Dude, Where's My Data?

Making a Case for Data Security Solutions

Brian Contos, CISSP, Chief Security Strategist

Agenda

- Background
- What do Auditors Want
- The Changing Threatscape
- Data Security Solutions
- Usage Scenarios
- Summary
- More Information

Data: One of Your Most Valuable Assets

She Knows It

"They" Do Too

Over 245 Million Records Containing Sensitive Information have been Compromised Between January 2005 and December 2008

Privacy Rights Clearinghouse "A Chronology of Data Breaches"

Breach Costs Part I

Investigate the Breach

Provide Credit Monitoring Services

Public Relations

Notify Victims

Breach Costs Part II

Fines

Brand Damage

Lawsuits

Customer Loss

56% of data breach related costs are from customer loss

After a database breach of around 40M+ customer records in 2005 – CardSystems went under and had its assets sold off

In 2007 the total average cost of a data breach was $6.3 million per breach or $197 per compromised record.

Ponemon Institute, "2007 Annual Study: Cost of a Data Breach", 2007

Verizon Data Breach Investigations Report 2008
Based on 4 Years and 500 Cases

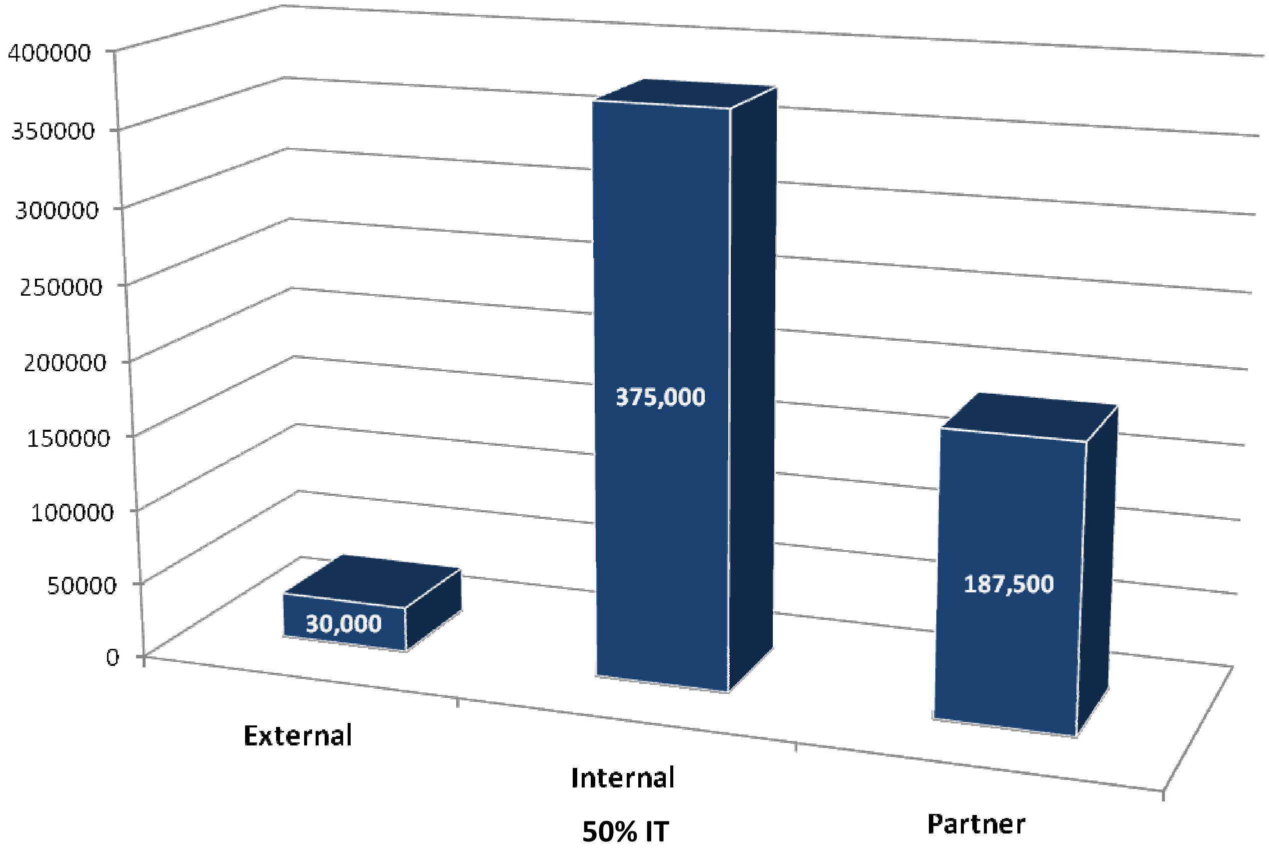
90% Breaches Involved One of the Following

- A system unknown to the organization (or business group affected)
- A system storing data that the organization did not know existed on that system
- A system that had unknown network connections or accessibility
- A system that had unknown accounts or privileges
- 66% involved data the victim did not know was on the system
- 75% of breaches were not discovered by the victim
- 83% of attacks were not highly difficult

Source: 2008 Data Breach Investigations Report Verizon Business Risk Team
http://www.verizonbusiness.com/resources/security/databreachreport.pdf

