信息审计系统

全面记录、深度还原、合规审计

## 产品概述

捷普信息审计系统是国内首款融合数据库审计、网络信息内容审计、网络风险行为审计以及安全审计四大功能于一体的信息系统审计产品。该系统广泛应用于业务专网、涉密信息系统、企事业单位及政府机关，成为掌控网络行为、降低泄密风险、规避法律风险、保障网络安全的一把利器。

## 产品特点



**深度协议解析还原能力**

系统融合了对数据包的特征匹配和语义分析技术，实现对网络层到应用层的协议分析。邮件审计功能能够审计发件人、收件人、主题正文、附件，并能深度解析pdf、doc、zip、rar等7大类164种文件格式。通过深度解析还原数据的审计事件、日志、会话信息、会话交互的完整记录和回放，实现网络系统的全面安全监控。

**全面的协议覆盖能力**

提供OA操作的审计，支持包括网站访问、邮件收发等应用的HTTP、SMTP、POP3、IMAP、FTP、Telnet、SAMBA、NFS等协议，能够实现URL、邮件内容的审计；针对多种类型数据库系统审计，能够还原登陆用户、SQL命令和字段级审计，并能对SQL命令、字段、字段值、安全级别进行自定义审计；针对运维操作审计，支持包括Telnet、FTP、Radius、Rlogin等协议，能够实现全程操作的过程回放以及关键命令的审计。

**多编码方式处理能力**

具备多种编码识别能力，支持包括ASCII、GB2312、UTF-8/16/32、GBK、BIG5、GB18030等编码方式、有效杜绝不同编码方式数据库审计的遗漏，规避了审计记录乱码不易阅读和审计的问题。

**便捷的系统使用维护**

采用“零配置”技术，从系统正确部署运行后实时的内容监测、规则更新、报表统计生成、审计数据备份活动都将智能进行，管理员只需要定期对审计报告进行查阅就能轻松掌握网络安全状态。旁路部署方式不需要对现有的网络体系结构进行调整，工作时也不会影响网络的运行与性能。支持多点分布部署集中统一进行日志收集管理。

**IPv4/IPv6双栈高效审计**

系统基于双栈架构，完善支持IPv6协议环境下的安全审计，为IPv6环境提供有力的安全审计保障。

## 产品功能

**网络行为审计**

捷普JBCA可全面记录用户的网络使用行为，基于系统内置的强大应用特征库和URL分类库，可以对各种常见网络应用访问及站点访问进行精准识别，进而规范办公时间的网络使用行为，促进工作效率。

**内容还原与审计**

捷普JBCA支持客户端邮件和19种主流WEB邮件的正文、主题、附件等进行完整内容还原，用户可根据需要进行查看、附件下载、敏感关键字审计等操作。支持32种常用博客论坛发帖与文件上传内容、20大类URL及网页内容、常用即时通信的聊天内容还原与敏感信息审计。

**合规性审计**

互联网加速了信息的传播速度、扩大了传播范围，一旦出现利用企业、政府网络散播非法言论的行为，将会给企业带来巨大的法律风险，有损政府权威形象。捷普JBCA全面支持30余种主流论坛博客的发帖内容审计，内置敏感信息关键字库，帮助企业和政府规避风险。系统通过对合规性的深入分析，满足用户对法律、法规，如等级保护、分级保护和行业内规的要求。

**敏感信息外泄监控**

信息是企业的核心资产，利用网络进行敏感信息的泄漏和传播的安全事件时有发生。捷普JBCA提供强大的内容审计功能，针对邮件外发、论坛发帖、文件上传等各种途径，文档压缩、变换文件格式等各种手段，均可有效识别敏感信息，降低泄密风险。

**网络风险识别**

捷普JBCA内置安全审计引擎，对各种漏洞扫描、恶意脚本、异常协议行为可以准确识别和审计，同时提供病毒扫描功能，对邮件附件进行安全扫描，及时发现危害网络安全的攻击行为。系统支持与防火墙联动，对各种异常行为进行阻断。

**APP移动管理**

支持捷普设备管家（IOS/Android版）移动管理，便于随时随地查看捷普JBCA及捷普其他安全设备的运行状况，快速了解业务情况、响应安全问题。

## 产品部署

捷普信息审计系统多采用旁路部署方式与核心交换镜像口相连，对原有网络结构不产生影响。系统支持分级部署和集中管理，实现在大型网络中审计产品的统一安全管理和审计记录的综合分析。

