奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

BCS2022系列活动-冬奥网络安全“零事故”宣传周

冬奥数据安全实践典型产品分享

王爱兵 奇安信集团数据安全子公司总架构师

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

01 冬奥数据安全实践

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

冬奥数据安全实践

① 做好基础安全防护

1. **重要数据资产的隔离保护与访问控制**：
   - ✓ 对于竞赛数据、个人隐私数据等高敏数据存储在Secure域，仅允许Trust域访问
2. **特权账号管理和堡垒机**
   - ✓ 后台数据库访问须通过堡垒机操作，并进行数据访问操作监控，对未授权的数据访问和操作行为进行监控和告警
3. **数据访问审计**：
   - ✓ 对数据访问和操作进行全路径监控审计，包括但不限于数据库直接访问、数据提取、数据接口访问、用户帐号访问等，数据安全审计到字段；
4. **数据加密**：
   - ✓ 信息系统数据传输全部采取安全加密通道（如HTTPS）
   - ✓ 信息系统之间通过API接口方式使用数据，API接口调用使用AccessKey进行验签并设置时间戳进行时效性验证；
   - ✓ 高敏感级数据通过专线或VPN进行加密传输，或加密后通过专用移动介质拷贝的方式进行；
   - ✓ 磁盘加密、文件加密；
5. **终端管控**：
   - ✓ 控制外设与网络访问进行控制，启用屏幕水印警示拍照和事后追踪

② 分类分级，敏感数据识别

数据分类	数据分级			
	公开级（L1）	内部级（L2）	敏感级（L3）	高敏感级（L4）
个人数据（A）	个人公开信息（A1）	个人内部信息（A2）	个人信息（A3）	个人敏感信息（A4）
竞赛数据（B）	竞赛可公开数据（B1）	竞赛内部数据（B2）	竞赛敏感数据（B3）	竞赛保密数据（B4）
业务数据（C）	业务可公开数据（C1）	业务内部数据（C2）	业务敏感数据（C3）	业务保密数据（C4）
运行和安全数据（D）	运行和安全可公开数据（D1）	运行和安全内部数据（D2）	运行和安全敏感数据（D3）	运行和安全保密数据（D4）

数据安全级别	数据示例	流转范围	管控要求
第4级：高敏感级（L4）	1. **个人敏感信息**，如个人身份信息（A2）、个人生物识别信息（A3）、网络身份鉴权信息（A5）、个人健康生理信息（A6）、个人财产信息（A8）、其他隐私信息（A14）等 2. **竞赛保密数据** 3. **业务保密数据**，如预算和投资计划、财务报表等财务保密数据 4. **运行和安全保密数据**，如网络设备/IT系统/应用的密码及关联信息、核心网络设备及IT系统配置数据等 5. **安全事件信息**（D6）	1. 按照批准的授权列表严格管理，禁止对外披露或共享高敏感级数据	1. 实施严格的技术和管理措施，保护数据的机密性、完整性和可用性，**应加密存储** 2. 确保数据访问控制安全 3. 建立严格的数据安全管理规范以及数据实时监控机制
第3级：敏感级（L3）	1. 个人信息，如个人基本资料（A1）、网络身份标识信息（A4）、个人教育工作信息（A7）、个人通信信息（A9）、联系人信息（A10）、个人上网记录（A11）、个人设备信息（A12）、个人位置信息（A13）等 2. 涉及特定个人的汇总数据，或大量群体的群体数据。 3. **竞赛敏感数据** 4. **业务敏感数据**，如会计凭证等财务敏感数据、人事档案等人力敏感数据、合同协议文件等电文敏感数据、供应商名单及考核等供应商敏感数据、重要业务系统的业务运营数据、上报监管数据等 5. **运行和安全敏感数据**，如重要网络设备及IT系统配置数据、安全漏洞信息等	1. 只能由授权的内部机构或人员访问 2. 如果要将敏感级数据披露到外部，需要满足相关条件并获得相关方的授权	1. 实施较严格的技术和管理措施，保护数据的机密性、完整性和可用性，**建议加密存储** 2. 确保数据访问控制安全 3. 建立数据安全管理规范以及数据准实时监控机制
第2级：内部级（L2）	1. 个人脱敏数据、标签数据，内部公开的工作人员信息（如工作人员的职务、电子邮箱、工作电话等） 2. 竞赛内部数据 3. 业务内部数据，如财务内部数据、人力内部数据、供应商内部数据、电文内部数据、一般业务系统的业务运营数据等 4. 运行和安全内部数据，如一般网络设备/IT系统/应用配置数据、备份数据、监测数据、日志数据等	1. 默认在北京冬奥组委、业务系统服务提供单位、国家奥委会等冬奥会利益相关方内部使用、分发和共享 2. 如果要将内部级数据披露到外部，需要获得相关方的授权	1. 实施必要的技术和管理措施 2. 建立数据安全管理规范
第1级：公开级（L1）	1. 从合法公开披露的信息中收集的个人信息，或经用户授权的可公开个人信息。 2. 竞赛可公开数据，如可公开的赛事日程、比赛成绩等 3. 业务可公开数据，如冬奥组委公开披露信息、可公开的业务运营数据等 4. 运行和安全可公开数据，如冬奥会网站域名等可公开的数据	1. 直接对外共享或披露，但要避免由于类别较多或者数据量过大，被用于关联分析	1. 实施基本的技术和管理措施

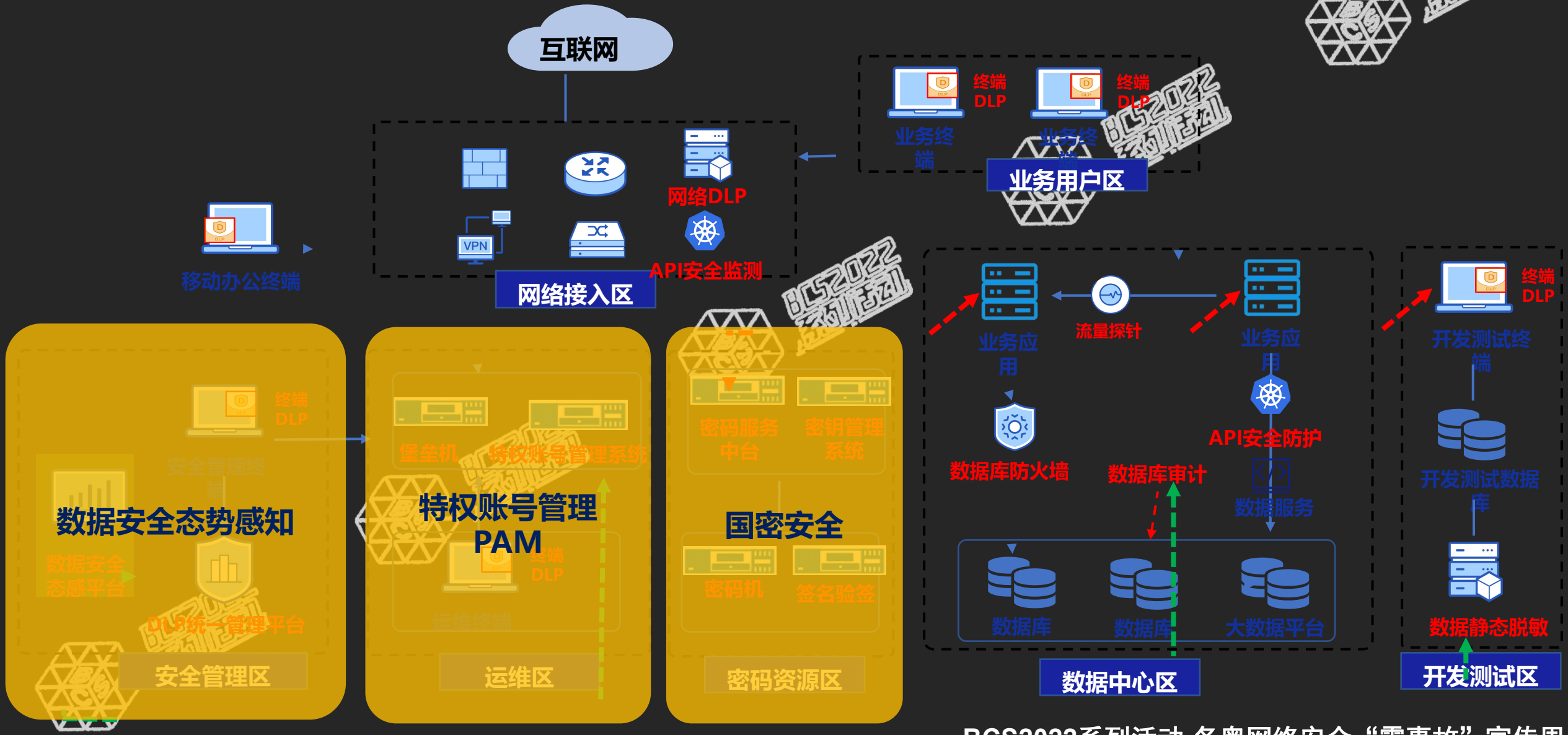
③ 敏感数据做分级管控和安全防护

1. **针对不同级别的数据制定不同的加密策略**
   - ✓ 针对高敏数据根据数据的级别及使用场景采取**字段加密、数据库加密、文件加密**等不同的加密方式
2. **建立与数据级别相对应的分层数据权限管理体系：**
   - ✓ 根据数据级别制定相应数据授权审批流程，合理授予、管理数据权限；
   - ✓ 高敏感级和敏感级数据仅能通过高权限账户访问、提取和使用，高权限账户的数量应严格限制；
   - ✓ 采取措施保障数据细粒度访问控制：
     - 结构化数据权限申请的数据单元应能细化到表、表中的字段；
     - 半结构化数据权限申请的数据单元细化到字段
     - 非结构化数据权限申请的数据单元细化到文件。