Verizon Data Breach Investigations Report 2008
Based on 4 Years and 500 Cases

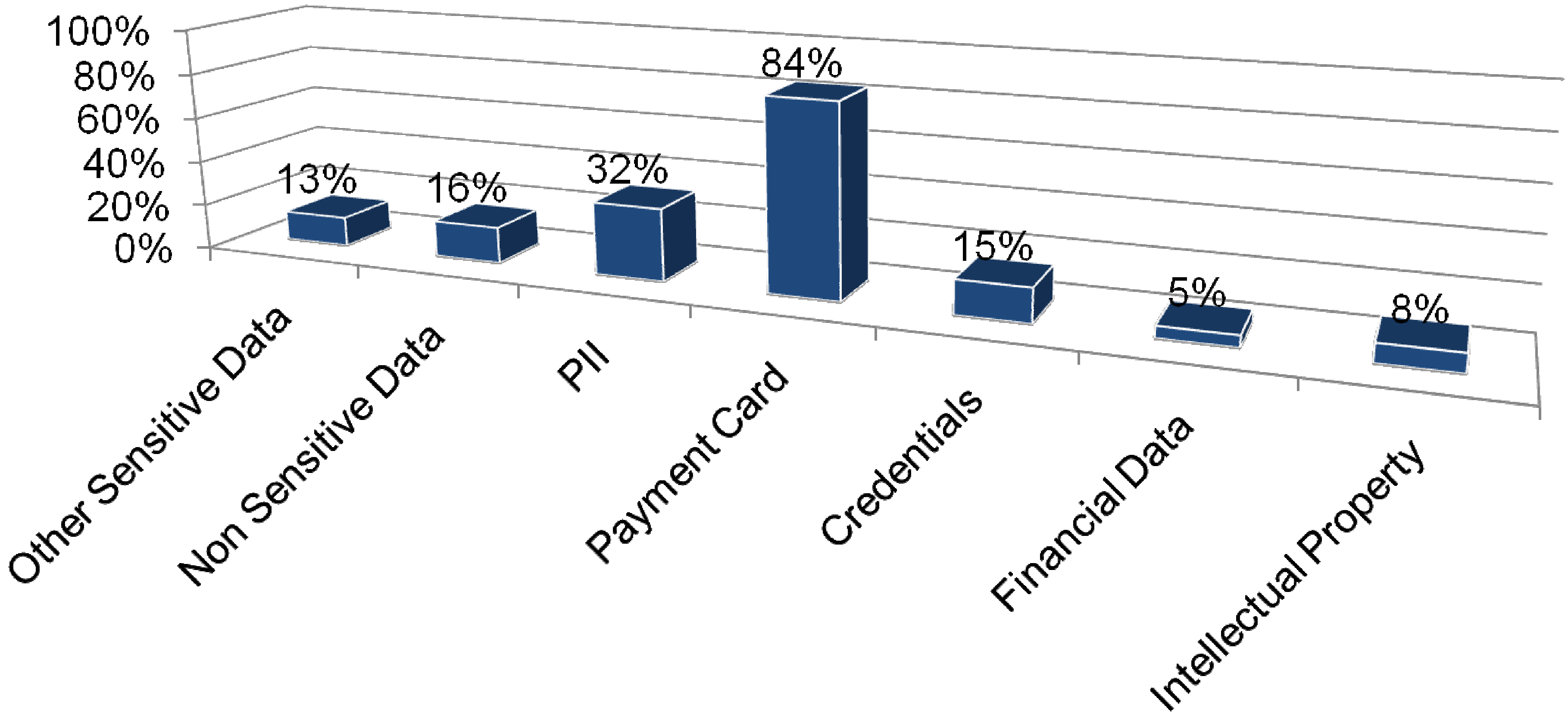
Median Number of Records Compromised



Source: 2008 Data Breach Investigations Report Verizon Business Risk Team
http://www.verizonbusiness.com/resources/security/databreachreport.pdf

Verizon Data Breach Investigations Report 2008
Based on 4 Years and 500 Cases

Percentage of Breach Type in Case Load



Source: 2008 Data Breach Investigations Report Verizon Business Risk Team
http://www.verizonbusiness.com/resources/security/databreachreport.pdf

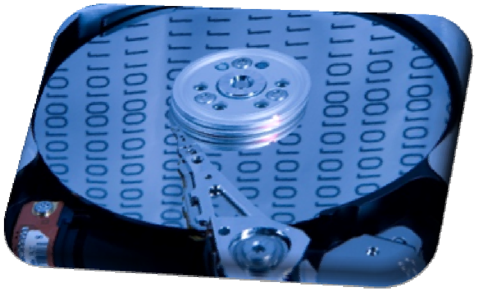
IMPERVA®

Who Else Knows: Government & Industry Groups

Two Primary Categories of Standards and Regulations

Data Integrity

- Monitor Changes to Data
- Verify Actions Meet Internal Controls
- Record Activity in Audit Trails



Data Protection

- Security Policies to Protect the Confidentiality
- Security Policies to Protect the Integrity

Data Integrity and Data Protection

Standard/Regulation Name	Integrity or Security Requirement
Payment Card Industry Data Security Standard (PCI DSS)	Section 10 requires that merchants track and monitor all access to cardholder data. Merchants must “implement automated audit trails for all system components” and “secure audit trails so they cannot be altered”.
Sarbanes-Oxley Act (SOX)	Section 302 requires management to setup controls on financial statements, evaluate the controls and report on their effectiveness. Section 404 mandates IT controls and periodic reports to validate these IT controls.
Financial Instruments and Exchange Law in Japan (J-SOX)	J-SOX requires management to evaluate and prepare a report on the effectiveness of financial reporting. Companies must also demonstrate that system development and operations, change management, and security processes are in place and followed.
Health Insurance Portability and Accountability Act (HIPAA)	Title II of HIPAA defines the following security safeguards: • 164.308(a)(1) mandates risk analysis, risk management, and information system activity review. • 164.308(a)(6) enforces security incident response including mitigating and reporting on security events.
California Senate Bill 1386	Businesses must disclose any breach of their personal information to California residents.
Gramm-Leach-Bliley Act (GLBA)	The Financial Privacy Rule governs the collection and disclosure of customers’ financial information. The Safeguards Rule requires financial institutions to design and implement safeguards to protect customer information.
EU Privacy Directive	Directive 95/46/EC protects personal data that is processed or transferred. European companies must have IT controls in place to ensure and prove to auditors that data is processed correctly.
North American Electric Reliability Corporation (NERC)	CIPS 002-009: Identification of Critical Cyber Assets, Access Controls, Monitor, Audit, & Report

Not a Choice – A Cost of Doing Business

Example: Public U.S. Companies that Fail to Meet SOX

Fines

Most Volatile S&P 500 Stocks on Earnings Report Days

Stock	Company	Price	Expected Report Date	Average Absolute % Chg on Report Day
WFMI	WHOLE FOODS MKT	45.07	5/2/07	12.65
SNDK	SANDISK CORP	44.10	4/26/07	12.41
NVDA	NVIDIA CORP	[illegible]	5/11/07	11.75
SANM	SANMINA-SCI CORP	3.60	4/26/07	11.33
AV	AVAYA INC	12.10	4/26/07	10.44
DYN	DYNEGY INC-A	10.32	5/8/07	10.43
AMZN	AMAZON.COM INC	41.89	4/26/07	10.43
GTW	GATEWAY INC	2.17	4/23/07	9.95
HAR	HARMAN INTL	[illegible]	4/26/07	9.84
NOVL	NOVELL INC	[illegible]	5/31/07	9.76
HSP	HOSPIRA INC	40.78	5/8/07	9.22
ADCT	ADC TELECOM INC	17.31	5/31/07	8.90
WMB	WILLIAMS COS INC	28.88	5/7/07	8.90
YHOO	YAHOO! INC	31.80	4/17/07	8.85
ANDW	ANDREW CORP	10.81	4/27/07	8.64
BRCM	BROADCOM CORP-A	[illegible]	4/26/07	8.59
CTXS	CITRIX SYSTEMS	33.21	4/18/07	8.39
CTSH	COGNIZANT TECH	[illegible]	5/3/07	8.30
TLAB	TELLABS INC	9.68	4/26/07	8.12
SHLD	SEARS HOLDINGS	180.27	5/18/07	8.05
NTAP	NETWORK APPLIANC	35.32	5/24/07	8.05
TEX	TEREX CORP	[illegible]	5/4/07	8.04
PMCS	PMC-SIERRA INC	7.13	4/20/07	7.87
UNM	UNUM GROUP	23.86	5/2/07	7.83
NTAP	NETWORK APPLIANC	35.32	5/3/07	8.05

