# Imperva CounterBreach - When AI comes to IT security

Konstantin Solodilin

May 2016

IMPERVA®

# Imperva Inc.

IMPERVA®

There are two kinds of big companies
There are those who've been hacked… and
those who don't know they've been hacked.

FBI DIRECTOR JAMES COMEY

October 2014




IMPERVA®

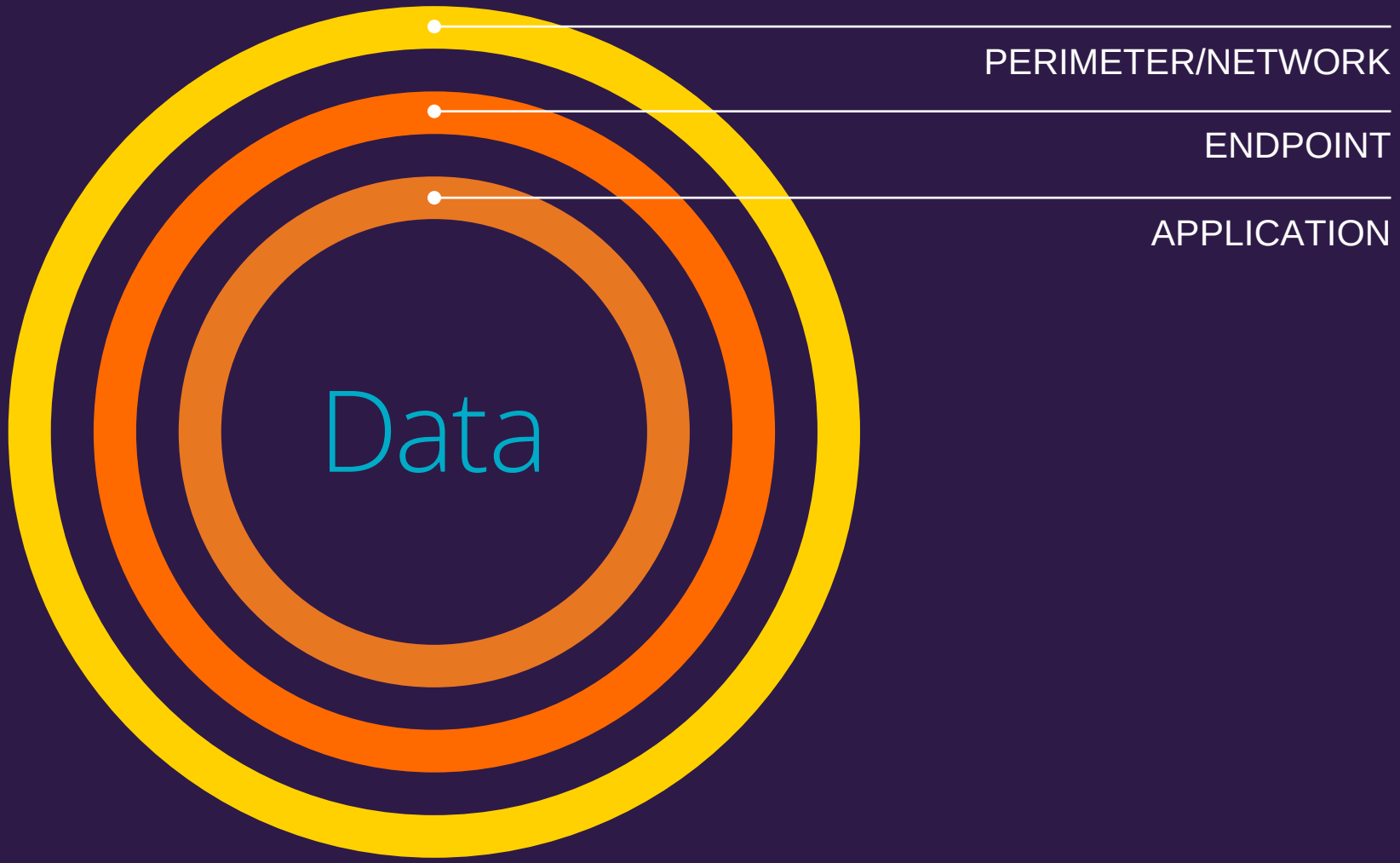
# 90%

of companies have been hacked at one time or another




IMPERVA®

# Traditional security doesn't work







IMPERVA®

# Traditional security doesn't work


PERIMETER/NETWORK

Insiders bypass the perimeter and compromise your data

Malware leverages unsuspecting users

Applications and data moving to the cloud




IMPERVA®

# Traditional security doesn't work


PERIMETER/NETWORK

Insiders bypass the perimeter and compromise your data

Malware leverages unsuspecting users

Applications and data moving to the cloud




IMPERVA®

# Traditional security doesn't work


PERIMETER/NETWORK

Insiders bypass the perimeter and compromise your data

Malware leverages unsuspecting users

Applications and data moving to the cloud




IMPERVA®

# Traditional security doesn't work


PERIMETER/NETWORK

Insiders bypass the perimeter and compromise your data

Malware leverages unsuspecting users

Applications and data moving to the cloud




IMPERVA®

# Traditional security doesn't work


PERIMETER/NETWORK

ENDPOINT

Conspiring with users to steal data

Duping users into opening up vulnerabilities

BYOD




IMPERVA®

# Traditional security doesn't work


PERIMETER/NETWORK

ENDPOINT

Conspiring with users to steal data

Duping users into opening up vulnerabilities

BYOD




IMPERVA®

# Traditional security doesn't work


PERIMETER/NETWORK

ENDPOINT

Conspiring with users to steal data

Duping users into opening up vulnerabilities

BYOD




IMPERVA®

# Traditional security doesn't work


PERIMETER/NETWORK

ENDPOINT

Conspiring with users to steal data

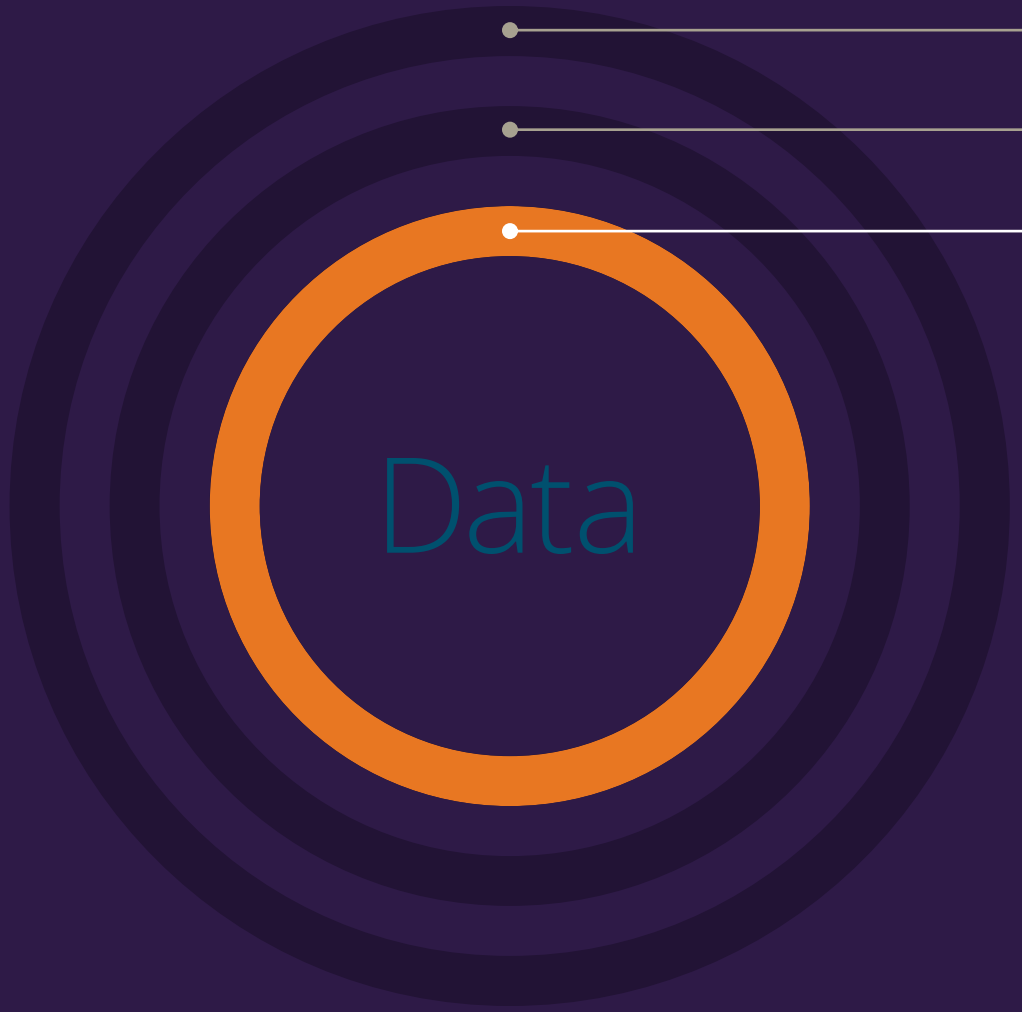
Duping users into opening up vulnerabilities