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

冬奥数据安全实践典型产品



奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

02 特权账号管理

奇安信 | BEIJING 2022

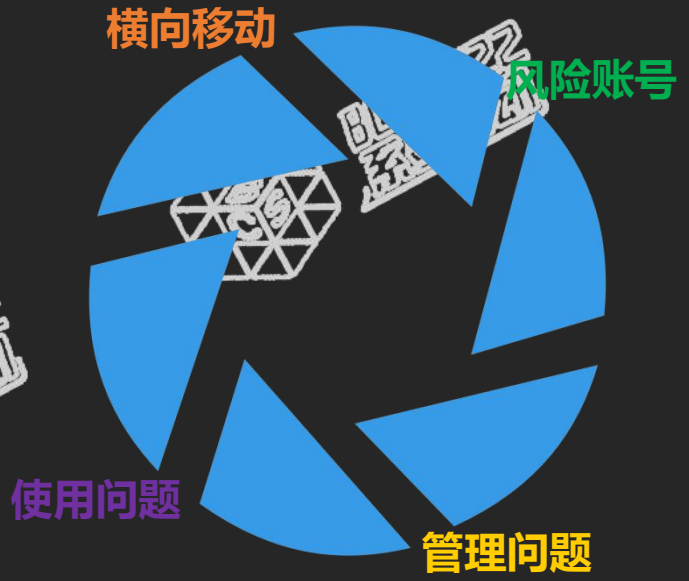
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

PAM能解决哪些账号安全问题及客户痛点？

不同的资源设置相同的账号密码

系统代码或配置文件中存在明文账号密码（称为“**硬编码**”）

不同资源之间存在互信关系



账号违规提权行为不能及时发现和阻断，存在**越权访问风险**

账号共享使用情况下可能存在账号密码的**人为扩散**风险

运维人员长期持有过高的账号权限，存在越权访问风险

长期未登录，长期无人使用的账号

幽灵账号，无人负责无人管理维护的账号

后门账号，有意或恶意创建的非法账号

弱口令，每年HW的十大安全漏洞之首

长期未改密，存在合规风险，也给攻击者提供充足的时间窗口

明文存储，如存在Excel表格、文本或笔记本中

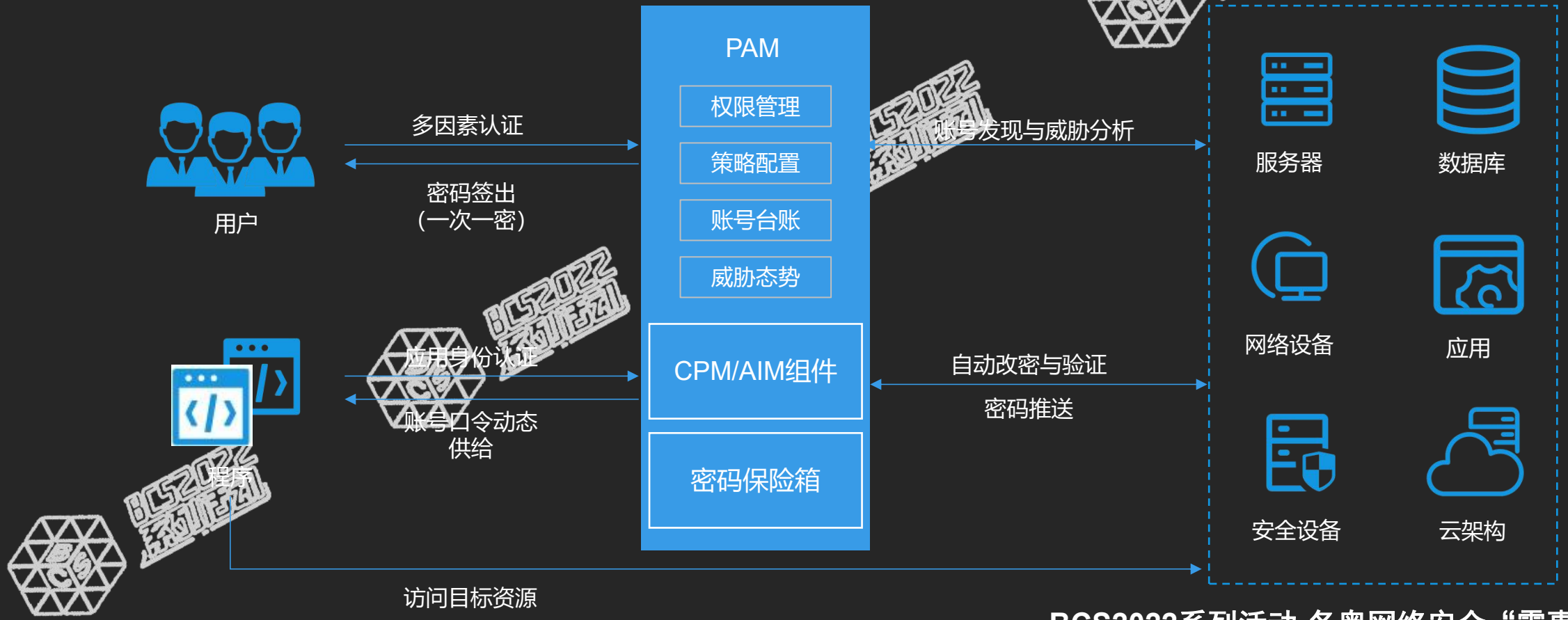
无备份机制，账号密码一旦丢失就会造成不可挽回的损失

实现**定期改密难**，手动改密工作量大、易出错；工具改密不可靠、担心改了不该改的密码。

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

特权账号管理系统产品概述

特权账号管理系统（PAM）是一款专业做**账号生命周期管理**的产品，能够**主动发现**各类基础设施资源的**账号分布、识别账号风险、管理账号使用**，可以作为**账号统一管理、统一调度**的基础平台，帮助客户实现账号安全管理和全局监控的目标。