Unable to File Earnings Reports

Exec Officers that Willfully Violate SOX can Face Imprisonment

What do Auditors Want Part I

Auditors are looking at regulated data residing in databases connected to enterprise applications such as SAP, Oracle E-Business Suite, PeopleSoft and others

- Regulations & Standards Demand it
  - Sarbanes-Oxley, PCI, HIPAA, and Others
- So they Analyze areas such as
  - User Management
  - Authentication
  - Separation of Duties (SOD)
  - Access Controls
  - Audit Trails

What do Auditors Want Part II

Consistent Themes for the Multi-Regulated

Full Audit of All Activity and Operations

- Covers Entire Database & Database Infrastructure
- All Databases, Tables, Columns, or Users

Separation of Duties

- Independent of Audited System
- Not Part of the Audited Database

User Accountability

- Audit Trail Must Demonstrate User Accountability
- Especially over “pooled” connections
- Not Part of the Audited Database

User Activity

- Separate Suspicious Behavior and Material Variances from “normal” Activity

Demonstrate Compliance

- Reports on the Above (Distributed, Reviewed, Approved)

IMPERVA®

What do Auditors Want Part III

Five Questions they Ask

1. Is the audit process independent from the database system being audited?
2. Does the audit trail establish user accountability?
3. Does the audit trail include appropriate detail?
4. Does the audit trail identify material variances from baseline activity?
5. Is the scope of the audit trail sufficient?

What do Auditors Want Part IV

Independence

1. Is the audit process independent from the database system being audited?

   - Process must be independent of the database server & DBAs
     - Rouge administrators could tamper with records and cover tracks
   - Audit duties must be separate from database administration
   - Audit data collection should be independent of native database software capabilities
   - External audit solutions provide independence, but can’t rely upon native database software capabilities

What do Auditors Want Part V

Accountability

2. Does the audit trail establish user accountability?

- Each database transaction must be contributed to a specific user
  - For SOX – each change to financial reporting data must have a user
- Problems
  - Most users don't directly interact with the database (pooled users)
- Solutions
  - Application rewrites – Unique accounts or references
  - Proprietary database audit mechanisms
  - Web application audit data - timestamp correlation
- Drawbacks
  - Issues with performance, user management, 3rd party software limitations, cost, time, code change risks

IMPERVA®

What do Auditors Want Part VI

Detail

3. Does the audit trail include appropriate detail?

- Example 1: JOHN requested DATA from the CUSTOMER database and the database **returned DATA**

- Example 2: JOHN requested FIRST NAMES, LAST NAMES, EMAIL ADDRESSES, PHON NUMBERS, and CREDIT CARD NUMBERS for ALL customer from the CUSTOMER database and the database **returned 65,000 records**

- Assuming that John is authorized Example 1 is of little use

- Detailed transactions logs can overwhelm processors, disks, and I/O resources (many organizations opt for basic)

The average score for your manual dexterity is 95%
The average note for your metallurgy is 85%

Pass #1

Pass #1

Parameters positions :

Technique : Push

The average score for your manual dexterity is 95%
The average note for your metallurgy is 85%

Screenshot of your weld

Execution

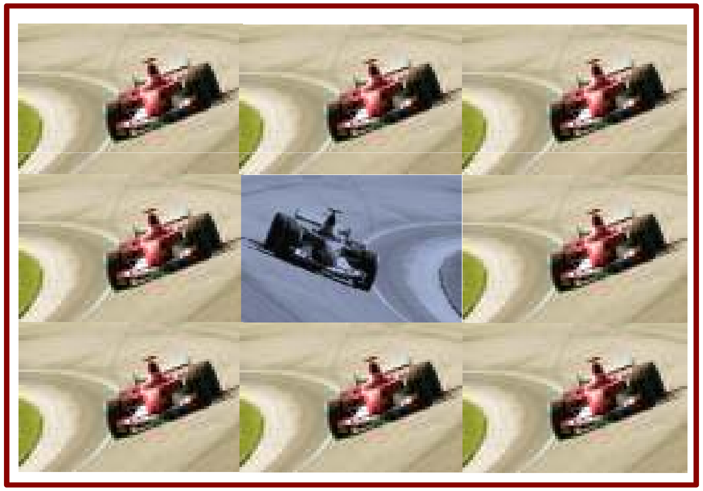
What do Auditors Want Part VII
Material Variances

4. Does the audit trail identify material variances from baseline activity?

- Chronological listing of transactions is insufficient – volume is overwhelming identification is difficult

- Prioritization is needed – separate variances from legitimate activity

- Most native auditing systems lack this capability – resulting in error-prone, manual, time-consuming and costly analysis

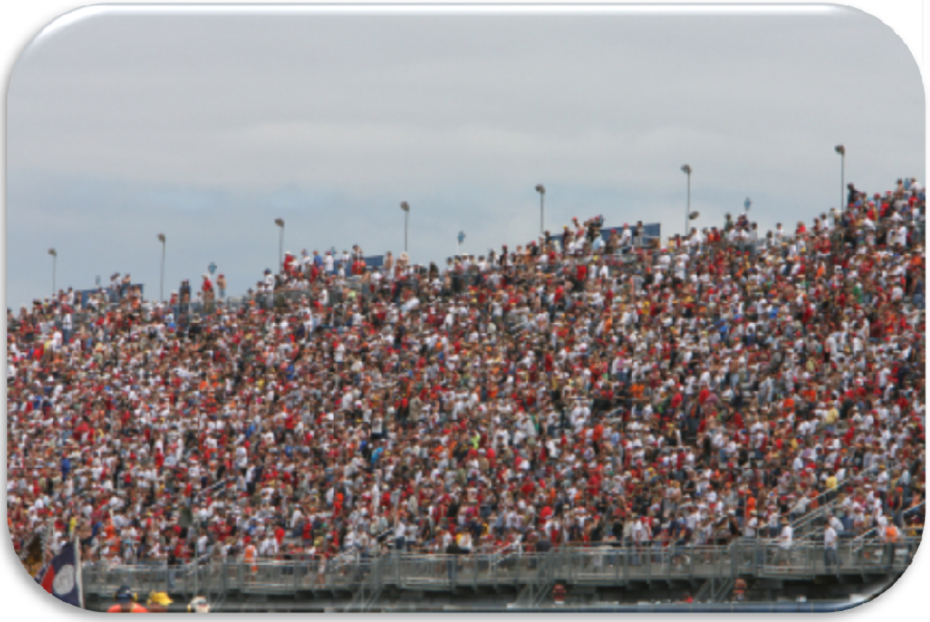


What do Auditors Want Part VIII

Sufficient Scope

5. Is the scope of the audit trail sufficient?

- Need to audit and monitor
  - Database software
  - Operating system software
  - Database Protocols
- To identify attacks on
  - Database platform vulnerabilities
  - Operating system vulnerabilities
  - Protocols (DB protocols don’t conform to an open standard & often change)
    - Unauthenticated data access
    - Native audit log evasion



