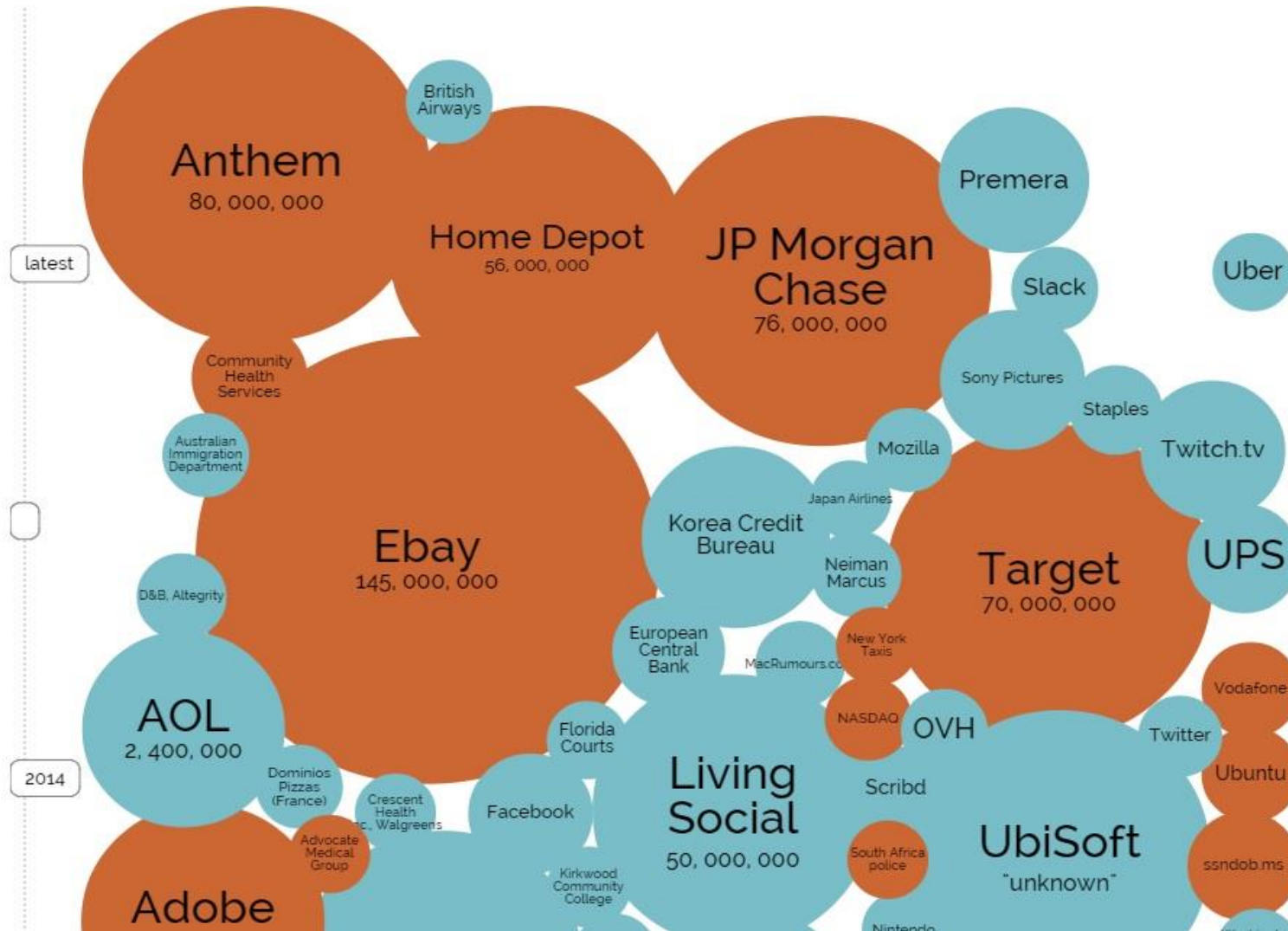


Мониторинг действий пользователей в СУБД – «страшилка» или реальная проблема?

Александр Шахлевич

И напрасно..



Зачем вообще защищать?

- **Критичный актив**

- СУБД – ядро операционной деятельности
- Содержит конфиденциальную информацию компании
- Содержит информацию о клиентах компании
- Вывод СУБД из строя может парализовать работу компании

- **Способы компрометации**

- Простые и доступные инструменты
- Появление более сложных инструментов совершения многоступенчатых атак
- Инсайдер - случайный\скомпрометированный\злоумышленный

- **Обширные возможности**

- Использование «толстых» клиентов
- Использование веб-интерфейса
- Отсутствие встроенного функционала безопасности
- Отсутствие защиты на уровне прикладных систем

Ключевые системы и задачи по отраслям

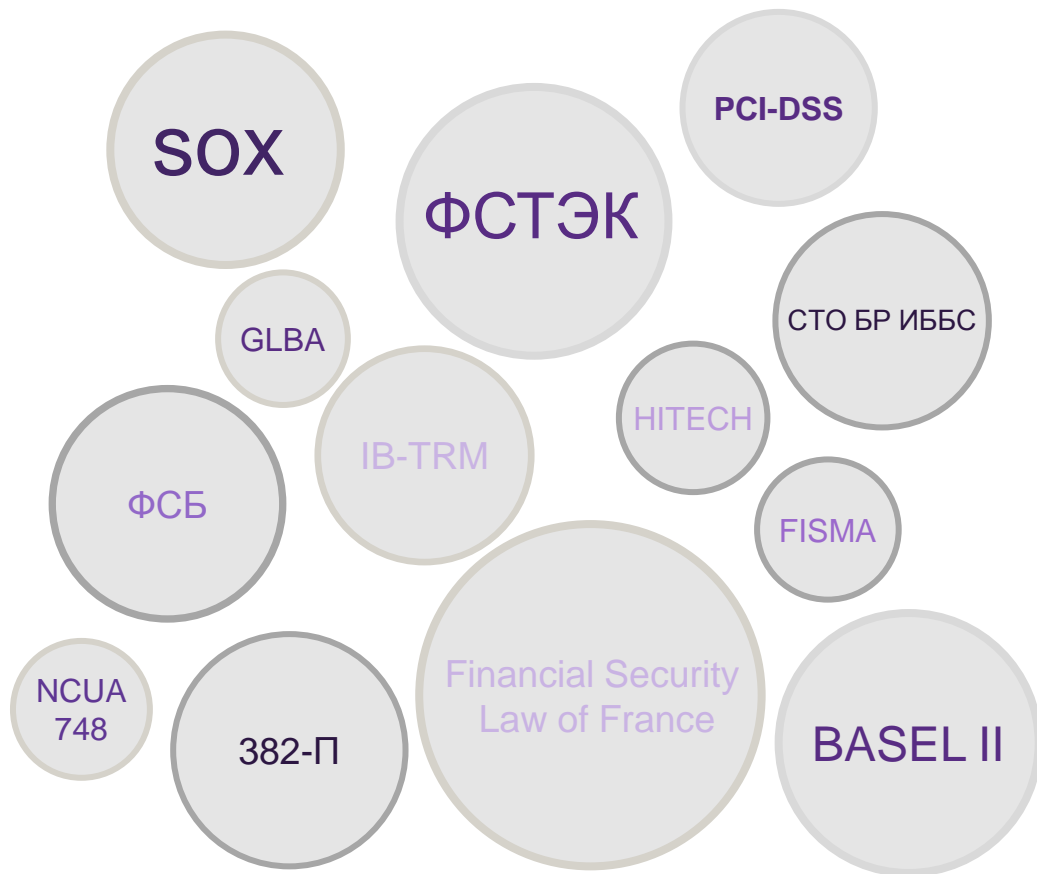
Отрасль	Критичные системы	Задачи
Финансовые компании	<ul style="list-style-type: none">• АБС• ДБО• Процессинг• Платежные системы• Онлайн-сервисы• Корпоративные ресурсы	<ul style="list-style-type: none">• Защита от мошенничества• Обеспечение доступности• Защита данных VIP• Контроль действий администраторов• Управление правами пользователей• Ограничение доступа• Защита ERP• Защита онлайн-сервисов• Соответствие требованиям регуляторов
Страховые, онлайн ритейл	<ul style="list-style-type: none">• Личный кабинет пользователя• Онлайн-сервисы• Корпоративные ресурсы• Логистика	
Телеком	<ul style="list-style-type: none">• Биллинг• Корпоративные ресурсы• Личный кабинет пользователя• Услуги хостинга• Облачные услуги	
Госкомпании	<ul style="list-style-type: none">• Корпоративные ресурсы• Госуслуги• СМЭВ• ГАСУ	
ТЭК и промышленность	<ul style="list-style-type: none">• SCADA• Система учета добычи\выработки• ERP• CRM• Корпоративные ресурсы	