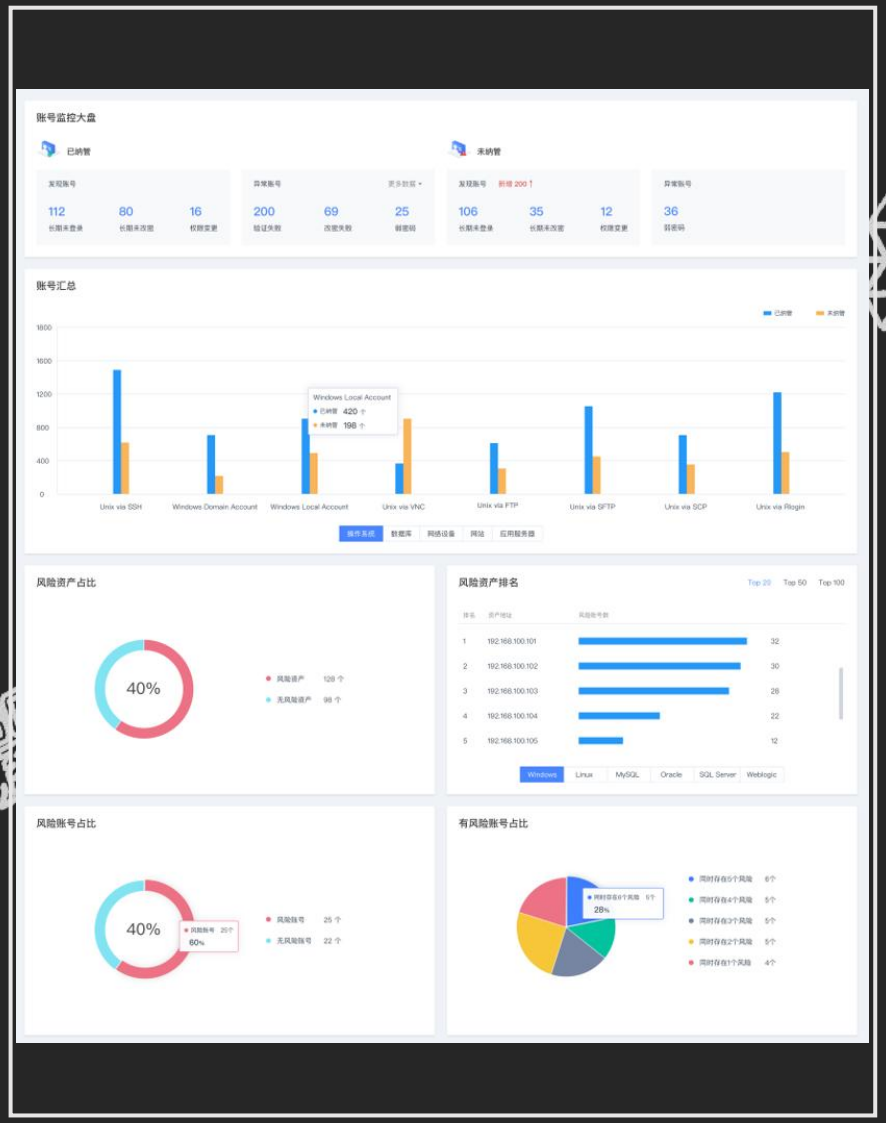


奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

特色功能1：账号风险持续追踪与治理

PAM提供账号发现与分析的能力，可以定期扫描，发现**弱口令、长期未登录账号（僵尸账号、幽灵账号）、新增账号、长期未改密账号、权限变更账号**等高风险账号及其分布情况，并通过**账号监控大盘**和**账号风险态势大屏**进行可视化的展示，管理人员可以通过PAM系统对高风险账号进行**添加**（将未纳管账号添加到PAM中）、**删除**（通过工单申请，在目标资源上删除该账号）、**启用**、**禁用**、**改密**等操作，实现对风险账号的快速治理。



奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

特色功能2：账号安全存储

问题：口令管理员将账号密码**明文存储**在文档工具中，一旦终端失陷，将造成大批核心主机或数据库失陷。

解决方案： **密码保险箱功能**，各类IT资产的账号口令及凭证集中安全存储；密码保险箱采用专属密钥加密，保障账号及凭证的安全性。

PAM

高可用部署

PAM

账号信息集中管理：

- 密码保险箱用于存储各类账号口令及访问凭证，包括password、token、SSH Key等。解决账号口令分散存放不好管理问题。

账号口令安全存储：

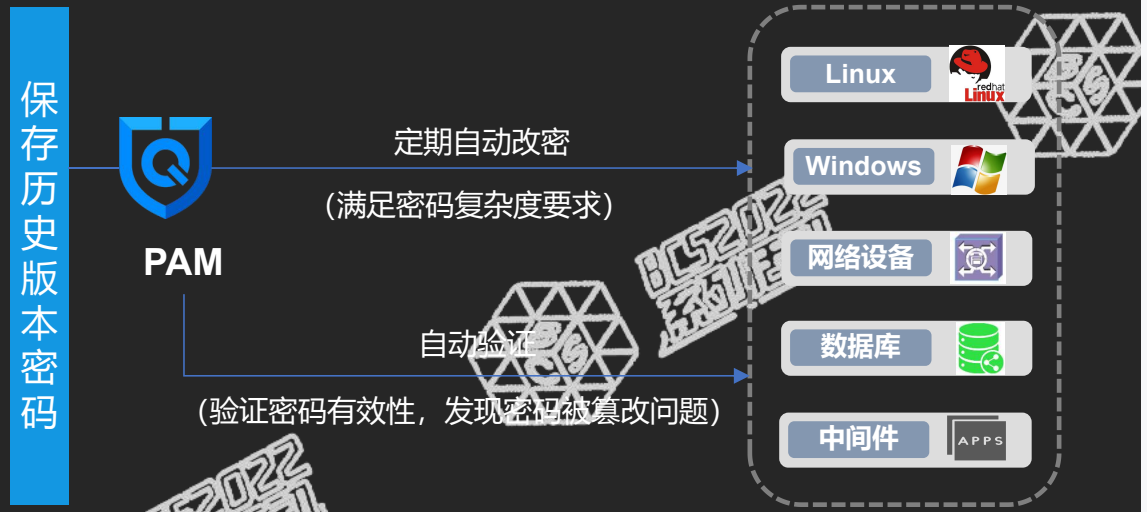
- **采用密码保险箱独立存储机制，**密码保险箱采用多级密钥加密技术，且密钥是随机生成的，各台PAM拥有不同的加密密钥。
- **采用SM2、SM3、SM4等国密算法**，实现核心数据的加密、解密和认证等功能。
- **采用部门分权管理机制**，可设置无超级管理员模式，此时不存在超级权限的用户，各部门管理员只能管理并查看归属于本部门的资源及账号口令。
- **支持安全备份机制**，保障极端情况下账号口令可以安全找回。

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

特色功能3：账号定期改密

问题：资产多账号多，改密工作量巨大，容易出现**弱口令**和**相同口令**的问题，工具/脚本改密**可靠性无法保障**，且部分账号存在**业务关联**情况，导致改密难度大大增加，无法做到定期改密，存在安全及合规风险。

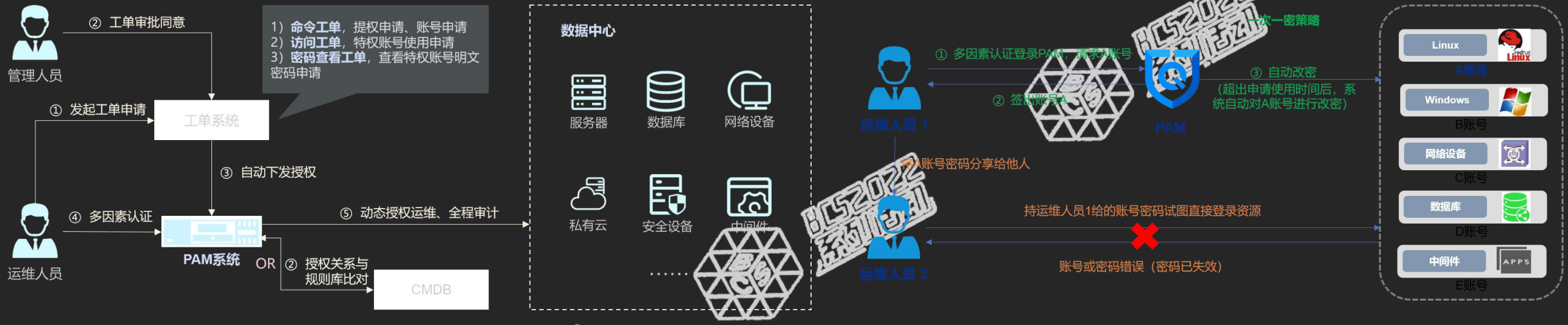
解决方案：PAM支持服务器、数据库、中间件、网络设备等资源账号的自动改密，支持**自定义密码复杂度**，且支持通过**保存历史版本密码、保存准密码、自定义改密尝试策略**等方式保障改密可靠性。同时支持**密码推送、等价改密组**等功能，可以覆盖多种业务场景的改密需求，帮助客户实现账号密码的安全合规。



