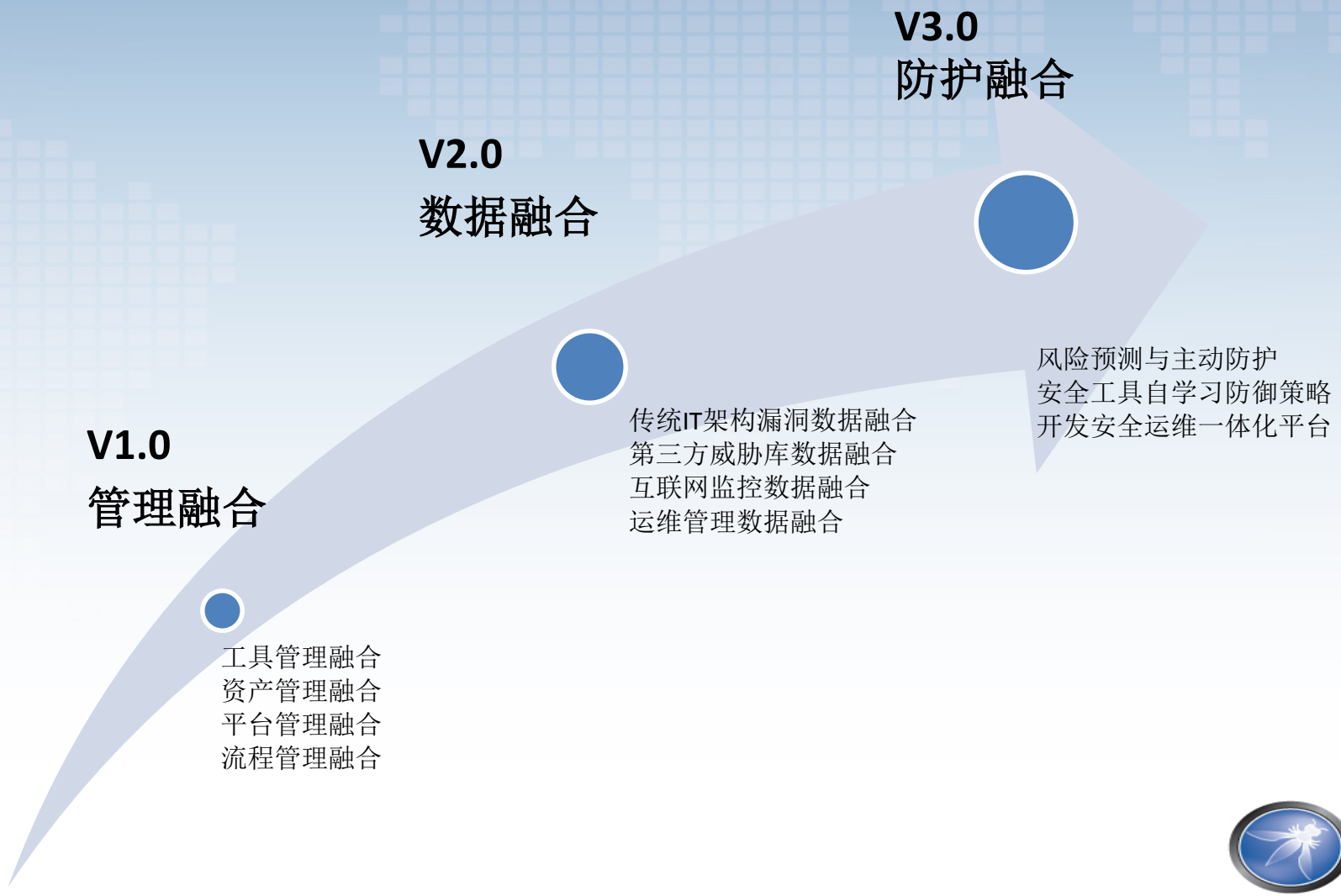
参照并匹配遵循国家、行业、企业相关安全规定，保障业务系统合法合规。

OWASP
Open Web Application Security Project

企业安全防护要素

云计算　大数据　人工智能　移动互联网　物联网　区块链　边缘计算

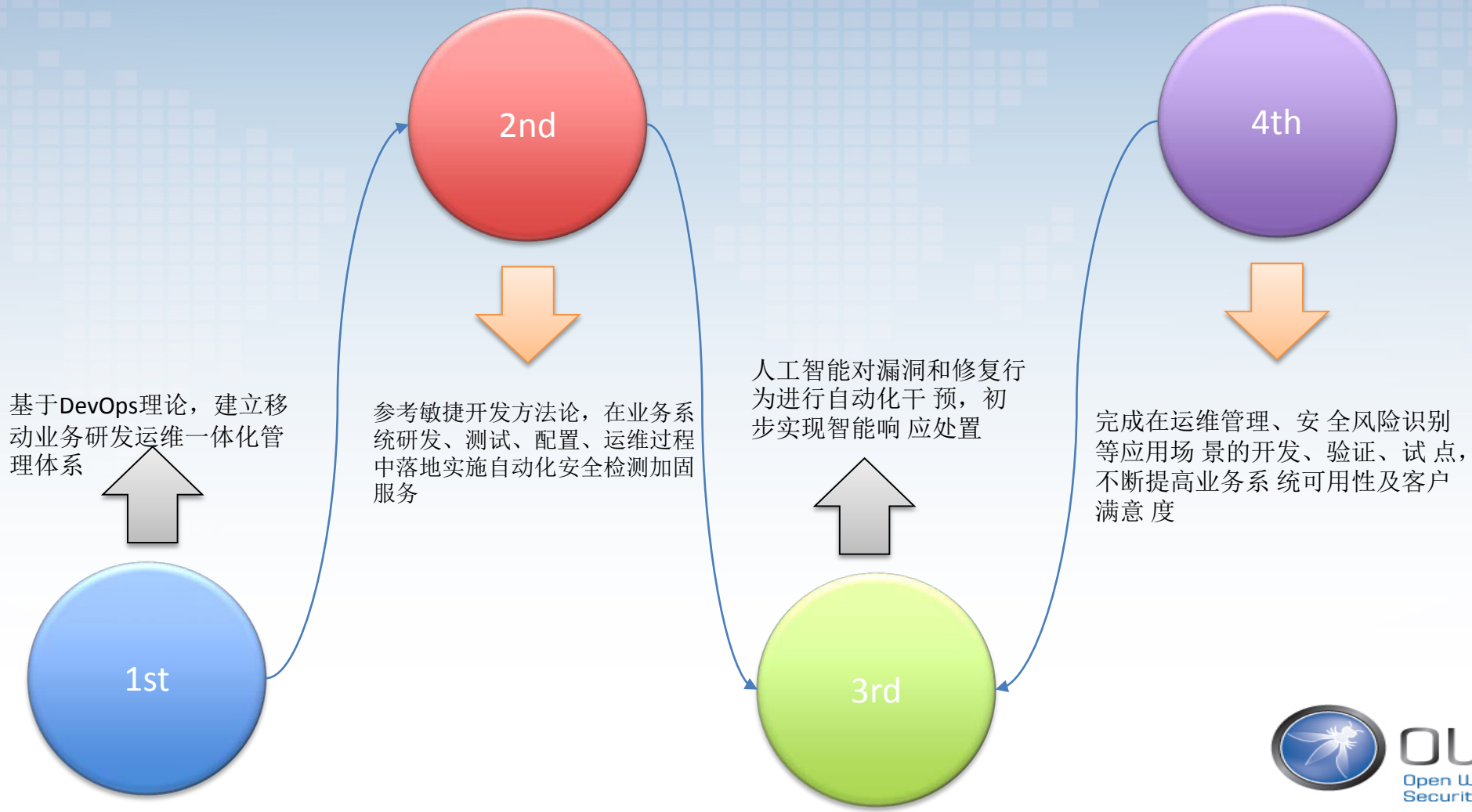
可持续性安全防护体系建设规划



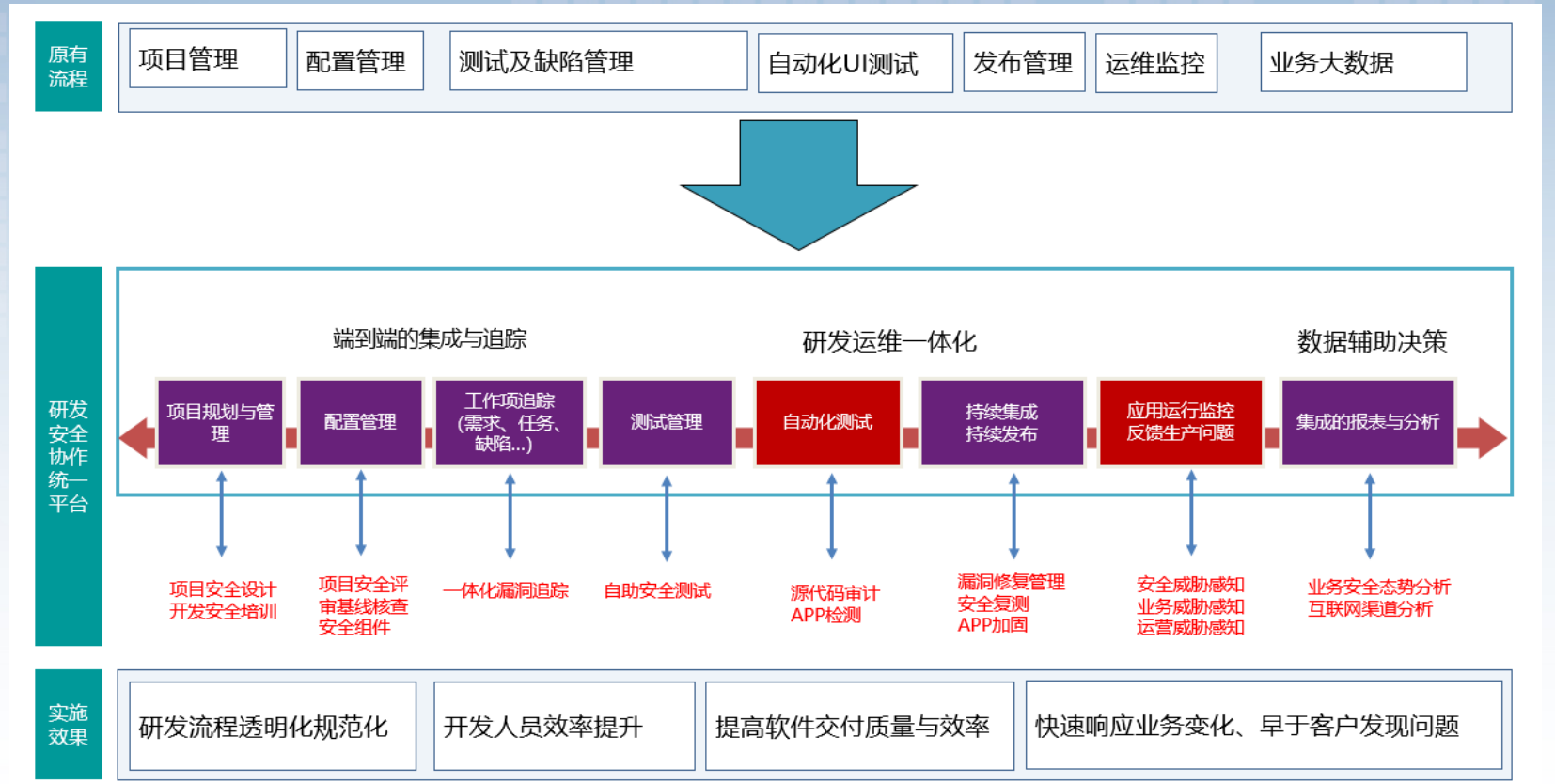
OWASP
Open Web Application Security Project

