安世加

Face the challenge, Embrace the best practice

EISS-2023

企业信息安全峰会

上海站 2023.11.24

基于原生安全范式构建可信纵深防御体系

吴飞飞（**FEEI/止介**），支付宝（中国）CISO

2023.11

蚂蚁集团 ANT GROUP | 支付宝

蚂蚁集团 ANT GROUP | 支付宝

目录

蚂蚁集团 ANT GROUP | 支付宝

01重新审视现有**安全体系有效性**

行业安全风险现状：现有安全体系有效性到底怎么样？

防护结果上看不容乐观

- 十年前的“乌云”时代，你我都见过太多白帽子漫游各大企业内网，如入无人之境。
- 今天，各大企业SRC上还是不断看到高危漏洞奖励、HW中被打穿等...
- 以及各种APT中导致数据泄漏、资金盗取的安全事件

各企业都建立了自己安全红队，进行实战红蓝演练。这些演练的结果都是必然以红队成功盗取数据或资金结束。

甚至攻击方法没有太大变化

多数公司还是无法缓解针**社工钓鱼**、**0day**、**软件供应链**、**业务滥用**等攻击威胁。

攻防不对等：发现了风险，原因只有一个。漏过了风险，理由有无数个。

每当出现各类漏洞遗漏、数据泄漏事件、红队突破时，内部复盘时总是能听到无数的理由。

- 老板问反入侵，为什么这次红队入侵成功了？
- 反入侵问安全能力，为什么没拦截？
- 安全能力问SDL，事前为什么没检测出来？
- SDL问研发，为什么要写出这个漏洞？

- 反入侵排查，发现有告警没仔细运营
- 安全能力排查，发现这个资产是非标的，没法覆盖
- SDL排查，这是历史存量老接口
- 研发排查，这个功能是为了更好的用户体验而设计的

蚂蚁集团 ANT GROUP | 支付宝

网络安全有效性影响因素

安全责任范围是否明确

网络安全、**数据安全**、内容安全、反欺诈、反洗钱、业务安全

安全目标与指标的正确性

公司威胁与团队目标是什么（合法合规/非针对性扫描/业余白帽子/资深白帽子/**竞争对手**/**商业黑客组织**/**国家级组织**），所有人做的事情到底对控制安全风险是否有帮助？核心指标是否能真实度量安全水位？（正向指标/**负向指标**，过程指标/**结果指标**，内部指标/**外部指标**...）

安全体系的完备性与合理性

风险识别与优先级：已知风险/**未知风险**，**存量风险**/增量风险，软件风险/**硬件风险**，可控风险/**不可控风险（供应链/云底座/供应商...）**，外部攻击/**内鬼**，有特征风险/**无特征风险**，...

风险阶段与检验机制：事前威胁识别、安全意识提升、上线前规避机制、**上线后防护能力**、攻击时感知与应急，甚至事后的**溯源打击**等。还有组织保障层面，规章制度/政策合规等。模拟实战进行**充分**、**持续**的红蓝演练。

安全资源投入度与重点风险匹配程度

安全资源（安全人员、安全预算）与上面三部分以及企业资产规模（资金规模/数据敏感量级/应用数量/研发数量/员工数量/业务开放范围...）的**匹配程度**，**优先级**与**建设周期**平衡。