BYOD




IMPERVA®

# Traditional security doesn't work




PERIMETER/NETWORK

ENDPOINT

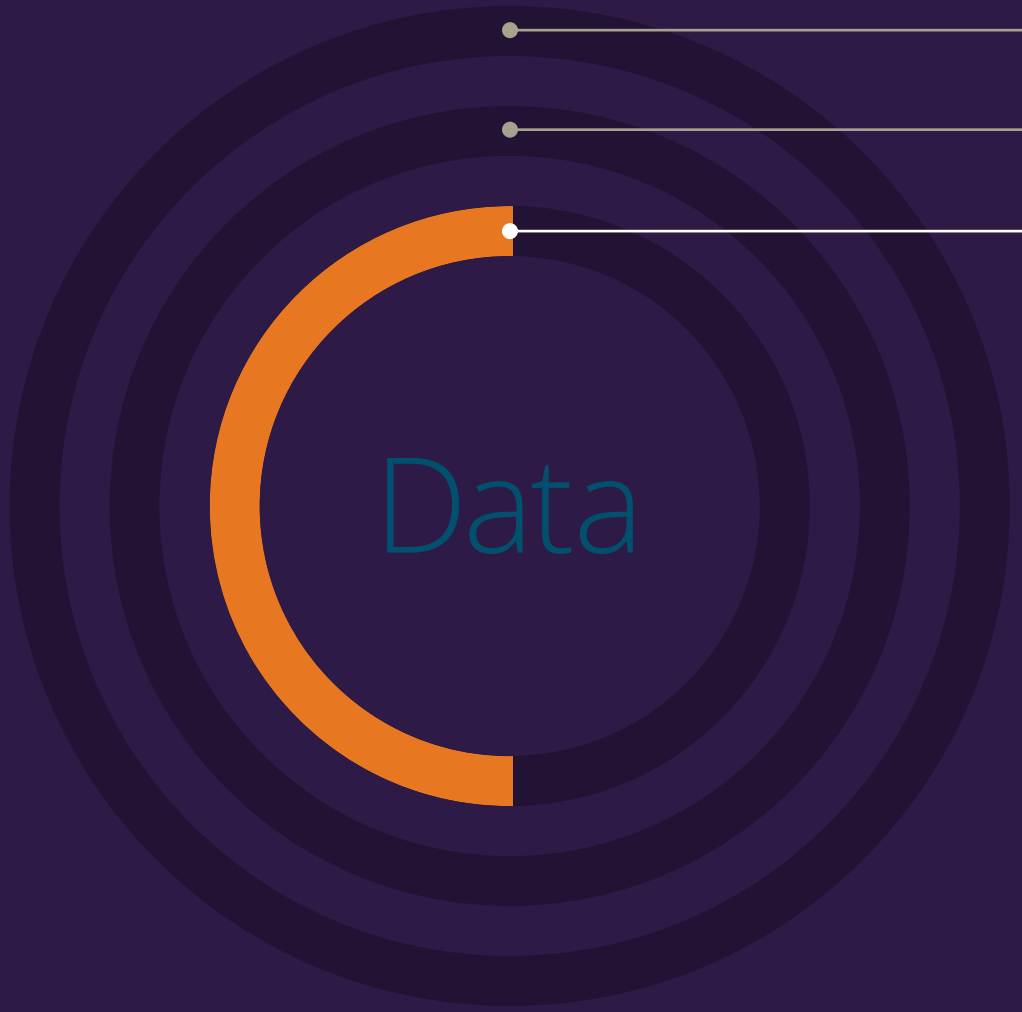
APPLICATION

Hackers breach applications effectively




IMPERVA®

# Traditional security doesn't work




PERIMETER/NETWORK

ENDPOINT

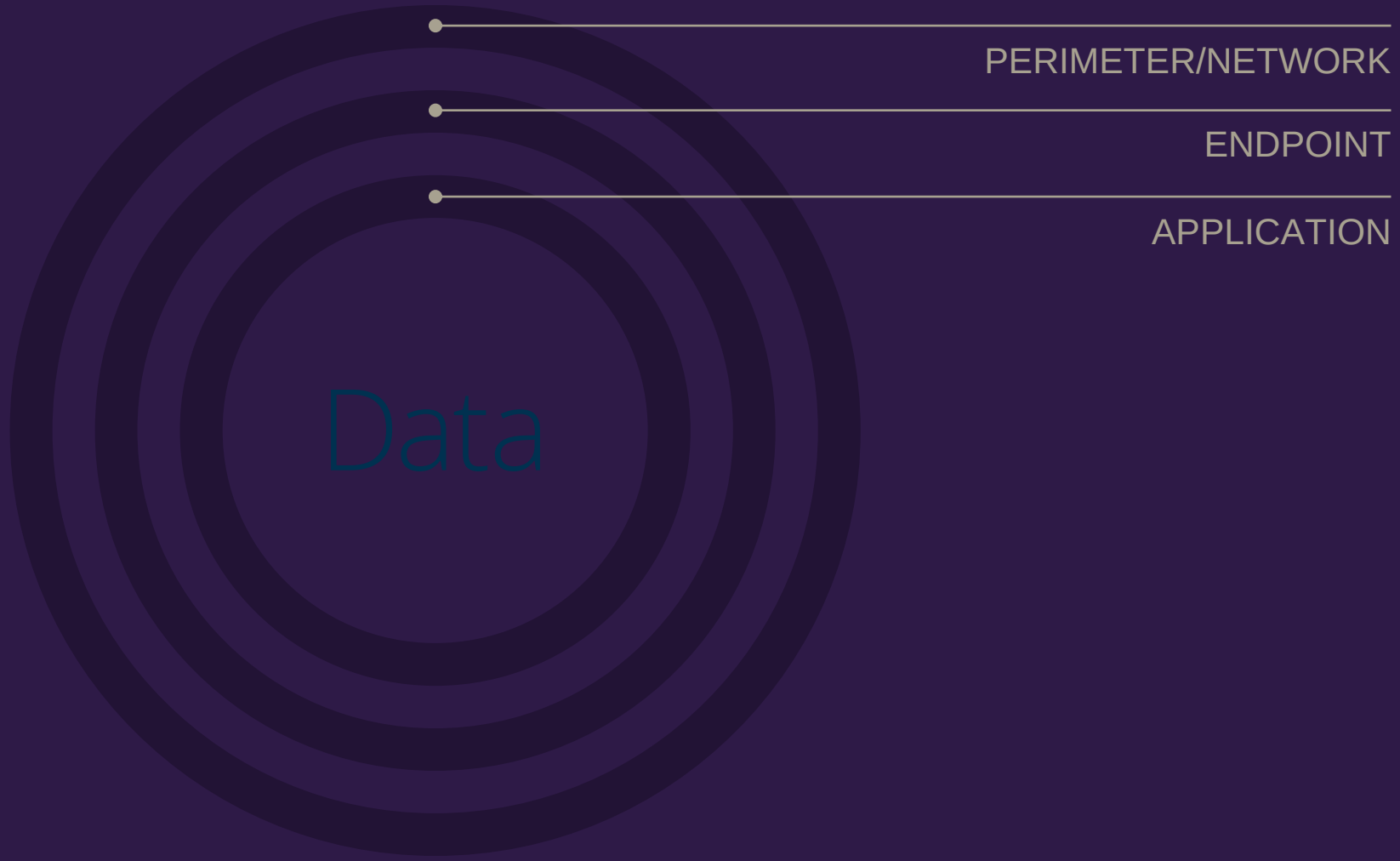
APPLICATION

Hackers breach applications effectively




IMPERVA®

# Traditional security doesn't work







IMPERVA®


Traditional
security

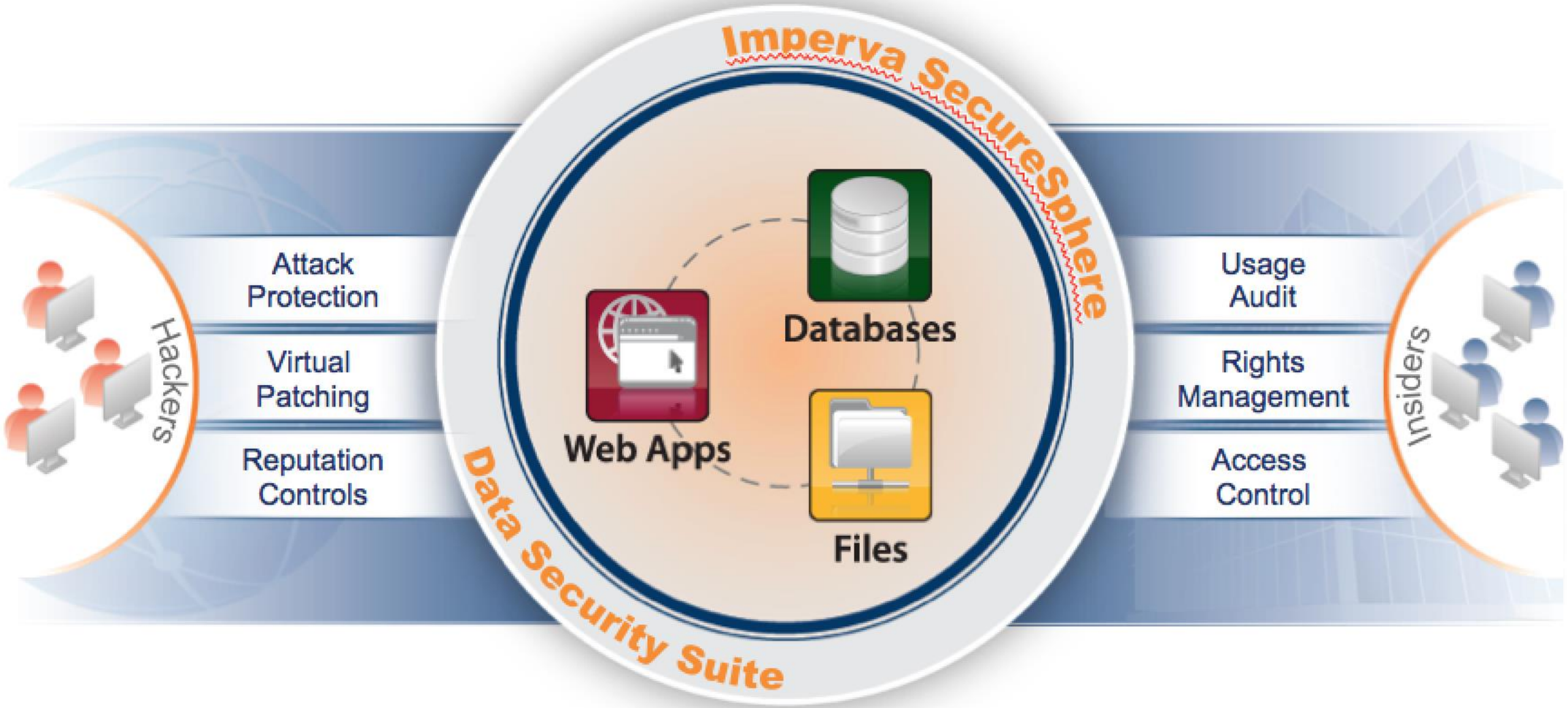
# Protect what's INSIDE

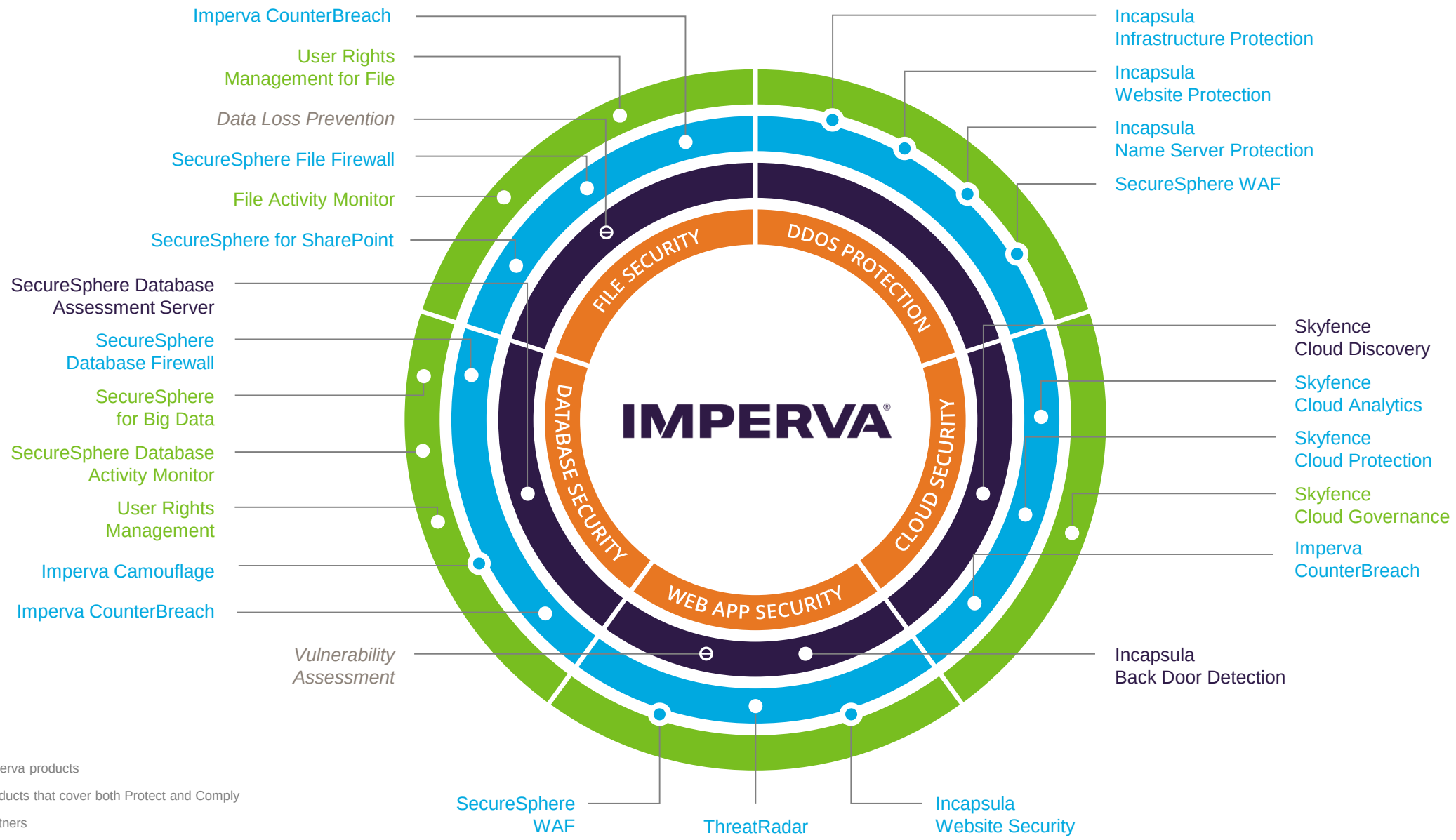

Protecting
DATA AND APPS
is exactly what Imperva does


- Protects structured and unstructured data where it resides: databases and file servers
