企业网络空间安全：困境、反思与实践

技术视角

韦韬

2025.1

蚂蚁集团
ANT GROUP

序章

雪崩时没有一片雪花是无辜的

网络安全挑战：现实的威胁

蚂蚁集团 ANT GROUP

各大企业都遭遇过不同类型的安全攻击

通过0day/供应链社工钓鱼/业务滥用实现盗取数据/情报/勒索

Operation Triangulation: 0click iMessage RCE 0day
收到一条包含附件的iMessage，无需任何交互即可出发代码执行漏洞，接着利用其它漏洞进行权限提升，并下载功能齐全的恶意软件，之后删除附件和原始消息。

Aurora: 浏览器及其相关RCE 0day
拥有多个可造成RCE的0day漏洞（比如Oracle Java/Internet Explorer/Firefox），这些漏洞被植入到各类有特定人群的网站上（比如伊斯兰圣战相关），甚至通过广告精准投放给特定人群，实现访问特定网页即可感染。

CA&Facebook: 合作伙伴数据滥用
Cambridge Analytica滥用Facebook接口采集超过8700万用户资料数据进行分析并出售。面对一方/二方/三方合作伙伴，数据安全水位各不一样。

SolarWinds: 供应链软件更新源被控
收SolarWinds遭到入侵，导致更新包被替换为存在后门的。超过18000个使用SolarWinds的企业被控制。

购买内部员工权限/入职为外包
业内曾出现多起将查询敏感数据的权限对外出售赚取利益，还不仅限于企业内部员工。甚至存在通过入职成为外包的方式，获取查询数据的权限甚至作为跳板进入内网收集数据。

LockBit: 各种供应链软硬件0day
通过钓鱼邮件以及0day/Nday漏洞（Fortinet/Citrix等软件）突破边界，进行感染以及自传播。通过窃取加密、威胁泄漏数据、DDoS等多重方式勒索赎金。勒索软件已RaaS化，通过利用Nday甚至储备0day方式进行攻击。

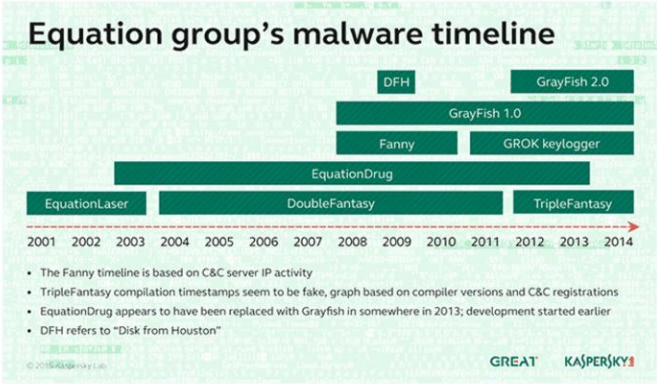
类似被攻击的安全事件数不胜数。震网, Stuxnet; LinkdIn数据泄漏; 斯诺登; Yahoo数据泄漏; Target数据泄漏; Adobe数据泄漏; Sony Picture数据泄漏; JP Morgan Chase数据泄漏; eBay数据泄漏; The Regin Platform; Uber数据泄漏; Adult Friend Finder数据泄漏; WannaCry勒索软件攻击; Vault 7/8; Under Armour MyFitnessPal数据泄漏; Marriott数据泄漏; Capital One数据泄漏; WhatsApp被NSO Group入侵; SolarWinds供应链攻击; Twitter钓鱼事件; Colonial Pipeline勒索软件攻击;

网络安全挑战：现实的威胁

蚂蚁集团 ANT GROUP

安全事件背后对手的实力

方程式组织持续十多年利用网络攻击武器库控制30多个国家数万名对象设备



经过十多年持续迭代更新的攻击武器库，7个0day漏洞

感染全球超过30多个国家的数万名受害者

APT各种形式社工钓鱼
通过邮件、聊天工具等各种形式，模拟你信任的人，诱导你打开存在木马的各种形式链接/附件。通过定向行业广撒网方式，控制大量电脑，并进一步潜伏。

GrayFish：无落地执行文件
依赖bookit启动，任何阶段执行失败都将启动自毁。运行在Windows注册表中，敏感信息储存在注册表中实现的加密虚拟文件系统，并利用三方合法签名的驱动程序漏洞执行任意命令。

Fanny/Stuxnet：连接U盘自我复制，实现感染和控制未联网电脑
在U盘联入电脑后，通过在.LNK嵌入恶意代码，实现插入U盘即可自动感染所连接的电脑，即使自动运行功能关闭。同时将收集到的数据存入U盘隐藏区域，一旦后续联入拥有互联网访问权限的机器，将会上传数据到攻击者服务器，并下载新的指令，在下次插入指定机器时运行。

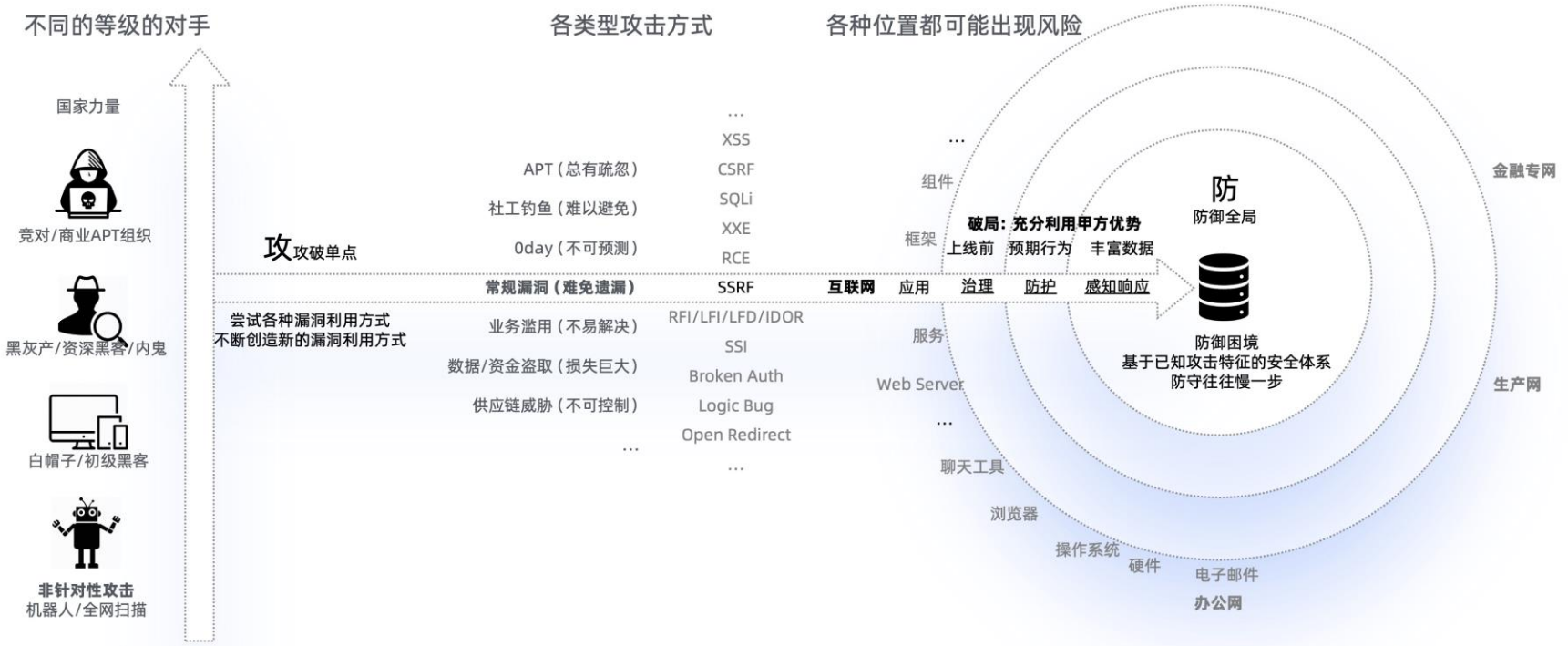
GrayFish：磁盘擦除和格式化后还能存活
通过重写受感染的电脑的硬盘驱动器固件，实现在你格式化或重装系统后，还能保留恶意软件以及窃取的敏感数据，并提供接口访问。

类似案例中所使用的高危漏洞数不胜数。Log4Shell（CVE-2021-44228）、EternalBlue（CVE-2017-0145）、NotPetya（CVE-2017-0147）、Stuts2 RCE（CVE-2017-5638）、Cloudbleed（CVE-2017-8817）、Heartbleed（CVE-2014-0160）、Shellshock（CVE-2014-6271）、POODLE（CVE-2014-3566）、KRACK（CVE-2017-13077）、Zip Slip（CVE-2018-5002）、Dirty COW（CVE-2016-5195）、EternalBlue（CVE-2017-0144）、SQL Slammer（CVE-2003-0352）、BlueKeep（CVE-2019-0708）、ZeroLogon（CVE-2020-1472）、SMBGhost（CVE-2020-0796）、ProxyShell（CVE-2021-34473/34523/31207/34474）、Meltdown（CVE-2017-5754）、Spectre（CVE-2017-5715）

网络安全挑战：面对高级威胁，破局攻防不对等

挑战：攻击只需突破一个点，防御需要防全局

破局：构建防守方主场优势（人和，地利，技术创新）



俄乌战争开启了后互联网时代人类社会战争的新形态

蚂蚁集团 ANT GROUP

热战，网络战，舆论战，金融战，贸易战，科技战，六战合一

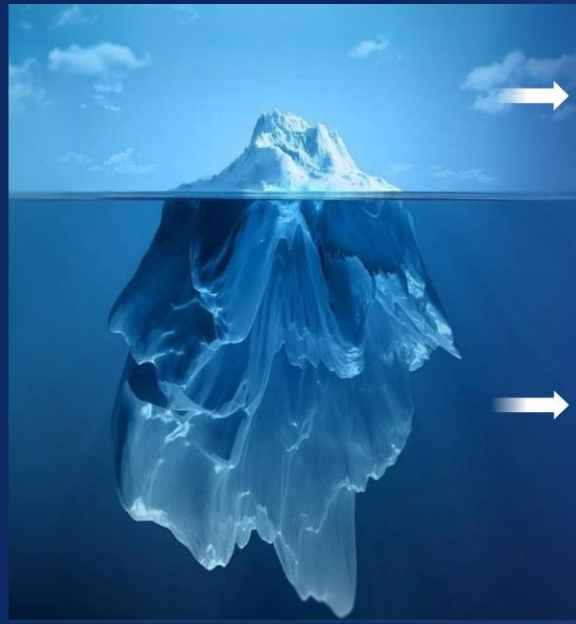
网络攻击	 DDoS攻击 – 大流量阻塞迫停服务	 网络定向攻击 – 窃密/勒索/摧毁系统
黑产	• 打击同行，不正当竞争 • 网络敲诈	• 窃取个人信息 ➔ 电信诈骗 • 加密/窃取商业信息 ➔ 网络勒索
日常/ 热战前	**低烈度攻击** • 乌克兰1月：外交部、教育部、内政部、能源部	**间谍行为，政治勒索** • 能源/金融/交通/矿业：BlackEnergy/KillDisk/CrashOverride • 政府机密：美国政府遭受SolarWinds供应链攻击 • 军事机密：美国国防部和情报部门的众多承包商 (AA22-047A) • 白俄罗斯铁路遭受Scorching Heat政治勒索攻击
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消息

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，衡量网络与系统的安全状态并进行安全处置决策

万级	百万级	万级	十万级	万级
服务器主机	业务容器	业务应用	公网API接口	办公终端



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

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

- 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

蚂蚁集团
ANT GROUP

核心难题：数字化业务复杂性爆炸下的安全与业务发展协同

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缩容加剧了问题，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）

防御体系的复杂性爆炸

蚂蚁集团 ANT GROUP

典型的网络纵深防御体系，蕴含网络空间安全各子学科体系，依然在高速发展中

- **单点增强：每个框都是一个或多个子学科**
  - 尽可能的消减信息系统中的安全漏洞
    - 代码安全，系统交付安全
  - 单点安全纵深扩展
    - 可信环境，安全容器，安全平行切面
- **多层防御：纵深的构建**
  - 区域隔离：核心是关键访问控制点收敛
    - 安全网关，虚拟安全域
  - 网络接入安全保障，零信任
    - 访问控制，应用网关，防DDoS
- **交叉补位：纵深的精髓**
  - 安全平行切面体系
  - 态势感知与融合对抗智能体系
  - 安全审计体系

安全体系的反思：失效度量的技术视角

蚂蚁集团 ANT GROUP

- 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

安全体系的反思：失效度量的组织视角

蚂蚁集团 ANT GROUP

- **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

蚂蚁集团 ANT GROUP

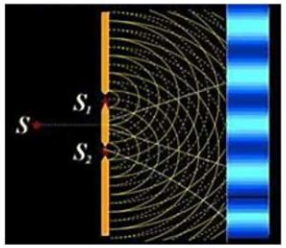
- 企业安全和稳定性的真正灾难：技术和业务历史负债积累成雪山，攻击和异常事件触发雪崩点，形成难以快速消解的安全或稳定性雪崩后果
- 没有绝对的安全，但我们也见过太多一个细节疏忽就导致整体安全失败的惨痛案例
- 安全体系设计正是这样，需要在本源层面思考充分，才能关注到、支撑住关键细节，从而避免安全雪崩

