亚信安全™

信御运维安全管理与审计系统_AIS iFort EE（堡垒机）

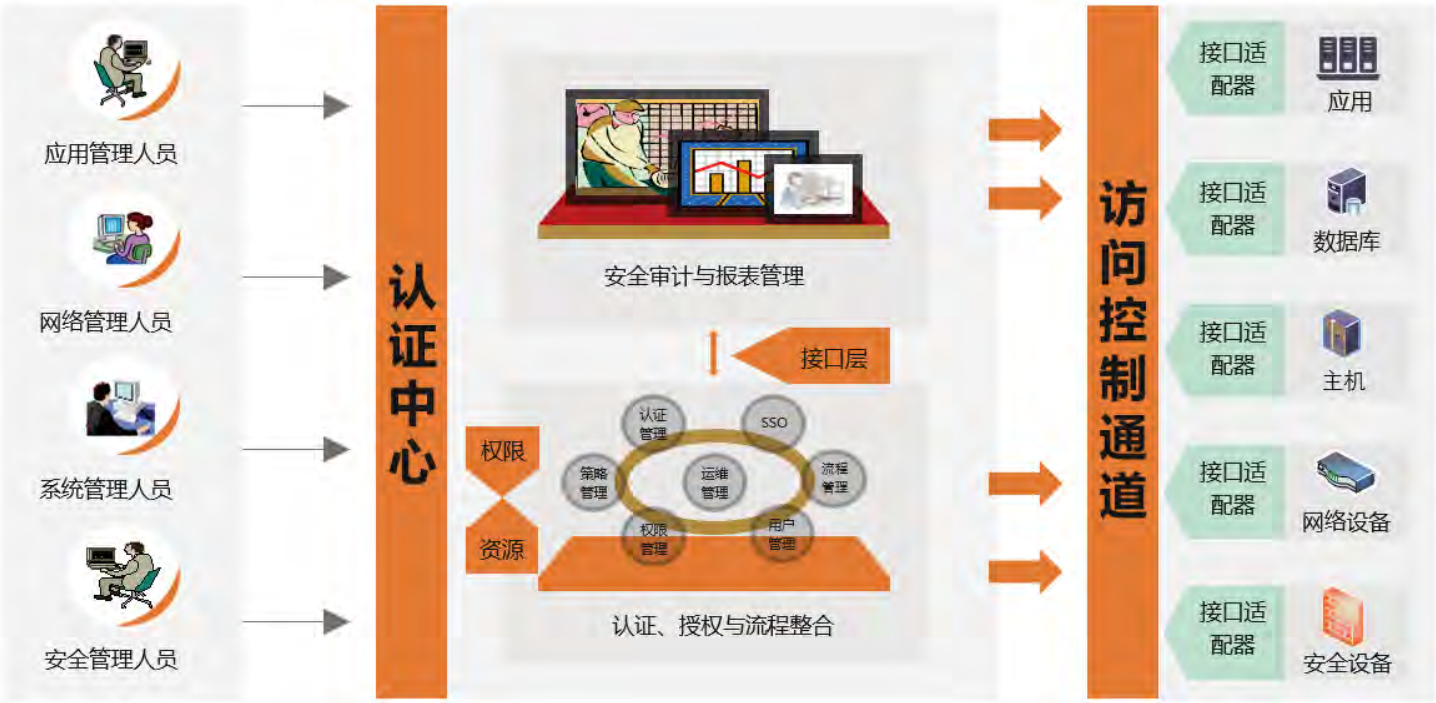
背景、需求分析：

企业使用规模庞大的主机、网络、安全设备来提供基础IT支撑服务。由于设备与系统众多，运维管理工作压力巨大，越权访问、误操作、滥用、恶意破坏等情况时有发生，不仅降低企业的运行效率，还会对企业声誉造成重大影响。如何提高系统运维安全管理水平，跟踪、控制用户的操作行为，防止非法入侵和破坏，提供控制和审计依据，降低运维成本，满足相关法律法规要求，成为企业迫切需要解决的核心问题之一。

常见问题

- 账号无法统一管理，账号密码认证方式安全性低
- 缺乏集中统一的授权管理平台、权限管理较为粗犷
- 独立的审计缺乏关联分析、运维事故难以定位
- 管理制度缺少技术层面的支持，第三方维护人员管理困难

我们的解决方案



产品核心功能

- 账号全生命周期管理
  通过制定统一的、标准的用户账号安全策略，实现账号与具体的运维人员（自然人）关联，通过主账号和从账号（被管资源上的账号）关联的方式实现用户管理和细粒度授权，支持自动改密。

- 强身份认证统一访问入口
  提供的统一访问门户，与管理后台实现服务级分离，门户集成静态密码、动态口令、AD域认证、数字证书、Radius认证、短信认证等主流双因素证方式，提高认证的安全性和可靠性，最终可以准确辨别访问者的真实身份。

- 细粒度授权和访问控制
  通过集中统一的访问控制管理和细粒度的命令级授权策略，确保每个运维人员拥有最小管理权限。系统管理员可根据运维人员的实际权限，对其访问所使用的协议、工具、目标系统账号等设置细粒度的访问策略。

- 集中化的操作监控和审计
  通过图像操作录像、操作命令审计、文件操作审计等方式，全方位建立账号的行为审计，在使用过程中对越权行为进行告警、阻断，对违规操作实现权限及时回收，对账号操作行为进行追溯。

产品优势

AsiaInfo 亚信安全

更多相关产品信息
请拨打免费咨询电话：
400-820-8839

或登录亚信安全官网：
www.asiainfo-sec.com