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

金融行业内生安全详解和实践

嘉宾照片

主持人/嘉宾

嘉宾名字

嘉宾介绍嘉宾介绍嘉宾

现有网络安全体系普遍问题

缺乏体系化，在理论层面**缺乏与EA、ITIL同等层次的**、以系统工程思想引导的规划与建设实践，导致形成了以“局部整改”为主的安全建设模式，致使网络**安全体系化不足、碎片化严重、协同能力差、可弹性恢复能力严重缺失。**

局部整改**造成惯性的认知，安全就是买盒子、应对检查。**本质上是缺乏对网络安全系统性、动态性的理解，**看不清网络安全体系的全景框架**，随着数字化业务对安全要求提高，机构对做好数字化时代的网络安全，普遍缺乏信心。

网络安全需要进化到“内生安全”时代，从单一的围墙式的防护，演变为与业务系统融合的多重、多维度防御。要以“三同步（同步规划、同步建设、同步运行）”为机制保障，以三个聚合（技术聚合、数据聚合、人的聚合）为落地保障。

构建内生安全体系

问题导向、框架引导、保障业务

- **体系化建设的前提，是能够体系化的识别出网络安全存在的问题。**
- **用安全能力全景框架引导，确保分析问题的准确性、全面性。**

网络安全亟需向新模式升级

以“一体之两翼、驱动之双轮”作为其信息化和网络安全的战略定位，**以“统一谋划”作为落实“四统一”的起点**，在做好“关口前移”的基础上，进一步加强安全与信息化融合。

将“局部整改”模式转变为体系化规划建设模式，以**系统工程方法论**来指导网络安全体系的规划、设计和建设工作。

新一代网络安全框架

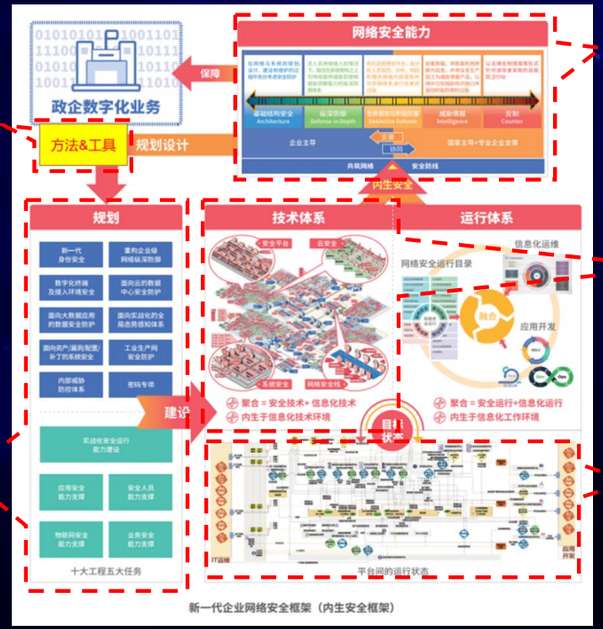
- 面向“十四五”期间的网络安全规划“十大工程、五大任务”建议框架
- **“甲方视角、信息化视角、网络安全全景视角”**出发的顶层规划与体系设计思路与建议。

框架的内涵

组件二：安全规划方法论与工具体系

组件三：组件化安全能力框架

组件四：规划纲要



组件一：安全能力体系

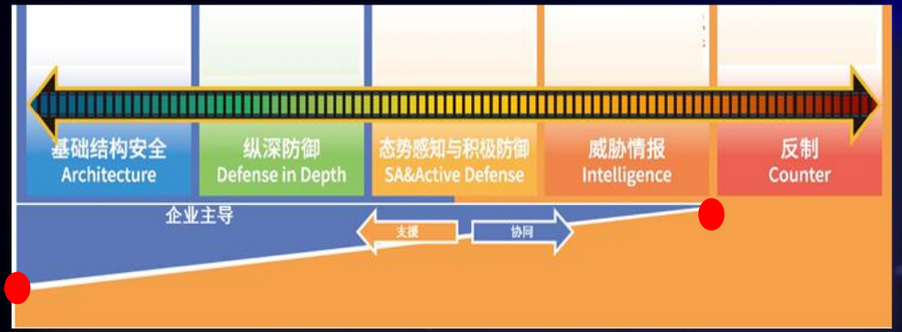
组件五：政企机构网络安全技术部署参考架构

组件六：政企机构网络安全运行体系参考架构

1. **一个框架：新一代网络安全框架**
2. **六个组件**
   - ①组件一：安全能力体系
   - ②组件二：规划方法论与工具体系
   - ③组件三：组件化安全能力框架
   - ④组件四：建设项目实施库
   - ⑤组件五：政企网络安全技术部署参考架构
   - ⑥组件六：政企机构网络安全运行体系参考架构
3. **八个工具**
   - ①现状调研问题模板
   - ②安全能力分析评价模型
   - ③组件化安全能力框架
   - ④安全建设路线图
   - ⑤安全项目规划纲要
   - ⑥项目投资概算模型等
   - ⑦政企机构网络安全防御全景模型
   - ⑧政企机构网络安全协同联动模型

