IT Security Briefing:
Security Risks in the Oracle Database

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

November 18, 2010

INTEGRIGY

Background

Speaker

Stephen Kost

- CTO and Founder
- 16 years working with Oracle
- 12 years focused on Oracle security
- DBA, Apps DBA, technical architect, IT security, …

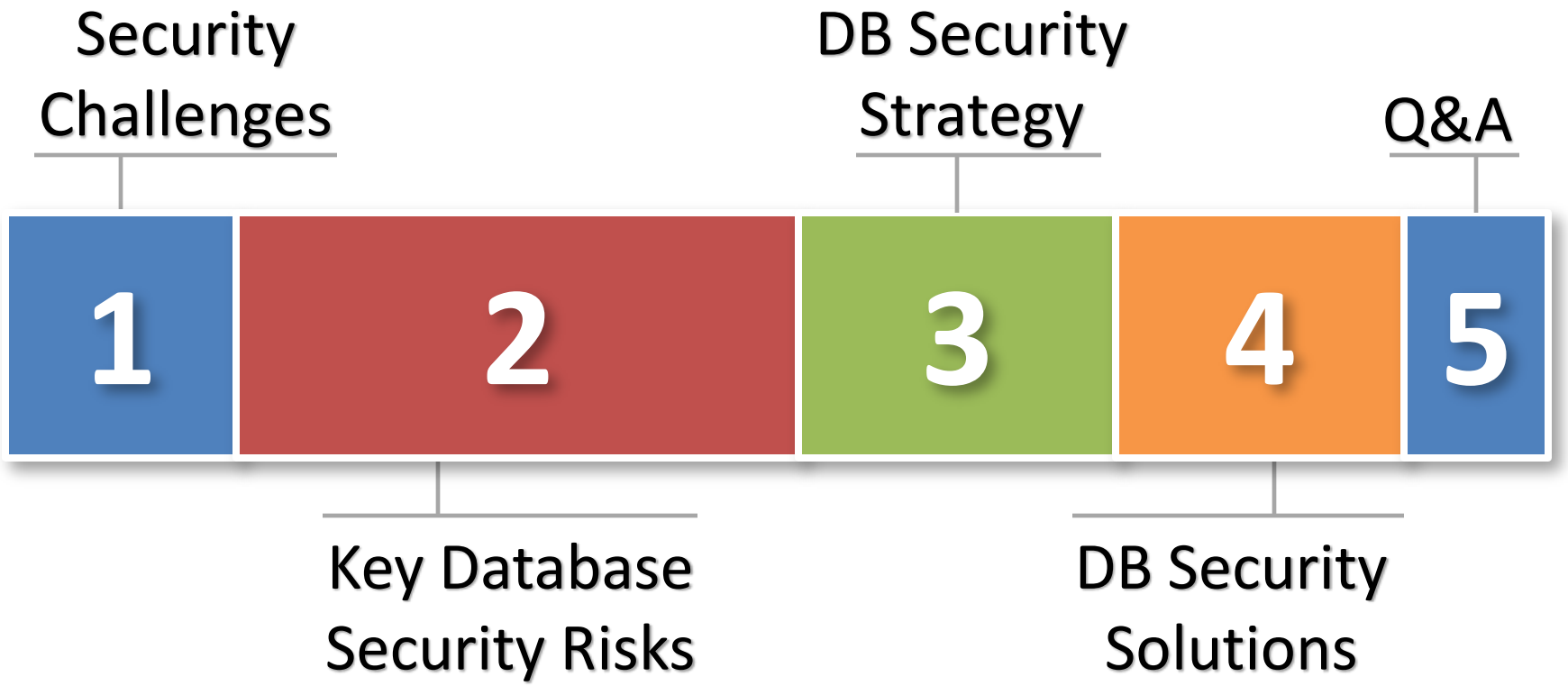
Company

Integrigy Corporation

- Integrigy bridges the gap between databases and security
- Security Design and Assessment of Oracle Databases
- Security Design and Assessment of the Oracle E-Business suite
- AppSentry - Security Assessment Software Tool

