

企业网络安全：困境、反思与实践

韦韬

2024.12



序章

雪崩时没有一片雪花是无辜的

俄乌战争开启了后互联网时代人类社会战争的新形态

热战，网络战，舆论战，金融战，贸易战，科技战，六战合一



网络攻击

DDoS攻击 – 大流量阻塞迫停服务



网络定向攻击 – 窃密/勒索/摧毁系统

黑产

- 打击同行，不正当竞争
- 网络敲诈

- 窃取个人信息 → 电信诈骗
- 加密/窃取商业信息 → 网络勒索

日常/
热战前

低烈度攻击

- 乌克兰1月：外交部、教育部、内政部、能源部

间谍行为，政治勒索

- 能源/金融/交通/矿业：BlackEnergy/KillDisk/CrashOverride
- 政府机密：美国政府遭受SolarWinds供应链攻击
- 军事机密：美国国防部和情报部门的众多承包商 (AA22-047A)
- 白俄罗斯铁路遭受Scorching Heat政治勒索攻击

热战

造成政府与民生混乱

- 乌克兰政府机构、武装部队、银行网站遭受重点攻击
- 俄罗斯遭受DDoS攻击同比增长7倍，聚焦在银行等金融机构

窃取军事机密，摧毁关键民生设施，制造社会混乱

- 乌克兰政府与银行遭受HermeticWiper数据擦除恶意软件攻击
- 乌克兰电网遭受Industroyer2攻击
- 通过官方信道散布虚假信息

高度复杂业务使安全保障任务面临巨大挑战

安全保障任务

持续采集网络环境、应用系统及数据资产等状态数据，通过对这些数据进行持续分析与研判，衡量网络与安全系统的安全状态并进行安全处置决策



万级

服务器主机

百万级

业务容器

万级

业务应用

十万级

公网API接口

万级

办公终端

用户登录日志

DNS记录

系统信息记录

电子邮件记录

文件下载记录

进程信息记录

网络访问记录

网络流量记录

不可见，不可控

追溯范围有限

上下文缺失

数据可集成度低

大规模运维难度大

抽样追溯效果差

- 企业安全监控覆盖高风险范围的比例平均只有29%，大量应用因技术栈陈旧、无人维护等原因处于观测盲区
- 大量用于风险研判的运行时上下文缺失，例如哪些调用栈触发了RCE漏洞、执行网络外联命令的代码片段等
- 不同安全产品的观测数据格式和接口标准不统一，安全日志和事件难以关联，限制了跨产品和跨领域的关联分析能力
- 缺乏针对安全产品的“基础设施”，以完成安全产品大规模的变更、监控和稳定性保障等方面的运维工作
- 抽样观测数据无法支撑链路追踪目标，全量观测的数据又因海量大小无法持久存储，当前的采样观测效果很难满足业务需求

难题一：组织内部生产关系复杂，安全在非事件时期各种让路

随着行业数字化推进，系统复杂度呈“爆炸式”激增的态势，云上业务实时弹性扩容加剧了问题，业务、安全、成本、效率难以协调，“晴天难于修屋顶”



帕累托改进：将安全逻辑与应用逻辑解耦

(生产关系复杂性)

VS

全面观测与精准防护：需要将安全逻辑内置

(安全生产力需求)

难题二：业务总在寻求更快发展，安全投入资源往往严重滞后

业务加剧数字生命体复杂性爆炸，大量安全问题有很强的业务属性，但传统安全模型游离在业务之外，教科书、培训课上的安全往往是模型清晰的，但实战中往往是黑产更加理解和善于利用业务的弱点



业务快速发展，过度KPI化导致黑产猖獗

(业务复杂性)

Vs

安全需要对业务进行深入的认知

(认知是防护的前提)

难题三：安全溯源与取证 难度高、效率低

各家往往技术负债长期积累成祖传🏞️山，资产/链路梳理不清。攻击者采用多种手段隐藏身份，使溯源和取证变得复杂，加上数据链路分析缺乏强有力的数据支撑，使得溯源取证难上加难



大规模网络复杂性，技术负债重，攻击面大

(时空复杂性)

VS

发现攻击链，铲除所有隐患

(对抗/治理快速溯源需求)

- 不存在绝对安全 aka 绝对安全的代价本身对于绝大部分场景来说是难以承受的
 - 安全是端到端的，现代系统复杂性往往无法安全穷尽分析
 - 代价不只是金钱，还包括 时间、专业保障团队 等等
- 安全性度量的本质在于需要付出多大的成本、克服多大的不确定性来攻破给定的安全防护保障，造成信息泄露或者系统失控的后果或风险
- 高安全等级系统的三类安全失败因素：
 - 禅宗 认知缺陷：安全模型设计上就不提供保障的安全缺口
 - 剑宗 复杂性漏洞：因为系统复杂性，难于发现，易于利用
 - 气宗 资源型攻击：机制明确拼资源，如算力门限，硬件保护等





● 表象：剑宗，复杂性漏洞失控

因为系统复杂性，未在攻击者之前发现漏洞/阻断攻击



● 内因：气宗，安全资源投入不足

安全工程师/技术工程人数 比例严重失衡
安全缺乏基础设施，难以高效对抗与弹性治理



● 根因：禅宗，安全认知缺失

在技术和管理层面对安全的认知缺失，
导致各类技术负债积累成雪山，
然后由攻击和异常事件触发成雪崩



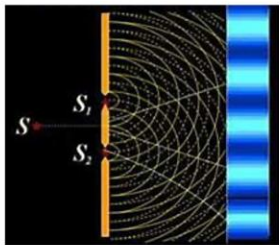
安全体系的反思：雪崩时没有一片雪花是无辜的

- **企业安全和稳定性的真正灾难**：技术和业务历史负债积累成雪山，攻击和异常事件触发雪崩点，形成**难以快速消解的安全或稳定性雪崩后果**
- 没有绝对的安全，但我们也见过太多一个细节疏忽就导致整体安全失败的惨痛案例
- 安全体系设计正是这样，需要在本源层面思考充分，才能关注到、支撑住**关键细节**，从而避免**安全雪崩**



- 专业之所以专业, 因为其**精确性导致的反直觉性**
 - 直觉是基于经验模糊推理的, 但专业上差之毫厘, 谬以千里
- 安全从业者的几个专业性要点:
 - **风险预警**: 对于复杂系统的风险敏锐度, **及时识别并预警雪崩风险**
 - 如: 识别协议、架构、实现层面对业务有严重危害的技术隐患
 - **对抗压制**: 有效消解攻击者的攻击威胁, **避免触发形成“雪崩”**
 - 如: 避免入侵者控制关键系统/获取关键数据/系统稳定性雪崩
 - **根因消解**: 对于高发、高危技术隐患的本质分析, 进而**消除“积雪”**
 - 如: 水平越权等漏洞根因的本质思考, 在技术组织层面共同解决
 - **防御基建**: 对于安全防御体系与基础设施的设计与推进, **改造“雪场”**
 - 将安全能力融入整体技术体系, 逐渐形成防御主场优势
 - **情报协作**: 业界多层面广泛合作联防, 对黑产知己知彼
 - 实战情报互通的前提是人之间的信任和互通

专业之反直觉案例



① 杨氏双缝干涉实验



② 密码过于复杂会破坏安全性

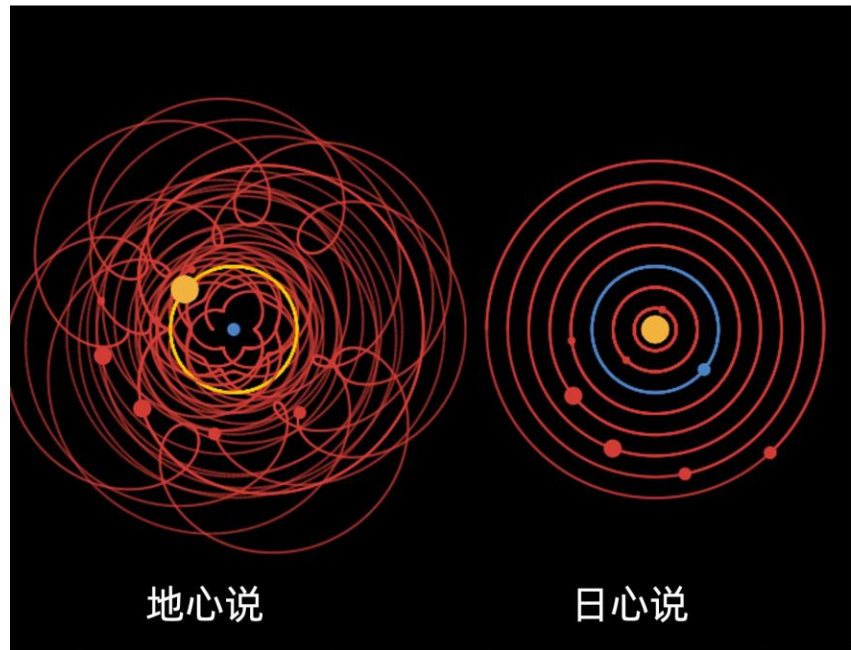
③ 稳定性过度追求会破坏安全性

范式重构

最大的漏洞是认知的缺失



图片来源: Arutthaphon Poolsawasd / Getty Images (如有侵权请联系删除)



图片来源: <http://www.malinc.se/math/trigonometry/geocentrismen.php>
(如有侵权请联系删除)

安全的微观原子问题：访问控制

安全管控的复杂性爆炸



访问控制的原生安全范式 ① OVTP可溯范式（策略层）

Operator-Voucher-Traceable Paradigm



- OVTP可溯范式: 完整研判一个访问是否合法, 应该基于该访问的 操作者链路(O) 和 凭证链路(V)
- 从单机时代走向云原生时代, 从简单权限场景走向复杂业务场景, 从访问凭据走向身份追溯与业务凭证
- 安全防御研判的困难往往在于 OV链路追溯的断档, 很不幸, 这是常态

访问控制的原生安全范式 ② NbSP零越范式 (机制层)

Non-bypassable Security Paradigm



- NbSP零越范式: 应当确保关键安全检查点不被绕过, 所有绕过的行为皆为非法
- 是一个基础技术要求, 是实现机密性、完整性、可追究性的更基础性的要求

- 在复杂网络系统中保障挑战很大, 可以结合系统安全、形式化验证以及密码学技术实现
- 内存安全漏洞、ODD反序列化、SSL POODLE等漏洞的最大威胁本质上就是破坏了NbSP范式