细节决定成败：安全从业者专业性和组织通达的重要性

蚂蚁集团 ANT GROUP

- 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

蚂蚁集团
ANT GROUP

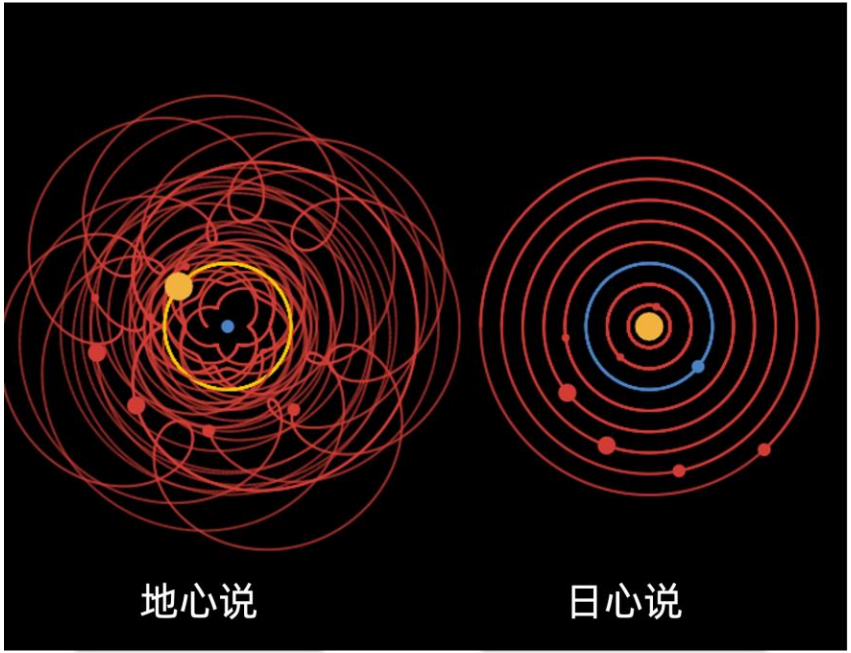
范式重构

最大的漏洞是认知的缺失

蚂蚁集团
ANT GROUP

对于世界本源的认知探索（范式）的追求推动了文明的进步

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

原生安全范式重构：OVTP可溯范式（策略层）

Operator-Voucher-Traceable Paradigm

- 财务人员有了合同、发票才能付款，但计算机访问控制模型中一直缺乏这样的业务凭证概念
- 传统访问控制强调角色，在复杂访问链路中真实身份缺失给攻击者巨大攻击空间

- 大模型应用的新兴安全风险
  - 需要透传实际用户身份权限
  - 模型内置信息角色失控
  - 需要做失陷假设

- 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 业务凭证链路(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
- 大模型的工具调用和信息查询，目前普遍缺乏身份和业务凭证透传，造成严重的安全风险

原生安全范式重构：NbSP零越范式（机制层）

Non-bypassable Security Paradigm

- 大模型Agent框架、第三方库、网络环境等等的系统安全机制缺失都成为潜在攻击点

- 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

- 随着大模型应用的爆发，ChatInjection已经发展成类似SQLInjection般的严重漏洞类型
- Prompt攻击，大模型越狱，Prompt窃取等等，都是大模型应用中NbSP范式遭到了破坏

原生安全范式重构: ARCP攻击回报范式（价值层）

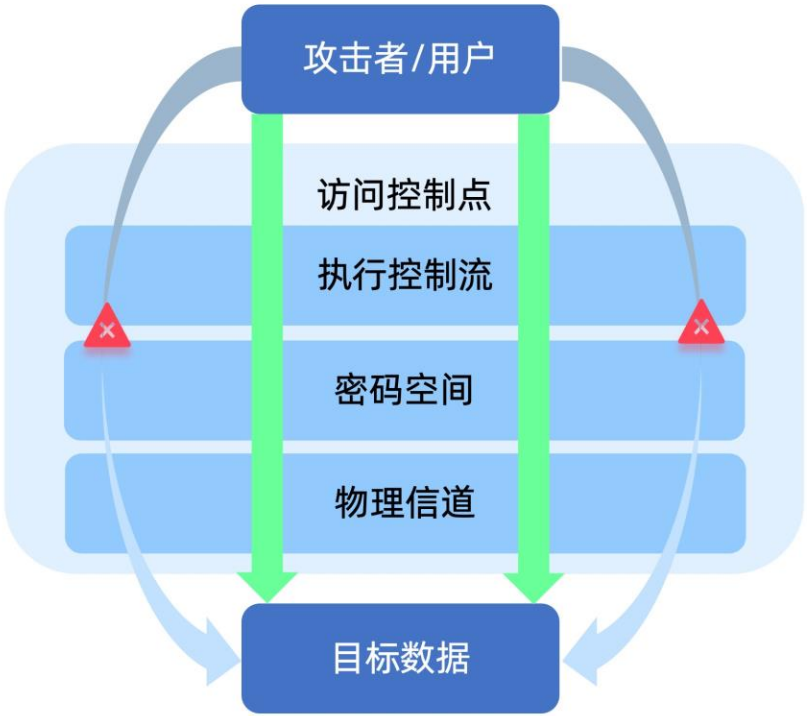
Attack-Reward-Cost Paradigm

- 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零越范式视角下的攻击分类

蚂蚁集团 ANT GROUP

- 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)

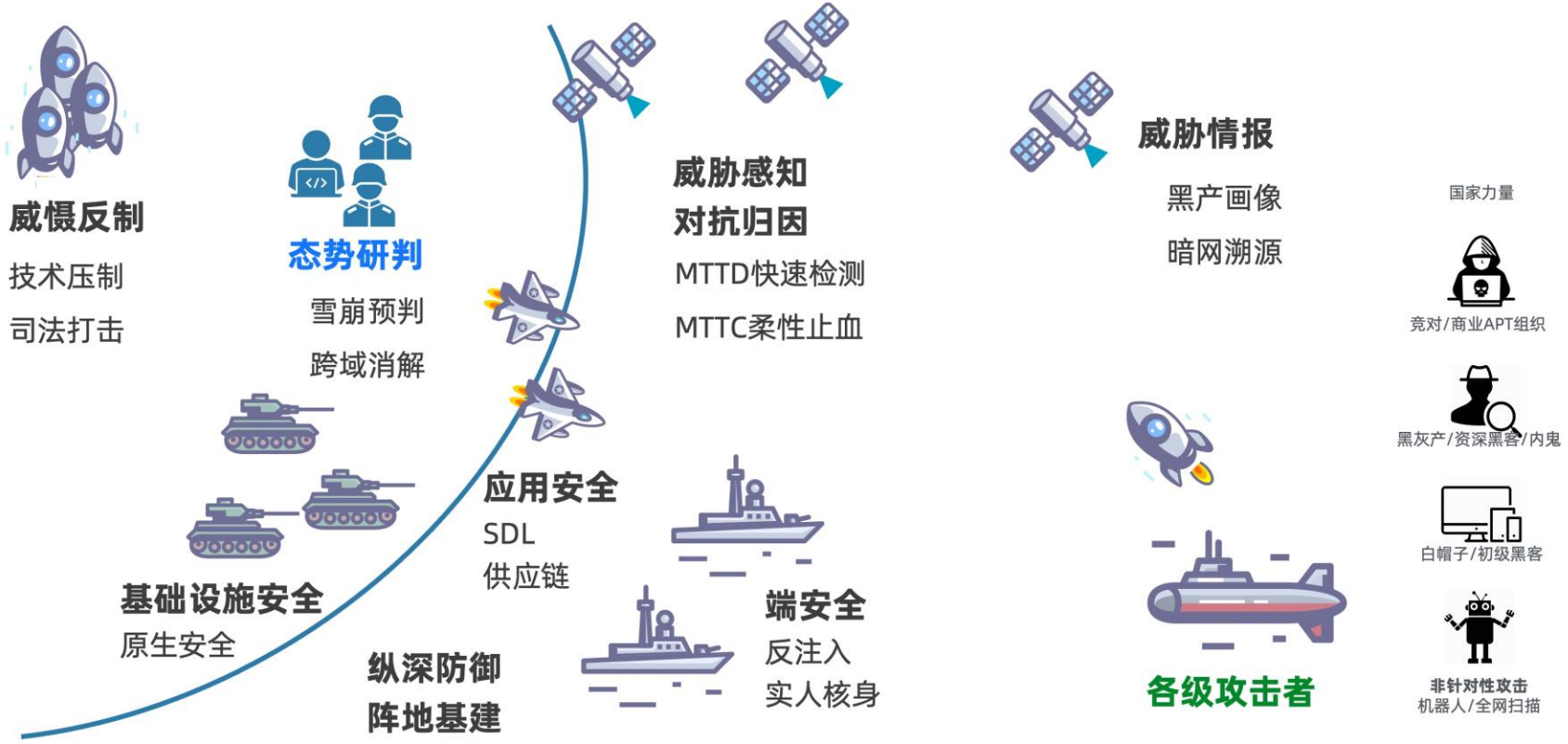


ARCP视角下的安全对抗全链路

蚂蚁集团 ANT GROUP

“纵深防御，威胁情报，威胁感知，对抗归因，态势研判，威慑反制”

完整的网络安全攻防对抗组织体系，对抗的TCO成本核算：快速止血，长效压制



原生安全范式视角下“安全范式三问”

待评估目标:

- 控制: 网络、系统、应用
- 资产: 数据、资金、账号

安全技术评估三要素:

① 横: NbSP

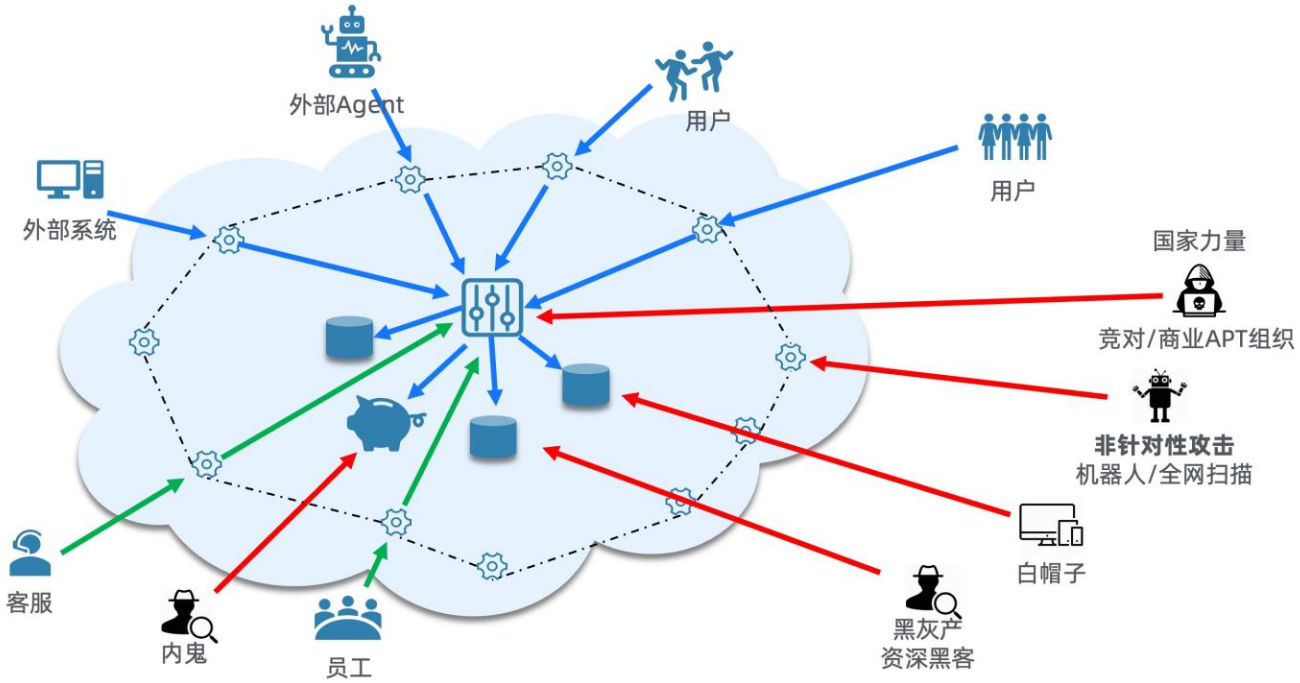
隔离是伪命题, 但安全域间访问控制点收敛么?

② 纵: OVTP

教科书过时了, 但访问控制点上策略满足链路要素可溯么?

③ 动: ARCP

防守不可能完备、对抗不可缺失, 但攻防对抗成本经济么?



蚂蚁集团
ANT GROUP

体系反思

最大的漏洞是认知的缺失

蚂蚁集团
ANT GROUP

安全体系① 纵深防御

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

蚂蚁集团
ANT GROUP

安全体系① 纵深防御的现实

纵深究竟要多深?