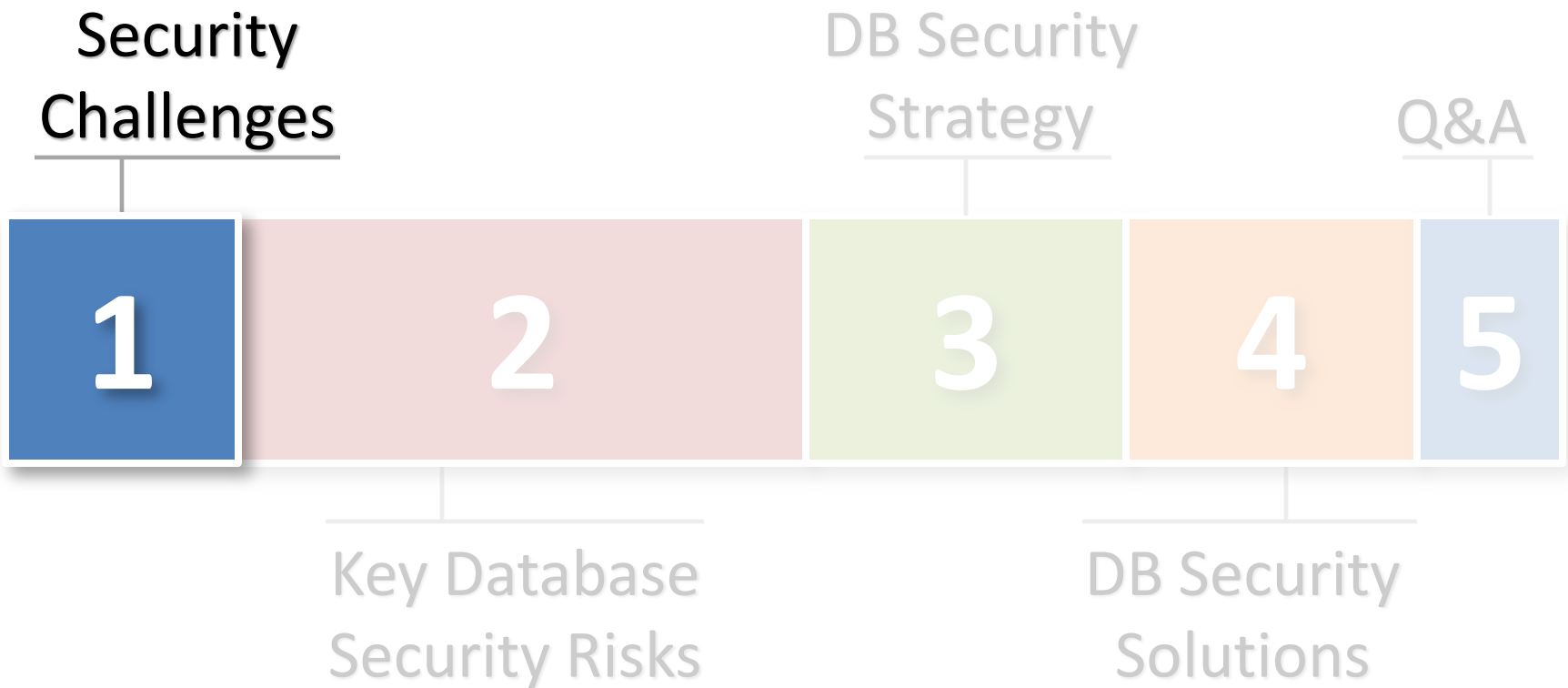
INTEGRIGY

Agenda



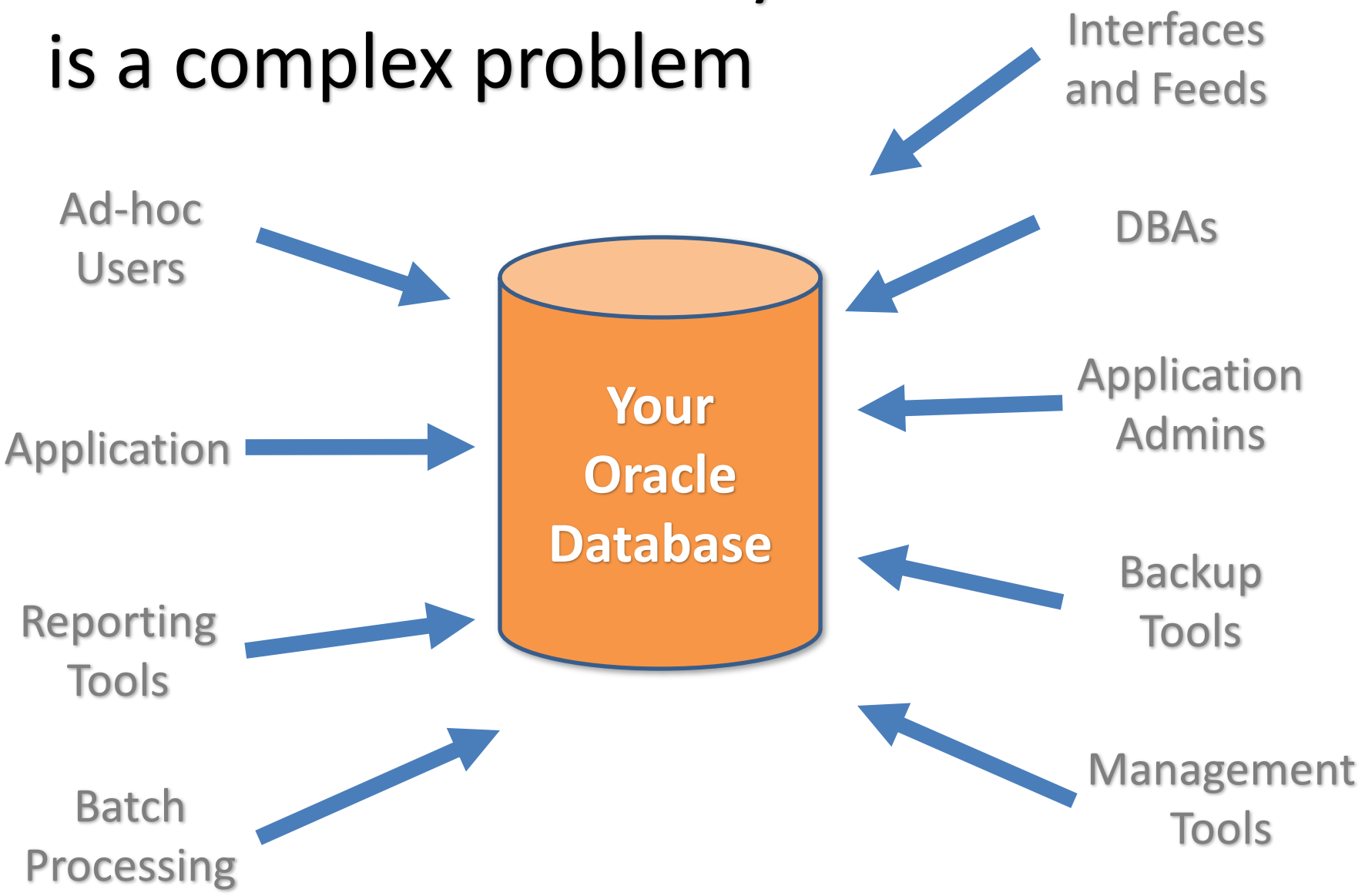
INTEGRIGY

Agenda

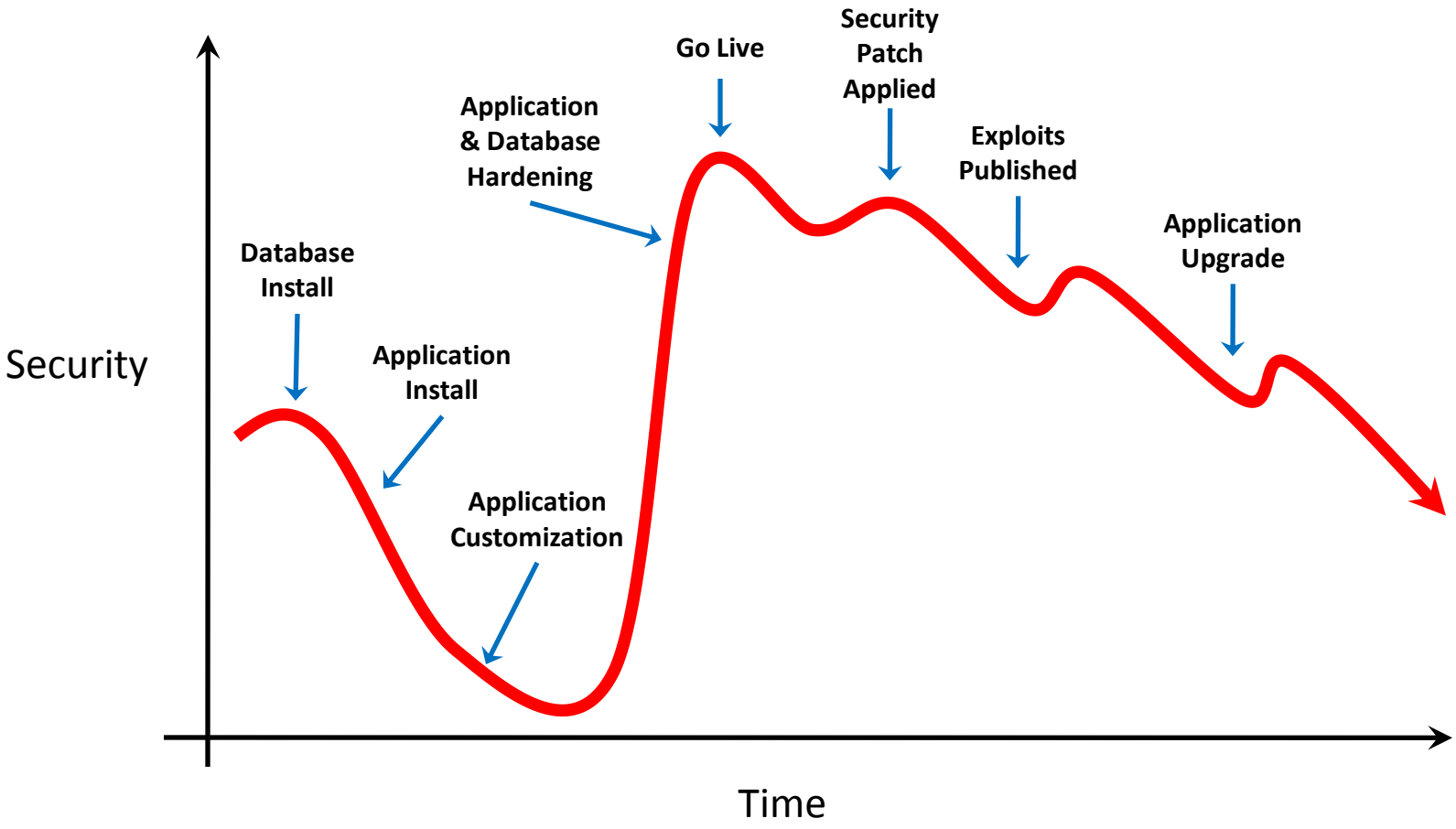


INTEGRIGY

Database connectivity is a complex problem



Database security **decays** over time



Organizational Misalignment

- **IT Security**
  - Excellent at network and operating system security
  - Limit or no understanding of database security
  - Securing Oracle EBS is different than networks and operating systems – SQL, application architectures, data warehousing, etc.
- **Risk Management**
  - Database risk not properly quantified
  - Data classification not extended to caretaker of data
  - Databases and applications poor at handling data classification
- **Database Administrators (DBAs)**
  - Not aware of security requirements nor security-focused
  - No time to properly secure the database and application
  - Always afraid of impacting the application or performance of the database

Security and Compliance Drivers

- **Sarbanes-Oxley (SOX)**
  - Database object, structure, and configuration changes
  - User and privilege creation, deletion, and modification
  - Reports for sampling of changes to change tickets
- **Payment Card Industry - Data Security Standard (PCI-DSS)**
  - 12 stringent security requirements
- **Privacy (National/State Regulations)**
  - Read access to sensitive data (National Identifier and Bank Account Number)
  - California and Massachusetts data privacy laws
- **Business Audit and Security Requirements**
  - Internal adoption of COBIT or COSO
  - Preventative and detective controls

INTEGRIGY

PCI-DSS Compliance Example

- **PCI 6.1 – "*Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.*"**

- **Few Oracle customers install patches within 30 days**
- **Most customers are 1 to 2 quarters behind**
- **Business must prioritize applying security patches – effort to functionally test and apply, down-time**