框架不只是一张图，还包括多个工具，还可以使用其中的工具建立自己的内生安全体系。

组件一：安全能力体系



有助于建立一种鼓励防御者逐步提升的观念，从而更好地理解资源投入的目的与影响，建立安全项目的成熟度模型。

按安全建设演进路线维度分类，更适合国内需要从基础能力建设做起的现状。

开发

基础架构安全	被动防御（纵深防御）	积极防御	威胁情报
日志采集与存储	网络区域边界防护（FW、IPS、防	日志汇聚、分析、共享	情报收集
网络结构分区隔离	内外隔离保护（安全隔离与交换）	安全态势分析	情报分析与验证
云内云外网络分层与加密	基础平台网络边界防护	响应处置	情报生产
终端安全管理（信息内网）	各层流量可见及威胁检测	情报使用	情报共享
终端基线、漏洞与补丁管理（信息内网）	攻击诱捕	设备运行态势监控	工控威胁情报
终端安全管理（信息内网）	准入控制	追踪溯源	
终端基线、漏洞与补丁管理（信息内网）	终端安全防护（信息内网）	编排与自动化	
主机基线、漏洞、补丁管理与加固	终端防病毒（信息内网）	敏感数据检测	
虚拟化底层隔离	终端安全防护（信息外网）	用户行为检测	
应用开发安全	终端防病毒（信息外网	环境感知	
应用安全加固	虚拟机系统安全防护	工控态势感知	
应用访问控制	宿主机系统安全防护	物联网态势感知	
数据安全治理/分级分类	应用安全防护		
数据加密与隔离	应用动态安全防护		
数据访问控制	数据访问与使用动态保护		
数据脱敏与安全共享	特权操作控制		
身份安全管理及访问控制	工控网络边界防护		
密码服务	物联网设备接入边界防护		
数据备份容灾	5G接入及边缘计算安全防护		
工控网络分区隔离			
工控系统加固			
工控远程采集认证			
物联网架构分区隔离			
物联网设备认证与加固			
5G基础结构及切片网络安全			
人工智能基础结构安全			
具备良好的基础。十四五期间需要坚实安全基础，扩大覆盖面	具备良好的基础。需要面向数字化转型完善缺失的安全控制能力	具备一定的基础。需持续提升安全态势分析及覆盖范围	初步具备

