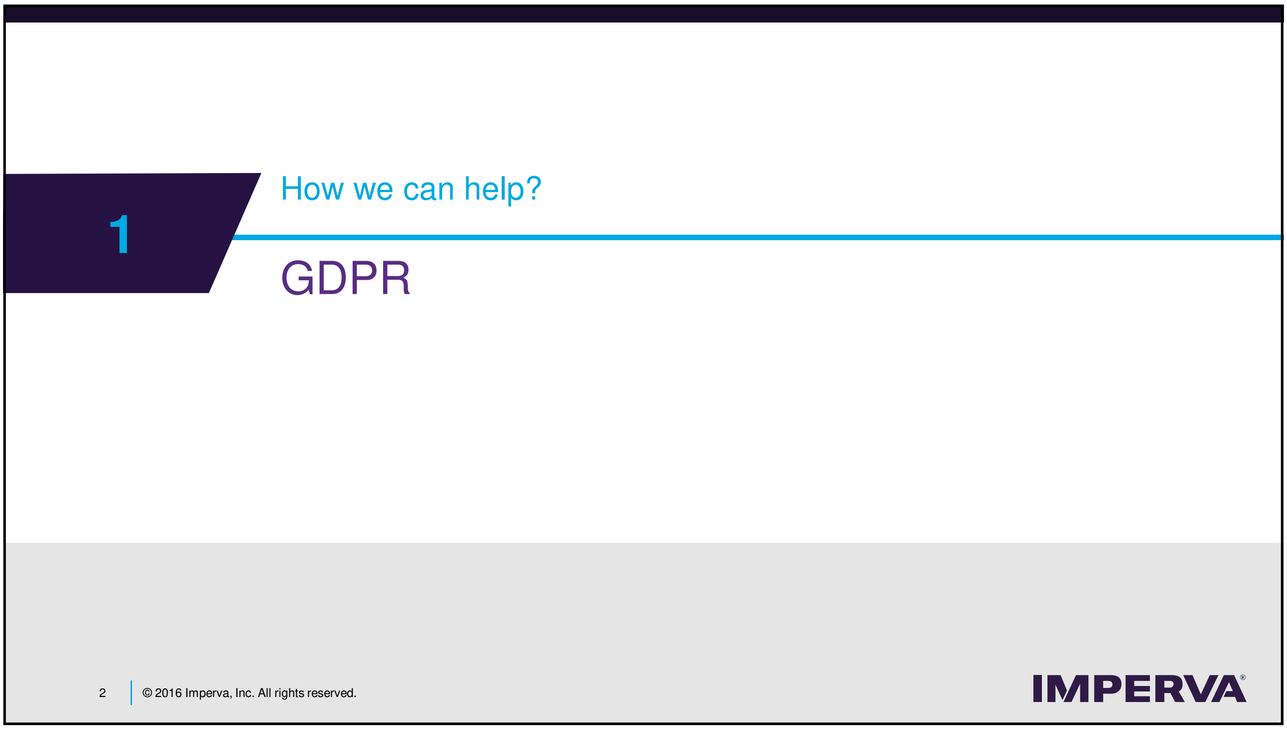
Database Activity Monitoring

Darren Harter, SE Manager, North EMEA

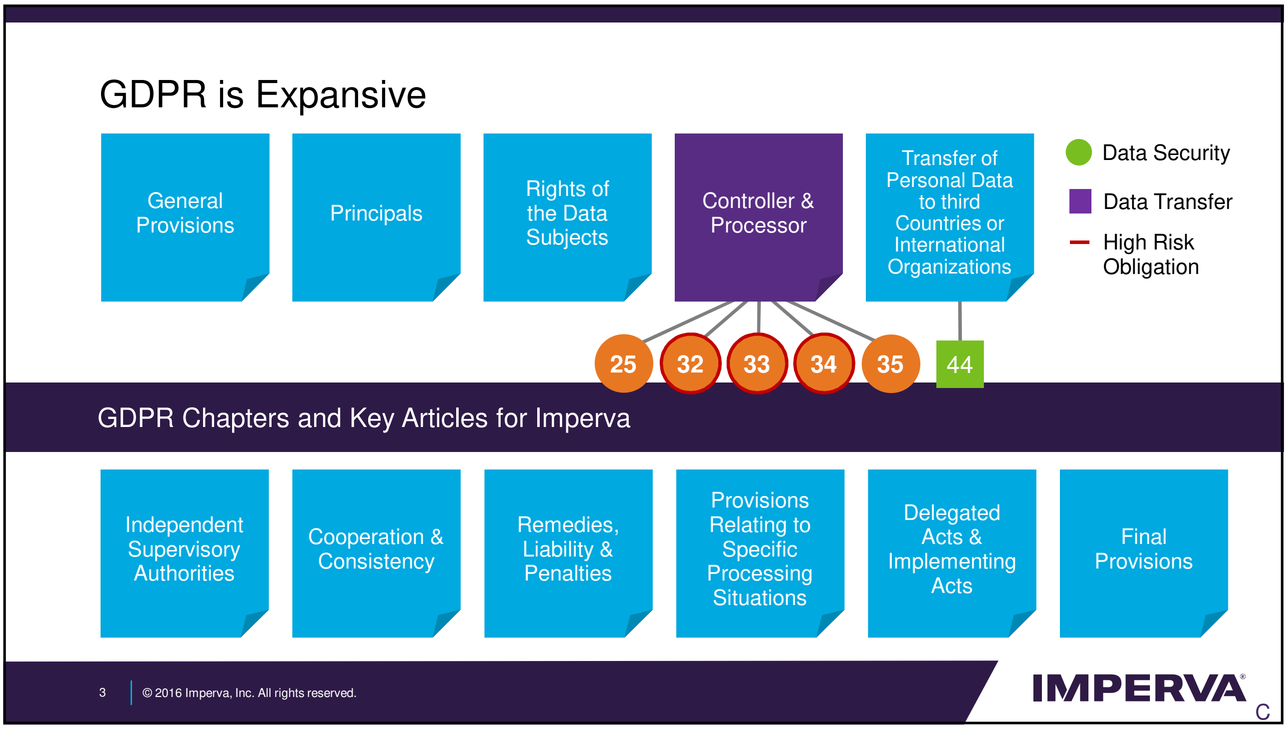


1

How we can help?

GDPR

2 |



GDPR is Expansive

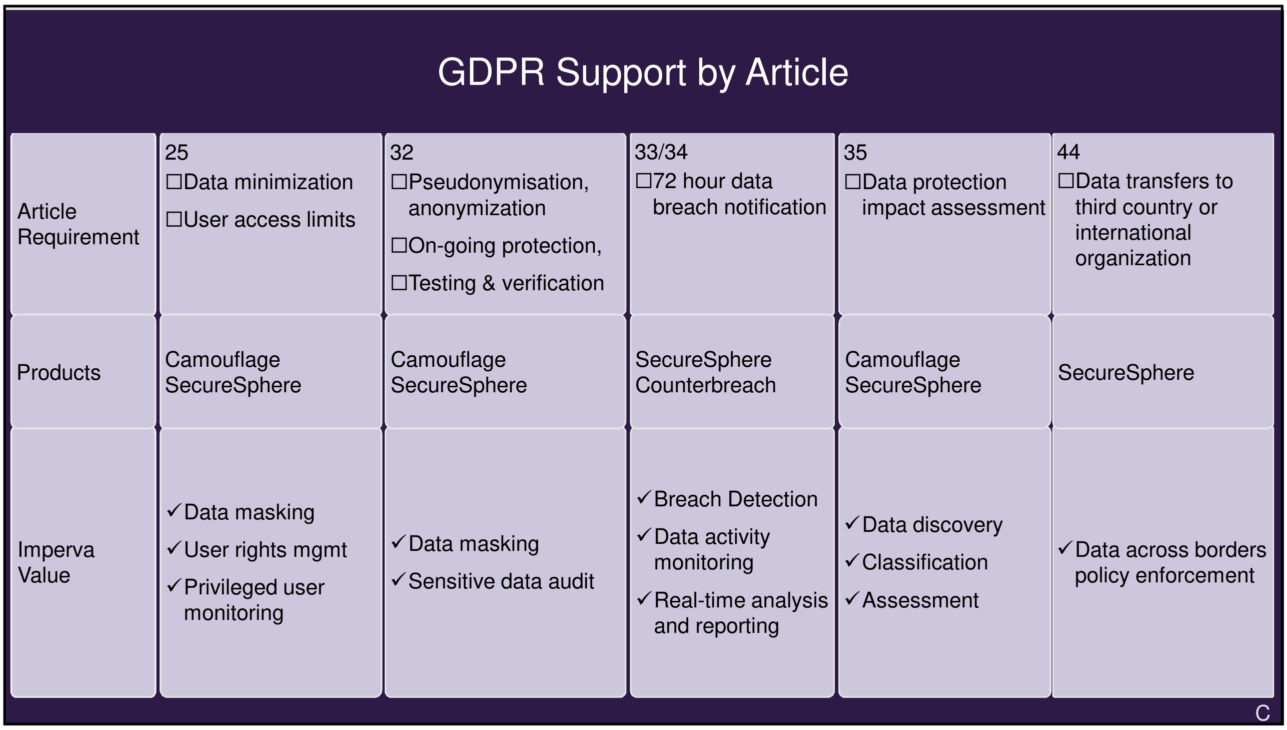
General Provisions
Principals
Rights of the Data Subjects
Controller & Processor
Transfer of Personal Data to third Countries or International Organizations
● Data Security
■ Data Transfer
— High Risk Obligation
25
32
33
34
35
44
Independent Supervisory Authorities
Cooperation & Consistency
Remedies, Liability & Penalties
Provisions Relating to Specific Processing Situations
Delegated Acts & Implementing Acts
Final Provisions