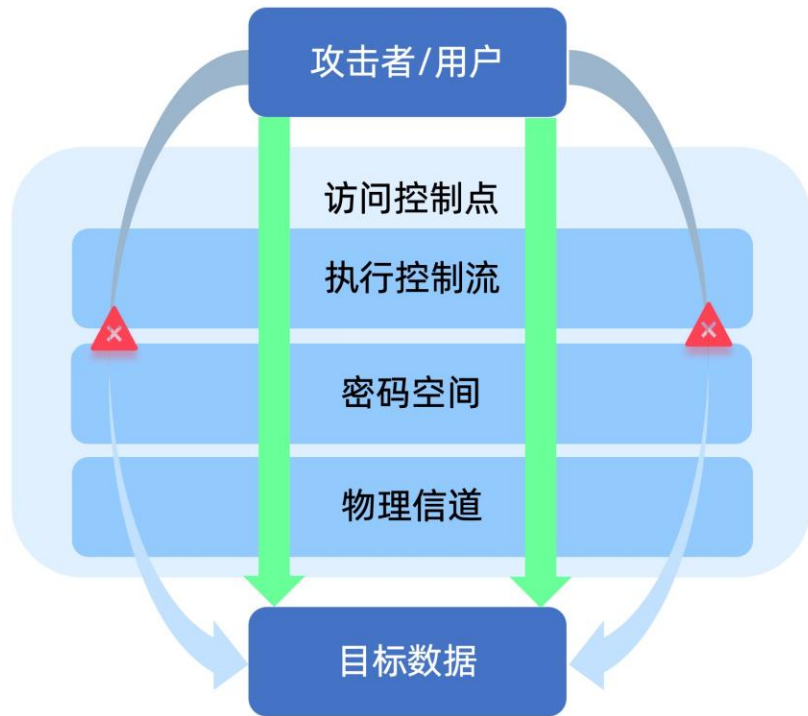
原生安全范式 ③ ARCP攻击回报范式 (价值层)

Attack-Reward-Cost Paradigm



- 相关业务, 即面向合法用户, 也面向攻击者
- 如果攻击者攻击收益超过成本, 那么黑产攻击者将最大化榨干这个业务的价值
- 攻击者成本是全生命周期的成本

- ※ NbSP零越范式以访问控制点为基础提出了四种不同的**攻击类别**:
 - ★ **B3攻击**: 预设的访问控制点被**完全绕过**, 攻击者能够任意读取或篡改敏感数据, **内存安全是一类重要的B3攻击类型**
 - ★ **B2攻击**: 预设的访问控制点被**部分绕过**, 攻击者读取或篡改部分敏感数据, 一般不能绕过日志审计
 - ★ **B1攻击**: 功能**滥用型** (OVTP)
 - ★ **B0攻击**: **拒绝服务/资源耗费攻击** (ARCP)



体系反思

最大的漏洞是认知的缺失

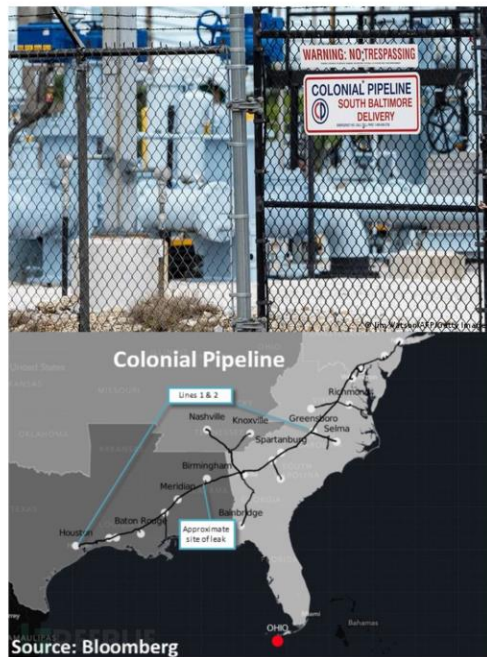
地者，远近，险易，广暇，死生也

- **保护目标：数字资产**
 - 高敏数据，高敏应用，关键基础设施
- **安全假设：**
 - 敌手有我方未知安全漏洞（零日漏洞）
 - 员工会被收买/欺骗诱导（社会工程学）
 - 单点防护在一段时间内总会被突破
- **纵深防御策略：多层防御 交叉补位**
 - 相互独立多层防护降低突破可能
 - 增加网络杀伤链长度，为检测赢得空间，为响应赢得时间



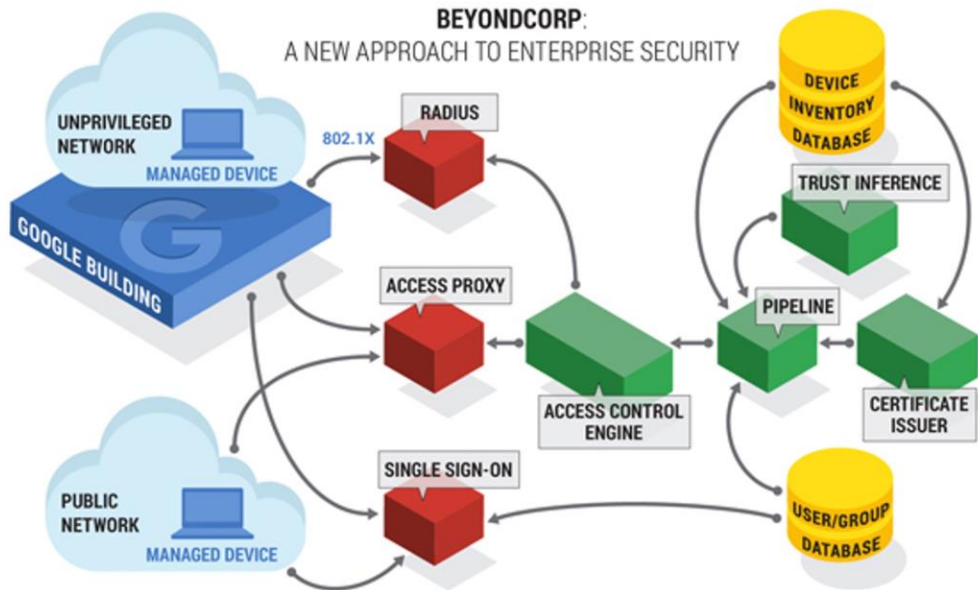
纵深究竟要多深？

- 网络纵深 往往远低于 物理纵深
 - 美国科洛尼尔公司严密的铁丝网隔不住来自欧洲的网络攻击者
- 人与大量敏感信息之间隔多深？
 - 一个服务账号
 - 现实：现有访问控制体系 有权限，没凭证 (-OVTP)
- 供应链与网络渗透之间隔多深？
 - 一个自动版本升级，一个云输入设置，一个短信云同步
 - 现实：现有网络体系大量隐藏访问通道 (-NbSP)
- 有多层，多暴露，没交叉
 - 网络拓扑混乱且动态变化
 - 现实：安全观测数据不全，不准，不及时，难以关联 (-OVTP)

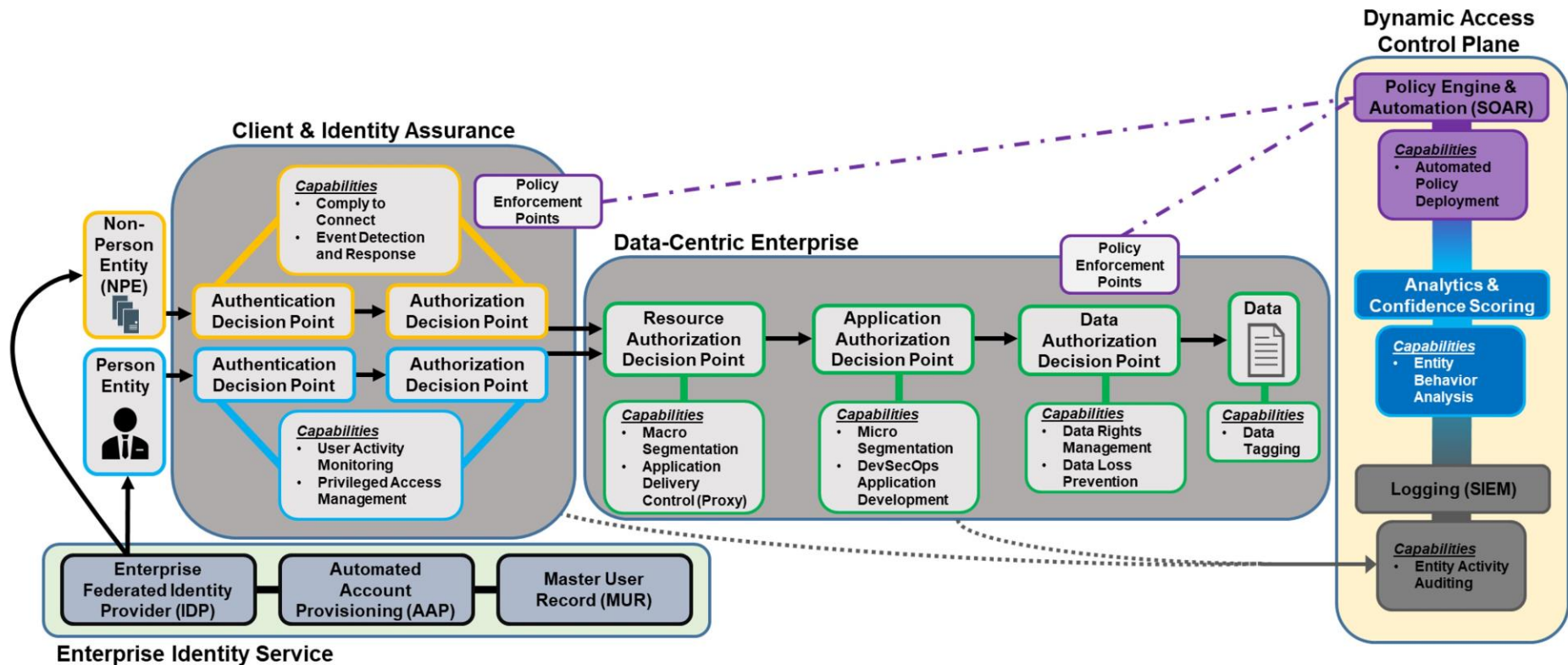


Google BeyondCorp

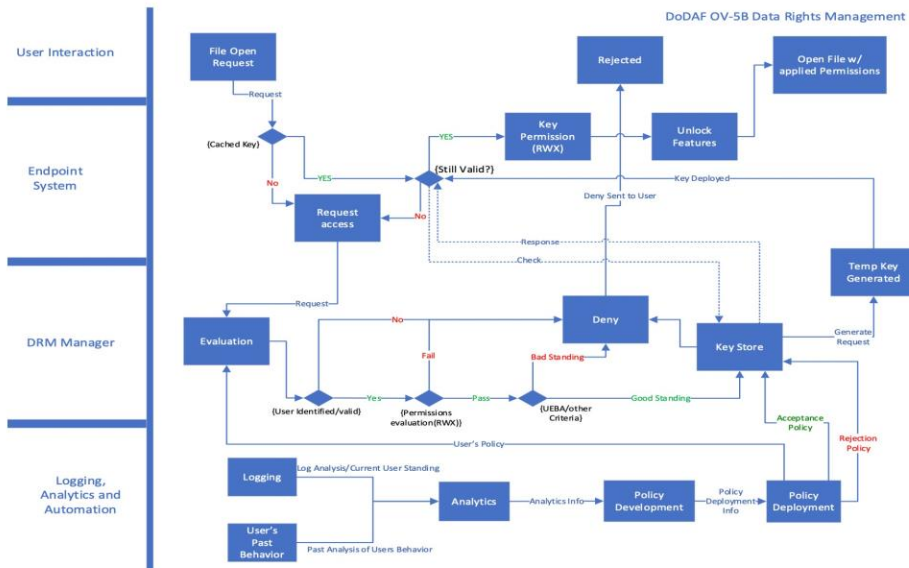
- 零信任是一种用于保护组织的安全模型，它的理念是默认不信任任何人员或设备，即使人员或设备已经位于组织的网络内也是如此。
- 零信任方法在整个网络中（而不仅仅是在可信边界上）强制执行严格的身份验证和授权，以消除隐式信任。在此模型中，每个访问资源的请求都被视为来自不受信任的网络，系统会对其进行检查、身份验证和核实。



