2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

内生安全 从安全框架开始

ENDOGENOUS SECURITY:
STARTING FROM A CYBERSECURITY FRAMEWORK

云原生下安全方法的重新构建

———私有云原生安全的未来思考

嘉宾照片

林晓明

奇安信 战略咨询规划部

- **云原生对金融机构网络安全工作的影响**
- 云原生安全工作方法的“7个重构”
- 金融云原生下的“内生安全”理念

越来越多的金融机构在靠近云原生

- 云原生代表了一系列新技术，包括容器编排、微服务架构、不可变基础设施、声明式API、基础设施即代码、持续交付/持续集成、DevOps等，且各类技术间紧密关联。
- 过去云的发展极大提升了数据中心的运行效率，而今天的云原生直接面向开发者提供服务，透明化了基础设施运行环境，屏蔽了运行稳定需求与业务快速变化之间的矛盾。

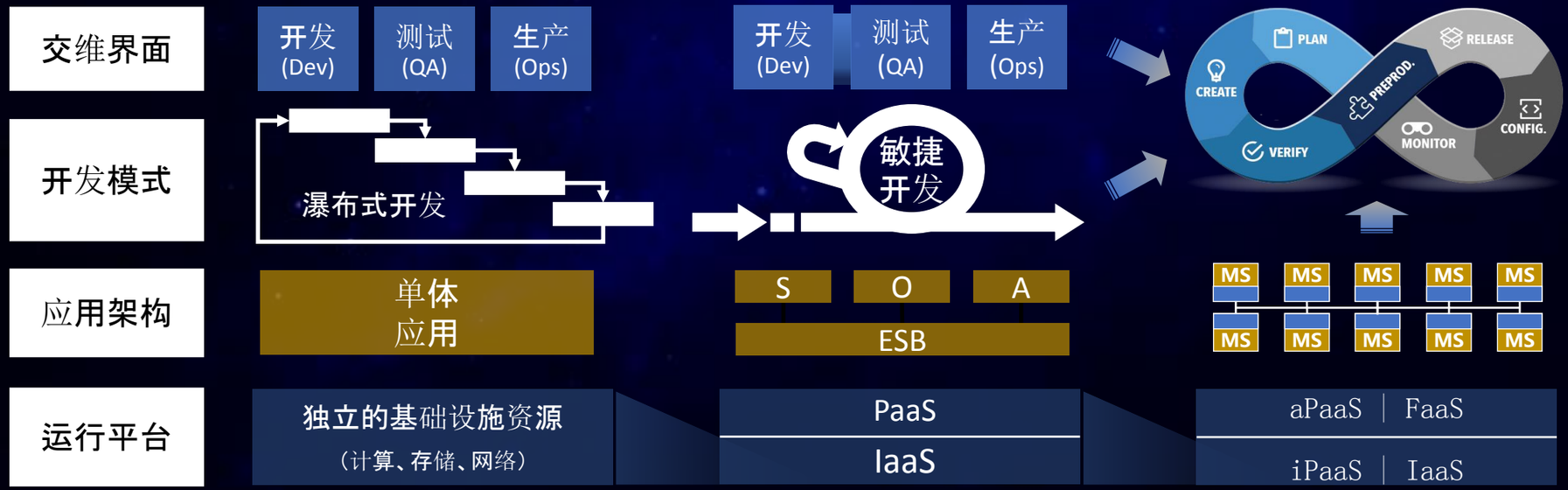
金融机构采用云原生的驱动力：

- 开发运行环境一致性
- 业务敏捷与弹性化
- 高度的容错性
- 助力企业的中台建设
- 混合云部署

云原生发展过程中的阻碍：

- 大量新技术与开源软件
- 与传统单体应用、SOA应用架构不完全兼容

云原生开始重新定义IT组织的多个方面



云原生表面上是资源的高度集中，而背后是对组织协作方式的变革，从组织责任边界（交维边界），产品迭代（开发模式），业务设计（应用架构）到数据中心基础设施（运行平台）都产生了影响。最常见的是数据中心的运维职责变化。

