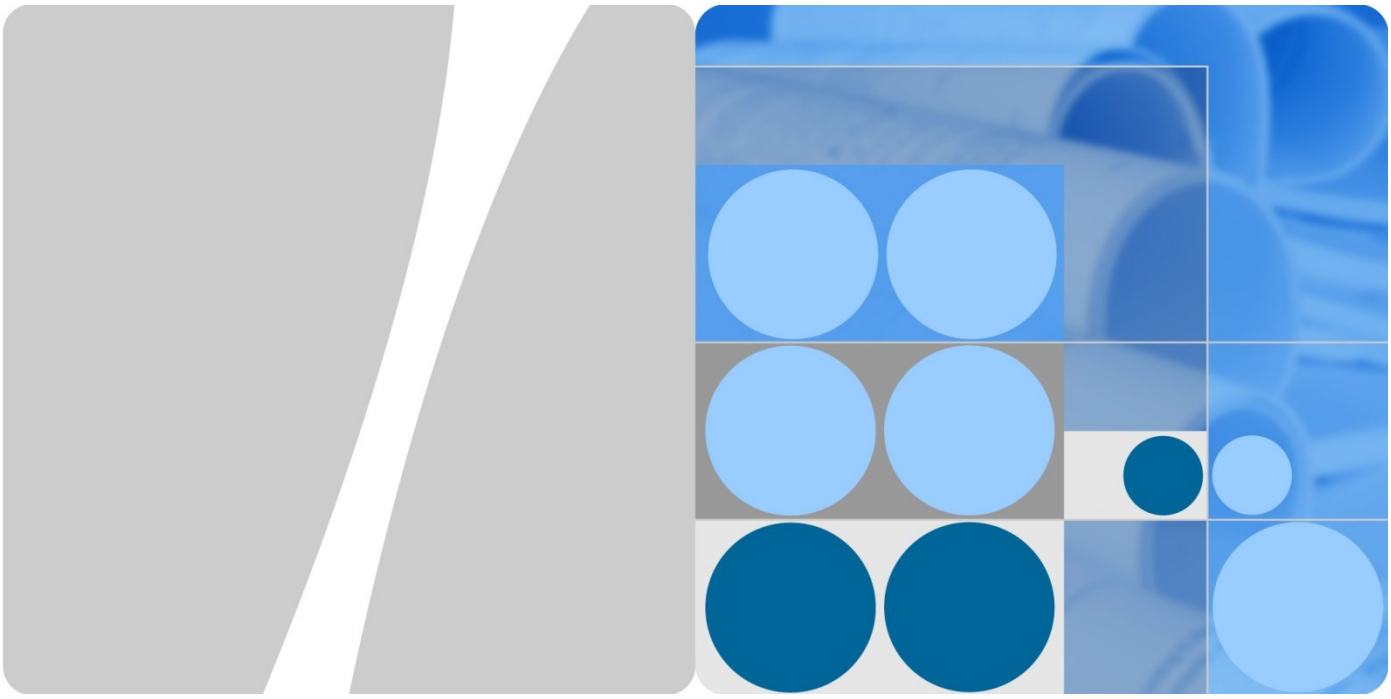


华为 UMA-DB 数据库审计产品销售指导书

华为技术有限公司

HUAWEI

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 总体销售策略

1.1 产品定位

华为数据库审计系统是华为公司面向**医疗卫生、政府、金融、能源、交通、运营商、电力、大中型企业以及上市公司**推出的数据解决方案，为用户解决**数据核心信息泄露篡改，数据库操作不可控**和**IT内控外审**的问题。有效帮助用户满足法案法规要求，顺利通过IT审计；实时进行异常监控，及时发现安全事件；完整审计业务信息，重溯业务准确定责。

华为数据库审计系统（UMA-DB）通过旁路侦听的方式对访问数据库的数据流进行采集、分析和识别。实时监视数据库的运行状态，记录多种访问数据库行为，发现对数据库的异常访问，并对访问数据库的相关行为、发送和接收的相关内容进行存储、分析、排名和查询。通过专门细致的网络数据获取协议分析技术、数据存储技术、数据查询技术并配合完善的管理规则，帮助用户应对来自网络中的风险和挑战。