总体架构示意图

管理融合设计思路



研发安全运维一体化流程设计



漏洞作为核心指标参数

全业务范围采集

漏洞全生命周期管理

流程与业务协同自适应

高管层

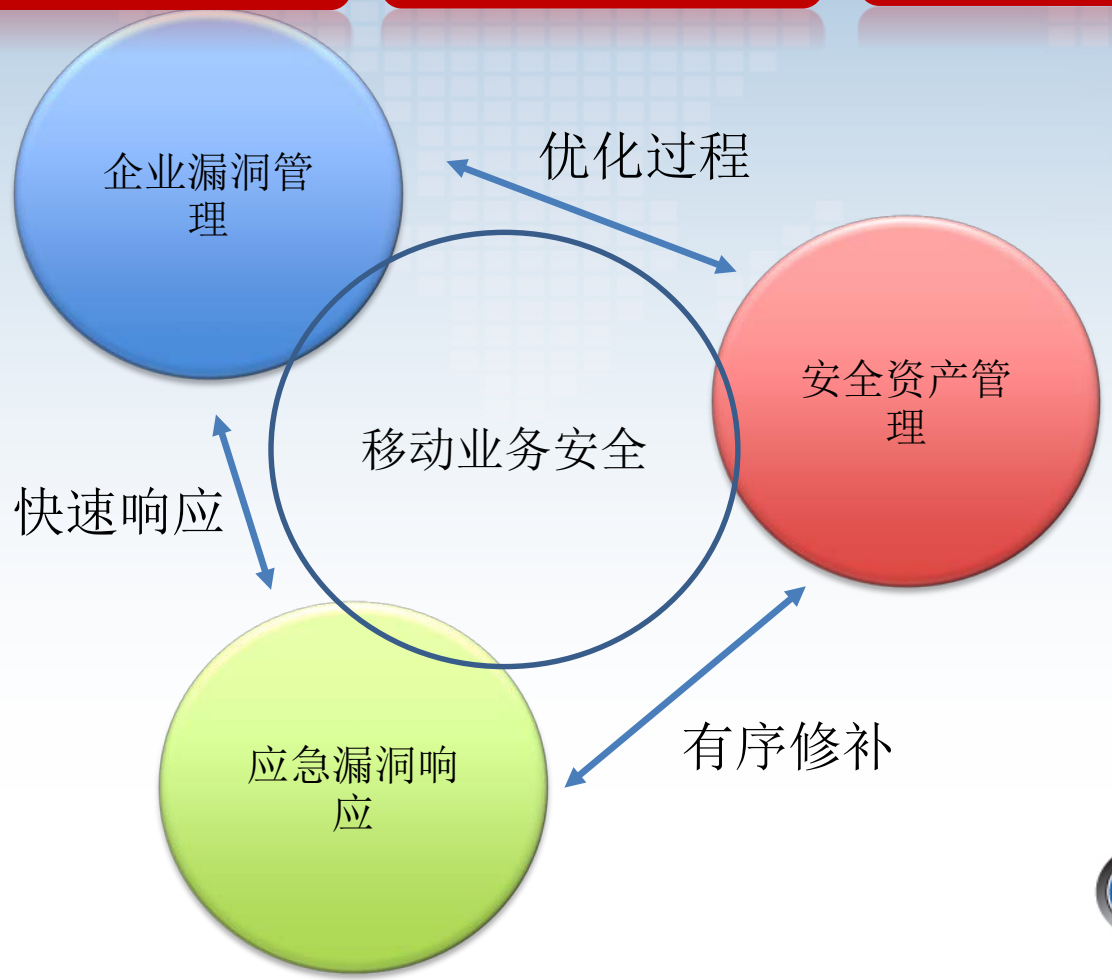
法规遵从，法律免责

管理层

新技术、安全规划、业务防护、工作量化、运维优化

技术层

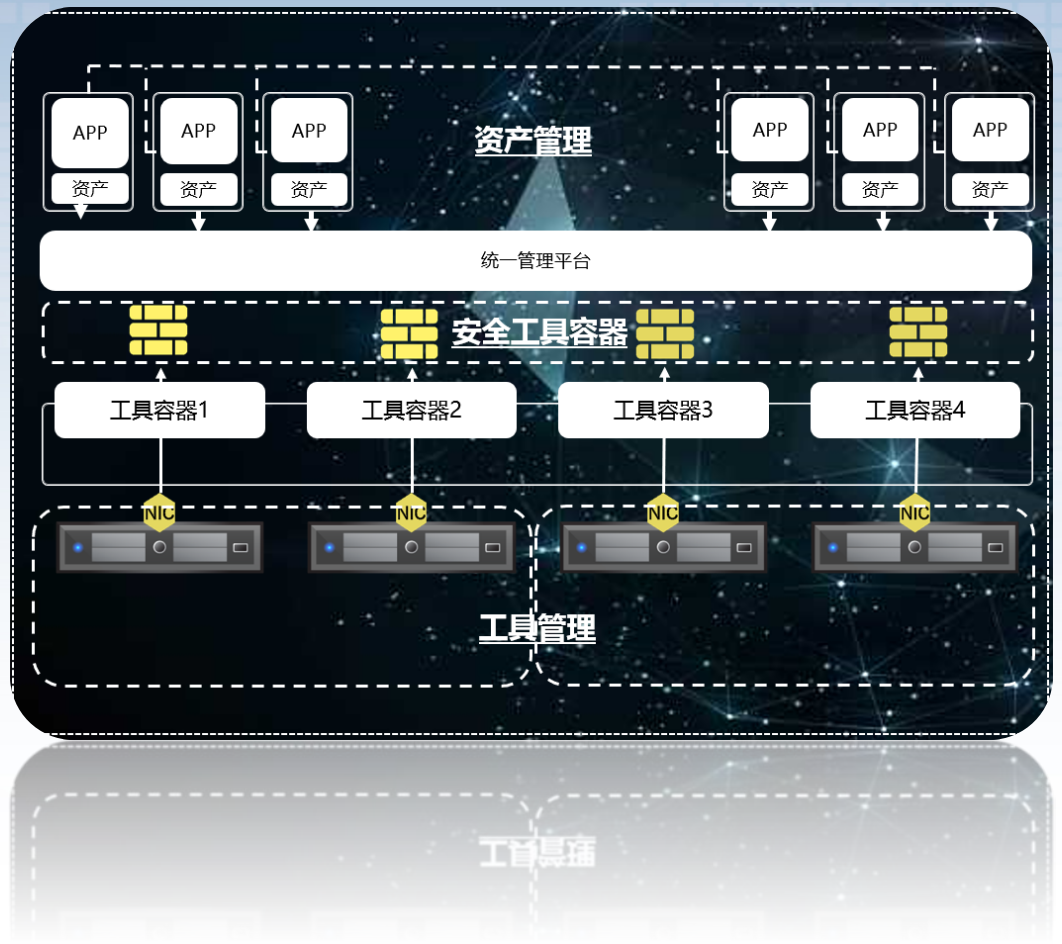
框架融合，问题跟踪，主动防护



管理融合核心目标

安全自动化

快速实现基于云架构的安全工具集成



工具中心

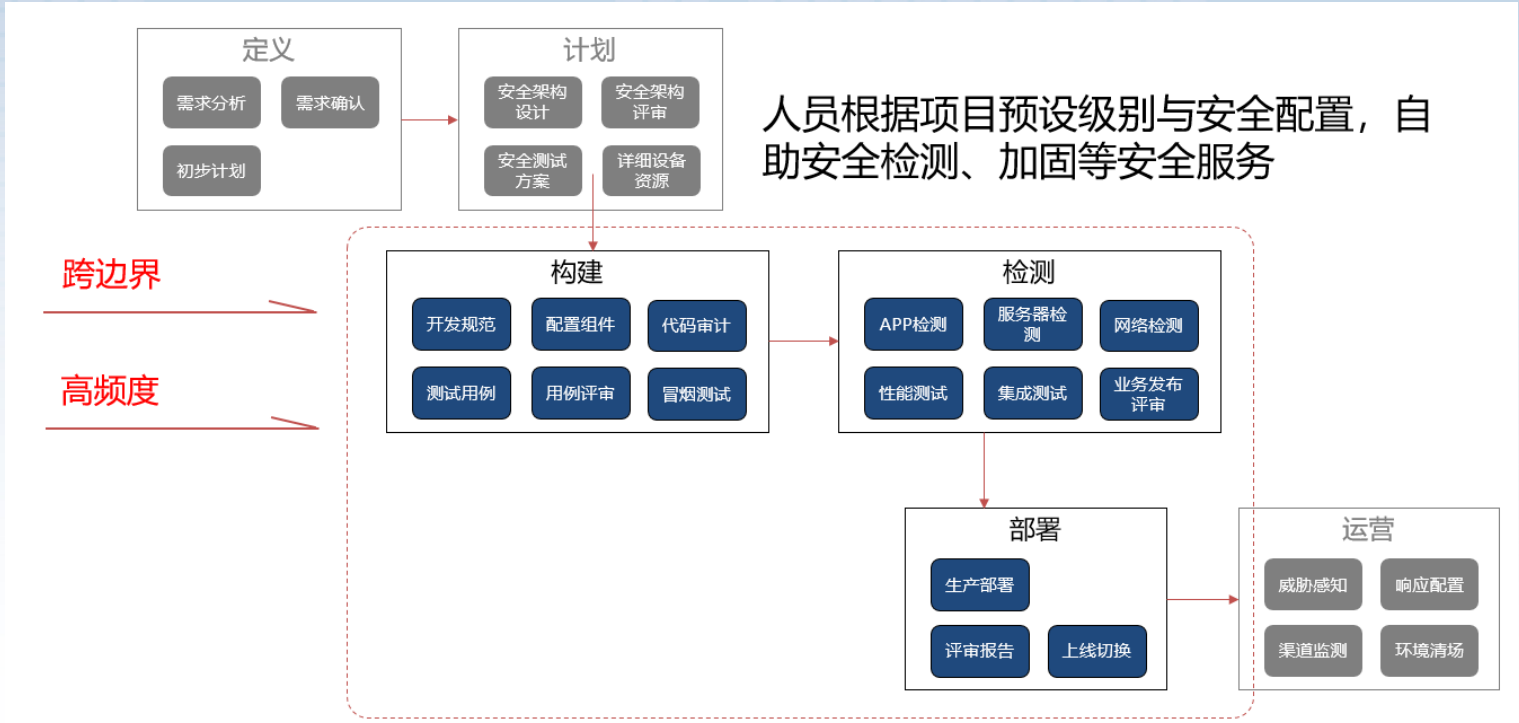
安全运营管理平台为企业安全工具及服务提供基础统一的运行环境。

- 通过容器化技术可以将现有企业安全工具集成到同一平台进行管理运行
- 支持快速集成扩展第三方安全工具
- 支持底层数据打通与安全数据采集
- 支持上层安全工具联动进行协同防御
- 支持统一安全管理与系统管理

