HUAWEI ENTERPRISE A BETTER WAY

华为数据库审计系统主打胶片

enterprise.huawei.com

HUAWEI TECHNOLOGIES CO., LTD.

目　　录

数据库泄密典型事件

凤凰网资讯 news.ifeng.com 凤凰网资讯 > 社会 > 法制经纬 > 正文 梦之蓝 特约

银行职员成个人信息买卖最大“掮客”

银行“内鬼”频出

朱凯华知道，互联网上活跃着一批声称可以帮[illegible]查到客户身份证号、余额等信息资料的“卡贩子”。很快，他通过QQ联系到几名“卡贩子”。经[illegible]，这些“卡贩子”有的是银行员工，有的是游荡在网上专门从事银行卡信息买卖的“二道贩子”。

胡斌是某知名银行信用卡中心的工作人员。他从2010年11月起，在互联网上以“战无敌”、“夜光杯”等网名发布可以提供银行信息查询的广告。胡斌收到朱凯华发来的银行客户身份证号码、姓名之后，利用银行内部网络系统进行违规查询，并将查询所获的银行客户个人征信报告、银行账户相关情况等信息，以每条几十元至100余元不等的价格出售给朱凯华，共出售300余条信息，非法获利两万余元。

另一名信息“供应商”曹晓军，原系某知名银行客户经理，网名“四一人生”，其在2011年2月至6月期间，通过中介向朱凯华出售个人征信报告多达2318份，非法获利23180元。

向朱凯华出售个人征信的还有某知名银行员工董婕和某知名银行客户经理陈荣哲。

除了这些银行员工，“二道贩子”任恩波也是朱凯华的一名重要“供应商”。任恩波是一名将客户银行卡信息低买高卖的“中间商”。从2010年10月起，他通过互联网以“明哥”、“强哥信用社”等网名倒卖他人的银行账户资料、个人征信报告等信息。

据查，在网上专门从事银行卡信息买卖的“二道贩子”共有6人，他们相互之间并不认识，平时靠QQ联系。

内部泄密

当前位置：首页 >>安全管理 >>安全曝光 >> 正文

奇虎声明破解一卡通两员工已被法办 微博致歉

2011-09-26 Techweb / Techweb

外部威胁

奇虎360公司发布声明，证实网络工程师破解一卡通漏洞并恶意充值遭拘役

9月25日消息，日前有媒体报道奇虎360公司网络工程师杨某破解市政一卡通的系统漏洞后，帮自己和同事恶意充值2600余元，并因此获拘役6个月。360公司今日发布声明证实此事，并向公众道歉。

360在声明中称，确有两名技术部门关公利用研究之便破解了北京市政一卡通密码，并恶意充值刷卡消费，涉及金额1700元。

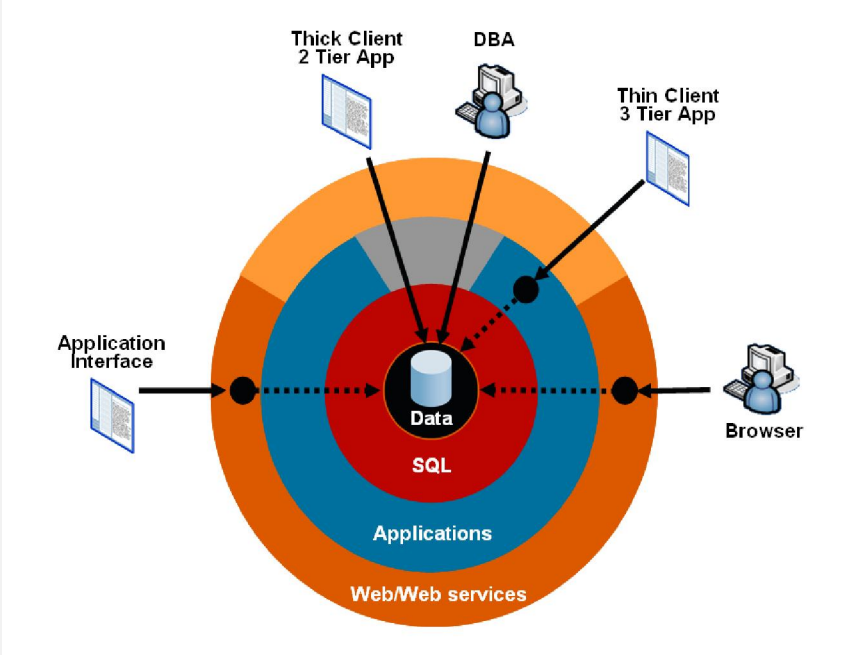
360公司表示，“两名员工利用一卡通漏洞消费获刑，虽然是个人行为，但我公司应承担员工教育的责任，并已采取相应的措施加强管理，避免类似事件的再次发生。在此，我们郑重向公众表示真挚的歉意。”

HUAWEI

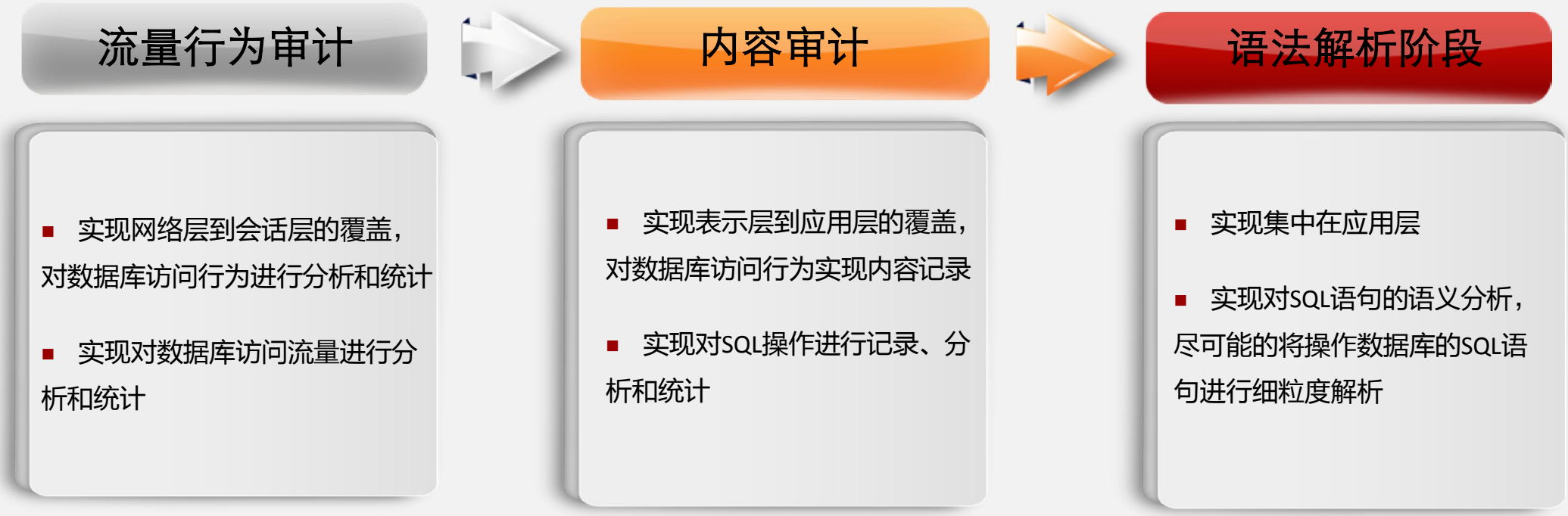
数据库维护现状分析

数据库威胁总结

- 数据库操作过程“雾化”，无有效快速分析依据。
- 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。
- 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。
- 不能实时监控对数据库的非法访问，没有预警。
- 一旦数据库日志被清除，无法发现事故，无法做到事故定位。
- 对于黑客攻击，无法做到有效防范和攻击留痕。
- 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。