Требования регуляторов

- ФСТЭК №17\21\31
 - ОЦЛ.2 - Контроль целостности информации, содержащейся в базах данных информационной системы
 - ОЦЛ.5 - Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы
 - ЗИС.1 - Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы
- PCI DSS
 - Требование 7. Ограничить доступ к данным держателей карт в соответствии со служебной необходимостью
 - Требование 10. Контролировать и отслеживать любой доступ к сетевым ресурсам и данным держателей карт
- СТО БР ИББС
- 382-П
- SOX
- И другие..

Формальные требования или полезные наставления?

Требования регуляторов



Лучшие практики

Оценка
рисков

Мониторинг и
аудит

Управления
правами

Защита от
атак

Реагирование и отчетность

Что делать?

Ничего!

Ни защиты, ни compliance!

Использовать Native Audit

Можно получить compliance, но реальная защита будет посредственная

Использовать решения класса DAM

Защита и compliance

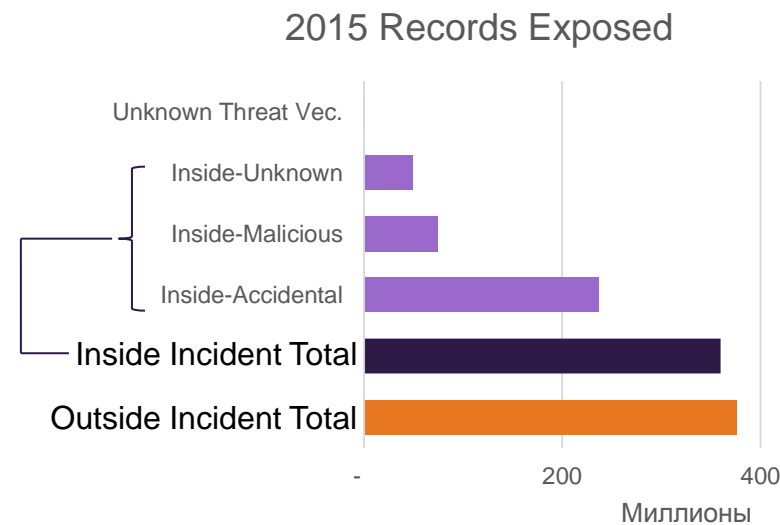
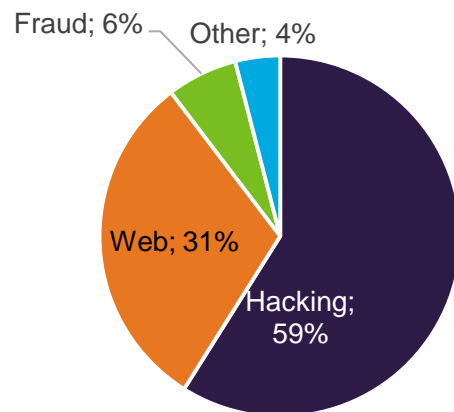
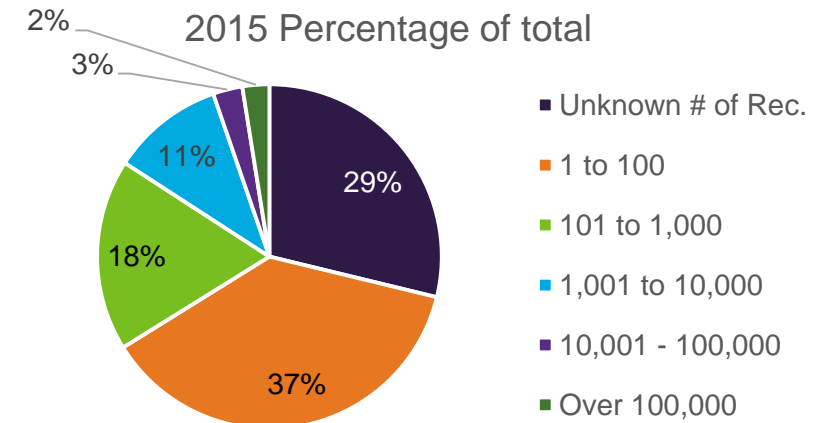
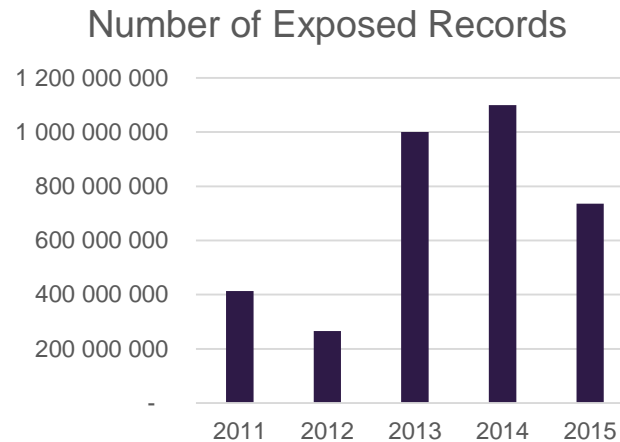
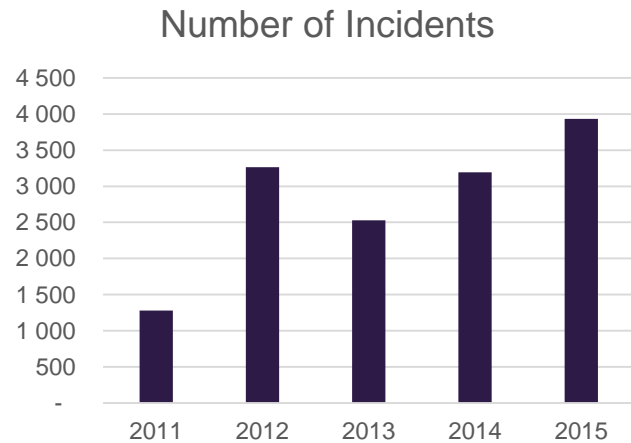


Аудит СУБД? Нет, не слышали..