GDPR Chapters and Key Articles for Imperva

3 |

IMPERVA

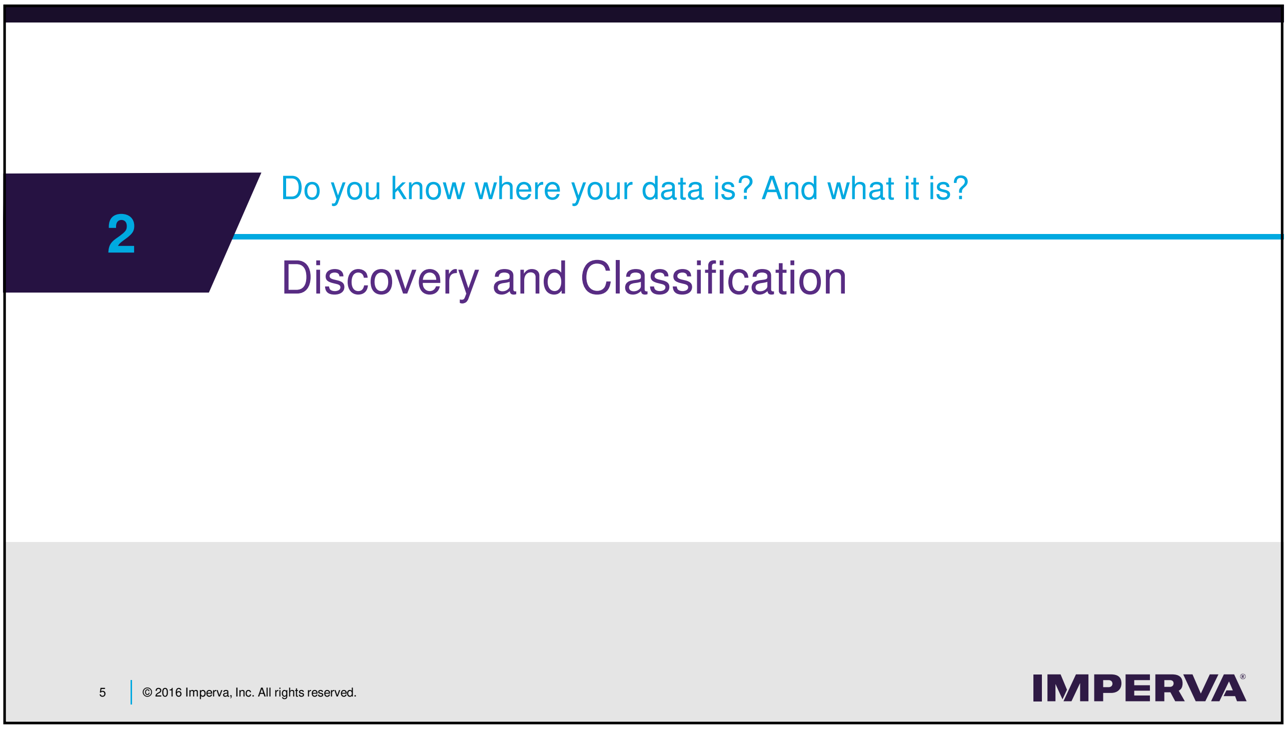
C



GDPR Support by Article

Article Requirement	25 ☐Data minimization ☐User access limits	32 ☐Pseudonymisation, anonymization ☐On-going protection, ☐Testing & verification	33/34 ☐72 hour data breach notification	35 ☐Data protection impact assessment	44 ☐Data transfers to third country or international organization
Products	Camouflage SecureSphere	Camouflage SecureSphere	SecureSphere Counterbreach	Camouflage SecureSphere	SecureSphere
Imperva Value	✓Data masking ✓User rights mgmt ✓Privileged user monitoring	✓Data masking ✓Sensitive data audit	✓Breach Detection ✓Data activity monitoring ✓Real-time analysis and reporting	✓Data discovery ✓Classification ✓Assessment	✓Data across borders policy enforcement

C



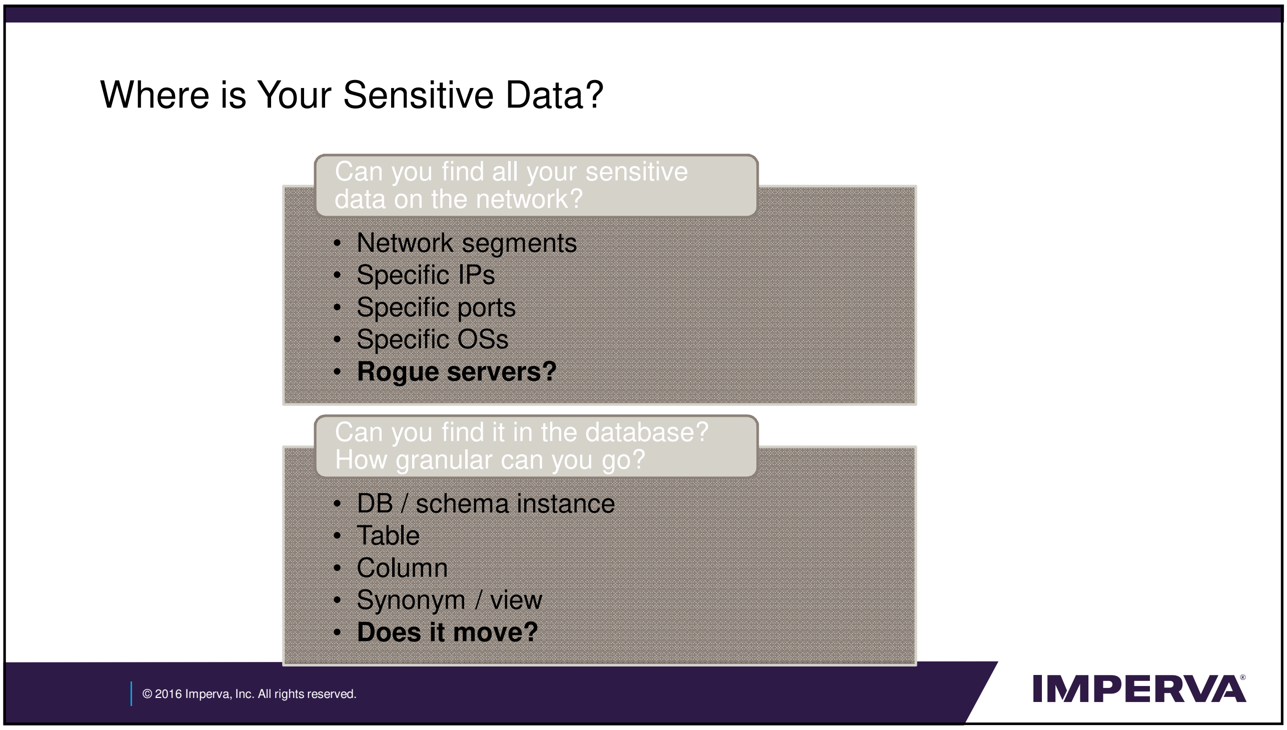
2

Do you know where your data is? And what it is?

Discovery and Classification

5

IMPERVA



Where is Your Sensitive Data?

Can you find all your sensitive data on the network?

- Network segments
- Specific IPs
- Specific ports
- Specific OSs
- **Rogue servers?**

Can you find it in the database? How granular can you go?

- DB / schema instance
- Table
- Column
- Synonym / view
- **Does it move?**

IMPERVA

How Do You Know Where Data Is?

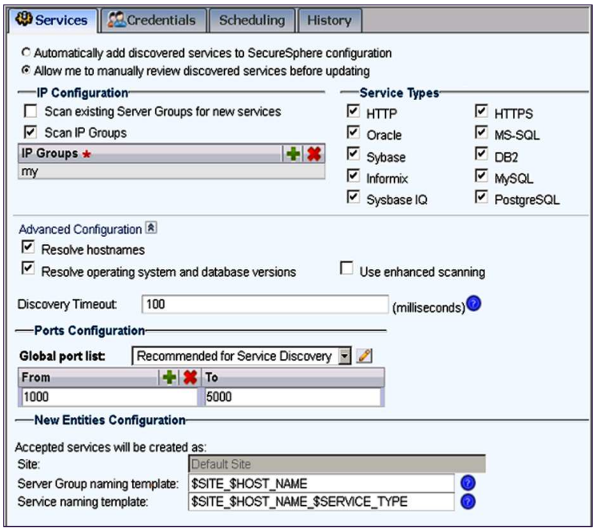
How do you know today?

- Direct knowledge
- Trust business owner
- Trust DBA
- Scan with 3rd party tool
- Team Discovery project

How do you know when it changes?

- Direct knowledge
- Email / phone call?
- Manual 3rd party tool?
- Automatic 3rd party tool?
- Track external change controls?
- You don't…?

Server / Database Discovery Scan



○ Automatically add discovered services to SecureSphere configuration
● Allow me to manually review discovered services before updating

IP Configuration

□ Scan existing Server Groups for new services
☑ Scan IP Groups

IP Groups *
my

Service Types

☑ HTTP ☑ HTTPS
☑ Oracle ☑ MS-SQL
☑ Sybase ☑ DB2
☑ Informix ☑ MySQL
☑ Sysbase IQ ☑ PostgreSQL

Advanced Configuration

☑ Resolve hostnames
☑ Resolve operating system and database versions
□ Use enhanced scanning

Discovery Timeout: 100 (milliseconds)

Ports Configuration

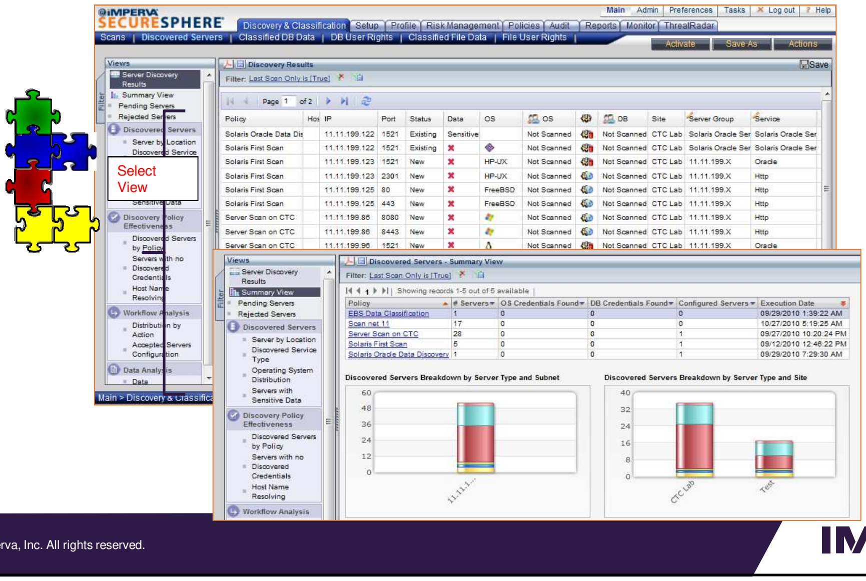
Global port list: Recommended for Service Discovery

From	To
1000	5000

New Entities Configuration

Accepted services will be created as:
Site: Default Site
Server Group naming template: $SITE_$HOST_NAME
Service naming template: $SITE_$HOST_NAME_$SERVICE_TYPE

Discovered Server Results



Select View

Discovery Results

Filter: Last Scan Only is [True]

Page 1 of 2

Policy	Hos	IP	Port	Status	Data	OS	OS		DB	Site	Server Group	Service
Solaris Oracle Data Dis		11.11.199.122	1521	Existing	Sensitive		Not Scanned		Not Scanned	CTC Lab	Solaris Oracle Ser	Solaris Oracle Ser
Solaris First Scan		11.11.199.122	1521	Existing	✗		Not Scanned		Not Scanned	CTC Lab	Solaris Oracle Ser	Solaris Oracle Ser
Solaris First Scan		11.11.199.123	1521	New	✗	HP-UX	Not Scanned		Not Scanned	CTC Lab	11.11.199.X	Oracle
Solaris First Scan		11.11.199.123	2301	New	✗	HP-UX	Not Scanned		Not Scanned	CTC Lab	11.11.199.X	Http
Solaris First Scan		11.11.199.125	80	New	✗	FreeBSD	Not Scanned		Not Scanned	CTC Lab	11.11.199.X	Http
Solaris First Scan		11.11.199.125	443	New	✗	FreeBSD	Not Scanned		Not Scanned	CTC Lab	11.11.199.X	Http
Server Scan on CTC		11.11.199.86	8080	New	✗		Not Scanned		Not Scanned	CTC Lab	11.11.199.X	Http
Server Scan on CTC		11.11.199.86	8443	New	✗		Not Scanned		Not Scanned	CTC Lab	11.11.199.X	Http
Server Scan on CTC		11.11.199.96	1521	New	✗		Not Scanned		Not Scanned	CTC Lab	11.11.199.X	Oracle