示例

颜色含义：能力显著　能力不足　能力缺乏

以滑动标尺分类，将安全能力在认知范围内，全面的、完整的、体系化的识别出来，形成知识资产。

组件二：安全规划方法论

规划项目实施活动

现状分析

- 业务现状调研
- 信息化现状调研
- 安全能力现状调研
- 差距及挑战分析

规划安全战略

- 信息化战略分析
- 网络安全战略目标制定
- 网络安全能力体系制定

目标安全体系展望

项目规划与路线图设计

- 急迫性
- 重要性
- 可行性

可研与立项

- 数据安全
- 态势感知
- 云安全
- ……

知识传递

实施内容&工具

调研访谈模板（工具）

- 等级保护 ISO27001 NIST CSF
- 最佳实践（对标）
- 风险识别（威胁分析）
- 奇安信咨询规划经验

网络安全能力体系

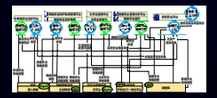
网络安全能力评价模型（工具）

项目库（工具）

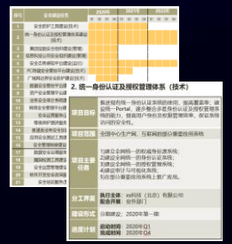
网络安全体系参考架构（工具）

网络安全防御全景模型（工具）

网络安全协同联动模型（工具）



项目规划与路线图设计（工具）



投资概算模板（工具）

方法论的好处：

一是，充分体现安全规划的专业性。

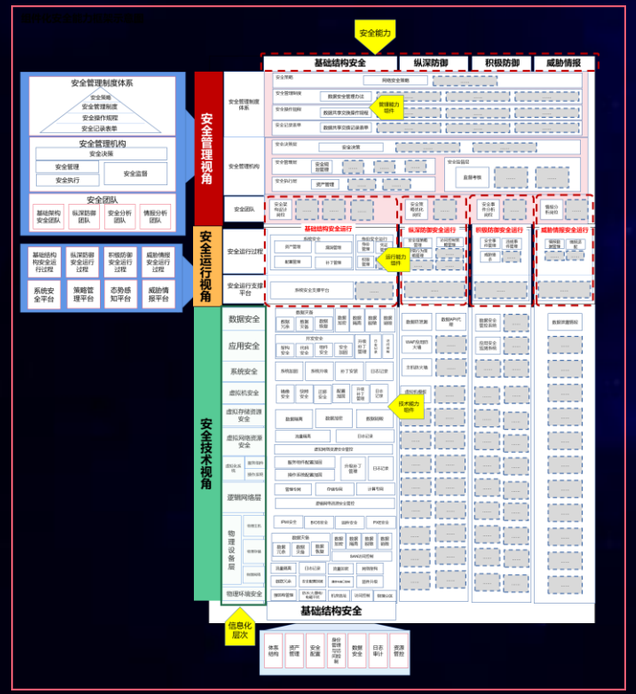
二是，使网络安全和信息化全面融合。

三是，加强网络安全能力体系化。

四是，加强项目的过程与成果管控。

五是，为可研、立项、预算提供模板。

组件三：组件化安全能力框架



使用方法：

组件化安全能力框架是将网络安全能力**映射成为可执行、可建设**的网络安全能力组件的重要工具。使用该框架将保障数字化业务所必须的**安全能力映射到安全组件。**

安全能力组件是安全能力的实现载体，包括**安全机制、技术手段、安全系统、安全管理制度、安全责任等**内容。在政企机构信息化的所有层面，把**安全能力组件与信息化组件相结合**，保证了安全能力对信息化的**覆盖性与融合性**。通过对安全组件的组合，定义出要建设的项目，**使项目的建设内容被清晰的表达**。

关键点：

1. 首先，使用网络安全滑动标尺模型对网安能力分类，结合网络安全专业知识，识别出保障数字化业务所需的**安全能力全集。**

2. 然后，结合政企机构信息化范围，利用组件化安全能力框架，**在信息化的各层次**，识别出所有安全能力组件，**科学、合理的将安全能力组合、归并**，建立相互作用关系，**形成各领域逻辑架构**。

3. 最后，将安全能力**分布到每一个建设工程和任务中**，确保能力的**可建设、可落地、可度量**。

组件四：建设实施项目库（由15个纲要组成的项目库）

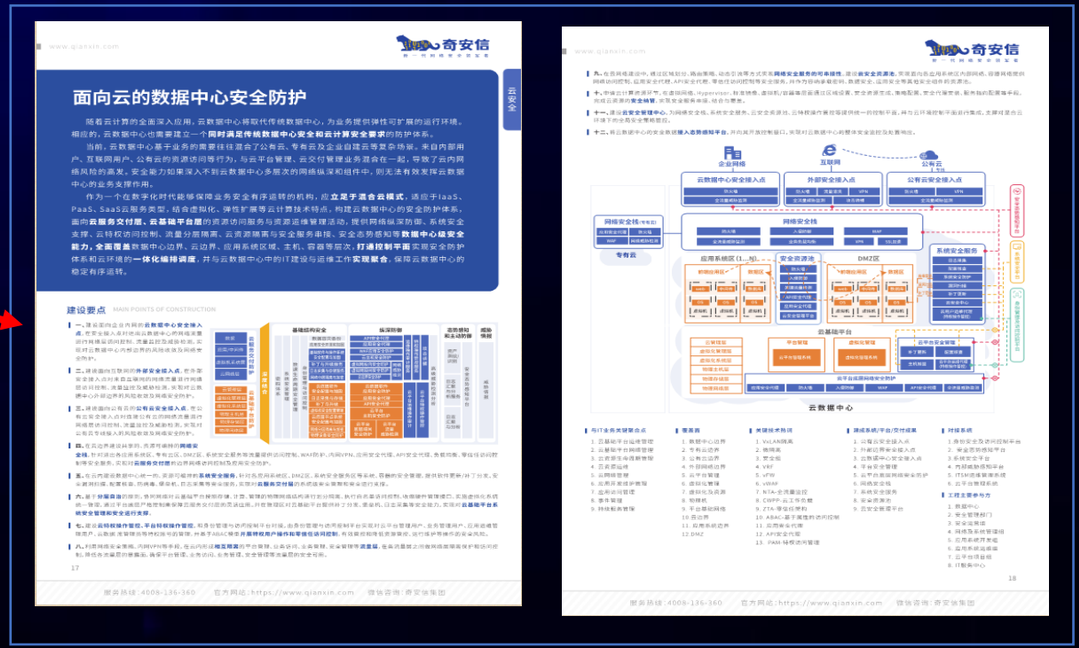
十大工程

- 新一代身份安全
- 重构企业级网络纵深防御
- 数字化终端及办公环境安全
- 面向云的数据中心安全防护
- 面向大数据应用的数据安全防护
- 面向实战化的全局态势感知体系
- 面向资产/漏洞/配置/补丁的系统安全防护
- 工业生产网安全防护
- 内部威胁防控体系
- 密码专项

