ORACLE®

SECURE DATA AT THE SOURCE
SAVE TIME AND MONEY

Security Inside Out | Oracle Database Security

ORACLE®

Preventing Database Attacks and Data Breaches with New Oracle Database Firewall

Agenda

- Evolving Threats to Databases
- Oracle Database Firewall
  - Security Models
  - Policy Enforcement
  - Reporting
  - Architecture and Deployment Modes
- Oracle Database Security Solutions
- Q&A

ORACLE

How is Data Compromised?

Investigations Reveal 92% of Breached Records from Compromised Databases

Table 7.Types of compromised assets by percent of breaches and percent of records*

Type	Category	% of Breaches	% of Records
Database server	Servers & Applications	25%	92%
Desktop computer	End-User Devices	21%	1%
Web app/server	Servers & Applications	19%	13%
Payment card	Offline Data	18%	<1%
POS server (store controller)	Servers & Applications	11%	<1%
Laptop computer	End-User Devices	7%	<1%
Documents	Offline Data	7%	<1%
POS terminal	End-User Devices	6%	<1%
File server	Servers & Applications	4%	81%
Automated Teller Machine (ATM)	End-User Devices	4%	<1%
FTP server	Servers & Applications	2%	3%
Mail server	Servers & Applications	2%	4%
Customer (B2C)	People	2%	<1%
Regular employee/end-user	People	2%	<1%

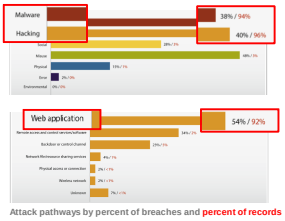
verizon business
2010 Data Breach Investigations Report

ORACLE

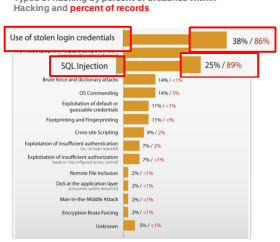
#1 Cause of Data Breaches:

Web Applications Hacked with SQL Injection and Stolen Credentials Obtained Using Malware

Threat action categories by percent of breaches and records



Types of hacking by percent of breaches within Hacking and percent of records



Attack pathways by percent of breaches and percent of records

verizon business
2010 Data Breach Investigations Report

ORACLE

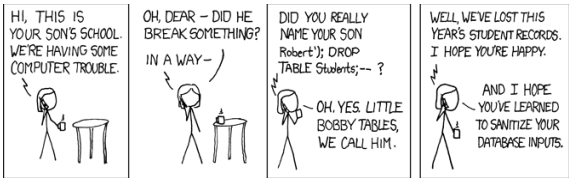
SQL Injection

Too much trust in applications

```
<?php
$dbhost = 'localhost';
$dbuser = 'root';
$dbpass = 'password';

$conn = mysql_connect($dbhost, $dbuser, $dbpass)
        or die ('Error connecting to mysql');

$dbname = 'petstore';
mysql_select_db($dbname);

// get password based on form input
$result = mysql_query("SELECT password FROM users WHERE username =
                '$form_username'")
or die(mysql_error());

$row = mysql_fetch_array($result);

if ($row['password'] == $form_password) {
                echo "Authenticated successfully<br>";
} else {
                echo "Wrong password<br>";
}
?>
```

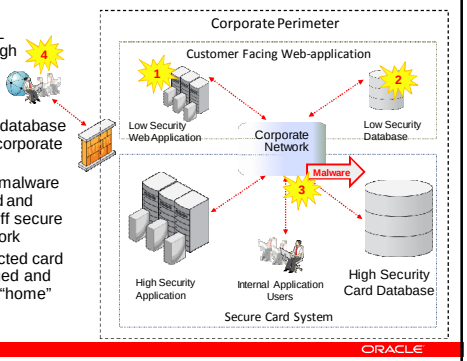
ORACLE

SQL Injection
Too much trust in applications

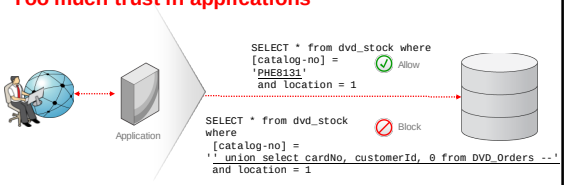


How 130M Credit Cards Were stolen

1. Attack via SQL Injection through bespoke web-application
2. Attacker owns compromised database connected to corporate network
3. Undetectable malware commissioned and installed to sniff secure payment network
4. Malware collected card details packaged and regularly sent "home"

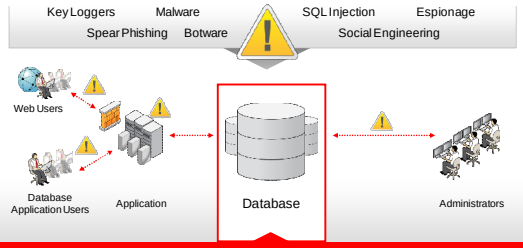


SQL Injection
Too much trust in applications



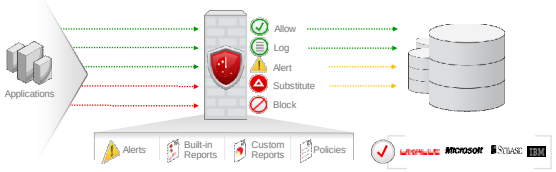
- Applications are given high levels of privilege
- Database trusts the application
- (Mis)users subvert the application to access to the database (and beyond)
- Each application is unique
- Regular expression black lists are ineffective
- Grammar based white-list blocks SQL injection attacks

