AsiaInfo | 亚信安全

亚信安全™

亚信安全4A统一帐号认证授权审计平台

IT系统统一智能化安全支撑

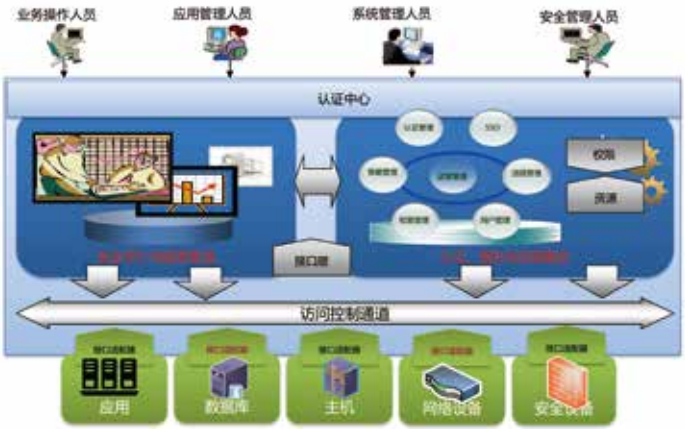
产品概述

4A平台是指对IT系统的帐号（Account）、认证（Authentication）、授权(Authorization)和审计(Audit)进行统一、集中的安全管理的平台。为企业提供统一安全框架，整合企业应用系统、网络设备、主机系统。

解决了“When”、“Where”、“What”、“Who”、“How”这样的问题，也就是说谁能够在什么时候获得谁的授权来使用某一个应用或设备，如何去使用这样的应用或设备，以及知道谁在什么时候访问了某些应用或设备等。

确保合法用户安全、方便使用特定资源。这样既有效地保障了合法用户的权益，又能有效地保障IT系统安全可靠地运行。

产品总体架构



应用案例

- 中国移动总部和22省级4A平台
- 中国联通总部和5省4A平台
- 中国电信18省4A平台

产品功能

- 统一的身份认证和单点登录；
- 4A统一门户作为应用资源、系统资源的集中、唯一访问入口，禁止用户绕过4A统一门户直接登录应用资源和系统资源,安全、高效的使用各类IT资源，降低操作复杂度；
- 统一的帐号、授权管理,对用户能够在被管资源中行使的权限进行分配，实现用户对资源的访问控制，降低日常安全管理工作量，提升安全管理效率；
- 全面审计业务操作行为、系统操作行为，落实安全政策，降低安全事件的影响；
- 安全、可靠、易用的人机交互界面，为使用人员提供身份管理、登录认证的相关服务。

产品优势

- 完全自主知识产权的身份管理、访问管理系统；
- 平台对用户的管理权限严格分明，各司其职，分为系统管理员、审计管理员、运维管理员、口令管理员四种管理员角色，平台也支持管理员角色的自定义创建，对管理权限进行细粒度设置，保障了平台的用户安全管理；
- 支持多种强认证方式：静态口令、令牌卡、USB – KEY、IC卡、手机短信、数字证书等；
- 基于用户、目标设备、运维时间等组合授权功能，满足用户实际授权的需求。授权可基于：用户到资源、用户到资源组，支持批量功能；
- 金库模式操作强制要求必须由两人或以上有相应权限的员工共同协作完成敏感高风险操作，通过相互监督、利益制约确保关键操作的安全性；
- 基于Solr全文检索，基于Hadoop海量数据采集和分析的日志审计平台；
- 图形堡垒机唯一实现对运维人员可登录到远程虚拟服务器对目标服务器进行访问，同时避免敏感数据直接流失到用户终端。在图形堡垒上可发布数据库维护工具，方便运维人员进行运维操作。

AsiaInfo | 亚信安全

亚信安全™

亚信安全BDS大数据安全管控系统

产品概述

亚信安全大数据安全管控系统BDS针对大数据广泛应用的背景和安全需求，以企业内部人员和业务系统为主要管理对象，将大数据系统的帐号权限集中管理、集中认证、集中鉴权和集中审计作为切入点，集中管理业务系统和运维操作人员对大数据系统的访问操作和审计日志，保障大数据系统的安全。

产品总体架构

大数据安全管控系统以云平台为管理对象，集中管理云平台Hadoop数据库的帐号、权限、认证和审计，并对云平台的敏感数据进行重点管控，确保大数据云平台的集中化数据安全。系统特有的代理模式将云平台Hadoop数据库与运维访问人员和业务系统隔离开来，形成访问缓冲区，既便于对云平台Hadoop数据库的使用者进行统一管理，也保障了云平台的安全性。

典型案例

- 中国移动13个省份大数据安全管控系统
- 中国电信3个省份大数据安全管控系统
- 中国电子科技集团公司第二十八研究所

产品功能

- **管理平台**：提供本系统基本的维护功能，包括用户管理、认证管理、授权管理、审计管理、敏感数据管理；
- **门户**：门户为大数据用户提供了统一、集中的数据访问方式。提供web的可视化大数据访问，包括JOB的提交和状态查询、HIVE的DDL和SQL执行及结果展现、HDFS文件系统管理、HBASE管理；
- **代理**：代理是实际向生态系统发出操作请求的组件。用户在门户中对生态系统的所有操作均由代理转发给实际生态系统。代理会在执行之前判断操作是否已被授权，若未授权则不会执行操作，并通过门户提示用户。同时，代理分析操作的内容是否包含敏感数据，如果包含敏感数据，将按即定的敏感数据访问策略对请求进行阻断、脱敏等控制。包括HDFS代理、HIVE代理、HBASE代理、MapReduce JOB访问代理；
- **审计采集**：系统统一采集、存储各生态系统的访问日志，并允许在要求的情况下转发给第三方审计系统；
- **认证中心**：系统能够为主帐号登录门户和从帐号登录生态系统提供集中的认证。

产品优势

- 完全自主知识产权的大数据安全管控产品；
- 在管理大数据安全的同时，重点对大数据中的敏感数据进行安全控制，创新性的提供了阻止访问、允许访问并告警、允许访问不告警、默认为允许访问不告警等多种敏感数据的访问控制手段，明确设置了敏感数据的多种访问级别。并且全流程告警、事后审计，将敏感数据的泄漏可能性降低到最低水平；
- 使用代理对大数据系统进行安全管理。代理在访问者和大数据系统之间充当缓冲，增加了大数据系统的安全保障；
- 充当大数据系统的防火墙，外部攻击首先需要冲破代理的保护才能进一步攻击大数据系统，增加了恶意用户的攻击难度；
- 代理能够对大数据系统进行访问控制，在事前和事中对违规和非法操作进行阻断，从而降低损失，事后进行审计和追责定位，为违规事件处理提供依据。