数据库审计系统的发展


流量行为审计
内容审计
语法解析阶段
实现网络层到会话层的覆盖，对数据库访问行为进行分析和统计
实现对数据库访问流量进行分析和统计
实现表示层到应用层的覆盖，对数据库访问行为实现内容记录
实现对SQL操作进行记录、分析和统计
实现集中在应用层
实现对SQL语句的语义分析，尽可能的将操作数据库的SQL语句进行细粒度解析

语法解析的数据库审计

SQL分解

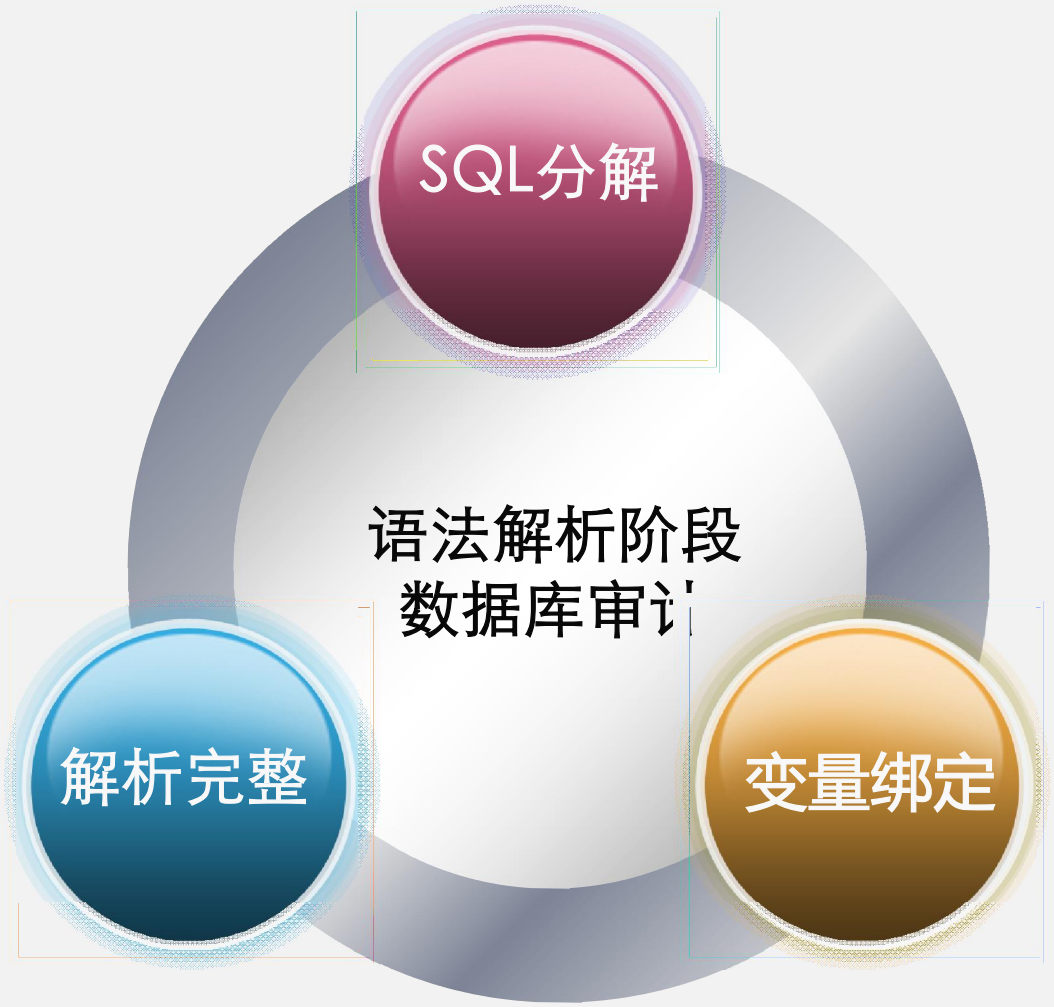
分解成多个字段进行响应和记录，任意一列都可以单独设定审计规则，单独查询，这样就可以满足用户精确响应和精确查询的要求

变量绑定

实现对绑定变量传输情况下的字段与数值的自匹配解析，通过对字段值的解析、设定字段数值条件。在大多数情况下，数据表关键字段往往对应着现实世界中资金或物品的数量及额度，对关键字段改变操作的精确检测非常重要

解析完整

满足不同种类数据库系统、满足不同版本的数据库系统、满足不同通讯协议下的数据库环境。满足对各操作对象及DML、DCL、DDL命令支持是审计完整性的重要指标之一



合规性需求

萨班斯法案

强调通过内部控制加强公司治理，包括加强与财务报表相关的IT系统内部控制，其中，IT系统内部控制就是面向具体的业务，它是紧密围绕信息安全审计这一核心的

企业内部控制规范

提出健全内部审计机构、加强内部审计监督是营造守法、公平、正直的内部环境的重要保证。企业应当加强内部审计工作，在企业内部形成有权必有责、用权受监督的良好氛围

计算机等保要求

详细说明了计算机信息系统为实现GB17859所提出的安全等级保护要求对数据库管理系统的安全技术要求，以及确保这些安全技术所实现的安全功能达到其应有的安全性而采取的保证措施

数据库管理系统的安全审计应建立独立的安全审计系统；定义与数据库安全相关的审计事件；设置专门的安全审计员；设置专门用于存储数据库系统审计数据的安全审计库；提供适用于数据库系统的安全审计设置、分析和查阅的工具。

行业标准

行业	法规标准
互联网服务商	《互联网安全保护技术措施规定（82号令）》
电信行业	《中国移动集团内控手册》
	《中国移动业务支撑网安全域划分和边界整合技术规范》
	《中国电信股份有限公司内部控制手册》
	《中国网通集团信息质量问责管理若干规定 》
	《中国网通集团内部控制体系建设指导意见 》
金融保险行业	《银行业金融机构信息系统风险管理指引》
	《商业银行合规风险管理指引》
	《中国银行业监督委员会办公厅文件银监办通313号》
	《保险公司内部审计指引（试行）》
	《保险公司风险管理指引（试行）》
	《电子银行安全评估指引（2007）》
	《电子银行业务管理办法（2008）》
	《期货公司信息技术管理指引》
	《商业银行内部控制指引》——计算机信息系统的内部控制
	《支付卡行业数据安全标准——要求和安全评估程序（2008）》
国内上市企业	《深圳证券交易所上市公司内部控制指引 》
	《上海证券交易所上市公司内部控制指引 》
电力行业	《电力二次系统安全防护总体方案（2005）》
	《国家电网公司信息化“SG186”工程安全防护总体方案（实行）(2008)》
医疗行业	《互联网医疗保健信息服务管理办法》(卫生部令第66号)