OWASP
Open Web Application Security Project

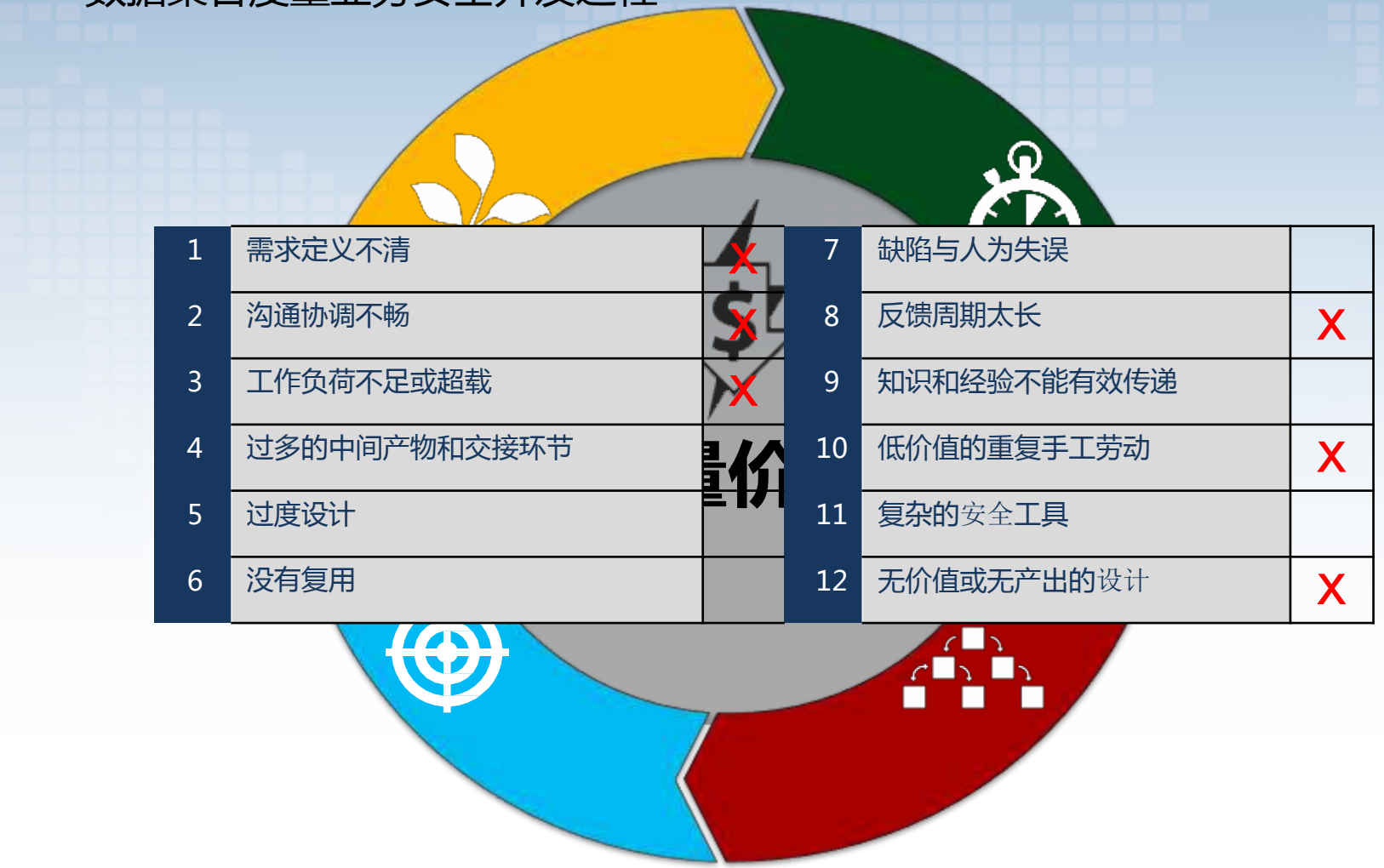
服务自动化

梳理核心开发流程，线上定义安全自助服务



趋势可度量

数据聚合度量业务安全开发过程



1	需求定义不清	X	7	缺陷与人为失误	
2	沟通协调不畅	X	8	反馈周期太长	X
3	工作负荷不足或超载	X	9	知识和经验不能有效传递	
4	过多的中间产物和交接环节		10	低价值的重复手工劳动	X
5	过度设计		11	复杂的安全工具	
6	没有复用		12	无价值或无产出的设计	X

漏洞风险闭环管理

“事前”

漏洞发现和管理

checklist
应用检测
病毒检测
权限检测
信息采集
…

“事中”

行为检测与阻断

界面劫持感知
Gdbserver调试感知
Ida调试感知
Inject注入检测
Xposed插件和
zjdorid攻击…

消息提示
页面弹窗
终止程序
…

“事后”