IMPERVA®

Changing Threatscape

Complexity Has Increased

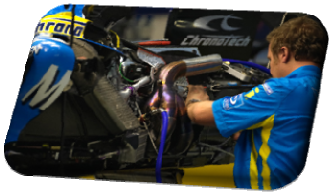
→

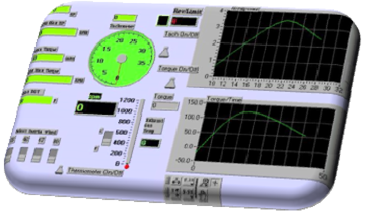
- Attacks are now financially motivated; valuable information resides in applications and databases
- Application and database exposure was historically internal
- They have limited security; often not coded by experts
- They are highly complex, customized, and often change (no longer static)
- Issues on the user (browser side) and organization (server side)
- Attack vectors have moved from open ports/services, OS vulnerabilities, & bypassing network firewalls to: SQL Injection, CSRF, Clickjacking
- Applications need their own layers of protection (Network security won't save you)
- Databases need their own layers of protection (Database controls won't save you)

Data Security Solutions: Pre Race Prep Part I

Pre Race

- Security Development Life Cycle (SDLC) – Microsoft for example
- Developer Education, Training and Awareness
- Static Code Testing (Reviews and Walkthroughs)
- Dynamic Code Testing (Executing Programmed Code)
- Architectural Risk Analysis
- Abuse Cases
- Black Box Testing (No Internal Knowledge)
- White Box Testing (Internal Knowledge)
- Discovery and Validation
- Vulnerability Assessment and Pen Testing (L7)





Data Security Solutions: Pre Race Prep Part II

- Turn off default output/error messages to users (just needed for testing)
- Trap and log errors using log files (or leverage alternative logging/auditing solutions)
- Don’t divulge information such as OS, application, database, etc. (modify headers to hide)
- Don’t leave old versions of backed up code on production servers
- Don’t give the Application full access to the Database (two separate layers/secured separately)
  - Might reveal embedded passwords used in testing
  - Might reveal source code information or configuration information
- Define inputs; drop everything else (input validation on application and database)
  - If you want an integer – only allow integers
  - Set length limits (prevents buffer overflows)
  - Do this for all inputs, alpha and/or numeric
- Cleaning/filtering doesn’t scale because there are too many was to say the same thing

Complexity Example - Web Escaping And Encoding: How many ways can you hide <

<

Percent Encoding

```
%3c
%3C
```

HTML Entity Encoding

```
&#60
&#060
&#0060
&#00060
&#000060
&#0000060
&#60;
&#060;
&#0060;
&#00060;
&#000060;
&#0000060;
&#x3c
&#x03c
&#x003c
&#x0003c
&#x00003c
&#x000003c
&#x3c;
&#x03c;
&#x003c;
&#x0003c;
&#x00003c;
&#x000003c;
&#X3c
&#X03c
&#X003c
&#X0003c
&#X00003c
&#X000003c
&#X3c;
&#X03c;
&#X003c;
&#X0003c;
&#X00003c;
&#X000003c;
&#x3C
&#x03C
&#x003C
&#x0003C
&#x00003C
&#x000003C
&#x3C;
&#x03C;
&#x003C;
&#x0003C;
&#x00003C;
&#x000003C;
&#X3C
&#X03C
&#X003C
&#X0003C
&#X00003C
&#X000003C
&#X3C;
&#X03C;
&#X003C;
&#X0003C;
&#X00003C;
&#X000003C;
&lt
&lT
&Lt
&LT
&lt;
&lT;
&Lt;
&LT;
```

JavaScript Escape

```
\<
\x3c
\X3c
\u003c
\U003c
\x3C
\X3C
\u003C
\U003C
```

CSS Escape

```
\3c
\03c
\003c
\0003c
\00003c
\3C
\03C
\003C
\0003C
\00003C
```

Overlong UTF-8

```
%c0%bc
%e0%80%bc
%f0%80%80%bc
%f8%80%80%80%bc
%fc%80%80%80%80%bc
```

US-ASCII

```
¼
```

UTF-7

```
+ADw-
```

Punycode

```
<-
```

Simple Double Encoding

```
< --> &lt; --> &#26;lt&#59 (double entity)
< --> %3c --> %253c (double percent)
etc...
```

Double Encoding with Multiple Schemes

```
< --> &lt; --> %26lt%3b (first entity, then percent)
< --> %26 --> &#25;26 (first percent, then entity)
etc...
```

Simple Nested Escaping

```
< --> %3c --> %%33%63 (nested encode percent both nibbles)
< --> %3c --> %%33c (nested encode first nibble percent)
< --> %3c --> %3%63 (nested encode second nibble percent)
< --> &lt; --> &&108;t; (nested encode l with entity)
etc...
```

Nested Escaping with Multiple Schemes

```
< --> &lt; --> &%6ct; (nested encode l with percent)
< --> %3c --> %&#x33;c (nested encode 3 with entity)
etc...
```