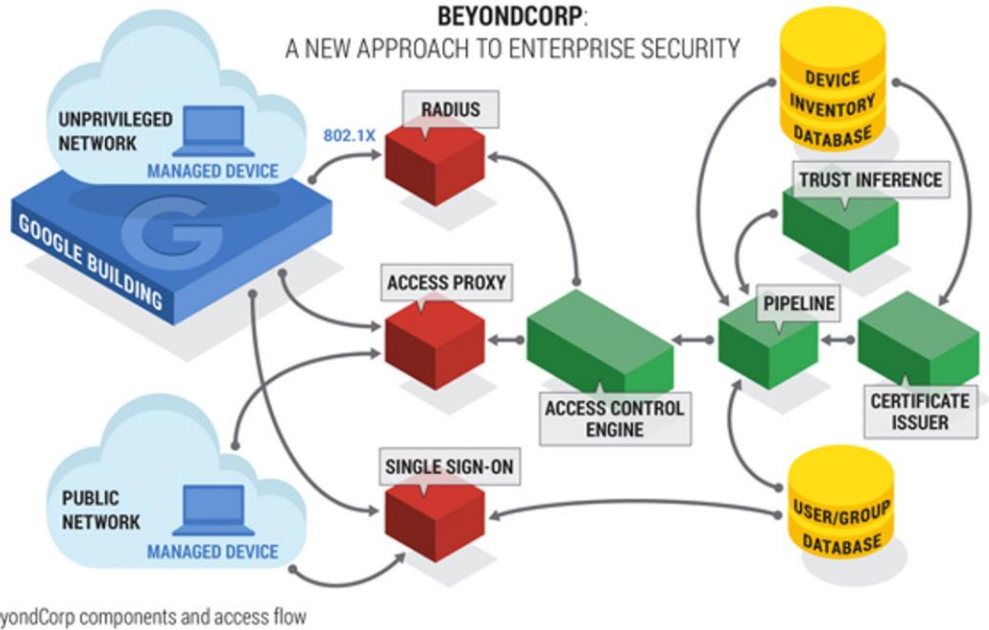
- 网络纵深 往往远低于 物理纵深
  - **美国科洛尼尔公司严密的铁丝网隔不住来自欧洲的网络攻击者**
- 人与大量敏感信息之间隔多深?
  - **一个服务账号**
  - **现实: 现有访问控制体系 有权限，没凭证（-OVTP）**
- 供应链与网络渗透之间隔多深?
  - **一个自动版本升级，一个云输入设置，一个短信云同步**
  - **现实: 现有网络体系大量隐藏访问通道（-NbSP）**
- 有多层, 多暴露, 没交叉
  - **网络拓扑混乱且动态变化**
  - **现实: 安全观测数据不全，不准，不及时，难以关联（-OVTP）**

蚂蚁集团
ANT GROUP

安全体系② 零信任

Never Trust, Always Verify

- 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。

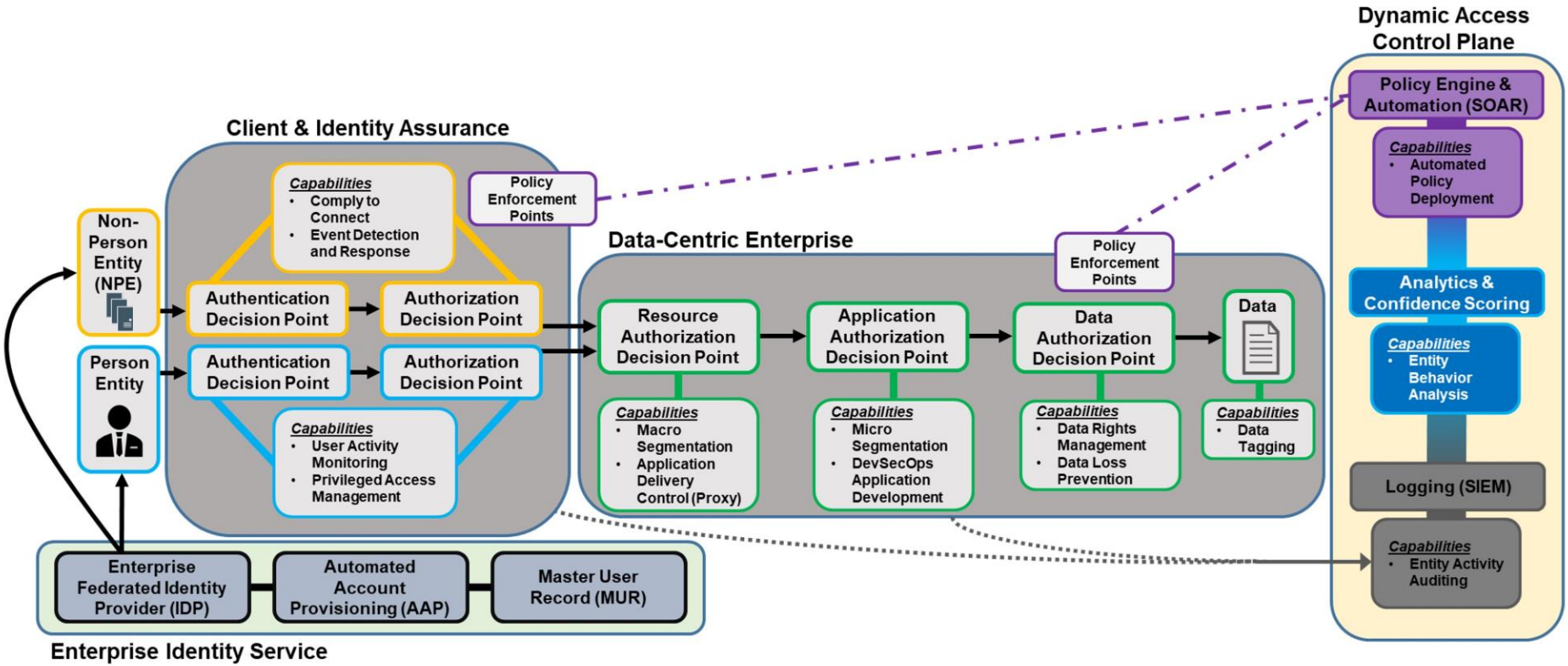


BeyondCorp components and access flow

蚂蚁集团
ANT GROUP

安全体系② DoD零信任参考架构

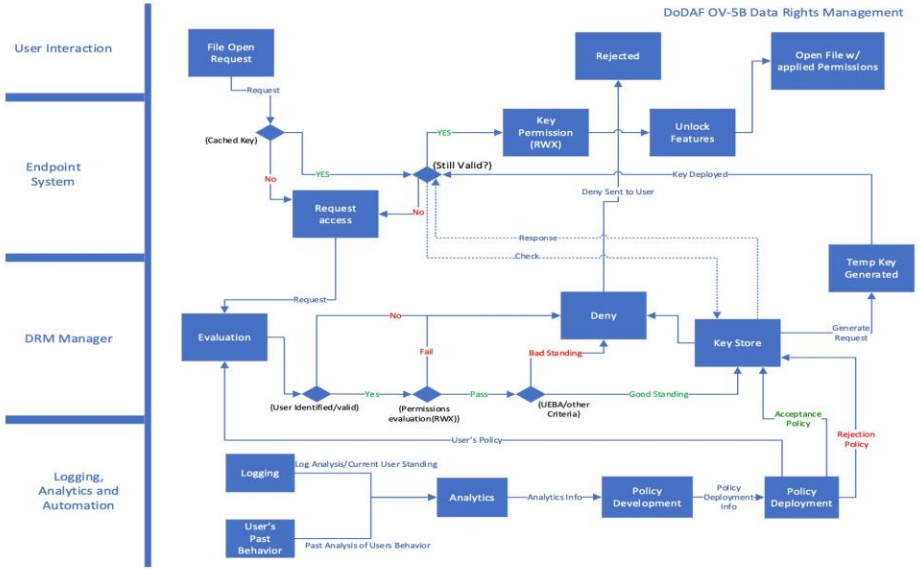
从零信任理念到新纵深防御架构



安全体系② 零信任的现实

检查很多，但缺乏范式保障

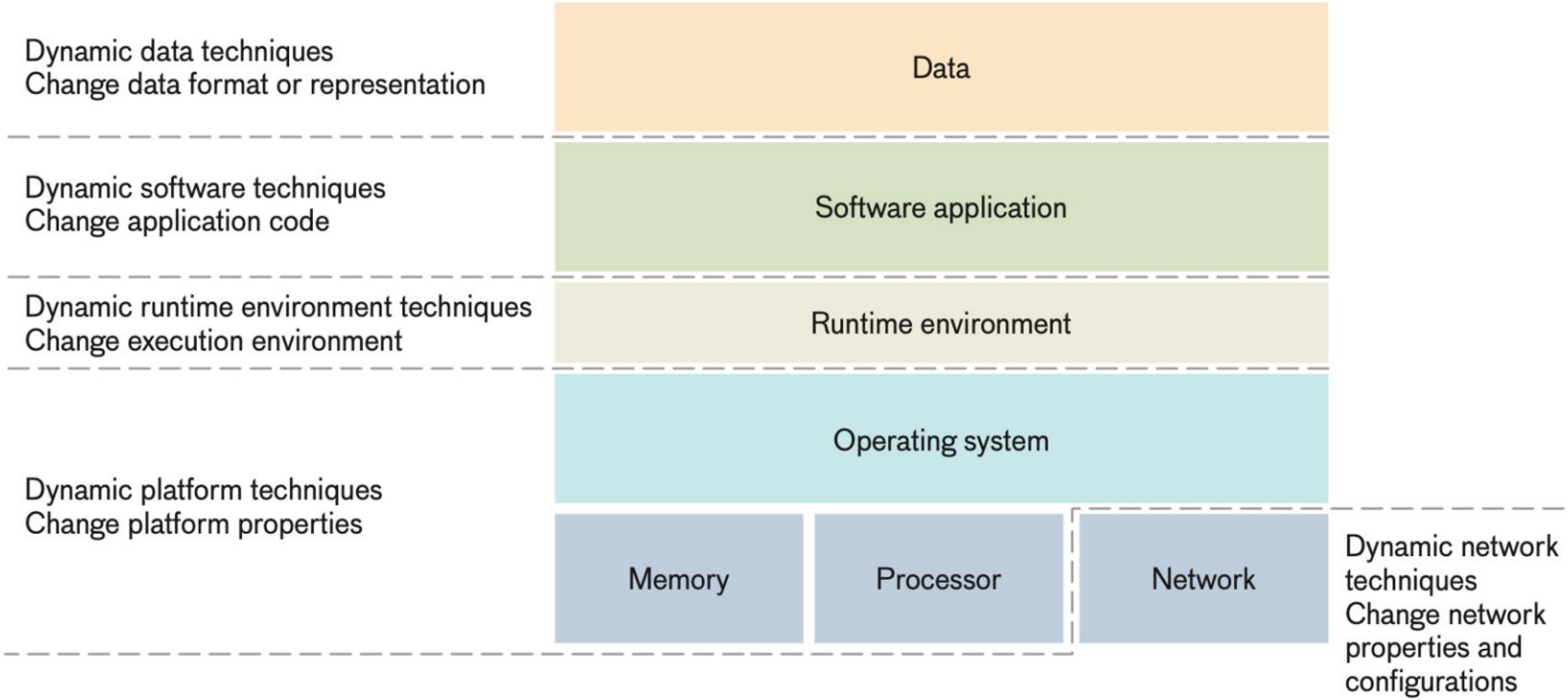
- 其实高安全等级网络中强访问控制不是新要求
- **OVTP的缺失**
  - 用凭据（Credentials）代替操作人
  - 业务凭证（Voucher）的缺失
  - 访问链路的可追溯性的缺失
- **NbSP的缺失**
  - 访问边界缺乏收敛
- **已有应用系统的改造与兼容**
  - 对于已有系统和IT基础设施系统，难以直接改造应用



蚂蚁集团
ANT GROUP

安全体系③ Moving Target Defense

不确定性是攻击者最痛恨的问题之一



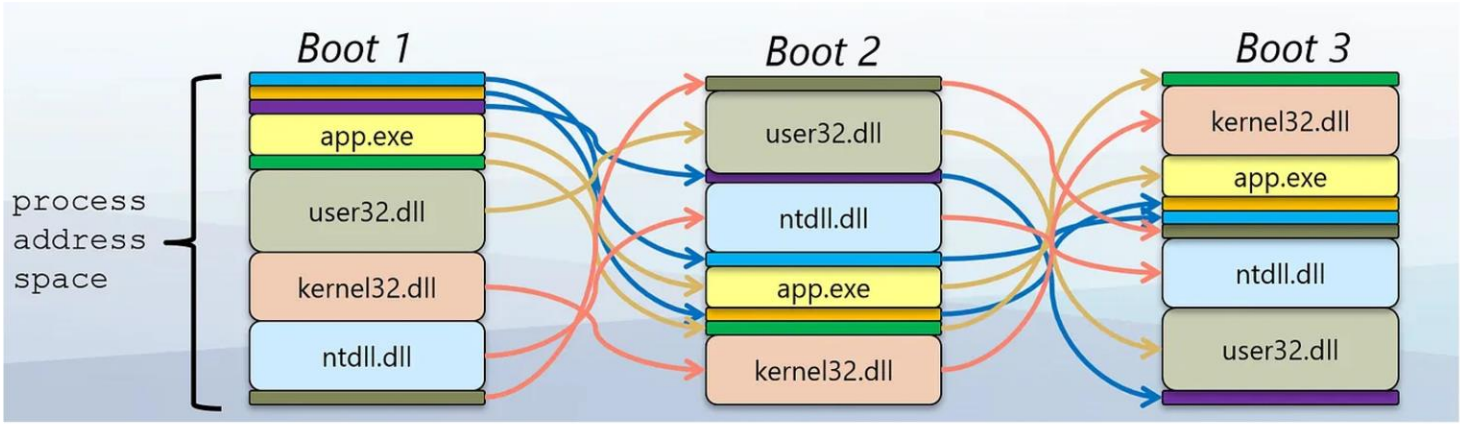
From "Moving Target Techniques: Leveraging Uncertainty for Cyber Defense"
By Hamed Okhravi et al

蚂蚁集团 ANT GROUP

安全体系③ Moving Target Defense的强与弱

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



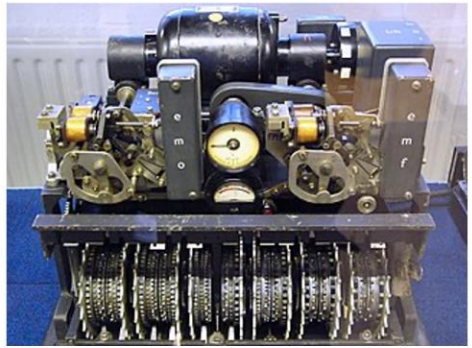
Address Space Layout Randomization (ASLR)