1.2 产品规格

华为数据库审计产品共分为两个型号：UMA-DB标准版和UMA-DB企业版；标准版主要面向中低端市场，企业版主要面向高端市场。

硬件规格：

华为UMA-DB数据库审计规格清单		
产品型号	UMA-DB标准版	UMA-DB企业版
设备规格	2U	2U
SQL交易量	峰值:20000条/秒	峰值:30000条/秒
会话并发	2000	4000
硬盘	2T*4（可扩展）	2T*4（可扩展）
RAID	RAID10	RAID 10
内存	8G	16G
CPU	1*四核	2*四核
网口	6个千兆以太网电口	8个千兆以太网电口（可扩展）
电源风扇	1+1冗余电源、风扇	1+1冗余电源、风扇

兼容性	ORACLE、DB2、SYSBASE、INFORMIX、SQL SEVER等以及其子版本	ORACLE、DB2、SYSBASE、INFORMIX、SQL SEVER等以及其子版本

功能规格：

华为UMA-DB数据库审计规格清单		
产品型号	UMA-DB标准版	UMA-DB企业版
Ø 系统管理	对数据库审计系统本身的配置，以便对系统的访问、授权与管理等功能。其中包括：接口配置、用户管理、输出配置与授权许可。	
策略管理	对目标数据库服务器资产的添加、授权、策略制定、告警设置等配置功能。其中包括：资产、白名单、对象、策略、动作与管理。	
日志审计	日志审计是以数据库服务器资产为审计对象，从而记录运维人员对数据库服务器的操作与访问的行为；便对数据库运行情况的实时查看、故障分析以及告警级别的确定。其中包括：会话审计、策略告警、异常告警与系统事件。	
实时监控	实时监控提供数据库实时监控功能，可以对总体或数据库类型或数据库组别进行实时监控，监控其网络流量、数据包、突发链接、并发连接数、SQL语句数。并提供波形图展示，用户能够直观地了解当前数据库运行状态。	
系统监测	系统监测是用户通过数据库审计系统的审计数据信息的显示；以便用户全面的、统一的、及时的对数据库服务器的运行情况进行分析与排错。其中包括：最新策略告警、最新违规操作、最新系统事件。	
变量绑定	无	能够完整、细粒度地解析绑定变量。可以精确定位到操作客体，真正审计到数据发生了什么事情。
超长SQL解析	无	支持对超过1500字节的SQL语句进行完整重组，实现审计和解析，保证审计日志的完整性和可靠性，无遗漏。
会话PCAP记录	无	能够完整记录会话的原始PCAP数据包，并提供下载分析。

1.3 应用场景

UMA-DB作为专业的数据库审计产品，主要应用于医疗卫生、金融、政府、能源、交通、电力、企业、教育、运营商等领域，为客户提供全方位的数据库审计和监测解决方案。

1.3.1 金融行业应用场景

行业需求：

随着信息系统在金融行业业务运营中的作用越来越重要，金融行业信息系统所面临的威胁和风险也越来越大。在网络传输中的大量金融交易数据，以及所涉及的公民和机构的个体资金信息，必然引来外部黑客或不法分子虎视眈眈，巨大的商业利益驱使让内部违规或犯罪事件逐年大幅提升。

而数据库作为金融行业信息系统的核心和基础，承载着越来越多的关键业务系统，整个业务流程过程中的操作、数据的变更、新增、删除都存储在数据库中，保存着客户的个人以及资金等各类信息。信息一旦被篡改或者泄露，不仅损害到公民自身利益，机构的品牌形象，甚至影响到公共秩序和国家利益。所以对数据库的保护是一项必须的，关键的，重要的工作任务