安全能力与风险匹配度

是否**所有的安全风险类型**都有对应的**安全检测、防御、感知能力**或机制保障？以及可以保障到什么**程度**？

能力与运营有效性

是否**所有**规则有效、是否能覆盖**所有**资产，是否能得到**及时**运营处置，是否在**真实威胁**下可以**持续**有效。

高威胁、高度复杂且体量巨大的业务场景下安全技术困境

威胁等级

国家力量

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

APT

社工钓鱼

0day

业务滥用

供应链威胁

数据盗取

常规漏洞

…

Q1：每个人对于安全怎么做，每个安全产品如何实现安全需求都有不同的理解
有没有一种指导原则，让大家统一认识和实现？

数十
安全产品

数百
安全人员

数万
安全策略

Q2：有没有一种能统一各层面安全产品的技术实现方式？

千级
域名

万级
应用

十万级
接口

百万级
容器

供应链

亿级
用户

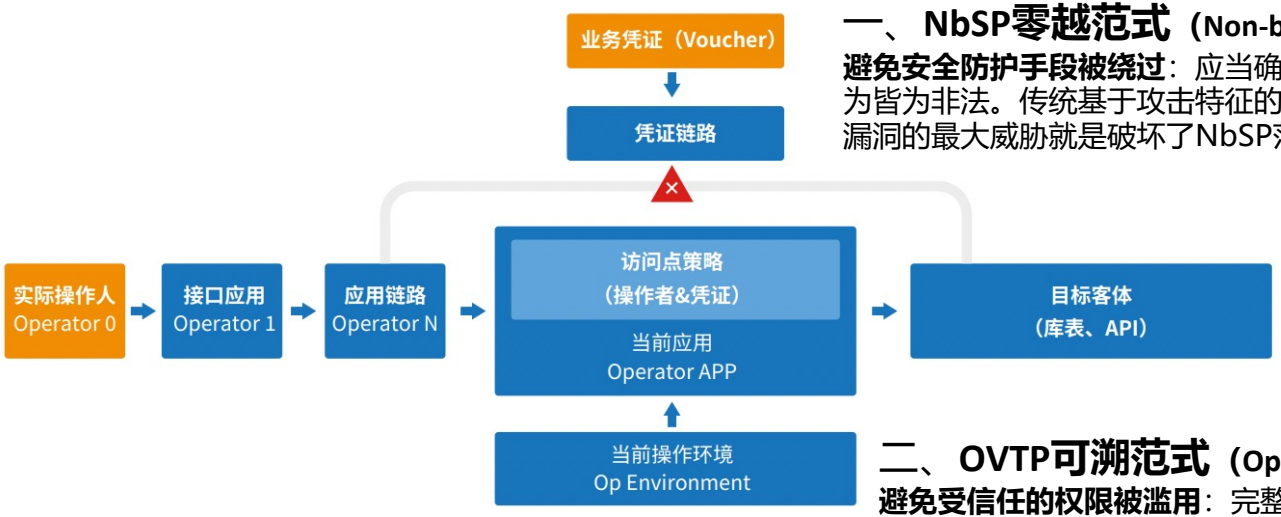
万亿级
资金

蚂蚁集团 ANT GROUP | 支付宝

02原生安全范式：指导安全体系建设

原生安全范式：指导所有安全能力建设

蚂蚁集团基于大量安全领域创新探索实践，由副总裁、首席技术安全官韦韬提出两项安全范式指导安全体系建设



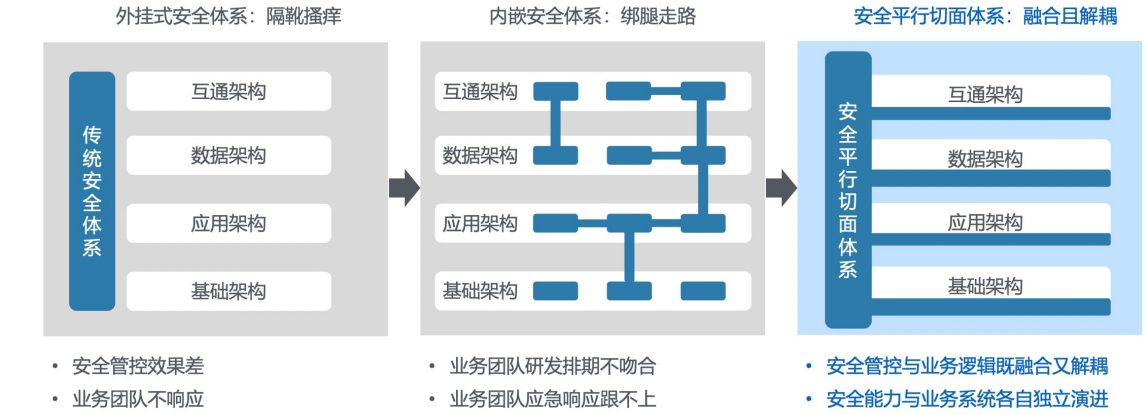
一、NbSP零越范式（Non-bypassable Security Paradigm）

