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

守护云安全 构建冬奥安保最后一道防线

王健 奇安信集团服务器安全事业部负责人

奇安信

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

从主机侧保障冬奥所有业务安全运行

服务器跨区域管理

基于奇安信服务器安全管理系统，实现云上+云下服务器跨区域统一管理，涵盖赛事管理、运维管理、冬奥场馆等数十个冬奥业务系统

让业务以最小代价获得安全防护

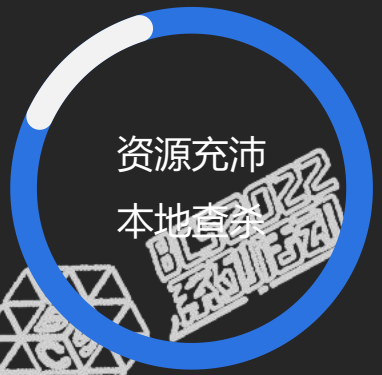
采用业务优先原则，限制agent客户端自身CPU使用率，当业务应用资源使用率超过设置阈值时，agent自动停用

奇安信 BEIJING 2022

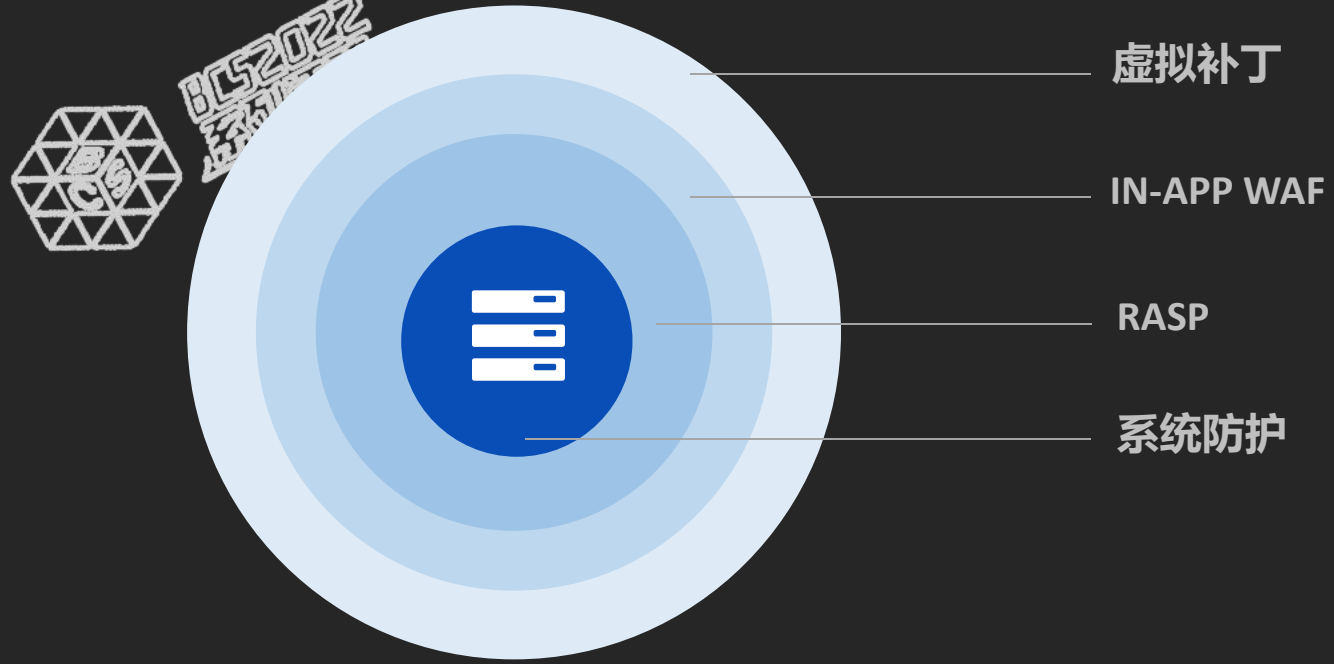
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

