AccessMatrix™ UCM
凭证安全管理

通用凭证管理 (UCM)是新一代特权账户活动管理（PAAM）解决方案，集成了无代理连接器、录像记录和单点登录

关键优势

- 采用通用认证平台降低运营成本
- 简化集成和部署工作
- 处理复杂的认证需求
- 符合未来身份认证选择
- 提供高可扩展，开放和可靠的平台
- 消除硬编码，提高安全性

特点

灵活的细粒度管理

- 已获专利的分层分区管理和授权模型
- 策略驱动的方法
- 支持以资产属性为维度，统计异常账号
- 动态改密，支持基于凭证和保险箱的弹性动态改密规则
- 支持批量改密计划的全局暂停和开启
- 双重控制（Maker / Checker），最小特权和管理角色的职责分离

简单部署 轻松管理

- 便于管理的分组凭证
- 目标资源信息批量导入
- 与现有用户目录集成
- 自动发现非法账户

安全的特权访问

- 自定义审批工作流和凭证管理
- 命令过滤，限制管理员活动
- 单点登录到目标资源，不会泄露密码
- 采用双因素认证的强身份认证来访问关键目标资源

特权凭证管理的通用平台

AccessMatrix™通用凭证管理（UCM）提供一个由HSM设备进行强加密的虚拟密码保险箱来存储已授权的用户ID和密码（即凭证）。UCM的安全特性满足企业在管理凭证和会话活动中面临的主要审计和运作挑战。主要挑战有：

- 手动管理 ID 和密码
- 缺乏特权会话活动的跟踪和控制
- 批处理脚本和应用程序中的硬编码特权账号 ID 和密码
- 提供对特权访问关键服务器和计算资源的合法跟踪和虚拟记录

全面的 PAAM 特性

内置办公时间或非办公时间工作流 或 与外部工作流集成

支持各种身份认证选项

工作流驱动的凭证签入/签出，签入时密码自动更新

采用会话录像记录单点登录到目标资源，

标签凭证（特权密码）如项目、UAT、产品、OS

非代理集成数据库、Unix、Windows、路由器、防火墙

CSV 导入 和 PDF 版本备份凭证

无缝集成现有企业用户存储或目标资源存储

使用加密密钥、安全策略与可选 HSM 来进行安全保护

安全访问并无缝连接任何位置的 任何设备 (桌面、笔记本电脑、手机)

全面的审计日志和细节报告

- 会话日志使用录像记录和基于命令文本的审计日志
- 安全的审计日志和活动报告

高级安全特性

- FIPS 认证的 HSM 进行密钥管理
- 可定制化的 API
- 自定义规则检测弱密码
- 支持紧急情况下凭证批量导出

UCM提供什么?

特权用户访问（PUA）模块

UCM 提供一个多层审批流程的安全途径，授权企业控制安全管理员检索和存入特权凭证。这使授权用户能够在日常运维或在紧急情况下签入和签出特权凭证。UCM 互动功能包括：

- 灵活访问控制的基于报告层次的凭证
- 含命令捕捉和会话录像记录的审计跟踪
- 支持含多因素认证的强身份认证
- 多层双控制工作流审批
- 在签出后可手动登陆、单点登陆或自动登陆到目标资源
- 使用无代理技术进行自动密码管理
- 灵活的 API，可与外部工作流软件集成
- 可自动对目标资源账号进行扫描，发现垃圾账号、幽灵账号并进行告警和快速纳管

特权会话管理（PSM）模块

- UCM 提供了附加的 Windows RDP 网关记录仪和一组网络协议代理模块来监视和记录特权会话。它支持录像和按键记录回放取证分析，还支持特定的协议命令访问控制

应用程序密码管理（APM）模块

UCM 使企业能够在运行特定应用程序时检索用户 ID 和密码，使用户的认证信息不需要在应用程序或命令文件进行硬编码。UCM 提供两种集成方法：

- 应用程序 API: 一套灵活和简单的 API，可以从 UCM 服务器来检索当前的 ID 和密码；
- 审计密码用户: 可在命令协议，例如 ODBC、JDBC、ADO.NET、Windows 和 Unix 脚本中，进行动态和透明的用户名和密码重置；