Discovered Servers - Summary View

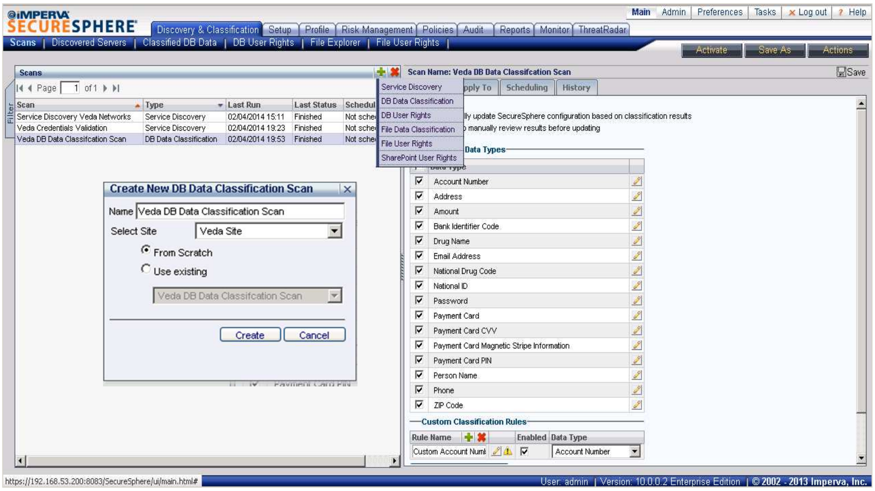
Filter: Last Scan Only is [True]

Showing records 1-5 out of 5 available

Policy	# Servers	OS Credentials Found	DB Credentials Found	Configured Servers	Execution Date
EBS Data Classification	1	0	0	0	09/29/2010 1:39:22 AM
Scan net 11	17	0	0	0	10/27/2010 5:19:25 AM
Server Scan on CTC	28	0	0	1	09/27/2010 10:20:24 PM
Solaris First Scan	5	0	0	1	09/12/2010 12:46:22 PM
Solaris Oracle Data Discovery	1	0	0	1	09/29/2010 7:29:30 AM

@IMPERVA SECURESPHERE
Main | Admin | Preferences | Tasks | Log out | Help
Discovery & Classification | Setup | Profile | Risk Management | Policies | Audit | Reports | Monitor | ThreatRadar
Scans | Discovered Servers | Classified DB Data | DB User Rights | Classified File Data | File User Rights
Activate | Save As | Actions
Save
Views
Server Discovery Results
Summary View
Pending Servers
Rejected Servers
Discovered Servers
Server by Location
Discovered Service Type
Operating System Distribution
Servers with Sensitive Data
Discovery Policy Effectiveness
Discovered Servers by Policy
Servers with no Discovered Credentials
Host Name Resolving
Workflow Analysis
Distribution by Action
Accepted Servers Configuration
Data Analysis
Data
Main > Discovery & Classifica
Filter
Discovered Servers Breakdown by Server Type and Subnet
60
48
36
24
12
0
11.11.1...
Discovered Servers Breakdown by Server Type and Site
40
32
24
16
8
0
CTC Lab
Test

DB Data Classification Scan



Scans

Page 1 of 1

Scan	Type	Last Run	Last Status	Schedul
Service Discovery Veda Networks	Service Discovery	02/04/2014 15:11	Finished	Not sche
Veda Credentials Validation	Service Discovery	02/04/2014 19:23	Finished	Not sche
Veda DB Data Classifcation Scan	DB Data Classification	02/04/2014 19:53	Finished	Not sche

Create New DB Data Classification Scan

Name: Veda DB Data Classification Scan

Select Site: Veda Site

● From Scratch

○ Use existing

Veda DB Data Classifcation Scan

Create | Cancel

Scan Name: Veda DB Data Classifcation Scan

lly update SecureSphere configuration based on classification results

p manually review results before updating

Data Types

	Data Type
☑	Account Number
☑	Address
☑	Amount
☑	Bank Identifier Code
☑	Drug Name
☑	Email Address
☑	National Drug Code
☑	National ID
☑	Password
☑	Payment Card
☑	Payment Card CVV
☑	Payment Card Magnetic Stripe Information
☑	Payment Card PIN
☑	Person Name
☑	Phone
☑	ZIP Code

Custom Classification Rules

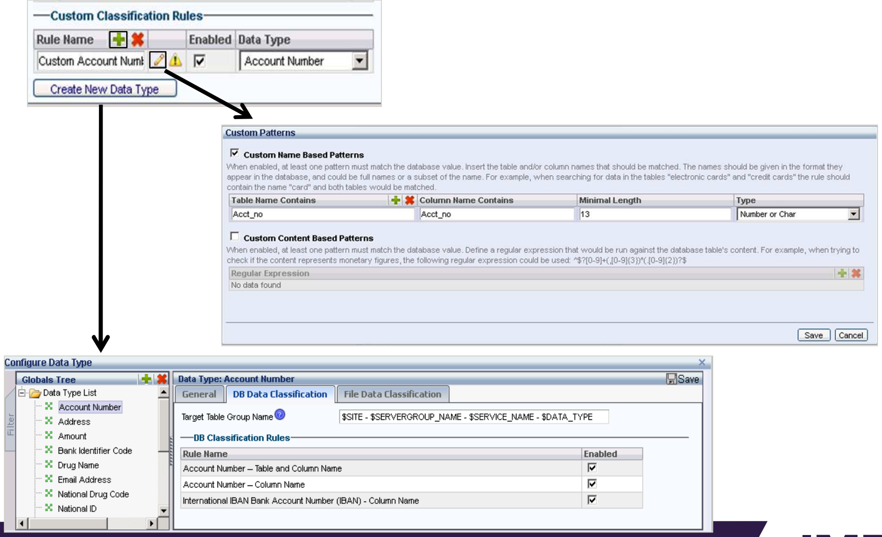
Rule Name	Enabled	Data Type
Custom Account Numl	☑	Account Number

https://192.168.53.200:8083/SecureSphere/ui/main.html#

User: admin | Version: 10.0.0.2 Enterprise Edition | © 2002 - 2013 Imperva, Inc.

@IMPERVA SECURESPHERE
Main | Admin | Preferences | Tasks | Log out | Help
Discovery & Classification | Setup | Profile | Risk Management | Policies | Audit | Reports | Monitor | ThreatRadar
Scans | Discovered Servers | Classified DB Data | DB User Rights | File Explorer | File User Rights
Activate | Save As | Actions
Service Discovery
DB Data Classification
DB User Rights
File Data Classification
File User Rights
SharePoint User Rights
pply To | Scheduling | History
Save
Filter

Configuring Custom Classification Rules



Custom Classification Rules

Rule Name	Enabled	Data Type
Custom Account Numb	☑	Account Number

Create New Data Type

Custom Patterns

☑ **Custom Name Based Patterns**

When enabled, at least one pattern must match the database value. Insert the table and/or column names that should be matched. The names should be given in the format they appear in the database, and could be full names or a subset of the name. For example, when searching for data in the tables "electronic cards" and "credit cards" the rule should contain the name "card" and both tables would be matched.

Table Name Contains	Column Name Contains	Minimal Length	Type
Acct_no	Acct_no	13	Number or Char

□ **Custom Content Based Patterns**

When enabled, at least one pattern must match the database value. Define a regular expression that would be run against the database table's content. For example, when trying to check if the content represents monetary figures, the following regular expression could be used: ^$?[0-9]+(,[0-9]{3})*(.[0-9]{2})?$

Regular Expression
No data found

Save Cancel

Configure Data Type

Globals Tree

- Data Type List
  - Account Number
  - Address
  - Amount
  - Bank Identifier Code
  - Drug Name
  - Email Address
  - National Drug Code
  - National ID

Data Type: Account Number

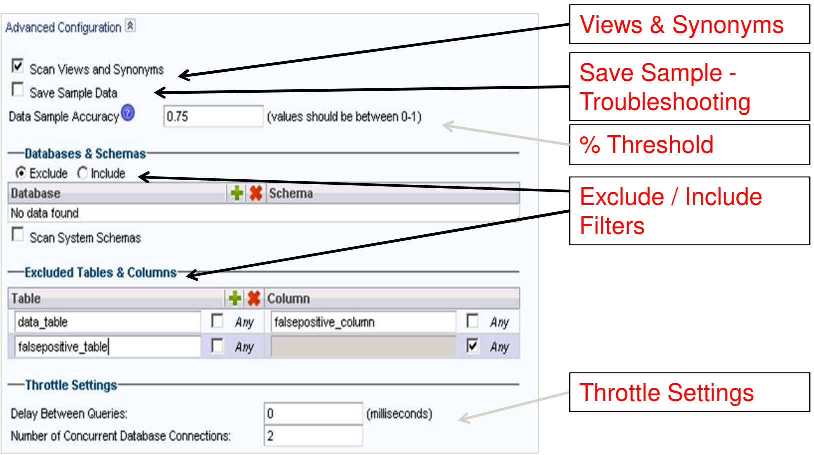
General | DB Data Classification | File Data Classification

Target Table Group Name: $SITE - $SERVERGROUP_NAME - $SERVICE_NAME - $DATA_TYPE

DB Classification Rules

Rule Name	Enabled
Account Number – Table and Column Name	☑
Account Number – Column Name	☑
International IBAN Bank Account Number (IBAN) - Column Name	☑

DB Data Classification Advanced Configuration



Advanced Configuration

☑ Scan Views and Synonyms

□ Save Sample Data

Data Sample Accuracy: 0.75 (values should be between 0-1)

Databases & Schemas

● Exclude ○ Include

Database	Schema
No data found	

□ Scan System Schemas

Excluded Tables & Columns

Table		Column	
data_table	□ Any	falsepositive_column	□ Any
falsepositive_table	□ Any		☑ Any

Throttle Settings

Delay Between Queries: 0 (milliseconds)

Number of Concurrent Database Connections: 2

Views & Synonyms

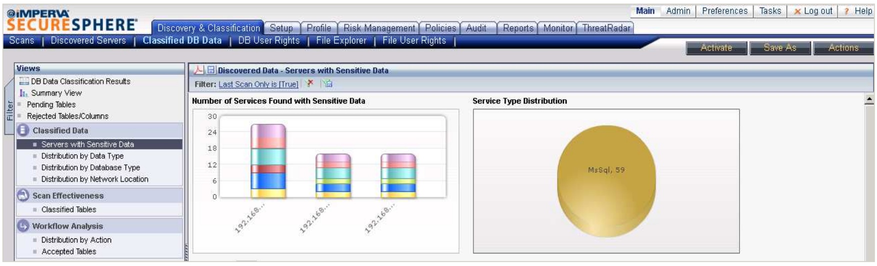
Save Sample - Troubleshooting

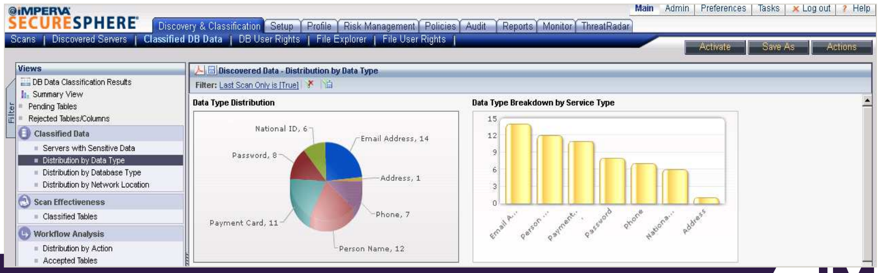
% Threshold

Exclude / Include Filters

Throttle Settings

Data Classification Results


IMPERVA SECURESPHERE
Main | Admin | Preferences | Tasks | Log out | Help
Discovery & Classification | Setup | Profile | Risk Management | Policies | Audit | Reports | Monitor | ThreatRadar
Scans | Discovered Servers | Classified DB Data | DB User Rights | File Explorer | File User Rights
Activate | Save As | Actions
Views
DB Data Classification Results
Summary View
Pending Tables
Rejected Tables/Columns
Classified Data
Servers with Sensitive Data
Distribution by Data Type
Distribution by Database Type
Distribution by Network Location
Scan Effectiveness
Classified Tables
Workflow Analysis
Distribution by Action
Accepted Tables
Filter
Discovered Data - Servers with Sensitive Data
Filter: Last Scan Only is [True]
Number of Services Found with Sensitive Data
30
24
18
12
6
0
192.168...
192.168...
192.168...
Service Type Distribution
MsSql, 59