事件报告、分析与整改

破解痕迹确认
溯源与反制策略
日志审计
整改与**加固**
…

安全报表
攻击态势统计
事件分析
…

漏洞闭环管理

数据融合的基础边界

自构体系

自构体系指企业内部自构的数据采集体系，如APP中的自埋点数据，历史数据以及各种业务产生的日志信息。

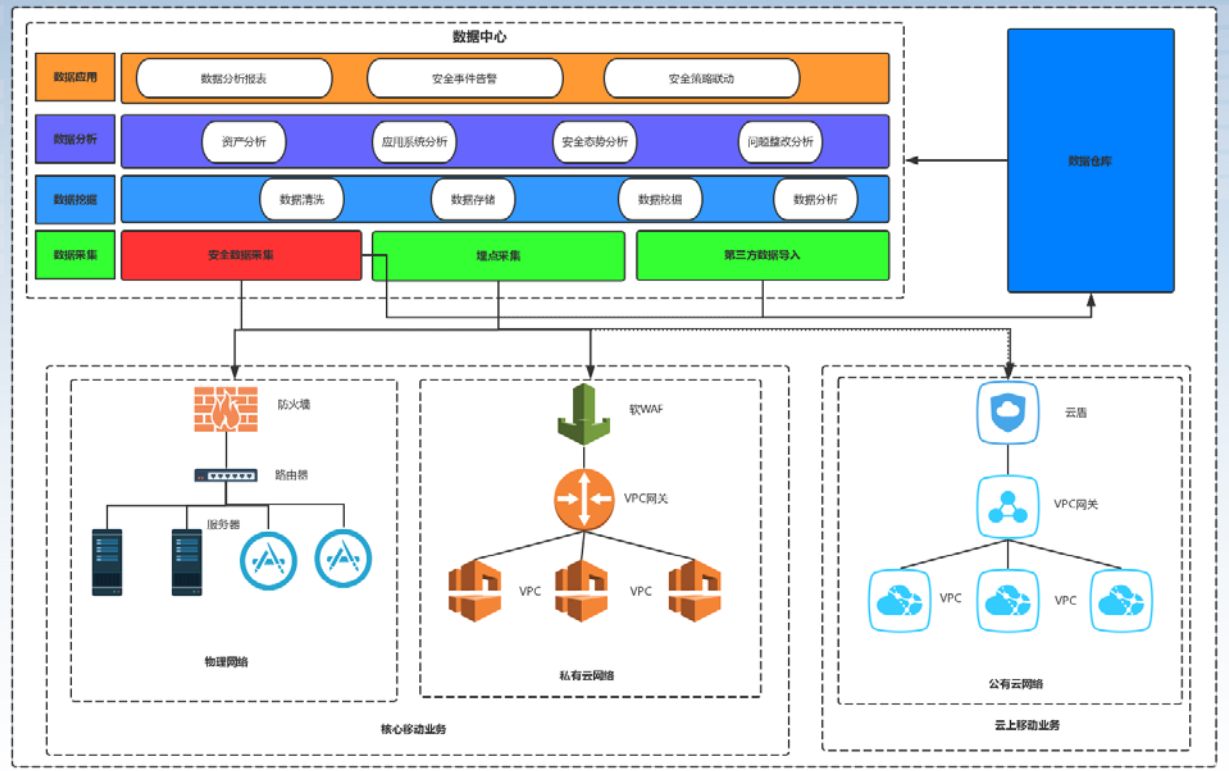
赋能体系

赋能体系指感知系统为客户提供的数据采集体系，包括爱加密的感知SDK采集和业务层的可视化埋点采集数据。

派生体系

派生体系指第三发提供的数据采集体系，包括客户处集成的第三方SDK的数据采集，客户处第三方服务平台的数据导入以及从合作伙伴处获取的相关数据。

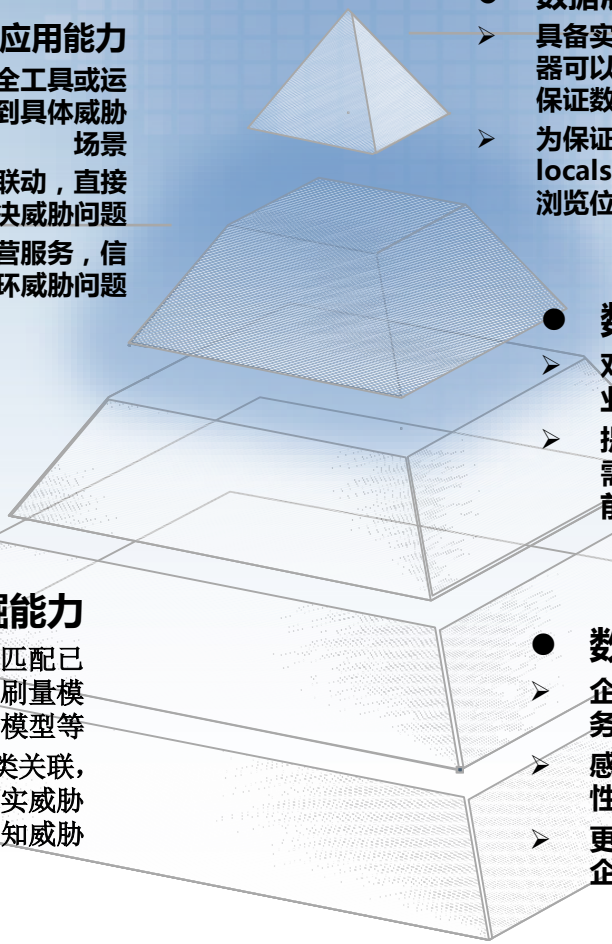
基于云架构数据融合处理中心



数据处理中心

- 数据采集：通过安全运营管理平台的安全数据采集，埋点采集以及安全工具数据导入或第三方平台安全数据导入，采集多维数据并汇总到数据仓库统一处理
- 数据挖掘：采用大数据与机器学习算法对数据进行清洗，存储，挖掘产生大量数据标签提供计算
- 数据分析：提供自定义的场景分析，用户可通过标签关联威胁场景进行未知威胁分析
- 数据应用：通过数据应用可以提供上层工具间的安全告警和智能联动

数据融合能力设计



数据展示能力

- 具备实时消息推送的通讯架构能力，当发生数据变换时，服务器可以主动推送信息到展示端，无需人工刷新再拉取数据更新，保证数据展示的即时性。
- 为保证用户在多个切换可以关联查看分析，展示框架上应采用localstorage等技术，保证页面切换后返回上一页面保留用户浏览位置与信息，方便用户在多页面关联查看。

数据应用能力

- 数据分析得出的决策可以与企业自身安全工具或运营等工具联动，直接推动策略下发应用到具体威胁场景
- 通过提供安全，运营等产品与感知体系联动，直接解决威胁问题
- 通过服务方式为企业提供安全服务，运营服务，信息服务等多种服务闭环威胁问题

数据分析能力

- 对已知威胁的分析能力，包括：安全数据分析，业务数据分析，运营数据分析等
- 提供扩展分析接口，企业基于某威胁场景导入需要分析的数据，通过机器学习快速分析出当前场景下的潜在威胁

数据挖掘能力

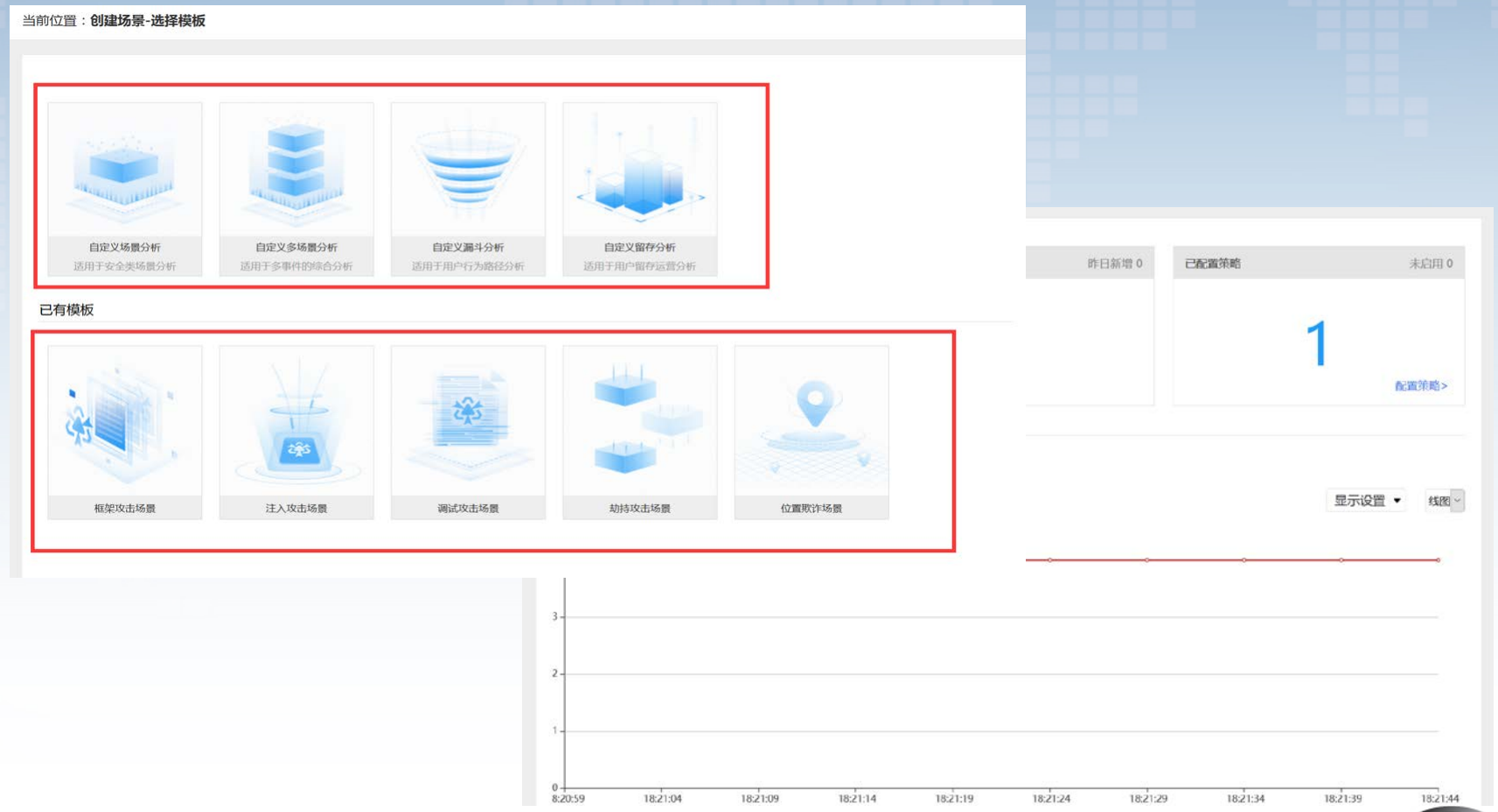
- 具备常见已知威胁的模型库可以快速匹配已知威胁，如位置欺诈分析模型，刷单刷量模型，常见攻击分析模型等
- 采用机器学习算法，对海量数据做分类关联，可以通过人工训练不断纠错，建立真实威胁模型，预测未知威胁