分层分区的管理和授权模型

企业可以通过定义细粒度级别来控制本地的安全管理员的管理权限，以提高安全性和降低管理成本

策略驱动的方法

- 自动执行企业级安全策略来管理密码、身份认证方法、时间和访问限制；
- 企业能够基于指定的安全策略，跨组织机构应用相同的安全策略；

双重控制（Maker / Checker），最小特权和职责分离管理角色

使企业无需启用超级用户管理权限即可部署 UCM 解决方案，并限制部分及下属部门安全管理权限的范围，以避免任何潜在的利益冲突

自动发现非法账户

系统要求

- UCM 服务器 / UCM 网关: MS Server 2008/ 2012 R2/ 2012 R2/ 2016/ 2019
- Java 运行环境: JRE 1.8 及以上
- 应用服务器: Oracle WebLogic, IBM WebSphere 和 Apache Tomcat
- 数据库存储: MS SQL Server, Oracle RDBMS, IBM DB2 和 Oracle MySQL
- 外部用户存储: AD目录, LDAP v3 兼容目录和 JDBC 兼容数据库
- 支持的目标资源: JDBC 数据库服务器, UNIX 服务器, Windows 服务器, AD 目录, Weblogic,Websphere,SAP, AS400, IBM RACF 主机, Cisco / Array, Cisco ACS, Scriptable SSH / 基于远程登录的网络设备，如 TopSec, Juniper, Huawei, H3C, RuiJie, http, https, Z/OS, Weblogic, Websphere, Webportal
- 支持的UCM网关的自动登陆客户端: 数据库客户端, VNC, rdp, 基于网络的操作台, PuTTY, Tera Term, secureCRT 和 CuteFTP, WinSCP, SSH Secure File Transfer, IBM Data Studio, PComm, Exceed 和 vSphere Client

提供自动帐户发现报告，并将新增帐户通知给管理员

工作流审批

- 提供一个内置的工作流引擎，管理员能够通过执行自助服务来检索机密凭据，也能跟踪凭证所有者在使用凭证信息后进行密码重置；
- 提供多种工作流类型，适应不同类型的企业和方案：多级审批、非工作时间审批、经理和下属的工作流审批；