BeyondCorp components and access flow

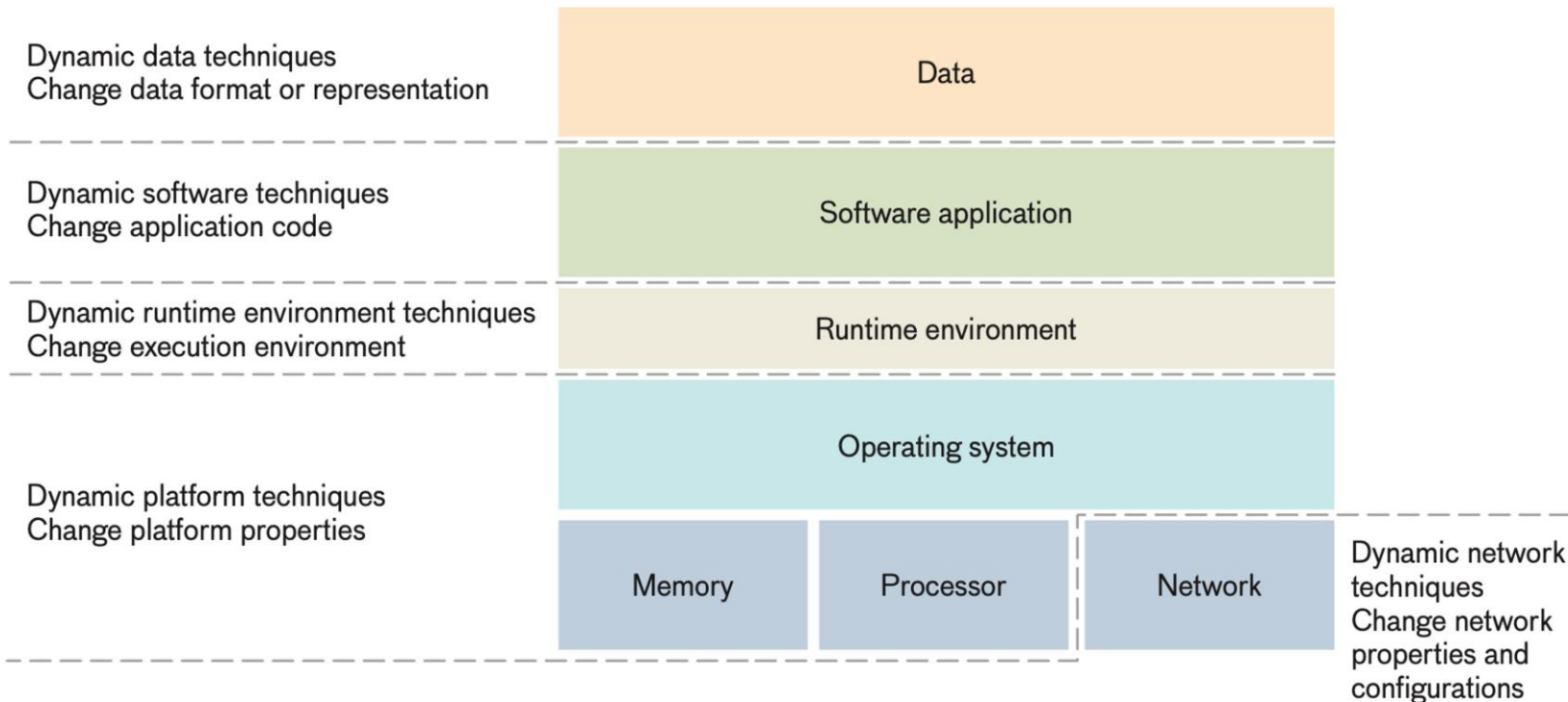


- 其实高安全等级网络中强访问控制不是新要求
- **OVTP的缺失**
 - 用凭据 (Credentials) 代替操作人
 - 业务凭证 (Voucher) 的缺失
 - 访问链路的可追溯性的缺失
- **NbSP的缺失**
 - 访问边界缺乏收敛
- **已有应用系统的改造与兼容**
 - 对于已有系统和IT基础设施系统, 难以直接改造应用



安全体系③ Moving Target Defense

不确定性是攻击者最痛恨的问题之一



From "Moving Target Techniques: Leveraging Uncertainty for Cyber Defense"

By Hamed Okhravi et al

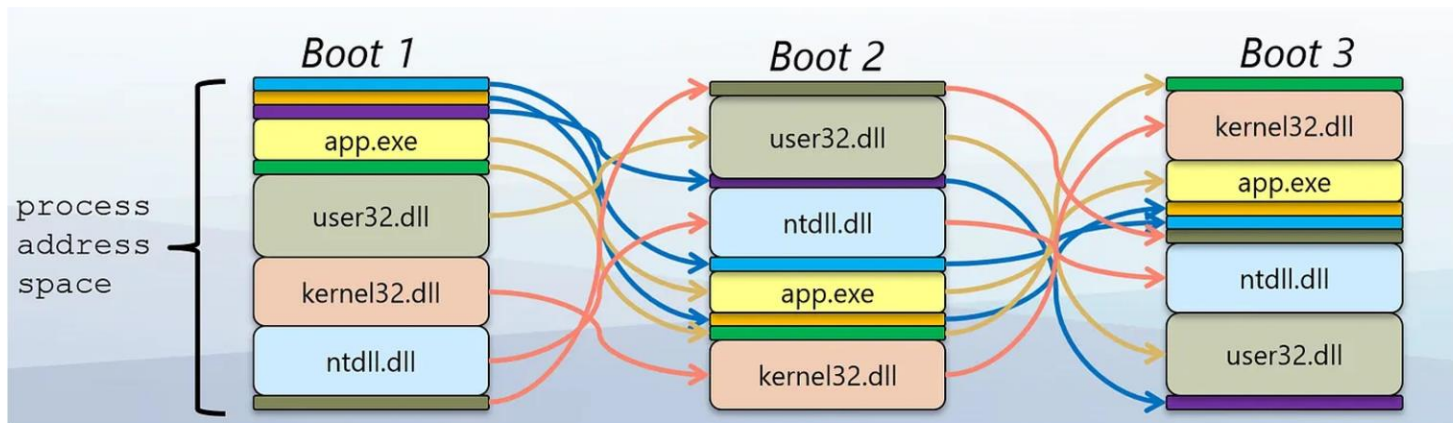
NbSP+, OVTP-

- **NbSP的增强**

- 非定义路径稳定性严重下降
- 攻击需要更多的探测和尝试

- **OVTP的无力**

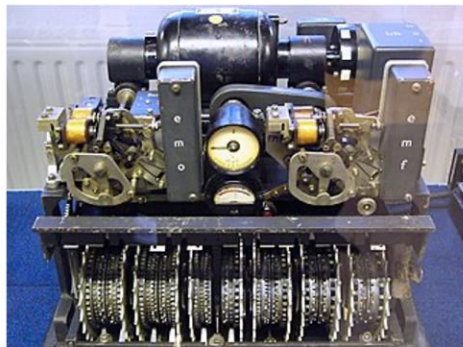
- 发生在定义路径上的攻击难以防范
- 身份假冒, 权限滥用, 逻辑短接



Address Space Layout Randomization (ASLR)

安全体系的重要基石

- 密码学在数字空间的核心作用是提供经过严格证明的安全基
 - 有明确的威胁模型和安全保障模型
 - 可以为数字空间各种业态提供长效的保障能力
- **将主体运维的物理边界扩展到密钥管控的虚拟边界**
 - 应对业态在系统边界动态变化或者跨组织延伸时所遇到的种种安全挑战
 - 提供基于技术信任的跨域管控能力
- 安全攻防角度, 数字化业务因为巨大的普遍性风险对密码学和安全体系需求越来越强, 密码学是纵深防御体系中的重要组成
- 安全治理角度, 数据业务由于合规和隐私需求, 也对密码学产生了庞大的普遍性需求, 隐私计算等新兴需求也迅速增长

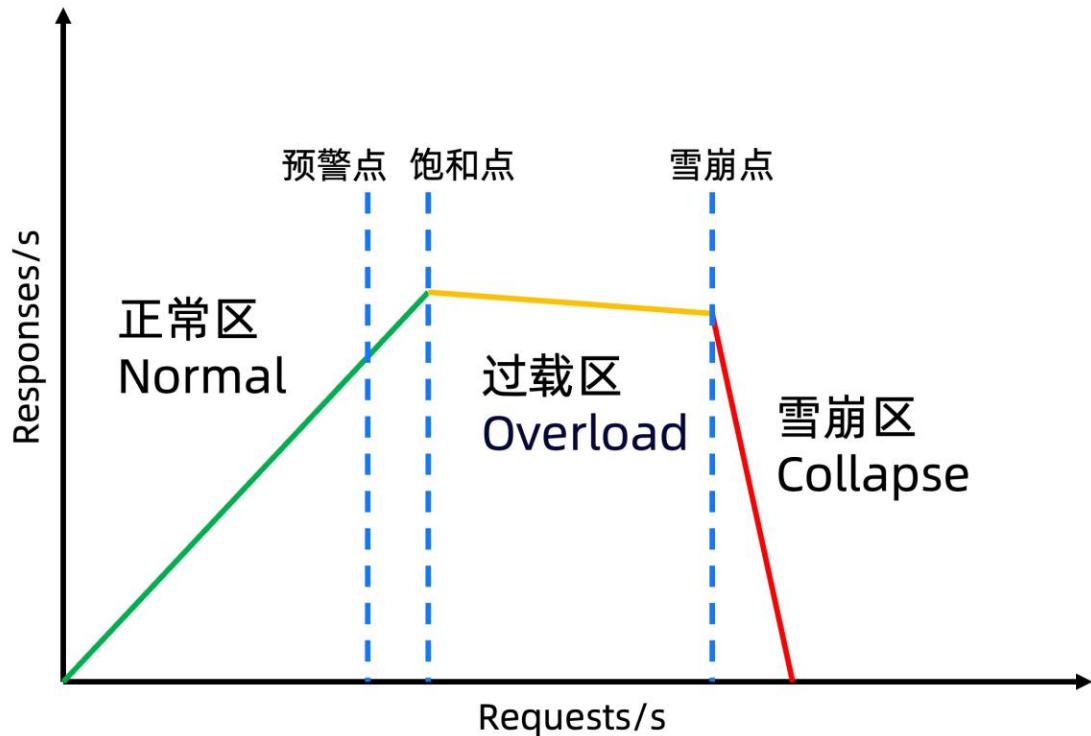


德国的洛伦兹密码机
二战期间用于加密机密邮件

- **访问凭据滥用对应的密钥保障问题 (-OVTP)**
 - 这个往往会形成递归循环问题, 已经成为云服务最严重的安全风险之一, 需要**硬件可信根**或者软件安全对抗体系来提供保障 → **可信计算普及需要加速**
- **效率导致的威胁模型妥协问题 (-NbSP)**
 - 虽然密码学在单项应用领域的性能不断突破, 但在综合场景下的性能依然无法独立承载大规模工业级数据处理的需求 (**半诚实模型, 该不该相信?**)
- **密码协议正确构建和应用的问题**
 - 密码学是非常专业的领域, 安全性依赖于严格的前置条件, 这个对于普通程序员来说依然是很难做到全面保证的