五大任务

- 实战化安全运行能力建设
- 应用安全能力支撑
- 安全人员能力支撑
- 物联网安全能力支撑
- 业务安全能力支撑

建设项目实施库

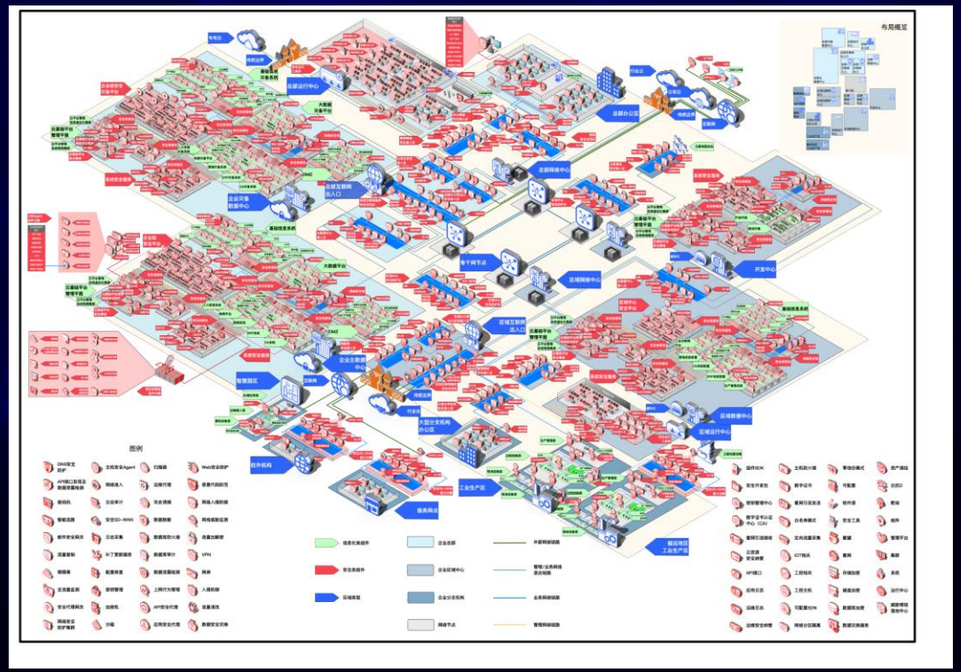


项目规划纲要

组件五：政企机构网络安全技术部署参考架构

三全特性

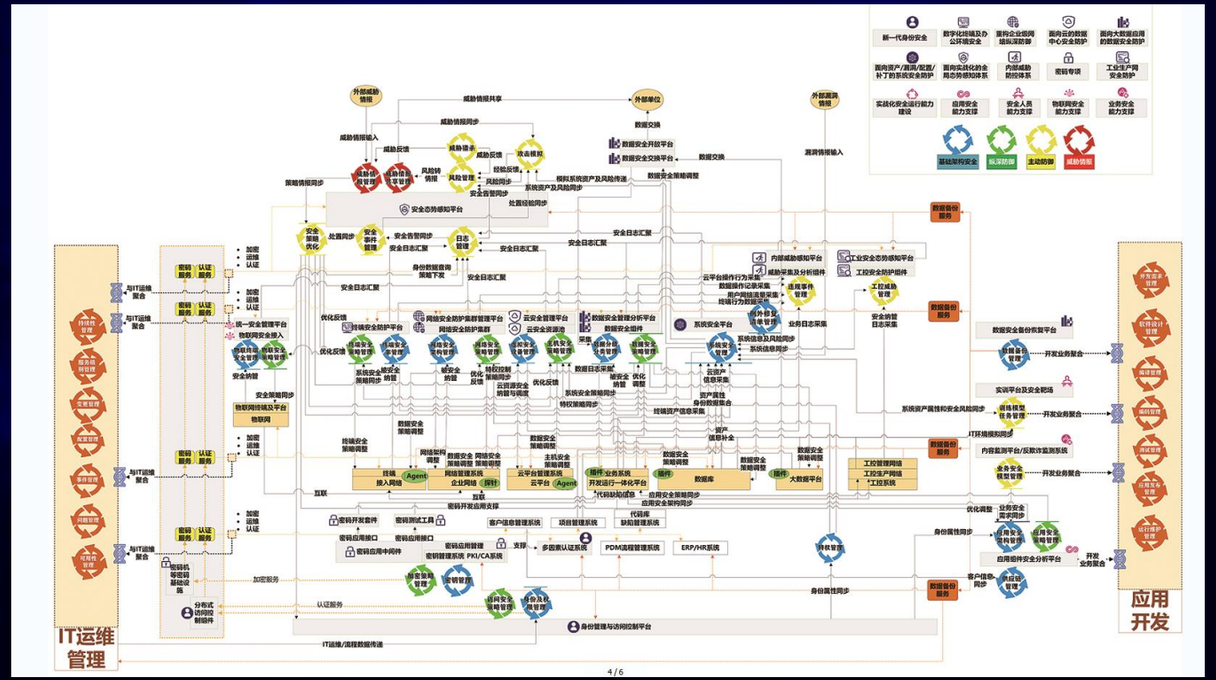
1. 在全景的网络覆盖区域融入纵深防御能力
2. 安全技术与信息化技术聚合，安全能力全面内生于信息化技术环境
3. 安全的全能力视图，覆盖整个IT范围