- Protects where it’s accessed: Web applications
- Guards against both outside threats and internal actors

IMPERVA®

# PROTECTING business-critical data and applications

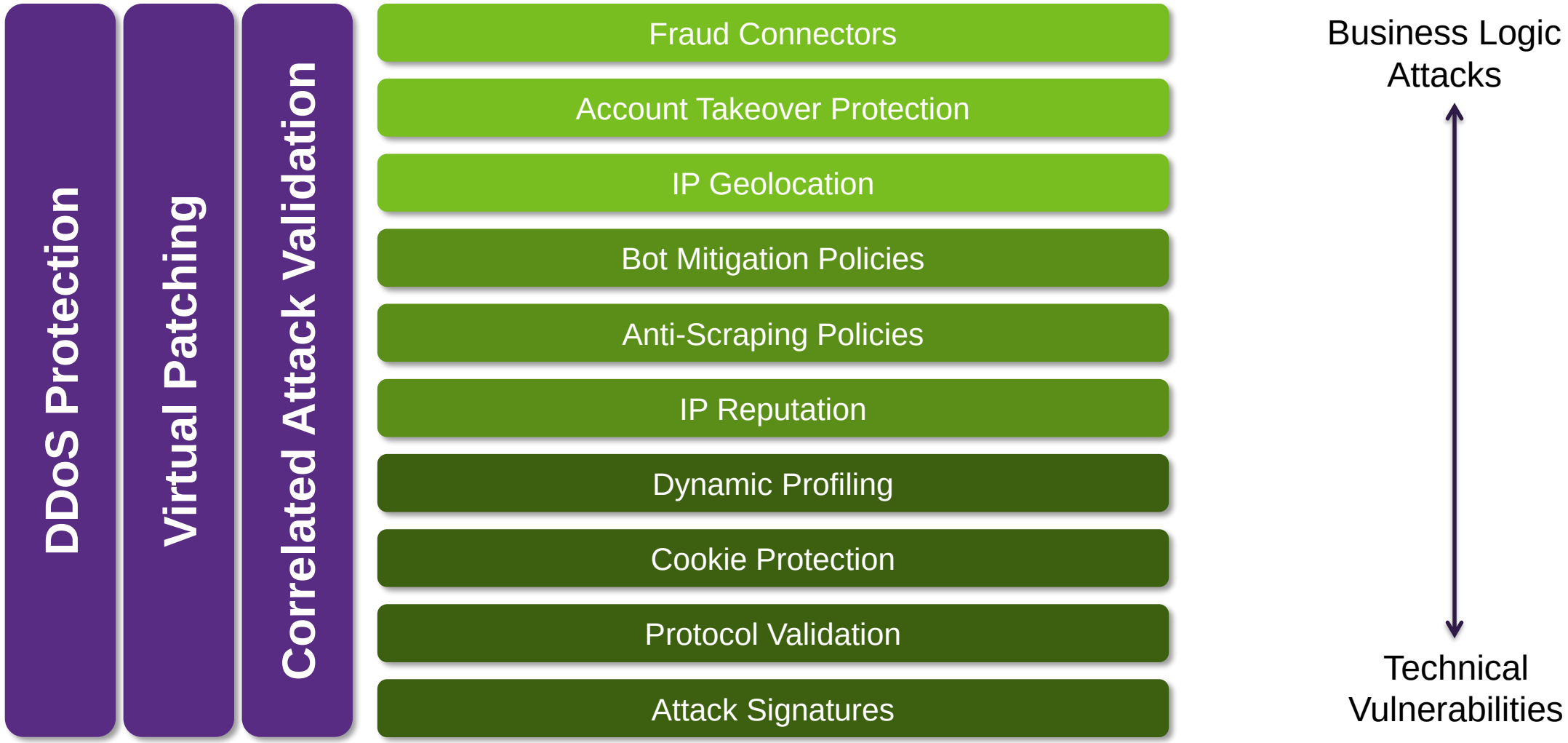

Imperva SecureSphere
Data Security Suite
Hackers
Attack Protection
Virtual Patching
Reputation Controls
Web Apps
Databases
Files
Usage Audit
Rights Management
Access Control
Insiders


Imperva CounterBreach
User Rights Management for File
Data Loss Prevention
SecureSphere File Firewall
File Activity Monitor
SecureSphere for SharePoint
SecureSphere Database Assessment Server
SecureSphere Database Firewall
SecureSphere for Big Data
SecureSphere Database Activity Monitor
User Rights Management
Imperva Camouflage
Imperva CounterBreach
Vulnerability Assessment
SecureSphere WAF
ThreatRadar
Incapsula Website Security
Incapsula Back Door Detection
Skyfence Cloud Discovery
Skyfence Cloud Analytics
Skyfence Cloud Protection
Skyfence Cloud Governance
Imperva CounterBreach
Incapsula Infrastructure Protection
Incapsula Website Protection
Incapsula Name Server Protection
SecureSphere WAF
FILE SECURITY
DDOS PROTECTION
DATABASE SECURITY
CLOUD SECURITY
WEB APP SECURITY
IMPERVA
Imperva products
Products that cover both Protect and Comply
Partners

# Imperva SecureSphere WAF

IMPERVA®

# Defenses Required to Protect Web Applications






IMPERVA®


Source: Gartner (June 2014)