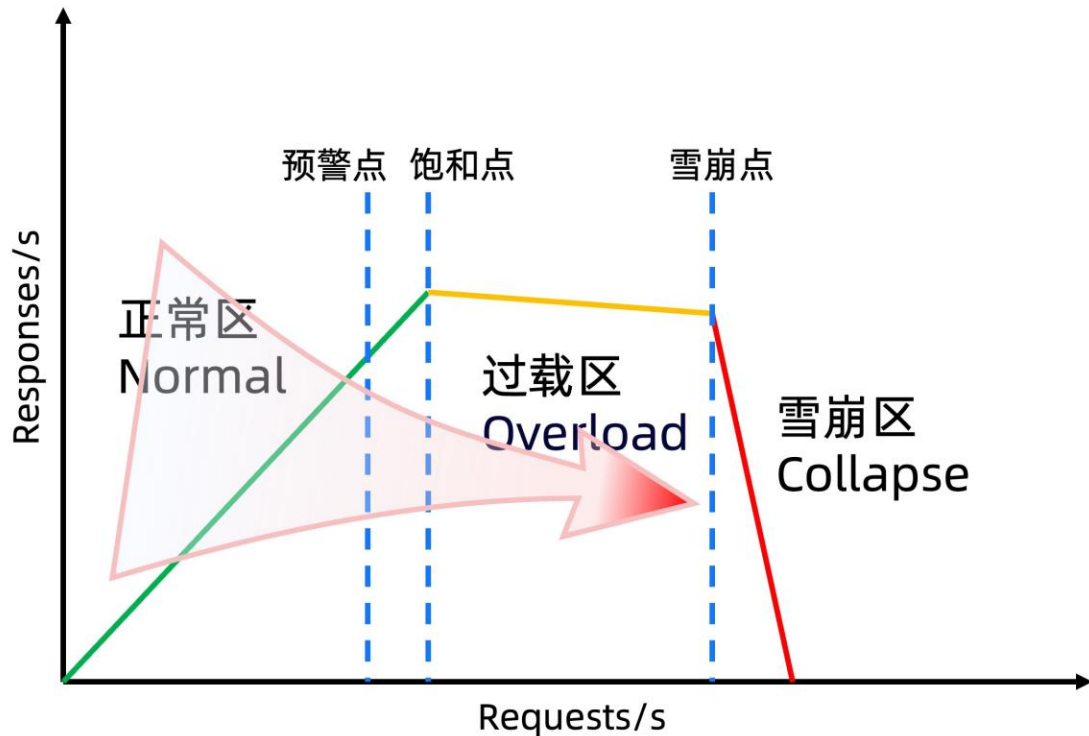


⑤ CC流量攻击与稳定性：网络应用流量响应N-O-C曲线



- 过载区:
 - 服务质量有下降
 - 一般随着负载下降能快速自愈
- 雪崩区:
 - 服务质量严重受损, 业务代价急剧上升
 - 难以快速自愈
- 底线: 避免雪崩
 - 手动调节: 及时干预
 - 自动调节: 流控反压
- 雪崩与级联雪崩:
 - ① 业务不知雪崩点, 无自适应流控能力
 - ② 被网关等上游节点压挂
 - ③ 级联雪崩, 导致其他相关服务停滞

⑤ CC流量攻击与稳定性：ARCP攻击回报范式



- 流量攻击机制
 - ① 占据正常服务流量, 降低服务质量
 - ② 打到服务过载甚至雪崩
- 防御机制
 - 避免雪崩 (手动, 自动)
 - 识别正常用户 vs 攻击者
 - 强: Token校验
 - 弱: 攻击模式识别
 - 处罚攻击者相关资源
 - 强: 设备, 账号
 - 弱: 高频IP封禁
 - 伤: 国际IP封禁

安全平行切面

承载范式重构的下一代安全基础设施

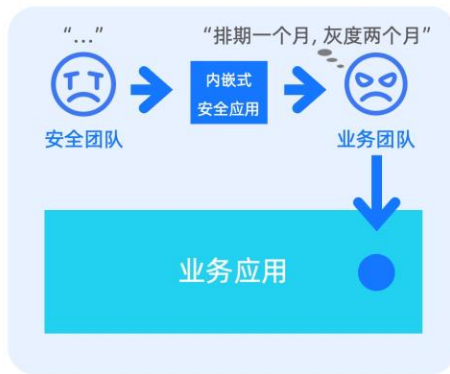
安全平行切面体系（国际首创）实现了动态部署到目标系统执行空间内部的安全可信的管控能力，从而能够对系统内部数据流与控制流进行自主观测与精准管控，从而推动安全智能和管控效能的跨越式提升

外挂式安全体系：
“可见”不足



- 看不清，堵不住
- 安全管控效果差

内嵌安全体系：
“可控”欠缺

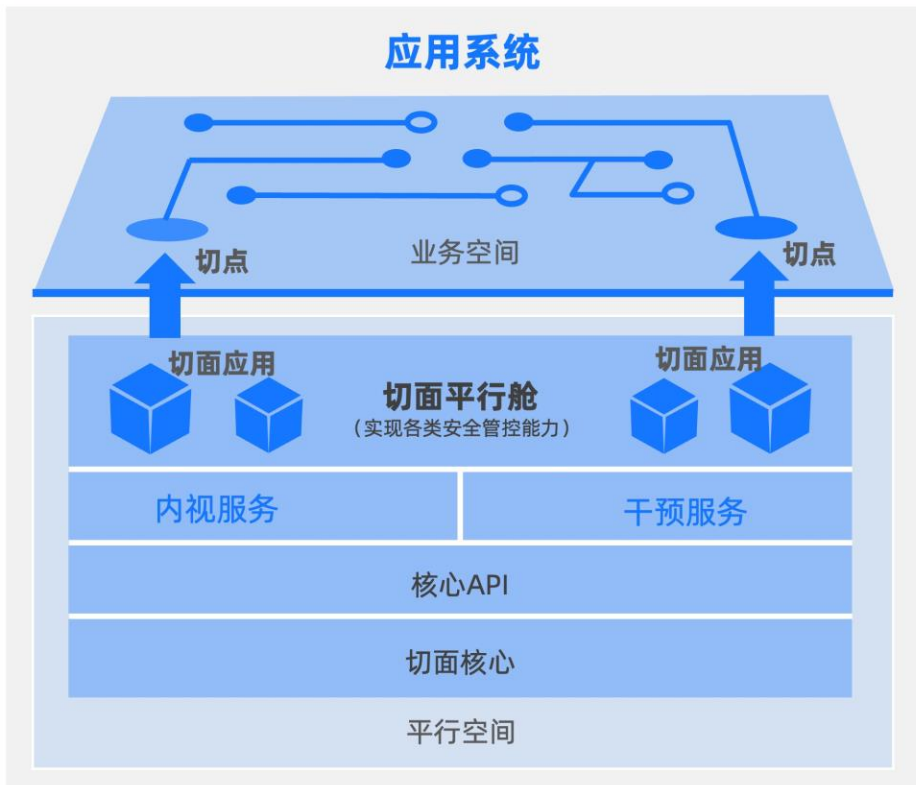


- 业务团队研发排期不吻合
- 安全治理不响应，安全应急跟不上

安全平行切面体系：
“可见可控，可治可战”



- 安全实现对业务内部的自主观测能力
- 安全获得自己的阵地，与业务独立演进



安全平行切面体系实现了动态部署到目标系统执行空间内部的安全可信的管控能力, 从而能够对系统内部数据流与控制流进行自主观测与精准管控

切面应用

通过注入等技术, 在不修改源代码的情况下在切点处修改或添加的动态逻辑组合

切点

原应用逻辑中的某一代码位置。切面应用可以注入一个或一组切点以进行观测或干预

切面平行舱 (类似云原生Sidecar)

平行舱是在切面空间内, 切面应用的执行环境单元, 是切面应用调度和管控的基本颗粒度

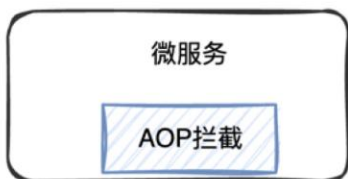
- 可信度量、隔离
- 调度、编排、管控

不同切点的植入方式

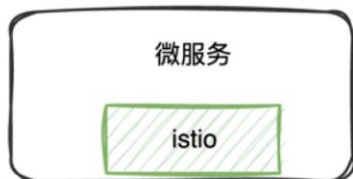
SDK 接入



动态代理



service mesh



字节码切面



采集方式	SDK 接入	动态代理	Service Mesh	字节码切面
优点	技术通俗易懂	借助Spring原生AOP能力，性能比较好 解耦性和插拔性比较好	完全解耦，对业务代码&容器无任何侵入影响	与业务代码完全解耦 无感接入 任意可序列化数据的采集
缺点	代码侵入性强，开发维护成本高	存在兼容性问题、内部方法采集受限	只能采集入口流量，不支持子调用数据采集 需要对流经mesh层的流量进行筛选采集，容易造成服务耗时过高。	对业务容器性能存在些许影响