蚂蚁集团
ANT GROUP

安全体系④ 密码学

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

蚂蚁集团
ANT GROUP

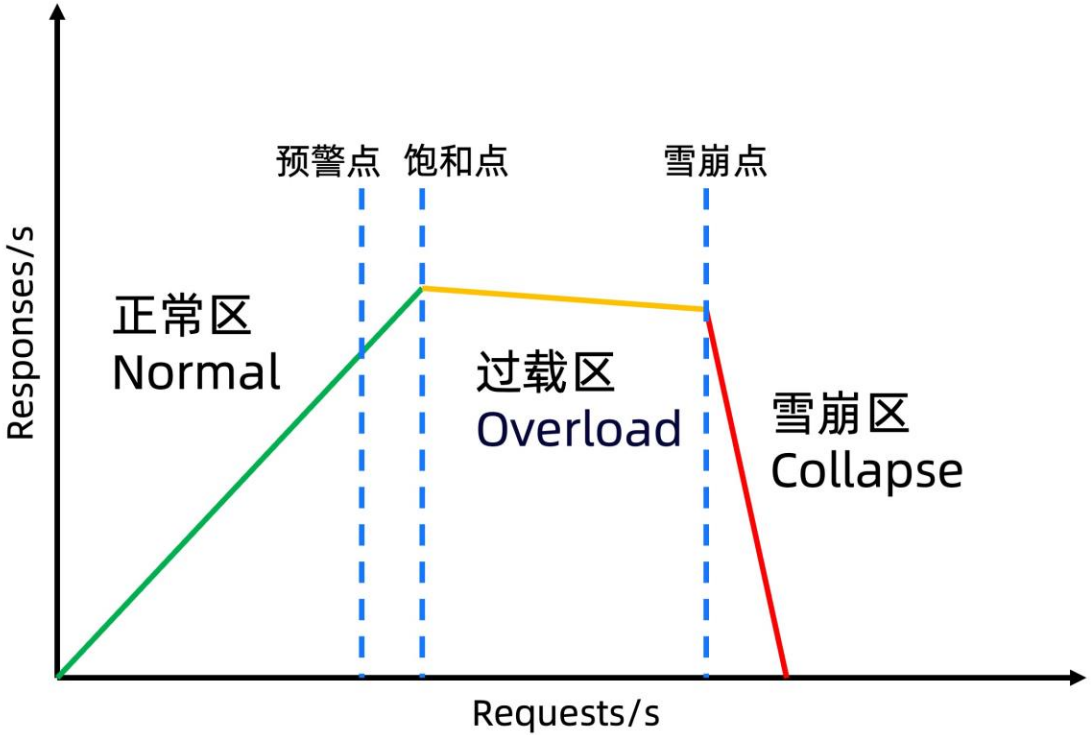
安全体系④ 密码学应用的现状

数字魔法的阿克琉斯之踵

- **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

蚂蚁集团 ANT GROUP

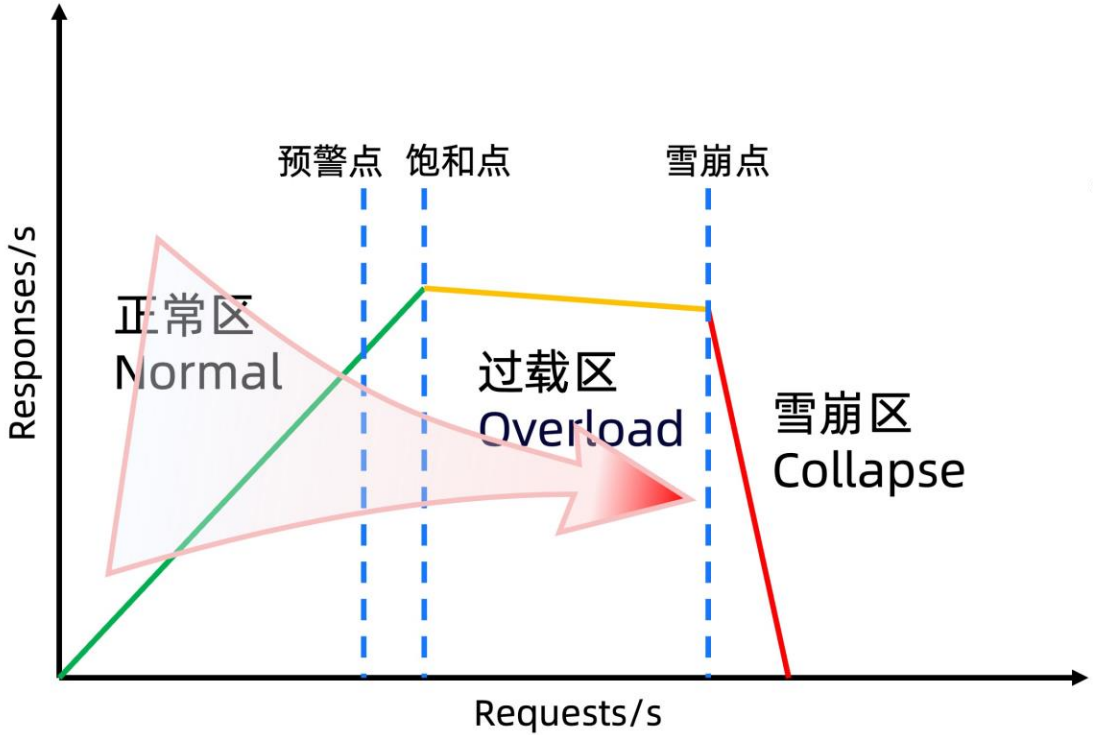
⑤ CC流量攻击与稳定性：网络应用流量响应N-O-C曲线



- 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

蚂蚁集团
ANT GROUP

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

蚂蚁集团
ANT GROUP

安全平行切面

承载范式重构的下一代安全基础设施

蚂蚁集团
ANT GROUP

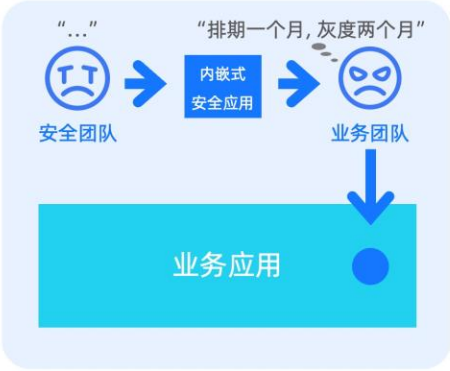
安全体系建设的困境和解法

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

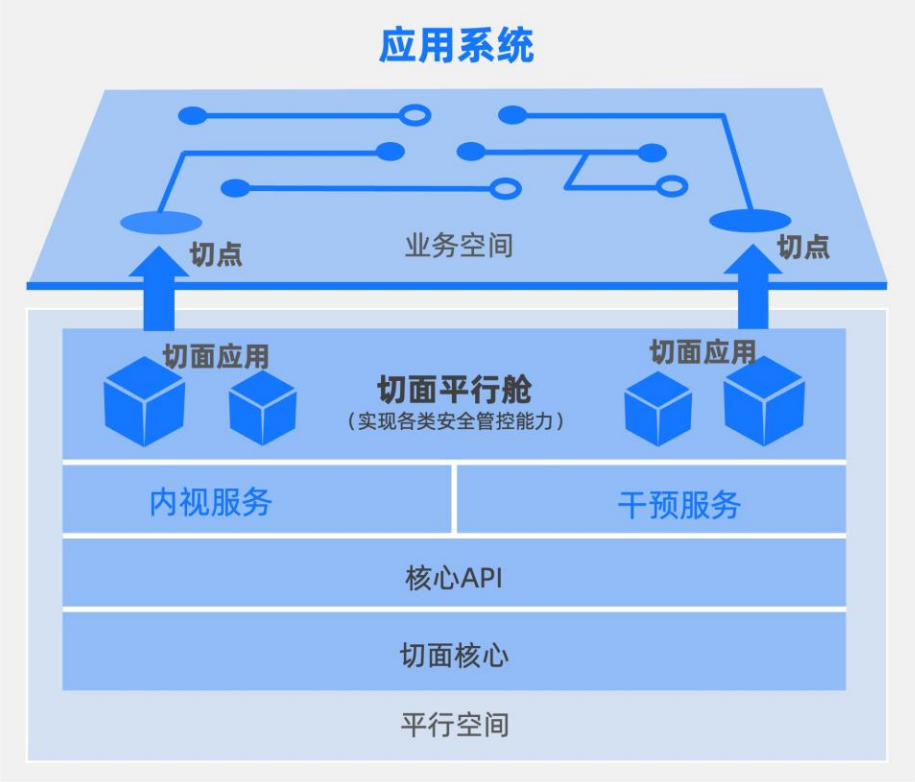


- 业务团队研发排期不吻合
- 安全治理不响应，安全应急跟不上

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

切面技术体系：切面应用，切点与切面平行舱



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

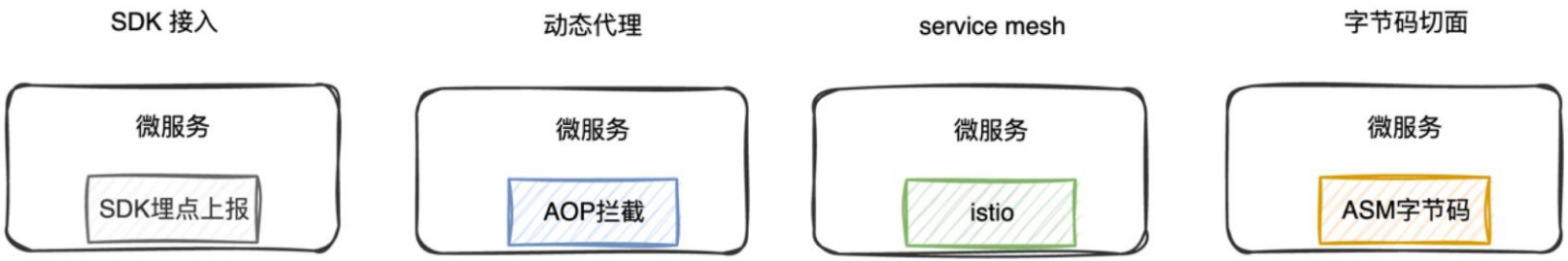
原应用逻辑中的某一代码位置。切面应用可以注入一个或一组切点以进行观测或干预

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

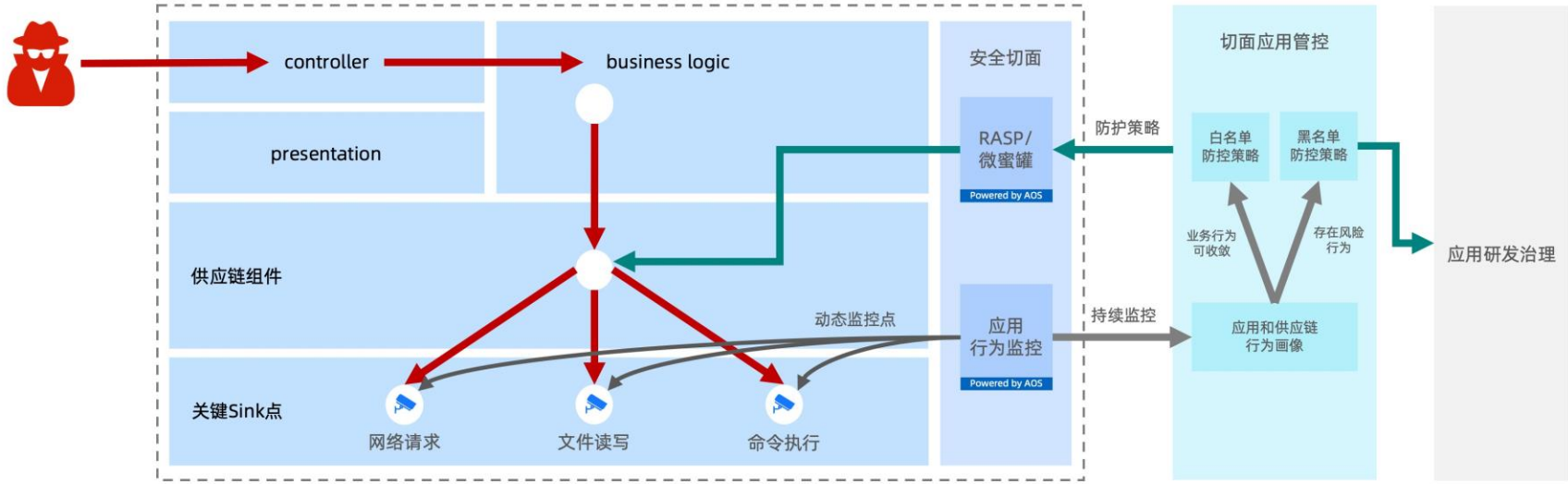
- 可信度量、隔离
- 调度、编排、管控

不同切点的植入方式



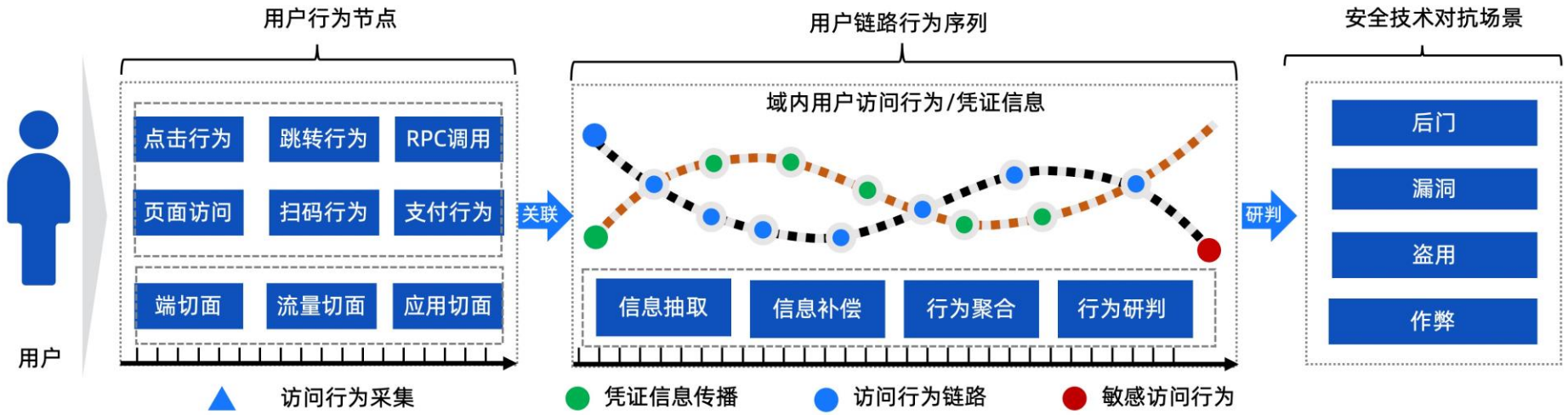
采集方式	SDK 接入	动态代理	Service Mesh	字节码切面
优点	技术通俗易懂	借助Spring原生AOP能力，性能比较好 解耦性和插拔性比较好	完全解耦，对业务代码&容器无任何侵入影响	与业务代码完全解耦 无感接入 任意可序列化数据的采集
缺点	代码侵入性强，开发维护成本高	存在兼容性问题、内部方法采集受限	只能采集入口流量，不支持子调用数据采集 需要对流经mesh层的流量进行筛选采集，容易造成服务耗时过高。	对业务容器性能存在些许影响