账号关联服务配置界面

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

特色功能4：特权即时授权



内置工单或对接客户工单：

实现特权访问的动态即时授权，避免运维人员长期持有特权账号而带来的特权泄漏或被滥用的风险。

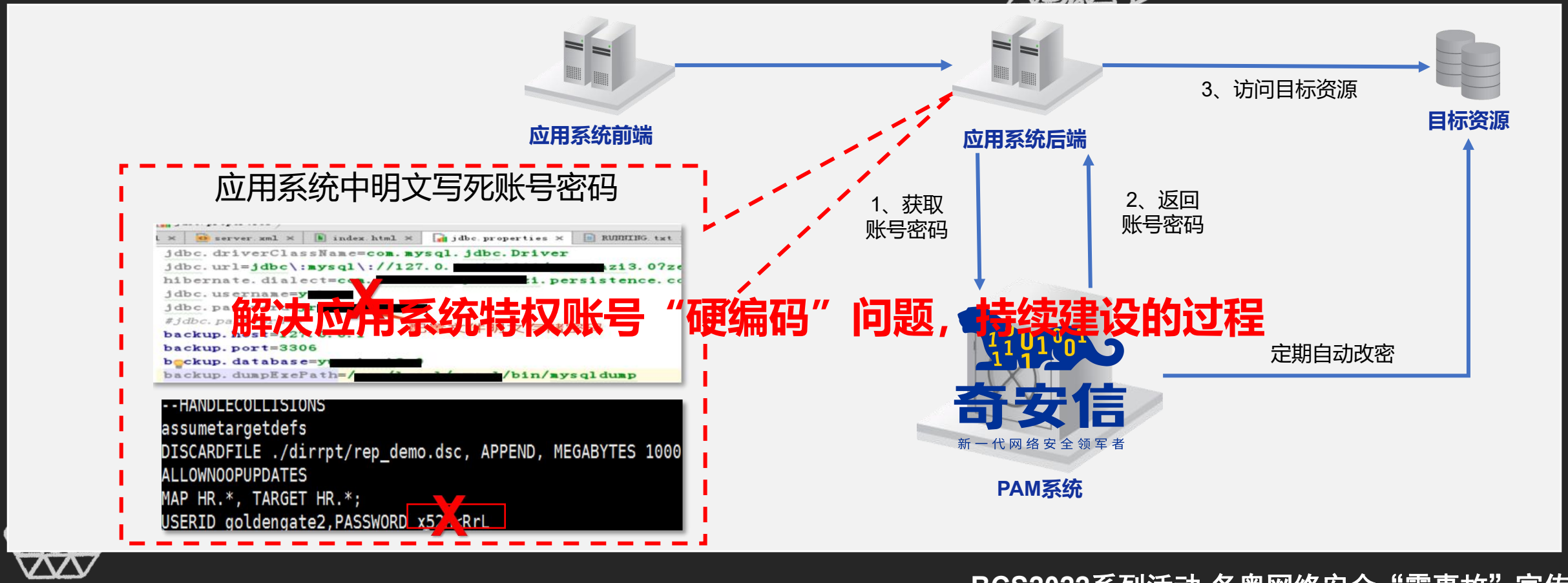
一次一密（临时运维场景）：

运维人员使用完密码后，立即执行改密，防止密码落地后被人为共享、扩散，同时降低因人为保管不当而被窃取的风险。

特色功能5：消除应用程序“硬编码”

需求场景： 1）应用系统访问数据库的账号密码一般是**明文存储**在应用系统的配置文件中的，存在账号密码泄露的风险；2）应用系统内嵌的数据库账号改密需要应用系统重启才能生效，影响业务系统连续性。

解决办法： 通过提供接口或开发SDK的方式，使应用系统动态从PAM中获取账号密码，帮助解决账号密码明文存储在配置中容易泄露的问题，同时可以对应用使用的账号定期进行改密，应用系统不需要重启，同时满足合规要求。



奇安信

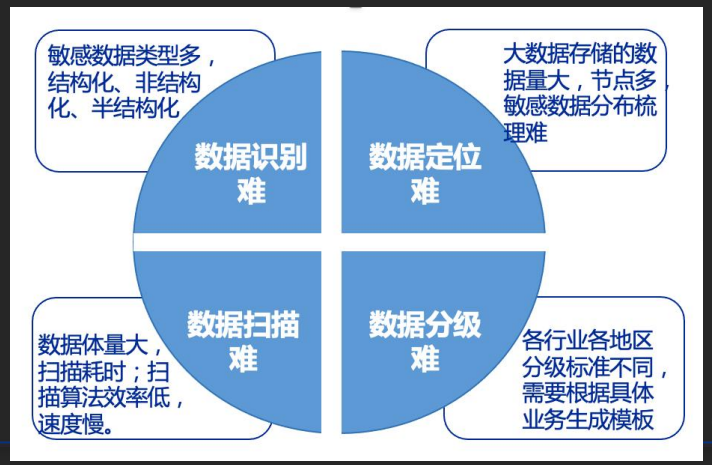
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