Quadrillion

1,677,721,600,000,000

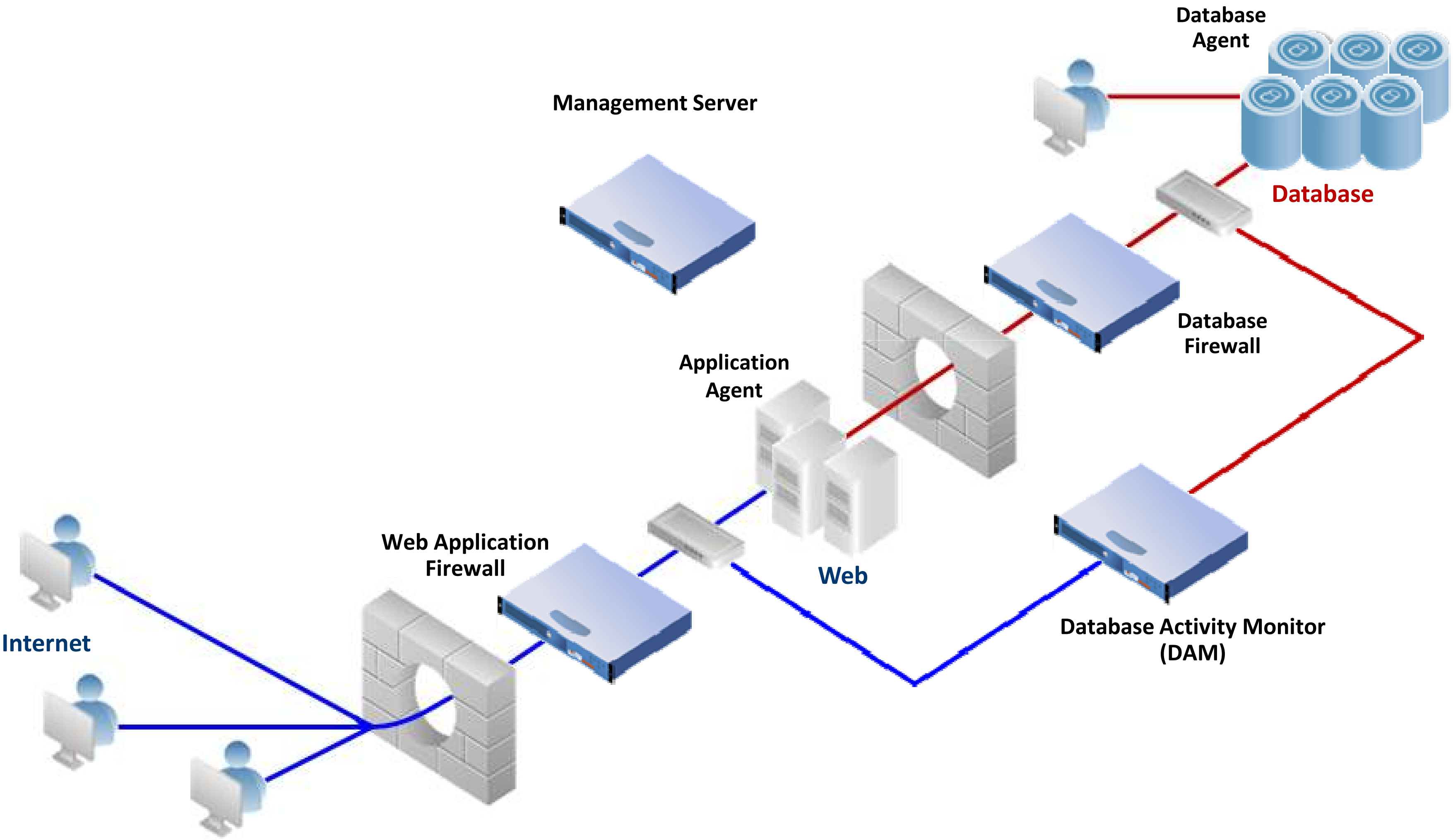
ways to encode <script>

Data Security Solutions: Race Day

Race Day

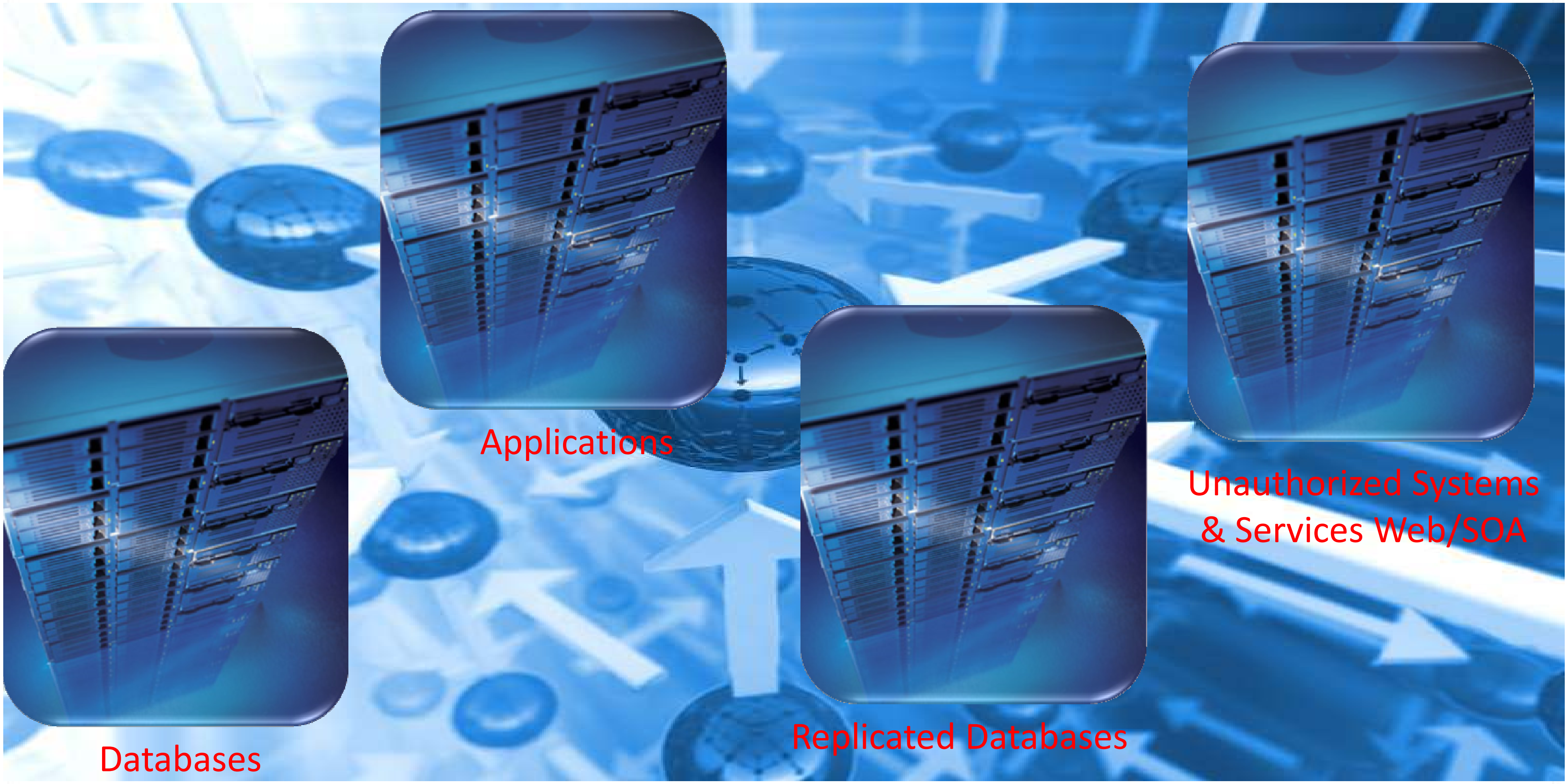
- Web Application Firewalls (WAF)
- Database Firewalls
- Database Activity Monitoring (DAM) Solutions

WAF and DAM Architecture Options



Usage Scenario:
Discovery, Categorization, & Validation Part I

Where are my applications & databases?



Applications

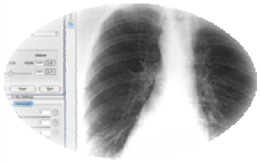
Unauthorized Systems
& Services Web/SOA

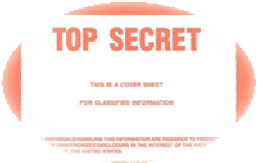
Databases

Replicated Databases

Usage Scenario:
Discovery, Categorization, & Validation PII

What sensitive data resides on them?