NbSP零越范式 -防止后门/漏洞击穿，并进行微蜜罐对抗



- 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

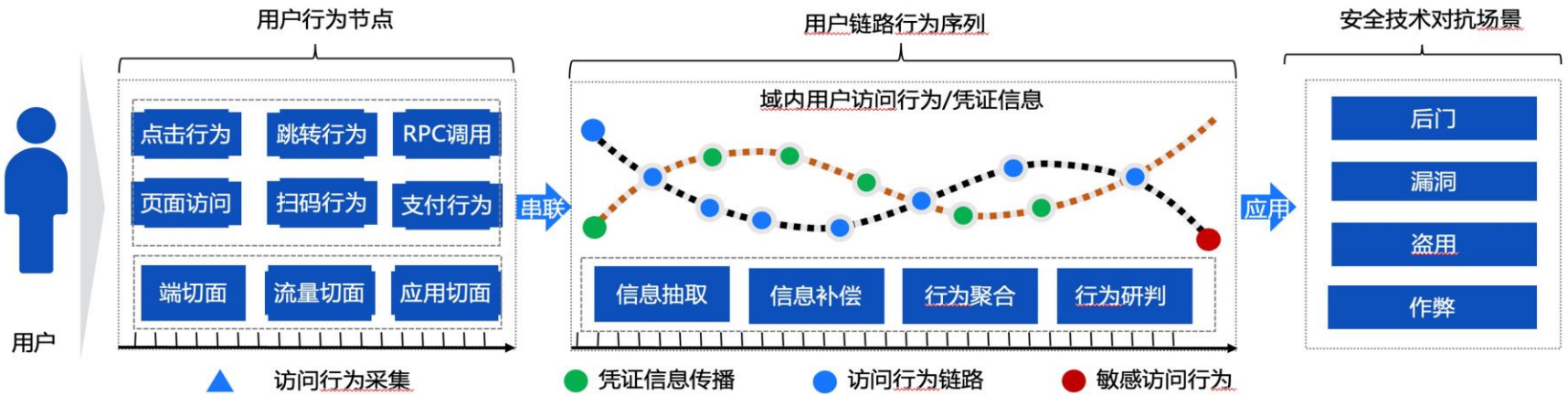
OVTP可溯范式 -实时全链路行为序列补全，高效防控



「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

安全平行切面与DKCF大模型框架的结合：先有数据，再有智能，精准防控



「链路行为节点串联实现业务场景全息判断」

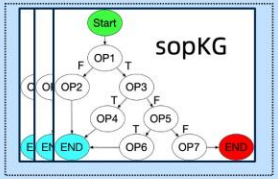
- **Data** **专业数据供给**：数据决定AI能力的上限。安全平行切面实现信息采集解耦，提供“数据观测自由”
- **Knowledge** **专业知识工程**：大模型精调内化+专业SOP知识编程，利用大模型对多维实时行为序列抽取，构建主客凭据关联以及行为依赖生成行为知识图谱，结合ATT&CK技战术领域知识库，提供分析依据
- **Collaboration** **人机高效协同**：基于用户行为链构建行为序列校验引擎，实现了研判检测智能体调用链，融合专家智能和机器智能；安全平行切面提供精准干预能力
- **Feedback** **残差迭代**：专家分析失效案例，监督精调预防降级，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

DKCF网络安全智能体反入侵安全运营实践

蚂蚁集团 ANT GROUP

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

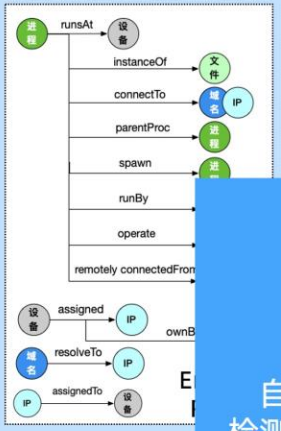
获取网安领域知识 ✓

依据sopKG分步骤拆解COT

无SOP

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



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

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

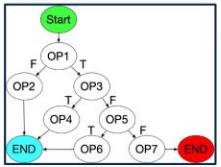
智能专业工具

- 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

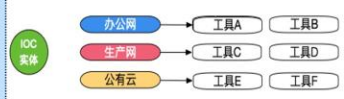
决策白盒化，推理核验 ✓

结合推演图谱验证



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



蚂蚁集团
ANT GROUP

安全平行切面应用实践效果

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 打扰化解危机
- 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

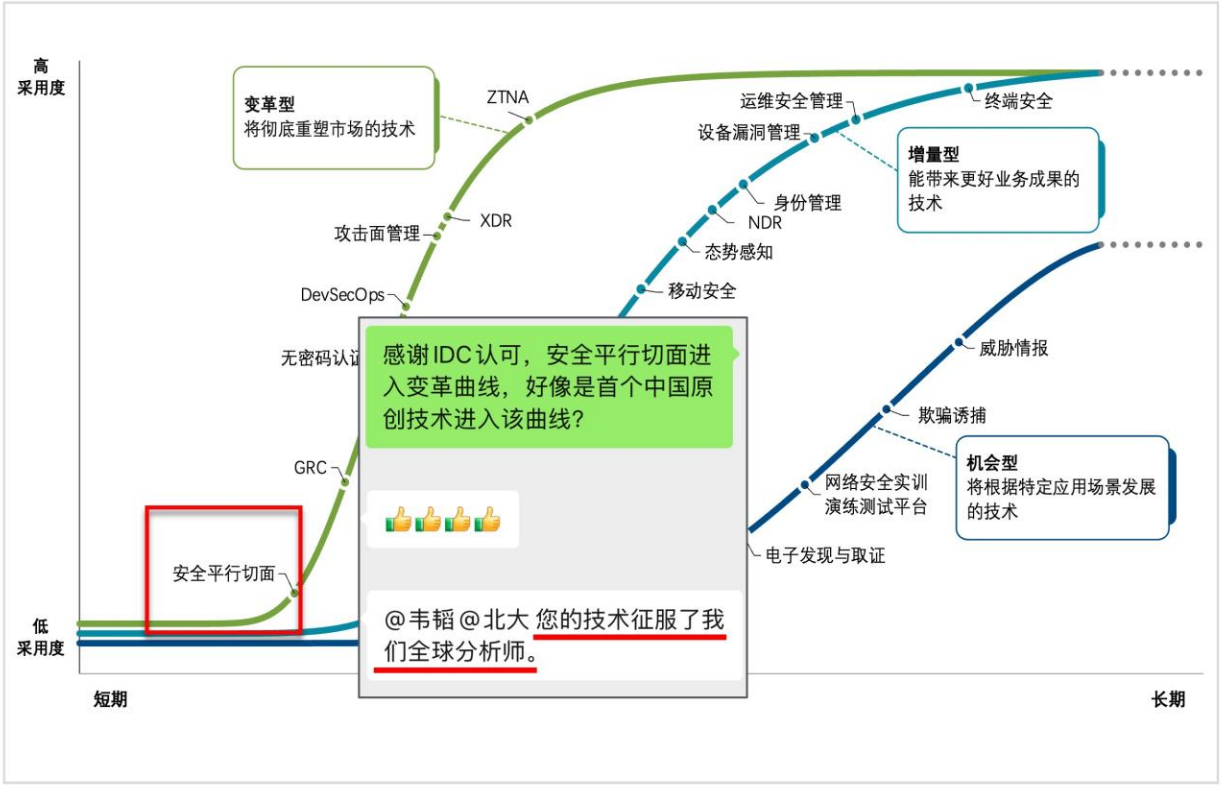
隐私保护

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

蚂蚁集团 ANT GROUP

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

蚂蚁集团 ANT GROUP | 中国移动通信 CHINA MOBILE 移动通信专家 | 中国电信 CHINA TELECOM 研究院 CTRI | 招商银行 CHINA MERCHANTS BANK | 网商银行 | 中国平安 PING AN | 启明星辰 Venus | 安天 ANTIY | 货拉拉 | 红途科技 HONGTU.TECH | 超眼数动 XDD.AI X DIGITAL DYNAMICS | 默安科技 值得信赖的安全伙伴 | boundaryx 边界无限 | 之江实验室 ZHEJIANG LAB | 中测安华 CNAH | 中金安服 | 未来安全 XFUTURE SECURITY | 锦行科技 Jeesen Technologies | 翼盾智能 Wingshield Intelligent 让人工智能世界更安全 | 四叶草安全 Clover Sec | MINGSHI | VUL·AI 华云安 | 云钜天成 SecRisk | 知其安 ZHIQIAN

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0day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马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。

蚂蚁集团
ANT GROUP

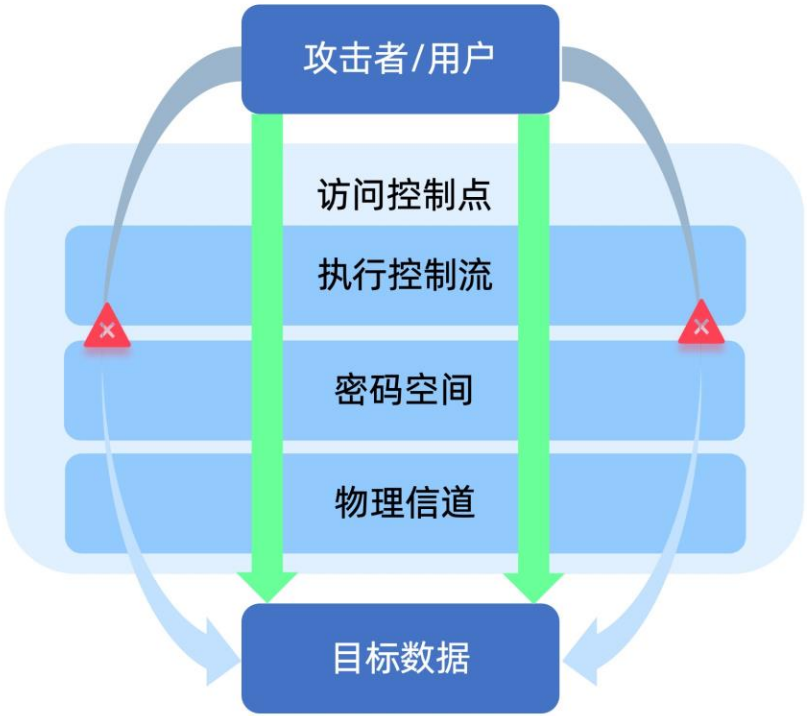
安全范式视角下的系统研发

NbSP防绕过, OVTP可追溯, ARCP可对抗

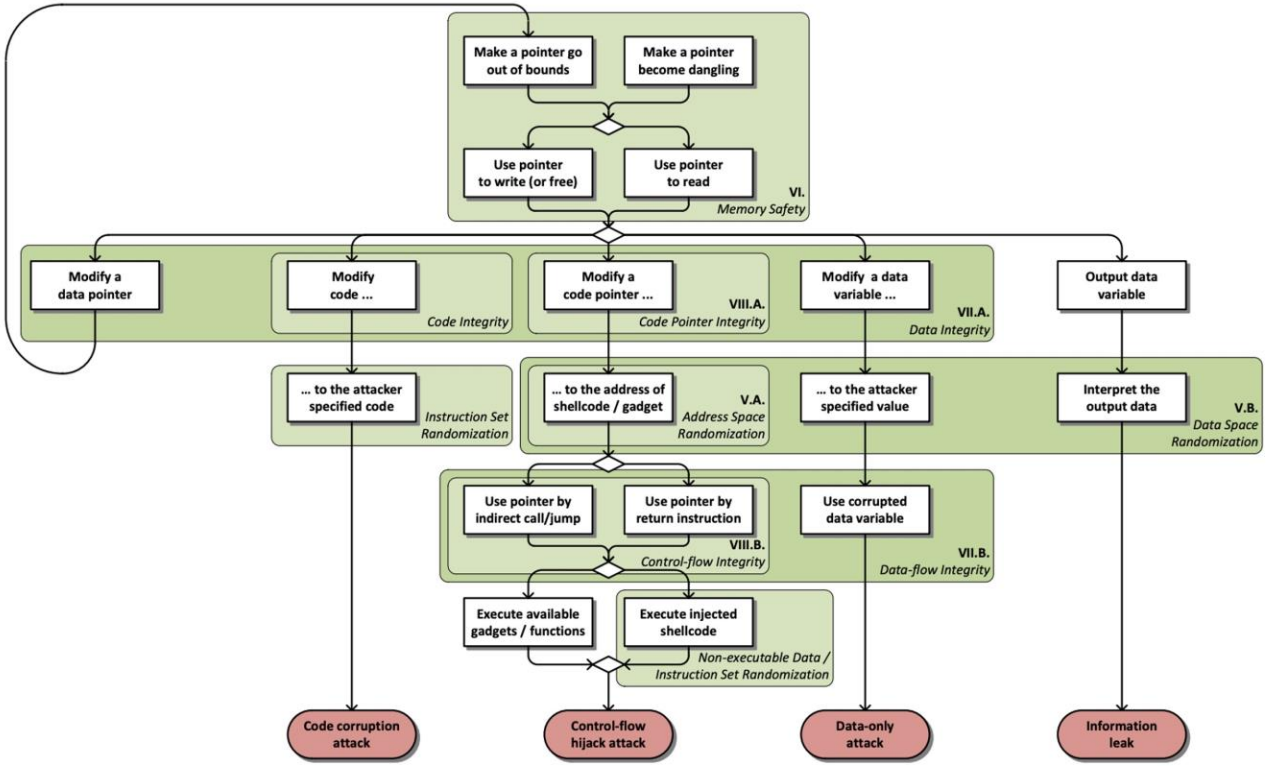
范式视角下的攻击分类 ① NbSP内存安全

蚂蚁集团 ANT GROUP

- 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)