Почему организации не включают штатный аудит?

- **Влияние на производительность СУБД**
- **Требования к СХД**
- **Ручное составление политик для разрозненных баз**
- Сложность составления и поддержания политики безопасности без инструментов автоматизации
- Большие трудозатраты для эффективного анализа результатов аудита
- Не знают какие политики аудита настраивать
- **Не знают где могут находиться ценные данные**
- Администраторов БД, как правило, мало, и они очень занятые люди

Data breach trends 2015



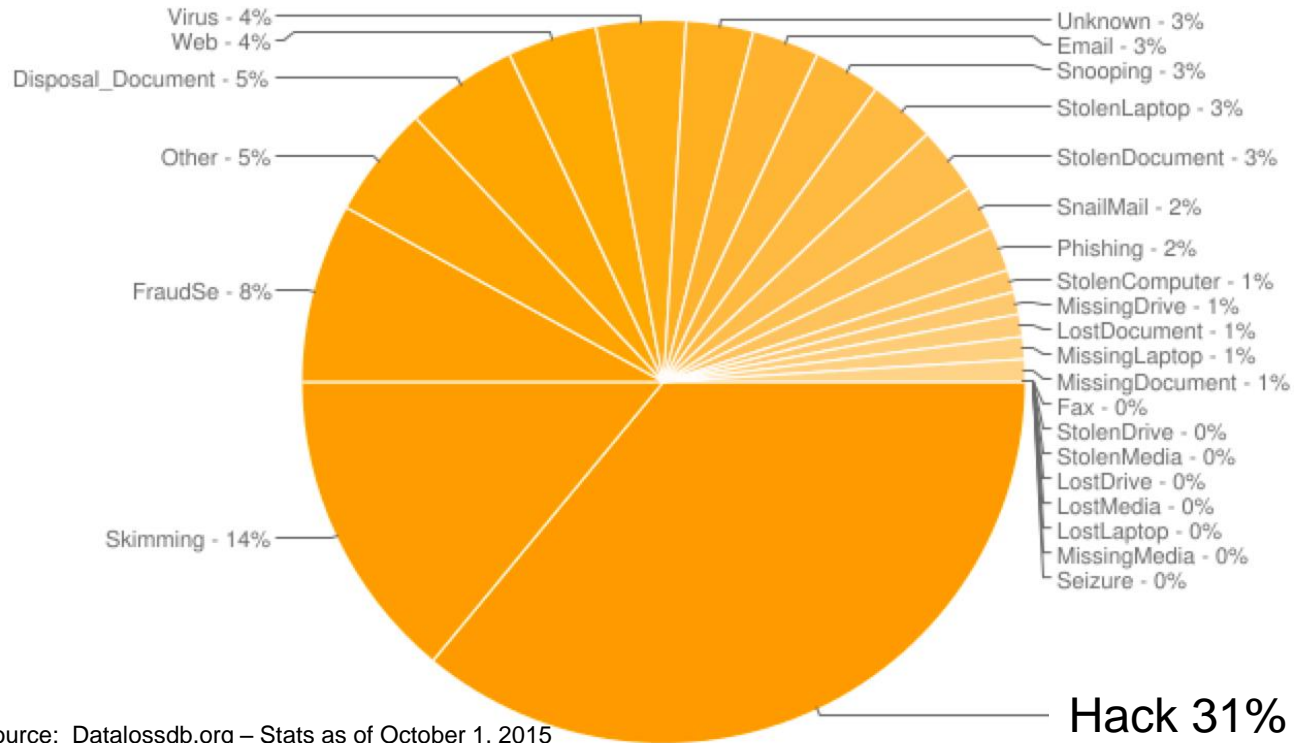
Inside incidents represent 22% of total incidents, but result in 49% of record exposure

Top 3 items stolen:

1. Passwords
2. Email addresses
3. User name

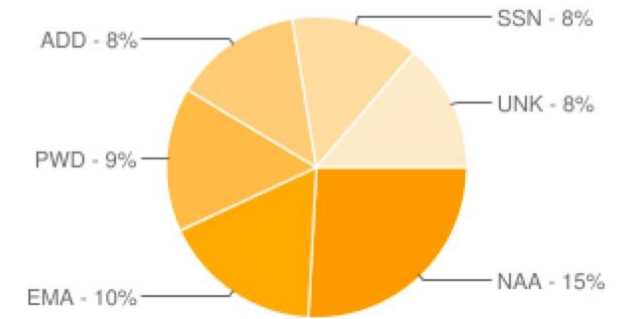
2015 Data Loss: Breach Type and Data Type

Incidents by Breach Type - Current Year



* Source: Datalossdb.org – Stats as of October 1, 2015

Incidents by Data Type - Current Year



1. NAA: Names
 2. EMA: Email Addresses
 3. PWD: Passwords
 4. ADD: Addresses
 5. SSN: Social Security Number
- CCN: No financial data in top categories*



Так давайте включим Native Audit?

Почему Native Audit?

- “Открытый”, “Дешевый”, “Достаточно хороший”
- Так ли это?



Проблемы Native Audit и решений, работающих на его базе

- Сложность администрирования
- Нет идентификации пользователя в трёхзвенной архитектуре
- Нет контроля привилегированных пользователей и администраторов
- Отсутствие механизмов противодействия атакам
- Нет единого средства для гетерогенных сред
- Потеря производительности на уровне 20-70%

Process Hacker [WIN-MQ7VBQ1SR8V\Administrator] +

Hacker View Tools Users Help

Refresh

Options

Find Handles or DLLs

Processes

Services

Network

Disk

Name

LogonUI.exe

lsass.exe

lsmd.exe

msdtc.exe

MsDtsSrvr.exe

MsDtsSrvr.exe

msmdsrv.exe

msmdsrv.exe

notepad.exe

omtsreco.exe

oracle.exe

ProcessHacker.exe

rdpclip.exe

RemoteAgentCli.exe

ReportingServicesServic...

ReportingServicesServic...

services.exe

smss.exe

SMSvcHost.exe

spoolsv.exe

sqlbrowser.exe

CPU

40%

HD I/O

120 Kb/s

Response

1000 ms

TPS

1000

No Audit

Administrator: Command Prompt - go_select.exe 11.11.199.120 1521 orcl system barbabapa 1000000

ies: 1027 millis. TPS: 973

es: 987 millis. TPS: 1013

es: 986 millis. TPS: 1014

es: 965 millis. TPS: 1036

es: 1020 millis. TPS: 980

es: 1056 millis. TPS: 946

es: 1066 millis. TPS: 938

es: 951 millis. TPS: 1051

es: 1016 millis. TPS: 984

es: 982 millis. TPS: 1018

es: 965 millis. TPS: 1036

es: 959 millis. TPS: 1042

es: 1024 millis. TPS: 976

es: 974 millis. TPS: 1026

es: 1019 millis. TPS: 981

es: 1021 millis. TPS: 979

es: 993 millis. TPS: 1007

C:\TEMP>go_select.exe 11.11.199.120 1521 orcl system barbab

1000 time to run 1000 queries: 1220 millis. TPS: 819

2000 time to run 1000 queries: 1088 millis. TPS: 919

3000 time to run 1000 queries: 994 millis. TPS: 1006

4000 time to run 1000 queries: 1000 millis. TPS: 1000

5000 time to run 1000 queries: 966 millis. TPS: 1035

6000 time to run 1000 queries: 932 millis. TPS: 1072

7000 time to run 1000 queries: 932 millis. TPS: 1072

8000 time to run 1000 queries: 938 millis. TPS: 1066

9000 time to run 1000 queries: 965 millis. TPS: 1036

10000 time to run 1000 queries: 968 millis. TPS: 1033

11000 time to run 1000 queries: 950 millis. TPS: 1052

12000 time to run 1000 queries: 944 millis. TPS: 1059

13000 time to run 1000 queries: 984 millis. TPS: 1016

CPU Usage: 55.66%

Physical Memory: 80.93%

Processes: 76

Process Hacker [WIN-MQ7VBQ1SR8V\Administrator]+

Administrator Command Prompt - no select.exe 11.11.199.120 1521 orcl system barbabapa 1000000