切面应用



安全能力可编程

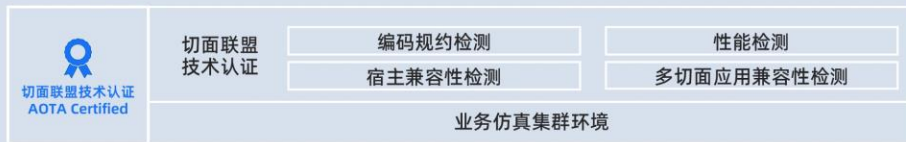
🔍 切面观测应用

⚡ 切面防护应用

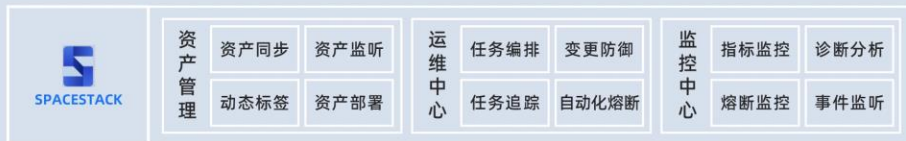
📄 切面治理应用

三重保障加速创新落地

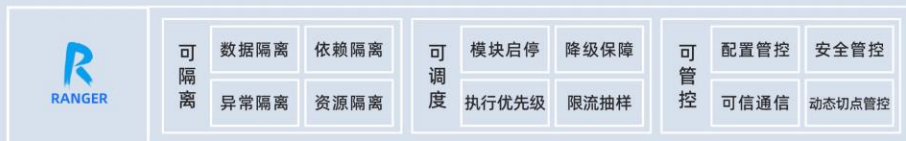
出厂前：仿真环境与兼容性认证，提供出厂质量保障



变更中：统一PaaS管控，提供遵循OCMS规范的三板斧流程保障



运行时：高可用注入框架，提供稳定可靠的运行时保障



三道防线构筑可靠安全基座

定制开发

- 通过切面提供的安全可编程能力，可低成本定制实现多种不同类型的安全能力，**大大降低**企业在定制化开发、新产品开发、已有产品维护等方面的开发成本。

质量保障

- 提供统一质量测试环境，确保产品性能、兼容性、运行可靠性等经过充足验证。**大大节约**企业在稳定性保障方面的人力投入和测试资源投入。

规模化实施保障

- 通过平台对创新技术提供治理能力，避免走入边开发边治理的老路，降低数字基座后续的治理改造成本。

运行保障

- 为已运行的安全能力提供隔离、调度、管控等安全保障机制，降低产品对数字业务连续性的稳定性影响，提升客户使用信心。

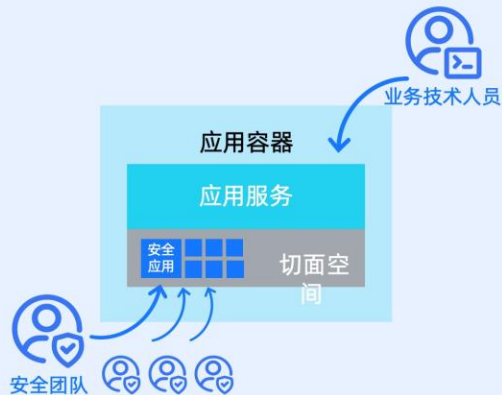
蚂蚁内部覆盖超过95%的应用服务, 核心业务100%覆盖, 整套体系足够稳定, 运行至今0故障

1. 切面底座部署

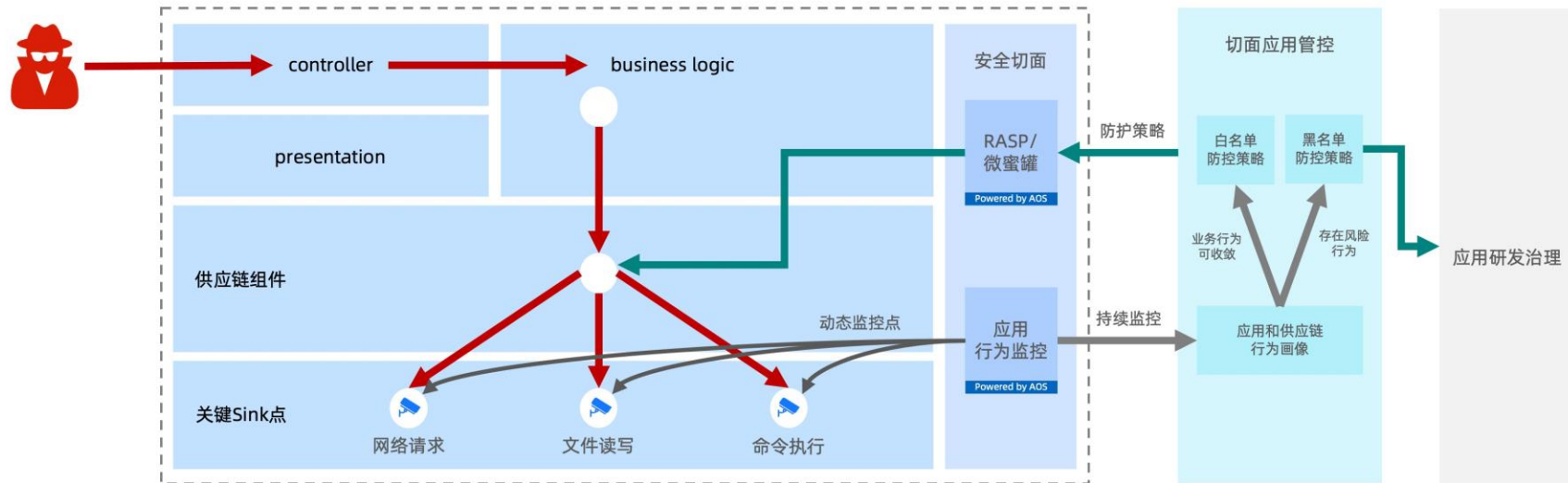


- 无需修改业务代码, 即可快速部署
- 应用一次接入, 持续受益

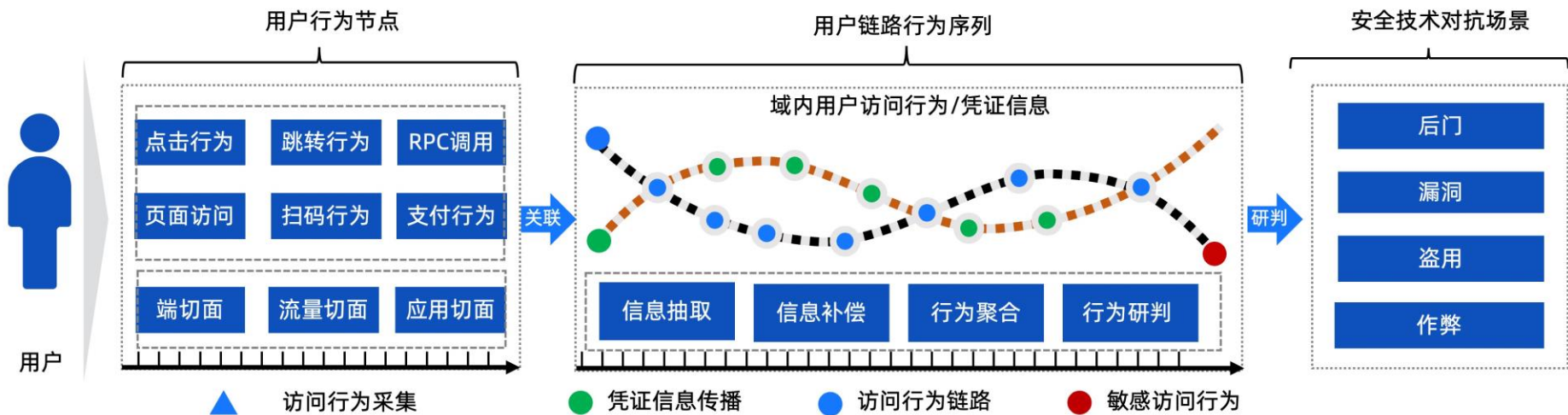
2. 安全自主运营



- 切面应用能力可持续拓展, 动态升级
- 安全与业务平行演进, 效率跨越式提升

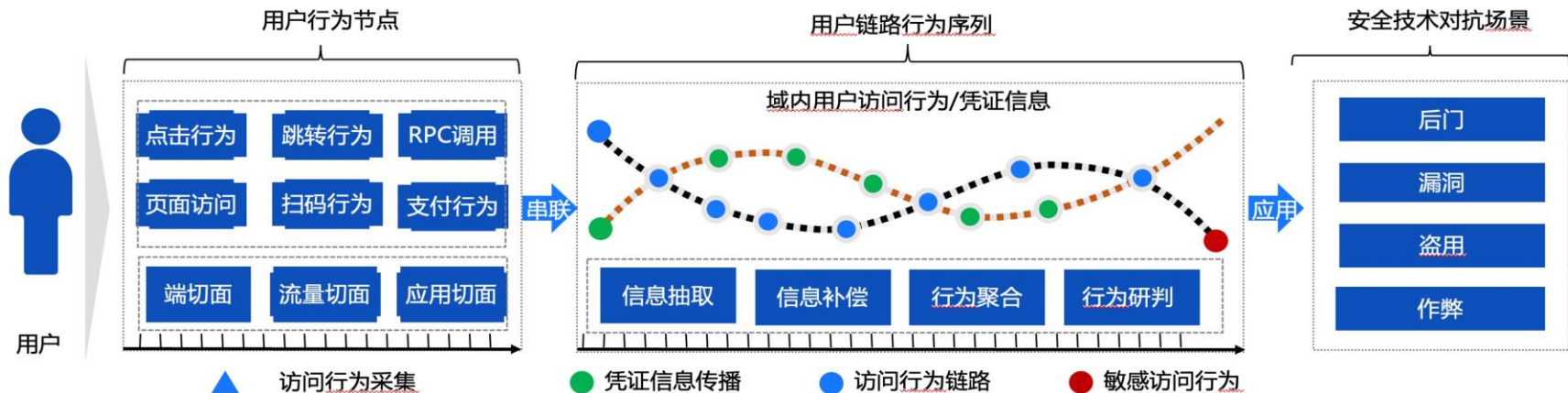


- 基于安全平行切面，对动态对关键sink点进行持续监测，细粒度刻画应用和供应链行为画像，防止非法绕过
- 相比对比传统的网络、系统层面的监测或静态扫描，通过切面实现的动态监测识别颗粒度更细，结果更为精准
- 能够高效阻断1day攻击



「链路行为节点串联实现业务场景全息判断」

- 针对敏感业务行为可通过“业务操作凭证链”的方式进行风险刻化、识别、和拦截管控：
 - 依托安全平行切面技术, 以无业务侵入的方式实现了业务全域流量统一智能管控, 统一采集生成多维实时用户行为序列, 通过数据服务化和行为序列校验引擎, 拓展了安全策略的校验的能力, 极大提升了供应链风险管控策略准确性、时效性和防控效果
 - 实际挖掘识别和阻断端上供应链SDK的滥用后门 (0day), 并发现攻击者的攻击尝试 (-1day), 提升防御性威慑



「链路行为节点串联实现业务场景全息判断」

- Data** **专业数据供给**: 数据决定AI能力的上限。安全平行切面实现信息采集解耦，提供“数据观测自由”
- Knowledge** **专业知识工程**: 大模型精调内化+专业SOP知识编程，利用大模型对多维实时行为序列抽取，构建主客凭据关联以及行为依赖生成行为知识图谱，结合ATT&CK技战术领域知识库，提供分析依据
- Collaboration** **人机高效协同**: 基于用户行为链构建行为序列校验引擎，实现了研判检测智能体调用链，融合专家智能和机器智能；安全平行切面提供精准干预能力
- Feedback** **残差迭代**: 专家分析失效案例，监督精调预防降级，反馈与弥补各层次（策略、知识、能力等）不足，解决误报多，未知威胁发现能力弱，可解释性差的痛点

风险告警场景

异常流量

异常进程

钓鱼事件

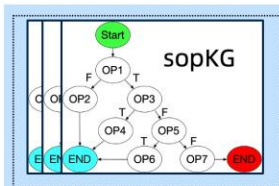
网络扫描

命令执行

异常账户

漏洞

...



有 SOP

无 SOP

获取网安领域知识 ✓

依据sopKG分步骤拆解COT

推理自解构 ✓

以风险实体为中心，
通过entityR-KG
拓展风险调查半径，
分步骤拆解COT

SOC智能体

知识构建

任务规划

线索调查

线索编排

运营研判

推理验证

智能专业工具

监控快照类

探查取证类

知识检索类

情报查询类

基线类

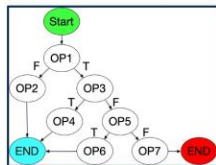
...