ABC	123	Other
ert	654	5546 4857 8138 9872
ffdd	555	8574 2201 1587 1295
ytryj	1265	3571 2252 4467 8849
nnj	98	7145 7585 9872 0002

ABC	123	Credit Card Numbers
ert	654	Cat
ffdd	555	Dog
ytryj	1265	Fish
nnj	98	Bird

Test Server Using Real Customer Data

Leveraging Validation Algorithms Such as the Luhn Algorithm

Usage Scenario: Profiling Application-Database-User Communications Part I

SELECT * FROM table_name

SELECT LastName FROM Persons

SELECT E_Name FROM
Employees_Norway
UNION
SELECT E_Name FROM
Employees_USA

Changing URLs

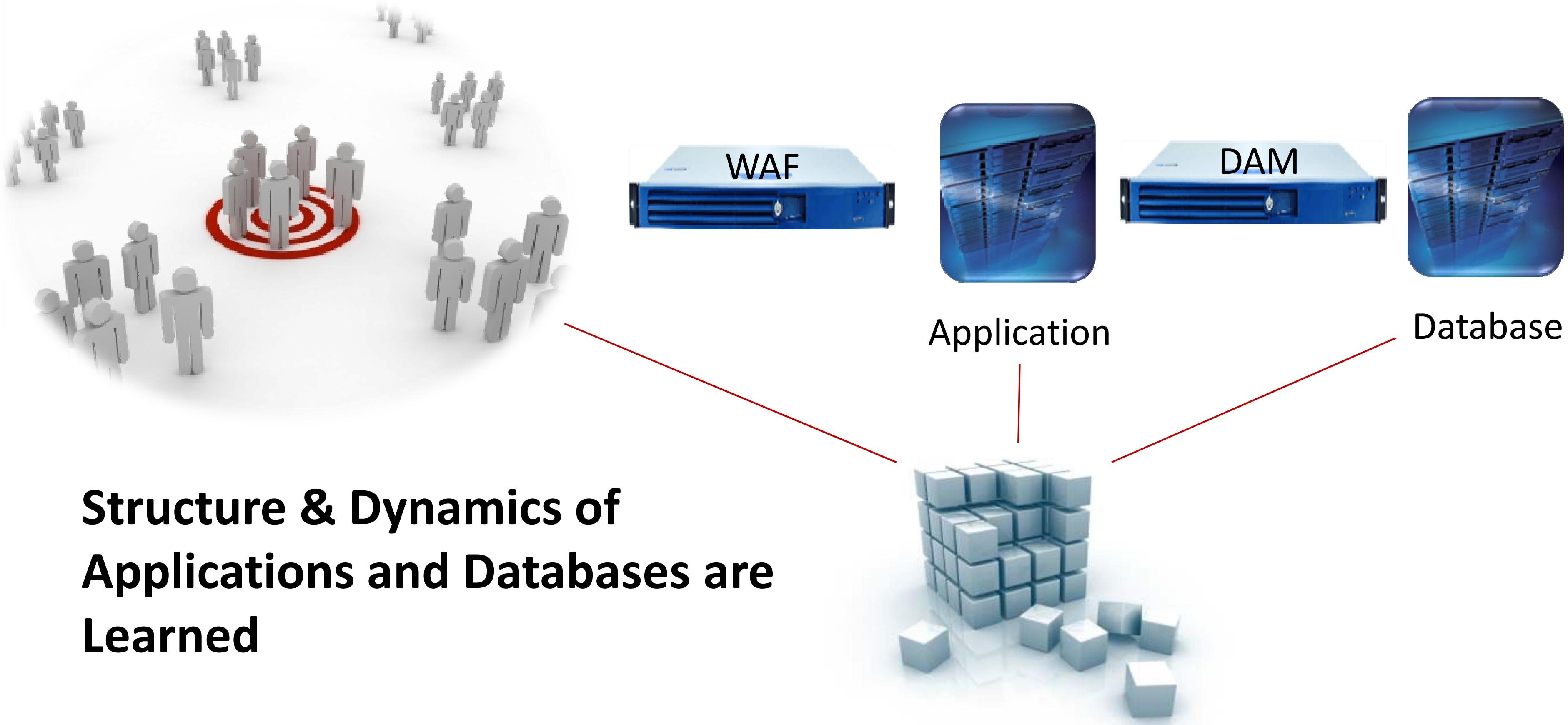
Changing Cookies

Changing Queries

Parameters, Commands, Stored Procedures, Etc.

IMPERVA®

Usage Scenario: Profiling Application-Database-User Communications Part II



Structure & Dynamics of Applications and Databases are Learned

Behavior is Modeled

Usage Scenario: Profiling Application-Database-User Communications Part III

Compare Profiles Against Observed Traffic
Detect Malicious Activity
Detect Usage Policy Exceptions

- **Volume**
- **Location**
- **Time**
- **Data Type**
- **Upload**
- **Download**

- **Login**
- **BCOPY**
- **BDELETE**
- **GET**
- **POST**
- **Etc.**

(SQL Injection) 1 OR 1=1, 1' OR '1'='1, 1'1, 1 EXEC SP_ (or EXEC XP_), 1 AND USER_NAME() = 'dbo‘

Select, update, insert, alter, drop, backup, kill, shutdown, **truncate**, create, revoke, deny, restore

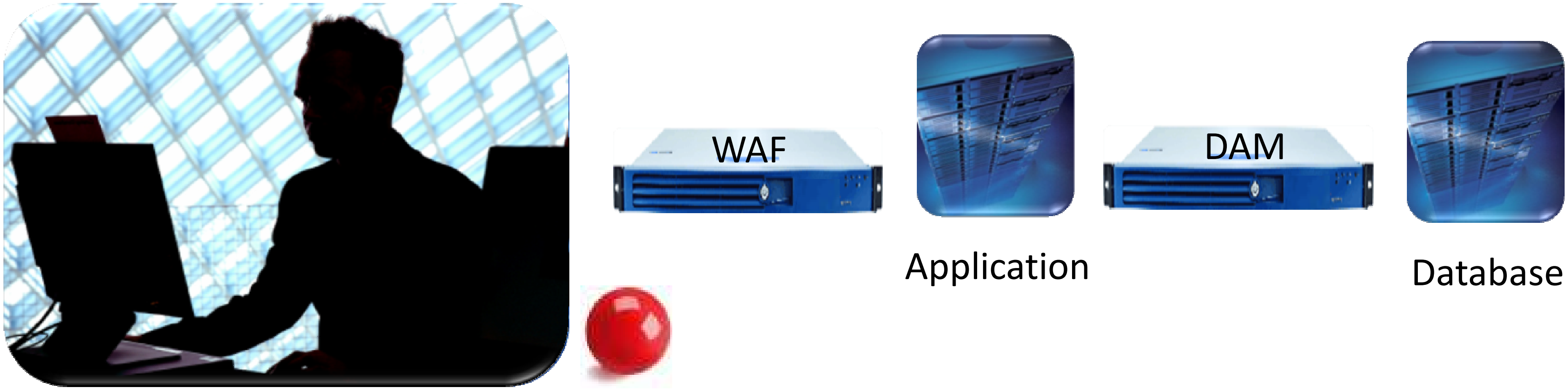
Usage Scenario: Tracking Pooled Users Part I

User Pooling – Common & Negates Accountability

Can You Spot The Bad Guy?