Source: Gartner (July 2015)

# Imperva SecureSphere DBF

IMPERVA®

| Audit Requirements | CobiT (SOX) | PCI DSS | HIPAA | GLBA | ISO 17799 | EU Data Privacy Directive |
|---|---|---|---|---|---|---|
| 1. **System Access** (Successful/Failed Logins; User/Role/Permissions/ Password changes) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 2. **Data Access** (Successful/Failed SELECTs) | | ✓ | ✓ | ✓ | ✓ | ✓ |
| 3. **Data Changes** (Insert, Update, Delete) | ✓ | | ✓ | | ✓ | ✓ |
| 4. **Privileged User Activity** (All) | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 5. **Schema Changes** (Create/Drop/Alter Tables, Columns) | ✓ | ✓ | ✓ | ✓ | ✓ | |

# Purpose of Database Security Products

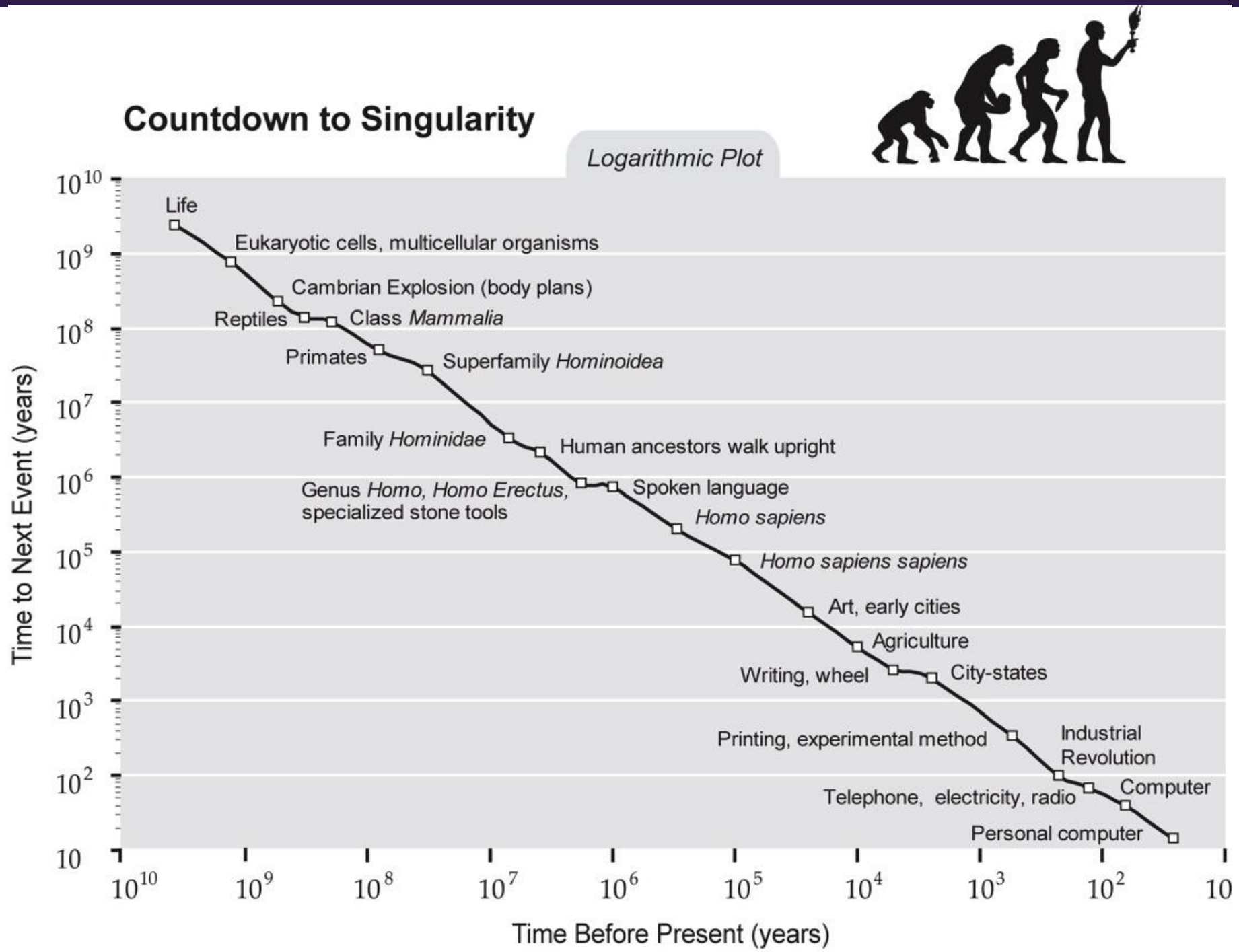

- Audit all access to sensitive data by privileged and application users
  - As required by PCI 10, SOX, HIPPA and other regulations
- Alert or block database attacks and abnormal access requests, in real time
- Detect and virtually patch database software vulnerabilities
- Identify excessive & dormant user rights to sensitive data
  - Aggregate DB user rights from across all DBs on the network
  - Reduce access to business need to know level (PCI 7)
- Accelerate incident response and forensic investigation with advanced analytics



IMPERVA®

# Imperva CounterBreach

IMPERVA®


Countdown to Singularity
Logarithmic Plot
Time to Next Event (years)
Time Before Present (years)
$10^{10}$
$10^{9}$
$10^{8}$
$10^{7}$
$10^{6}$
$10^{5}$
$10^{4}$
$10^{3}$
$10^{2}$
10
Life
Eukaryotic cells, multicellular organisms
Cambrian Explosion (body plans)
Reptiles
Class *Mammalia*
Primates
Superfamily *Hominoidea*
Family *Hominidae*
Human ancestors walk upright
Genus *Homo, Homo Erectus,* specialized stone tools
Spoken language
*Homo sapiens*
*Homo sapiens sapiens*
Art, early cities
Agriculture
Writing, wheel
City-states
Printing, experimental method
Industrial Revolution
Telephone, electricity, radio
Computer
Personal computer