目　　录

华为数据库审计解决思路

部署安全

- 采用网络监听审计技术
- 无需安装代理
- 不改变原有网络拓扑结构
- 系统故障不影响现有网络稳定

策略灵活

- 支持实时告警和异常告警功能
- 支持异常数据自动发现
- 支持多条件符合条件策略设置
- 支持精细到表、字段的告警策略设置

事件完整

- 采用以会话流进行记录和分析
- 采集时间所有因素进行综合分析
- 原始记录用户访问网络数据包
- 完整展现用户单个会话所有操作

自身安全

- 采用盘路镜像方式部署
- 隐藏在用户与数据库之间
- 采用系统加固以及安全扫描加固
- 系统故障不影响现有网络稳定

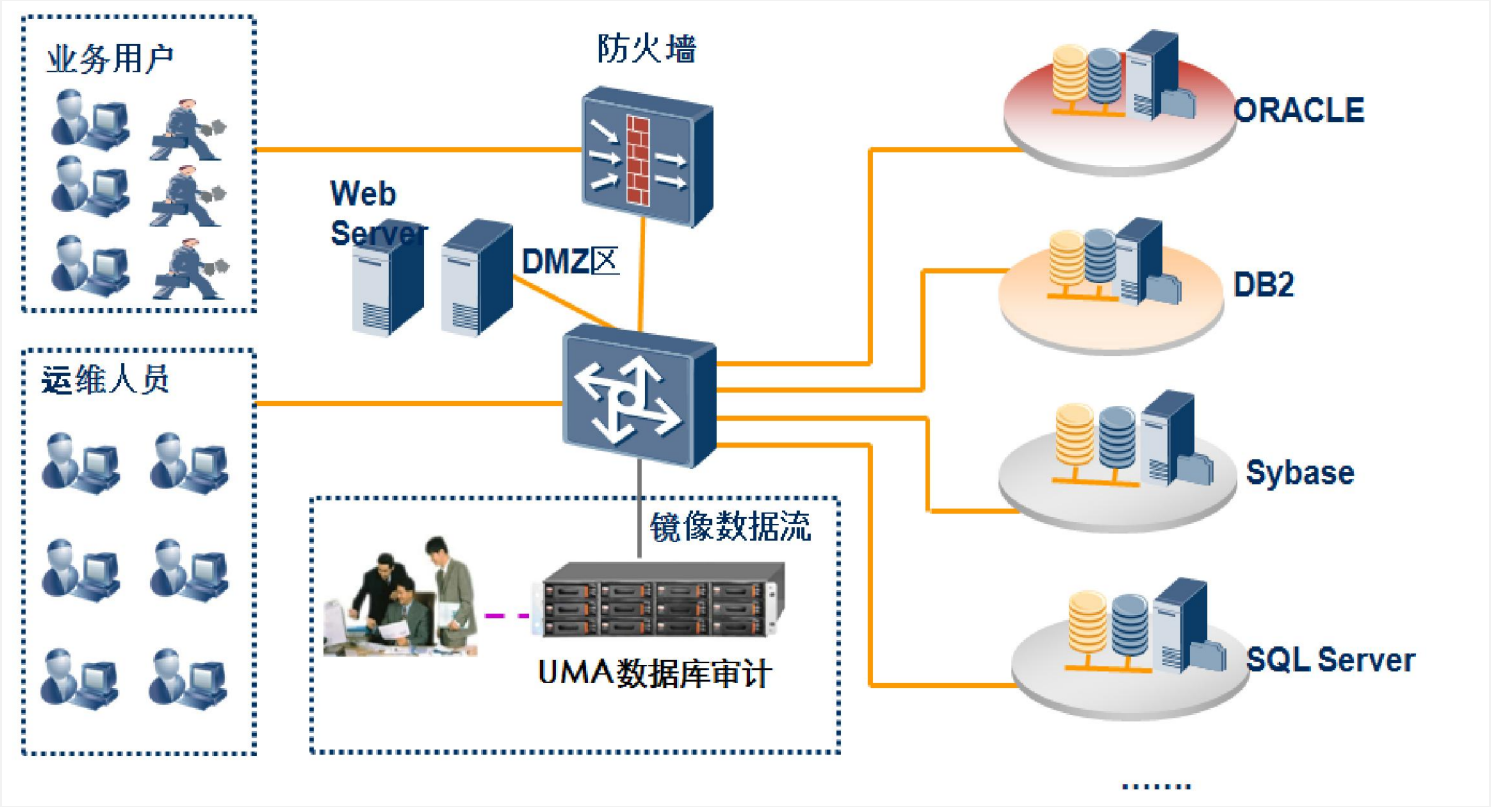
数据库审计网络部署

部署策略

- 通过数据库审计系统，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，记录各种数据库访问行为，即时发现对业务数据的违规操作和异常行为，长期保存审计数据，满足审计及合规要求。

部署原则

- 数据库深度协议审计,完整再现协议操作所有过程和细节(串联/并联)
- 提供强大的策略配置和告警动作，为用户规范数据库访问使用
- 针对所有企业用户服务器集群资产和企业私有财产
- 不安装任何引擎,不影响业务系统,不改变网络拓扑,不安装任何客户端软件