- **See Integrigy Whitepaper "Oracle Applications 11i: Credit Cards and PCI Compliance Issues"**

INTEGRIGY

Agenda

INTEGRIGY

Key Security Risks

1. Exploitation of Oracle security vulnerabilities
2. Brute forcing of Oracle database passwords
3. Lack of and trustworthiness of DB auditing

Database Vulnerabilities (October 2010)

Supported Database Version	Exploitable Without Authentication	PUBLIC	Other Advanced Privileges (i.e., SELECT_CATALOG_ROLE)
10.1.0.5	CVE-2010-2407 - XDK	CVE-2010-2419 - JVM CVE-2010-2391 - Core	CVE-2010-2415 - CDC
10.2.0.4	CVE-2010-2407 - XDK	CVE-2010-2419 - JVM	CVE-2010-2415 - CDC
11.1.0.7	CVE-2010-2407 - XDK	CVE-2010-2419 - JVM CVE-2010-2412 - OLAP	CVE-2010-2415 - CDC
11.2.0.1		CVE-2010-2419 - JVM	CVE-2010-2415 - CDC
Unsupported Versions			CVE-2010-1321 - CDC CVE-2010-2411 - Job Queue

Who can exploit a PUBLIC bug?

Anyone with a database account

Remember those application accounts with generic passwords such as APPLSYSPUB/PUB in Oracle E-Business Suite

INTEGRIGY

Oct 2010 DB Bugs – Highest Risk

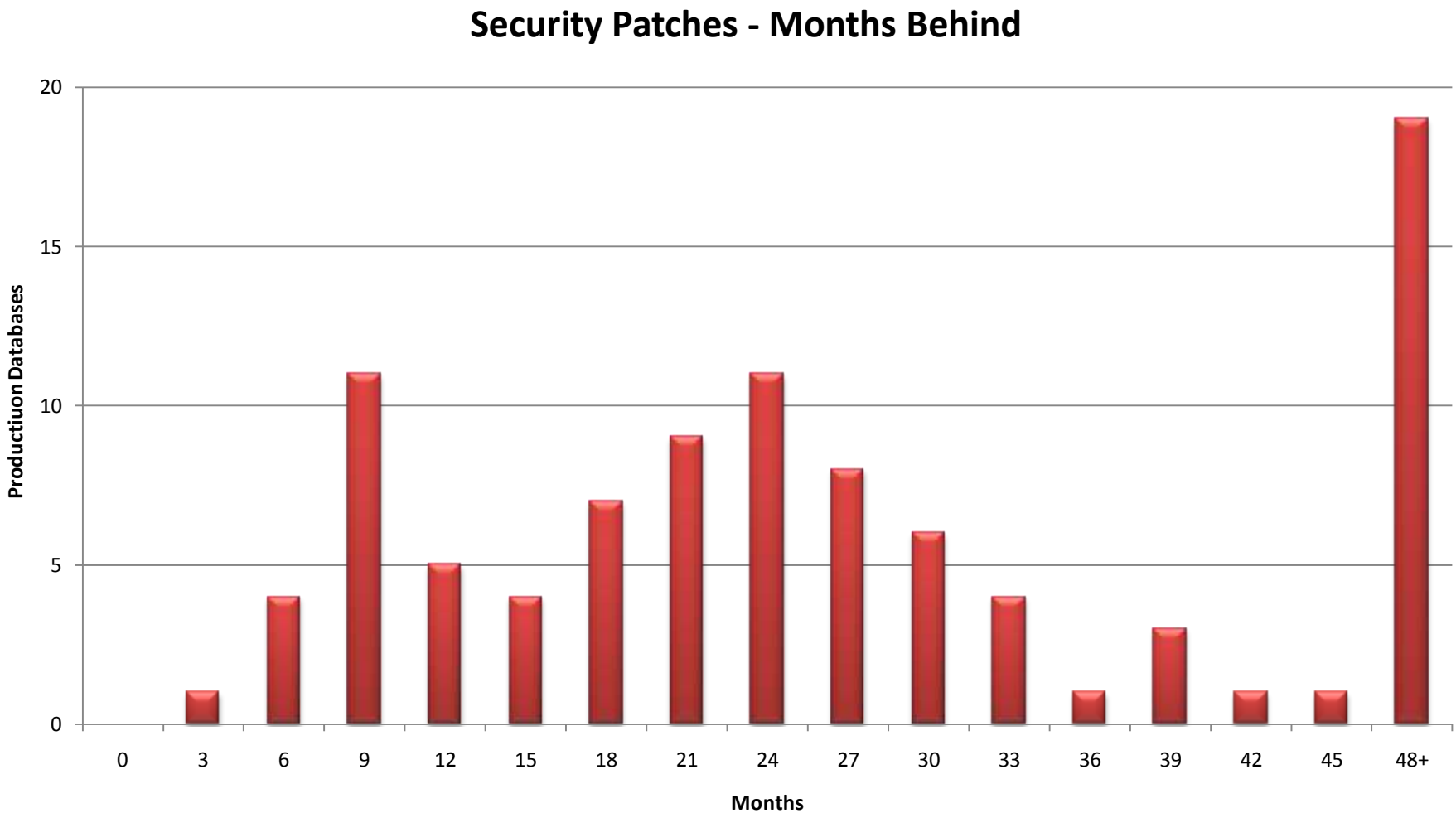
CVE	Component	CVSS 2.0	Notes
CVE-2010-2419	Java Virtual Machine	**6.5** Conf = Partial+ Integrity = Partial+ Avail = Partial+ Require Auth = Yes	**Requires only CREATE SESSION system privilege** Bug fix is - ***revoke execute on "oracle/aurora/vm/HotLoader" from public*** Similar to April 2010 Java Bugs (CVE-2010-0866 and CVE-2010-0867)
CVE-2010-2412	OLAP **11.1.0.7 only**	**5.5** Conf = Partial+ Integrity = Partial+ Avail = None Require Auth = Yes	**Requires only CREATE SESSION system privilege** Updates DBMS_ODM package, which has PUBLIC EXECUTE privileges SQL injection in DBMS_ODM
CVE-2010-2319	Core RDBMS **10.1.0.5 and 10.2.0.3 only**	**3.6** Conf = Partial Integrity = Partial Avail = None Require Auth = Yes	**Requires only CREATE SESSION system privilege** No information released regarding the vulnerability