03 数据安全态势感知

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

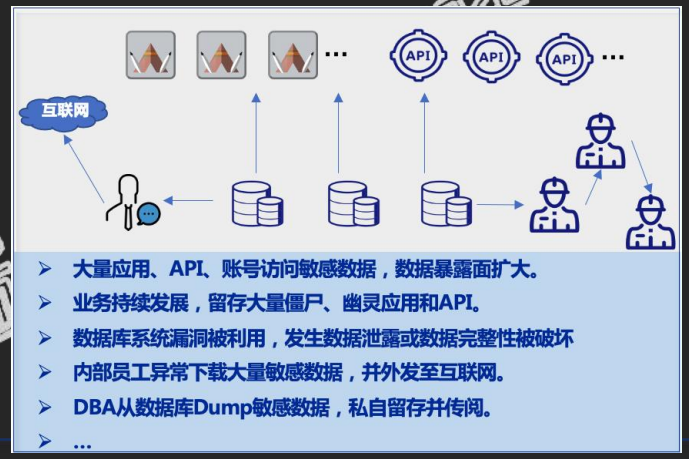
痛点：数据态势难梳理监测，安全风险难发现溯源

数据资产难梳理



流动态势难监测

异常风险难预警

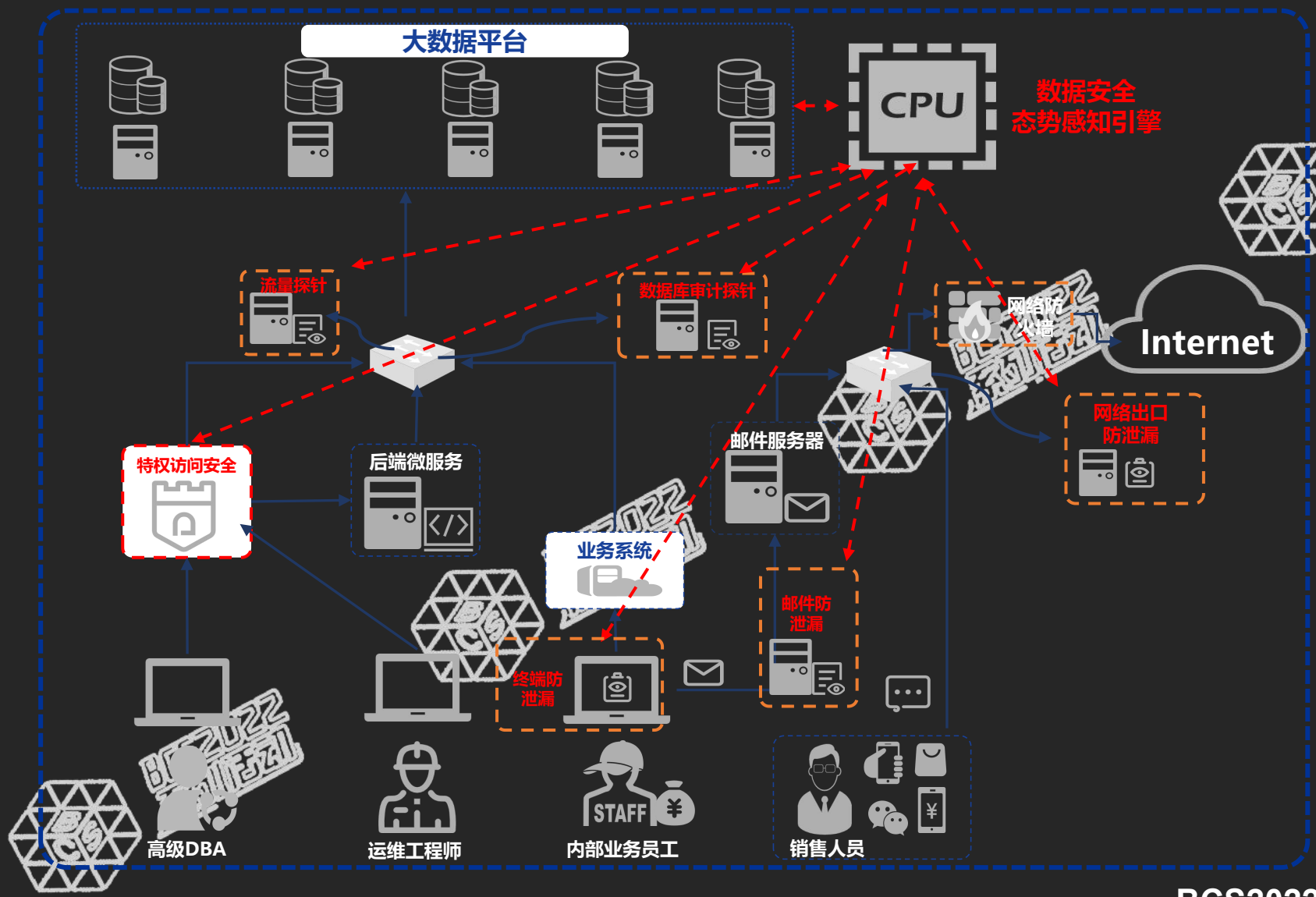


安全事件难闭环

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

数据安全多点联动全局态势感知



敏感数据分布态势

敏感数据流动态势

数据安全风险态势

能力1：敏感数据梳理与分类分级

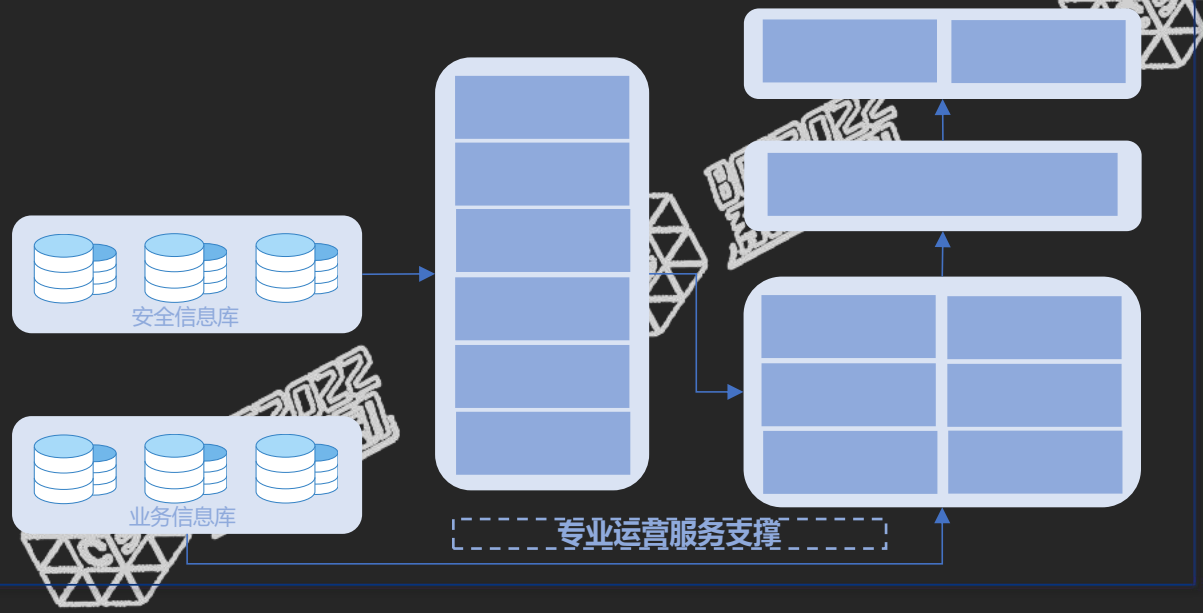
数据安全态势感知

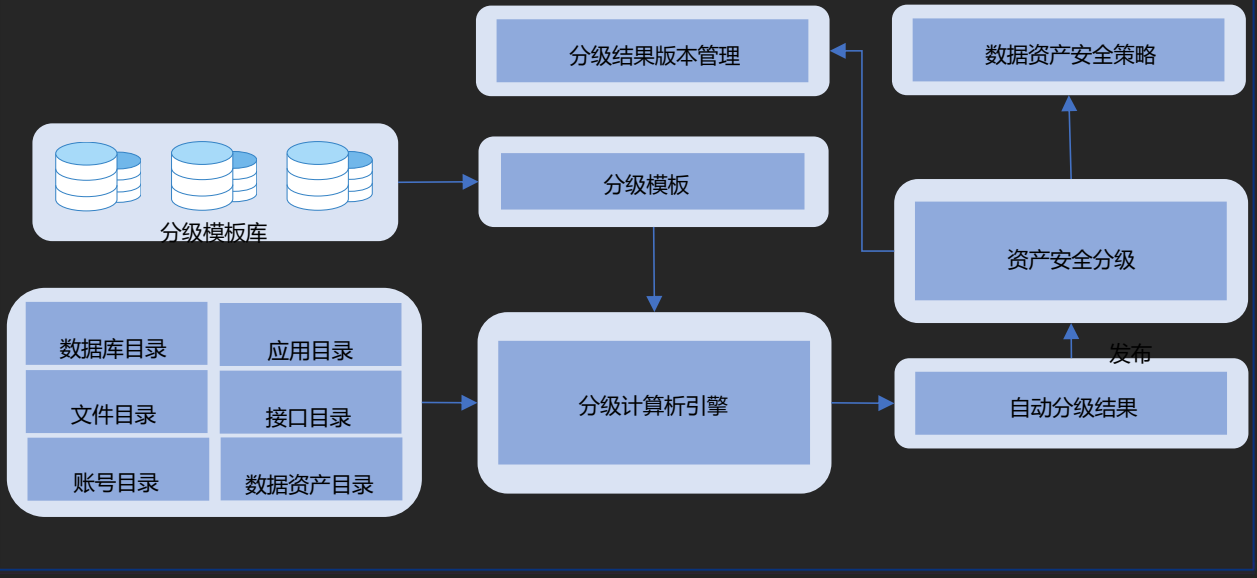
敏感数据识别与数据资产梳理

◆基于IP段主动扫描和对安全日志进行解析识别网络中的数据库、数据库账号、文件系统、应用、接口的基础信息，配合用户输入的业务信息形成数据库目录、数据库账号目录、文件目录、应用目录、接口目录；同时对所有目录对象进行敏感数据探测与识别，形成数据资产地图和异常资产。

数据安全分级

◆根据法律法规、行业标准及业务需求，定义数据安全分级模板；分级计算引擎根据安全分级模板结合各个数据资产目录对数据资产进行分级计算与级别推荐，同时生成相应的数据安全策略，为数据的权限管理与防护提供依据。

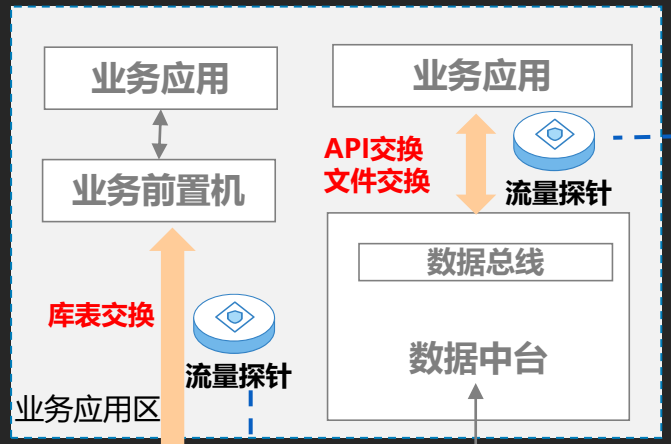




奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

能力2：敏感数据流动监测预警

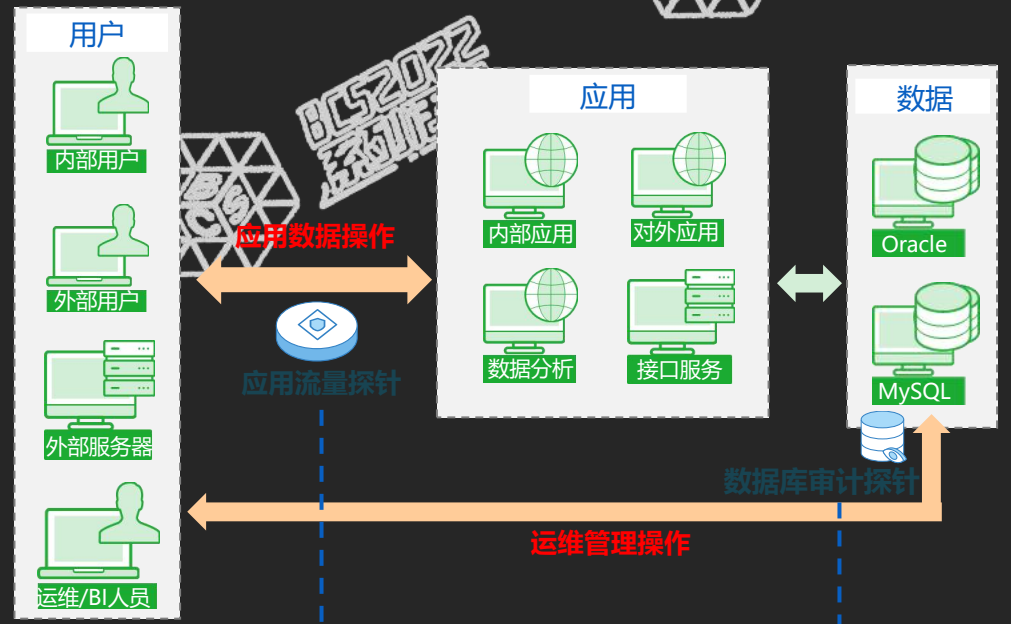
机机交互敏感数据流动监测



数 据 安 全 态 势 感 知

- **风险：**交换接口繁多，通过API、文件、库表的方式对业务应用共享交换数据时，可能发生敏感数据、重要数据违规共享。
- **方案：**通过流量探针，解析敏感数据机机交互流量，审计分析数据交换行为，监测敏感数据流动