流技术与会话方式审计

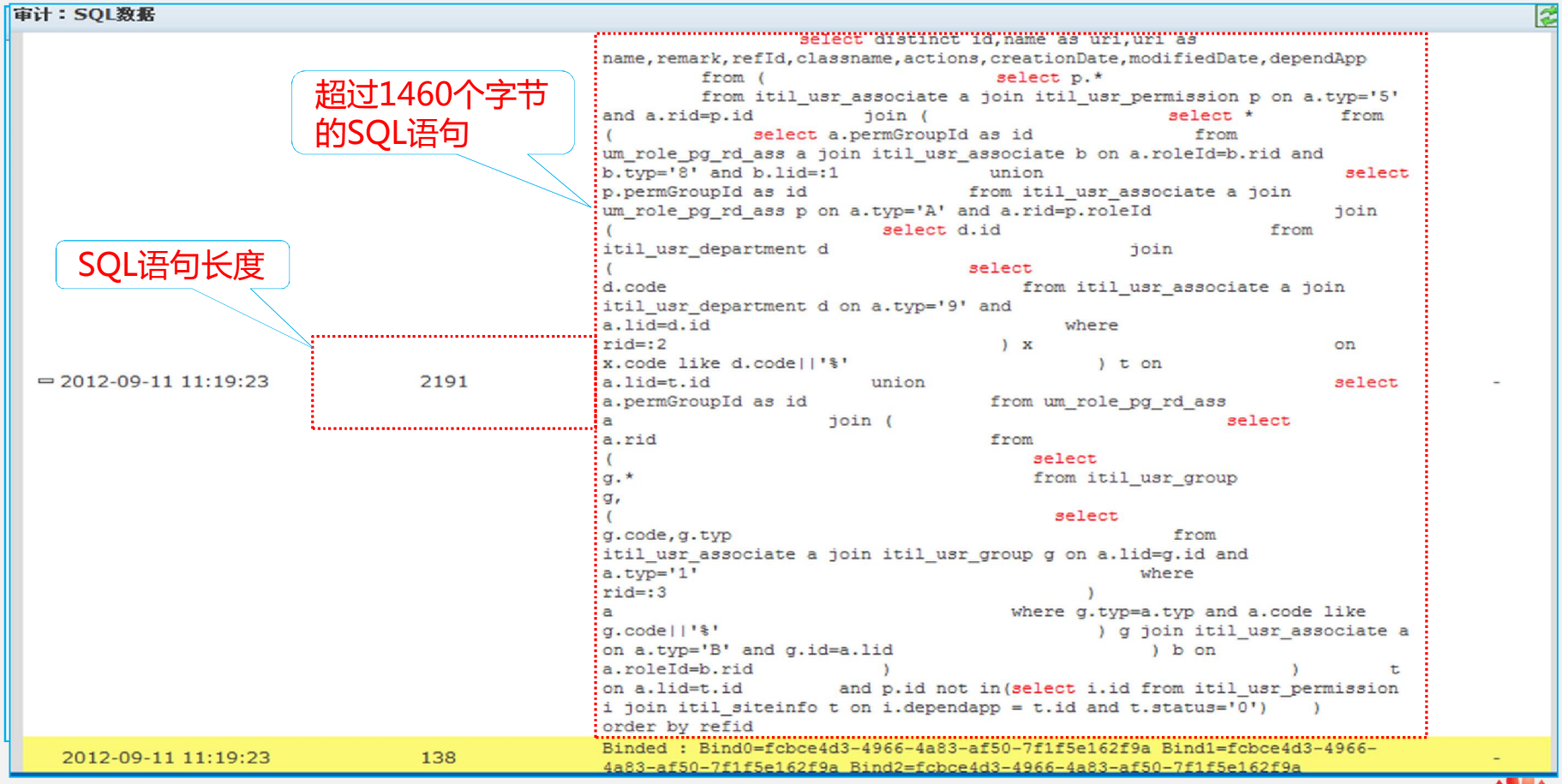
业界领先的流会话方式审计的领导厂商

流技术与会话审计：当前最先进的网络数据审计技术，是指从访问的发起、过程、结束的完整记录。

	消息长度	消息	操作
2012-09-18 19:14:23	56	NS version Number = 308 Compatible With Version = 300	-
2012-09-18 19:14:23	131	(DESCRIPTION=(CONNECT_DATA=(SID=orcl)(CID=(PROGRAM=)(HOST=__jdbc__)(USER=)))(ADDRESS=(PROTOCOL=tcp)(HOST=10.142.59.34)(PORT=1521)))	-
2012-09-18 19:14:23	40	SessionLoginClientMachine = [__jdbc__]	-
2012-09-18 19:14:23	56	NS version Number = 308 Compatible With Version = 300	-
2012-09-18 19:14:23	131	(DESCRIPTION=(CONNECT_DATA=(SID=orcl)(CID=(PROGRAM=)(HOST=__jdbc__)(USER=)))(ADDRESS=(PROTOCOL=tcp)(HOST=10.142.59.34)(PORT=1521)))	-
2012-09-18 19:14:23	23	Accept Version := 308	-
2012-09-18 19:14:23	77	SessionLoginUsername = [COSS] SessionLoginClientMachine = [svctag-375xt2x]	-
2012-09-18 19:14:23	779	select ci.id, ci.ciname as name, b2.ds_label as category, b3.ds_label as status, ci.version, ci.assetCode, b.ds_label as location, b4.ds_label as comeFrom, b5.ds_label as supplier, ci.contract, ci.supplyDate, ci.dutyPerson as duty, b6.ds_label as vindicater, d.name as department, ci.acceptDate, ci.warranty, ci.memo, ci.serviceLevel, ci.lastModifyDate from itil_cm_ci ci left join itil_cm_cilocation cil on ci.id=cil.ciid left join itil_bizcode b on cil.locationid=b.ds_id left join itil_bizcode b2 on ci.cicategory=b2.ds_id left join itil_bizcode b3 on ci.status=b3.ds_id left join itil_bizcode b4 on ci.comefrom=b4.ds_id left join itil_bizcode b5 on ci.supplier=b5.ds_id left join itil_bizcode b6 on ci.vindicater=b6.ds_id left join itil_usr_department d on ci.department=d.id	-
2012-09-18 19:14:23	44	DbXpert Session is Terminated Successfully	-