Vulnerability Demonstration

Oracle Database Java 0-day release at Black Hat DC 2010 – February 2, 2010

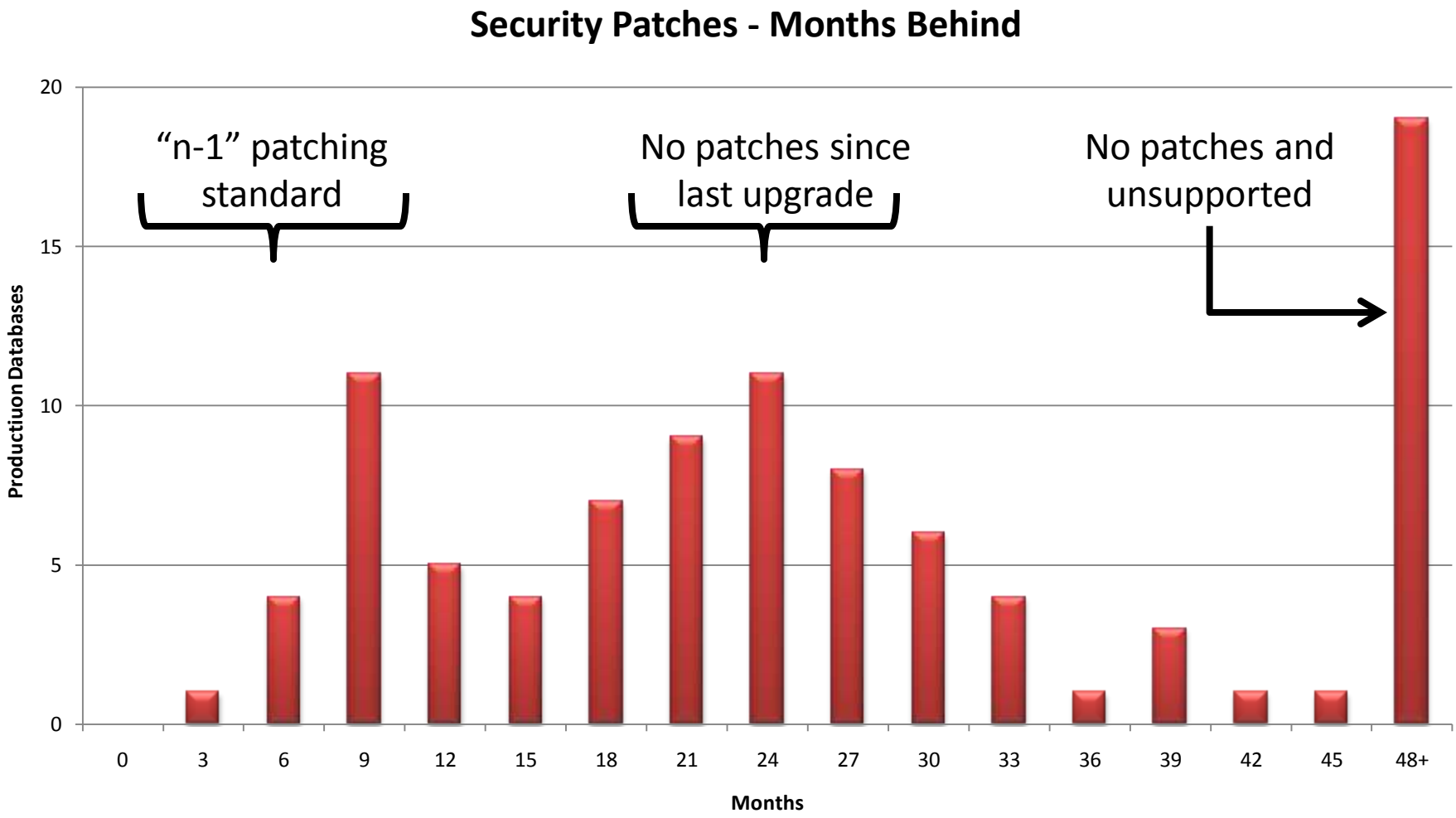
INTEGRIGY

Oracle CPU Patching Metric



INTEGRIGY

Oracle CPU Patching Metric



INTEGRIGY

Database Upgrades and CPU Patches

Database Version Upgrade Patch	Latest CPU Patch Included In Upgrade Patch
9.2.0.8	July 2006
10.1.0.5	October 2005
10.2.0.3	October 2006
10.2.0.4	April 2008
11.1.0.6	October 2007
11.1.0.7	January 2009
11.2.0.1	January 2010

Default Oracle Password Statistics

Database Account	Default Password	Exists in Database %	Default Password %
SYS	CHANGE_ON_INSTALL	100%	3%
SYSTEM	MANAGER	100%	4%
DBSNMP	**DBSNMP**	**99%**	**52%**
OUTLN	**OUTLN**	**98%**	**43%**
MDSYS	MDSYS	77%	18%
ORDPLUGINS	ORDPLUGINS	77%	16%
ORDSYS	ORDSYS	77%	16%
XDB	CHANGE_ON_INSTALL	75%	15%
DIP	DIP	63%	19%
WMSYS	WMSYS	63%	12%
CTXSYS	**CTXSYS**	**54%**	**32%**

* Sample of 120 production databases

INTEGRIGY

Oracle Database Passwords

Oracle Password algorithm is published on the Internet

- Algorithm uses two cycles of DES encryption with the username to produce a one-way hash of the password
- Oracle 11g – hash changed to SHA-1 – old DES hash also stored

Hash is unique to the username, but common across all versions and platforms of the Oracle database

- SYSTEM/MANAGER is always D4DF7931AB130E37 in every database in the world
- Oracle databases often cloned to test and development

Database installed with 8 to 20 default database accounts

- All have default passwords
- Many default password lists published on the Internet