一个战场
一个整体
各司其职
全面覆盖、深度融合
合理组合、消除异构

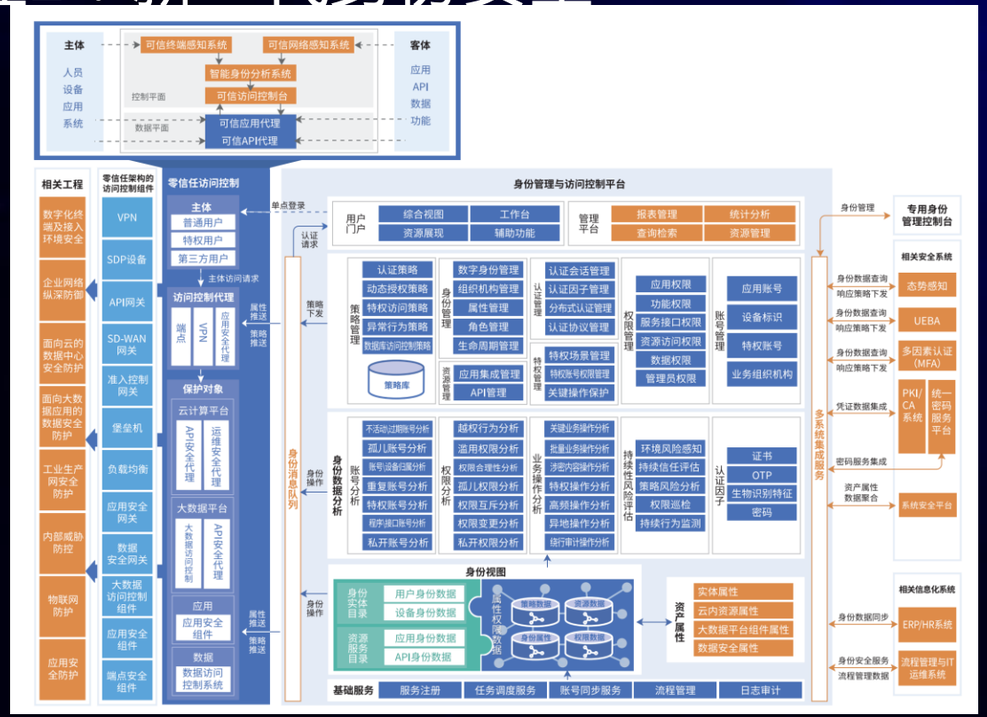
组件六：政企机构网络安全运行体系参考架构

通过安全与信息化技术聚合、
数据聚合、人才聚合，构建
一体化的协同运行能力。



一个战场
一个整体
各司其职
整体运转、数据互通
协同联动、互为依赖

工程1：新一代身份安全



云计算、大数据、移动应用等技术改变了以往身份管理和使用模式，从功能驱动模式转变为数据驱动模式，基于零信任架构的现代身份与访问管理技术为信息系统和网络安全运营奠定了基础。