部署UMA-DB带来的用户收益：

1. 满足合规性要求，顺利通过 IT 审计

数据库审计系统为用户核心系统提供了独立的审计解决方案，有助于完善组织的 IT 内控体系，从而满足各种合规性要求，并且使组织能够顺利通过 IT 审计。

2. 有效减少核心信息资产的破坏和泄露

对金融行业的业务系统来说，真正重要的核心信息资产往往存放在少数几个关键系统上(如数据库服务器、应用服务器等)，通过使用数据库安全审计产品，能够加强对这些关键系统的审计，从而有效地减少对核心信息资产的破坏和数据泄露。

3. 追踪溯源，便于事后追查原因与界定责任

负责运维的部门通常拥有数据库管理系统的最高权限(掌握 DBA 账号的口令)，因而也承担着很高的风险(误操作或者是个别人员的恶意破坏)。审计系统能够帮助企业进行事后追查原因与界定责任。

4. 直观掌握业务系统运行的安全状况

业务系统的正常运行需要一个安全、稳定的网络环境。对管理部门来说，网络环境的安全状况事关重大。审计系统提供业务流量监控与审计事件统计分析功能，能够直观地反映网络环境的安全状况。

5. 实现独立审计，完善 IT 内控机制

从内控的角度来看，IT 系统的使用权、管理权与监督权必须三权分立。审计系统实现独立审计，帮助监督人员获得有效的技术手段，从而完善企业 IT 内控机制。

1.3.2 医疗行业应用场景

行业需求：

作为支撑深化医药卫生体制改革“四梁八柱”的八柱之一，建立实用共享的医药卫生信息系统被明确纳入方案中。伴随着医疗信息建设的发展，医院信息系统等数据安全需求也成为发展的重点关注对象。而医疗机构作为涉及国计民生的重要组成部分，其安全保障事关社会稳定，因此必须按照国家政策的相关要求，全面实施信息安全等级保护。《医疗机构信息系统安全等级保护基本要求》也成为对各级医疗信息系统的合规性要求。

医疗行业数据库安全需求有以下几方面：

部署UMA-DB带来的用户收益：

针对医院各信息系统（HIS系统、RIS系统、LIS系统、CIS系统、PACS系统、CPR系统）数据库进行全面的风险分析与安全监控审计，关注核心数据和业务的完全审计，对业务不产生任何影响。

- 白名单自学习机制：快速为用户建立安全模型，优化策略体系，提高数据存储效率。

- 变量绑定：完美识别与匹配变量绑定值，精确跟踪个人信息、病历号、社保号、身份证号等关键信息的操作与变更，为业务审计提供精准信息来源。
- Select 返回值解析：实现双向审计。通过记录访问的回应信息可对敏感数据进行追踪，防止数据丢失和泄密，有效防止非法“统方”和患者信息泄露。
- 异常接入监控：对登录参数准确捕获与解析，及时发现数据泄密、非法接入、SQL 注入等多种安全事件。
- 分流器和分布式：通过分流器和分布式处理架构设计，提高 UMA-DB 的数据处理能力和可扩展性。满足卫生管理部门（卫生厅、卫生局）对下属各医院进行监管的需求。