Brute Forcing Database Passwords

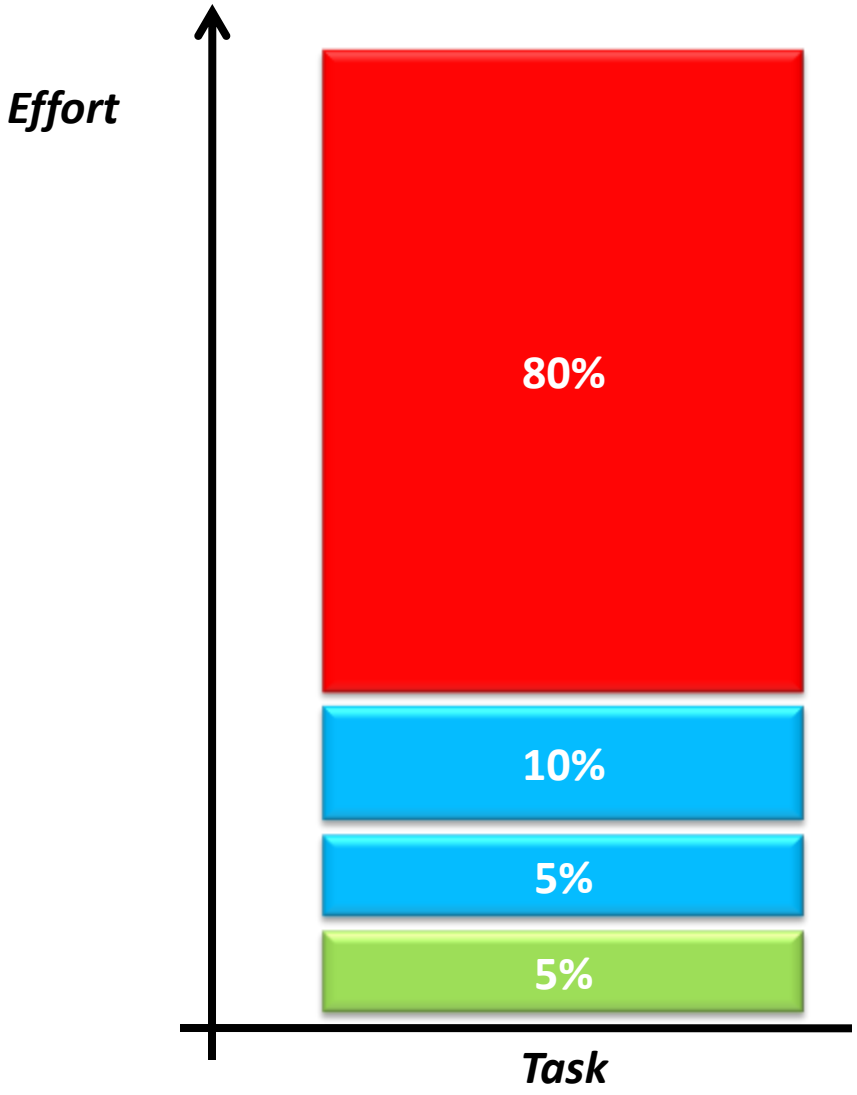
A number of efficient password brute forcing programs exist for Oracle

- Speed is at least 1 million passwords per second for desktop/laptop
- Speed is around 100 million passwords per second for specialized hardware (FGPA/GPU)
- Only the username and hash are required
- Estimated time to brute force a password of x length –

Length	Permutations	Time (desktop)	Time (GPU)
1	26 (26)	0 seconds	0 seconds
2	1,040 (26 x 39)	0 seconds	0 seconds
3	40,586 (26 x 39 x 39)	0 seconds	0 seconds
4	1,582,880	1.5 seconds	0 seconds
5	61,732,346	2 minute	6 seconds
6	2,407,561,520	40 minutes	24 seconds
7	93,894,899,306	1 day	15 minutes
8	3,661,901,072,960	42 days	10 hours
9	142,814,141,845,466	1,600 days	16 days

INTEGRIGY

Enabling auditing is the easy part

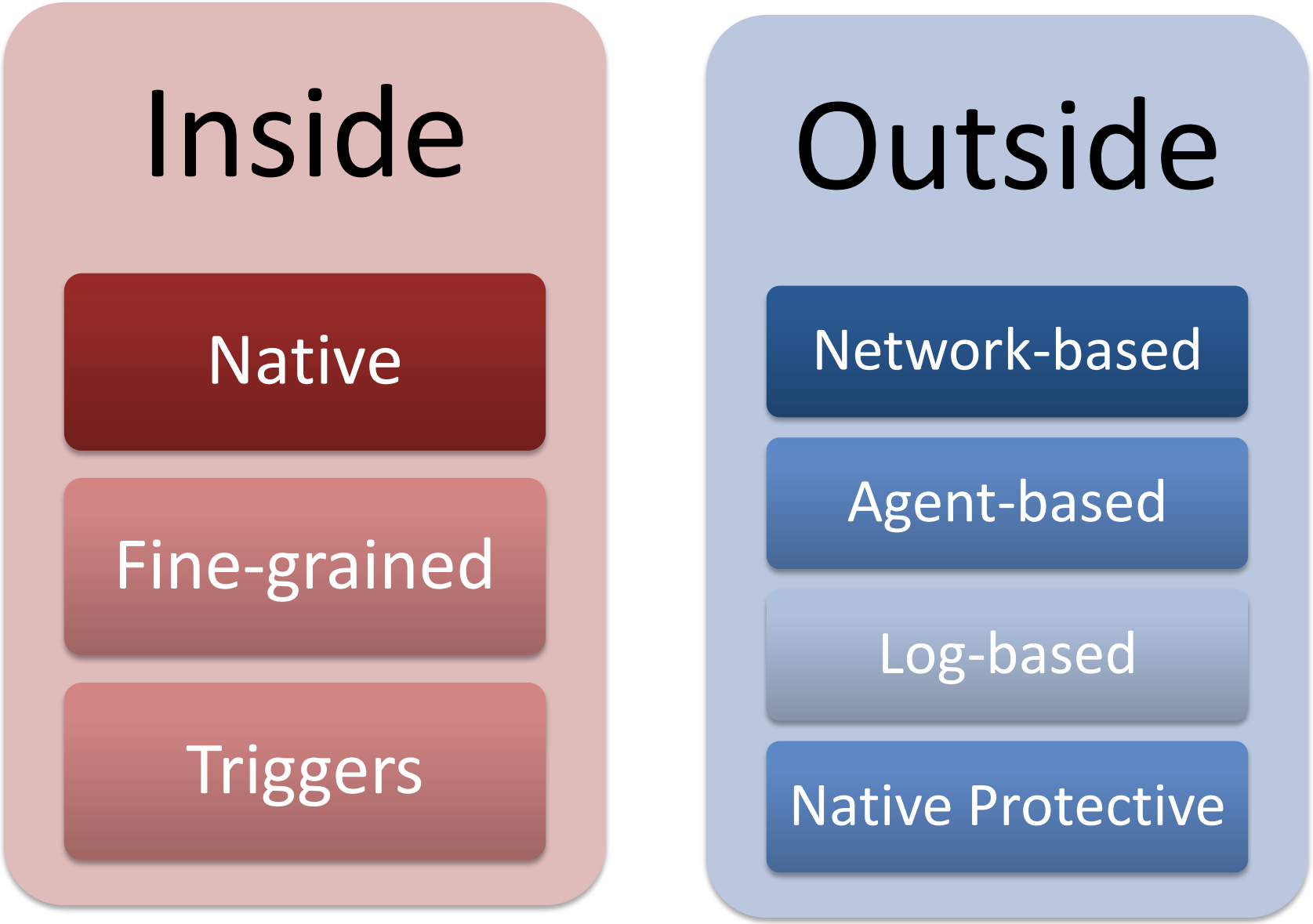


Monitoring,
Alerting,
Reporting,
Reviewing

Archiving & Purging

Designing

Enabling


Inside
Native
Fine-grained
Triggers
Outside
Network-based
Agent-based
Log-based
Native Protective