Refresh Options Find Handles

Processes Services Network Disk

Name	CPU	HD I/O	Response	TPS
LogonUI.exe				
lsass.exe				
lsm.exe				
msdtc.exe				
MsDtsSrvr.exe				
MsDtsSrvr.exe				
msmdsrv.exe				
msmdsrv.exe				
notepad.exe				
omtsreco.exe				
oracle.exe	39.84	670.45 kB/s	1.24 GB	
ProcessHacker.exe	0.89		13.84 MB	
rdpclip.exe			2.68 MB	
RemoteAgentCli.exe			2.47 MB	
ReportingServicesServic...	0.05		328.82 MB	
ReportingServicesServic...	0.27	864 B/s	138.52 MB	
services.exe	1.84		5.18 MB	
smss.exe			496 kB	
SMSvcHost.exe			30.13 MB	
spoolsv.exe			9.29 MB	
sqlbrowser.exe				

CPU Usage: 50.49% Physical Memory: 80.96% Processes: 76

ies: 925 millis. TPS: 1081
 es: 918 millis. TPS: 1089
 es: 938 millis. TPS: 1066
 es: 948 millis. TPS: 1054
 es: 934 millis. TPS: 1070
 es: 909 millis. TPS: 1100
 es: 1061 millis. TPS: 942
 es: 926 millis. TPS: 1079
 ies: 918 millis. TPS: 1089
 ies: 955 millis. TPS: 1047
 ies: 914 millis. TPS: 1094
 ies: 917 millis. TPS: 1090
 ies: 943 millis. TPS: 1060
 ies: 971 millis. TPS: 1029
 ies: 1008 millis. TPS: 992
 ies: 1005 millis. TPS: 995
 ies: 923 millis. TPS: 1083
 ies: 909 millis. TPS: 1100
 queries: 936 millis. TPS: 1068
 queries: 946 millis. TPS: 1057
 queries: 930 millis. TPS: 1075
 queries: 920 millis. TPS: 1086
 queries: 971 millis. TPS: 1029
 queries: 938 millis. TPS: 1066
 queries: 941 millis. TPS: 1062
 queries: 1400 millis. TPS: 714
 queries: 1811 millis. TPS: 552
 queries: 1848 millis. TPS: 541
 queries: 2080 millis. TPS: 480
 queries: 1859 millis. TPS: 537
 queries: 1829 millis. TPS: 546
 queries: 1729 millis. TPS: 578
 queries: 1919 millis. TPS: 521
 queries: 1834 millis. TPS: 545



01:16



-01:32

Process Hacker [WIN-MQ7V8Q15R8V\Administrator] - Administrator Command Prompt - select sys 11.11.199.120 1521 orcl system barbabapa 1000000

Hacker View Tools Users Help

Refresh Options Find Handle

Processes Services Network Disk

Name

	CPU	HD I/O	Response	TPS
No Audit	40%	120 Kb/s	1000 ms	1000
Native Audit	40%	600 Kb/s	2000 ms	500
DAM Agent	42%	110 Kb/s	1000 ms	1000

Interruptions

java.exe

LogonUI.exe

lsass.exe

lsmd.exe

msdtc.exe

MsDtsSrvr.exe

MsDtsSrvr.exe

msmdsrv.exe

msmdsrv.exe

notepad.exe

omtsreco.exe

oracle.exe

Process Hacker.exe

rdpclip.exe

RemoteAgent.exe

RemoteAgentCli.exe

RemoteAgentCtrl.exe

RemoteAgentWd.exe

ReportingServicesServic...

ReportingServicesServic...

CPU Usage: 55.68% Physical Memory: 88.47% Processes: 82

299000 time to run 1000 queries: 948 millis. TPS: 1054

300000 time to run 1000 queries: 950 millis. TPS: 1052

301000 time to run 1000 queries: 2253 millis. TPS: 443

302000 time to run 1000 queries: 969 millis. TPS: 1031

303000 time to run 1000 queries: 920 millis. TPS: 1086

304000 time to run 1000 queries: 1006 millis. TPS: 994

305000 time to run 1000 queries: 993 millis. TPS: 1007

306000 time to run 1000 queries: 1105 millis. TPS: 904

307000 time to run 1000 queries: 923 millis. TPS: 1083

308000 time to run 1000 queries: 1107 millis. TPS: 903

309000 time to run 1000 queries: 1193 millis. TPS: 838

310000 time to run 1000 queries: 1253 millis. TPS: 798

311000 time to run 1000 queries: 970 millis. TPS: 1030

312000 time to run 1000 queries: 1020 millis. TPS: 980

313000 time to run 1000 queries: 1247 millis. TPS: 801

314000 time to run 1000 queries: 1259 millis. TPS: 794

time to run 1000 queries: 1057 millis. TPS: 946

time to run 1000 queries: 1153 millis. TPS: 867

time to run 1000 queries: 969 millis. TPS: 1031

time to run 1000 queries: 994 millis. TPS: 1006

time to run 1000 queries: 925 millis. TPS: 1081

time to run 1000 queries: 953 millis. TPS: 1049

time to run 1000 queries: 918 millis. TPS: 1089

time to run 1000 queries: 937 millis. TPS: 1067

time to run 1000 queries: 930 millis. TPS: 1075

time to run 1000 queries: 974 millis. TPS: 1026

time to run 1000 queries: 1105 millis. TPS: 904

time to run 1000 queries: 993 millis. TPS: 1007

time to run 1000 queries: 946 millis. TPS: 1057

time to run 1000 queries: 970 millis. TPS: 1030

time to run 1000 queries: 969 millis. TPS: 1031

time to run 1000 queries: 925 millis. TPS: 1081

time to run 1000 queries: 850 millis. TPS: 1176

time to run 1000 queries: 951 millis. TPS: 1051

Сопряженные расходы

- Дополнительные расходы при использовании Native Audit



Затраты на Hardware и
Software



Дополнительные СХД



Человеческие
ресурсы

Решения класса Database Activity Monitoring

Что входит в процесс защиты БД?