IMPERVA SECURESPHERE
Main | Admin | Preferences | Tasks | Log out | Help
Discovery & Classification | Setup | Profile | Risk Management | Policies | Audit | Reports | Monitor | ThreatRadar
Scans | Discovered Servers | Classified DB Data | DB User Rights | File Explorer | File User Rights
Activate | Save As | Actions
Views
DB Data Classification Results
Summary View
Pending Tables
Rejected Tables/Columns
Classified Data
Servers with Sensitive Data
Distribution by Data Type
Distribution by Database Type
Distribution by Network Location
Scan Effectiveness
Classified Tables
Workflow Analysis
Distribution by Action
Accepted Tables
Filter
Discovered Data - Distribution by Data Type
Filter: Last Scan Only is [True]
Data Type Distribution
National ID, 6
Email Address, 14
Password, 8
Address, 1
Phone, 7
Payment Card, 11
Person Name, 12
Data Type Breakdown by Service Type
15
12
9
6
3
0
Email A...
Person ...
Payment...
Password
Phone
Nationa...
Address

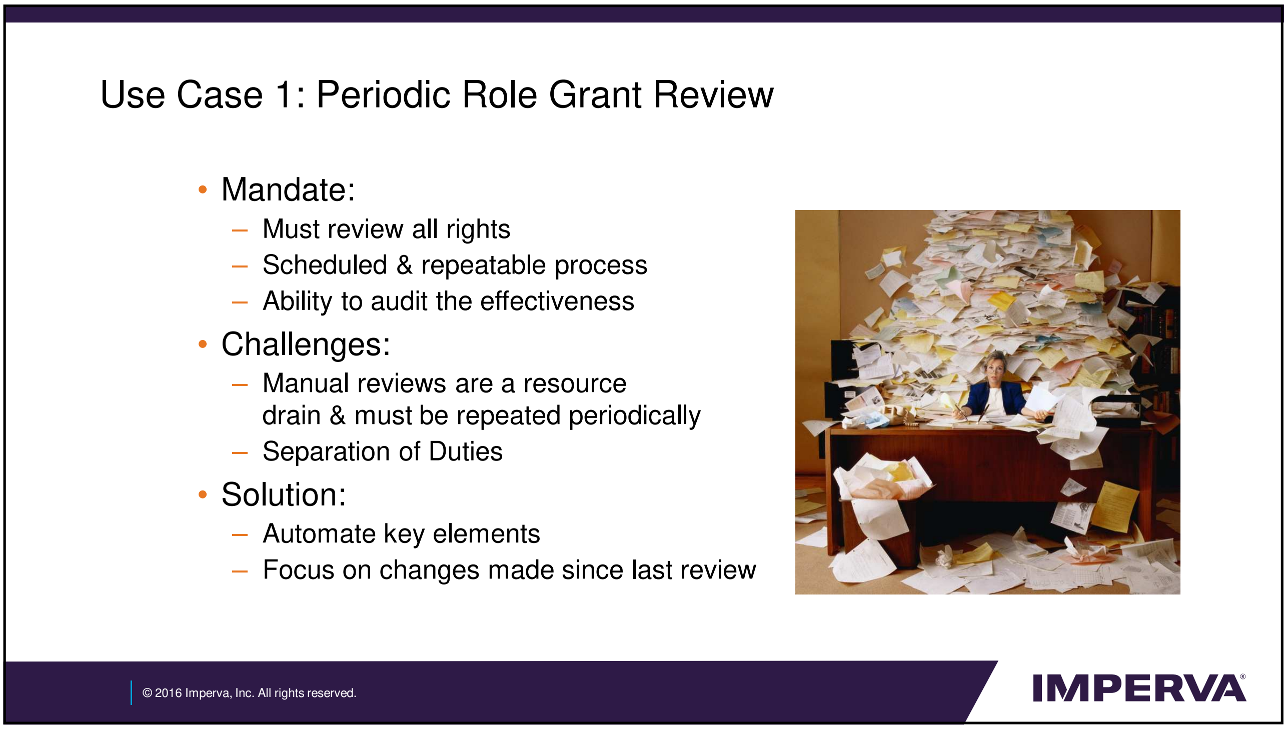
IMPERVA

6

Who has access to your data? And How?

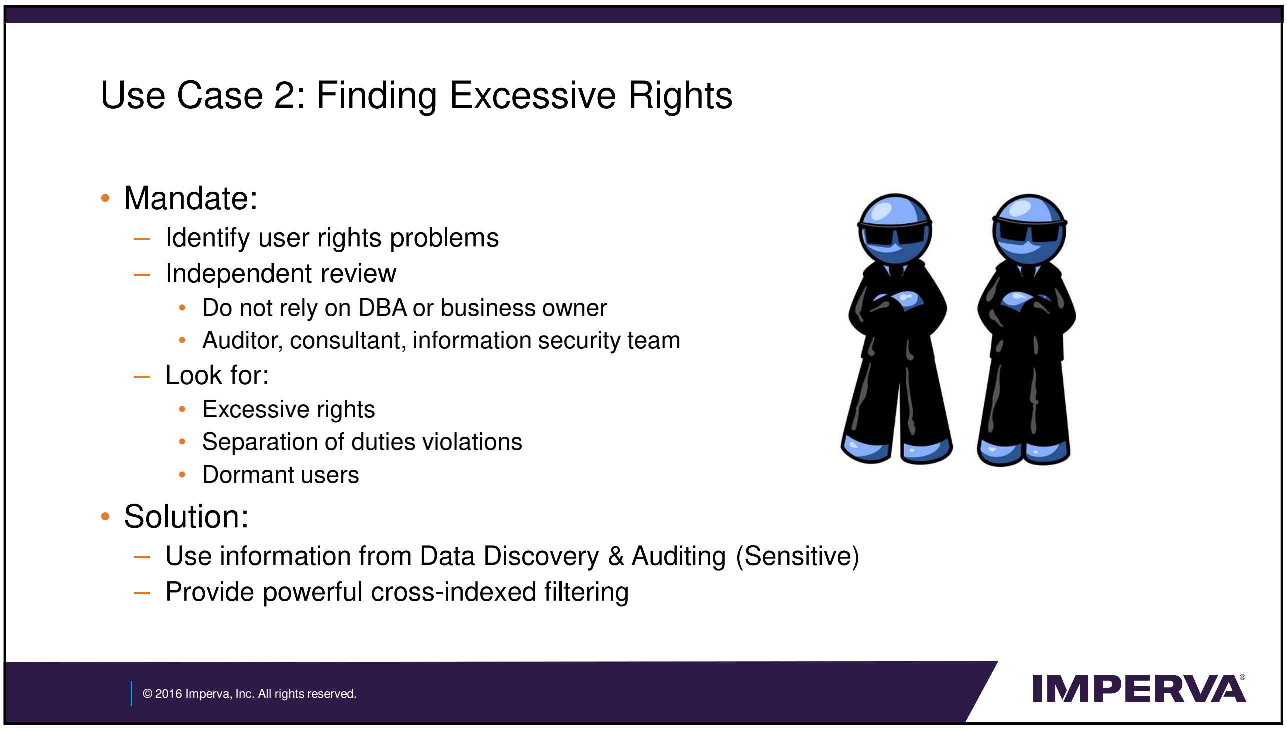
User Rights Management

IMPERVA



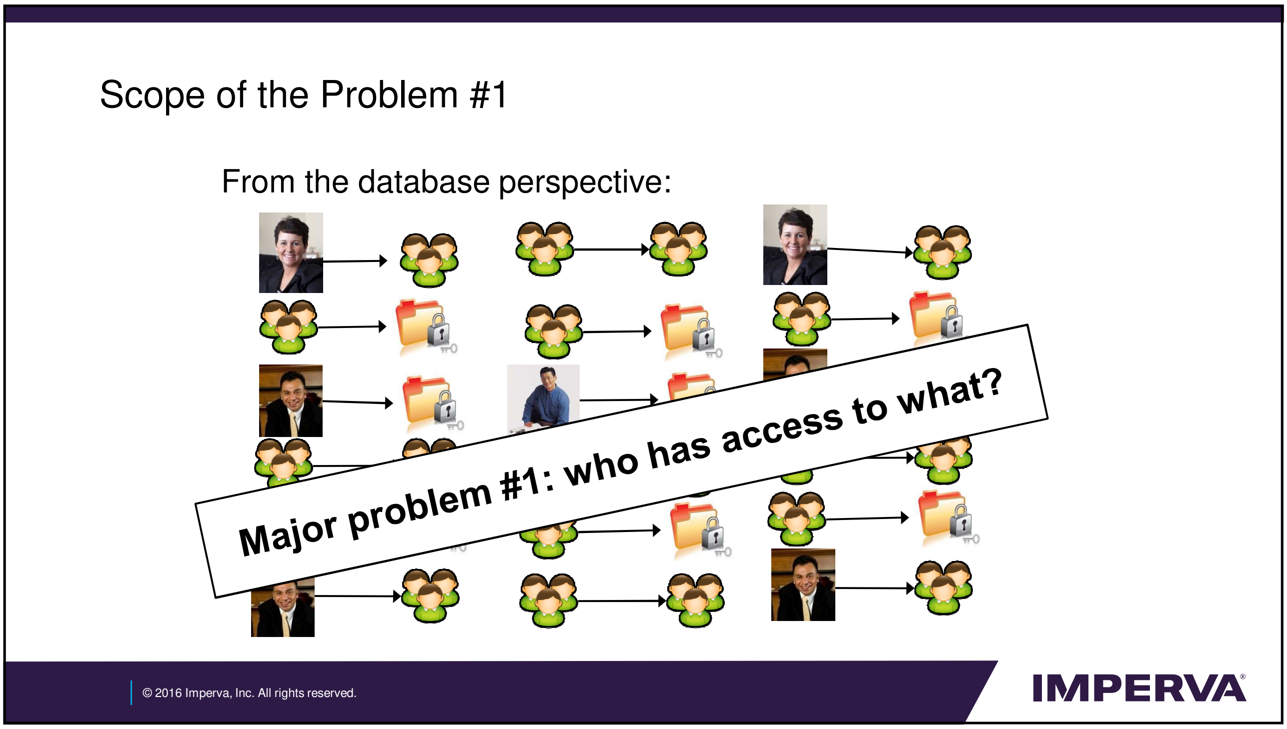
Use Case 1: Periodic Role Grant Review

- Mandate:
  - Must review all rights
  - Scheduled & repeatable process
  - Ability to audit the effectiveness
- Challenges:
  - Manual reviews are a resource drain & must be repeated periodically
  - Separation of Duties
- Solution:
  - Automate key elements
  - Focus on changes made since last review