云原生对安全团队带来的挑战

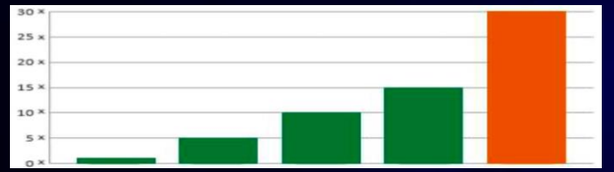
- **技术挑战**：云原生引入了大量基础设施新技术，导致安全工作者理解难度增加，云越来越像个黑盒，过去的安全工作多数只是围着核心业务外围转。
- **组织挑战**：安全建设和云基础设施关系紧密，导致安全职责需要重新考虑，安全组织和信息化其他组织的关系无法简单定义为谁主管、谁建设、谁负责。
- **能力服务化挑战**：应用上云后也会的提出安全服务化的诉求，开发团队短期找不到现成的安全服务时，可能自行使用开源安全工具，但却难于兼顾安全责任。

- 云原生对金融机构网络安全工作的影响
- **云原生安全工作方法的“7个重构”**
- 金融云原生下的“内生安全”理念

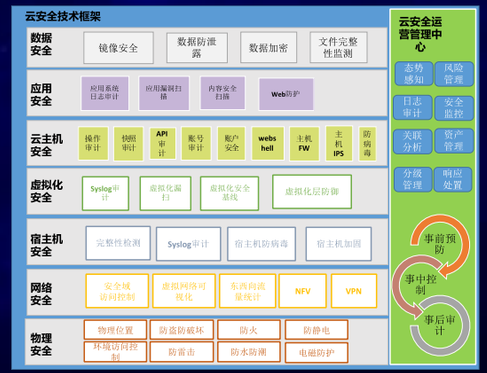
1.不可变基础设施导致安全的“重新左移”

当前

来源：US National Institute of Standard and Technology

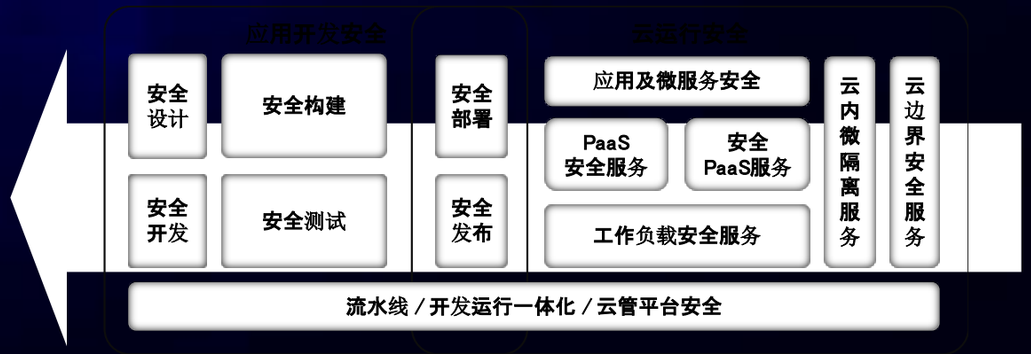


培训	需求	设计	编码	测试	发布	响应
• 安全意识培训 • 软件安全培训 • 进阶安全培训	定义安全需求	制定安全设计需求	使用批准的工具	动态代码测试	事件响应计划	执行事件响应计划
	制定质量门	分析攻击面/缓解措施	禁用不安全的函数和组件	模糊测试	最终安全评审	
	进行安全和隐私风险评估	使用威胁建模	静态代码分析	攻击面评析	发布和存档	



- 资产安全漏洞及基线问题从开发阶段开始关注
- 定期对运行环境进行安全扫描发现资产安全风险
- 在运营过程中，发现漏洞需要及时协同运行团队进行修复
- 运行态的安全基本上与开发态的安全工作相互割裂