- Поиск конфиденциальной информации
- Определение, настройка и поддержание политик безопасности
 - Отдельные политики для безопасности и аудита
- Мониторинг нарушений политик безопасности
- Динамическое профилирование
 - Выявление поведенческих аномалий
- Оповещение, карантин и блокировка на выбор
- Отчетность в соответствии с выбранным стандартом или пользовательским шаблоном



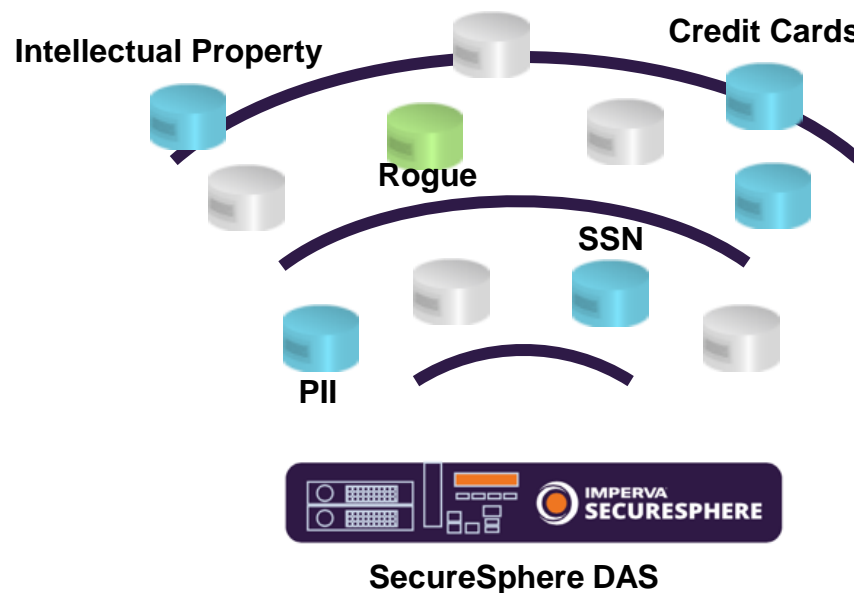
Имя	Паспорт	Зарплата
Петр Иванов	4600№300200	77,000
Начальник Петра И	4700№100000	7,700,000

Поиск и классификация

Поиск и классификация

Поиск сущностей БД и классификация конфиденциальной информации

- Поиск активных сущностей в сети
- Определение мошеннических БД
- Определение областей мониторинга

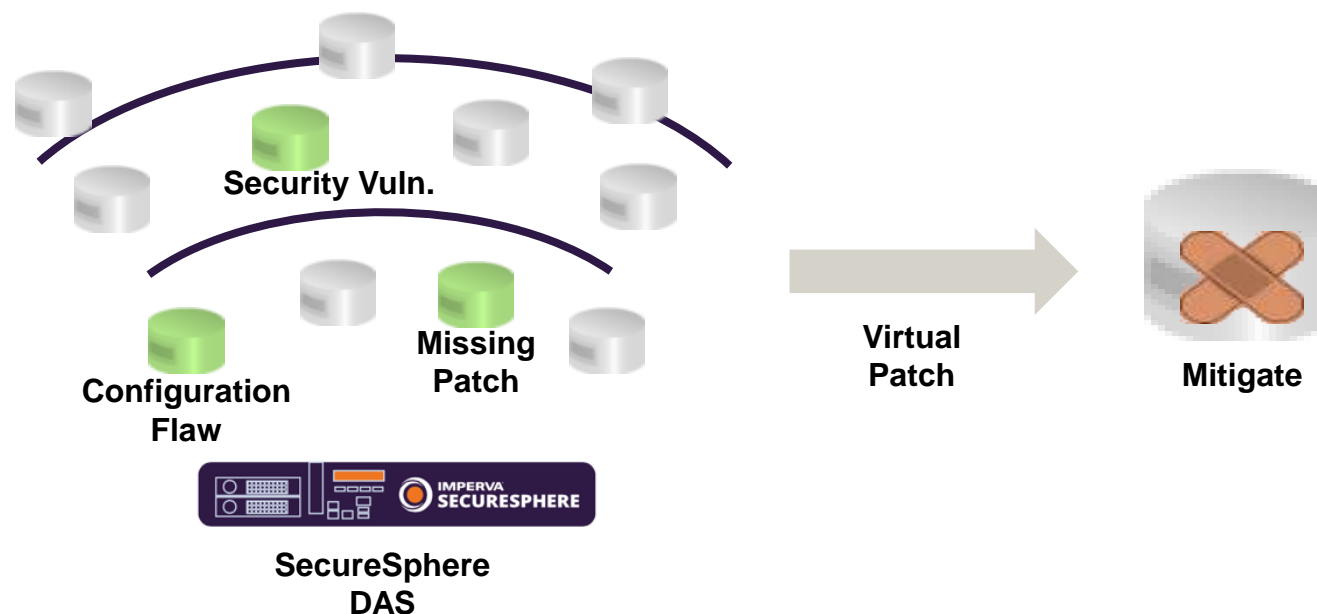


Анализ рисков и закрытие уязвимостей ПО

Сканирование
уязвимостей и их
устранение

Поиск и устранение
уязвимостей и ошибок
конфигурации

- Автоматизированный процесс поиска и закрытия уязвимостей

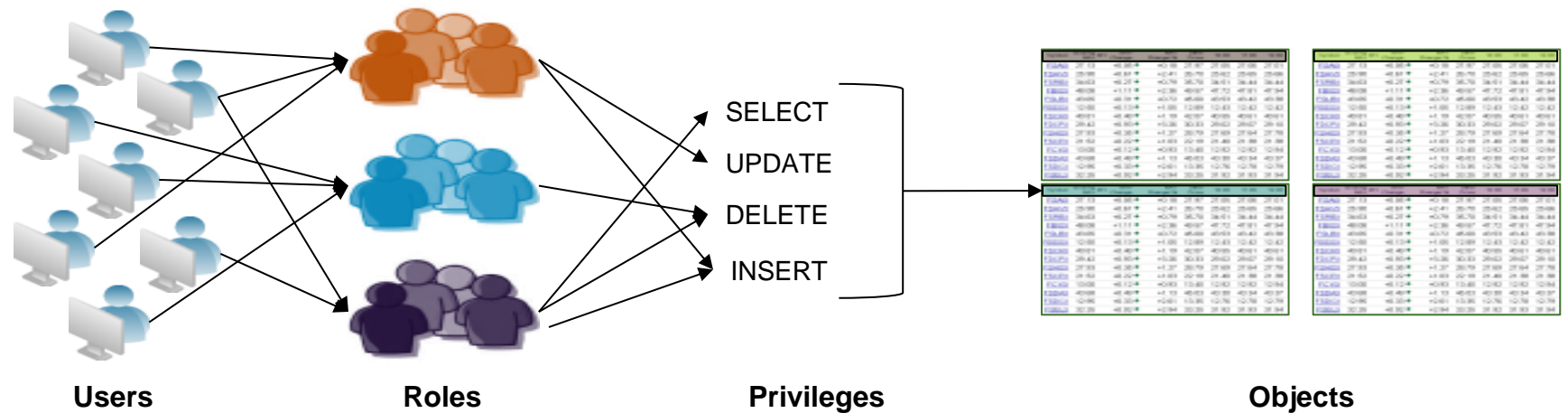


Анализ и управление правами пользователей

Анализ прав доступа

Сканирование и анализ предоставленных прав

- Устранение нежелательного доступа
- Определение собственников информации
- Снижение риска утечки