① 历史的回顾 2013年 SoK: Eternal War in Memory



- 大型C/C++系统软件的安全漏洞有大约70%的根因是内存安全问题
- 各种内存安全漏洞缓解机制虽然提升了攻击难度，但依然不停的被攻击者突破
- 该结论在Chromium、Firefox、微软产品、以及Linux等多个不同来源的独立实证研究得到证实

① 沙滩上的城堡需要重新筑基：内存安全迫在眉睫

蚂蚁集团 ANT GROUP

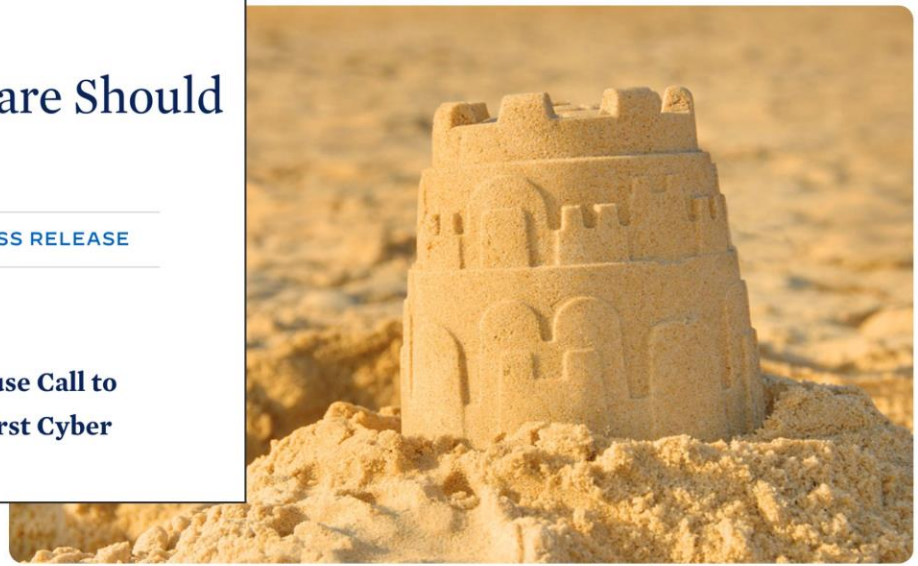
THE WHITE HOUSE

FEBRUARY 26, 2024

Press Release: Future Software Should Be Memory Safe

ONCD › BRIEFING ROOM › PRESS RELEASE

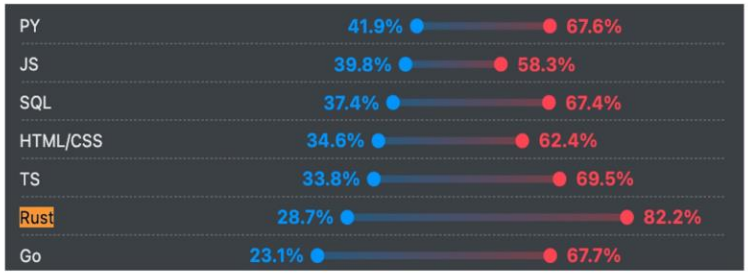
Leaders in Industry Support White House Call to Address Root Cause of Many of the Worst Cyber Attacks

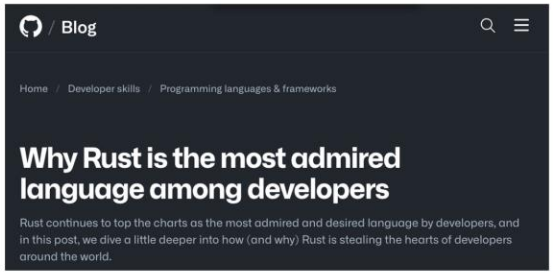


① Rust语言：系统编程的大潮

蚂蚁集团 ANT GROUP

- 业界对使用内存安全语言正在形成共识
- Rust语言：连续9年被StackOverflow评为“最受喜爱的编程语言”