命令过滤

提供限制命令功能，管理用户可在特权访问会话期间使用

会话日志

利用录像和命令日志提供无法抵赖的电子取证和活动日志

安全的审计日志和活动报告

日志功能，记录所有事件，使审计员能够获得完整的审计跟踪信息，减少凭证管理的时间

FIPS 认证的 HSM 进行密钥管理 和加密过程

企业无需启用超级用户管理权限即可部署 UCM 解决方案，并限制下属部门安全管理权限的范围，以避免任何潜在的利益冲突

轻松管理

- 支持凭证标记，便于管理和检索凭证
- 通过目标资源的类型和安全机制进行动态标记

密码消费器和灵活的 API

企业能够使用 API 和密码消费器的快速解决方案解决动态更改密码参数的安全挑战

基于 Web 的自助服务门户

门户网站具有基于对角色的访问控制来进行请求提交、签入、签出和审批的功能

灵活的请求审批过程

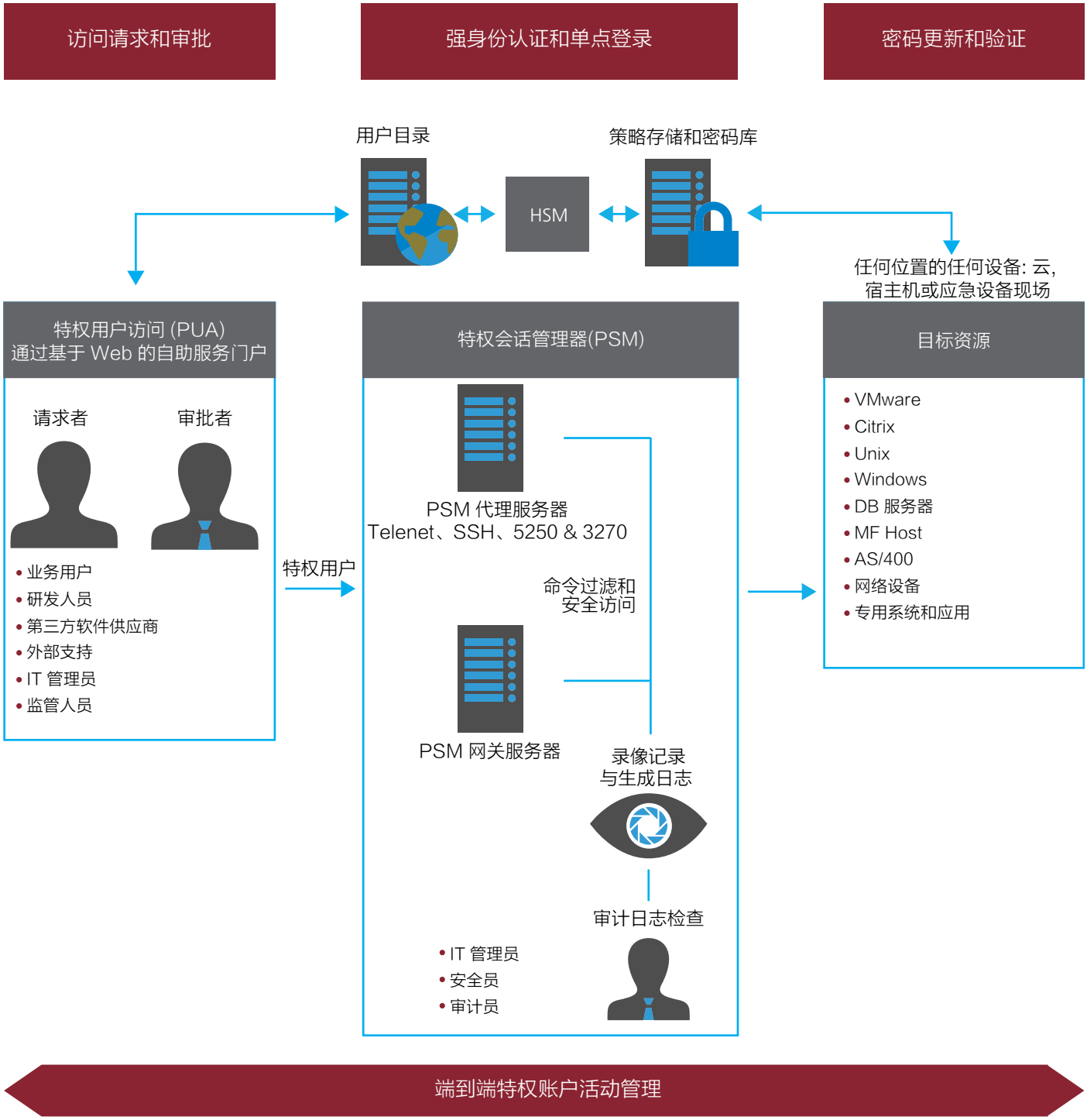
支持不同的请求审批程序，包括基于安全和资源类型的访问控制策略和基于凭证导向或者报告层次的审批程序

通过移动界面的审批

支持来自移动电话或平板电脑的审批签出请求 ，提高生产力和服务水平

UCM程序化/ UCM硬编码

多数应用程序都把凭证（比如连接数据库的用户名和密码）写在应用端内部/配置文件，这其实是一个不安全的做法。UCM 提供了程序化功能，最大限度地消除安全隐患。



北京安讯奔科技有限责任公司
北京市丰台区南四环西路188号十八区25号楼701
咨询热线：010-82736009
www.axbsec.com

安讯奔分公司和办事处
北京丨上海丨广州 丨深圳丨成都丨珠海