超长SQL语句解析

能完整解析与审计超长SQL语句（缺乏超长SQL语句解析审计，提供逃避审计通道）



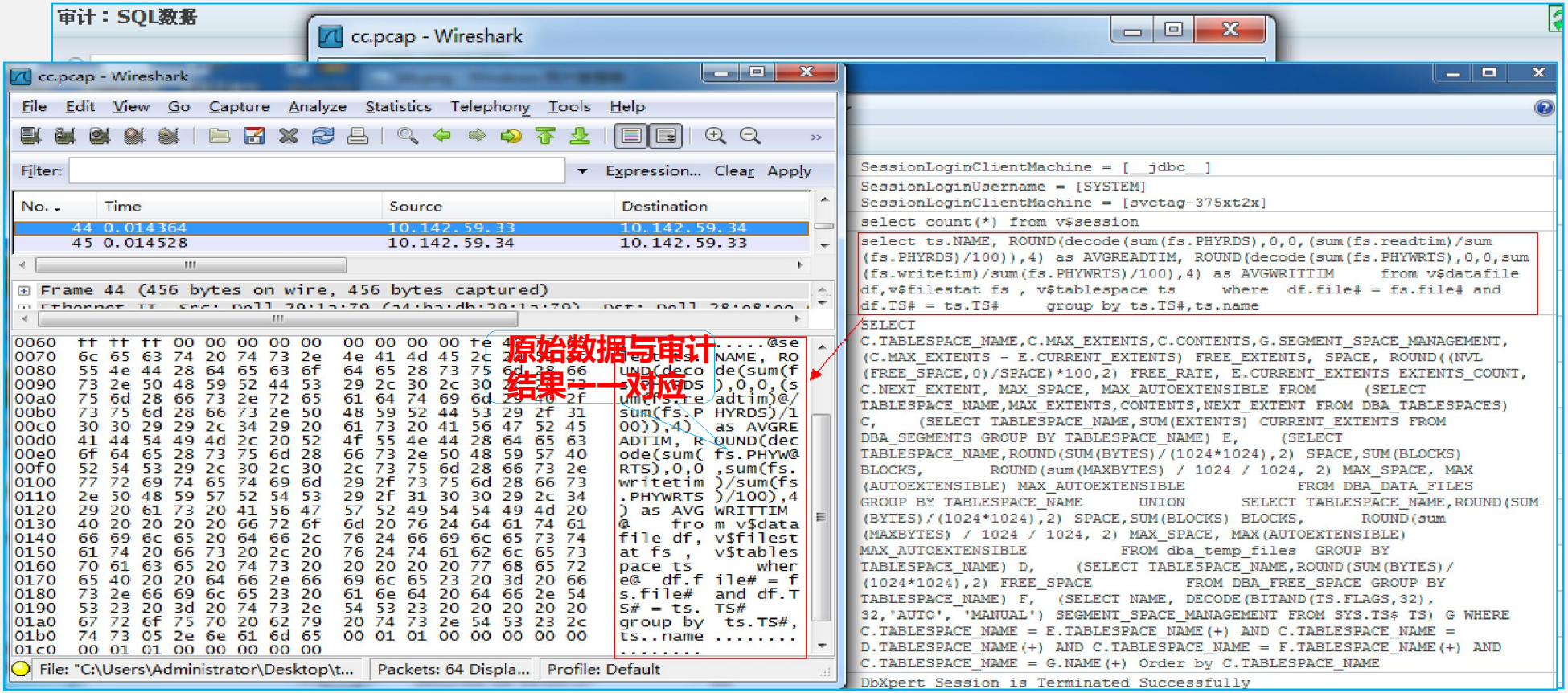
绑定变量解析

数据库系统中存在大量变量绑定的应用，用于实现业务操作关联

	消息长度	消息	操作
2012-09-11 10:26:16	130	update RES_P_S_cpu_use set SAMPLETIME=:1, STEP=:2, OBTAINABLE=:3 ,cpu_use_util=:4 where OBJECTID=:5	-
2012-09-11 10:26:16	77	Binded : Bind0=2012-09-11 10:17:59 Bind1=606 Bind2= 0x80 Bind3=2 Bind4=46157	-
2012-09-11 10:26:16	63	select nvl(sum(id_int),-1) from res_object_real where id=:1	-
2012-09-11 10:26:16	52	Binded : Bind0=245e31e9-4442-432b-afdc-aa7aeb346e2a	-
2012-09-11 10:26:16	58	select count(*) from RES_P_S_cpu_use where OBJECTID=:1	-
2012-09-11 10:26:16	21	Binded : Bind0=46165	-
2012-09-11 10:26:16	130	update RES_P_S_cpu_use set SAMPLETIME=:1, STEP=:2, OBTAINABLE=:3 ,cpu_use_util=:4 where OBJECTID=:5	-
2012-09-11 10:26:16	77	Binded : Bind0=2012-09-11 10:26:07 Bind1=606 Bind2= 0x80 Bind3=1 Bind4=46165	-
2012-09-11 10:26:16	63	select nvl(sum(id_int),-1) from res_object_real where id=:1	-
2012-09-11 10:26:16	52	Binded : Bind0=723b89e4-21b5-4180-87d8-bff44fb50f97	-
2012-09-11 10:26:16	58	select count(*) from RES_P_S_cpu_use where OBJECTID=:1	-
2012-09-11 10:26:16	21	Binded : Bind0=46206	-
2012-09-11 10:26:16	130	update RES_P_S_cpu_use set SAMPLETIME=:1, STEP=:2, OBTAINABLE=:3 ,cpu_use_util=:4 where OBJECTID=:5	-
2012-09-11 10:26:16	77	Binded : Bind0=2012-09-11 10:20:12 Bind1=606 Bind2= 0x80 Bind3=8 Bind4=46206	-
2012-09-11 10:26:16	63	select nvl(sum(id_int),-1) from res_object_real where id=:1	-
2012-09-11 10:26:16	52	Binded : Bind0=3647f5a3-a6ff-4d50-84c4-7681720b565a	-
2012-09-11 10:26:16	58	select count(*) from RES_P_S_cpu_use where OBJECTID=:1	-
2012-09-11 10:26:16	20	Binded : Bind0=7507	-