数据采集能力

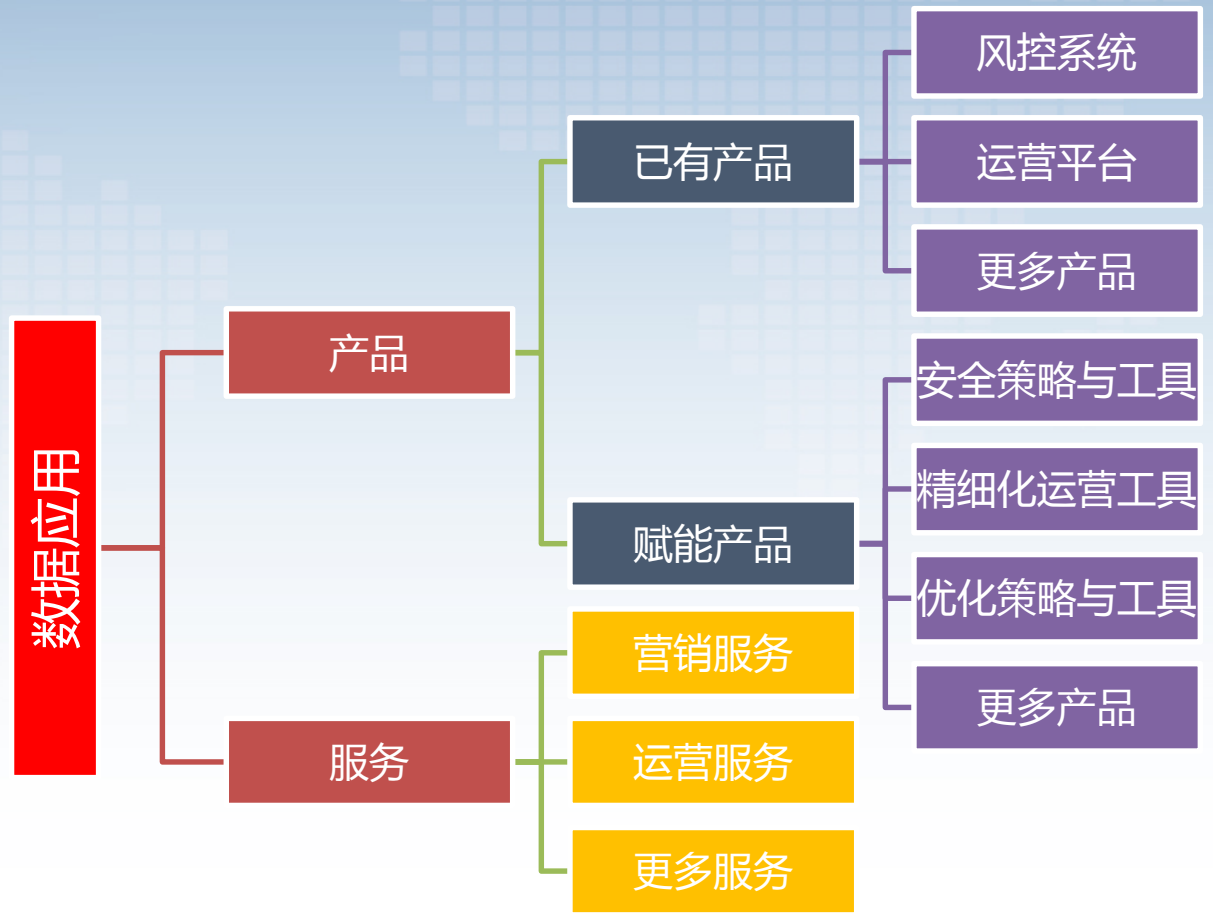
- 企业自身数据的采集，包含自埋点数据，历史数据及各业务产生的日志信息数据
- 感知体系采集的数据，包含基础数据采集，安全数据采集，性能数据采集，崩溃数据采集等
- 更多第三方体系的数据采集，包括第三方SDK采集的数据，企业自身运营或安全平台的数据导入等