1.3.3 政府行业应用场景

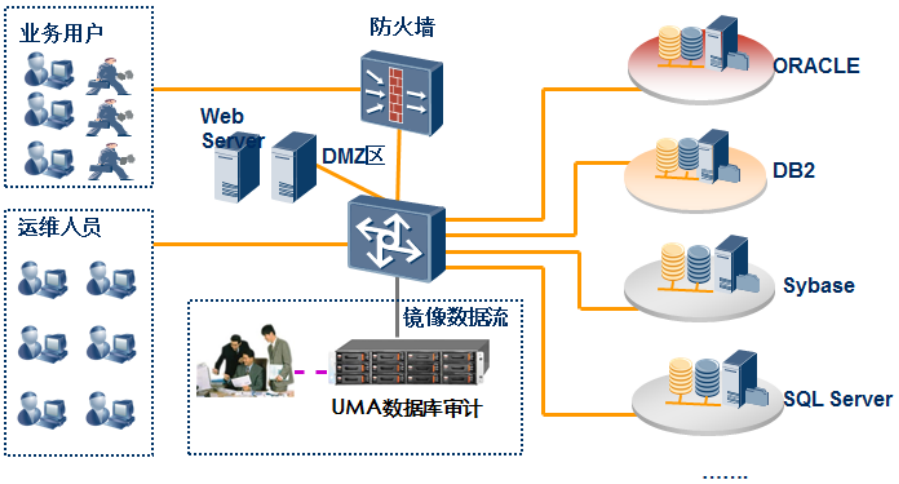
行业需求：

在网络信息技术高速发展的今天，信息安全的问题已经成为当下最热门的话题。信息是社会发展的重要战略资源，国际上针对信息的窃取、使用和控制的斗争越演越烈，各国暗地组织开展的网络对抗，直接影响国家大局和长远利益。信息安全成为维护国家安全和社会稳定的一个焦点，成为抵御网络战争攻击的屏障。政府机构从事的行业性质是跟国家紧密联系的，所涉及信息可以说都带有机密性，所以其信息安全问题，特别是对敏感信息的保护、核心数据资源的监控与审计成为政府信息系统建设的重要安全设计对象。

随着政府信息系统的建设，系统应用复杂化，电子政务网公开普及化，给数据安全性带来了高要求。但是针对于目前的建设状况，特别是对数据库的安全管理和审计，还存在着以下的一些问题：

- 无法有效分析数据来源，做到快速定位；
- 对关键数据的访问无记录，出现事故无法追踪；
- 对于黑客攻击，无法做到有效防范和攻击留痕；
- 非授权进入业务系统或误操作、越权操作，导致数据泄漏或被修改；
- 一旦数据库日志被清除，无法发现事故，无法做到事故定位；
- 没有数据库的完整审计记录，无法满足相关审计方面的要求。

部署UMA-DB带来的用户收益：



- 满足法案法规要求，顺利通过 IT 审计。
- 完整审计业务信息，重溯业务准确定责。
- 实时进行异常监控，及时发现安全事件。
- 掌控业务运行情况，直观评估运行性能。
- 调试分析查明真相，迅捷准确可靠伴侣。
- 三权分立独立审计，高效运维提高内控。

1.4 销售策略

1.4.1 国内运营商市场

在运营商市场，华为数据库审计系统可以为运营商各业务系统实现数据的风险监控和审计管理，记录所有业务数据的使用情况，还原所有业务过程，提供业务审计和调查取证的原始依据，同时满足合规审计的需求。

1.4.2 国内行业市场

主要目标市场有医疗卫生、电力、政府、金融、能源、交通、大中企业以及上市公司，以独立销售为主，重点从防泄密、合规性、安全审计方向引导。

1.4.3 海外市场

主要配合其他产品线以整体方案销售，可以适当独立拓展。

1.4.4 与其他整体方案配套销售

可以配合其他解决方案如安全审计、合规管控、等级保护等方案整合销售。

2 产品卖点

2.1 平台部署收益

华为数据库审计系统是组织核心资源安全运维管理与审计的一项有力工具和措施，可以在核心资源运维管理方面节省大量的人力、财力等，帮助用户构建更为安全、规范的IT运维环境。

- **满足法案法规要求，顺利通过 IT 审计。**

随着信息化的建设，安全性和标准化越来越被重视。特别来自监管部门，通过颁布各种法案法规以及相关指引，来加强企业内控。比如：政府行政事业单位或者是国有企业需要满足《信息系统安全等级保护基本要求》，国内上市公司需要执行《企业内部控制基本规范》，各行业合规性满足《银行业信息科技风险管理指引》、《证券公司内部控制指引》、《电力二次系统安全防护规定》等。