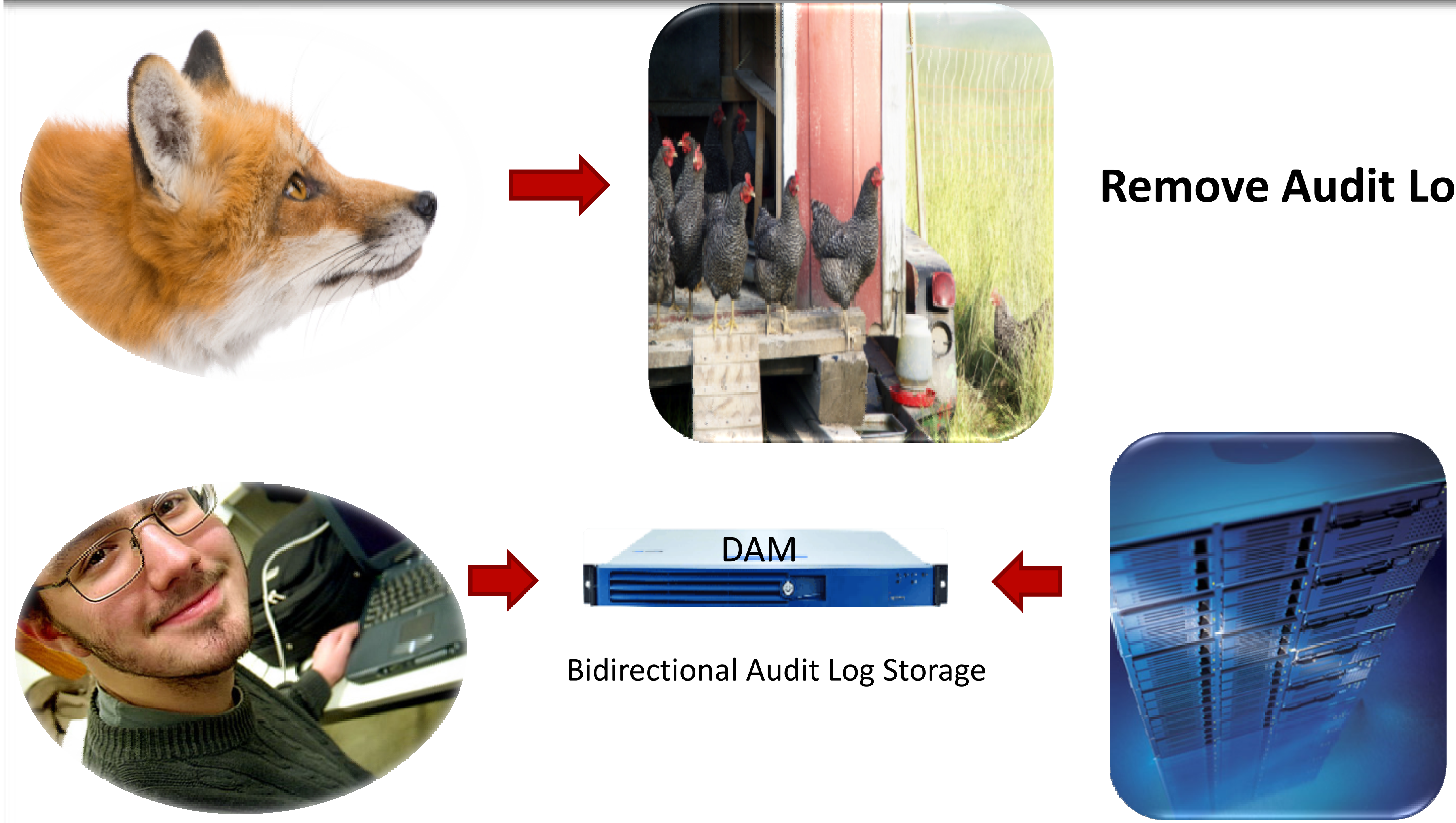
How About Now?

Usage Scenario: Tracking Pooled Users Part II



- Application Authentication
- Database SQL Queries
- Database Response
- Session Associated with Individual User
- Timestamps Captured for Full Audit Trail