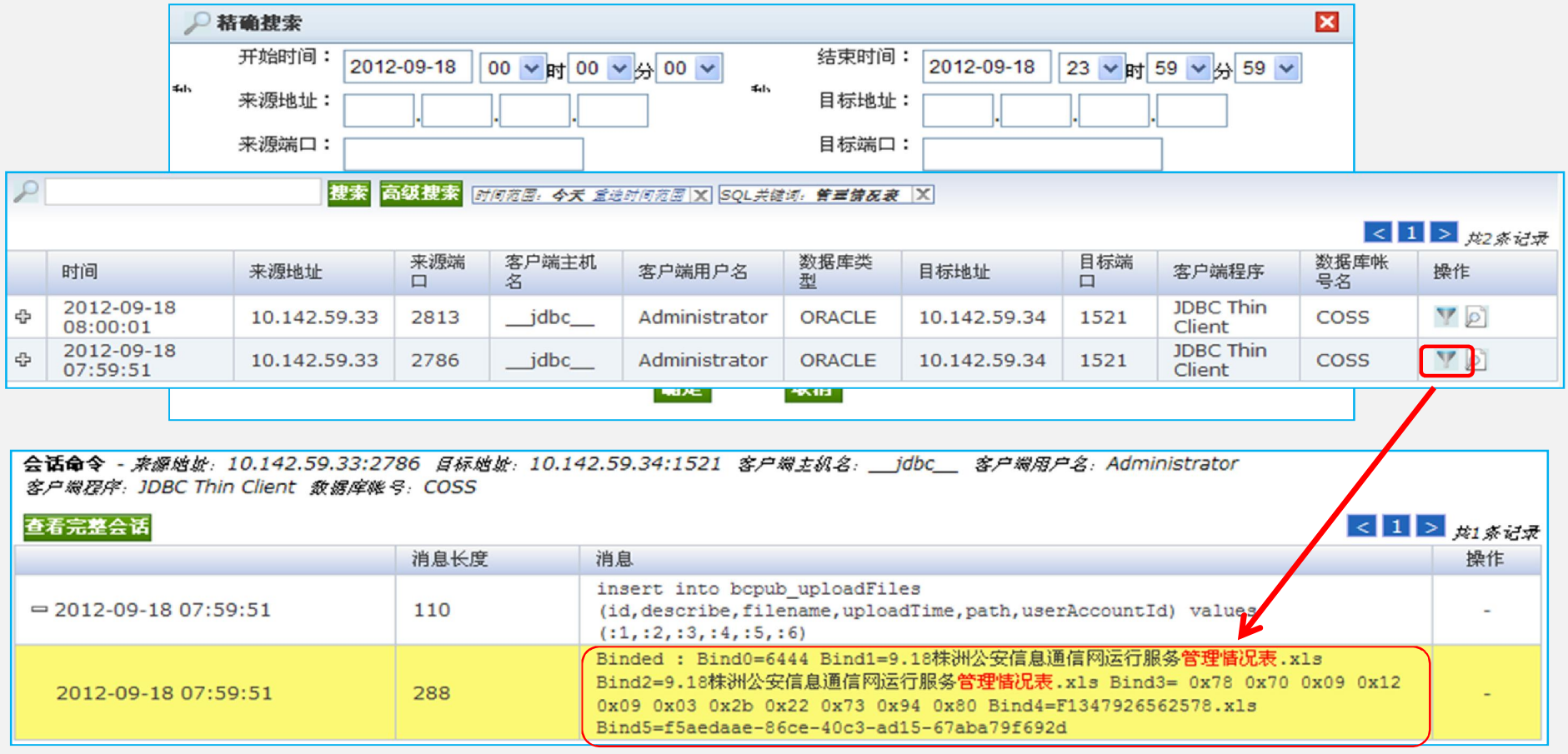
原始流数据包记录

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



全文检索功能

通过细粒度的过滤条件，在海量数据中快速定位审计日志



异常告警、实时监控

自动发现接入信息：数据库账号、数据库客户端程序、客户端主机、客户端系统用户名，并且自动监控异常接入信息，保证来源数据的安全与可靠

细粒度告警条件

包括：SQL命令、表名、列名、数据库账号、客户端IP、客户端程序名、客户端主机名、客户端系统用户名等。

业务系统数据审计

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

产品其他功能

功能特点	功能描述
实时监控	支持对数据库服务器的运行状态进行实时监控，为管理者提供一个数据库监控工具。
数据备份	支持对审计日志进行自动定期备份存储。
对外输出	支持与syslog日志服务器的对接。
告警方式	支持邮件告警与WEB告警方式。
黑白名单	支持对数据库帐号、数据库客户端程序、客户端主机、客户端系统用户名的黑白名单设置，并进行实时告警。
来源限制	支持对来源地址进行忽略审计与限定审计。
协议兼容	支持主流数据库协议以及子版本的审计：oracle、 DB2、 SQL server、 sybase、 informix
报表统计	支持自定义报表统计：PDF/EXCEL格式，可进行周期统计，提供3D柱状图和饼状图等
网络抓包	支持多抓包口，满足用户的负载均衡网络环境。

目　录

应用场景---业务操作事故追踪

如何确认是谁在业务系统上添加了一个”F1347927451281.xls”文件？

会话命令 - 来源地址：10.142.59.33:1055 目标地址：10.142.59.34:1521 客户端主机名：__jdbc__ 客户端用户名：Administrator
客户端程序：JDBC Thin Client 数据库帐号：COSS

查看与F1347927451281.xls匹配语句 < 1 > 共5条记录

	消息长度	消息	操作
2012-09-18 08:14:40	56	NS version Number = 308 Compatible With Version = 300	-
2012-09-18 08:14:40	144	(DESCRIPTION=(CONNECT_DATA=(SID=orcl)(CID=(PROGRAM=)(HOST=__jdbc__) (USER=Administrator)))(ADDRESS=(PROTOCOL=tcp)(HOST=10.142.59.34) (PORT=1521)))	-
⊕ 2012-09-18 08:14:40	86	SessionLoginClientMachine = [__jdbc__] SessionLoginClientUsername = [Administrator]	-
⊕ 2012-09-18 08:14:40	119	SessionLoginUsername = [COSS] SessionLoginProgram = [JDBC Thin Client] SessionLoginClientMachine = [svctag-375xt2x]	-
⊖ 2012-09-18 08:14:40	110	insert into bcpub uploadFiles (id,describe,filename,uploadTime,path,userAccountId) values (:1,:2,:3,:4,:5,:6)	-
2012-09-18 08:14:40	539	Binded : Bind0=6446 Bind1= 0x32 0x30 0x31 0x32 0xe5 0xb9 0xb4 0x39 0xe6 0x9c 0x88 0x31 0x38 0xe6 0x97 0xa5 0xe6 0xb9 0x98 0xe8 0xa5 0xbf 0xe5 0x85 0xac 0xe5 0xae 0x89 0xe4 0xbf 0xa1 0xe6 0x81 0xaf 0xe9 0x80 0x9a 0xe4 0xbf 0xa1 0xe7 0xbd 0x91 0xe8 0xbf 0x90 0xe8 0xa1 0x8c 0xe6 0x9c 0x8d 0xe5 0x8a 0xa1 0xe7 0xae 0xa1 0xe7 0x90 0x86 0xe6 0x83 0x85 0xe5 0x86 0xb5 0xe8 0xa1 0xa8 0x20 Bind2=20120918.xls Bind3= 0x78 0x70 0x09 0x12 0x09 0x12 0x20 0x10 0xbf 0xb8 0x40 Bind4=F1347927451281.xls Bind5=e41f1e0f-3a29-4f9c-9721-2249f7ca76d6	-
2012-09-18 08:14:40	19	Client disconnect	-
2012-09-18 08:14:40	44	DbXpert Session is Terminated Successfully	-

添加的文件名

业务操作的用户ID

操作的具体时间

应用场景---高危SQL命令告警

如何对高危的SQL命令(如:delete/drop/truncate等)进行实时告警？

应用场景---异常来源信息告警

如何对非正常的来源信息(如:数据库账号/客户端程序/客户端主机名等)进行异常告警？

异常客户端主机名

异常告警列表

今天 (2278) 过滤

NO.	告警级别	告警时间	类型	源地址	目标地址	数据库用户	
1	低危险	2012-09-18 18:45:18	ORACLE	10.142.59.33:1586	10.142.59.34:1521	SYSTEM	登录源主机名异常
2	低危险	2012-09-18 18:45:18	ORACLE	10.142.59.33:1586	10.142.59.34:1521	SYSTEM	登录数据库账号异常
3	低危险	2012-09-18 18:45:18	ORACLE	10.142.59.33:1586	10.142.59.34:1521	SYSTEM	登录源主机名异常
4	低危险	2012-09-18 18:44:23	ORACLE	10.142.59.33:1431	10.142.59.34:1521	COSS	登录源主机名异常
5	低危险	2012-09-18 18:44:23	ORACLE	10.142.59.33:1431	10.142.59.34:1521	COSS	登录源主机名异常
6	低危险	2012-09-18 18:44:15	ORACLE	10.142.59.33:1405	10.142.59.34:1521	COSS	登录源主机名异常
7	低危险	2012-09-18 18:44:15	ORACLE	10.142.59.33:1405	10.142.59.34:1521	COSS	登录源主机名异常
8	低危险	2012-09-18 18:44:15	ORACLE	10.142.59.33:1402	10.142.59.34:1521	COSS	登录源主机名异常
9	低危险	2012-09-18 18:44:15	ORACLE	10.142.59.33:1402	10.142.59.34:1521	COSS	登录源主机名异常
10	低危险	2012-09-18 18:44:15	ORACLE	10.142.59.33:1398	10.142.59.34:1521	COSS	登录源主机名异常
11	低危险	2012-09-18 18:44:15	ORACLE	10.142.59.33:1398	10.142.59.34:1521	COSS	登录源主机名异常
12	低危险	2012-09-18 18:44:10	ORACLE	10.142.59.33:1386	10.142.59.34:1521	COSS	登录源主机名异常
13	低危险	2012-09-18 18:44:10	ORACLE	10.142.59.33:1386	10.142.59.34:1521	COSS	登录源主机名异常

违规操作详情

10.142.59.33:1586
客户端用户名： n/a
客户端主机名： __jdbc__

客户端应用程序
程序名称： n/a
程序版本： n/a

服务端详情
服务端地址：
10.142.59.34:1521
用户名称： SYSTEM
服务器名称： ORACLE
语句组： n/a
语句长度： 79
原始SQL语句：

```
SessionLoginUsername =
[SYSTEM]
SessionLoginClientMachi
ne = [svctag-375xt2x]
```