IMPERVA®

# People are the WEAK LINK


Compromised


Careless

Malicious

# THE SOLUTION


# Truly Detecting and Containing Breaches Requires Addressing All

# Breach Detection Solution

Employee Profile

John Smith

Controller, CA

- DASHBOARD
- EMPLOYEE DETAILS
- INCIDENTS
- ANOMALIES
- BEHAVIOR PROFILE

## DASHBOARD

### EMPLOYEE DETAILS

**EMAIL**
John.Smith@mycompany.com

**PHONE**
+1 925-245-7645 +1 925-245-7647...

**OFFICE**
Redwood Shores, CA. BLD 3400...

SHOW MORE

### INCIDENTS

| | |
|---|---|
| CRITICAL | 2 |
| HIGH | 1 |
| MEDIUM | 1 |
| LOW | 15 |
| **TOTAL OPEN INCIDENTS** | **16** |

SHOW MORE

### ANOMALIES

**56**
**ANOMALIES**

John

LOW HIGH

SHOW MORE

## behaviorprofile for last 90 days

### ENDPOINTS

4
Endpoints used to access resources

**Last used**
7010-WT-RANG
25 October 2015, 13:07

SHOW MORE

### DATABASES


10
Databases accessed

**Recently accessed**
Master / ORACLE
25 October 2015, 13:07

SHOW MORE

### FILE ACCESS STATISTICS


800
Files accessed daily

**Recently accessed**
FileShare
25 October 2015, 13:07

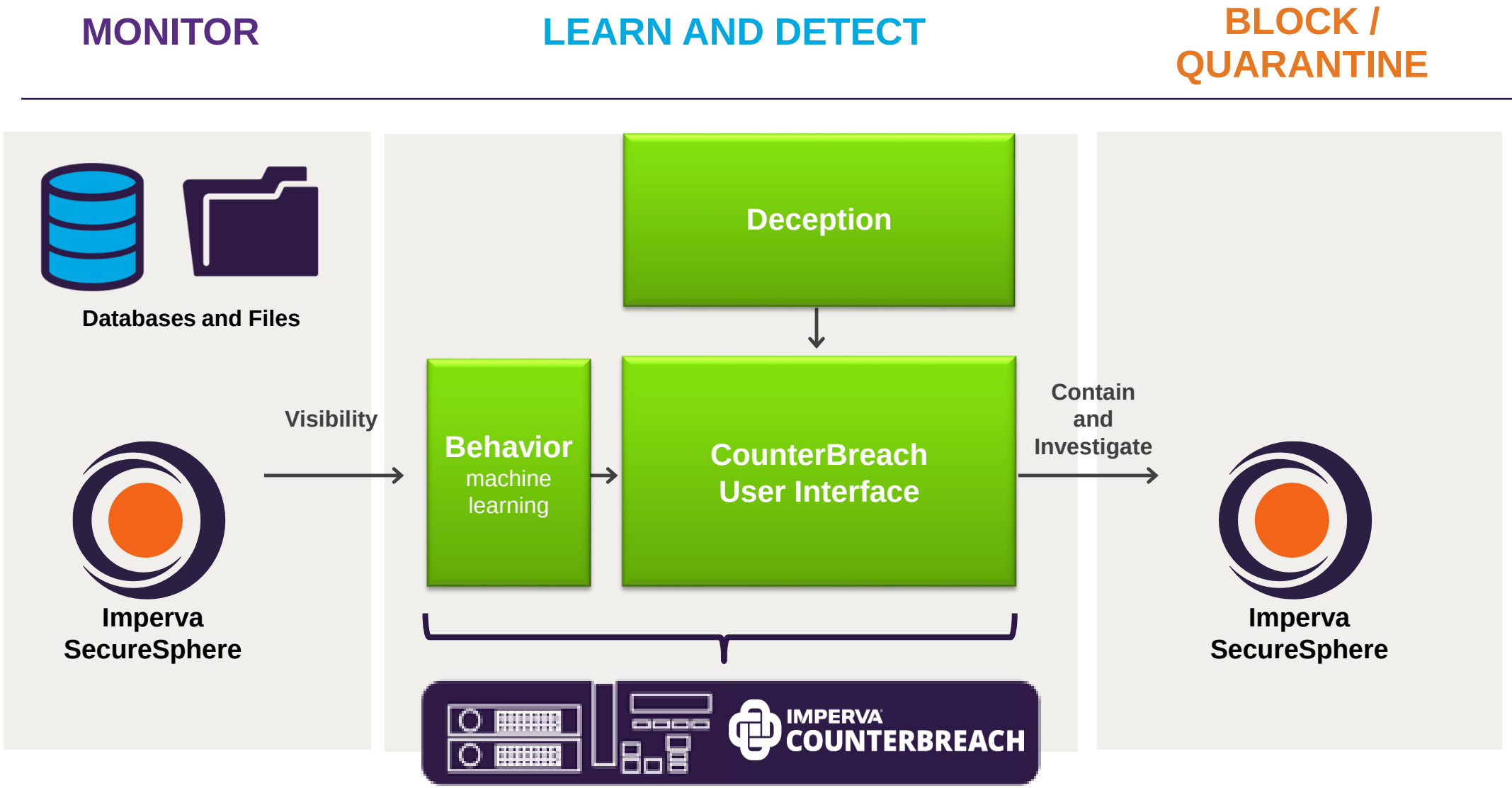
SHOW MORE

### CLOUD ACCESS


12
Cloud services accessed

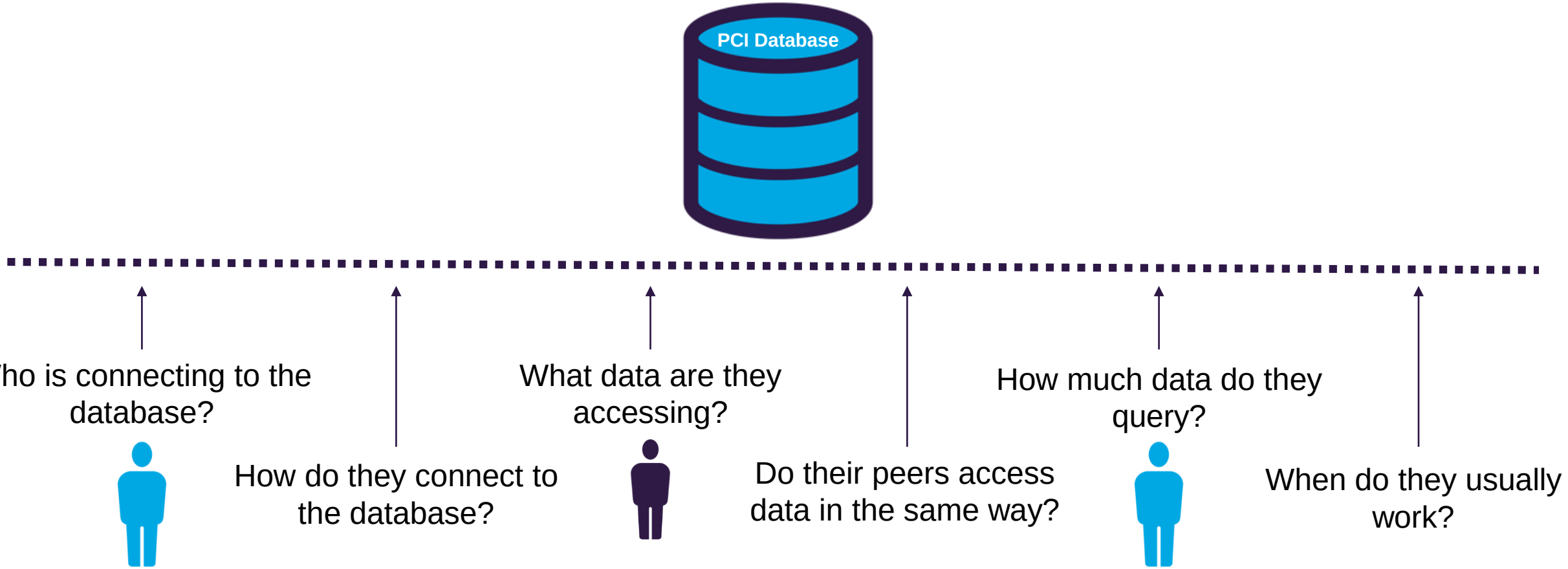
**Recently acsessed**
Salesforce
25 October 2015, 13:07

SHOW MORE


MONITOR
LEARN AND DETECT
BLOCK / QUARANTINE
Databases and Files
Imperva SecureSphere
Visibility
Deception
Behavior
machine learning
CounterBreach User Interface
Contain and Investigate
Imperva SecureSphere
IMPERVA COUNTERBREACH

