# 机密计算技术与龙蜥社区云
# 原生机密计算SIG

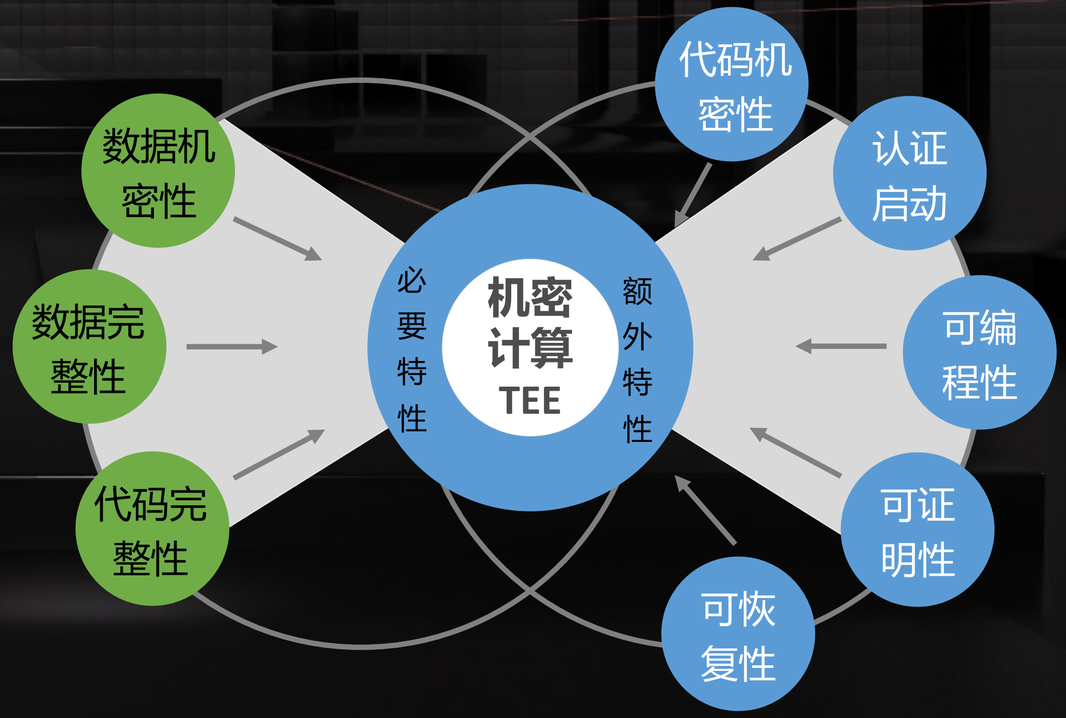
达摩院操作系统实验室系统安全
乾越

# 什么是机密计算？

一种通过具有通用计算能力的硬件可信执行环境（Trusted Execution Environment，即TEE）对使用中的数据提供安全保护的计算模式，其可信执行环境应具有可编程能力，实现数据的可用不可见。


**隐私计算与机密计算的关系**

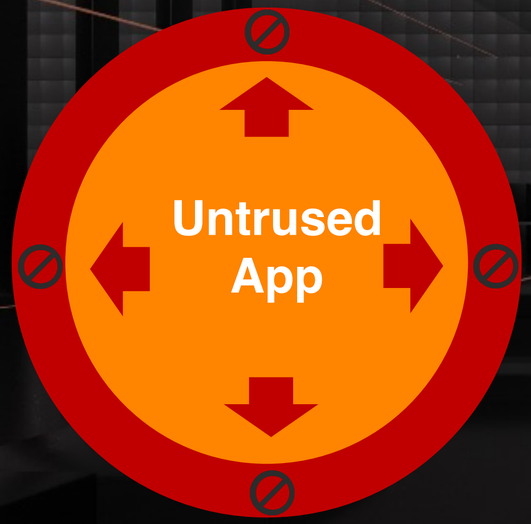
- 隐私计算是一种面向隐私信息全生命周期保护的计算理论和方法。
- 机密计算是隐私计算方法论中的一种解决方案。