- **完整审计业务信息，重溯业务准确定责。**

审计数据是否完整直接决定审计的成败，0.01%数据的丢失也不能完整重溯业务流。特别是关键信息、敏感数据的丢失，将会影响到最终事件的追溯和相关责任人事故的认定。

- **实时进行异常监控，及时发现安全事件。**

通过对登录参数的完整获取，能够及时的发现恶意人员的非法访问；对敏感数据的追踪，能有效的发现数据泄密；对协议解析的完善，能准确的发现SQL注入等安全事件。

- **掌控业务运行情况，直观评估运行性能。**

业务系统的正常运行需要一个安全、稳定的运行环境，而数据库作为业务系统核心源泉其实时性能的掌握对管理部门来说事关重大。审计系统通过多窗口多参数，实时展示数据库运行情况，直观反映业务系统的稳定性和安全性，提高管理效率和降低运维成本。

- **三权分立独立审计，高效运维提高内控。**

审计系统作为第三方独立审计设备，实现了使用权、管理权与监督权的三权分立；同时也帮助监督人员获得有效的技术手段，完善企业IT内控机制。

2.2 我司产品优势

2.2.1 流技术与完整会话审计

数据库审计系统采用现今最先进的网络数据审计技术——流技术，保存“流生命期”内“上下文”相关环境，进行分析解码。数据库审计系统根据流ID进行相关记录，每个会话数据流具备一个64位长的唯一ID。流与流之间，保证高度唯一性。

深度解码数据库网络数据流传输协议，完整、细粒度分析并再现用户数据库操作活动会话过程。会话审计内容从访问的发起、连接、到结束进行完整记录。完整记录用户数据库会话细节，包括用户数据库登录行为、登出行为、SQL操作用户名称、SQL操作源程序名称、SQL操作源终端名称、SQL操作源终端登录用户名称、SQL会话参数设置、SQL操作语句、SQL操作返回状态、SQL操作涉及表组、字段、视图、索引、过程 、函数、SQL DML操作影响行数、SQL语句执行时间、原始数据库记录包等。

完整解析、记录、关联SQL操作语句参数，可自动回溯重构完整SQL操作语句。

2.2.2 “细粒度”数据库审计

提供灵活的数据库访问行为来源限制，可选择忽略审计特定网络和主机产生的数据库SQL操作；亦可限制仅对特定“嫌疑”对象进行细粒度、全方位审计，包括记录整个数据库操作会话过程所有网络数据包。

覆盖主流商用数据库，包括：Oracle 8/9/10/11等、Sybase所有版本、SQL Server 2000/2005、Informix所有版本、DB2所有版本。

2.2.3 超长 SQL 语句审计

在以太网传输中，链路层所能承受的最大数据长度(MTU)为1500字节，除去IP/TCP头长度最大报文段长度有1460字节。若总长度大于1500字节，数据包将会被分片。所以我们把超过1460个字节的SQL语句称之为超长SQL语句。

目前国内数据库审计产品多数是基于IDS产品改造而成，只能对单个网络数据包进行分析，加之协议解码的不完全，使超长SQL语句无法审计，提供了逃避审计的通道，造成了审计数据的不完整。实际应用中由于SQL语句的长度无限制，使长SQL语句的使用非常普遍，形成了业务操作审计信息的缺失；同时，利用超长SQL语句特点以及SQL语句可注释功能，恶意攻击者可以构建出针对“初级简单数据库协议审计”的

“逃避审计办法”，达成非法操作的目的。

数据库审计系统是基于流和会话技术，进行全状态、全协议解码，能完整的、细粒度的解析超长SQL语句。通过对超长SQL语句的完全审计，监控了恶意攻击者妄想通过逃避审计对数据库造成非法操作的途径，为安全事件的追溯提供了强有力的证据；同时也为实际业务中SQL语句的全面审计提供了保障。

2.2.4 绑定变量解析技术

SQL语句允许通过符号占位，然后再通过对占位符号赋值的方式，完成SQL语句操作请求。绑定变量是替代SQL语句中的常量的替代变量。目前五大商用数据库管理工具与服务端之间数据库的查询大量使用变量绑定来完成，任何标准数据库管理工具，都会使用变量绑定对数据库进行管理。