避免安全防护手段被绕过：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。传统基于攻击特征的防御、软件内存安全漏洞、ODD反序列化等漏洞的最大威胁就是破坏了NbSP范式，从而破坏了OVTP范式。

二、OVTP可溯范式（Operator Voucher Traceable Paradigm）

避免受信任的权限被滥用：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)。传统的 RBAC、云AK机制、零信任 都没有认知到这个核心范式，缺乏对这个范式的支持。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

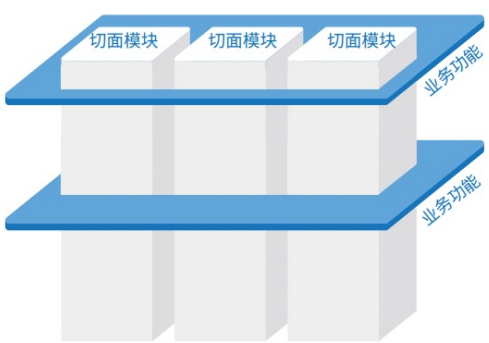
安全平行切面：高效、精细的观察和干预能力



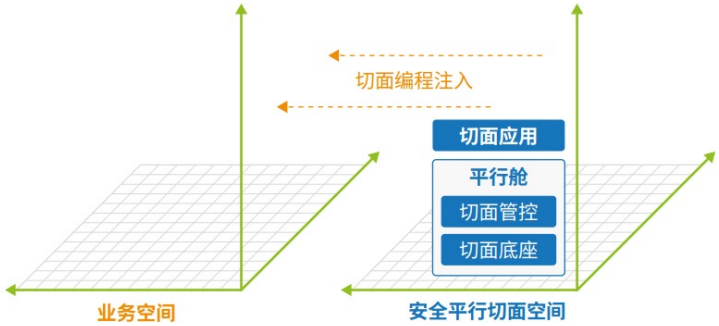
- 安全管控效果差
- 业务团队不响应

- 业务团队研发排期不吻合
- 业务团队应急响应跟不上

- 安全管控与业务逻辑既融合又解耦
- 安全能力与业务系统各自独立演进



AOP面向切面编程

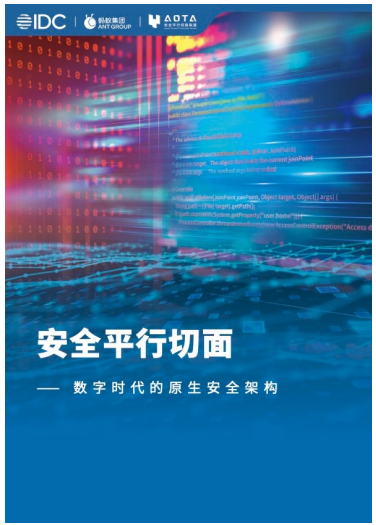


切面安全应用逻辑与业务应用逻辑解耦，