从主机侧保障冬奥所有业务安全运行

服务器杀毒双模式切换



服务器深层次入侵防御体系

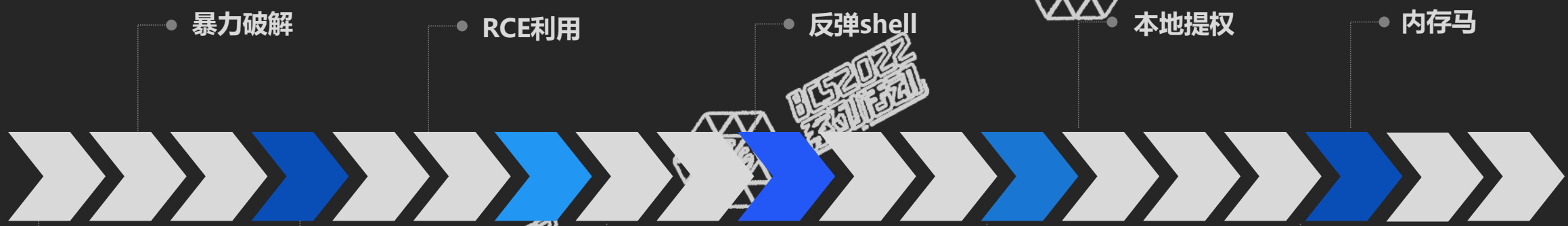


奇安信 BEIJING 2022

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

从主机侧保障冬奥所有业务安全运行

- 联合安服团队，打造基于攻防实战低误报、可研判的服务器威胁监测



- 暴力破解
- RCE利用
- 反弹shell
- 本地提权
- 内存马
- 恶意扫描
- 异常行为检测
- Webshell
- 无文件攻击
- 后门检测

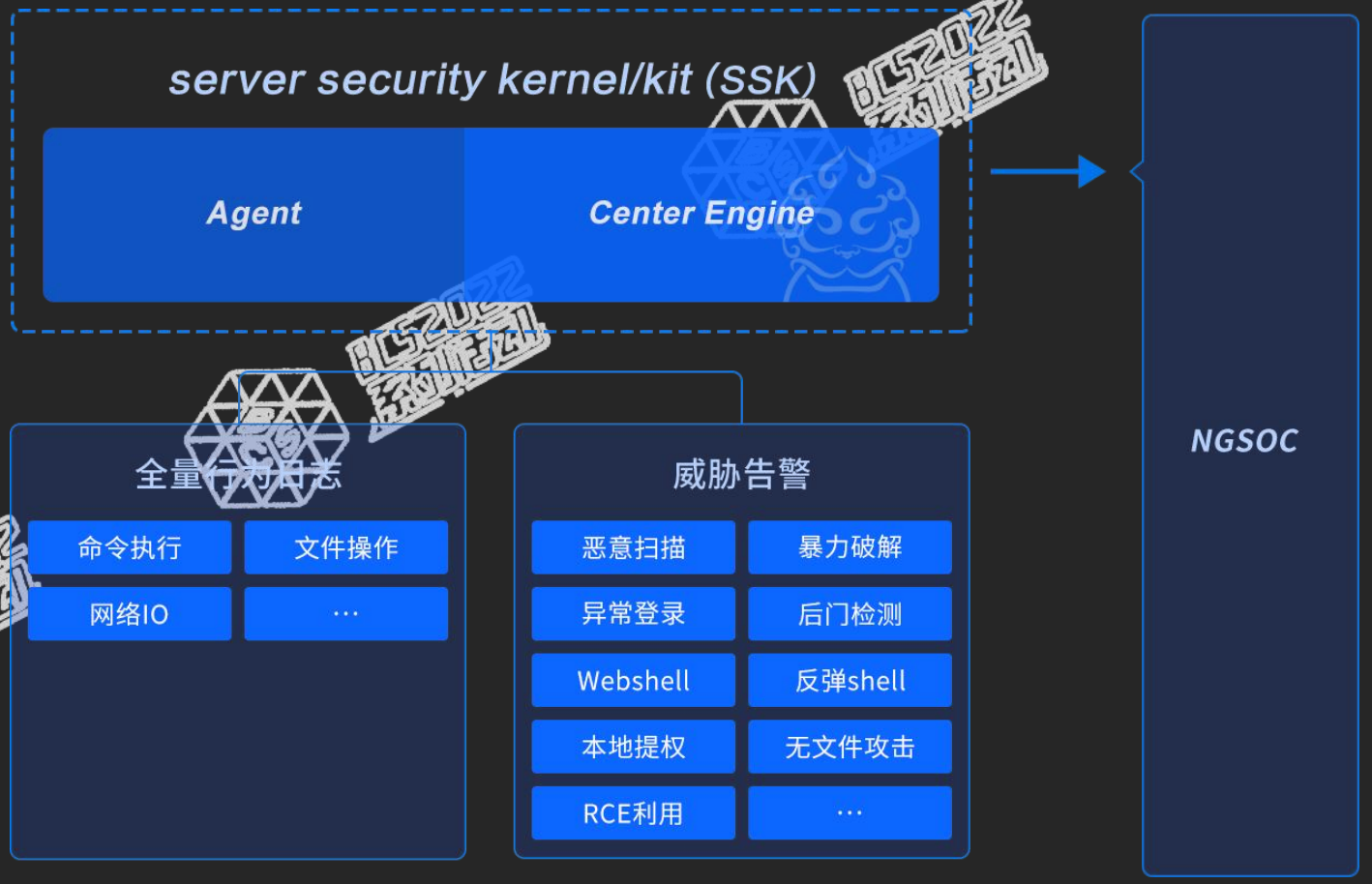
奇安信 BEIJING 2022
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