在使用变量绑定的数据库操作环境内，SQL语句仅仅是数据库操作动作，数据库操作涉及到的库和表，数据库数据操作关系等模态化硬解析固件，涉及到的数据库数据并不包含在SQL语句内。在现实业务活动过程中，数据库数据才同具体的财务和现实生活个体信息相关，而数据可能包含在变量绑定内。因此，变量绑定审计，成为数据库审计分析产品的必备和必需功能。只有实现变量绑定的数据库审计分析产品，才能定位SQL语句的操作客体，有能力解决中间件审计问题，具备真实可靠的有用性。

目前其他的旁路数据库审计厂商主要通过三层审计关联来解决中间件审计问题，这其实是一个误区。由于中间件应用没有一个统一的标准，因此要自动识别各种中间件的应用比较难，目前的做法大部分是通过对前端浏览器与WEB服务器之间的HTTP通讯协议进行分析，根据对URL、时间片及一些关键信息进行分析，然后再与后端的数据库操作进行关联来实现。这类厂商由于连最基本的协议解码和变量绑定都没有实现，数据库协议分析审计部分缺乏关联数据源，所谓关联审计根本不可行。

数据库审计系统是基于流和会话技术，进行全状态、全协议解码，能完整的、细粒度的解析绑定变量。可以精确定位到操作客体，真正审计到数据发生了什么事情。通过变量绑定以及SQL语句的全记录，可以完整的重溯整个业务流程，追溯信息的来龙去脉，成为全球第一家通过变量绑定技术真正解决中间件审计问题的数据库审计厂商，为数据的完整性、有用性和准确性提供了强有力的技术保证和原始证据。

目前DB2变量绑定特性：一次SQL语句提交，无限次变量提交，每次提交值都会产生数据变更，数据库审计系统能完整记录并准确关联（不是用流技术的其它同类产品基本无法实现）。

2.1.1 三层应用审计

- 业务帐号审计
  - 业务账号：业务系统账号、网银帐号、流水帐号、银行卡号、手机号、邮箱帐号等；
  - 业务账号以 SQL 语句提交或以绑定变量值提交至数据库；
  - 数据库审计系统在完成深度解码的基础上，完整解析数据协议中的业务账号。
- 业务操作审计
  - 业务操作：登录(login)、查询(select)、添加(insert)、删除(delete/drop)、修改(update)、登出(logout)等；
  - 数据库审计系统在完成会话审计与深度解码的基础上，完整解析数据协议中的业务操作动作。

2.2.5SELECT 返回值解析

数据库审计系统基于流会话跟踪审计，实现SELECT返回值解析。通过记录访问的回应信息，可以有效的防止数据泄密和窃取，监视和控制被存取的数据。

2.2.6 原始流数据包记录（PCAP）

数据库审计系统不仅完整记录SQL语句，还能完整审计原始数据包，实现超级嗅探器功能。只有原始数据才能还原真实的数据现场，提供无可抵赖的强有力证据。

审计记录记录原始数据网络流量包，可下载至本地。

2.2.7 灵活的数据库访问策略

提供来源（客户端）登录IP异常探测、数据库登录用户名称异常探测、数据库操作源终端异常探测、数据库操作源程序名称异常探测、数据库操作源终端用户名称异常探测。

提供数据库SQL语句执行时间、数据库操作闲置时间策略报警，提供数据库DML、DDL等操作影响行数策略报警，提供数据库SELECT SQL操作语句返回行数策略报警。

提供全方位的策略规则匹配，策略因子包括：数据库操作来源IP地址、数据库服务器IP/端口、数据库类型、数据库名称、数据库登录用户名称、数据库操作源程序名称、数据库操作源终端名称、数据库操作源终端用户名称、SQL操作语句（DDL、DML、DCL）、高级权限操作、存储过程、数据库表组（表、字段、