人机交互敏感数据流动监测



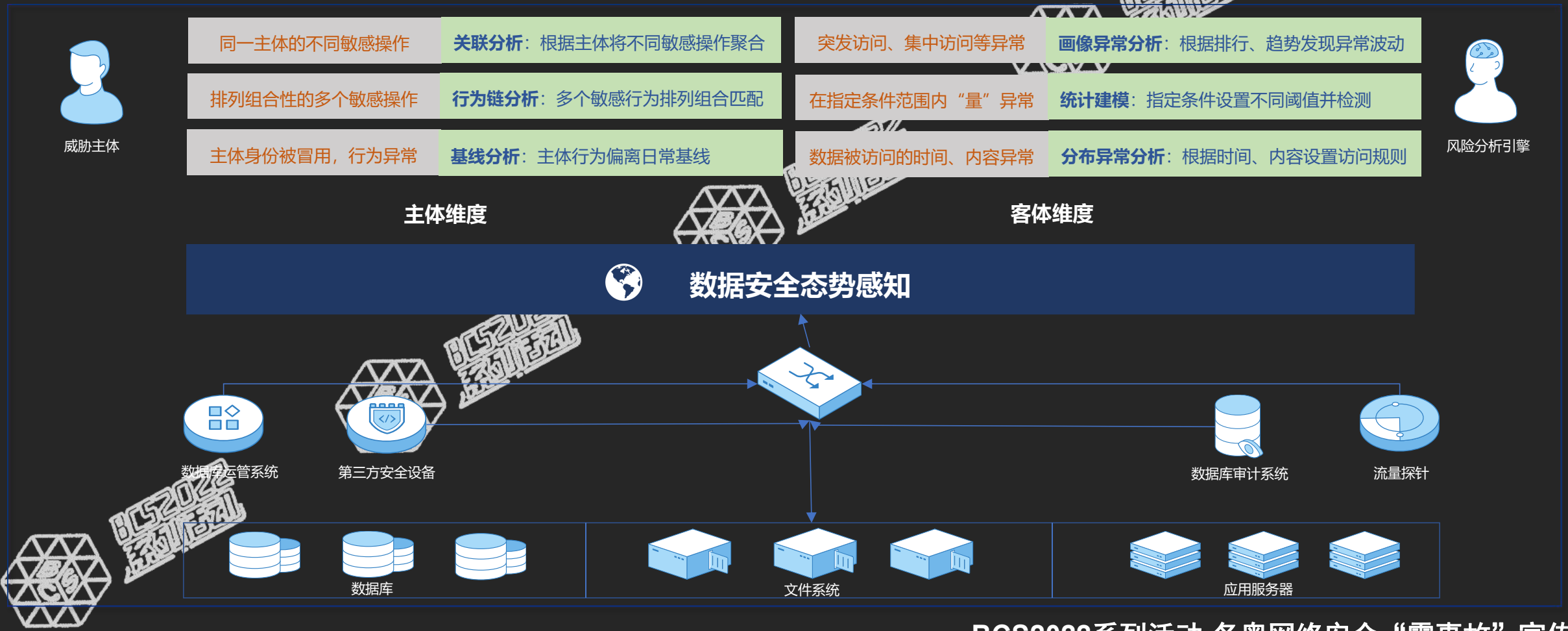
数 据 安 全 态 势 感 知

- **风险：**用户出于无心或恶意原因，进行违规访问，滥用权限，通过业务/运维权限窃取敏感数据。
- **方案：**通过应用流量探针和数据库审计探针，解析用户对敏感数据的访问流量，关联涉敏应用、接口，监测敏感数据流动，利用场景化数据访问风险

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

能力3：数据安全场景风险分析管理

数据安全态势感知可提供灵活的风险检测规则，针对主体维度提供关联分析、行为链分析、基线分析等分析技术，针对客体维度提供分布异常分析、统计建模、账号威胁分析等分析技术，主客体策略相互配合灵活应对**不同的风险场景。**



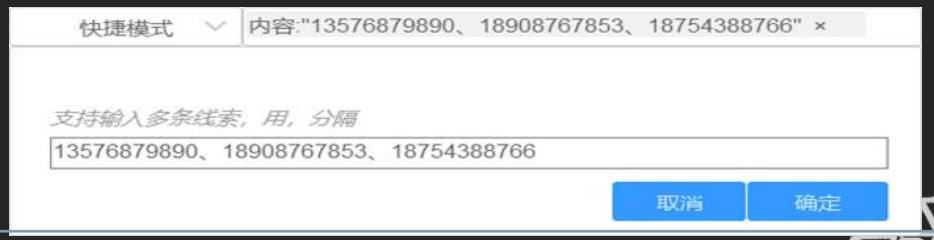
奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

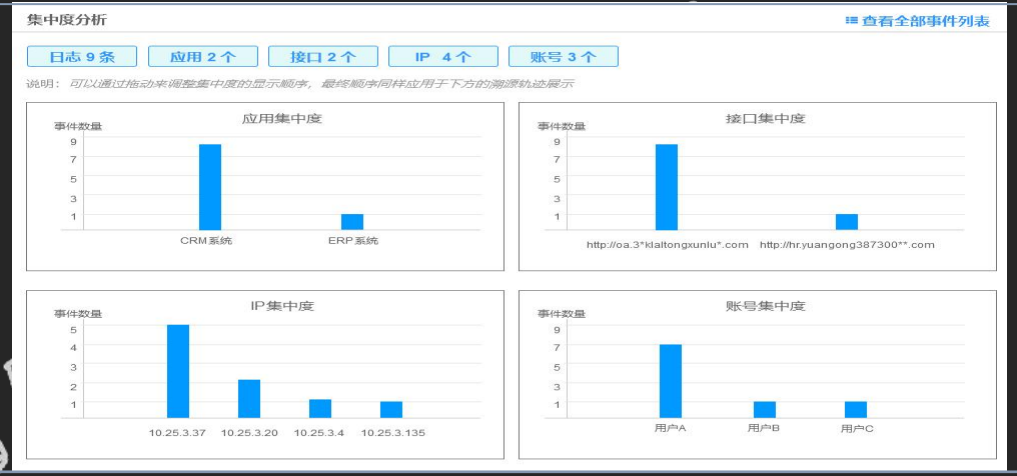
能力4：数据安全风险事件分析溯源

数据安全态势感知平台将应用、API、账号对敏感数据的访问行为信息存储到大数据平台，并提供详细的搜索手段，实现“以人追数”和“以数追人”，并支持下钻进一步搜索，能有效收窄泄密事件排查范围，还原泄密路径。