Native Audit Trail Destination Options

Oracle Version	AUDIT_TRAIL	SYSDBA	FGA
9.0.x	OS/DB	-	DB
9.2.x	OS/DB	OS	DB
10.1.x	OS/DB	OS	DB
10.2.x	OS/DB/XML/ SYSLOG	OS/XML	DB/XML
11.1.x	OS/DB/XML/ SYSLOG	OS/XML	DB/XML
11.2.x	OS/DB/XML/ SYSLOG	OS/XML	DB/XML

INTEGRIGY

Audit Trails Destinations and Values

Session Value	V$SESSION View	SYS_CONTEXT Function	SYS.AUD$ DBA_AUDIT_*	FGA_LOG$ AUDIT_TRAIL	Audit Vault
DB User Name	✓	✓	✓	✓	✓
Schema Name	✓	✓			
OS User Name	✓	✓	✓	✓	✓
Machine	✓	✓	✓	✓	✓
Terminal	✓	✓	✓		✓
Program	✓				✓
IP Address		✓	✓		✓
Client Process ID	✓				
Module	✓	✓			
Action	✓	✓			
Client Info	✓	✓			✓
Client ID	✓	✓	✓	✓	✓

Auditing Session Data

Database User Name	OS User Name	Schema Name
IP Address	Machine/ User host	Terminal
Program	Client Process ID	Module
Action	Client Info	Client ID

Auditing Session Data – Spoofable

Database User Name	~~OS User Name~~	~~Schema Name~~
IP Address	~~Machine/ User host~~	~~Terminal~~
~~Program~~	~~Client Process ID~~	~~Module~~
~~Action~~	~~Client Info~~	~~Client ID~~

INTEGRIGY

Key Security Risks

1 Exploitation of Oracle security vulnerabilities

- Apply security patches
- Limit direct connectivity to the database
- Prohibit use of generic accounts by individuals

2 Brute forcing of Oracle database passwords

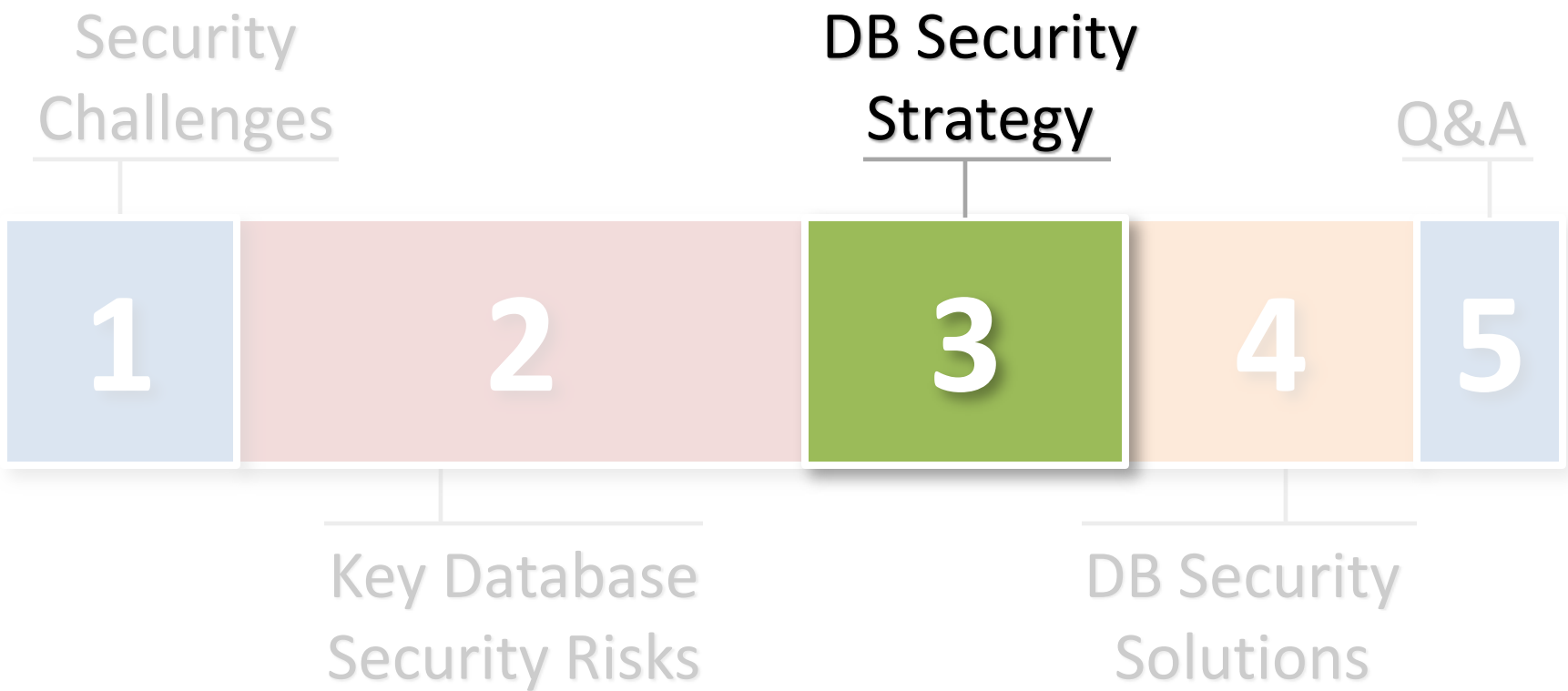
- Limit access to password hashes
- Change all database passwords in test and development

3 Lack of and trustworthiness of DB auditing

- Must enable database auditing
- Need to understand issues with audit data

INTEGRIGY

Agenda



INTEGRIGY

Traditional Database Security Approaches

- **Database security checklists**
  - Excellent baseline and starting point
  - Often in conflict with application configuration
  - Too many exceptions required to handle application limitations
  - Security decay requires constant or periodic assessments
- **Database security assessments**
  - Expensive and time consuming
  - Must be performed periodically to be effective
  - Database-centric or arbitrary standards often used
- **Database monitoring and auditing tools**
  - Expensive and time consuming
  - Difficult to implement with complex applications