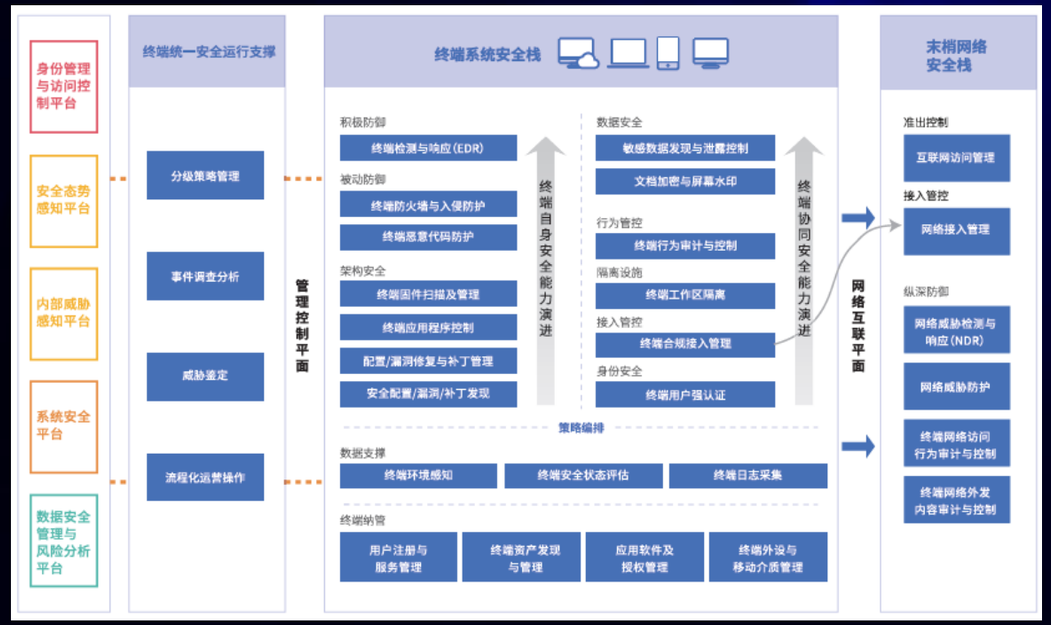
① **聚合人员、设备、程序**等主体的数字身份、认证因子等数据和IT服务**资源属性、环境属性、数据资源安全属性**等数据，结合访问控制策略，形成**统一身份数据**视图。

② 面向**云、大数据平台、应用系统的内部服务与资源**，建立基于资源属性的数字**身份统一授权管控策略，强化系统运维、权限变更等特权操控**，实现全场景统一授权管理和零信任细颗粒度控制。

③ 面向**流程管理系统和运维工单等系统**开放服务，实现多层级、流程化的身份与权限生命周期安全管理。

④ 与**UEBA集成**，支撑对异常行为发现与处置。

工程3：数字化终端及接入环境安全



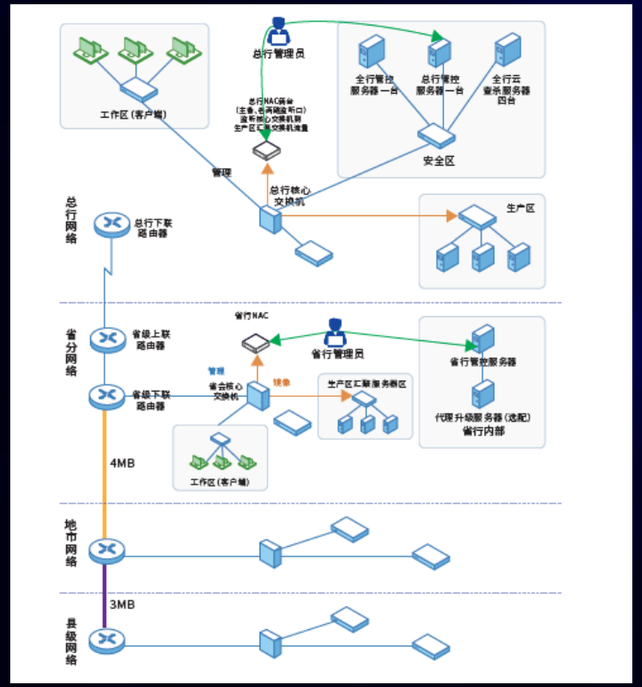
数字化时代终端管理的复杂性上升，终端类别繁多、管控难度加大，接入安全、数据安全风险剧增。在终端和接入环境上构建一体化终端安全技术栈，构建全面覆盖多场景的数字化终端安全管理体系，保障业务运营。

① 建设统一的终端安全管理客户端系统，一方面用于承载终端中的各种安全服务与控制能力，另一方面**统一提供面向用户和控制平面的接口**，实现各类安全能力在终端侧的部署都基于**统一的用户界面、统一的策略管理和统一的日志管理**。