残差识别，提供专业能力

DKCF反入侵实践效果

知识构建覆盖数百类风险
日均告警辅助运营数千条
自解构并正确推理比例超97%
检测研判从几十分钟降至十分钟级

结合推演图验证



1. 验证当前操作，以及操作结果合理性
2. 验证推理路径合理性 Start → OP1 → OP3

IOC + 按场景细分 线索调查工具KG

IOC 实体



决策白盒化，推理核检 ✓

平行切面已在运营商、金融、政务等行业的多家单位部署数万台办公终端、超百万台容器、数亿台移动终端，日均观测量级上千亿次，通过平行切面将漏洞的处置的投入人力从数千人天降低至几十人天、将处置时效从以月为单位缩短至天为单位，实现安全入侵零事件、安全生产零事故，有效应对日益庞大的信息系统所面临的复杂、隐蔽的安全威胁。

- 切面观测模块运行情况：部署100W+容器，生产环境稳定运行330+注入点，日均观测量级70亿次。
- 拦截40万+次log4j2攻击，小时级完成全站精准止血，0误拦，0漏拦，应急人力从6000人日降低到30人日（提效200倍）vs 微软最新SFI安全目标：应急止血提效50%
- 双12大促封网不受影响，平行止血加固，业务0干扰化解危机
- 双11、双12流量洪峰值不降级，安全策略检测2.2亿次/分钟
- 在运维、测试等关键应用场景下，均有约10倍效能提升表现

数据来源：参考蚂蚁内部实验结果统计

漏洞挖掘

遗漏率	检出量
60%	8倍
下降	提升

实时防御

攻击防护	漏洞探测防护	高风险攻击
70%+	90%+	60+类
拦截率	拦截率	防御策略

资产画像

接口画像	凭据治理
70%	50%
准确率提升	完整性提升

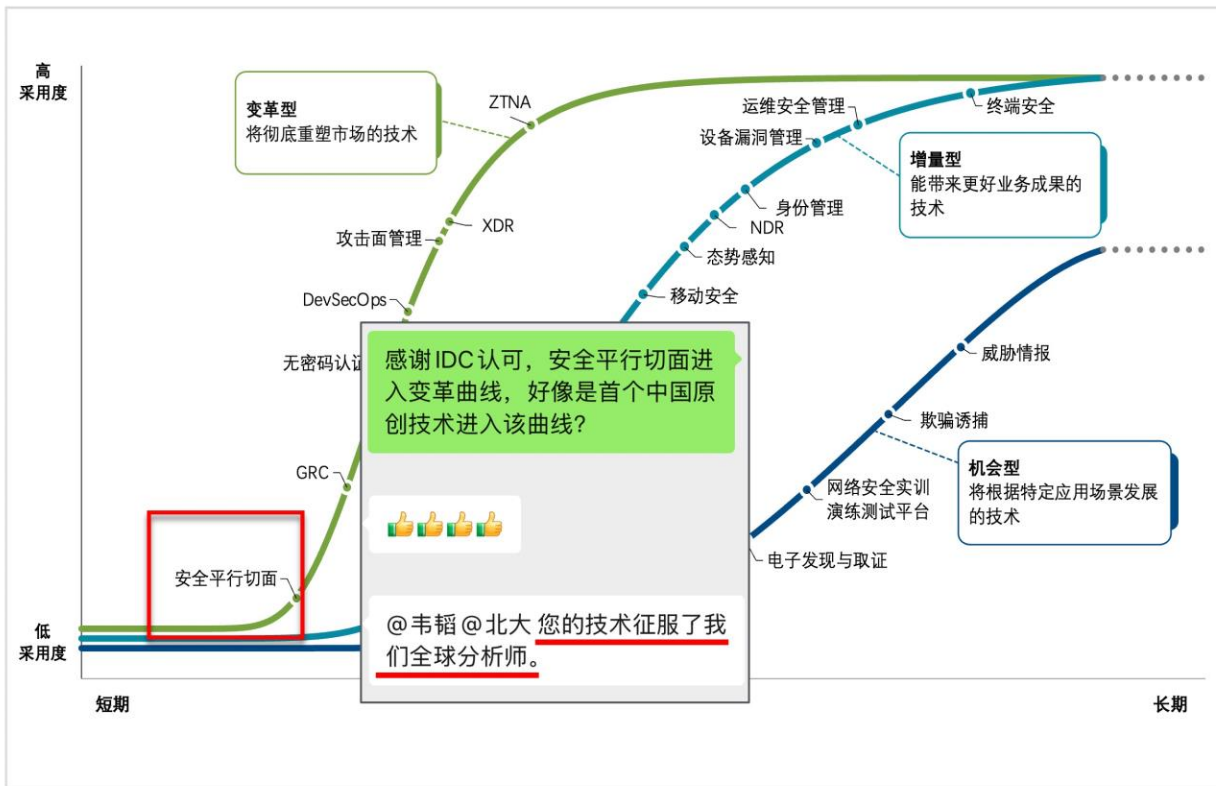
隐私保护

应用服务	高敏接口	隐私信息
27类	100%	100%
隐私风险防护	鉴权防护	流出识别

“安全平行切面是由中国人研发、为数不多的能够在国际舞台上正面竞争的网络安全理念和方法论，它或将引发网络安全行业的一场重大变革。”

谭晓生，著名安全专家，中国计算机学会(CCF)理事、副秘书长

安全平行切面技术进入IDC变革曲线，获得国际认可



对安全治理、攻防对抗、稳定性保障、数据治理等工作效能产生广谱性、跨越式提升，大部分提升10倍以上，获评：

- 2023年中国网络安全十大创新方向
- 2023（第三届）超级CSO特别创新奖
- 2024年《IDC TechScape: 中国网络安全软件技术发展路线图》变革曲线，是首个进入该曲线的中国原创安全技术

构建安全平行切面联盟，获得行业广泛高度评价

2023年成立AOTA平行切面联盟，31家企业共同参与协同推进企业安全建设的变革和可持续发展。

通过与多家成员单位合作，进行产、学、研、用深度融合，助力安全平行切面相关的技术研究、标准制定、行业应用及产品研发。

31家 成员单位

10场 重磅会议

200+人次社区活动

40项 特性更新

10+ 行业汇报

5项 行业殊荣



金融

招商银行、平安银行、网商银行等金融机构应用安全平行切面技术，部署攻防对抗产品RASP和数据安全组件，应对HW阶段及外部真实的高级威胁攻击，同时应用切面数据安全组件进行银行关键数据的监管上报和观测

政务

某国资委客户去年HW阶段被攻击队利用Oday漏洞打穿且溯源无果，造成HW失分。通过在其公网环境部署切面框架，在政务民生业务不中断的情况下，成功对三方企业开发的软件进行零改造加固，帮助用户成功拦截真实内存攻击并通过攻击溯源拿到防护分数，相比于上一次HW取得巨大提升。

运营商

浙江移动在集团内率先完成营业终端、业务中台核心数据库、B域服务器操作系统的100%信创替代，同时有大量营业厅及业务系统后端服务完成信创接入和适配改造。面向企业面临的信创软件安全共性问题，客户决策基于安全平行切面技术打造面向信创环境的原生应用安全态势管理平台。

企业安全实践



战争模式：（对外）威胁对抗



交管模式：（对内）安全治理

安全对抗：安全线主战，完整的网络安全攻防对抗组织体系

纵深防御, 威胁情报, 威胁感知, 对抗归因, 态势研判, 威慑反制



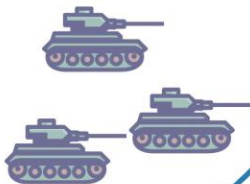
威慑反制

技术压制
司法打击



态势研判

雪崩预判
跨域消解



基础设施安全
原生安全



应用安全

SDL
供应链



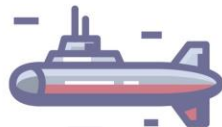
威胁感知 对抗归因

MTTD快速检测
MTTC柔性止血



威胁情报

黑产画像
暗网溯源



各级攻击者

国家力量



竞对/商业APT组织



黑灰产/资深黑客/内鬼



白帽子/初级黑客



非针对性攻击
机器人/全网扫描

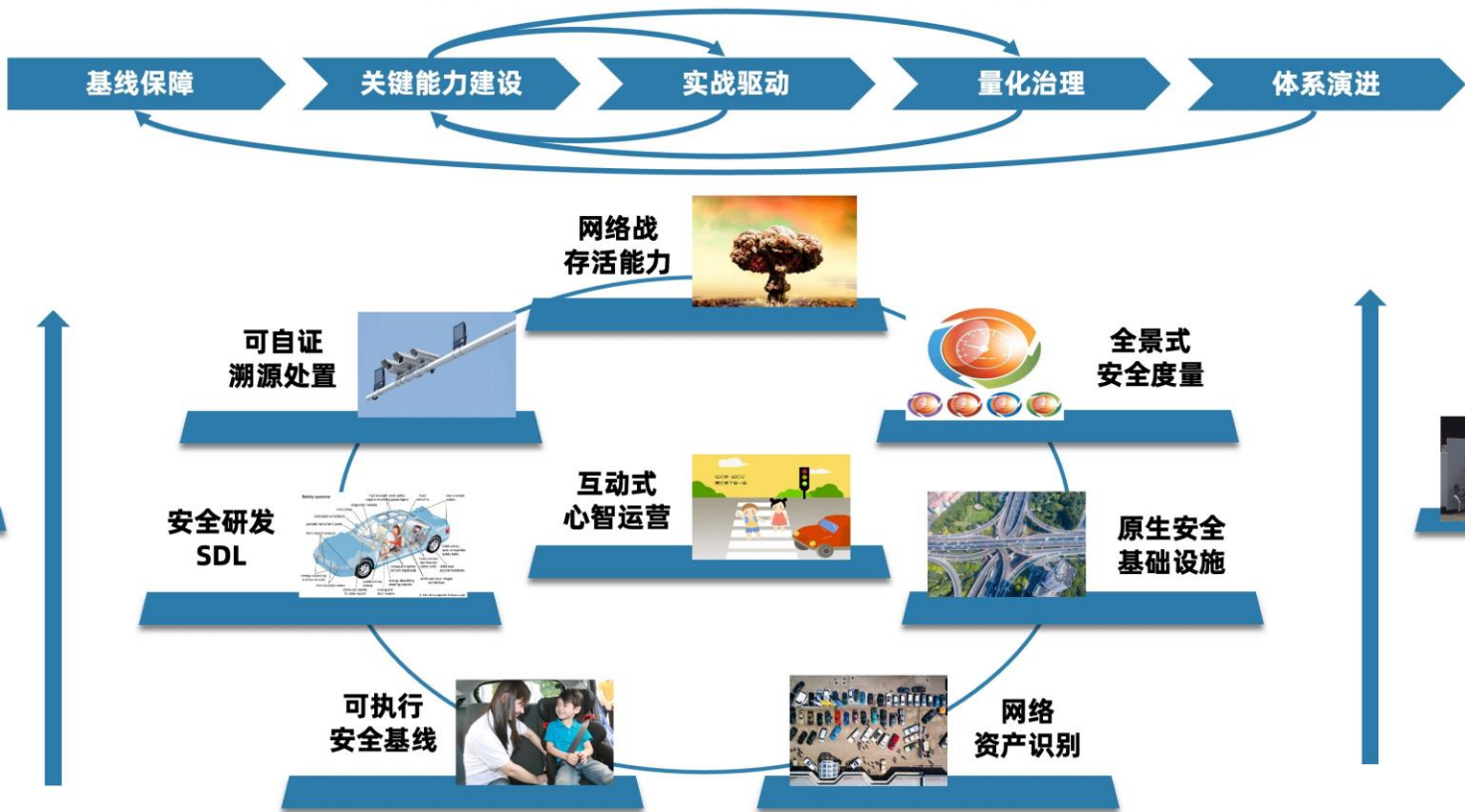
纵深防御
阵地基建

端安全

反注入
实人核身

安全治理：业务线自治，网络安全复合治理成熟度模型

战略要位，实战驱动，范式重构，技术破局





交通事故频发是导致堵车的重要原因



交通安全是行车通畅的前提

- 在数字化经济时代，安全不是业务发展的“阻碍”
 - 如果是，那么安全的认知和实际层面还没有跟上时代的发展
- 安全不仅仅是“成本”，而是“投资”，更加是未来国际竞争的核心竞争力
- 美国国家政策层面已经开始重视“内存安全”这样的核心安全技术问题