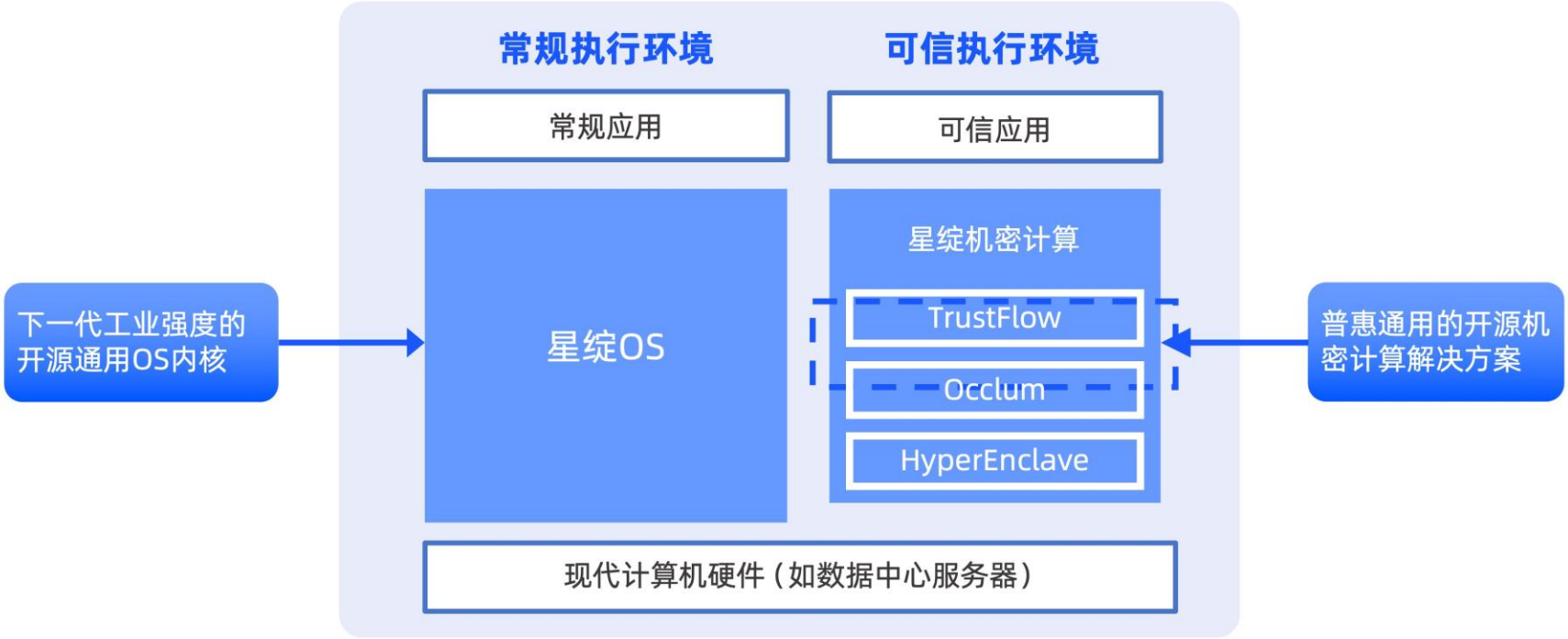




👉 未来的系统软件将被“锈”化，开发者应当最大程度地利用语言优势

① 星绽 (Asterinas)：下一代安全可信的系统软件栈

蚂蚁集团 ANT GROUP



代码已经全部开源: https://github.com/asterinas

① 星绽OS：下一代工业强度的开源OS内核

蚂蚁集团 ANT GROUP

主要特色

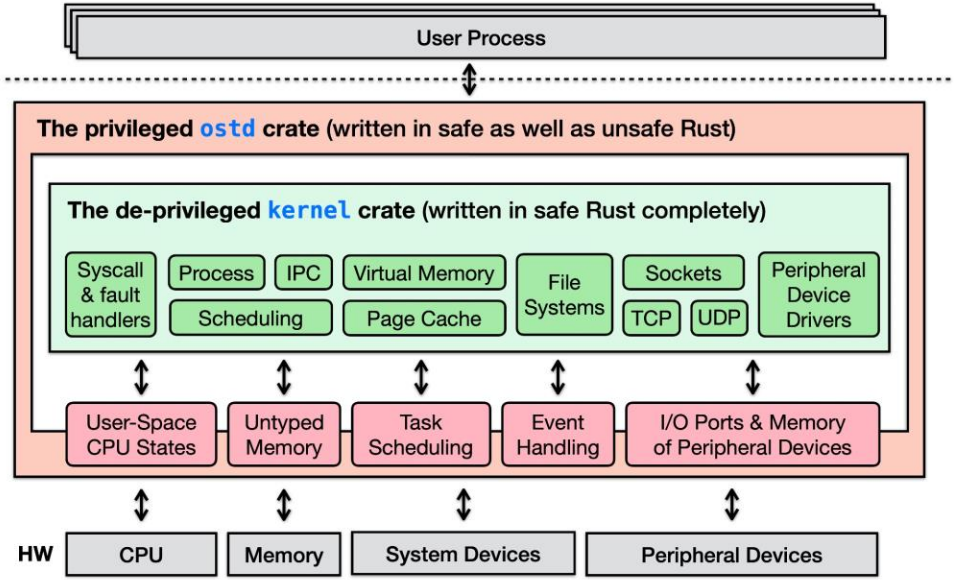
安全原生
基于框内核架构，极大降低了内存安全问题的可能性

性能卓越
在业界公认的基准测试上对齐Linux

广泛适用
支持多种CPU体系架构和应用场景，特别适合安全攸关应用场景

生态兼容
兼容Linux应用程序，无需移植，开箱即用

下一代技术路线：框内核架构 + Rust语言

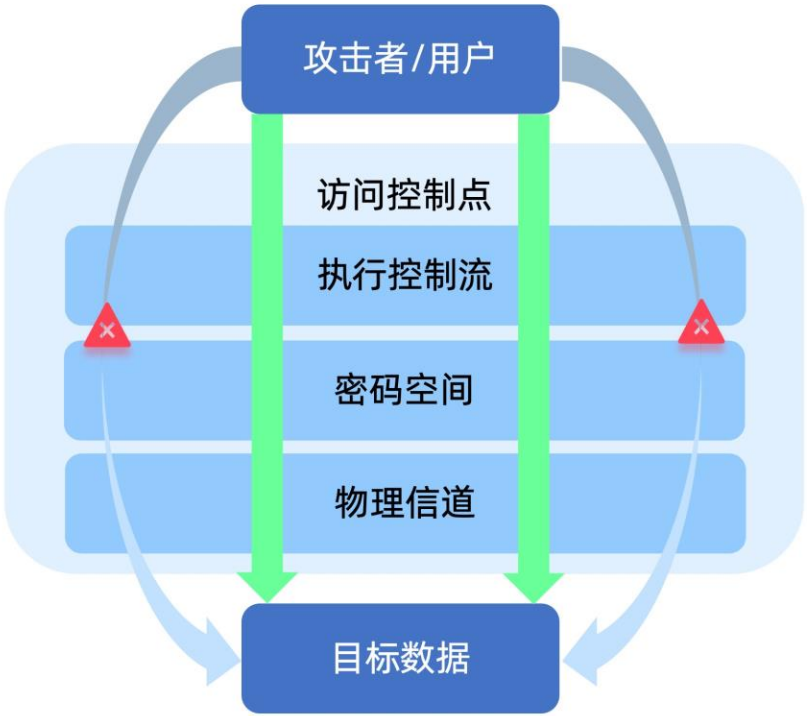


星绽OS系统架构图

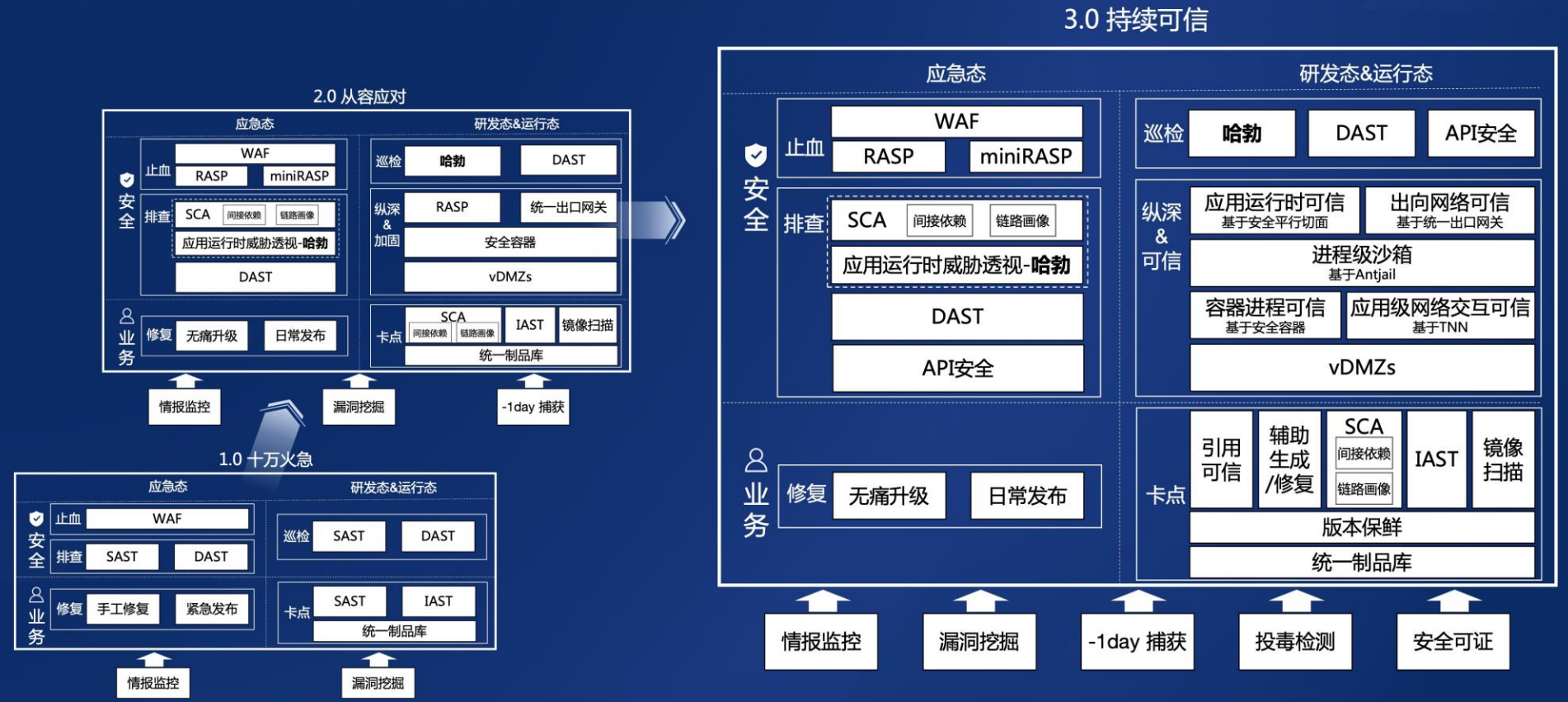
范式视角下的攻击分类 ② NbSP供应链安全

蚂蚁集团 ANT GROUP

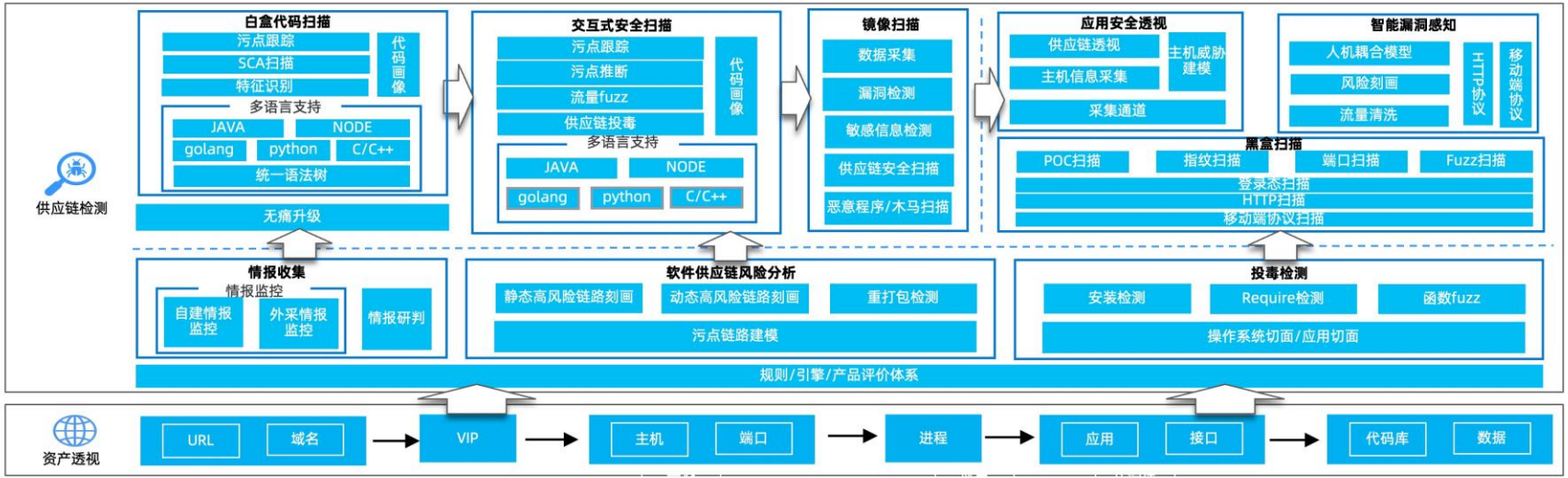
- NbSP零越范式以访问控制点为基础提出了四种不同的**攻击类别**:
  - ★ **B3攻击**: 预设的访问控制点被**完全绕过**, 攻击者能够任意读取或篡改敏感数据, 内存安全是一类重要的B3攻击类型
  - ★ **B2攻击**: 预设的访问控制点被**部分绕过**, 攻击者读取或篡改部分敏感数据, 一般不能绕过日志审计
  - ★ **B1攻击**: 功能**滥用**型 (OVTP)
  - ★ **B0攻击**: **拒绝**服务/资源耗费攻击 (ARCP)



② 蚂蚁软件供应链安全防护框架



② 软件供应链安全检测产品矩阵：1day排查与0day挖掘

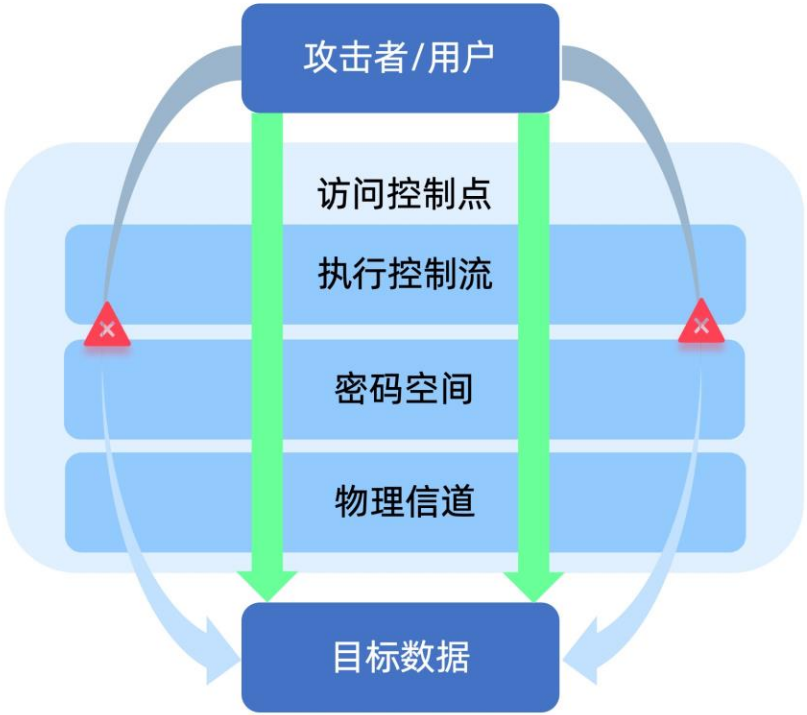


- 多维度交叉核查，供应链依赖，影响面排查
- 供应链本身风险的检测和发现，发现google、apache等多个基础组件的安全0day，以及20000+开源软件后门，已上报相关部门和相应社区

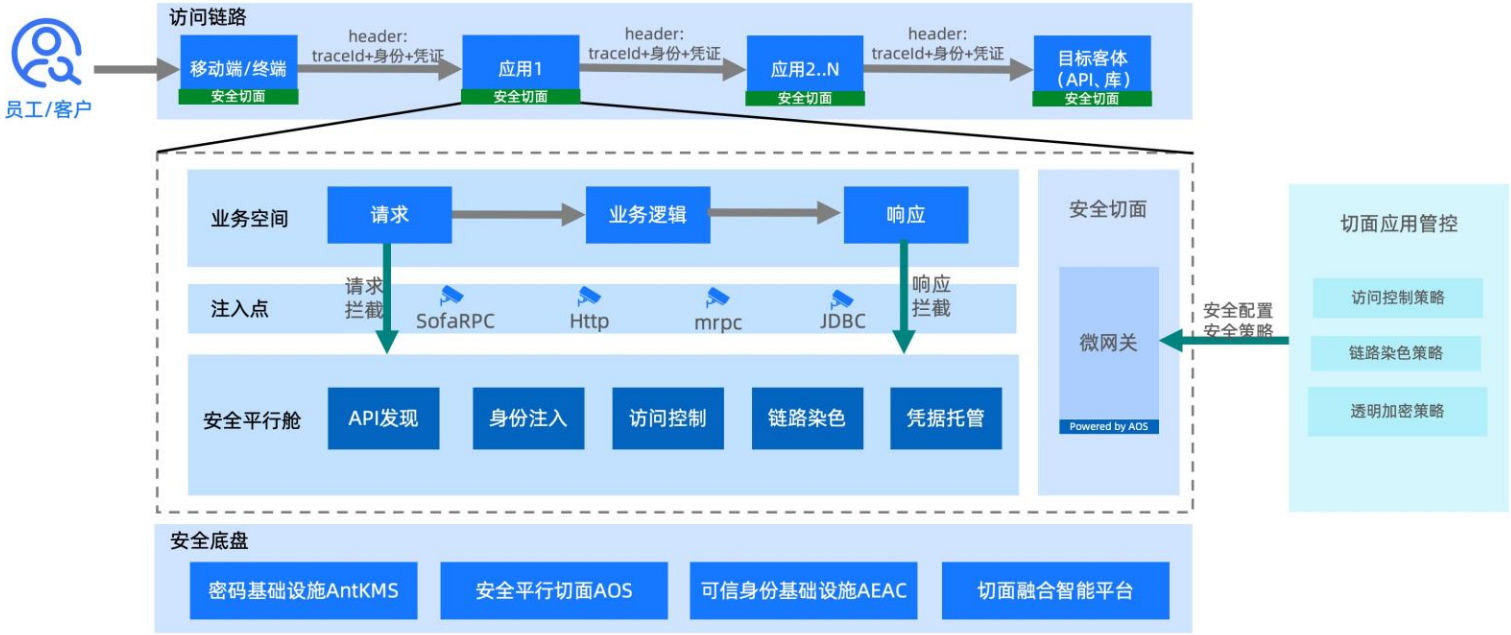
范式视角下的攻击分类 ③ OVTP鉴权安全

蚂蚁集团 ANT GROUP

- 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)



③ 切面微网关支持下的应用可信身份、密钥托管、业务凭证追溯



- 在应用空间内植入微网关能力，代理各类 请求（Http、JDBC、RPC），业务进出口流量动态感知，支持多协议流量按需采样
- 流量入口身份可进行身份鉴别，出口进行标识染色，从而实现OVTP链路刻画

小结：安全研发生命周期（SDL）

蚂蚁集团 ANT GROUP

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**

蚂蚁集团
ANT GROUP

安全度量

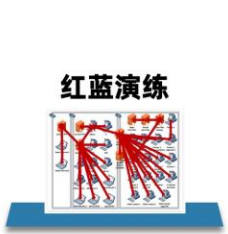
没出事，要你们安全干啥
出了事，要你们安全干啥

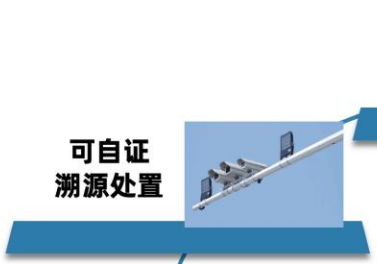
安全治理：网络安全复合治理成熟度模型

蚂蚁集团 ANT GROUP

战略要位，实战驱动，范式重构，技术破局

基线保障 → 关键能力建设 → 实战驱动 → 量化治理 → 范式演进





安全体系的度量：失效度量的技术视角

蚂蚁集团 ANT GROUP

- 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

量化治理：回顾“安全范式三问”