Аудит всей активности

Активный аудит

Сбор и запись всей активности в СУБД

- Выполнение требований регуляторов
- Независимое хранилище для анализа инцидентов



Мониторинг привилегированного доступа

Мониторинг привилегированных пользователей

- Разделение полномочий на практике
- Мониторинг всей активности, включая локальную
- Блокировка при необходимости



Обеспечение безопасности в реальном времени

Оповещение

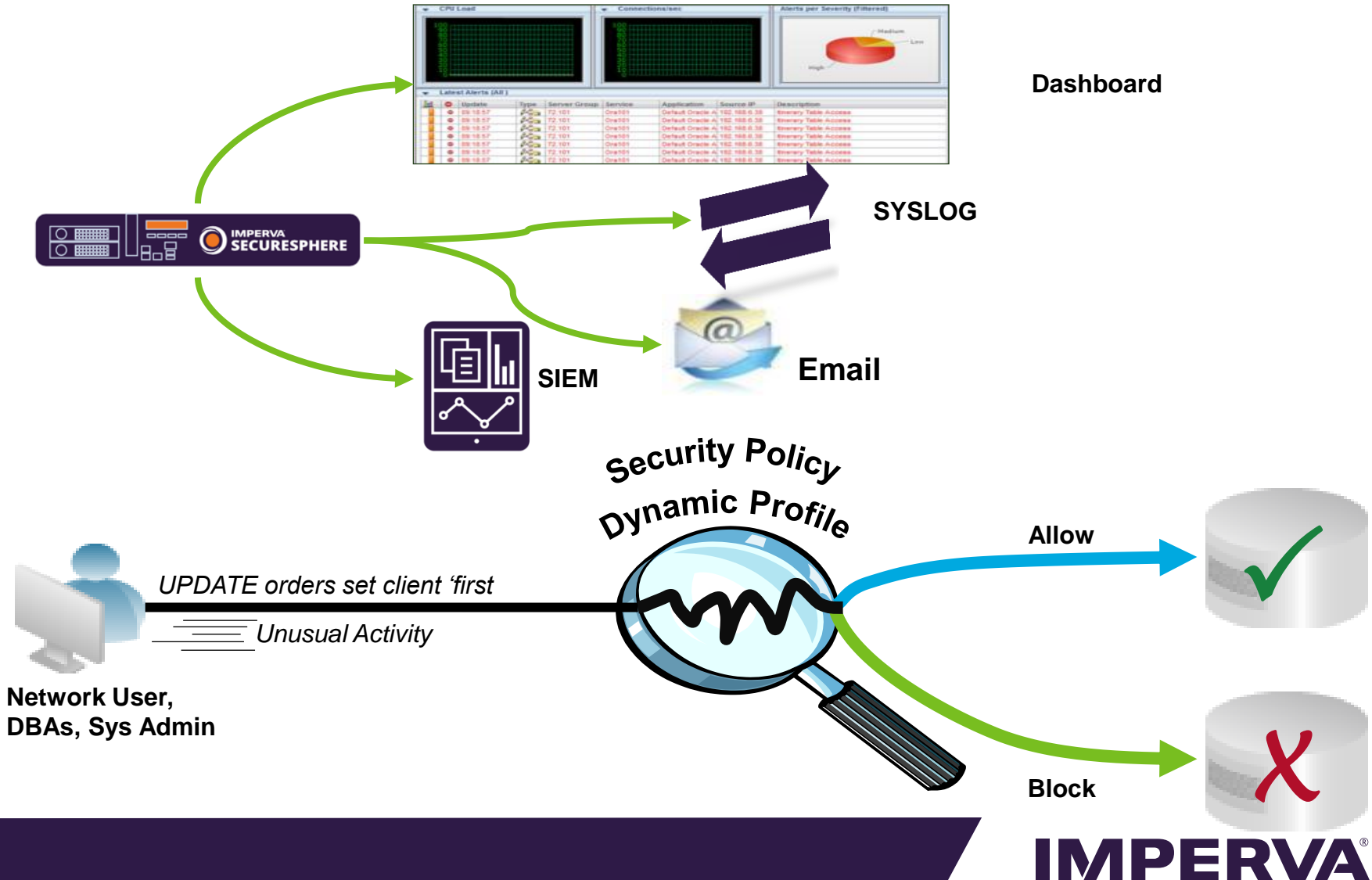
Оповещение в реальном времени о подозрительной активности пользователей

- Быстрая локализация атак
- Предотвращение кражи данных

Блокировка

Мониторинг доступа к БД

- Предотвращение неавторизованного доступа
- Защита конфиденциальной информации



Анализ и отчетность

Отчетность

Наглядная отчетность

- Анализ угроз
- Отчет по соответствию требованиям регуляторов
- Пользовательские отчеты

Аналитика

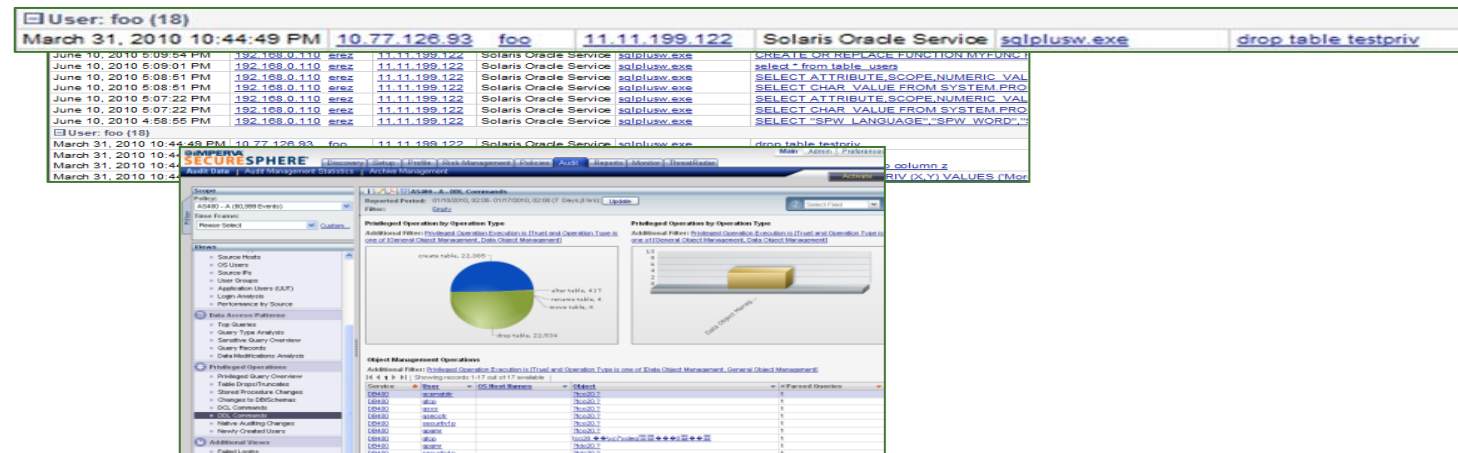
Детализированные логи аудита, интерактивные дашборды и отчеты