修道而保法，故能为胜败之政



安全第一责任人：

业务负责人（驾驶员）

三道防线体系：

业务（决策）

安全法务合规（吹哨，能力支持）

内审



安全制度体系

一级：总体方针

二级：分域规定

三级：实施指南

四级：过程文档



违规处罚

违法：上报司法

一类：开除

二类：绩效

三类：警告

四类：通晒+柔性计分

全员参与：每个人都是安全的潜在突破口

令素行者，与众相得也

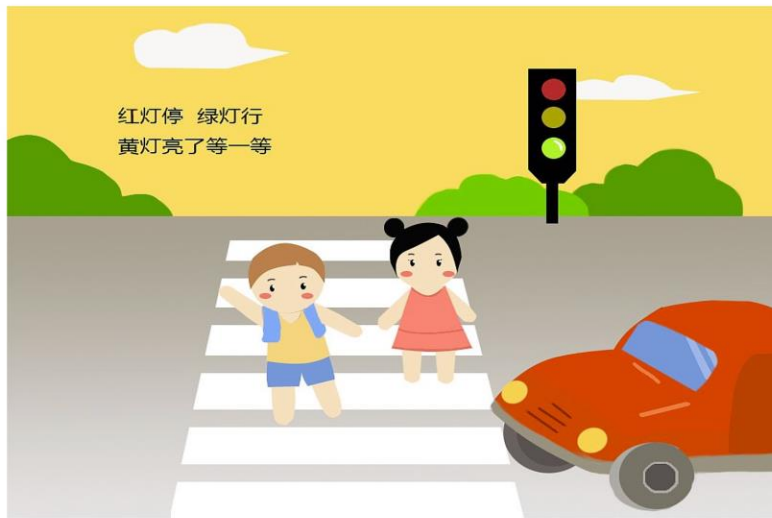


系好安全带

可执行的安全基线

安全教育与心智宣传

遵守交规



全员参与：可执行的安全基线 与 头部风险治理

令之以文，齐之以武

	安全基线	安全制度规范
管控范围	当前重点风险	全面风险
易理解	内容明确，目的性强，便于理解	内容全面，相对冗长繁琐
可执行	能度量，已验证，可落地	通用描述
灵活性	安全部门根据发展阶段统筹推动，持续运营	受制于组织流程，发布周期长，相对固定

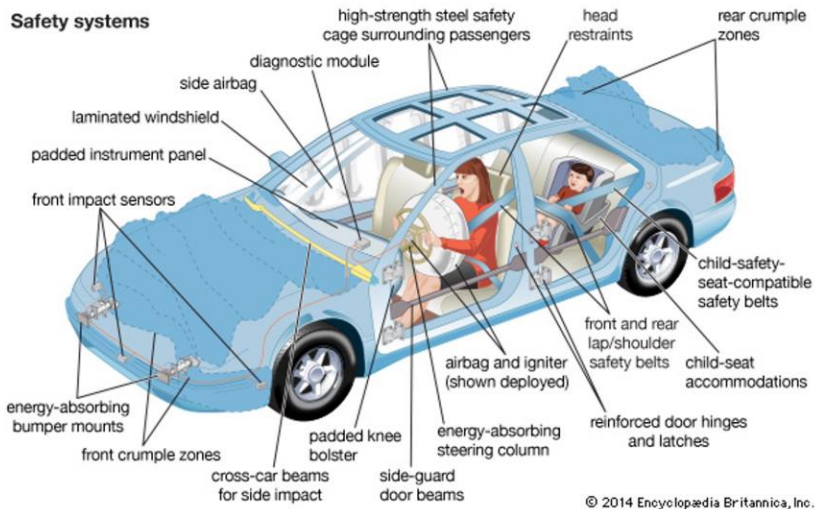
《个人信息保护法》颁布后的数据安全治理基线要则：

主体资产明归属
业务场景单授权
模型分析匿名化
审计举证可溯源



技术破局：从量变到质变

马车装上引擎也不能以百公里时速安全飞驰



汽车安全架构

安全研发生命周期 (SDL)

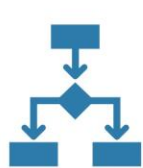
安全基础设施建设

交通基础设施



技术破局：安全研发生命周期 (SDL)

制造安全的汽车（应用系统）



设计与架构安全

基本要求: 新4A

(认证、授权、

密钥管控、

日志审计)



编码规范与 安全组件

业务代码遵从安全规范

关键组件专业团队提供

安全协议必须专家评估



代码安全漏洞分析

变更卡点

静态安全分析

动态模糊安全测试

交互式安全测试

(重专家投入)



安全交付

环境基线

暴露面控制

权限配置

日志保障

(缺省安全)



巡检保障

系统资产透视

漏洞态势监控

高危快速止血

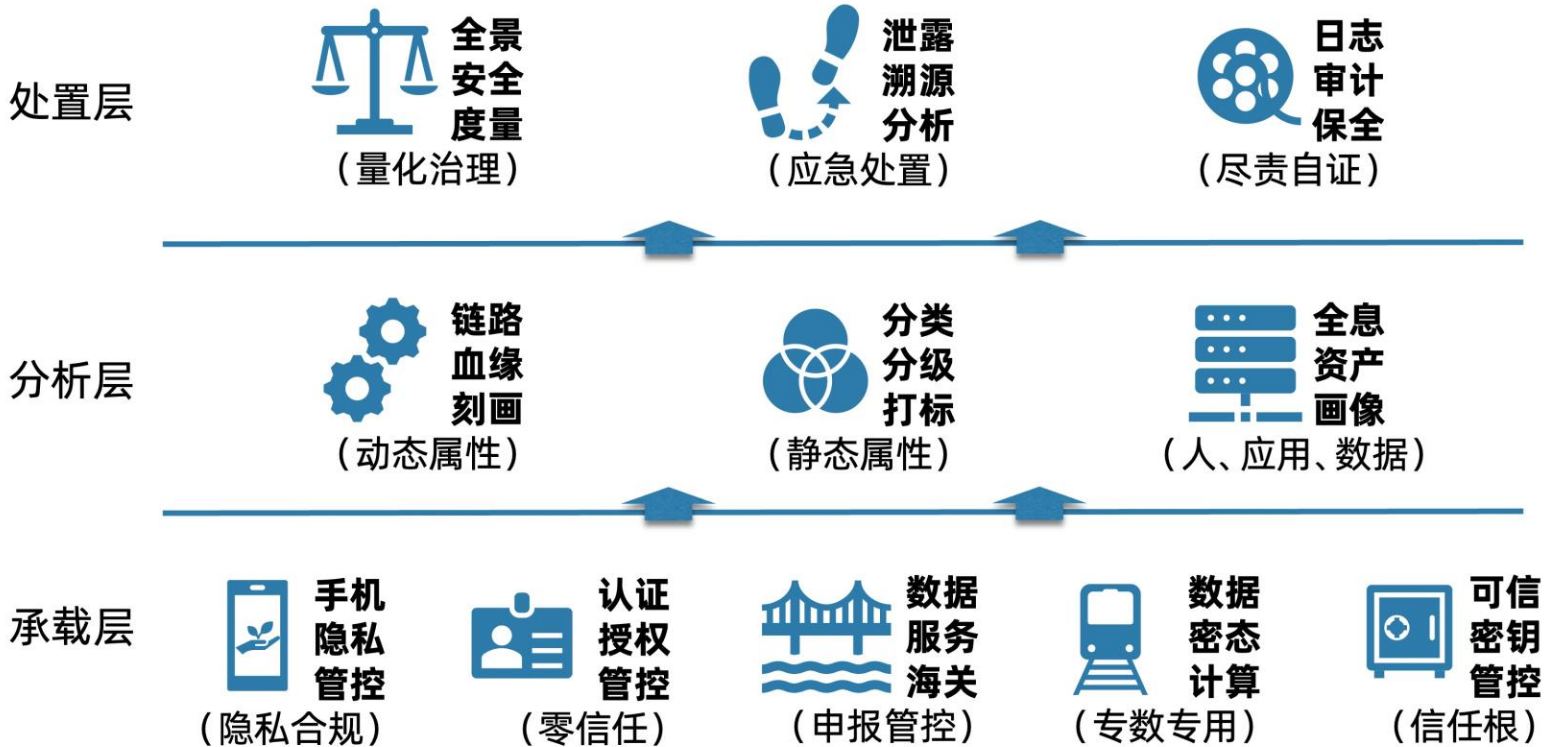
漏洞修复治理

(重治理压力)

- 现有的技术能力（国际范围），**无法确保大规模复杂系统中绝对不出现安全漏洞**
- 但通过正确的安全研发保障，可以大幅度降低漏洞（特别是高危漏洞）的出现，**使其引起的风险可以被纵深防御体系所容纳承受**