# CounterBreach Behavior Analytics

# Behavior: Develop a Baseline of User Data Access





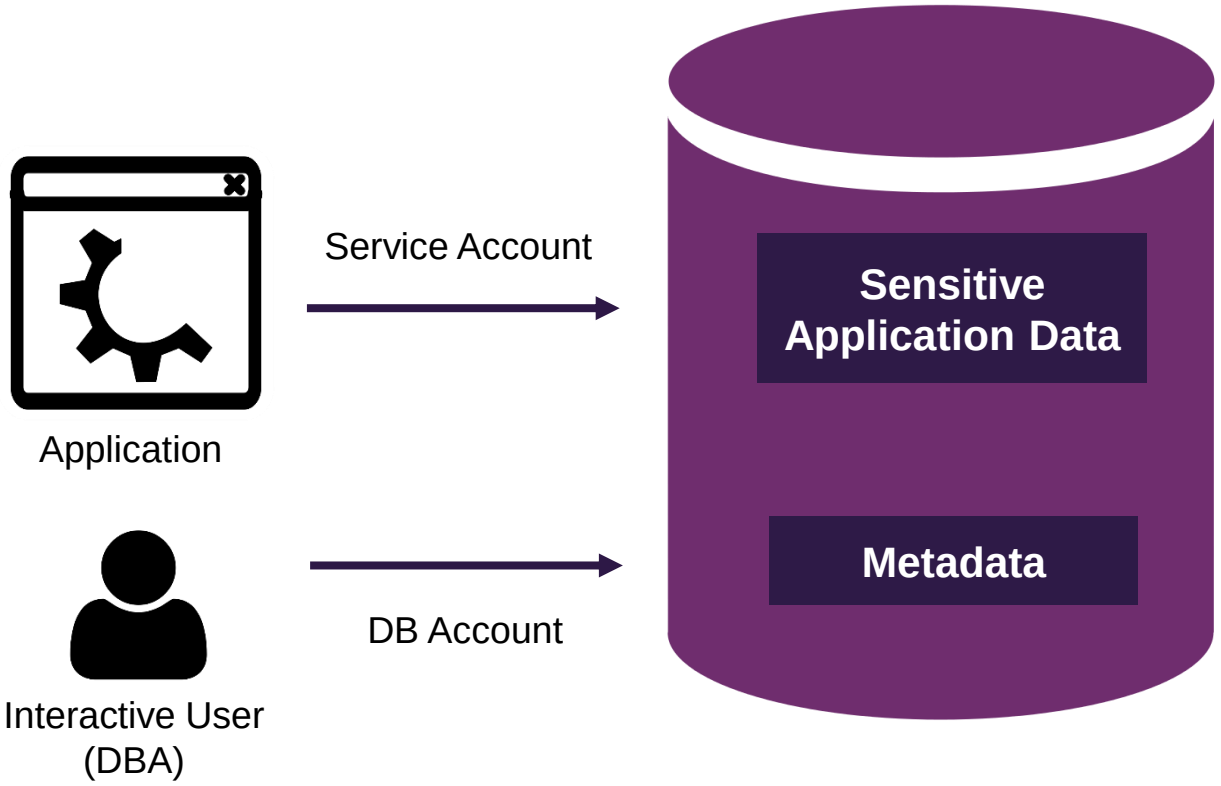

IMPERVA®

# Learning Data Access Patterns

**Learn**

- Leverage machine learning to understand the environment

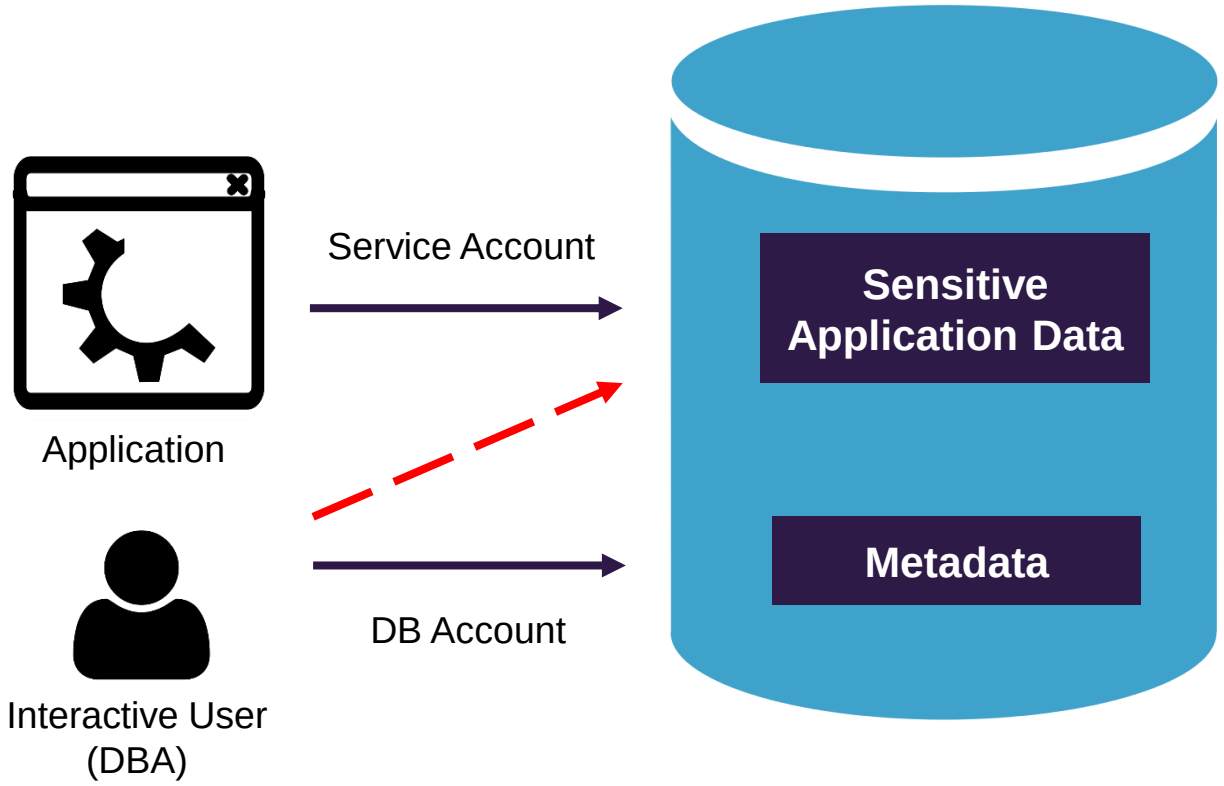
1. Identify user and connection types
2. Understand data
   - Typical purpose of data
3. Understand data access patterns
   - Amount of data
   - Comparison to peer groups
   - Typical working hours