- Помощь при расследовании инцидентов
- Автоматизация безопасности

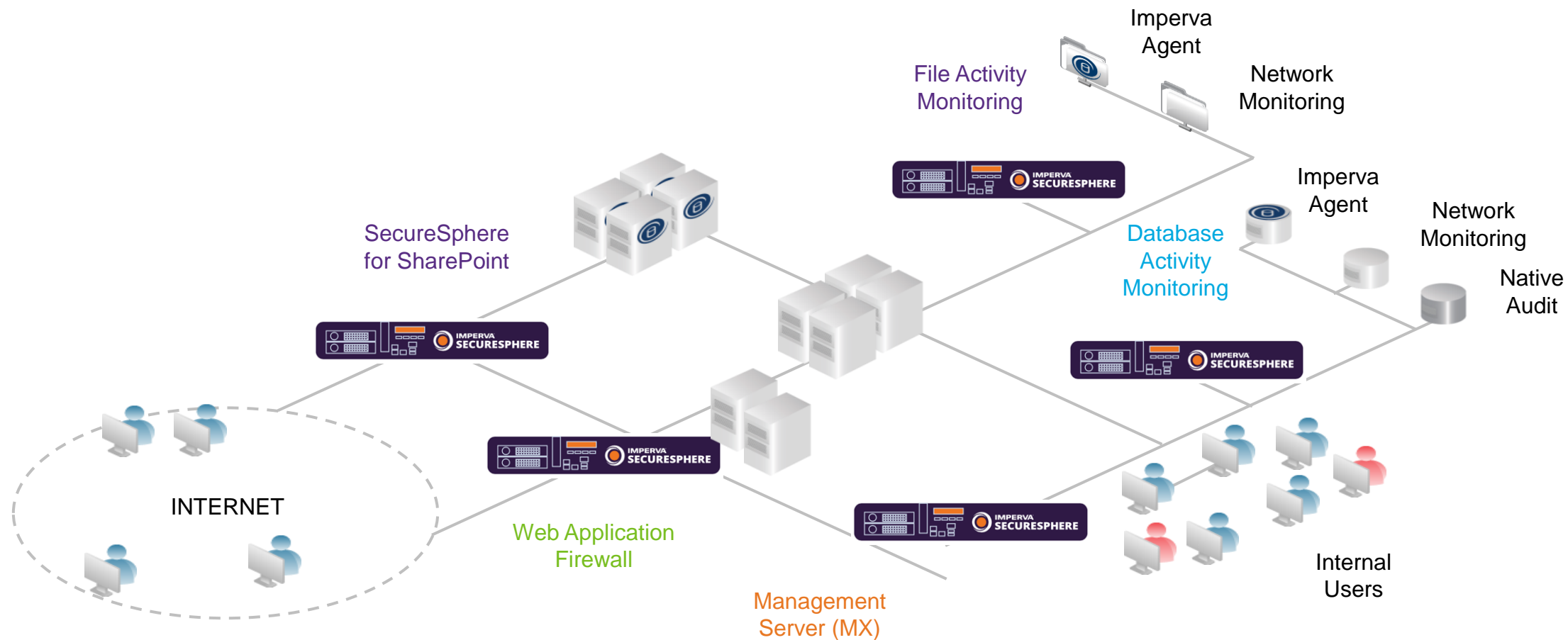


PCI, HIPAA, SOX...

Custom



Архитектура решения



Ключевой функционал решений Imperva DAM

1. Поиск
2. Классификация
3. Мониторинг
4. Аудит
5. Защита
6. Отчетность

Discover rogue databases	Map and classify sensitive information	Default and custom policy trees
300+ Out of the box policies	Automate user rights analysis and verification	Id and track vulnerabilities
Simple policy and rule creation	Data enrichment	Activity monitoring
Privileged user monitoring	Pan-enterprise reporting	Investigate and analyze

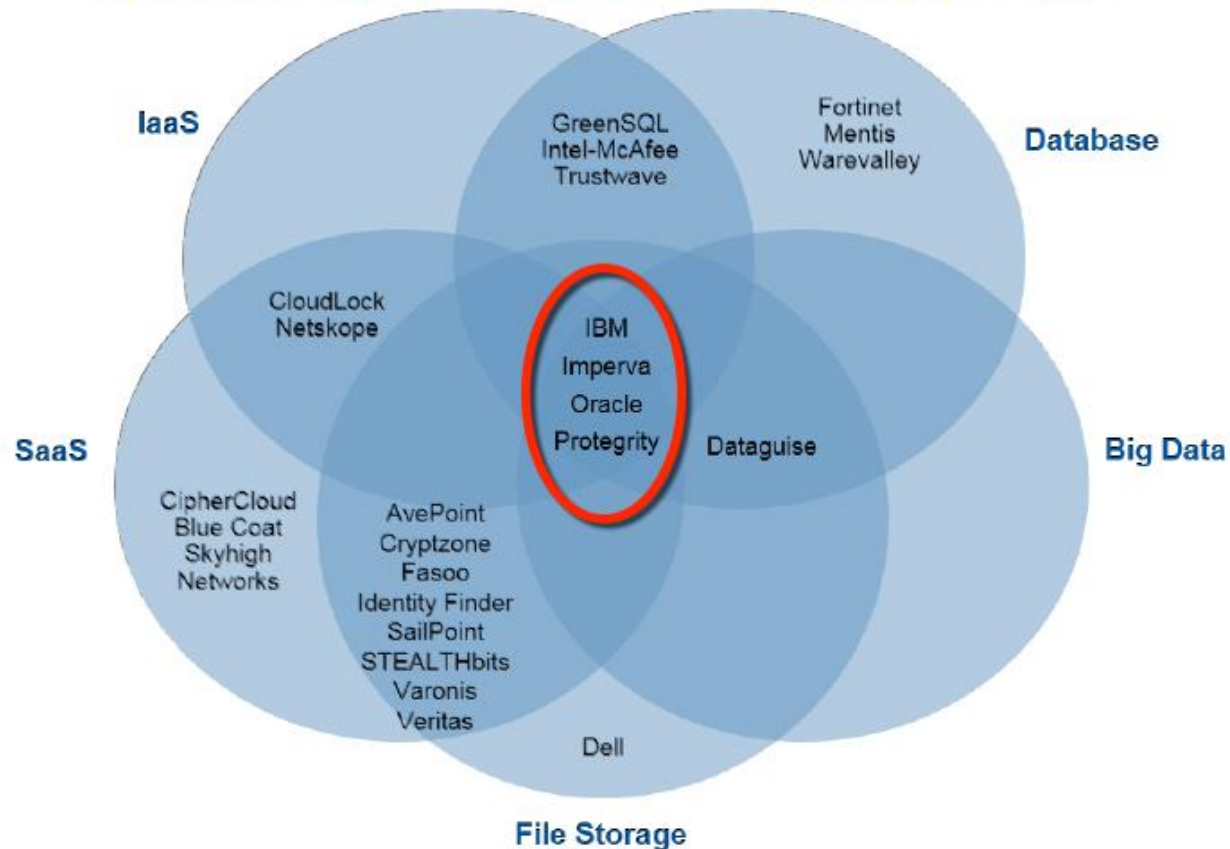
Поддержка широкого спектра СУБД

Database	Supported Database Versions
Caché	2011.1
DB2 LUW	7.2, 8, 9, 9.5, 9.7, 10.0, 10.5
Informix	7.31, 9.x, 10.x, 11.0-11.5, 11.7, 12.1
MS-SQL	7, 2000, 2005, 2008, 2008 R2, 2012, 2014
MySQL	4.1, 5.x
Netezza	4.x, 5.0, 6.0
Oracle	8i, 9i, 10g, 11g, 12c
Sybase ASE	11.9, 12.0, 12.5.x, 15.0-15.7
Sybase IQ	12.5, 12.6, 12.7, 15.0-15.4
Progress Openedge	10.1c, 10.2a, 10.2b
Teradata	2.6, 12, 13.0, 13.1, 14 Note: Auditing Teradata versions 2.6 and 12 requires enabling of native auditing and is supported using the SecureSphere Log Collector framework.
PostgreSQL	8.4 - 9.3
IMS for z/OS	11, 12, 13
DB2 for z/OS	10, 11