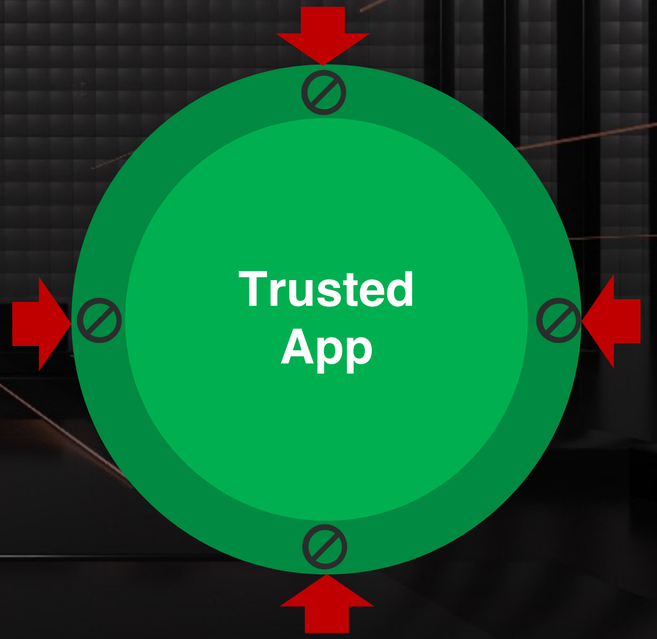
# 机密计算TEE技术与传统虚拟化隔离技术的关系

运行时安全

虚拟化（VM）




机密计算（TEE）



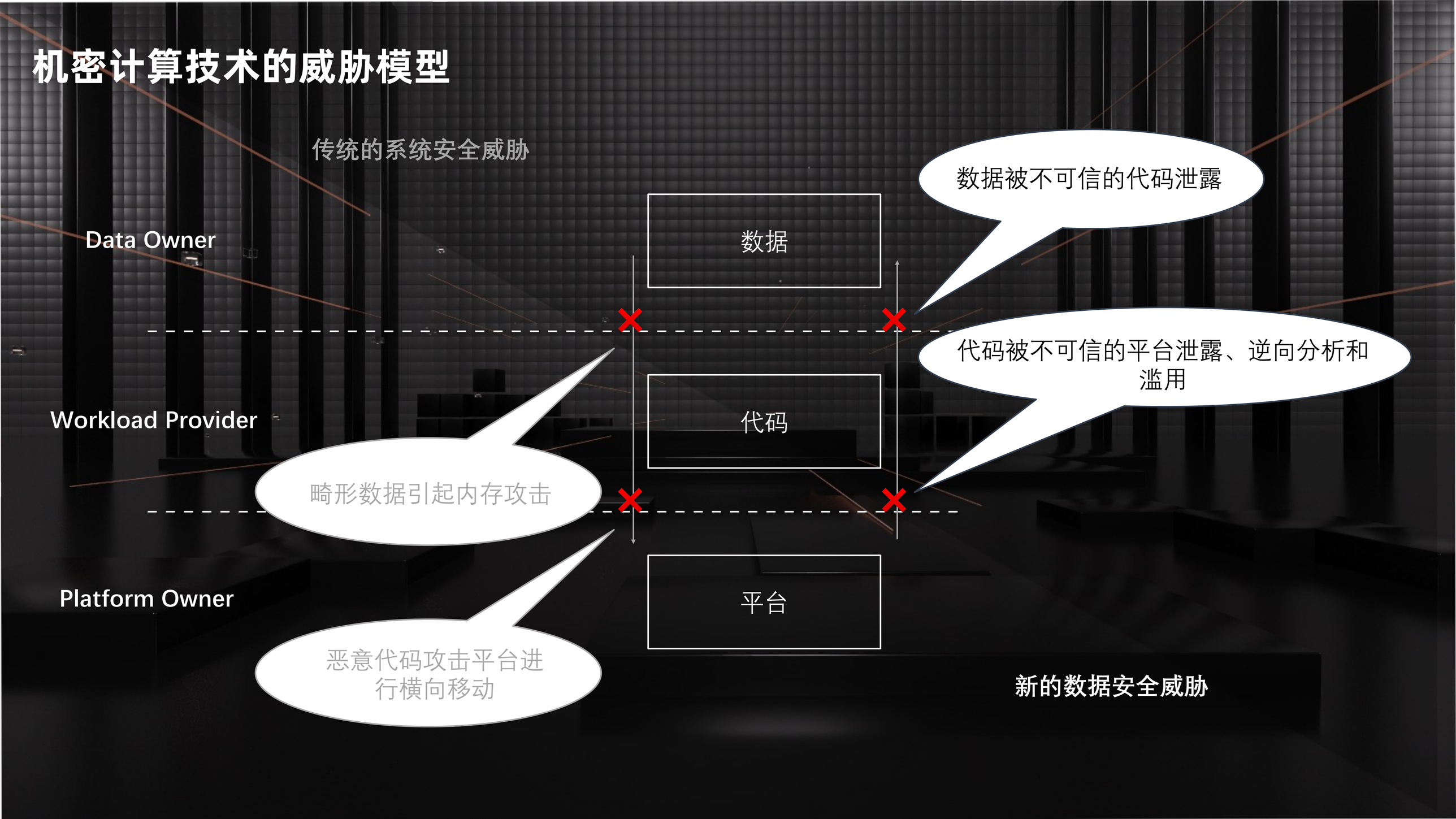

**隔离**

CSP的视角：不可信的多租工作负载隔离以及性能和故障隔离

**保护**

数据拥有者的视角：保护敏感代码和数据，防止来自CSP的非授权访问

# 机密计算技术的威胁模型



# 机密计算技术的发展趋势：机密互联

让机密计算不再局限于CPU TEE单点技术，而是在多个维度建立端到端的安全可信与互联互通

| 01 | 02 | 03 | 04 |
| --- | --- | --- | --- |
| 确保设备总线上传输的敏感数据的安全性 | 确保在位于后端的“小TEE” 中执行更为敏感的本地操作 | 确保移动端的敏感数据在云端被安全可信地保存和处理 | 确保机密计算技术的平台互通性 |
| 单节点上CPU与Device间 | 单节点上大小TEE间 | 平台特定的TEE节点间 | 任意TEE节点间 |

实现机密互联的技术手段：Attestation

# 龙蜥社区云原生机密计算SIG（CNCC）

https://openanolis.cn/sig/coco

- 使命和目标
  - 构建云原生机密计算开源技术栈，降低机密计算的使用门槛，简化机密计算在云环境上的部署和应用，拓展使用场景及方案。
- 定位
  - 定位于云原生机密计算底层基础设施，专注于机密计算底层技术。

| | |
|---|---|
| 解决方案 | **Confidential vTPM** / Intel CCZoo（TensorFlow横向联邦学习、在线推理服务、隐私集合求交） / **机密计算软件供应链安全服务** |
| 运行时 | **Enclave-CC** / Gramine / 海光CSV机密容器 / 海光CSV机密虚拟机 / **Occlum** / SEV机密容器 / SEV机密虚拟机 / SGX虚拟化 / **TDX机密虚拟机** |