Existing Security Solutions Not Enough



Data Must Be Protected at the Source

Oracle Database Firewall
First Line of Defense

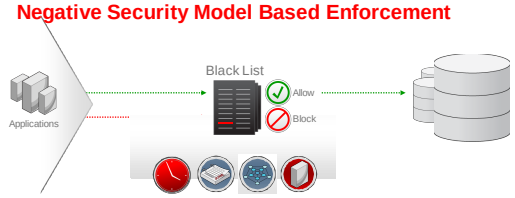


- Monitor database activity to help prevent unauthorized activity, application bypass and SQL injections
- Highly accurate SQL grammar based analysis
- White-list, black-list, and exception-list based security policies
- Built-in and custom compliance reports for regulations

Oracle Database Firewall
Positive Security Model Based Enforcement

- White-list based policies enforce normal or expected behavior
- Policies evaluate factors such as time, day, network, and application
- Easily generate white-lists for any application
- Out of policy SQL statements can be logged, alerted, blocked or substituted with a harmless SQL statement
- SQL substitution foils attackers without disrupting applications

Oracle Database Firewall
Negative Security Model Based Enforcement

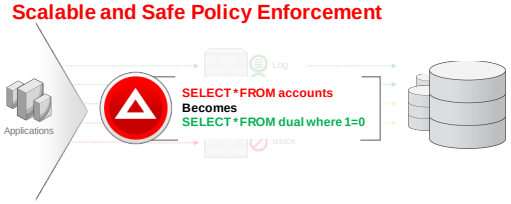


- Stop specific unwanted SQL commands, user, or schema access
- Prevent privilege or role escalation and unauthorized access to sensitive data
- Black list policies can evaluate factors such as day, time, network, and application

ORACLE

 13

Oracle Database Firewall
Scalable and Safe Policy Enforcement

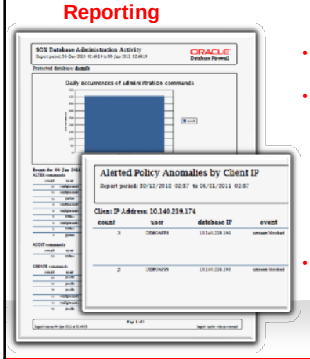


- Innovative SQL grammar technology reduces millions of SQL statements into a small number of SQL characteristics or "clusters"
- Flexible enforcement at SQL level: block, substitute, alert and pass, log only
  - SQL substitution foils attackers without disrupting applications
- Centralized policy management and reporting
- Superior performance and policy scalability

ORACLE

 14

Oracle Database Firewall
Reporting

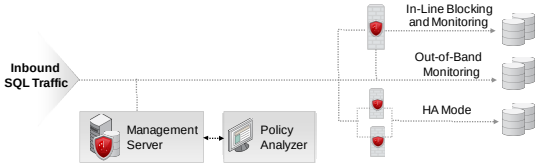


- Database Firewall log data consolidated into reporting database
- Dozens of built in reports that can be modified and customized
  - Database activity and privileged user reports
  - Entitlements reporting for database attestation and audit
  - Supports demonstrating controls for PCI, SOX, HIPAA, etc.
- Logged SQL statements can be sanitized of sensitive PII data

ORACLE

 15

Oracle Database Firewall
Architecture



- In-line blocking and monitoring, or out-of-band monitoring modes
- High availability with parallel firewalls
- Monitoring of remote databases by forwarding network traffic
- Application agnostic
- Support for Oracle and non-Oracle Databases

ORACLE

 16

Major US East-Coast Bank
Active Database Firewall

Business Challenges	• Protect business critical databases to prevent unauthorized access, data loss and PII exposure • Monitor and protect over 600 databases across 7 international data centers. • Minimal impact to existing database performance
Solution	• Oracle Database Firewall for real-time database protection and monitoring of billions of transactions per day • Prevent unauthorized data access and malicious activity
Business Results	• Passed internal and external audit • Demonstrate active controls over data access and database systems • Standardized security, alerts and reporting across the complete business

ORACLE

 17

Major US Investment Bank
Auditing Data Changes

Business Challenges	• Monitor 60+ databases • Track every change to customer data • Alert on unauthorized changes to stored procedures or user roles and privileges • Automated report distribution to internal auditors
Solution	• Database Firewall deployed in heterogeneous environments providing monitoring and reporting on every change to customer data • Monitor procedure and user role changes with full separation of duties from existing DBA team
Business Results	• Passes daily audits • Audit data ready for sign-off automatically emailed before the start of business

ORACLE

 18

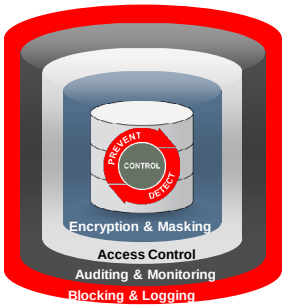
Major European Government

Protecting Government Data and PII

Business Challenges	• Prevent access to highly sensitive citizen data other than via certified application • Enforce strict application behavior through white-list • Monitor and audit every transaction 24 / 7 / 365
Solution	• Six fully redundant pairs of Database Firewall to maintain a complete database security perimeter • Critical high-availability architecture to meet strict service-level requirements
Business Results	• Complete protection from unauthorized access, hacking of malicious changes to application code • Highly sensitive citizen data protected by continuously available firewall perimeter • Meets government standards for PII data storage

ORACLE

DATABASE DEFENSE-IN-DEPTH



Blocking and Logging
- Oracle Database Firewall

Encryption and Masking
- Oracle Advanced Security
- Oracle Secure Backup
- Oracle Data Masking

Access Control
- Oracle Database Vault
- Oracle Label Security

Auditing and Monitoring
- Oracle Audit Vault
- Oracle Configuration Management
- Oracle Total Recall

ORACLE

For More Information

or

oracle.com/database/security

ORACLE

ORACLE

ORACLE IS THE INFORMATION COMPANY