Database Security Checklists

- **Center for Internet Security (CIS) Oracle Benchmark**
  - Oracle 8i, 9i, 10g, 11g checklists
- **Department of Defense DISA Oracle STIG**
  - Database Security Checklist and Guidance
  - Oracle 9i, 10g, 11g checklists
- **Oracle Security Whitepaper and Checklists**
  - Included with Oracle Security Guide manual
- **SANS S.C.O.R.E**
  - Last updated 2006
- **ISACA - Information Systems Audit and Control Association**
  - Security, Audit and Control Features Oracle Database, 3rd Edition
- **SANS Oracle Security Step by Step Book**
  - Last updated 2004

INTEGRIGY

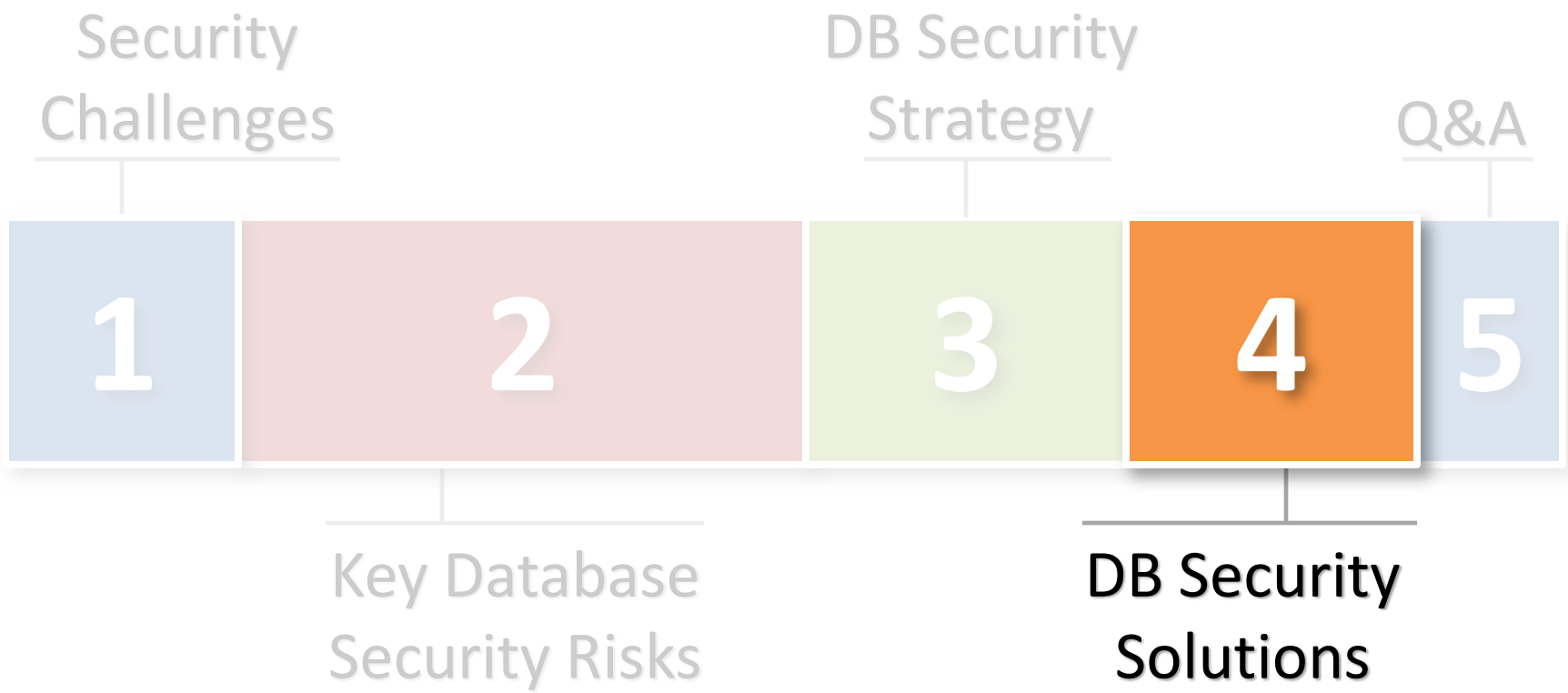
Defensive Security Strategies Themes

- **Reduce security vulnerability exposure**
  - Almost all database security vulnerabilities require a valid database session
  - Jump off or slow down the security patch hamster wheel
- **Classify databases and act appropriately**
  - The data determines the acceptable level of risk per database
- **Capturing audit data is the easy part**
  - Storing, protecting, and reporting is the hard part
  - Must transform audit data into actionable information
  - Auditing should enable information and action, not act as a black-hole

Defensive Security Strategies

- **“Virtual perimeters” for databases**
  - Limitation and segregation of access
  - Understand, channel, and manage ad-hoc access
  - Perimeters may be implemented at network, OS, database, and application layers
- **Configuration and vulnerability management**
  - Standardize configuration and operations where possible while minding application dependencies
  - Implement configurations that reduce security risk
  - Create consistency whenever possible
  - Mitigating controls when exceptions due to application limitations
  - Use existing management tools to validate and enforce configurations – continuously
- **Intelligent and business-focused auditing and monitoring**
  - Use auditing to enhance understanding of database operations
  - Intelligently capture, store, and disseminate information
  - Avoid auditing performance pitfalls

Agenda



INTEGRIGY

Database Security Solutions

- **A database security program is the solution**
  - Starts with a database security strategy
  - Effective and monitored policies and procedures are critical
  - Standardized configurations through a documented database configuration and security standard
  - Implement products to solve specific problems