场景化安全分析能力

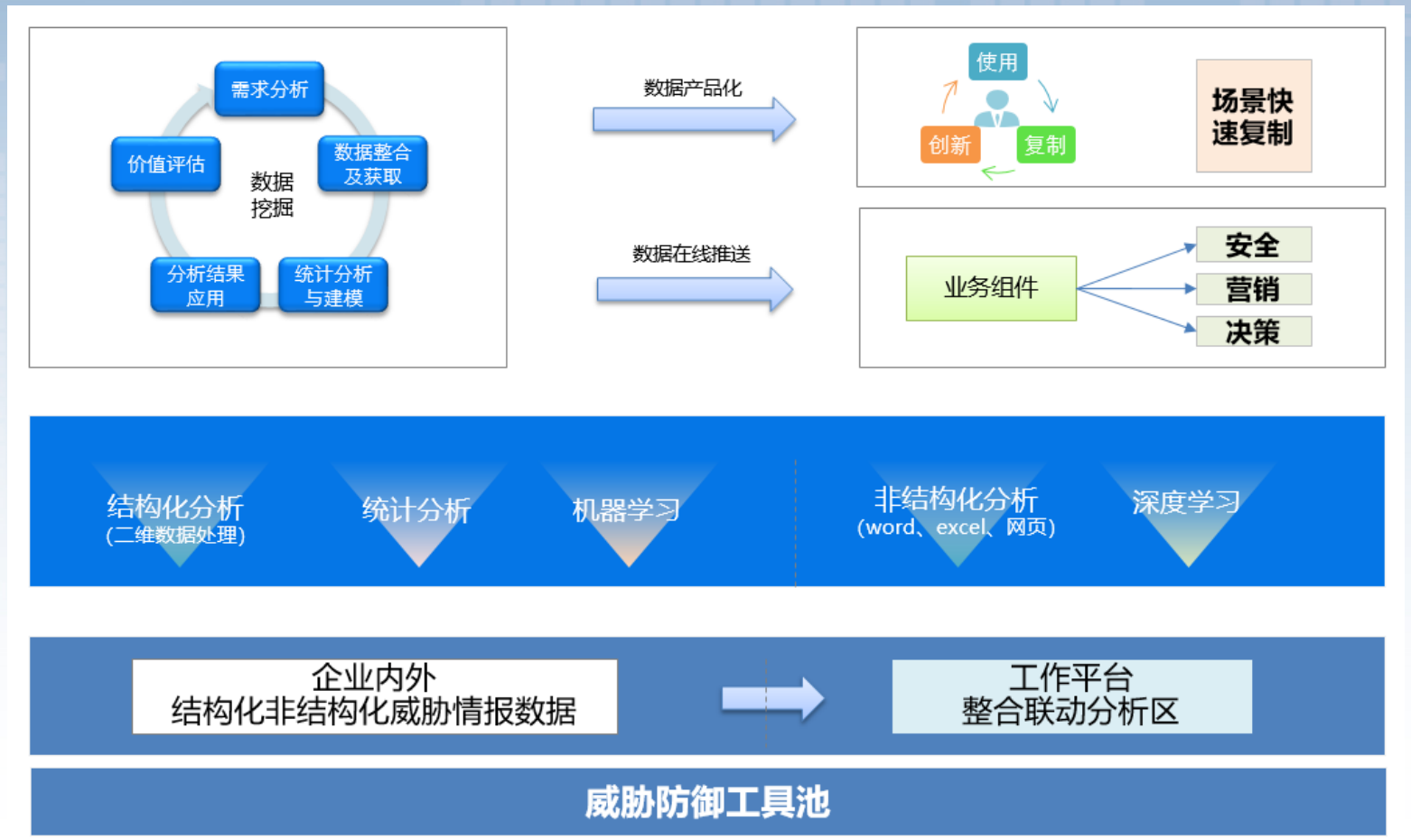
场景化安全分析能力



场景化数据应用能力扩展

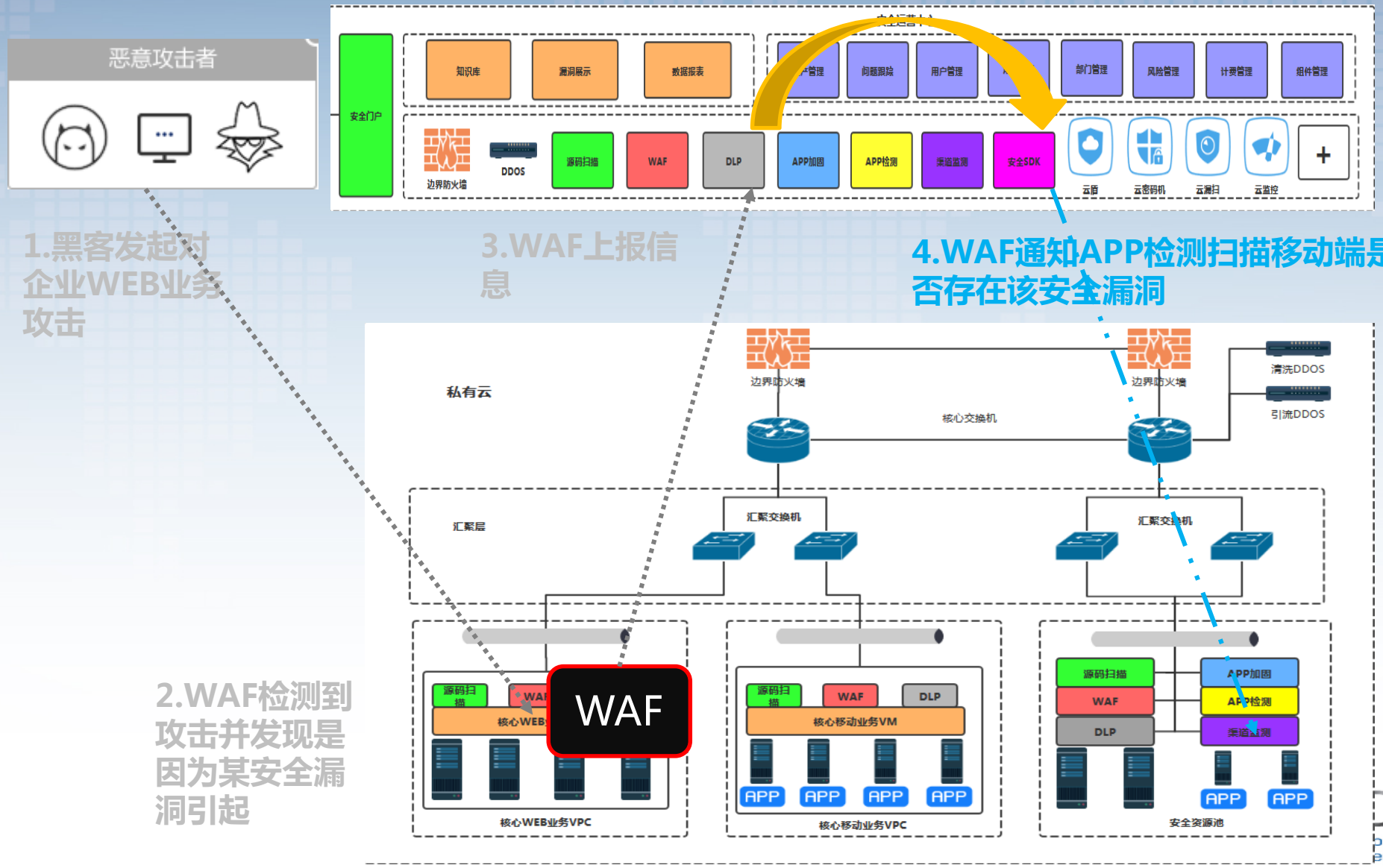


平台化持续性数据服务能力