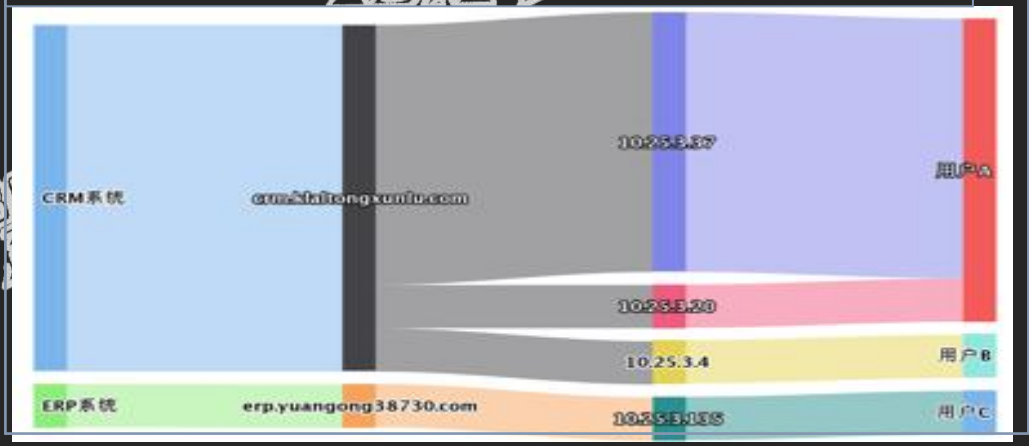
① 客户隐私信息泄漏，将多条泄漏手机号作为线索进行检索



② 得到与线索相关的日志9条、应用2个、接口2个、IP4个、用户3个，通过账号集中度分析发现用户A与线索相关日志7条，占日志总数的78%



③ 用户行为轨迹分析-桑吉图



④查看原始日志，发现用户A有非工作时间23点，使用非常用IP访问CRM的行为，而另外两个用户行为正常。初步判定用户A为数据泄漏源

时间	应用	接口	IP	账号	敏感标签	操作
2019-5-31 18:32:09	CRM系统	http://crm.klaltongxunlu.com	10.25.3.37	用户A	手机号	查看详情
2019-5-14 23:24:35	CRM系统	http://crm.klaltongxunlu.com	10.25.3.20	用户A	手机号	查看详情
2019-5-07 18:32:56	CRM系统	http://crm.klaltongxunlu.com	10.25.3.4	用户B	手机号	查看详情
2019-5-03 10:24:20	ERP系统	http://erp.yuangong38730.com	10.25.3.135	用户C	手机号	查看详情
2019-4-30 11:21:09	CRM系统	http://crm.klaltongxunlu.com	10.25.3.37	用户A	手机号	查看详情
2019-3-25 15:24:54	CRM系统	http://crm.klaltongxunlu.com	10.25.3.37	用户A	手机号	查看详情
2019-3-20 17:34:29	CRM系统	http://crm.klaltongxunlu.com	10.25.3.37	用户A	手机号	查看详情

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

04 国密安全

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

冬奥密码服务总体能力需求

冬奥密码专项于2020年（《密码法》颁布）完成设计、建设并持续运行维护到冬奥结束。冬奥存在50+以上信息系统，且为等保三级系统。根据冬奥会“网络安全总体规划”及GM/T 0054（也即2021年颁布的GB/T 39786前身）等相关技术要求，梳理出的密码服务能力需求。