未来



- 资产的安全变更及安全服务的选择，也需要在开发阶段执行
- 未发布时，需要定期在镜像仓库及制品库进行安全检查
- 上线发布即安全，脆弱性修补通过开发重新部署完成
- 对运行发现的安全问题需要在开发测试环境的进行持续跟踪

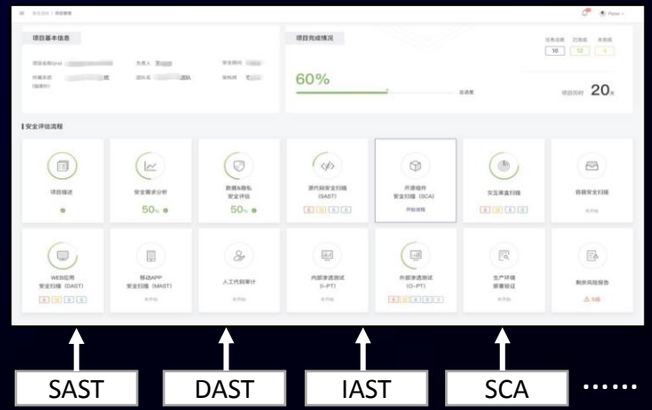
2. 面向开发全流程安全的“重新构建”

当前

- 在开发过程中有大量安全检测工作需要人工介入
- 安全测试卡点主要出现在上线前的上线部署环节
- 应用构建安全主要关注编译环境与代码安全问题
- 大量零散的安全工具相互孤立，没有形成整体

未来

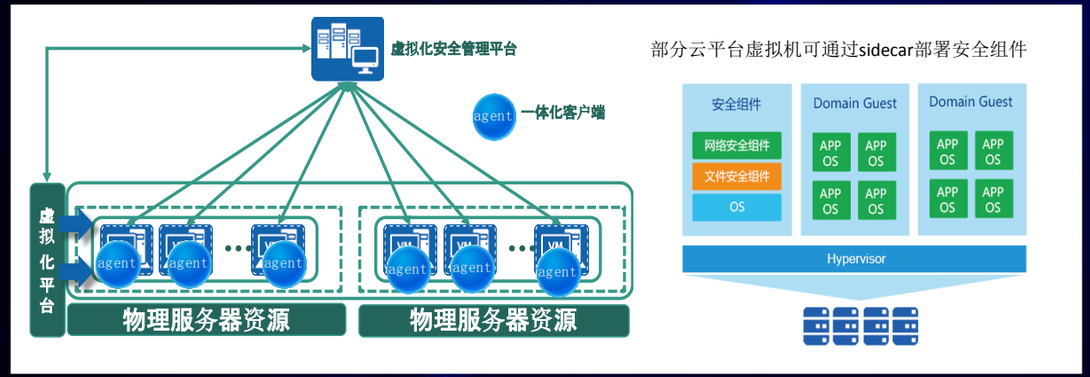
开发项目安全看板管理



- 自动化是所有安全工具集成到流水线的前提
- 在DEV/SIT/UAT各个阶段集成必要的安全测试
- 应用构建安全还需要考虑基础镜像、依赖库、构建过程等安全问题
- 形成基于不同开发项目在各阶段的研发安全看板管理

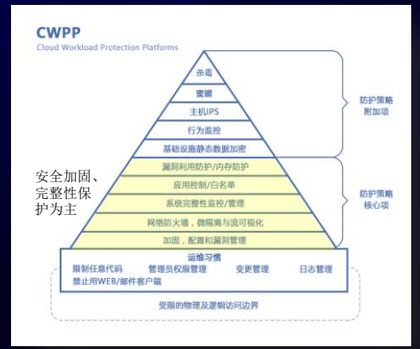
3. 容器化工作负载安全的 “重新部署”