又通过插桩或者AOP机制，将安全能力融入到业务应用系统中

实现业务解耦、精细观测、追溯以及精准阻断

万物可切，更高效和精细的观察与干预能力

在资产采集、漏洞发现、攻击拦截、入侵检测以及数据治理等方面有巨大提升。

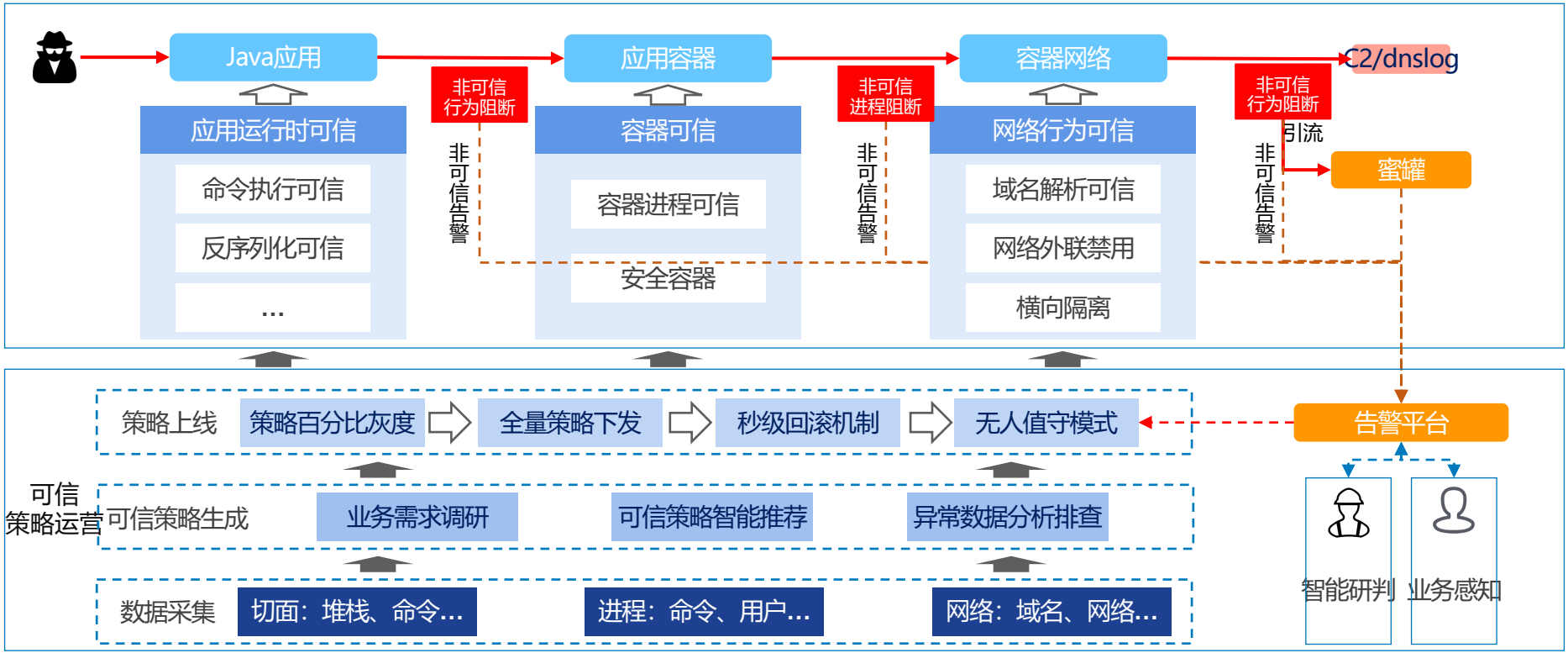


安全平行切面白皮书2.0

蚂蚁集团 ANT GROUP | 支付宝

03可信纵深防御在0day和数据保护实践

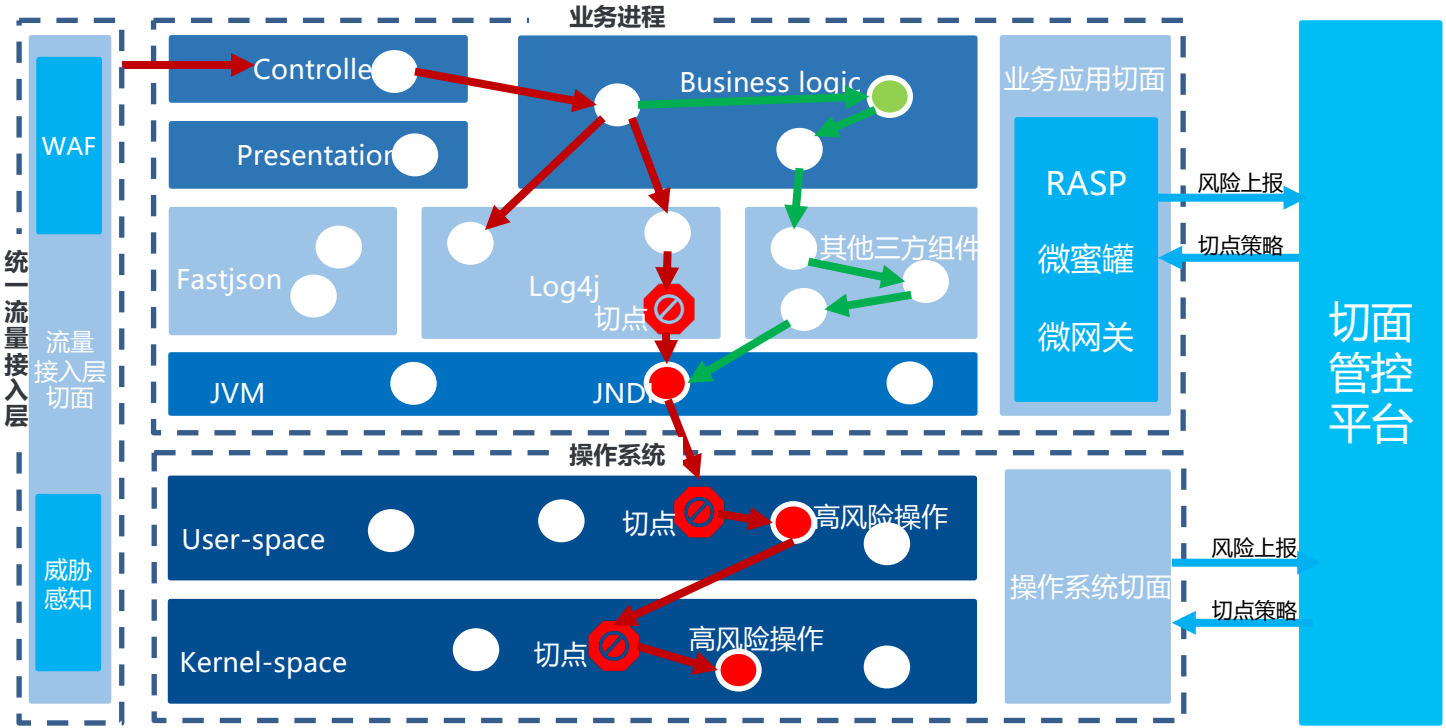
充分利用甲方内部数据的优势，实现行为可信能力，摆脱攻防不对等
所有安全能力逐步从基于攻击特征的防御模式升级至基于行为可信的防御体系