一、物理与环境

- 冬奥数据中心运行在北京政务云（由阿里承建），物理与环境层面的密码能力主要由阿里自身提供。

二、网络与通信

- 为冬奥服务商及相关人员提供远程访问接入的能力，实现接入人员身份鉴别、通讯数据机密性和完整性的安全能力

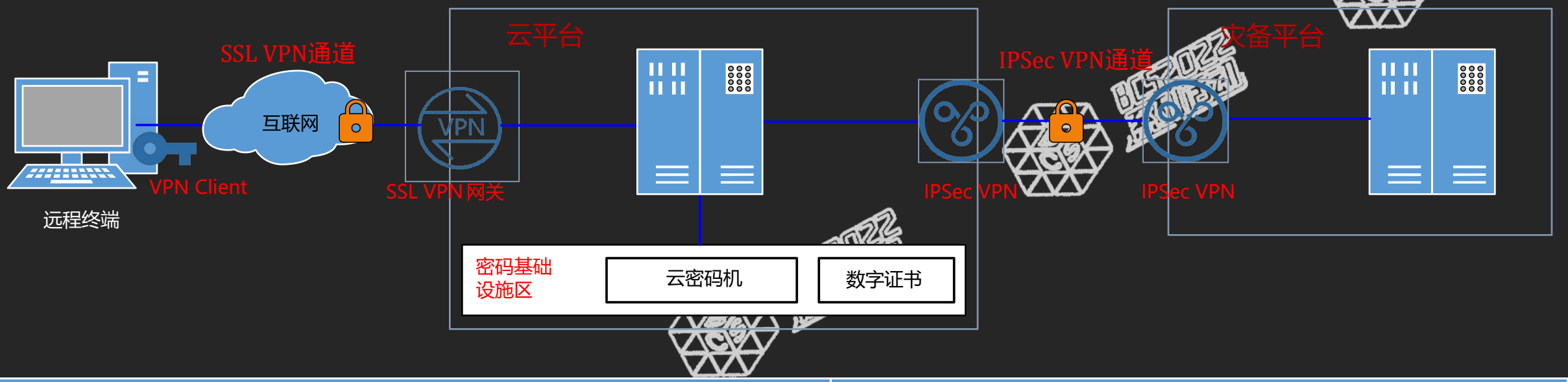
三、设备与计算

- 冬奥服务商及相关人员通过堡垒机对服务器、数据库、RDP应用运维审计过程中，实现人员身份鉴别、远程管理身份鉴别信息机密性、运维审计日志完整性的安全能力

四、应用与数据（重点）

- 冬奥个人隐私数据（如运动员、裁判员、志愿者等）在传输与存储过程中的机密性保护
- 用户身份鉴别以及身份鉴别信息的机密性的安全能力

网络与通信密码应用



场景1：终端与云平台之间通信

场景：

- 采用SSL VPN实现基于数字证书的终端身份鉴别；建立安全传输通道保护数据传输安全；
- 采用密码机保护用户访问控制信息和日志记录完整性；

密码产品：

- SSL VPN网关、服务器密码机等

场景2：云平台之间通信

场景：

- 采用IPSec VPN实现基于数字证书的通信双方身份鉴别；建立安全通道保护数据传输安全；
- 采用密码机保护用户访问控制信息和日志记录完整性

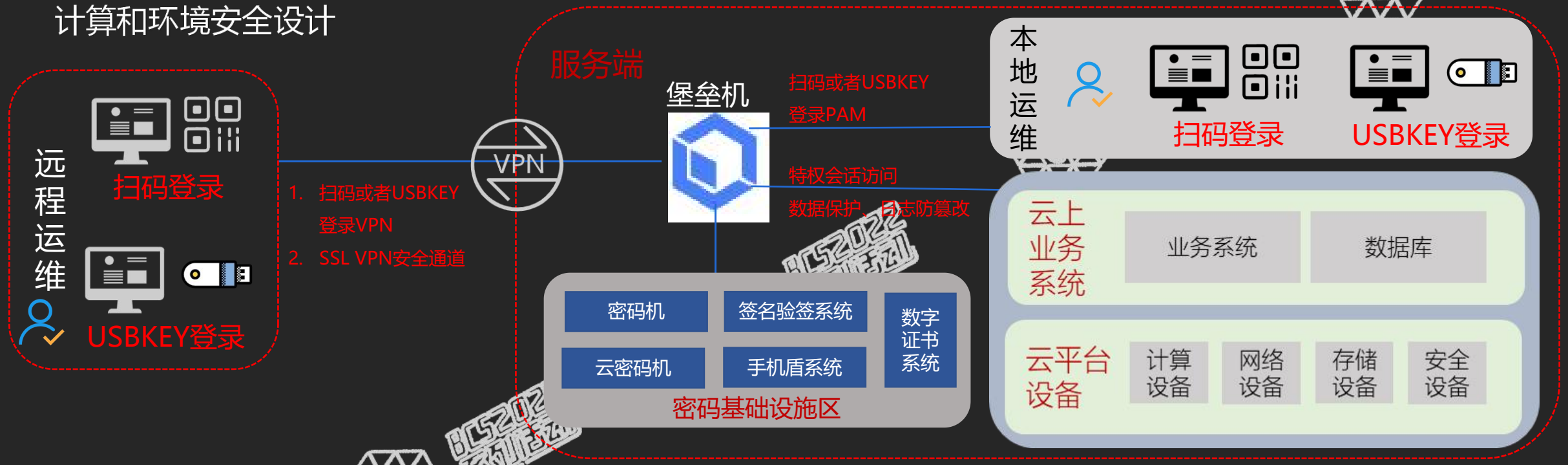
密码产品：

- IPSec VPN网关、服务器密码机等

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

设备与计算密码应用

计算和环境安全设计



场景：

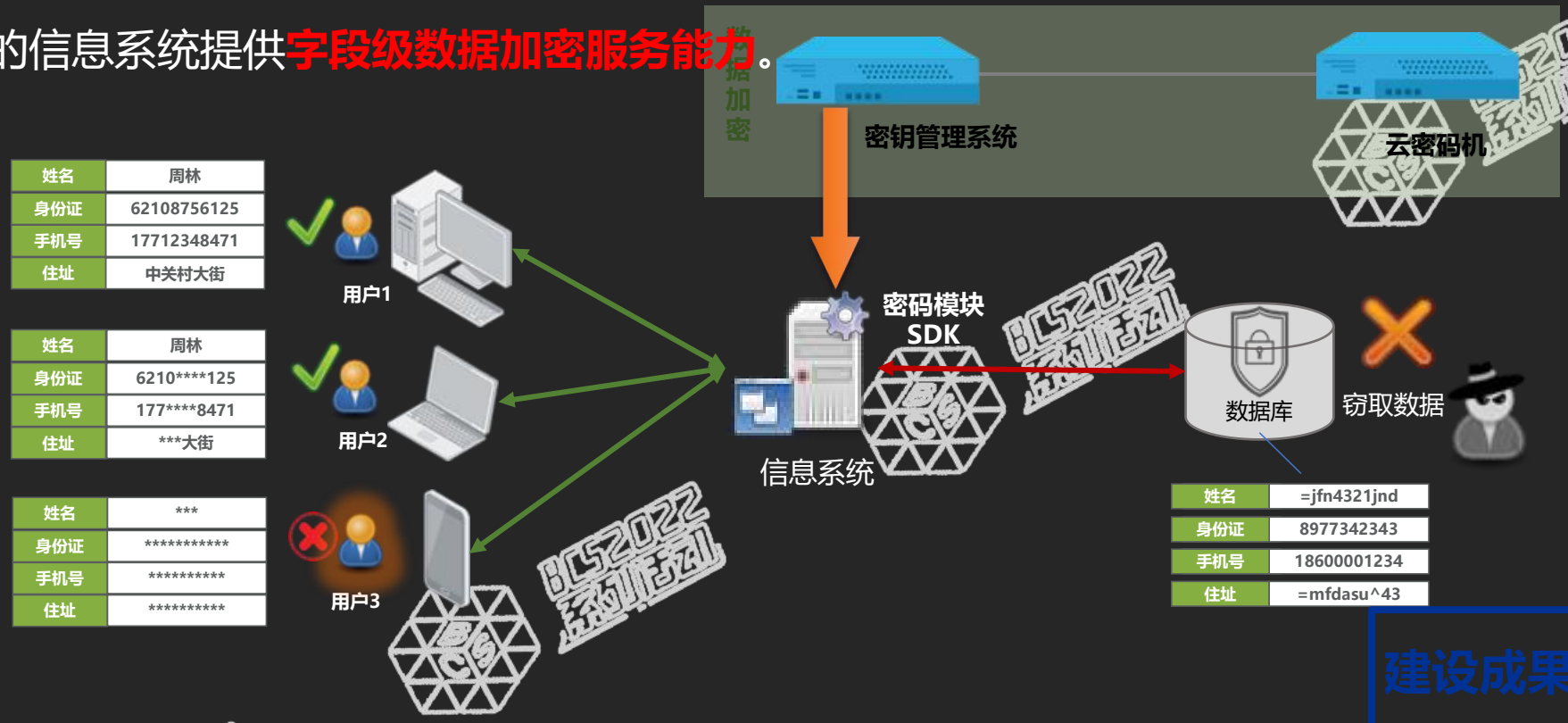
- 本地运维人员登录堡垒机、远程运维人员通过零信任TAP登录特权访问管理平台PAM时，采用手机盾扫码登录、USBKEY登录实现基于数字证书的身份鉴别；
- 采用服务器密码机实现用户访问控制信息和日志记录完整性保护

密码产品：

- USBKEY、服务器密码机、可信浏览器、SSLVPN网关以及国密堡垒机等

应用与数据密码应用

由密钥管理中心（KMC）提供集中的密钥管理能力，由密码模块SDK、云密码机（Cloud HSM）为冬奥50+以上的信息系统提供**字段级数据加密服务能力**。



密码产品：

- 密码模块SDK
- 密钥管理系统
- 密码机/云密码机

密码服务				
	对称加密（SM4）	公钥加密（SM2）	摘要运算（SM3）	/
	对称解密（SM4）	私钥解密（SM2）	设备证书服务	/
	创建应用主密钥	创建应用工作密钥	工作密钥加密数据	工作密钥解密数据

建设成果：

生产环境中共生成信息系统**主密钥47个，工作密钥621个， 涉及24个信息系统密钥，及12台密码机**的管理。

奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

冬奥密码成功经验总结

【冬奥密码专项】实现了高安全（等保三级），高复杂环境（国内外、云与本地），密码与网络安全密切配合的密码服务能力，是今后密码项目的标杆：

- 遵循“冬奥网络安全总体规划”、等保三级和密评安全三级的设计要求，方案先后通过多轮专家评审和安全评测；
- 密码作为基础设施，是冬奥第一个上线的安全专项，也先于所有的信息系统上线；
- 冬奥密码专项能容纳50+以上信息系统的密钥管理，实现了密钥集中统一管理，充分考虑了可靠性、安全性、容灾备份等设计。

BCS2022 系列活动

BEIJING 2022

冬奥历史上首次使用国密算法保护信息系统的核心数据

奇安信 新一代网络安全领军者

冬奥会官方网络安全服务
和杀毒软件赞助商

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

从冬奥密码专项走向更大的“密评”市场

随着《中华人民共和国密码法》、《GBT 39786-2021 信息安全技术 信息系统密码应用基本要求》、《信息系统密码应用测评要求》等相关法律法规的推出，国家高度重视商用密码的国产化，奇安信集团为了支持国家商用密码建设，大力发展商用密码业务。

目前，奇安信集团已经推出了适用于**各种应用场景的商用密码产品**，包括：服务器密码机、密码卡、签名验证服务器、安全认证网关、安全网关等硬件产品，以及国密安全密码应用中间件、可信浏览器、身份认证系统、密钥管理系统、手机盾、电子签章等软件系统。公司密码产品已应用于**北京冬奥会、全国疫情防控等**若干重大项目中。并具备将冬奥密码成功经验复制到关键信息基础设施、网络安全等级保护第三级及以上信息系统的国密改造上的能力。

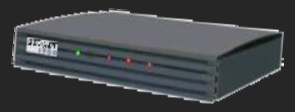
公司非常注重用户的售前/售后服务，我们认为优异的产品配合完善的服务才能形成良好的应用及高质量的客户满意度，奇安信集团拥有一支专业的、全国覆盖的、高质量的商用密码售前/售后支持团队，能够为用户提供全面的商用密码应用解决方案及技术咨询。

奇安信 BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

附件：冬奥密码建设产品列表

服务器密码机/云密码机



加解密服务运算的核心。满足《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》支持密钥生成与管理、密钥的安全存储、加解密服务，密码相关服务。

可信浏览器

满足国家标准《GM/T 0024-2014: SSL VPN技术规范》，支持国产密码算法，支持国密SM2证书、密码套件、国密SSL协议。

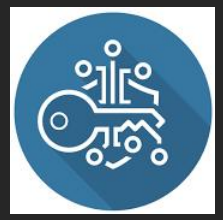
密码应用中间件（密码模块SDK）

满足《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》，作为信息系统与密码应用系统及密码设备之间的重要中间件，提供了统一的密码接口、密钥管理、密码设备与计算资源调度，以及特色的密码设备模拟器，一站式解决信息系统密码建设难的困境，快速赋能安全合规的国密能力。

智能密码钥匙

USBKey中存放标识用户身份的数字证书，满足《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》对身份鉴别、密钥管理、建设运行等方面的要求。

密钥管理系统



满足GM/T 0038-2014《证书认证密钥管理系统检测规范》，支持国产密码算法，提供密钥在整个生命周期中的安全管理，包括生成、存储、分发、备份、更新、撤销、归档和恢复等。

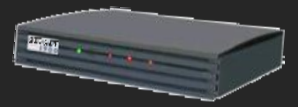
SSL VPN/IPsec VPN/安全网关

用于在网络上建立安全的信息传输通道，通过对数据包的加密和数据包目标地址的转换实现远程访问，进行加密通信。支持国密IPSec或SSL VPN通道的构建。

数字证书认证系统

满足标准GB/T 25056-2018《信息安全技术 证书认证系统密码及相关安全技术规范》，提供数字证书的申请、审核、签发、注销、更新、查询、下载等全生命周期的综合管理功能。

国密堡垒机



支持国产密码算法，采用旁路部署模式切断终端对网络和服务器资源的直接访问，使用协议代理方式，实现运维集中化管控、过程实时监管、访问合规控制、过程图形化审计，构建事前预防、事中监控、事后审计的安全管理体系。

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

BCS2022系列活动-冬奥网络安全“零事故”宣传周