# Finding Anomalies and Bad Practices

**Detect**

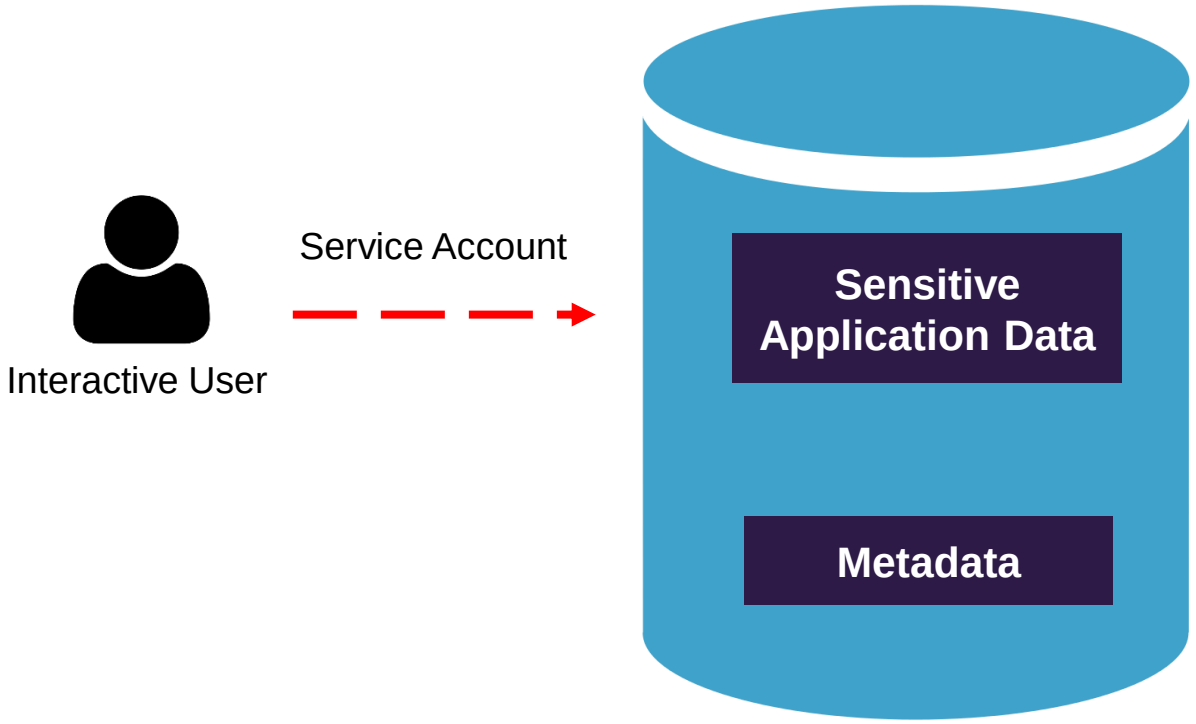
- Identify compromised, careless and malicious users
  - Application Table Access



# Finding Anomalies and Bad Practices

**Detect**

- Identify compromised, careless and malicious users
  - Application Table Access
  - Service Account Abuse



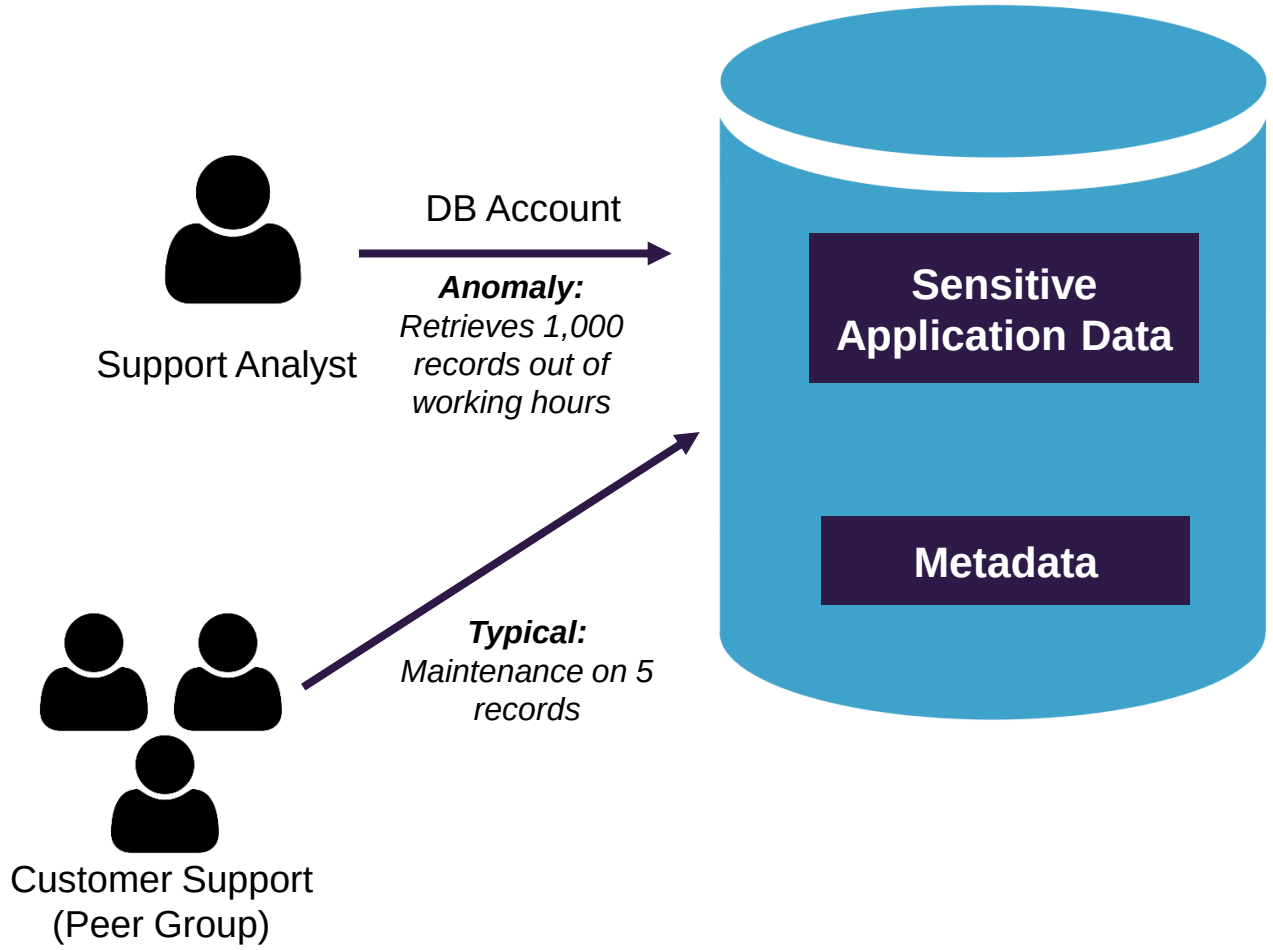



IMPERVA®

# Finding Anomalies and Bad Practices

**Detect**

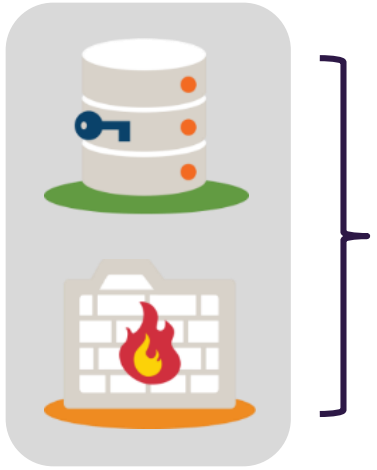
- Identify compromised, careless and malicious users
  - Application Table Access
  - Service Account Abuse
  - Unusual Data Retrieval






IMPERVA®

# How is Behavior Analytics deployed?



**1. Data Center Resources**
*Databases and File Servers*

Passively Monitors

**2. Imperva SecureSphere**
*Existing Setup or VM provided by Imperva*

Audit Archive
(e.g. SCP)

**3. CounterBreach Admin Server and CounterBreach Behavior Analytics Server**

SecureSphere logs are copied over to CounterBreach. The product will **not** interfere with existing SecureSphere deployments.

IMPERVA®