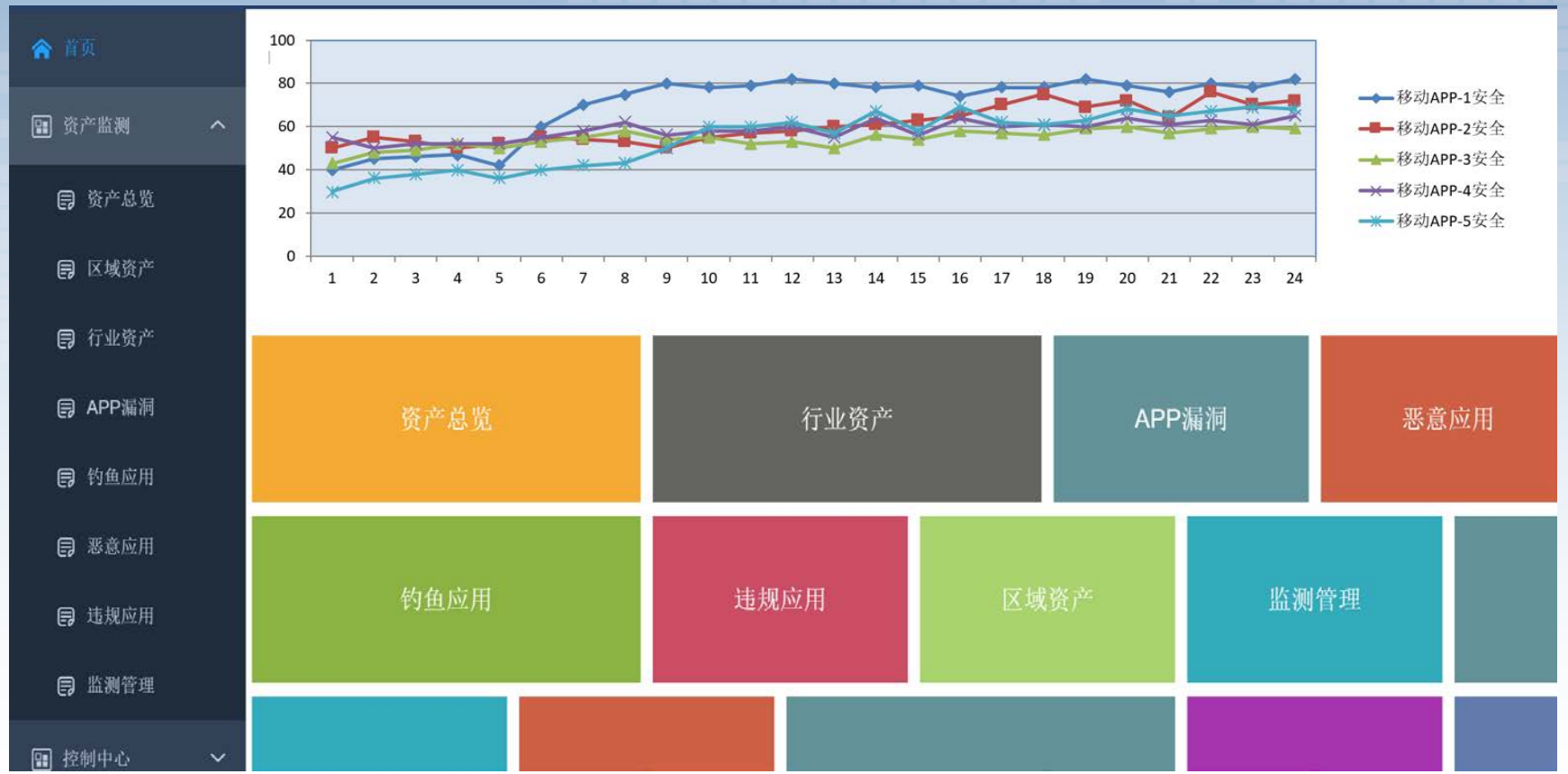
防护融合设计

主动防御示例



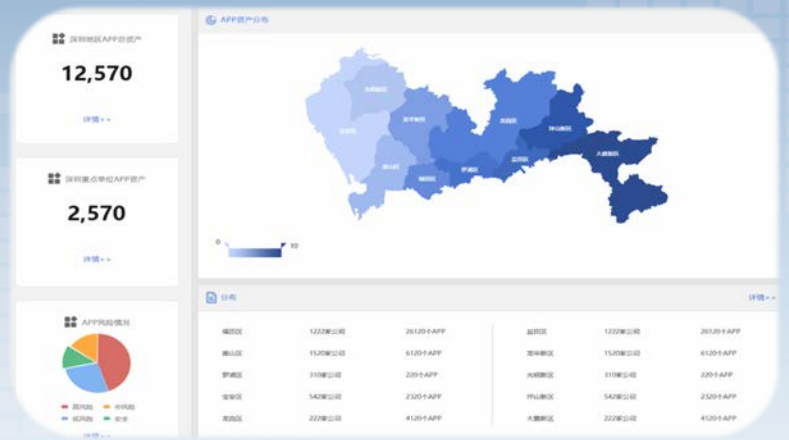
OWASP
Open Web Application Security Project