② 建设终端侧末梢网络安全管理系统，在满足网络接入层纵深防御的基础上，实现以**终端入网必合规、合规再入网为目标的动态控制能力**。

③ 建设以终端用户为中心的策略控制与运行管理平台，**打通PC终端、移动终端、云桌面、专用终端的控制平面**，实现终端管理过程中**服务能力、终端类别、数据资源三方面的统一**。

实践：某大型银行的终端安全防护系统

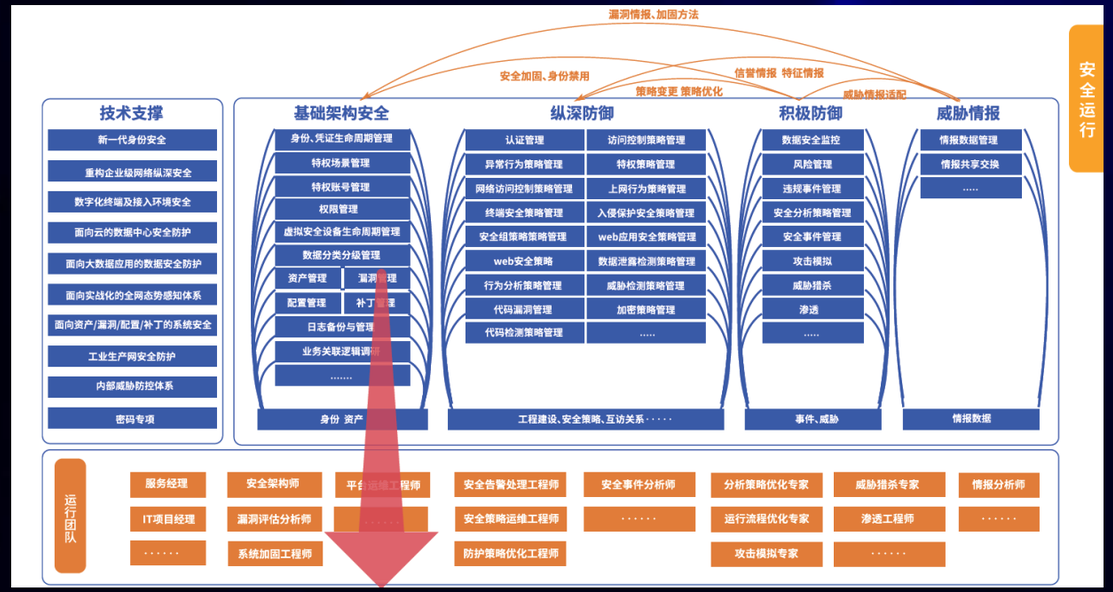


① 从互联网层面为银行提供更多的信息安全保证，**检测和发现从互联网引入的安全威胁**，成为银行所关注的安全重点。

② 由于BYOD等原因导致终端存储着大量的业务和办公数据，**敏感数据的管控，是银行数据安全的根本**。

③ 升级目前的终端安全架构，**实现管控统一化、数据可视化、预警全局化**，最终实现终端安全管理一体化是行内最大的诉求。

任务1：实战化安全能力建设



威胁瞬息万变，按次开展的安全检查与测评模式无法达到业务安全保障要求。建立实战化的安全运行体系，全面覆盖安全团队、安全运行流程、安全操作规程、安全运行支撑平台和安全工具等，并持续的评估、优化，持续提升安全运行成熟度，以达成对信息系统的持久性防护，保障业务运营。