奇安信产品体系内的协防及联动

- 目前攻击安全设备已经成为新型的攻击趋势，如果安全设备自身存在安全风险，也极易成为黑客攻击的入口，有了服务器安全管理系统的加持，让奇安信整个安全体系的安全性、可用性和可靠性进一步提升。

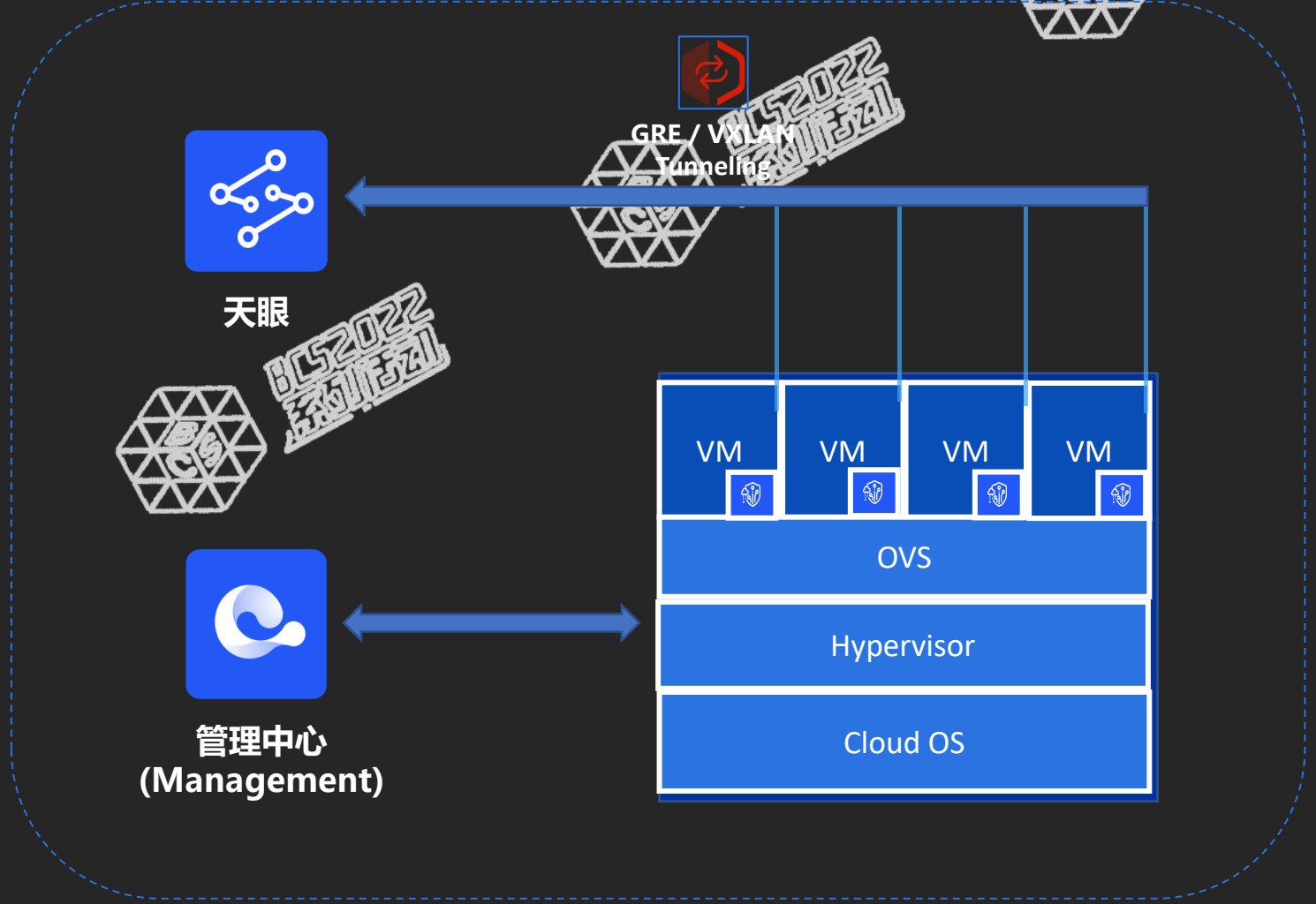
奇安信产品体系内的协防及联动

- 威胁告警及全量行为日志
  实时推送给NGSOC



奇安信产品体系内的协防及联动

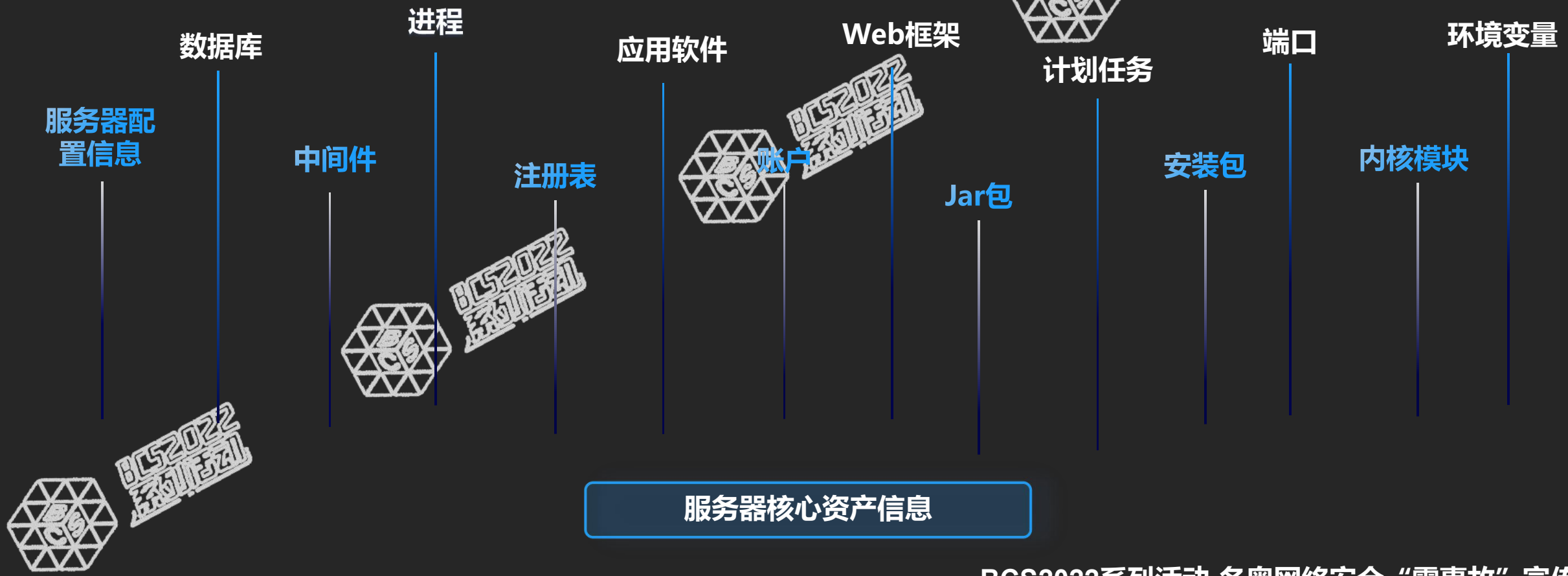
- 通过流量采集&转发模块，将云上网络流量牵引至天眼。保证天眼在云上/云下流量的可见性



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

奇安信产品体系内的协防及联动

- 服务器资产数据接入**奇安信系统安全平台**，实现漏洞资产快速排查。



奇安信

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

冬奥客户侧安保缩影：某集团客户

冬奥前准备

协助客户快速完成400+的重要业务系统服务器的产品部署和策略调试。

冬奥期间保障

由安服团队资深专家为客户提供服务器侧资产梳理、威胁狩猎、告警分析等核心安全服务，帮助客户实现实现服务器整体安全状态监控、资产与风险管理以及攻击事件的专业研判。

在冬奥期间，团队多次发现webshell文件异常上传的拦截告警，通过安全专家的远程分析，及时发现恶意webshell文件，并协助客户通过日志溯源能力锁定了攻击源地址进行处置。

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

THANKS