表组： n/a
响应时间： n/a

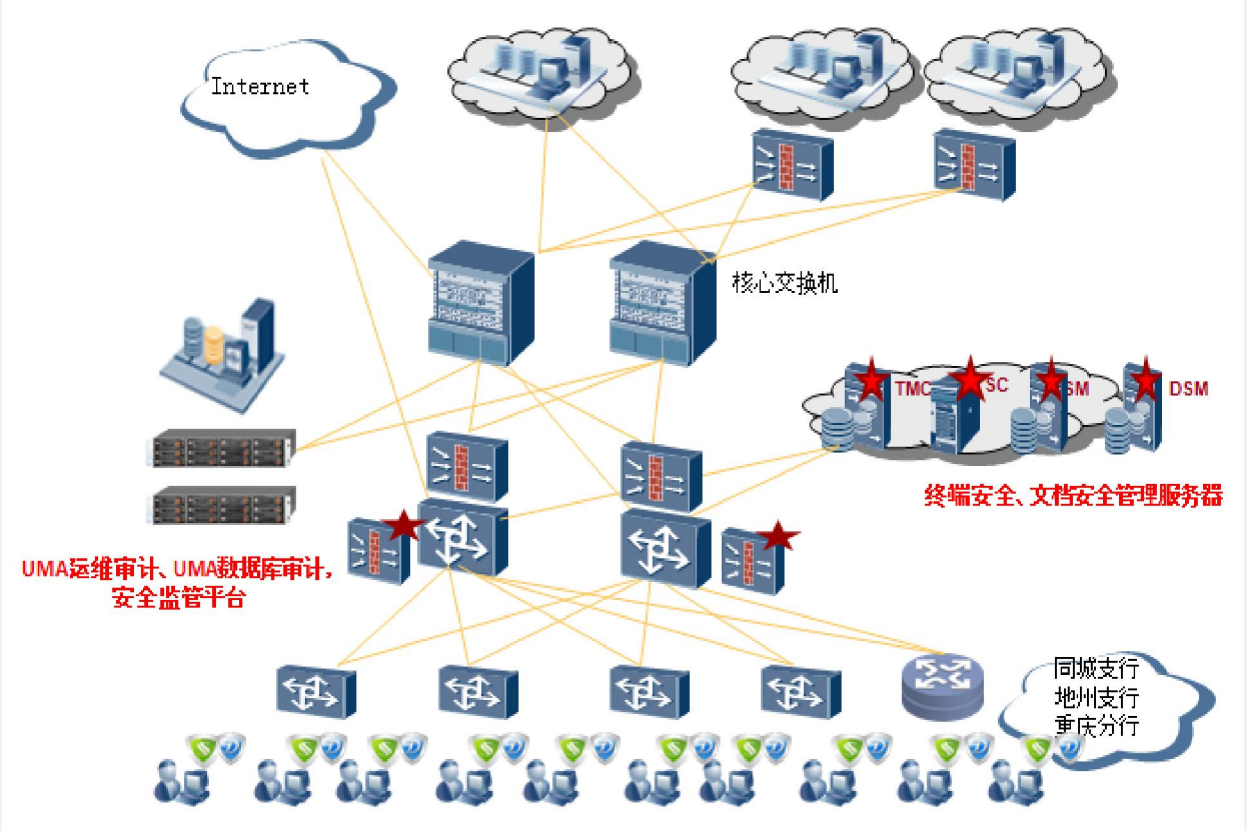
成功案例 - 云南富滇银行数据库审计项目

客户挑战：
富滇银行股份有限公司成立于2007年12月30日，是经中国银监会批准成立的云南省省级地方性股份制商业银行；银行核心业务数据都运行在数据库系统之上，如何保障这些核心业务数据的安全，防止核心数据被窃取和篡改是富滇银行面临的最大挑战。

华为方案：
华为根据富滇银行的业务特点，采用旁路方式部署一套专业数据库审计系统，通过镜像的方式将业务数据流引入UMA-DB进行深入分析，记录所有对核心业务数据的操作，对违规行为实时告警。

客户收益：
满足法案法规要求，顺利通过银监会的检查；实时进行异常监控，及时发现安全事件；完整审计数据库访问信息，重溯过程准确定责。

富滇銀行 FUDIAN BANK



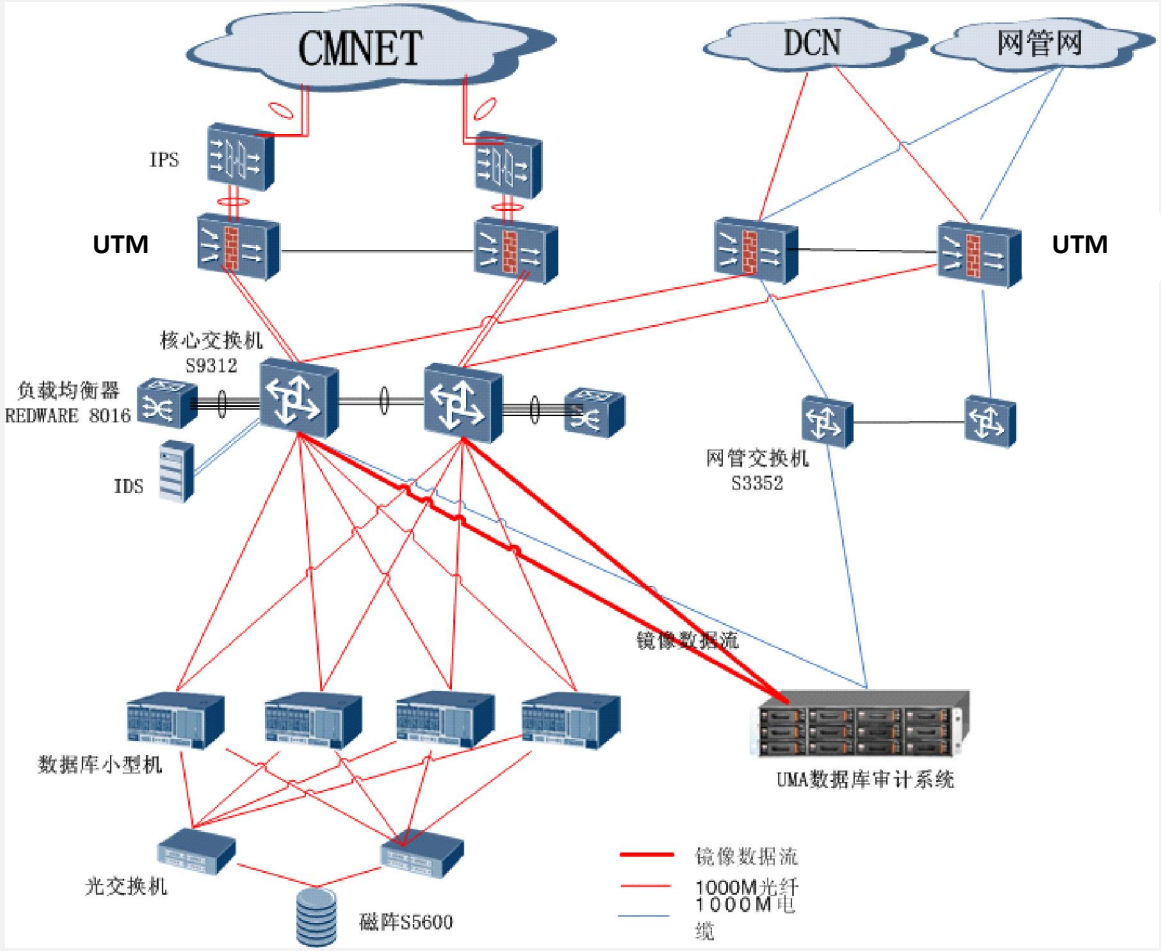
HUAWEI

成功案例 - 江苏移动游戏基地

客户挑战：
江苏移动游戏基地面向用户提供手机游戏、JIL游戏、PC游戏等业务。平台需支撑的手机游戏类型包括但不限于客户端单机游戏、客户端网游、图文单机游戏、图文网游、短信互动游戏、动漫游戏、套餐业务、棋牌类网游、对战游戏等；如何保障游戏业务数据的合法使用，防止账号盗用、篡改数据等违规行为，如何实现责任认定和追溯等是江苏游戏基地面临的挑战。