Database Security Program

Access and Authorization

Auditing, Logging, and Monitoring

Security Patching

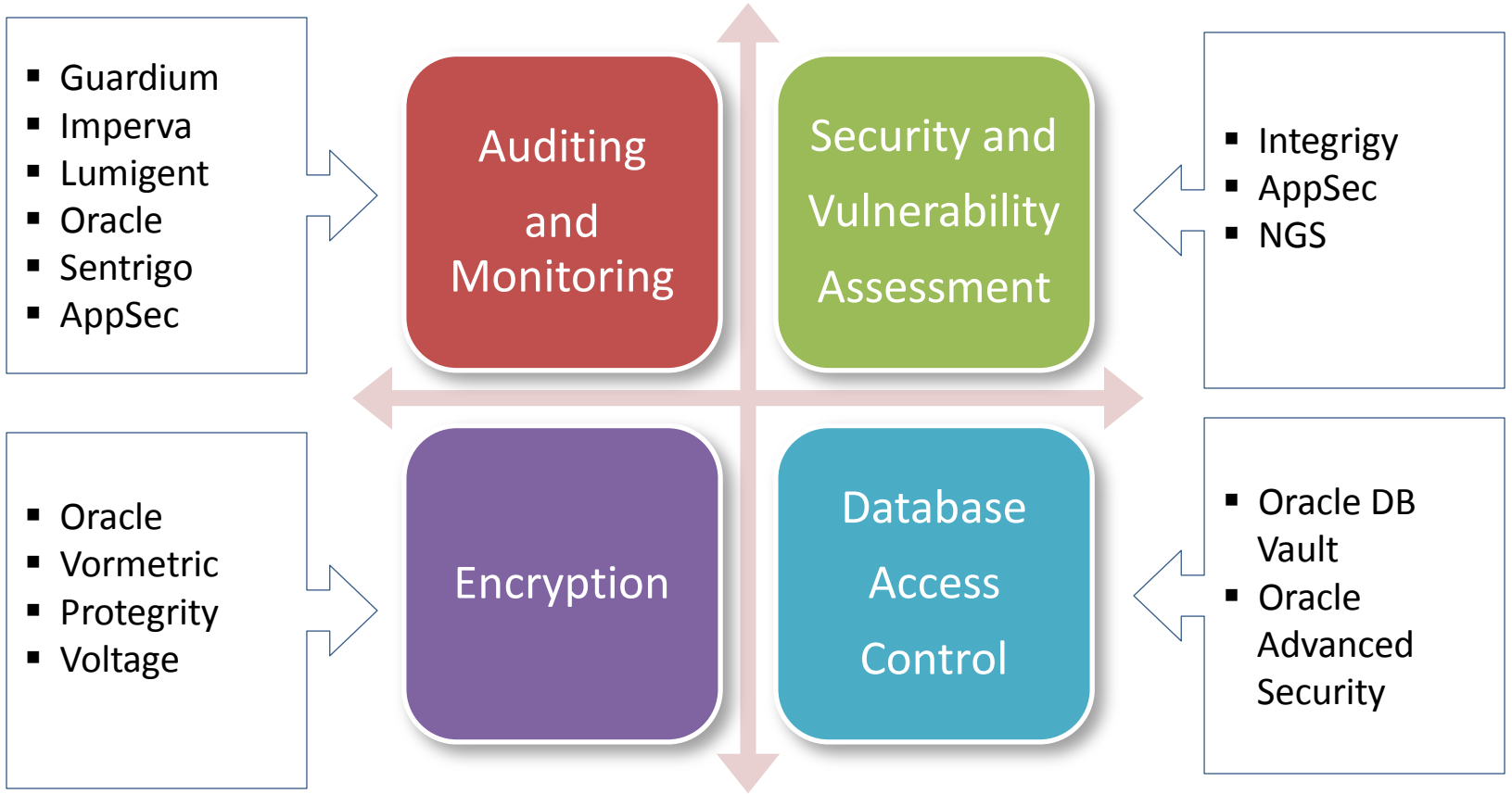
Configuration Standards

Change Management

Encryption

INTEGRIGY

Database Security Solution Products



** Not all vendors listed

INTEGRIGY

Third Party Auditing Solutions

- **Define your STRATEGY first**
  - Database security and auditing strategy is critical to successful implementation
  - Define responsibilities for DB security and auditing – difficult in most organizations
  - The strategy will drive the requirements

- **Goal is a complete auditing strategy**
  - No one tool or auditing technology is sufficient

INTEGRIGY

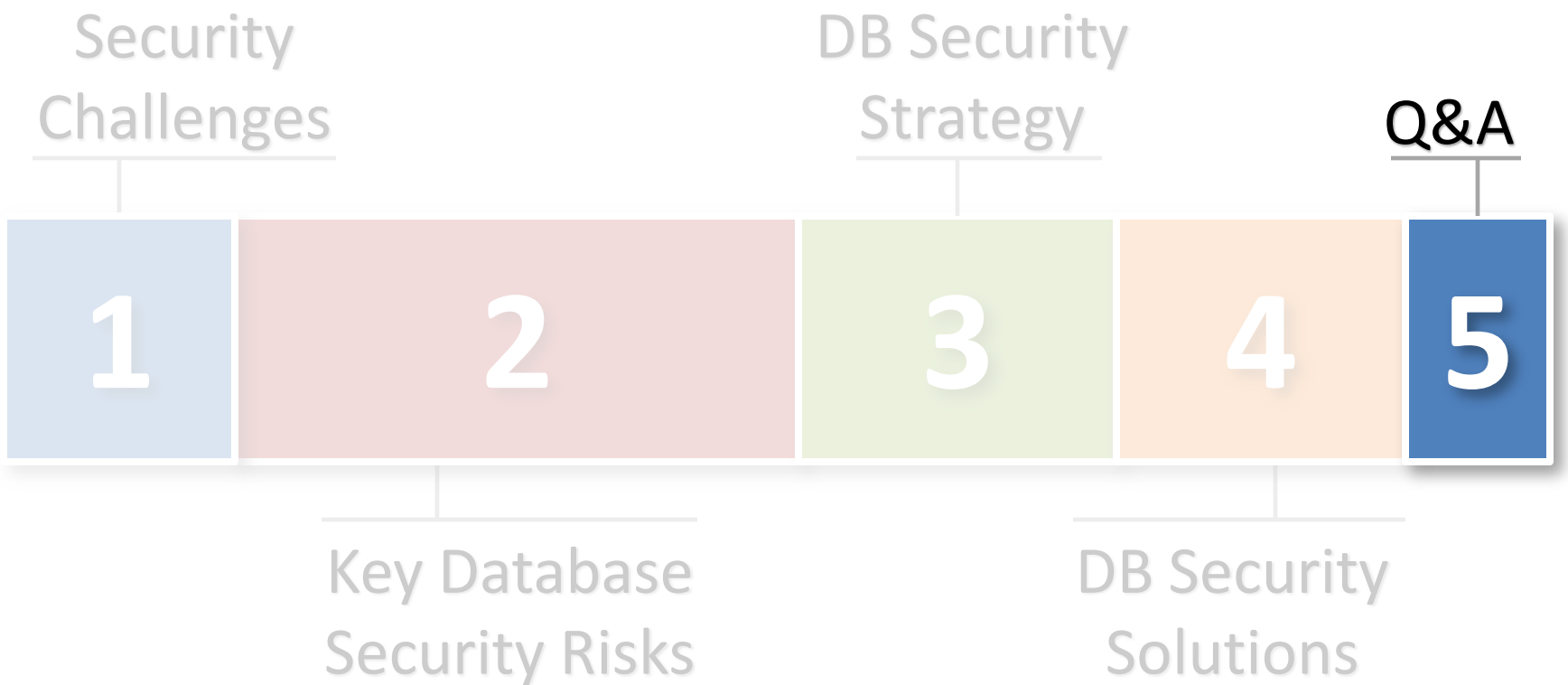
Third Party Auditing Solutions

- **There are fundamental differences among the vendors**
  - **Database activity capture vs. intrusion detection**
  - Data Capture Techniques = network, agent, log, native
  - Architecture = appliance vs. software
  - Bells and whistles = connection pooling, blocking, assessment, etc.

Application Security *AppRadar*	**Embarcadero** *DSAuditor*	**Guardium** *SQLGuard*
Imperva *DB Monitoring*	**Fortinet*** *IPLocks*	**Lumignet** *Audit DB*
Nitro Security *NitroGuard DBM*	**Oracle** *Oracle Database Firewall*	**Sentrigo** *Hedgehog*
Symantec *Database Security*	**Tizor*** *Mantra*	**Oracle** *Audit Vault*

INTEGRIGY

Agenda



INTEGRIGY

Integrigy Contact Information

Stephen Kost
Chief Technology Officer
Integrigy Corporation

e-mail: info@integrigy.com
blog: integrigy.com/oracle-security-blog

For information on -

- Oracle Database Security
- Oracle E-Business Suite Security
- Oracle Critical Patch Updates
- Oracle Security Blog

www.integrigy.com

INTEGRIGY