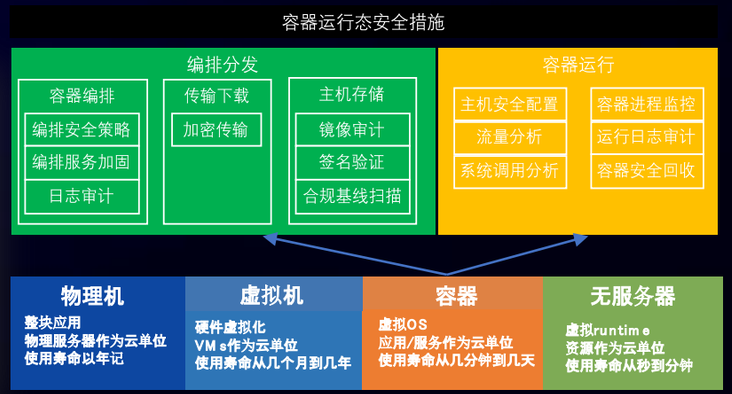
当前



- 以物理机、虚拟机为主的云工作负载安全
- 以防病毒、主机入侵防护为主的工作负载安全
- 主机应用安全软件部署/升级大多在运行态完成
- 主机系统安全软件直接嵌入到操作系统内部

未来



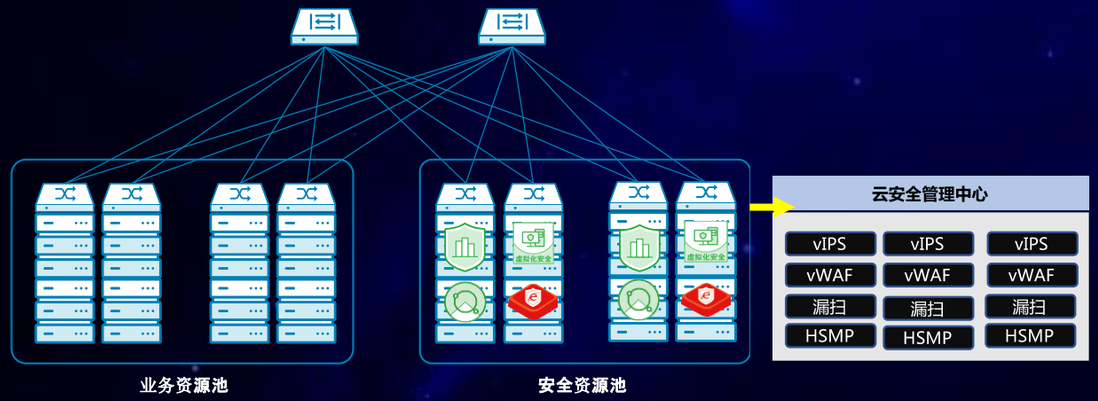


容器虚拟机/应用虚拟机

- 容器安全和Serverless安全需要重新考虑
- 以安全加固、完整性保护、异常检测为主的安全防护
- RASP等安全软件的部署可以打包进Docker file进行镜像构建
- 虚拟机和容器的安全都通过Sidecar部署，对应用无侵入
- 不同安全等级的容器编排至对应的Ingress入口

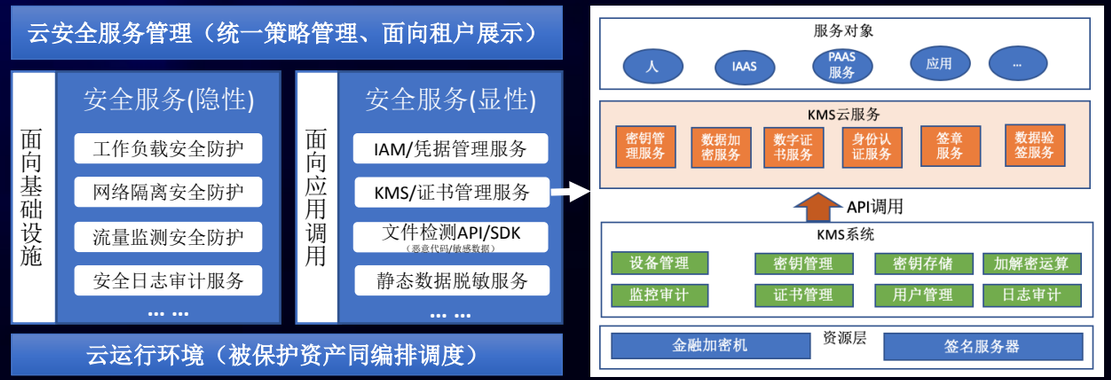
4. 云运行环境安全服务化的“重新思考”