值）、数据库SCHEMA、操作执行时间、操作返回条目大小等。

根据设定的数据库策略，可选择对关键资源操作行为进行数据包录像、深度分析解析开关。

2.2.8 全文检索功能

记录数据库会话详细细节，当发生数据库安全事件时，用户可根据数据库地址、源客户端地址、事件时间、SQL语句关键词、数据库账号、数据库地址等，快速检索定位操作会话。

数据库审计系统通过细粒度的过滤条件，在海量数据中快速定位审计日志。检索条件越丰富，查询越快，定位更准。

2.2.9 异常告警、实时监控

提供完善的违规实时告警，包括异常告警、违反策略告警等。及时发现数据库非法接入、SQL注入、数据泄密等安全事件。

高危SQL命令告警，如对drop、delete等高危SQL命令进行实时告警。

关注表列告警，如对数据库表做过drop或delete动作，进行实时告警。

多形式的实时告警：当检测到可疑操作或违反审计规则的操作时，系统可以通过WEB告警、邮件告警等方式通知数据库管理员。

实时监控来自各个层面的所有数据库活动，包括网络流量、数据包、突发连接、并发连接、SQL语句的实时数量，并且提供实时的视图窗口查看数据库的运行状态。它可以帮助DBA更好的管理数据库。

2.2.10 业务跟踪审计

拥有业务跟踪审计的能力，对于整个业务流程的操作以及业务数据的删除、添加或修改进行完全审计。通过审计信息，可以重溯整个业务流程。

第一步： 1.登录业务系统

2012-04-12 13:49:46	153	/*DbXpert Prepare SQL Statement: PKGSN = 3*/ call CB_PCKG_LOGON_CERT_USER_LOGON (?, ?)

2.提交登录参数

2012-04-12 13:49:46	323	/*DbXpert Prepare SQL Statement: PKGSN = 3*/ Binded:Bind0=1000011730 Bind1=000001 Bind2=0 Bind3=122.224.166.198 Bind4=NULL Bind5=NULL Bind6=NULL Bind7=NULL Bind8=NULL Bind9=NULL Bind10=NULL Bind11=NULL Bind12=NULL Bind13=NULL Bind14=NULL Bind15=NULL Bind16=NULL Bind17=NULL Bind18=NULL Bind19=NULL Bind20=NULL Bind21=NULL

第二步： 1.更新业务数据

2012-04-12 13:49:46	94	/*DbXpert Prepare SQL Statement: PKGSN = 4*/ call CB_UPDATEACCSTT (?, ?, ?, ?, ?, ?, ?)

2.业务数据内容

2012-04-12 13:49:46	164	/*DbXpert Prepare SQL Statement: PKGSN = 4*/ Binded:Bind0=1000011730 Bind1=201000044264927 Bind2=1 Bind3=1 Bind4=1 Bind5=杭州圣治实业有限公司 Bind6=NULL

第三步： 1.业务操作完成

2012-04-12 13:49:45	108	/*DbXpert Prepare SQL Statement: PKGSN = 2*/ call CB_LOG_WRITE_COMMON_LOG (?, ?, ?, ?, ?, ?, ?, ?, ?)

2.完成动作内容

2012-04-12 13:49:46	250	/*DbXpert Prepare SQL Statement: PKGSN = 2*/ Binded:Bind0=1000011730 Bind1=000001 Bind2=000000 Bind3=00000000 Bind4=企业客户内码|操作员编号 Bind5=1000011730|000001 Bind6=EMILHUCNIHBRATFBHCFOILJQCJJVARGZHCERFEAN Bind7=S Bind8=交易成功

2.2.11 灵活的统一报表

可灵活定制报表格式和规范，可根据要求生成用户环境（如：数据库地址、数据库名称、访问源IP地址、用户名称、源程序名称、源终端名称等）自定义报表。

3 竞争分析

3.1 竞争对手对比一览表

厂商	市场份额/地位	竞争力的体现	战略控制点	市场战略
imperva	份额上,基本定位高端金融用户与运营商	目前市面上最好的数据库审计产品，定位高端	SQL 操作建模能力自学习技术	高端 高价格
安恒信息明御	中小金融行业客户占有率比较高,慢慢往政府医疗用户靠拢	国内厂商来说技术最强,捆绑了应用防火墙,价格适中	合规性 与国外产品相比较有比较高的性价比	行业覆盖
国都兴业慧眼	政府与军队,军工企业	资质比较全,长期在政府与军企客户	资质与军队案例	继续深挖政府与军工用户
南京横渡	在医疗行业份额较高	与医疗 HIS 等生产系统捆绑销售	成熟的医疗客户群体	深挖医疗
启明星辰	运营商与政府	商务,价格 大方案捆绑	成熟的营销体系跟销售队伍	二线产品 投入力度不大