Use Case 2: Finding Excessive Rights

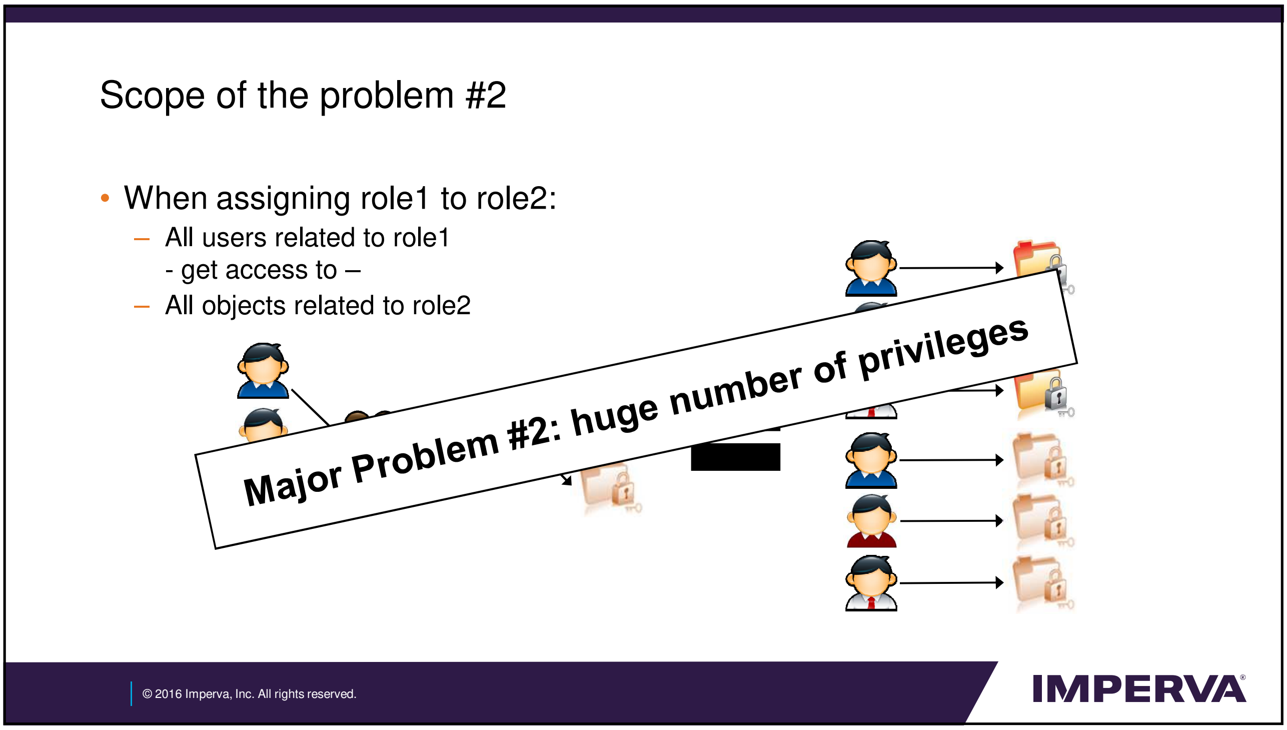
- Mandate:
  - Identify user rights problems
  - Independent review
    - Do not rely on DBA or business owner
    - Auditor, consultant, information security team
  - Look for:
    - Excessive rights
    - Separation of duties violations
    - Dormant users
- Solution:
  - Use information from Data Discovery & Auditing (Sensitive)
  - Provide powerful cross-indexed filtering



Scope of the Problem #1

From the database perspective:

Major problem #1: who has access to what?

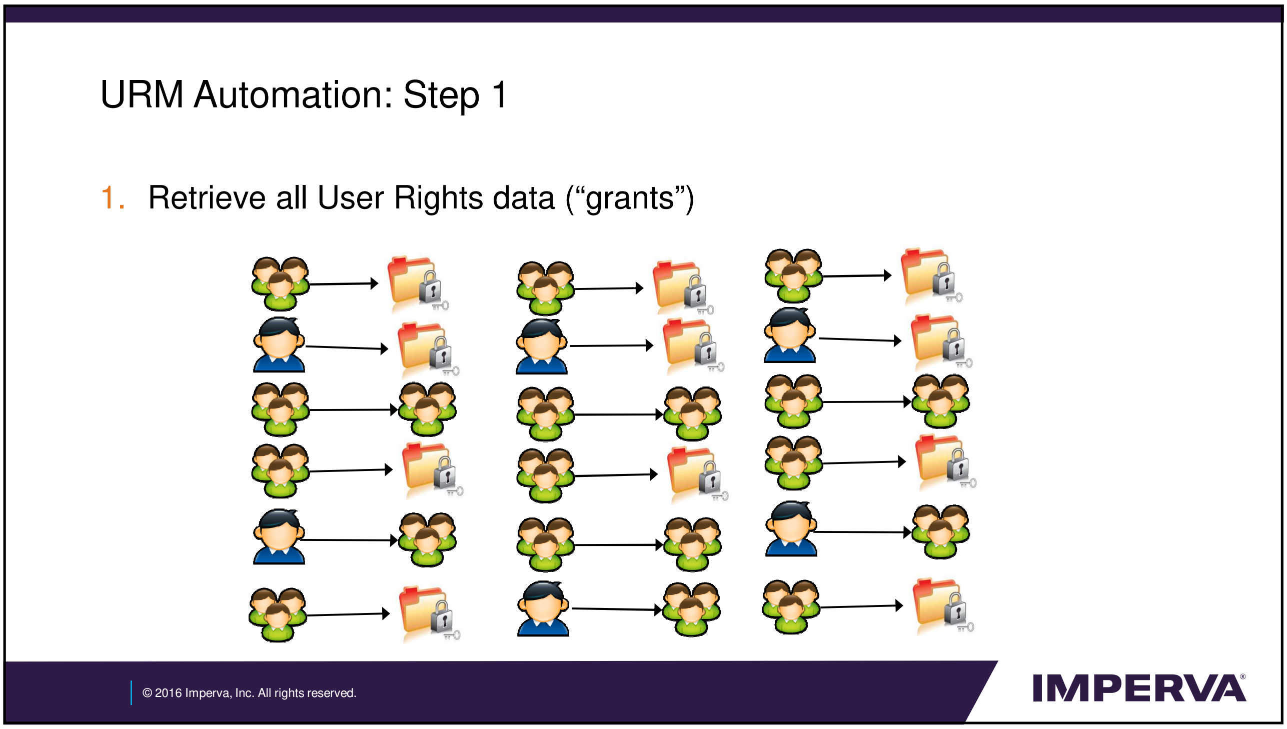


Scope of the problem #2

- When assigning role1 to role2:
  - All users related to role1
    - get access to –
  - All objects related to role2

Major Problem #2: huge number of privileges

[redacted]

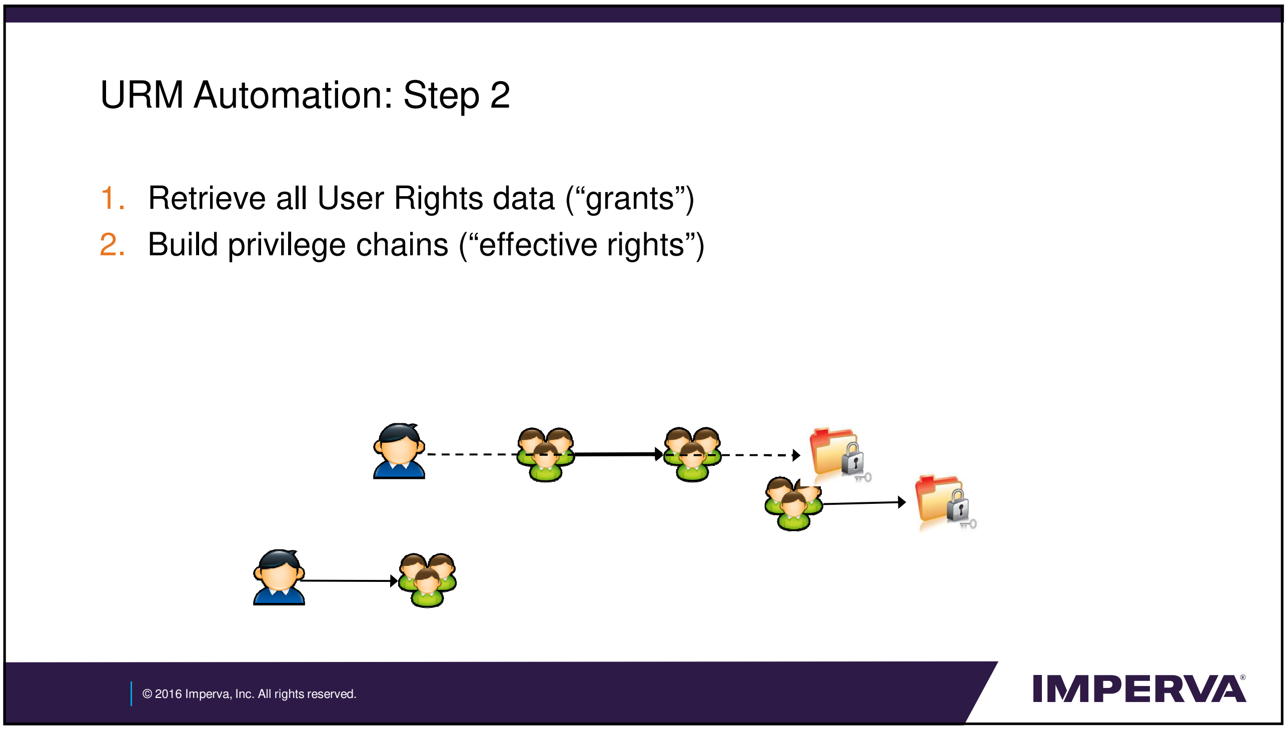


URM Automation: Step 1

1. Retrieve all User Rights data ("grants")

© 2016 Imperva, Inc. All rights reserved.

IMPERVA



URM Automation: Step 2

1. Retrieve all User Rights data ("grants")
2. Build privilege chains ("effective rights")

© 2016 Imperva, Inc. All rights reserved.

IMPERVA

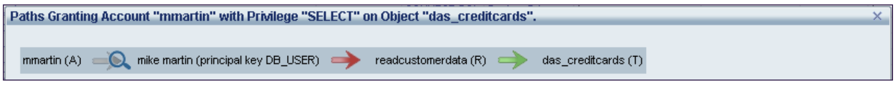
URM Automation: Step 3

1. Retrieve all User Rights data (“grants”)
2. Build privilege chains (“effective rights”)
3. Add enrichment information:
   1. Last login, last access, sensitive data types etc.