当前



- 私有云的安全能力基本以虚拟化的安全设备为主
- 安全防护资产信息难于与云资产信息进行打通
- 入侵防护、WAF、安全审计等安全服务直接面向租户提供策略管理
- 大量安全服务的云内集成很多时候变成租户的困扰

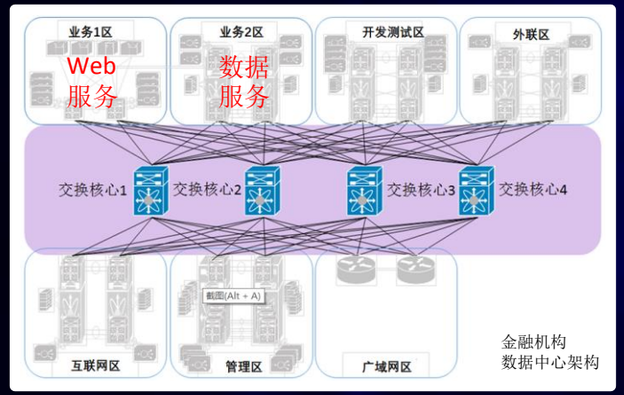
未来



- 私有云的安全服务本身需要原生化，充分利用云的弹性计算能力，并形成安全资源部署与云内资源管理、编排调度的协同。
- 安全策略集中管理控制，隐性安全服务只为租户提供结果展示
- 需要考虑安全显性化服务，IAM、KMS、凭据及证书管理、恶意代码/敏感数据检测API或SDK等，显性化服务的特点是直接可被应用调用

5. 云内基于业务属性横向隔离的“重新设计”

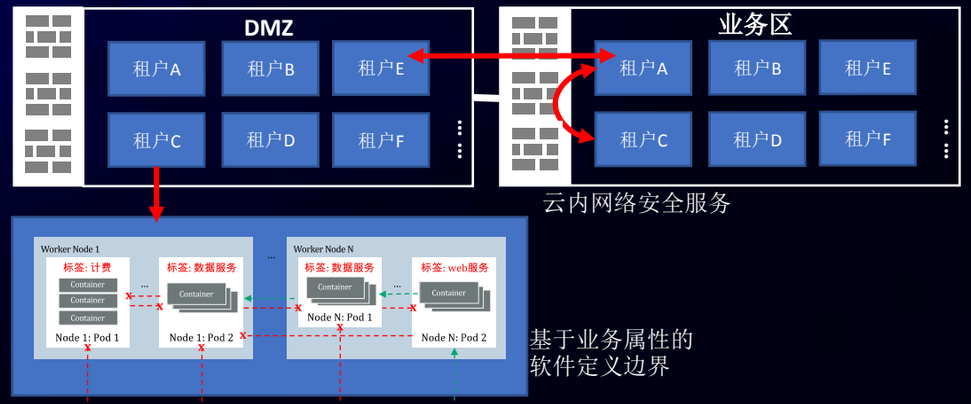
当前



- **业务区**：用于部署各类服务器；
- **开发测试区**：用于业务系统上线前的开发测试；
- **互联网区**：用于部署互联网业务；
- **外联网区**：用于部署与第三方外联机构业务；
- **广域网区**：用于与内部分支机构互联；
- **管理网区**：用于数据中心内部网络管理；

- 传统数据中心第一层隔离逻辑基于网络区域属性实现安全访问控制
- 云数据中心通过双层（物理+VPC）网络构建多租户网络基础设施
- 容器网络和微服务通讯架构的出现增加了数据中心网络复杂性
- 传统网络隔离机制在新的数据中心无法继续沿用，安全边界模糊化，