3.2 竞争对手分析和竞争策略

3.2.1 安恒信息-明御数据库审计与风险控制系统

杭州安恒信息作为应用安全及数据库安全整体解决方案提供商，其强项是对网页安全和数据库漏洞扫描，明御数据库审计与风险控制系统作为主打产品，技术方面在国内属于领先，市场覆盖面较广，对其主要从以下几方面展开竞争：

- 只是基于事件、单个数据包审计的，无法做到流和会话的深度解析，属于IDS改产品。。
- 无法实现绑定变量解析和超长SQL语句（1500字节以上）解析，select返回值解析。
- 无法会话的原始数据包捕获（Pcap），实现数据的完整真实记录。
- 基于单包分析的原理，无法实现对数据库进行实时监控，

同时，在竞争的过程中需要规避一下几点：

- 安恒明御数据库审计系统支持除了数据库协议之外的其他协议类审计，如telnet、POP3、HTTP、SMTP等等。但是这些并不是数据库审计的范畴，起到了混淆视听的作用
- 安恒明御数据库审计系统增加了数据库漏洞扫描功能，通过这些辅助非核心功能，往往起到干扰的作用，需要对客户进行引导，关注数据库审计的核心目标。

3.2.2 启明星辰 一天玥网络安全审计系统

启明天玥网络安全审计系统是针对业务环境下的网络操作行为进行细粒度审计的合规性管理系统，属于大而全的审计产品，覆盖了各类网络协议，除了数据库协议外，还有 FTP、Telent、HTTP、POP3 等等，但是都没有进行深化，审计力度和效果都不好。可以从以下几方面展开竞争：

- 只是基于事件、单个数据包审计的，无法做到流和会话的深度解析，属于IDS改产品。。
- 配置界面混乱，配置复杂，加大了管理人员的投入。
- 由于审计的内容覆盖面多，导致各种审计都没有深化，无法提供有效的审计数据
- 无法实现绑定变量解析和超长SQL语句（1500字节以上）解析，select返回值解析。
- 无法会话的原始数据包捕获（Pcap），实现数据的完整真实记录。
- 基于单包分析的原理，无法实现对数据库进行实时监控，

3.2.3 Imperva

Imperva 作为国外的专业数据库审计产品，在海外市场占有率较高，同时在技术层面是走在前端的，他们的定位和优势如下：

- 定位高端用户，价格偏高
- 往往和WEB应用防火墙一并组成统一方案销售，具备较大优势。

可以从以下几方面展开竞争：

- 相对imperva的价格优势
- 作为国外安全产品，无法进入国内政府和其他高安全需求的机构
- 配置和使用过于复杂，需要长时间培训和大量专业知识，不符合国内使用的环境
- 无法会话的原始数据包捕获（Pcap），实现数据的完整真实记录。
- 无法实现对数据库进行实时监控

4 销售注意事项

注意事项：

1、贸易禁运和贸易管制国家（5+9国家）禁止销售；

2、政府涉密类业务禁止销售；

3、国家与社会安全监控体系类项目管控销售；

4、其他类项目和业务正常销售；

管控销售解释：

1.要坚持被集成战略，不做直销，坚决不涉及内容解析，也不能集成和OEM内容解析产品。

2.要避免引导由中国政府直接/间接出资或优惠贷款。

3.在采取了规避相关法律及管制政策风险措施后（如在合同中明确了免责条款），基于商业原则和风险溢价原则，允许提供标准产品和部件。