Last Access: 01/31/2014

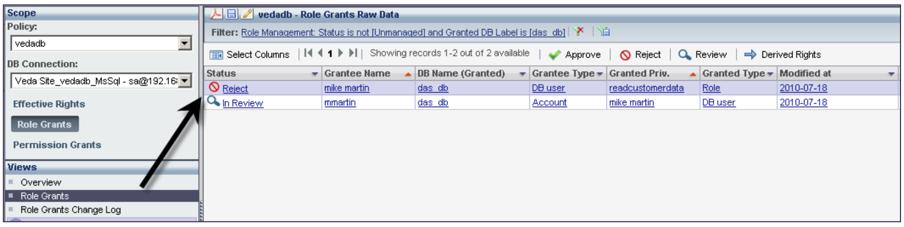
Last Login: 03/23/2014

Viewing Role Grants and Permission Grants



Paths Granting Account "mmartin" with Privilege "SELECT" on Object "das_creditcards".

mmartin (A) → mike martin (principal key DB_USER) → readcustomerdata (R) → das_creditcards (T)

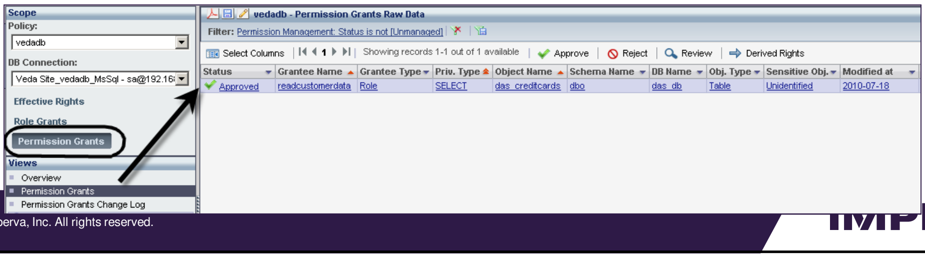


vedadb - Role Grants Raw Data

Filter: Role Management: Status is not [Unmanaged] and Granted DB Label is [das_db]

Showing records 1-2 out of 2 available

Status	Grantee Name	DB Name (Granted)	Grantee Type	Granted Priv.	Granted Type	Modified at
Reject	mike martin	das_db	DB user	readcustomerdata	Role	2010-07-18
In Review	mmartin	das_db	Account	mike martin	DB user	2010-07-18



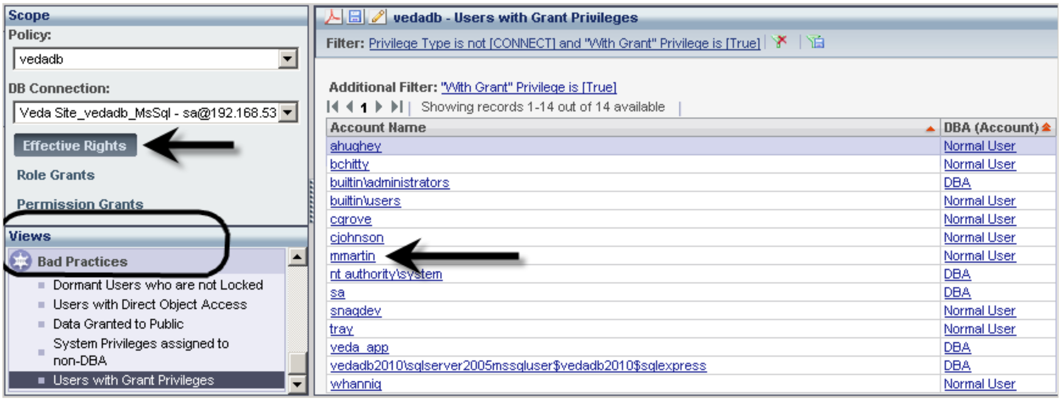
vedadb - Permission Grants Raw Data

Filter: Permission Management: Status is not [Unmanaged]

Showing records 1-1 out of 1 available

Status	Grantee Name	Grantee Type	Priv. Type	Object Name	Schema Name	DB Name	Obj. Type	Sensitive Obj.	Modified at
Approved	readcustomerdata	Role	SELECT	das_creditcards	dbo	das_db	Table	Unidentified	2010-07-18

Use Case 2: Finding Excessive Rights



Policy: vedadb

DB Connection: Veda Site_vedadb_MsSql - sa@192.168.53

- Dormant Users who are not Locked
- Users with Direct Object Access
- Data Granted to Public
- System Privileges assigned to non-DBA
- Users with Grant Privileges

vedadb - Users with Grant Privileges

Filter: Privilege Type is not [CONNECT] and "With Grant" Privilege is [True]

Additional Filter: "With Grant" Privilege is [True]

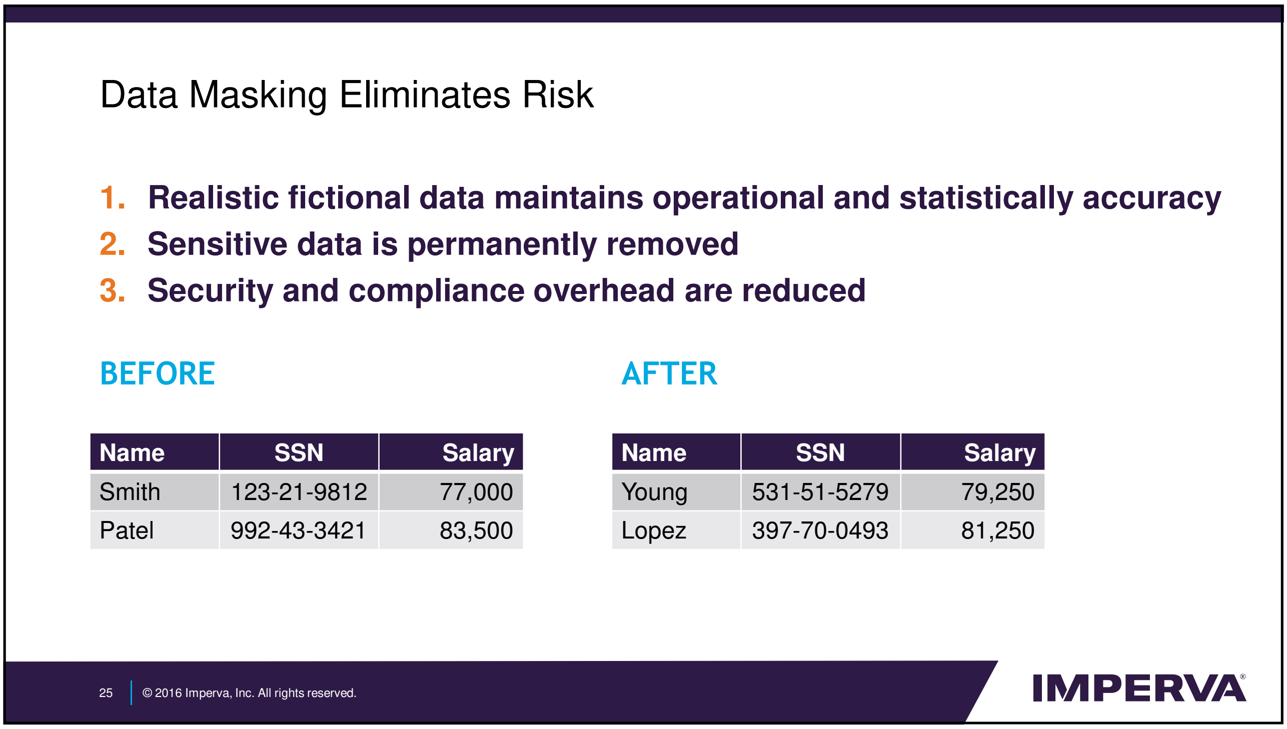
1 | Showing records 1-14 out of 14 available

Account Name	DBA (Account)
ahughey	Normal User
bchitty	Normal User
builtin\administrators	DBA
builtin\users	Normal User
cgrove	Normal User
cjohnson	Normal User
mmartin	Normal User
nt authority\system	DBA
sa	DBA
snagdev	Normal User
tray	Normal User
veda_app	DBA
vedadb2010\sqlserver2005mssqluser$vedadb2010$sqlexpress	DBA
whannig	Normal User

3

How to remove databases from GDPR scope

Minimization / Masking



Data Masking Eliminates Risk

1. **Realistic fictional data maintains operational and statistically accuracy**
2. **Sensitive data is permanently removed**
3. **Security and compliance overhead are reduced**