未来

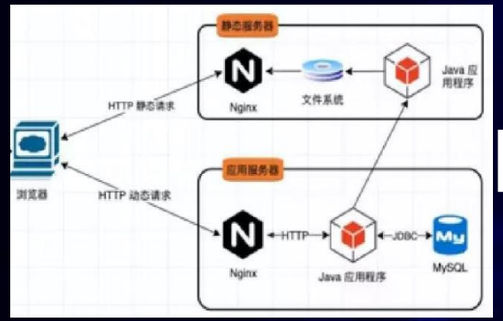


- 云数据中心的第一层隔离逻辑是基于业务单元（租户）资源隔离
- 大规模数据中心环境容器网络下沉至虚机网络是主要方向
- 基于业务属性标签进行安全访问控制隔离将是主要机制
- 租户内虚机/容器网络基于属性的微隔离，VPC间安全防护隔离、DMZ与业务域间安全防护隔离是云内实现隔离的主要位置

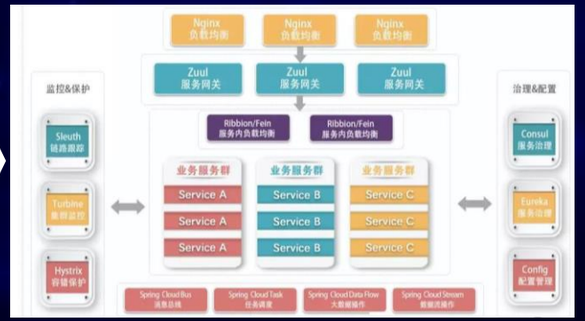
6. 微服务框架下服务安全边界 “重新定义”

当前

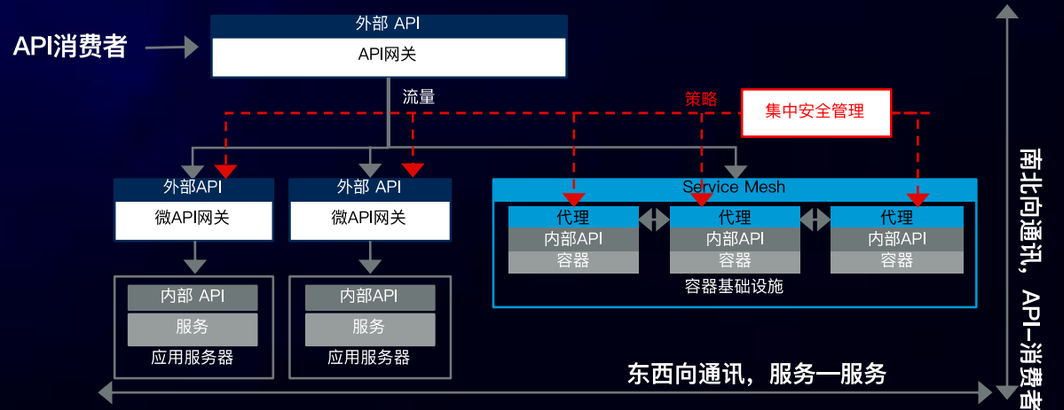
单体应用架构



微服务架构



未来



- 单体应用基于微服务理念进拆分，使用松耦合应用开发框架
- 侵入式（Spring cloud）微服务架构向无侵入式（服务网格）发展
- 越来愈多的API/SDK对内开放的同时还需要对外进行开放
- 安全防护仅仅依赖企业互联网边界过去的安全能力建设