待评估目标：

- 控制：网络、系统、应用
- 资产：数据、资金、账号

安全技术评估三要素：

① 横：NbSP

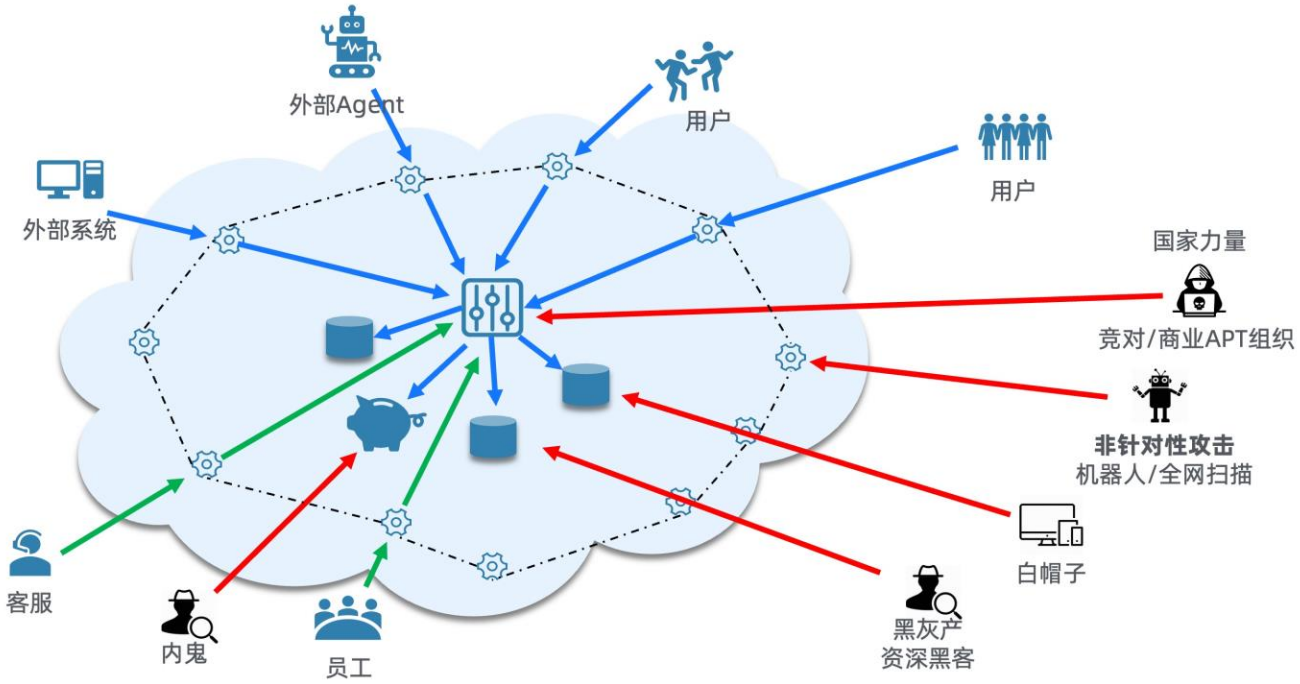
隔离是伪命题，但安全域间访问控制点收敛么？

② 纵：OVTP

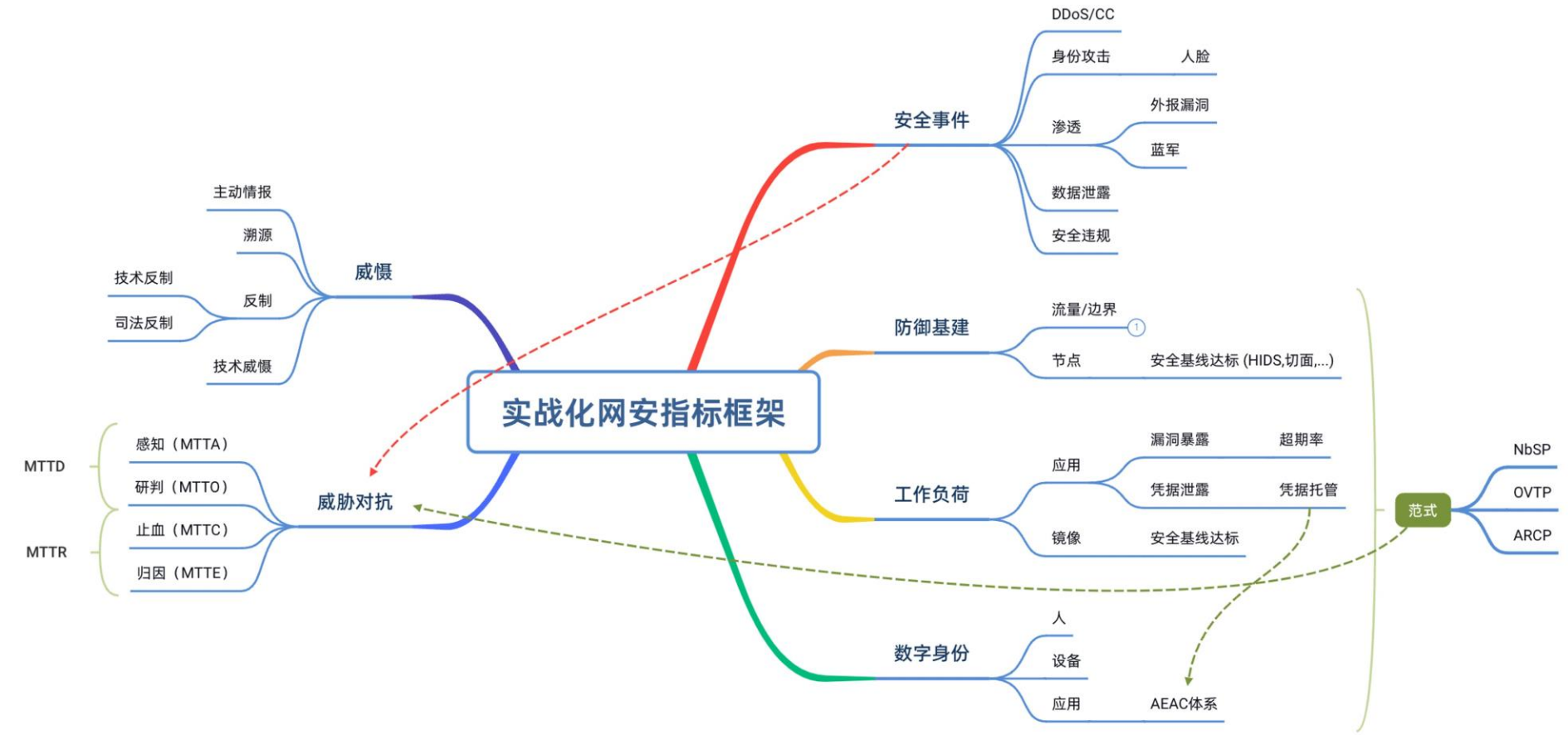
教科书过时了，但访问控制点上策略满足链路要素可溯么？

③ 动：ARCP

防守不可能完备、对抗不可缺失，但攻防对抗成本经济么？



量化治理：网络空间安全技术指标体系

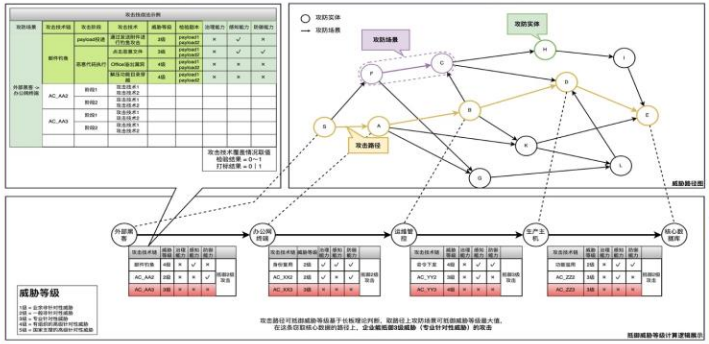


量化探索：基于威胁路径图的水位评估技术

蚂蚁集团 ANT GROUP

实战检验安全水位(全链路检验、安全产品检验、自动化检验等)

威胁路径图模型



威胁研究

- APT组织/事件/工具
- 金融业威胁研究(如信创)
- 资金/数据盗取研究

能力建设

- 漏洞挖掘利用(0Day、1Day)
- 安全水位检验平台(自动化能力)

实战检验

模拟黑客/内鬼

- 以盗取资金为目的
- 以盗取数据为目的

自动化检验

- 针对已知路径和攻击方法进行常态化的自动化检验，检验安全能力的有效性。

安全产品检验

- 通过对安全产品自身安全性、安全能力、安全策略进行体系化的测试，获得安全产品强度指标。

红蓝攻防检验

- 通过红蓝攻防检验，不断发现可能的攻击路径和新的攻击方法，拓展威胁路径图基础数据。

水位指标

网络安全域

- 网络安全域路径数：XXXX条
- 预防覆盖率 XX%，待覆盖高风险技术链 XX 个
- 感知覆盖率 XX%，待覆盖高风险场景 XX个
- 防御覆盖率 XX%，纵深防御能力覆盖率 XX%，待覆盖高风险场景 XX 个
- 可信防御覆盖率 XX%，可信纵深防御覆盖率 XX%，待覆盖高风险场景XX个

数据安全域

- 数据安全域路径数：XXX条
- 预防覆盖率 XX%，待覆盖高风险技术链 XX 个
- 感知覆盖率 XX%，待覆盖高风险场景 XX个
- 防御覆盖率 XX%，纵深防御能力覆盖率 XX%，待覆盖高风险场景 XX 个
- 可信防御覆盖率 XX%，可信纵深防御覆盖率 XX%，待覆盖高风险场景XX个

指导安全建设优先级

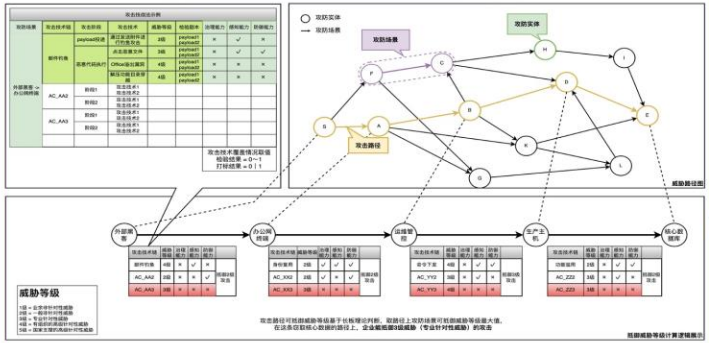
- 优先覆盖没有任何安全（预防、防御和感知）能力的攻击技术或场景
- 对预期可以覆盖而实际没有覆盖的能力，复盘排查根因

量化探索：基于威胁路径图的水位评估技术

蚂蚁集团 ANT GROUP

实战检验安全水位(全链路检验、安全产品检验、自动化检验等)

威胁路径图模型



威胁研究

- APT组织/事件/工具
- 金融业威胁研究(如信创)
- 资金/数据盗取研究

能力建设

- 漏洞挖掘利用(0Day、1Day)
- 安全水位检验平台(自动化能力)

实战检验

模拟黑客/内鬼

- 以盗取资金为目的
- 以盗取数据为目的

自动化检验

- 针对已知路径和攻击方法进行常态化的自动化检验，检验安全能力的有效性。

安全产品检验

- 通过对安全产品自身安全性、安全能力、安全策略进行体系化的测试，获得安全产品强度指标。

红蓝攻防检验

- 通过红蓝攻防检验，不断发现可能的攻击路径和新的攻击方法，拓展威胁路径图基础数据。

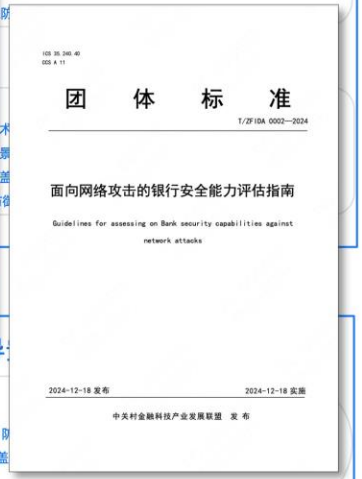
水位指标

网络安全域

- 技术链 XX 个
- 场景 XX个
- 覆盖率 XX%，待覆盖高风险场景 XX 个

指导

- 优先覆盖没有任何安全（预防、
- 对预期可以覆盖而实际没有覆盖



量化口径的游戏：Lies, Damned Lies and Statistics

蚂蚁集团 ANT GROUP

- 没有绝对的安全，但随意虚报、不明所以的安全指标是行业中更普遍的一种症候群

- 风险指标的分母：
  - 明确覆盖范围，特别是资产覆盖率
- 风险指标的分子：
  - 明确分子指标的定义，确认度量的准确性、及时性
- 指标的残差分析：
  - 当下没有覆盖的部分中，主要残留风险的定性分析
- 威胁的重入分析：
  - 黑产的重入成本，直接与ARCP范式强相关

量化指标的层次：业务指标，技术指标，产品指标，生态指标

蚂蚁集团 ANT GROUP

- 业务指标
  - 在具体业务场景中的应用效果指标
  - 安全业务指标的达成往往具有众多复杂的因素，包括运气因素
- 技术指标：度量技术进展
  - 能力指标，特别是技术目标分解后的支柱性技术能力指标
  - 技术指标需要体现技术能力的坚实挺进，不能用业务指标替代
- 产品指标：技术的承载体
  - 用户体验、成本、产品质量、可用性SLA、自服务能力等
  - 共同形成宏观层面的产品成熟度
- 生态指标：技术的应用范围
  - 社区规模，社会互助率，产业链健康度等

蚂蚁集团
ANT GROUP

总结

先进的安全能力，是业务持续发展的核心竞争力

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”
  - 各单位为了安全实战保障的实际投入占业务投入比例往往远远不达标
  - 真正阻碍业务发展的往往是“跟不上时代的合规要求”
- 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

结语：最大的漏洞是认知的缺失

蚂蚁集团 ANT GROUP

- **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
- **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
  - **基础设施：**基于安全平行切面的安全原生基础设施
  - **系统研发：**NbSP防绕过，OVTP可追溯，ARCP可对抗
  - **安全度量：**横NbSP，纵OVTP，动ARCP，残差分析，重入分析
- **企业安全的支柱：安全团队的专业度**
  - 避免企业走向安全与稳定性雪崩：预警、避免、消解、改造

谢谢

彩蛋