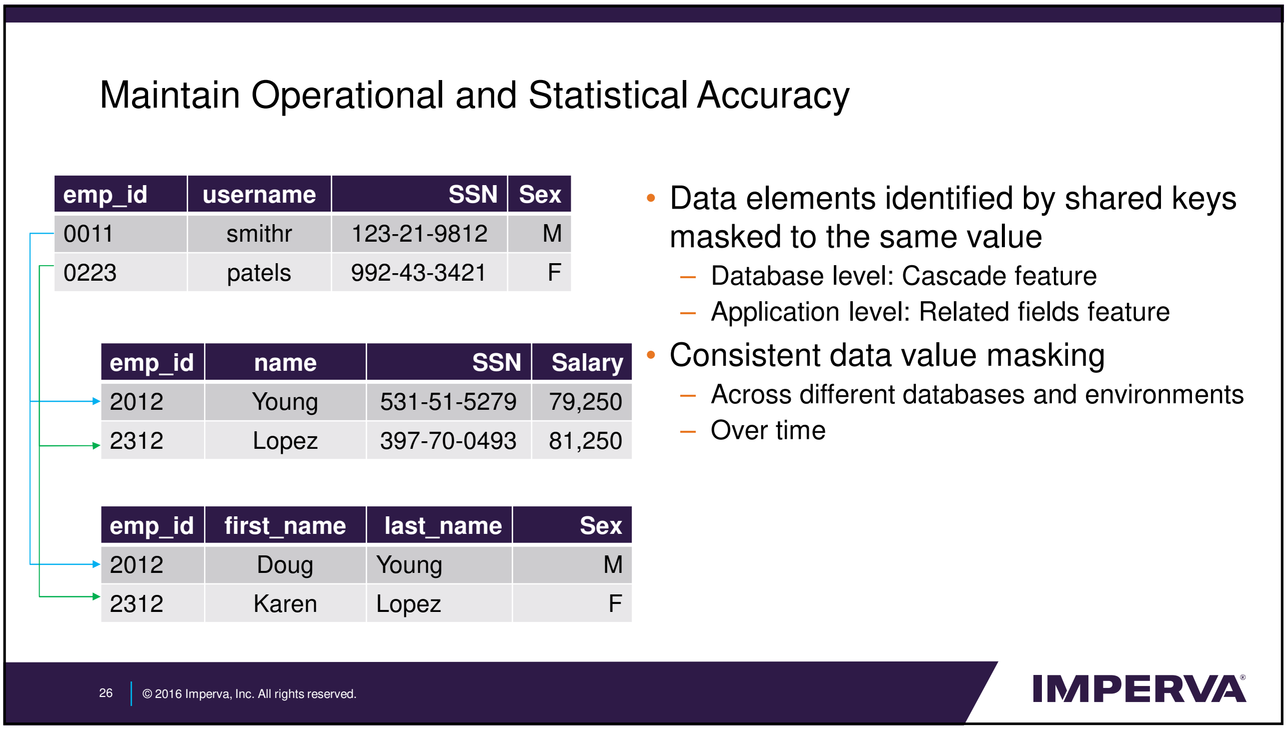
BEFORE

Name	SSN	Salary
Smith	123-21-9812	77,000
Patel	992-43-3421	83,500

AFTER

Name	SSN	Salary
Young	531-51-5279	79,250
Lopez	397-70-0493	81,250

25



Maintain Operational and Statistical Accuracy

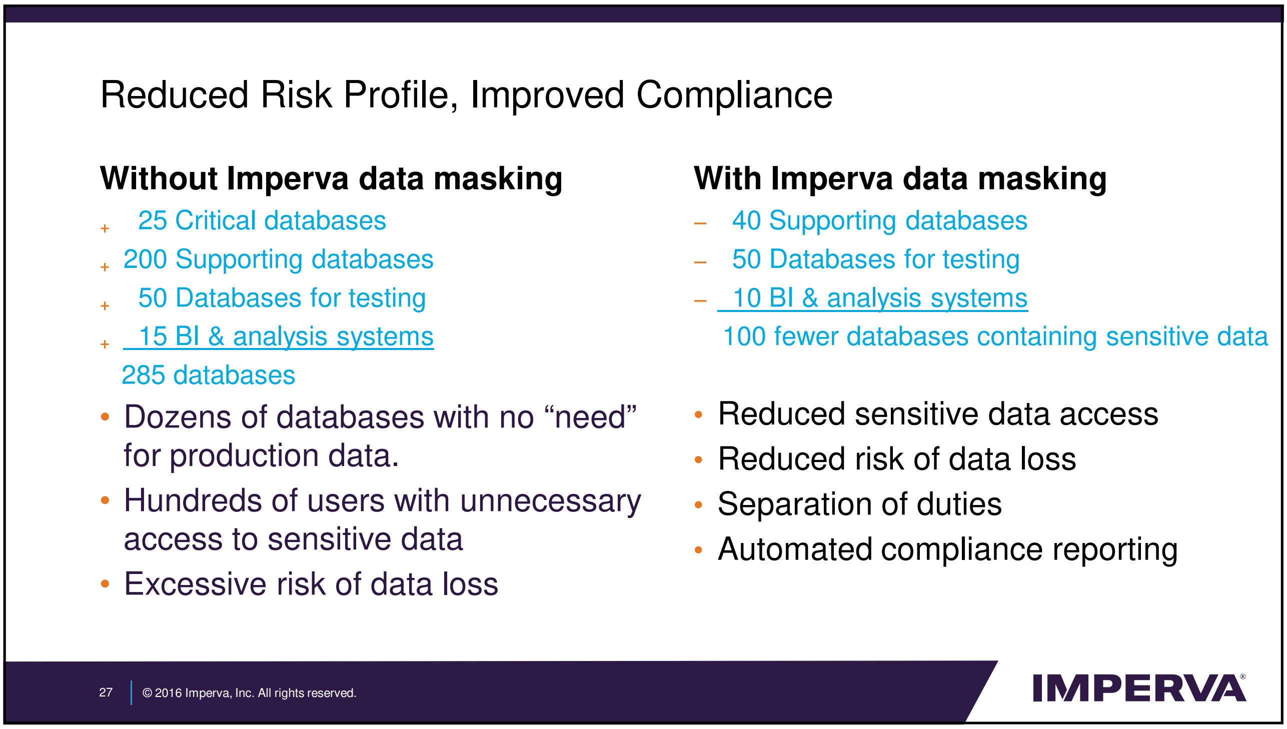
emp_id	username	SSN	Sex
0011	smithr	123-21-9812	M
0223	patels	992-43-3421	F

emp_id	name	SSN	Salary
2012	Young	531-51-5279	79,250
2312	Lopez	397-70-0493	81,250

emp_id	first_name	last_name	Sex
2012	Doug	Young	M
2312	Karen	Lopez	F

- Data elements identified by shared keys masked to the same value
  - Database level: Cascade feature
  - Application level: Related fields feature
- Consistent data value masking
  - Across different databases and environments
  - Over time

26



Reduced Risk Profile, Improved Compliance

Without Imperva data masking

+ 25 Critical databases
+ 200 Supporting databases
+ 50 Databases for testing
+ 15 BI & analysis systems
285 databases

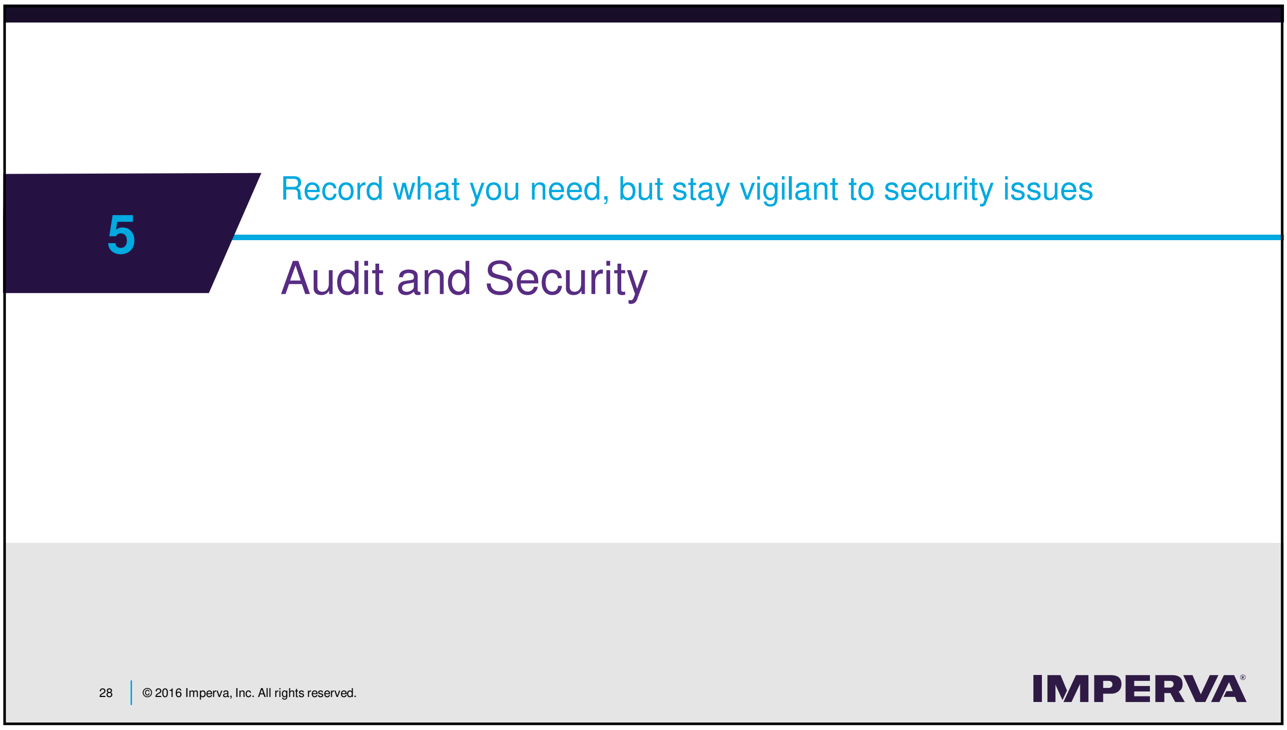
- Dozens of databases with no “need” for production data.
- Hundreds of users with unnecessary access to sensitive data
- Excessive risk of data loss

With Imperva data masking

– 40 Supporting databases
– 50 Databases for testing
– 10 BI & analysis systems
100 fewer databases containing sensitive data

- Reduced sensitive data access
- Reduced risk of data loss
- Separation of duties
- Automated compliance reporting

IMPERVA



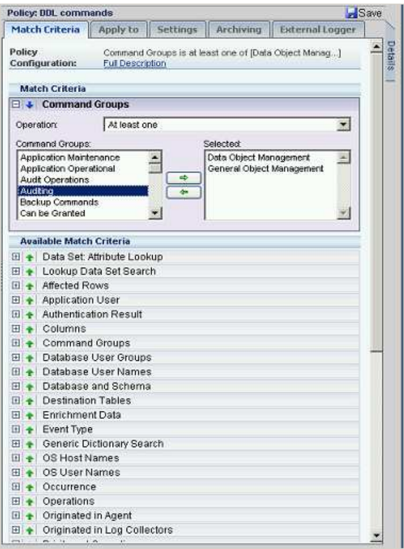
5

Record what you need, but stay vigilant to security issues

Audit and Security

IMPERVA

Audit Policy Structure



Policy: DDL commands

Policy Configuration: Command Groups is at least one of [Data Object Manag...] Full Description

Match Criteria

Command Groups

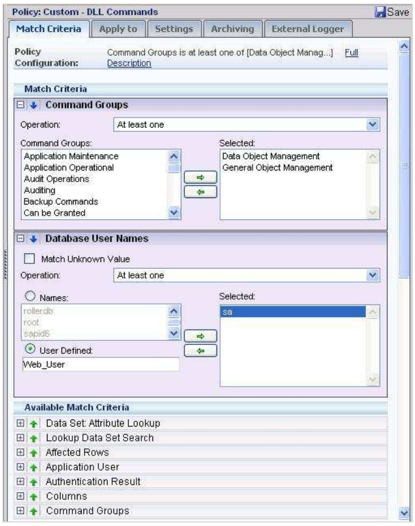
Operation: At least one

Command Groups: Application Maintenance, Application Operational, Audit Operations, Auditing, Backup Commands, Can be Granted

Selected: Data Object Management, General Object Management

Available Match Criteria

- Data Set: Attribute Lookup
- Lookup Data Set Search
- Affected Rows
- Application User
- Authentication Result
- Columns
- Command Groups
- Database User Groups
- Database User Names
- Database and Schema
- Destination Tables
- Enrichment Data
- Event Type
- Generic Dictionary Search
- OS Host Names
- OS User Names
- Occurrence
- Operations
- Originated in Agent
- Originated in Log Collectors



Policy: Custom - DLL Commands

Policy Configuration: Command Groups is at least one of [Data Object Manag...] Full Description

Match Criteria

Command Groups

Operation: At least one

Command Groups: Application Maintenance, Application Operational, Audit Operations, Auditing, Backup Commands, Can be Granted

Selected: Data Object Management, General Object Management

Database User Names

☐ Match Unknown Value

Operation: At least one

○ Names: rollerdb, root, sapid6

● User Defined: Web_User

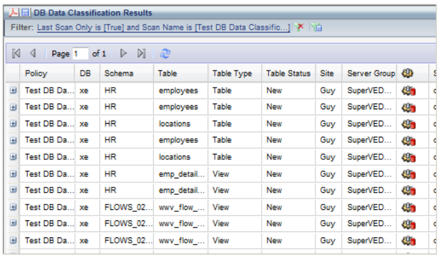
Selected: sa

Available Match Criteria

- Data Set: Attribute Lookup
- Lookup Data Set Search
- Affected Rows
- Application User
- Authentication Result
- Columns
- Command Groups

© 2016 Imperva, Inc. All rights reserved.

Sensitive Data Discovery populates Create Table Groups

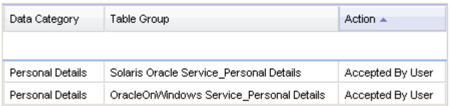


DB Data Classification Results

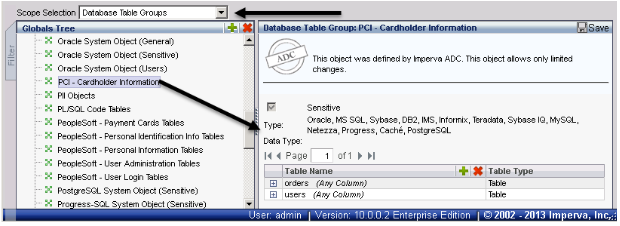
Filter: Last Scan Only is [True] and Scan Name is [Test DB Data Classific...]

Page 1 of 1

Policy	DB	Schema	Table	Table Type	Table Status	Site	Server Group
Test DB Da...	xe	HR	employees	Table	New	Guy	SuperVED...
Test DB Da...	xe	HR	employees	Table	New	Guy	SuperVED...
Test DB Da...	xe	HR	locations	Table	New	Guy	SuperVED...
Test DB Da...	xe	HR	employees	Table	New	Guy	SuperVED...
Test DB Da...	xe	HR	locations	Table	New	Guy	SuperVED...
Test DB Da...	xe	HR	emp_detail...	View	New	Guy	SuperVED...
Test DB Da...	xe	HR	emp_detail...	View	New	Guy	SuperVED...
Test DB Da...	xe	FLOWS_02...	wwv_flow_...	View	New	Guy	SuperVED...
Test DB Da...	xe	FLOWS_02...	wwv_flow_...	View	New	Guy	SuperVED...
Test DB Da...	xe	FLOWS_02...	wwv_flow_...	View	New	Guy	SuperVED...



Data Category	Table Group	Action ▲
Personal Details	Solaris Oracle Service_Personal Details	Accepted By User
Personal Details	OracleOnWindows Service_Personal Details	Accepted By User



Scope Selection: Database Table Groups

- Oracle System Object (General)
- Oracle System Object (Sensitive)
- Oracle System Object (Users)
- PCI - Cardholder Information
- PII Objects
- PL/SQL Code Tables
- PeopleSoft - Payment Cards Tables
- PeopleSoft - Personal Identification Info Tables
- PeopleSoft - Personal Information Tables
- PeopleSoft - User Administration Tables
- PeopleSoft - User Login Tables
- PostgreSQL System Object (Sensitive)
- Progress-SQL System Object (Sensitive)

Database Table Group: PCI - Cardholder Information

This object was defined by Imperva ADC. This object allows only limited changes.