| 编程框架 | Apache Teaclave Java TEE SDK / Intel HE Toolkit / Intel SGX & PSW & DCAP / **RATS-TLS & librats** |
| OS适配 | Anolis 8 + ANCK 5.10 / **Anolis 23** + **ANCK 6.1** |
| 硬件支持 | AMD SEV(-ES)+**SNP** / **Arm CCA** / 海光 CSV 1+2+**3** / Intel SGX 2.0 / Intel TDX 1.0+**1.5** |

- 已支持
- 今年提供支持

# 外部开源活动

- 开放原子开源大赛赛题《基于CPU TEE的SPDM通信协议实现》：https://competition.atomgit.com/competitionInfo?id=8aff7160f0a511ed99d49fc42bfa011c
  通过在CPU TEE远程证明场景中复用SPDM规范定义的标准化消息协议，SPDM消息协议能够提供了一种建立信任的CPU TEE身份认证机制，该机制使用经过验证的加密方法来保护CPU TEE的身份认证过程。

- 面向学生的学术合作项目《TEE Network Gateway》：https://talent.alibaba.com/campus/position-detail?lang=zh&positionId=2016102
  在客户端网络和服务端网络之间通过各自的数据网关建立基于机密计算远程证明技术的安全隧道，并在该安全隧道中封装来自客户端网络的任意网络协议负载，避免两端的已有应用和服务为支持机密计算远程证明协议而修改代码。

机密计算技术专栏：
https://www.zhihu.com/column/c_1444632556466044928

龙蜥社区云原生机密计算SIG

# THANKS !