Usage Scenario: Database Audit Part I



Remove Audit Logs

DAM

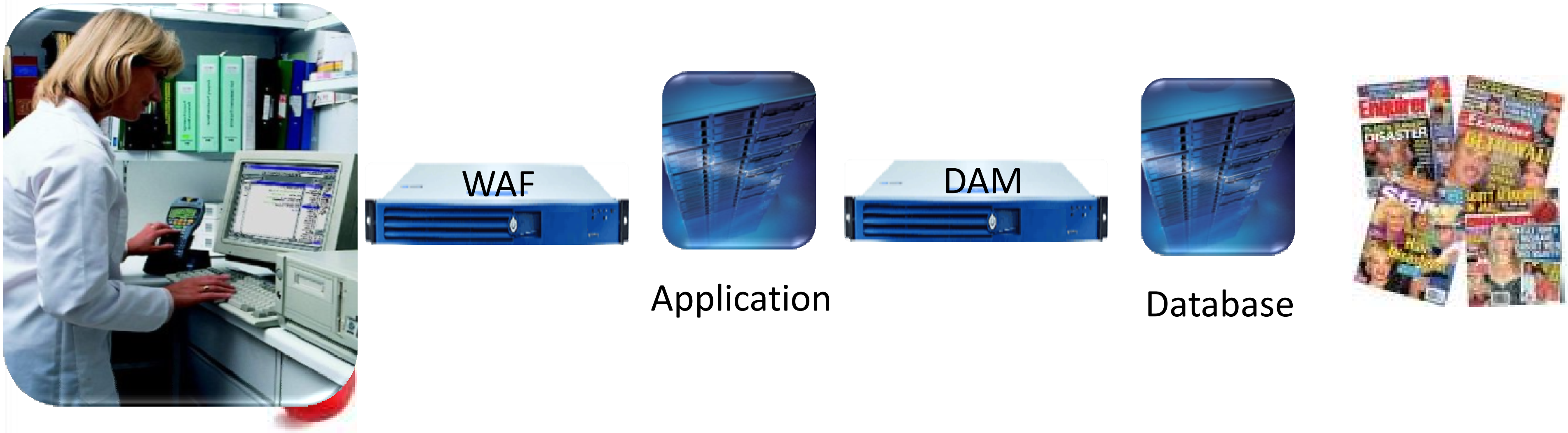
Bidirectional Audit Log Storage

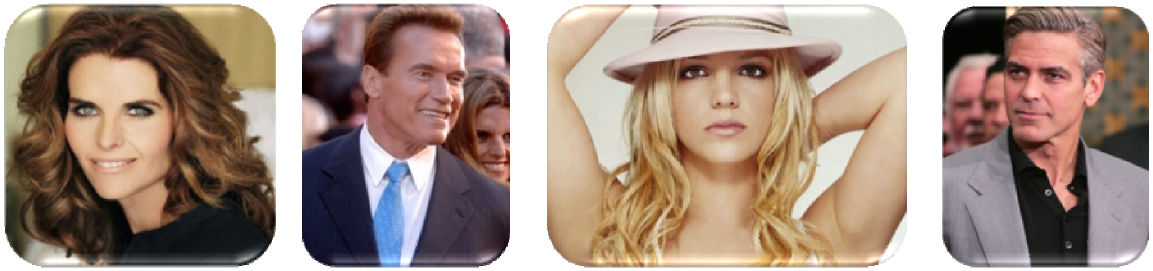
Database

Usage Scenario: Database Audit Part II

- No Audit Logs to Remove
- Capture Malformed Queries
- Separation of Duties (SOD)
- Performance Gain
- Centralized Analysis
- Heterogeneous support
- Understand Breach – Limit Liability
- Litigation-Quality Data

Usage Scenario: Privilege Abuse





Who? How? What? When?

Usage Scenario: Virtual Patching Part I

(Integration with VA)

XSS

SQL injection

Directory Traversal

Application

WAF

Directory Traversal

SQL Injection

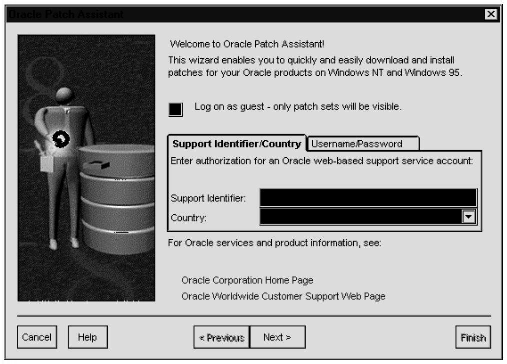
XSS

Vulnerability Information In

Blocking Rules and/or Alerts Out

Case Study: Virtual Patching Part II

(Integration with Reverse Engineered Vendor Patches)



Oracle Patch Assistant

Welcome to Oracle Patch Assistant!

This wizard enables you to quickly and easily download and install patches for your Oracle products on Windows NT and Windows 95.

■ Log on as guest - only patch sets will be visible.

Enter authorization for an Oracle web-based support service account:

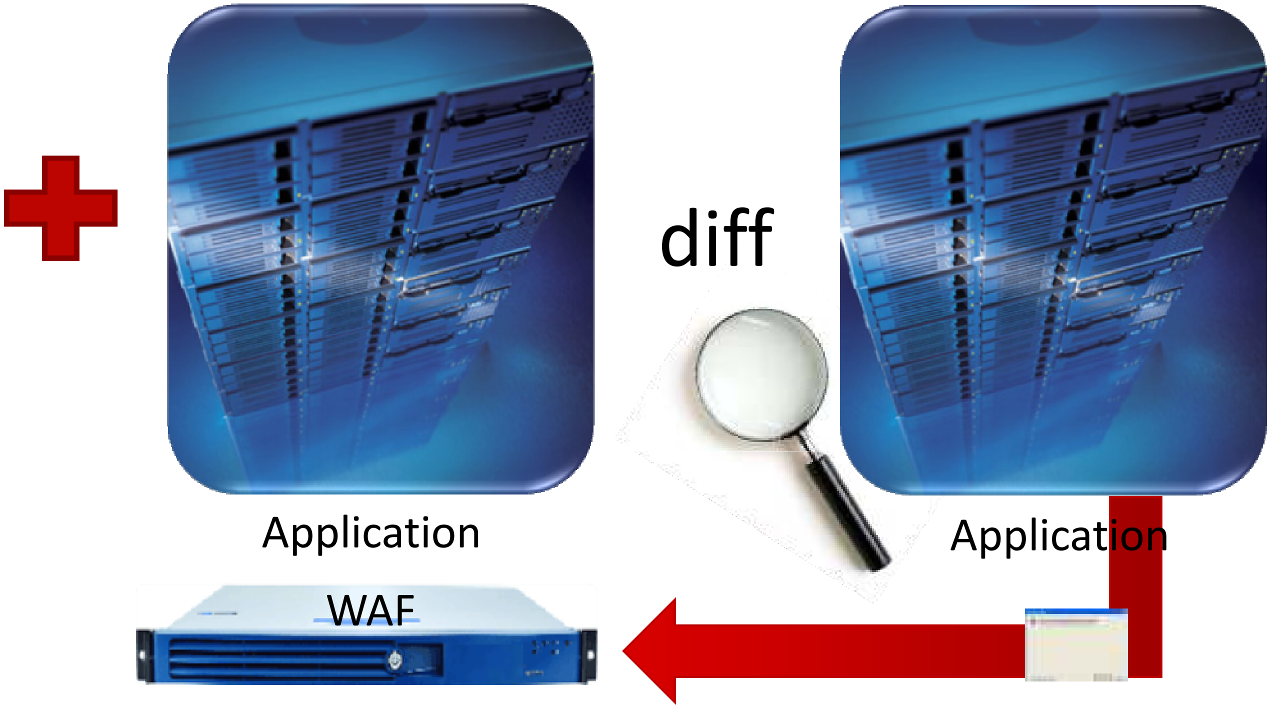
Support Identifier: [redacted]

Country: [redacted]

For Oracle services and product information, see:

Oracle Corporation Home Page

Oracle Worldwide Customer Support Web Page



Patch + 48 Hours = Exploit

App & DB Patching Practices are Slow (Operational Availability, Functionality

Patching Survey Results: 10% Days, 50% Weeks, 40% Months or Never

Who Needs a Zero Day?

Summary

- Sensitive Data is the New Target
- Bad Guys Want it; Good Guys Need to Protect it; Auditors Audit it
- Classic Network Security Solutions Aren't Enough
- Audit is Extremely Important for Sensitive Data
  - Is the audit process independent from the database system being audited?
  - Does the audit trail establish user accountability?

    (You can't arrest an IP Address)
  - Does the audit trail include appropriate detail?
  - Does the audit trail identify material variances from baseline activity?
  - Is the scope of the audit trail sufficient?
- Data Security Solutions Require a Holistic Approach
  - Pre Race & Race Day

More Information

- OWASP (Open Web Application Security Project) www.owasp.org
- WASC (Web Application Security Consortium)

  www.webappsec.org
- SANS Institute www.sans.org
- Imperva Data Security Blog blog.imperva.com
- Imperva Security Podcast *(or search for 'Imperva' on iTunes)*

  www.imperva.com/resources/podcasts.asp
- Imperva Channel on YouTube *(or search for 'Imperva' on YouTube)*

  www.youtube.com/user/ImpervaChannel
- Imperva on Twitter twitter.com/Imperva