企业资产互联网安全监测

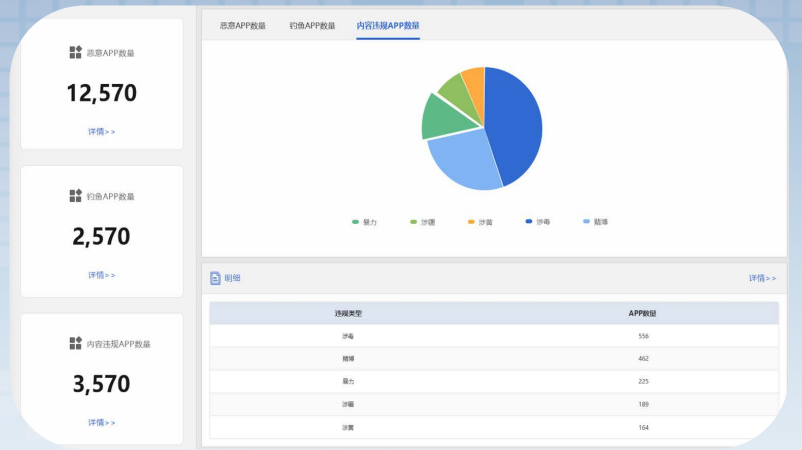


企业资产互联网安全监测

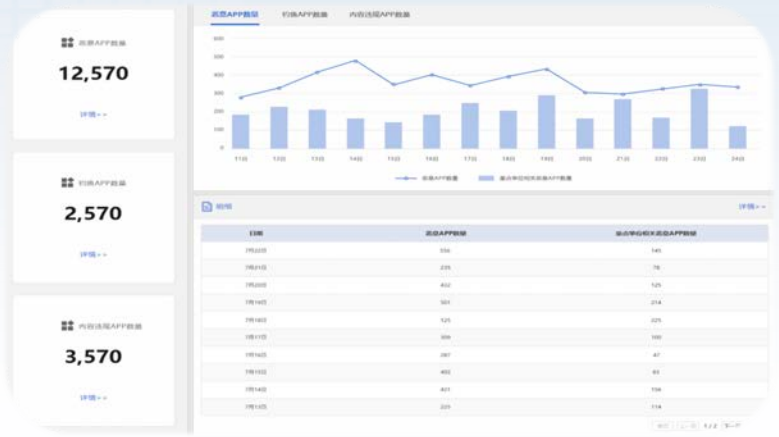
地区分布



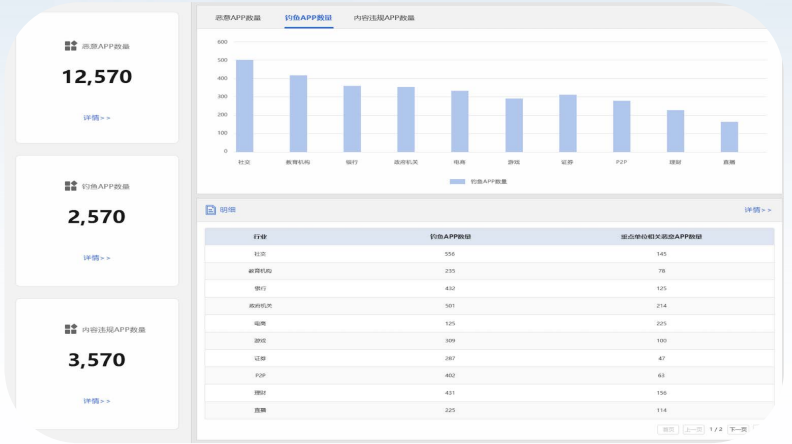
违规应用



恶意应用



钓鱼应用



OWASP
Open Web Application Security Project

可持续安全防护管理体系价值

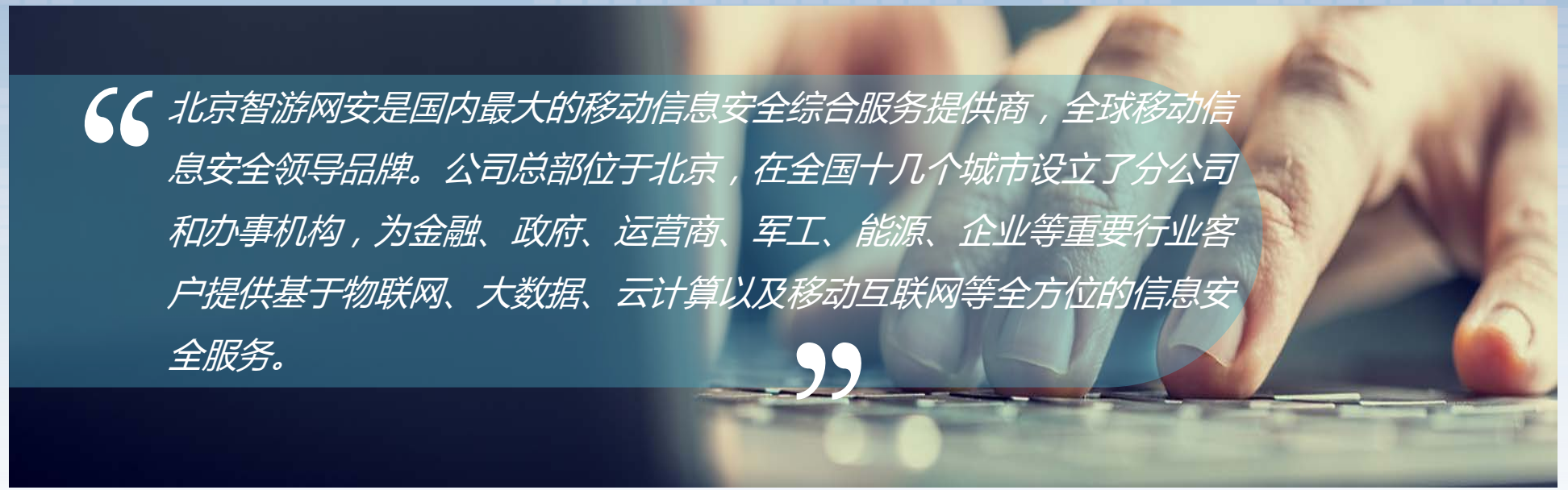
统一融合	数据驱动	智能连接
➢ 统一现有安全管理门户 ➢ 提供各安全工具统一运行环境 ➢ 统一安全策略，安全漏洞管理	➢ 可采集，汇总，接入多方数据，采用大数据架构挖掘，分析企业已知及未知安全风险	➢ 可打通企业各独立安全防御工具接口与数据，使各个安全工具可以联动运行，形成整体协同防御防御效果

目录

CONTENT

OWASP
Open Web Application Security Project

可持续漏洞安全管理体系价值



北京智游网安是国内最大的移动信息安全综合服务提供商，全球移动信息安全领导品牌。公司总部位于北京，在全国十几个城市设立了分公司和办事机构，为金融、政府、运营商、军工、能源、企业等重要行业客户提供基于物联网、大数据、云计算以及移动互联网等全方位的信息安全服务。

- 超过200员工
- 超过一半为技术人员
- 超过2000+标杆行业客户
- 50+公司权威资质认证

- 覆盖Android、iOS、H5及物联网传感器
- 保护100万+APP
- 覆盖9亿+个人智能终端
- 50+产品软著及专利

OWASP
Open Web Application Security Project

我们的优势

公司优势

- 垂直领域的技术与市场领先者
- 全面的权威资质认证
- 遍布全国的分公司与办事处
- 所有产品均为自助研发，拥有核心代码及知识产权
- 与网信办、工信部、公安、CnCert、计算机病毒防治中心等深入合作

技术优势

- 领先的双重VMP加固核心技术
- 创新的iOS加固技术
- 纯净防护，不侵入源代码
- 全面的Android、iOS、H5和物联网嵌入式系统覆盖
- 高性能、不影响兼容性
- 众多核心技术及软著、专利

人员优势

- 70%的专业技术人员
- 风险评估相关人员超过40人
- 众多CISSP/CISA/CISP/PMP/CISAW等专业安全资质认证

方案优势

- 移动安全前生命周期解决方案
- 物联网解决方案
- 安全态势感知解决方案
- 安全大数据解决方案
- 业务风险治理解决方案
- 围绕国家网络安全法和等保2.0的方案设计思想

OWASP
Open Web Application Security Project

感谢聆听

THANK YOU APPRECIATE

OWASP
Open Web Application
Security Project