☑ Sensitive

Type: Oracle, MS SQL, Sybase, DB2, IMS, Informix, Teradata, Sybase IQ, MySQL, Netezza, Progress, Caché, PostgreSQL

Data Type:

Page 1 of 1

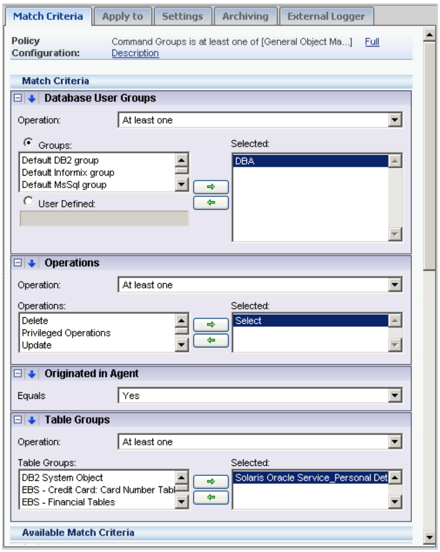
Table Name	Table Type
orders *(Any Column)*	Table
users *(Any Column)*	Table

User: admin | Version: 10.0.0.2 Enterprise Edition | © 2002 - 2013 Imperva, Inc.

© 2016 Imperva, Inc. All rights reserved.

Table Group Used in Policy

- Audit if…
  - A user from **DBA** group…
  - **Selects** information from…
  - Tables defined as sensitive in the **Solaris Oracle Service_ Personal Details** group…
  - …while logged in **local** to the database server.
- Data captured would include:
  - Audit all event details
  - Audit response data
    - So you can inform the affected person?
    - So you know the extent of the breach



Match Criteria | Apply to | Settings | Archiving | External Logger

Policy Configuration: Command Groups is at least one of [General Object Ma...] Full Description

Match Criteria

Database User Groups

Operation: At least one

● Groups:
- Default DB2 group
- Default Informix group
- Default MsSql group

○ User Defined:

Selected:
- DBA

Operations

Operation: At least one

Operations:
- Delete
- Privileged Operations
- Update

Selected:
- Select

Originated in Agent

Equals: Yes

Table Groups

Operation: At least one

Table Groups:
- DB2 System Object
- EBS - Credit Card: Card Number Tabl
- EBS - Financial Tables

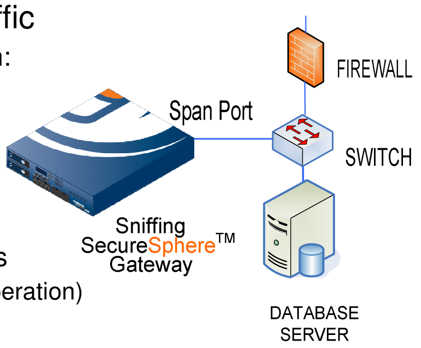
Selected:
- Solaris Oracle Service_Personal Det

Available Match Criteria

IMPERVA®

Behavioristic Profiling for Database Applications

- Builds a profile on database traffic
  - Gathers database user information:
    - Source IP addresses
    - Source applications
    - Source OS hosts
    - OS user name
    - Successful queries
  - Gathers queries into Query Groups
    - A Query Group = (Target Table, Operation)
    - Example (Users, Select)
    - Groups characterize the user's rights
    - Alert per-query or per-query group violation
    - Nested queries are documented



FIREWALL

Span Port

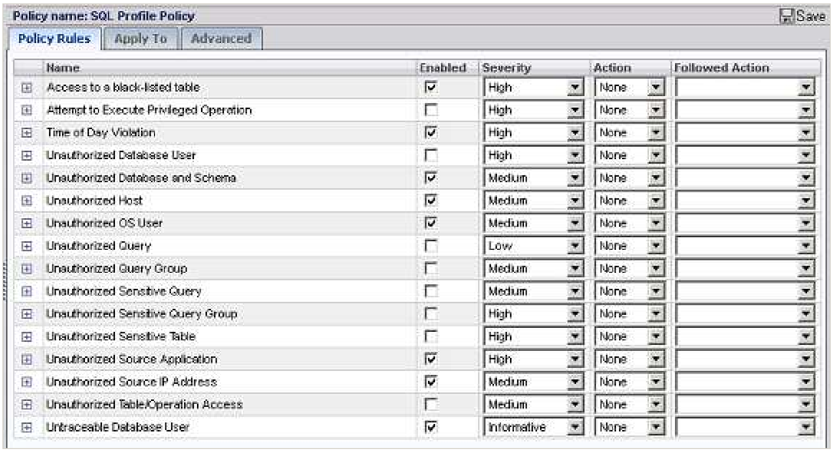
SWITCH

Sniffing SecureSphere™ Gateway

DATABASE SERVER

IMPERVA®

Database Profiling – Detecting changes in behaviour



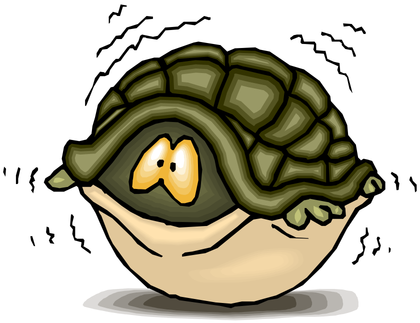
Policy name: SQL Profile Policy

	Name	Enabled	Severity	Action	Followed Action
⊞	Access to a black-listed table	☑	High	None	
⊞	Attempt to Execute Privileged Operation	☐	High	None	
⊞	Time of Day Violation	☑	High	None	
⊞	Unauthorized Database User	☐	High	None	
⊞	Unauthorized Database and Schema	☑	Medium	None	
⊞	Unauthorized Host	☑	Medium	None	
⊞	Unauthorized OS User	☑	Medium	None	
⊞	Unauthorized Query	☐	Low	None	
⊞	Unauthorized Query Group	☐	Medium	None	
⊞	Unauthorized Sensitive Query	☐	Medium	None	
⊞	Unauthorized Sensitive Query Group	☐	High	None	
⊞	Unauthorized Sensitive Table	☐	High	None	
⊞	Unauthorized Source Application	☑	High	None	
⊞	Unauthorized Source IP Address	☑	Medium	None	
⊞	Unauthorized Table/Operation Access	☐	Medium	None	
⊞	Untraceable Database User	☑	Informative	None	

IMPERVA

What about Security? Blocking SQL Transactions?

- Database security - perceptions:
  - Dangerous to connectivity
  - Change control nightmare
  - Not yet “required” by regulations
  - I might get fired if I do it wrong
  - I would if business owners would let me
  - …



  - Excuses, excuses, excuses… We have heard them all.
    - ...and we listened!

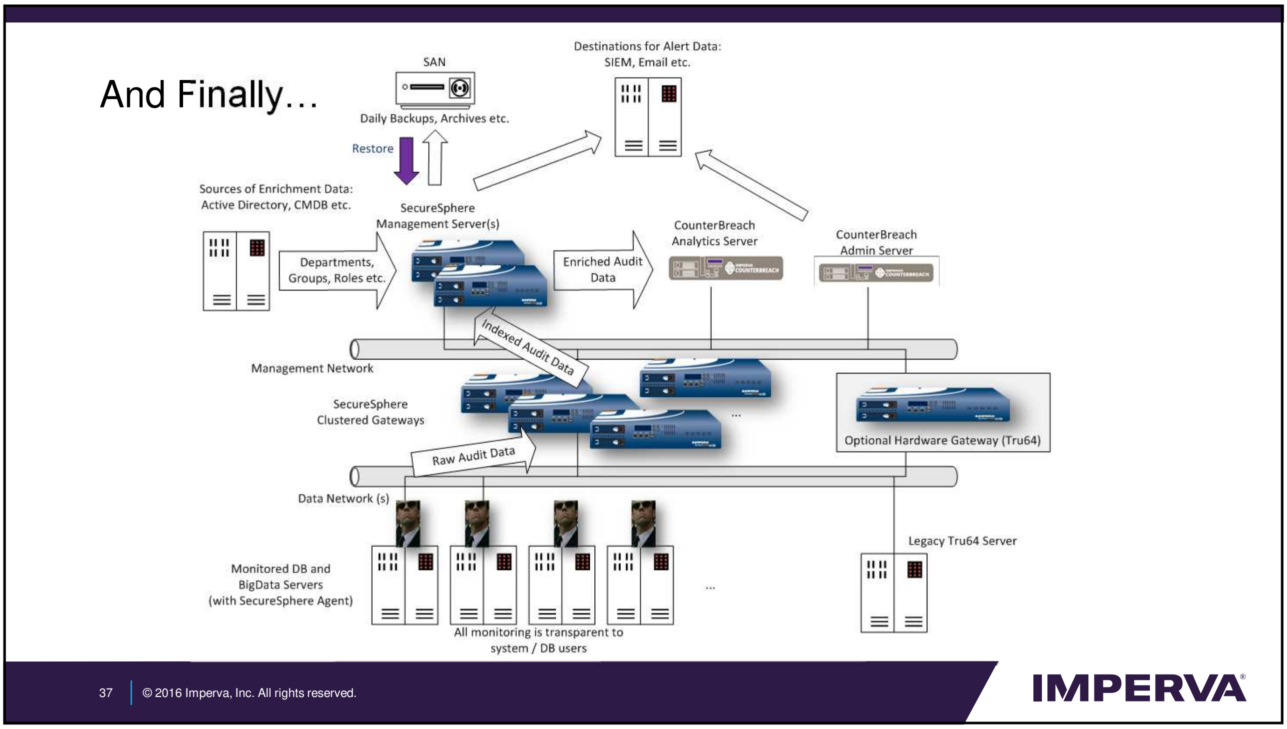
IMPERVA

Blocking Tools

- SecureSphere gives you the tools to be confident in blocking
- Architecture
  - Fail-open inline bridge mode
  - Sniffing with blocking interface configured
  - Blocking on the web application side
  - Agent-based blocking abilities
- Mode
  - Simulation / Active
- Policy granularity
  - Custom Correlation Policies
  - Profiling

Imperva Understands Reality

- If you cannot use database security blocking initially, leave it off until you can:
  - Security policies do not have to block – use for notifications
  - Leave in Simulation mode
  - Use sniffing without a blocking interface configured
- However, significant benefits
  - Web/DB correlation: audit web user and original source info
  - Block/quarantine web application user when abusing application
  - Prevent unauthorized database access by profile or custom policies
  - Prevent catastrophic events – SQL injection to “drop database”
  - Ability to focus only on the obviously “bad” events
  - Also able to aggressively secure very sensitive environments



And Finally…

SAN

Daily Backups, Archives etc.

Restore

Destinations for Alert Data: SIEM, Email etc.

Sources of Enrichment Data: Active Directory, CMDB etc.

Departments, Groups, Roles etc.

SecureSphere Management Server(s)

Enriched Audit Data

CounterBreach Analytics Server

CounterBreach Admin Server

Indexed Audit Data

Management Network

SecureSphere Clustered Gateways

...

Optional Hardware Gateway (Tru64)

Raw Audit Data

Data Network (s)

Legacy Tru64 Server

Monitored DB and BigData Servers (with SecureSphere Agent)

...

All monitoring is transparent to system / DB users

37 | © 2016 Imperva, Inc. All rights reserved.

IMPERVA®

IMPERVA®