技术破局：安全治理基础设施

应用为车，数据链为路



需要系统、
算法、数据
等多维度综
合技术突破

蚂蚁软件供应链安全防护框架

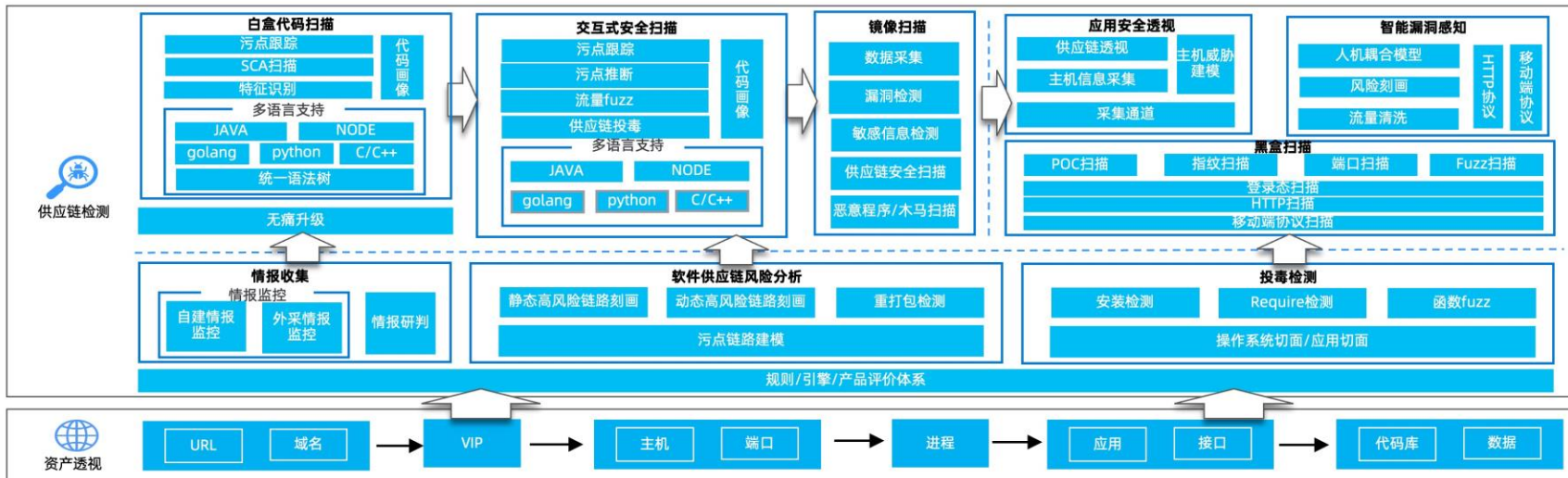
3.0 持续可信

2.0 从容应对



1.0 十万火急





- 多维度交叉核查, 供应链依赖, 影响面排查
- 供应链本身风险的检测和发现, 发现google、apache等多个基础组件的安全0day, 以及20000+开源软件后门, 已上报相关部门和相应社区

实战驱动：红蓝演练与安全运维验证，及时识别与化解**头部风险**

把不可预期的安全风险 变成 可重复检测的测评风险



真实车祸：损失惨痛



汽车碰撞测试：可控可度量

实战驱动：红蓝演练与安全运维验证，及时识别与化解**头部风险**

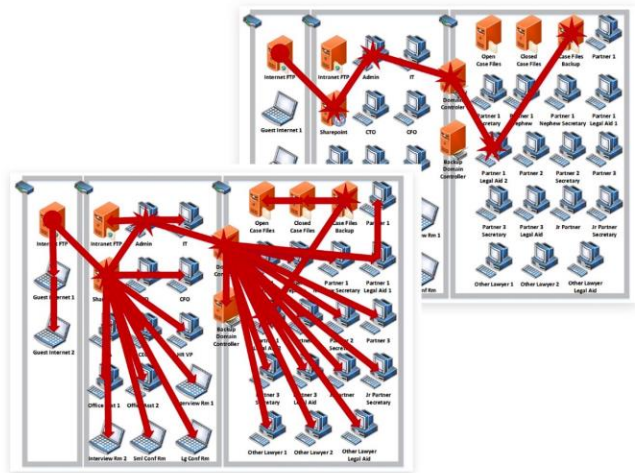
把不可预期的安全风险 变成 可重复检测的测评风险

红蓝演练与安全运维验证：

- 需要有阶段性目标，帮助防守侧渐进提升
- 检验重点防区与发现防守盲区相结合
- 检验防守提升效果（自动验证组件）
- 与威胁情报合作及时跟进业界攻击趋势

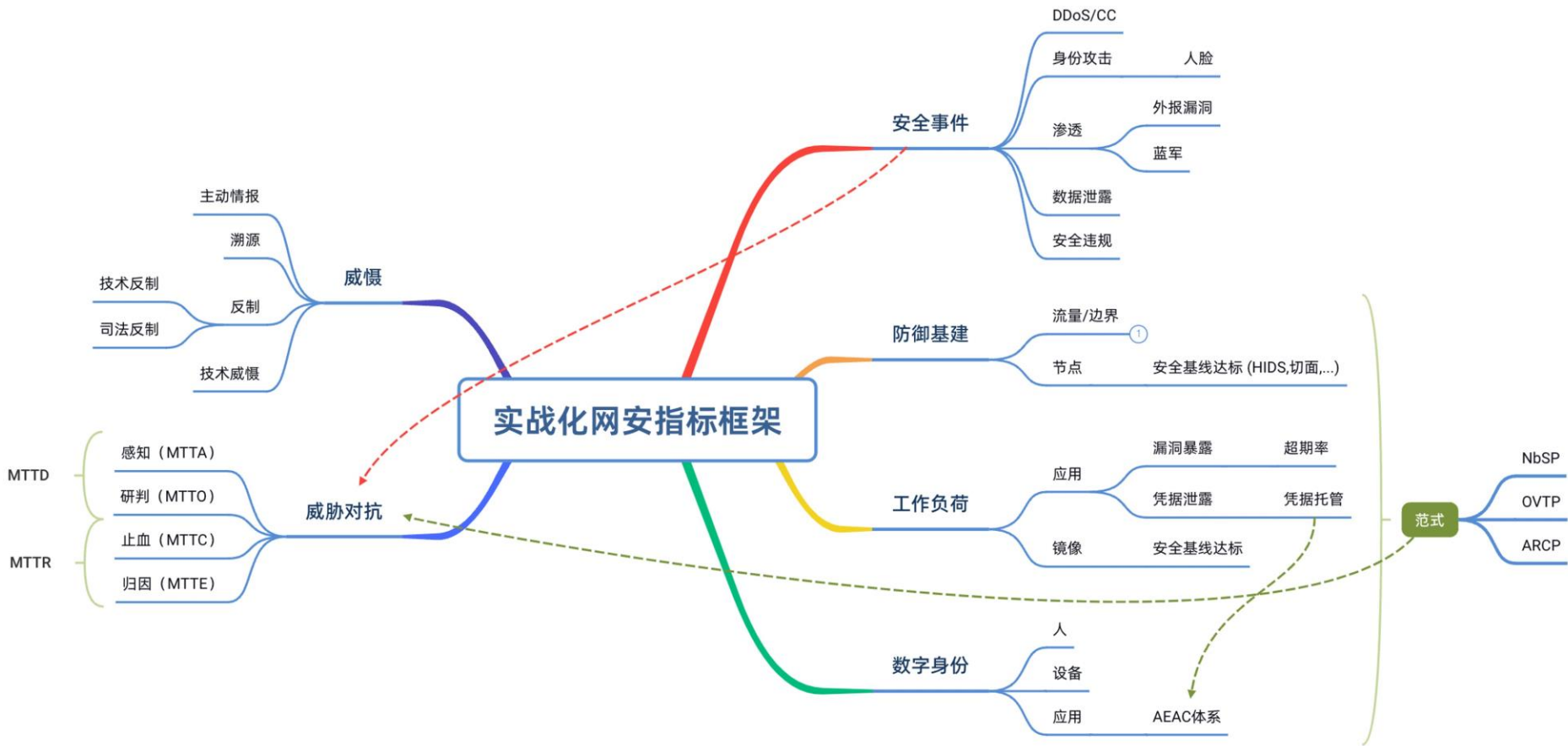
测评认证：内部认证与外部认证相结合

- 内部认证：应成为业务展开的必要前提
 - 人员认证、产品认证、业务认证
 - 根据数据敏感性、合规要求和风险态势分级
 - **测评方式需要紧跟技术发展而发展，否则会阻碍技术发展**
- 外部认证：积极与监管测评认证机构合作



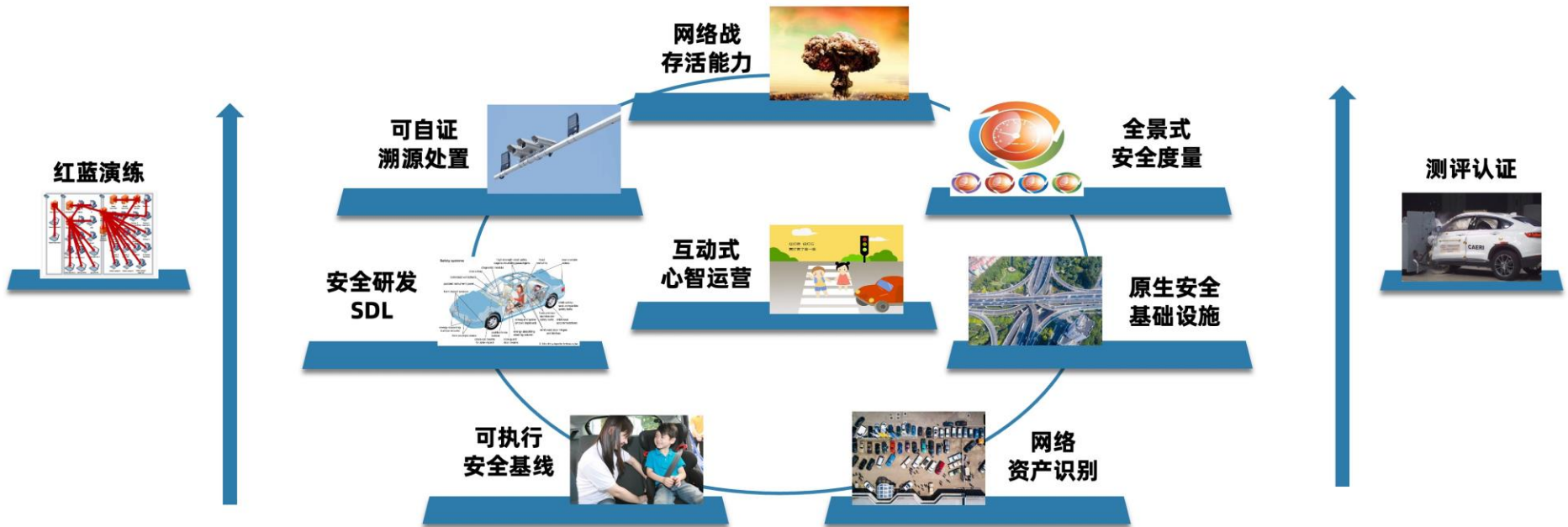
红蓝演练：多种方式相结合

量化治理：网络空间安全技术指标体系



网络安全复合治理成熟度模型

战略要位，实战驱动，范式重构，技术破局



总结

结语：最大的漏洞是认知的缺失

安全不仅仅是“成本”，而是“投资”，更是未来国际竞争的核心竞争力

- **安全的核心是对抗，对抗是多维度的、持续的**
 - 企业中安全受制于：生产关系复杂度，业务复杂度，时空复杂度
- **企业安全的根基：技术和管理层面的认知**
 - 禅宗：认知，气宗：资源，剑宗：技术
- **企业安全的支柱：安全团队的专业度**
 - 避免企业走向安全稳定雪崩：预警、避免、消解、改造
- **原生安全范式：NbSP、OVTP、ARCP、DKCF**
 - 在认知层面反思网络空间安全体系
 - 切面是有效支撑原生安全范式实现的新安全基础设施
- **企业安全实践：**
 - 明确管理责任，建立安全基线，消解头部风险，度量技术指标，推动基建演进，专业对抗保障



谢谢

彩蛋