华为方案：
华为数据库审计系统通过专业细粒度的网络数据包协议解析技术、数据存储技术、数据检索技术并配合完善的策略管理规则，通过镜像的方式将游戏基地近10台数据库系统流量引入UMA-DB系统，进行深入分析和还原，并对违规行为进行实时告警，帮助用户管理层应对来自网络中对数据库构成的风险和挑战。

客户收益：
1、职权分离：系统满足多种系统角色管理，满足法案法规的合规性要求。
2、细粒度审计：记录所有数据访问细节，提供策略告警、异常告警、实时监控等防护手段，保证各个层面的安全性。
3、策略管理：系统提供快速、灵活的告警策略机制，保证用户管理层实时了解到数据库的运行状况。
4、统计报告：系统提供模板化的报表展现功能，为用户出台新的政策制定提供依据。



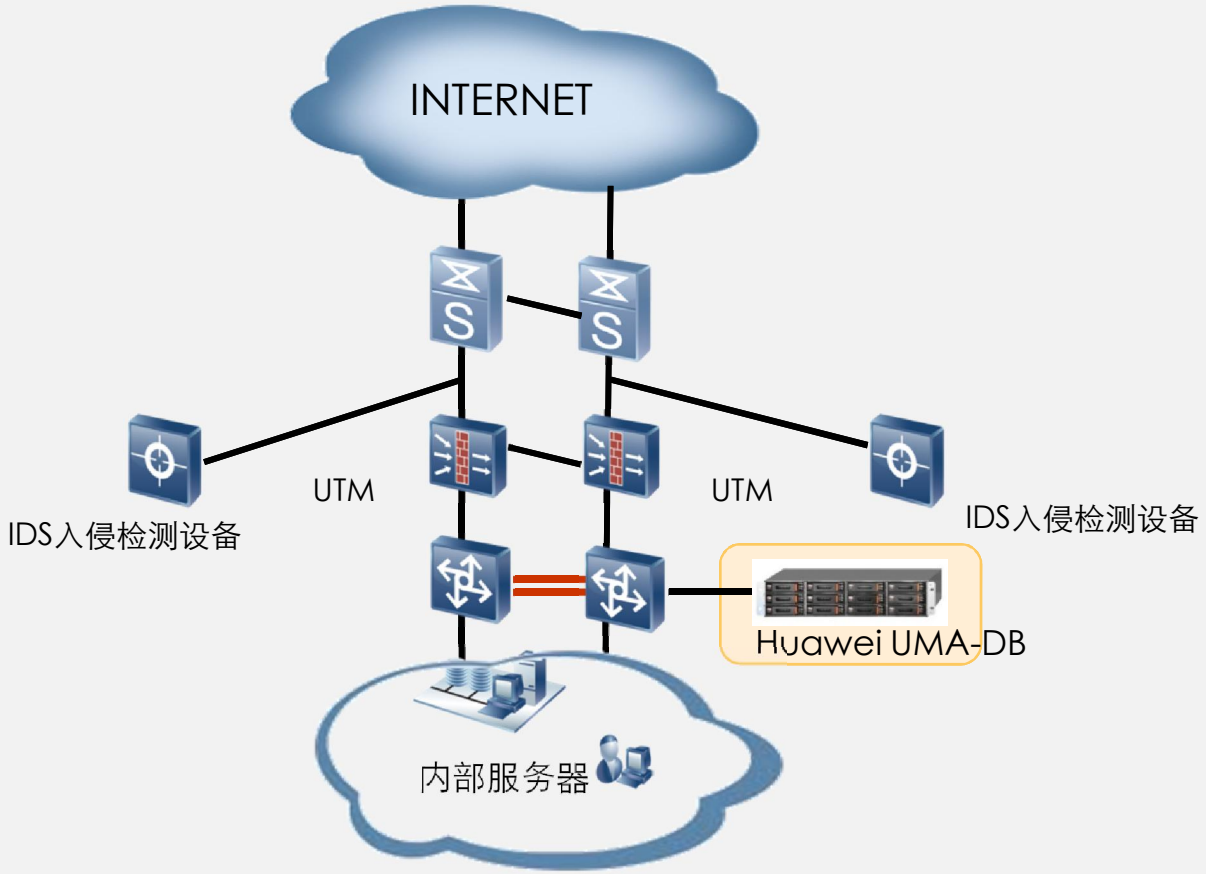
HUAWEI

成功案例 - 东北再担保公司数据库审计项目

客户挑战：
东北中小企业信用再担保股份有限公司（以下简称东北再担保公司）是由国家发改委、原国务院振兴东北办和国家开发银行发起，财政部、国家开发银行和辽宁省、吉林省、黑龙江省、内蒙古自治区和大连市人民政府共同出资设立的政策性区域再担保机构；公司要求对核心数据库资产实行规范化的管理，通过管理手段和技术手段，实现数据访问的可审计，可视，可重现。

华为方案：
根据东北再担保的数据业务情况，采用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。

客户收益：
掌控业务运行情况，直观评估运行性能；实现三权分立独立审计，高效运维提高内控；完整审计业务信息，重溯业务准确定责。
制定特定规则，实现数据库访问行为的实时告警。



更多成功应用案例

- 深圳超算中心
- 东方航空公司云南基地
- 安哥拉政府电子政务数据中心
- 安哥拉航空数据中心
- 上海闸北卫生局
- 华为互联网中心（廊坊）
- 江苏移动游戏基地
- 太原地税局
- 昆明国税局
- 甘肃民政局
- 上海无线电管理局
- 北京电信
- 东北再担保公司
- 安徽肿瘤医院

- 安徽芜湖社保局
- 上海金融学院
- 上海外国语学院
- 上海财经学院
- 江西移动
- 华为IT产品线云平台
- 华为IT产品线IDC方案
- 华为IT产品线EDC方案
- 华为业软
- 华为GNOC
- 华为GTS
- 华为互联网中心（北京）
- 深圳比亚迪

- 埃塞电信
- 意大利能源
- 阿尔及利亚电信
- 罗马尼亚GNOC
- 印度GNOC
- 莫桑比克电子政务
- 华为互联网中心（北京）
- 安哥拉政府电子政务数据中心
- 安哥拉航空数据中心

HUAWEI ENTERPRISE A BETTER WAY