Аудит СУБД с точки зрения нужд различных департаментов

Objective	IT	DBAs	Security	Risk and Compliance	Privacy & Legal	Application Development
Regulatory compliance	✓	✓	✓	✓	✓	✓
Corporate best practice policy adherence	✓	✓	✓	✓	✓	✓
Forensic data security visibility and investigation	✓		✓	✓	✓	
Change control reconciliation	✓		✓	✓		✓
DB performance and optimization	✓	✓				
Application development testing and verification			✓	✓	✓	✓

Imperva – лидер в области аудита и защиты данных (DCAP) по мнению Gartner



	Data Silos					DCAP Capabilities				
	Database	Files	Big Data	SaaS	IaaS	Integrates Policies Across Multiple Silos	Data Classification Is Integrated	Integrated Data Discovery Across Silos	Application Layer PAM	Data Protection Policy Integration
AvePoint		Y		Y		Y	Y	Y		Y
Blue Coat				Y			Y			Y
CipherCloud				Y			Y			Y
CloudLock				Y	Y	Y	Y	Y		Y
Cryptzone		Y		Y		Y	Y	Y		Y
Datagui	Y	Y	Y			Y	Y	Y	Y	Y
Dell		Y					Y	Y	Y	
GreenSQL	Y				Y	Y	Y	Y		Y
Fasoo		Y		Y			Y	Y		Y
Fortinet	Y									
IBM	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Identity Finder		Y		Y		Y	Y	Y	Y	Y
Imperva	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
Intel-McAfee	Y				Y					
Mentis		Y					Y			Y
Netskope				Y	Y	Y	Y	Y		Y
Oracle	Y	Y	Y	Y	Y	Y			Y	Y
Protegrity	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y
SailPoint		Y		Y		Y				
Skyhigh Networks				Y			Y			Y
STEALTHbits		Y		Y		Y	Y	Y	Y	Y
Veritas		Y		Y		Y			Y	
Trustwave	Y				Y		Y			
Varonis		Y		Y		Y	Y	Y	Y	
WareValley	Y						Y			

Imperva – один из немногих производителей, на 100% выполняющих требования Gartner к решениям класса DCAP

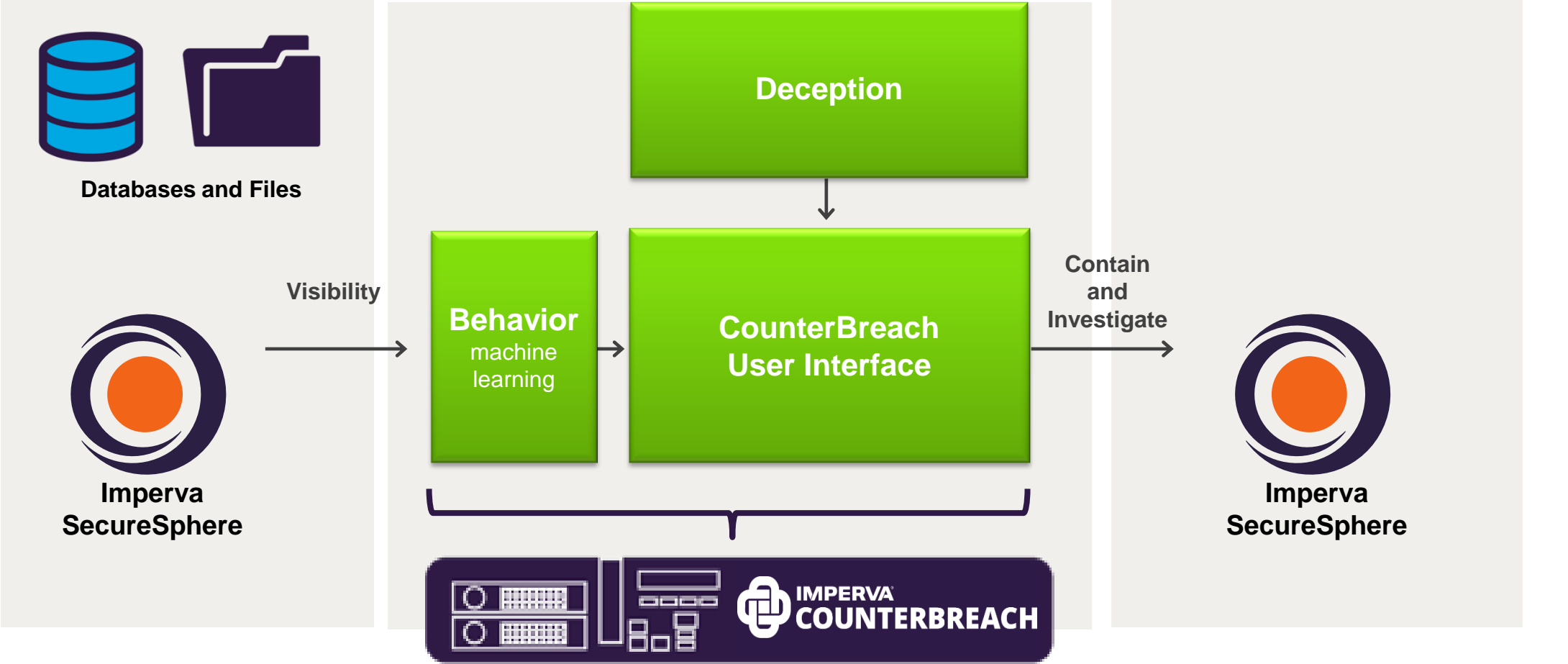
Gartner Market Guide for DCAP,
December 15, 2015

Продвинутый анализ активности пользователей

MONITOR

LEARN AND DETECT

**BLOCK /
QUARANTINE**



Детальный поведенческий анализ пользовательской активности



CounterBreach

- Новая технология
- Динамически определяет вредоносную активности на основе поведенческого движка
- Использует машинное обучение
- Приоритет на безопасности данных

Database Dynamic Profiling

- Более старая технология
- Быстрый способ определения действующих прав доступа
- Использует статический whitelist
- Фокус – мониторинг и автоматизация профилирования

Основывается на:	
User Data Access	Data Object Access
Database Tables and Files	
Access Types	
Data Types	
Account Types	
Source of Data Access	
Time & Length of Data Access	
Peer Group Comparison	

Desception – идентификация скомпрометированных устройств



- Разоблачение злоумышленников на стадии разведывательных действий перед атакой
- Ловушки имитируют ключевые ресурсы компании
- Срабатывание ловушки отображается как поведенческая аномалия в CounterBreach
- Дополняет поведенческий анализ

Вопросы?