基于安全平行切面和原生安全范式，在常规0day漏洞防护实践

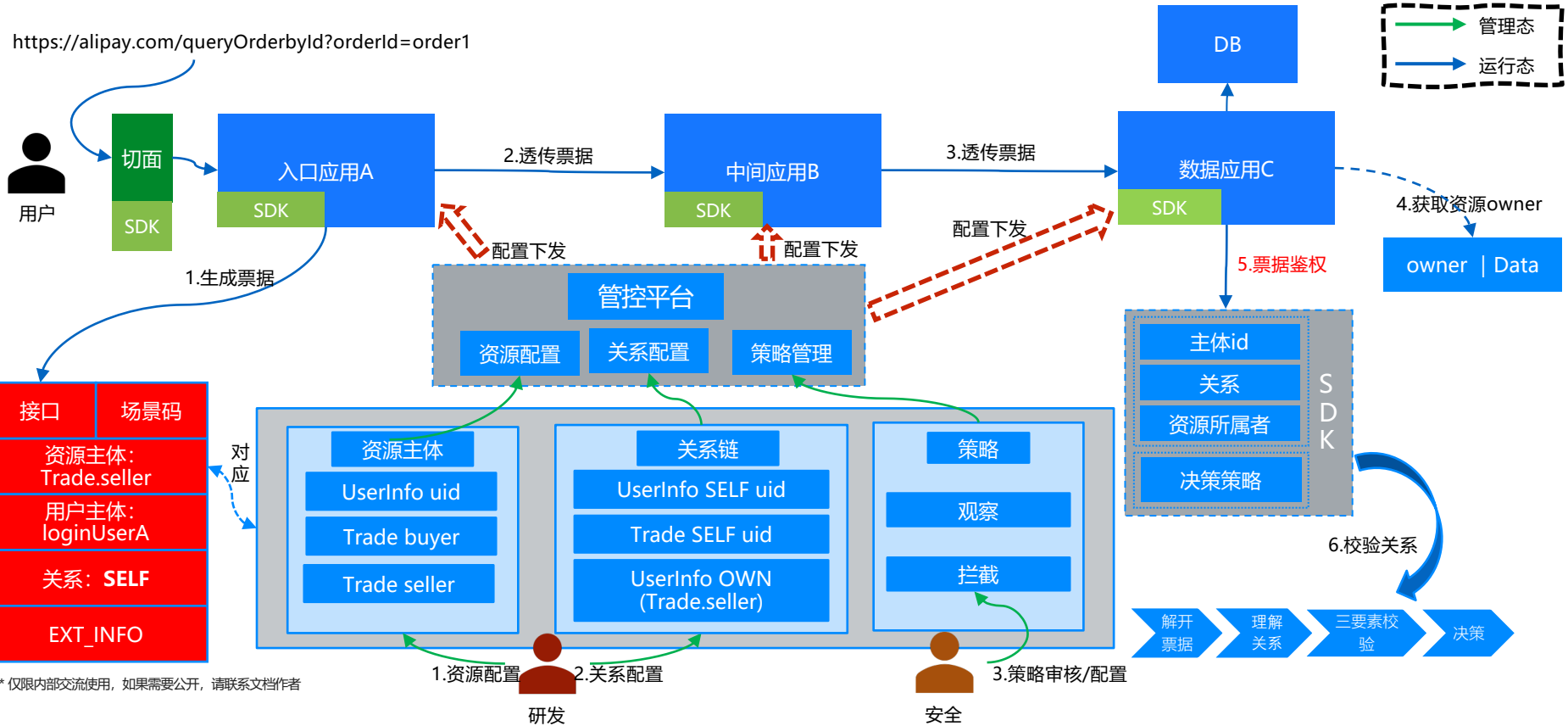
免疫常规0day漏洞，拦截40+万次Log4j2 RCE，0误拦截，0漏拦。

平行止血加固，应急业务0打扰。部署100w+容器，双十一不降级。



基于关系票据的水平越权防护方案

技术层实现所有数据只能被数据所有者及其授权者访问，逐步替换掉代码任意调用即可访问任何数据风险
不仅仅能解决互联网边界应用，也能逐步替换掉办公网管理后台基于角色的权限体系



* 仅限内部交流使用，如果需要公开，请联系文档作者

THE END

THANK YOU!

Feei <feei#feei.cn>, WeChat: FEEI_WU

Read more： https://feei.cn/building-a-trusted-in-depth-defense-system-based-on-native-security-paradigm/

蚂蚁集团 ANT GROUP | 支付宝

关注我们

安世加 专注于网络安全行业，通过互联网平台、线上线下沙龙、峰会、人才招聘等多种形式，致力于创建亚太地区最好的甲乙双方交流学习的平台，培养安全人才，提升行业的整体素质，助推安全生态圈的健康发展。

安世加