① 安全运行团队作为安全运行活动的执行者，需持续提升安全技能和安全经验并与先进的安全技术相匹配，**发挥人防与技防融合提升的效果**。

② 安全**运行流程和安全操作规程**是保证安全运行人员合规、快速、准确执行闭环安全运行活动的依据和指导。

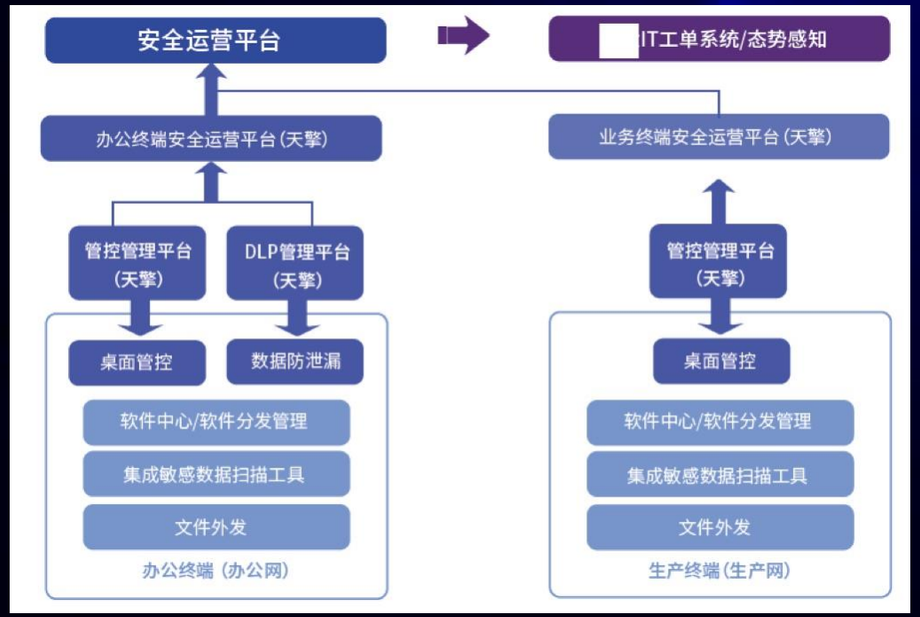
③ **人员身份为主线**的身份、凭证、权限管理，和**资产为主线**的资产、配置、漏洞、补丁管理是安全的基础，**安全策略和访问关系为主线**的纵深防御安全策略管理是安全的保证，**威胁和安全事件为主线**的安全事件处理、威胁猎杀、攻击模拟、策略优化提升安全防护水平，**情报数据为主线**的威胁情报运营和适配**提升响应速度及安全预防能力**。

④ 安全运行团队依照依照既定的**操作规程**快速有效的处理安全事务。

⑤ 安全运行支撑**平台和安全工具的建设**要与实战化安全运行能力相匹配。

⑥ 安全运行体系需**持续评估、优化，持续提升**安全运行体系的成熟度。

实践：某大型银行终端安全运营

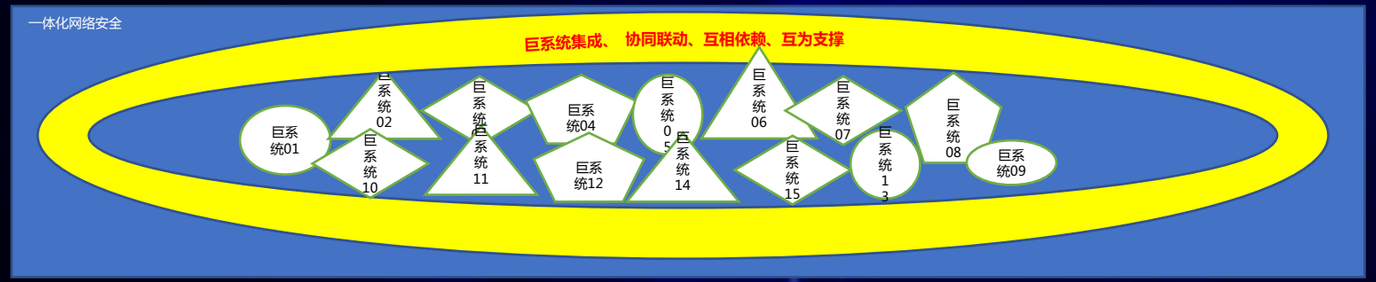


① 通过引入终端安全运营理念与实践，强化各类终端的安全策略与持续性执行；加固终端自身安全性，减少终端和内网出现故障的几率；

② 防止用户非法外发，监控用户的异常行为；

③ 规范用户日常终端使用。

在十四五规划期，以能力为导向，架构为驱动，建成“一体化”内生安全体系



总体技术部署参考架构

1. 企业级网络的全景是怎么样的？
2. 信息化的全景是怎么样的？
3. 安全组件放在信息化的什么位置？
4. 安全能力的全景是怎样的？

总体出发点是要解决技术部署的科学性、合理性问题，体现出了相对静态的**“部署态”**快照

总体运行体系参考架构

1. 解决信息化系统、安全系统协同；
2. 信息化人员、安全人员系统
3. 信息化数据、安全数据的互通，流动；

总体出发点是解决如何运行、如何联动、如何协同一致的问题，体现出了相对动态的**“运行态”**快照

一个形象比喻：

1. 一体化内生安全，安全是一道大菜，包含15种食材，用量与配方为核心；而不是用15种食材，炒15道菜。
2. 一道菜，用15种食材，必定要考虑用量、融合度、下锅的先后、以及火候；
3. 十五道菜单独做，必定只考虑自己，各自上桌之后，难以再次融合，尾大不掉，不可能再次下锅，只能推倒重来。

THANKS

全球网络安全 倾听北京声音