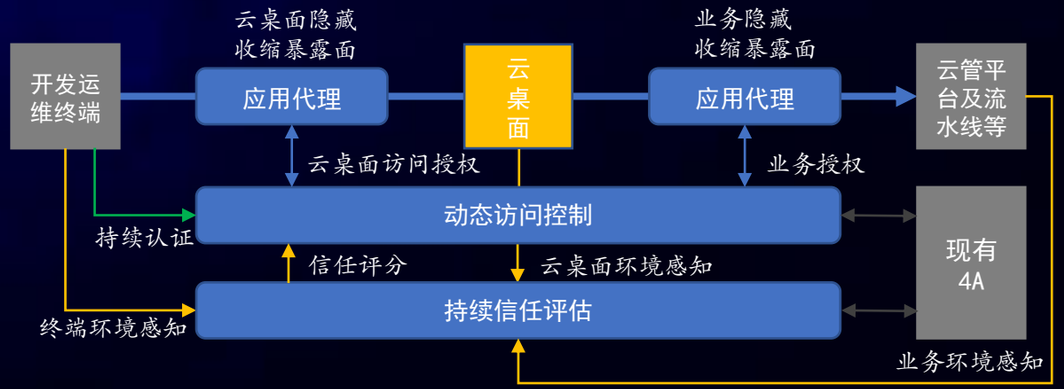
- 开放服务安全形成面向互联网，组织内，微服务架构内三层边界
- 微服务内部，服务治理与微服务安全访问控制的整合
- 微服务外部，实现面向三方访问场景的认证授权架构OIDC
- API与Web威胁防护在WAF侧能力的集成（WAAP）

7. 金融云各类访问通道的“重新建设”

当前

- 开发及运维接入包括互联网远程、办公网、生产网直接接入等
- 主要以转入NAC和VPN为主的接入控制方法
- 面向云生产环境、研发流水线平台的运维通道
- 研发人员的开发测试环境的接入通道

未来



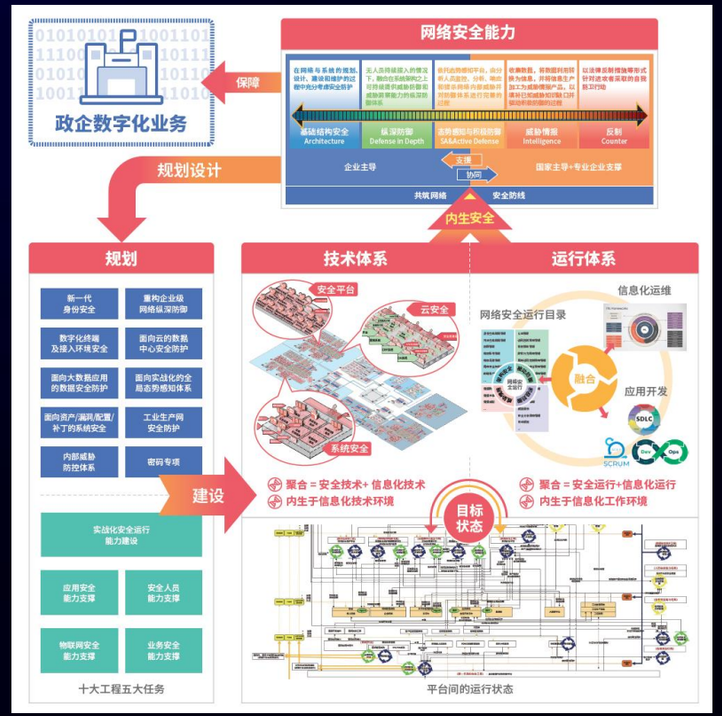
- 互联网远程的开发与运维接入变成后疫情时代的主旋律
- 确保无论从互联网接入还是办公网接入都具备相同的安全控制措施
- 基于接入过程的风险变化实时对访问的授权进行动态控制
- 简单化的用户体验与基于零信任的安全访问控制

- 云原生对金融机构网络安全工作的影响
- 云原生安全工作方法的“7个重构”
- **金融云原生下的“内生安全”理念**

“内生安全”理念指导云原生安全落地

- **开发运行一体化安全**，在开发测试与运行阶段的需要安全能力的一致性
- **安全与信息化的协同**，云原生安全建设运行需要与相关的IT组织高度协同
- **安全基础设施透明化**，大部分安全措施需要如云基础设施一样对应用透明
- **软件定义的原生安全**，在云高度软件定义的当前，安全也需要软件定义
- **安全能力内生于云上**，PaaS能力建设代表了企业中台化能力，安全也需PaaS化

从局部整改为主的外挂式建设模式走向深度融合的“内生安全”建设框架模式。



谢谢