- 授权动态化

权限不再是静态制定的，而是基于持续的风险度量和信任评估，动态调整访问权限，实现动态访问授权。

- 风险度量化

采用大数据分析和人工智能技术对用户、设备、环境属性等访问上下文进行感知和建模，实现风险和信任的持续度量。

- 管理自动化

借助策略分析和工作流引擎等机制，实现策略的自动优化分析和管理流程的自动化，提升管理运维效率，规避管理人为犯错。

5.3 新一代身份安全建设要点

5.3.1 建设要点

在数字化时代，身份安全对保障业务安全有序运转起到重要作用。政企可以将身份安全定位为信息化和网络安全的双基础设施，采用基于数据驱动的身份管理模式，结合零信任架构的访问控制技术路线，建设身份管理与访问控制平台。新一代身份安全的建设需要规划先行，然后需要结合业务的安全愿景与现状，分解建设任务并逐步建设，建设要点如下。

- 建设身份管理与访问控制平台，承载统一的数字身份视图，实现身份管理、账号管理、权限管理、资源管理等功能，覆盖人员、设备、应用等各类实体的数字身份及其权限管理。
- 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，结合访问控制策略数据，形成企业级的统一身份视图，实现人员、设备、接口、应用的全面身份化。
- 开展身份数据与权限数据分析，提升数据的质量。发现越权、滥用权限等异常行为，以及违反业务规程、保密要求、内控要求的各种违规类操作。以身份大数据支撑遍及所有工程中的“零信任”访问控制组件，为动态、精细化的访问控制奠定数据基础。