Решения Imperva для защиты веб-приложений и СУБД

Шахлевич Александр
RSD Russia

Alexandr.Shakhlevich@imperva.com

“Есть два типа организаций: одни, которые допускают возможность утечки данных, и те, кто об этом просто не знают.”

Shawn Henry, Former FBI Executive Assistant Director (NY Times, April 2012)

Направленные атаки

Report: Hacker breached SC database 2 ways

Records lost: 4M
Population: 5M
= 80%

Направленные, эффективные, незамеченные

Кража учетных данных через фишинговые атаки и зловреды

13-Aug-12

Разведка и получение информации об инфраструктуре, бизнес-процессах

27-Aug-12

Повышение привилегий, кража административных учетных данных

29-Aug-12 - 11-Sept-12

Получение полного доступа к информации – утечка\модификация, уничтожение

12-Sept-12 - 14-Sept-12

IMPERVA

Insider Threat Defined!

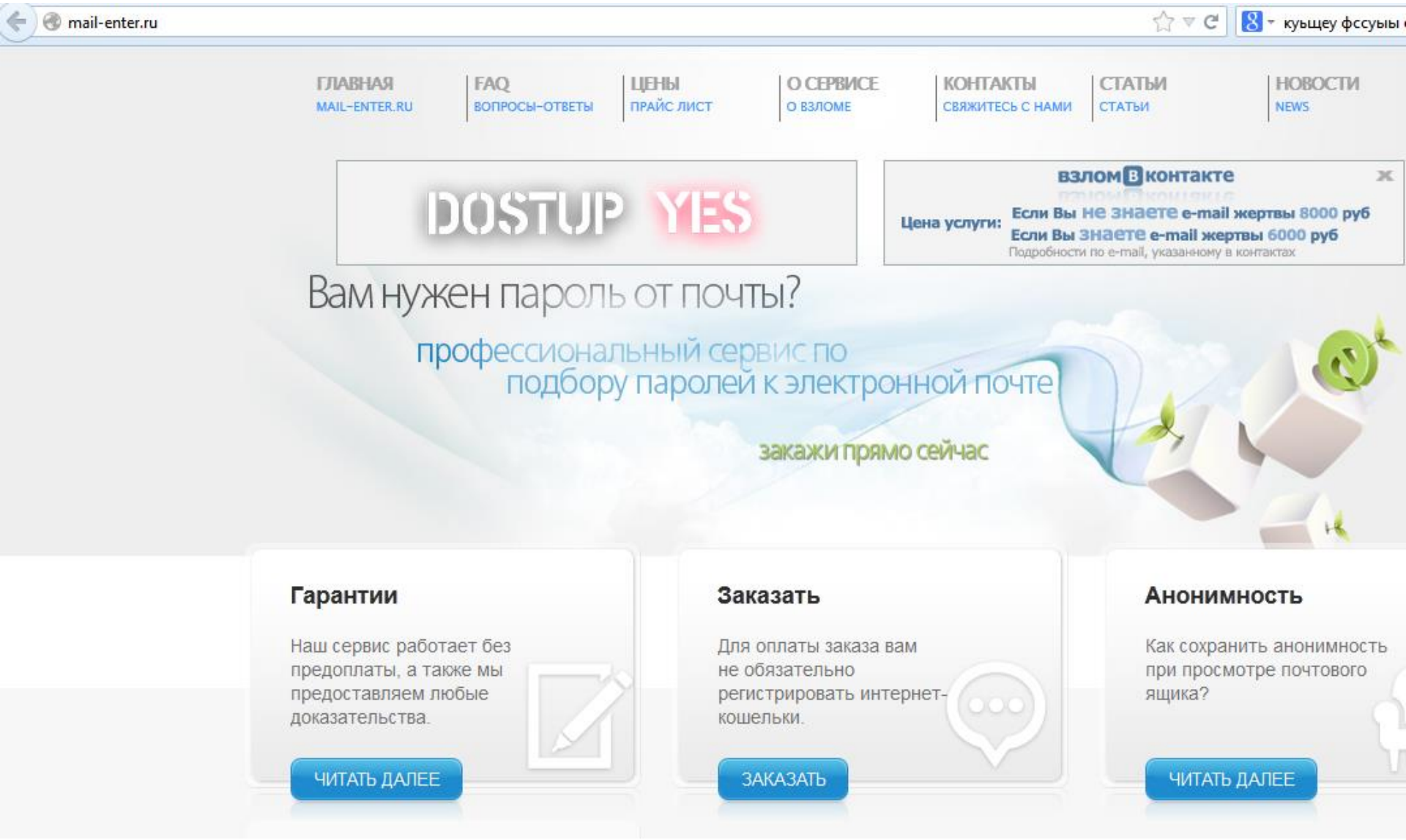
Угроза инсайда

Доверенный пользователь, имеющий легитимный доступ и совершающий утечку интелектуальной собственности компании или другой бизнес-критичной информации.

Зачем он это делает:

- Намеренно
- Случайно
- Скомпрометирован

Взгляд изнутри



IMPERVA

Verizon Data Breach Investigations Report 2013

- Жертвы, 38% - крупные корпорации, из них:
  - 37% - финансовые организации
  - 24% - ритейл
  - 20% - ТЭК, промышленный сектор
- Преступники:
  - 92% - внешние пользователи
  - 14% - злоумышленные инсайдеры (нарастающая угроза)
- Причины утечек:
  - 52% - разновидности веб-хакинга
  - 76% - кража учетных данных
  - 13% - результат завышенных прав пользователей
- Интересные особенности:
  - 78% - атак низкой сложности
  - 54% - скомпрометирован веб-сервер
  - 66% - инцидентов выявлено внешними сторонами
  - 66% - потрачены месяц и более на выявление атаки

Вектора атак

Table 10. Compromised assets by percent of breaches and percent of records*

Type	Category	All Orgs		Larger Orgs	
POS server (store controller)	Servers	50%	1%	2%	<1%
Desktop/Workstation	User devices	18%	34%	12%	36%
Automated Teller Machine (ATM)	User devices	8%	<1%	13%	<1%
Web/application server	Servers	6%	80%	33%	82%
Database server	Servers	6%	96%	33%	98%
Mail server	Servers	3%	2%	10%	2%
Payment card (credit, debit, etc.)	Offline data	3%	<1%	0%	<1%
Cashier/Teller/Waiter	People	2%	<1%	2%	<1%
Pay at the Pump terminal	User devices	2%	<1%	0%	<1%
File server	Servers	1%	<1%	5%	<1%
Laptop/Netbook	User devices	1%	<1%	5%	<1%
Remote access server	Servers	1%	<1%	7%	<1%
Call Center Staff	People	1%	<1%	7%	<1%

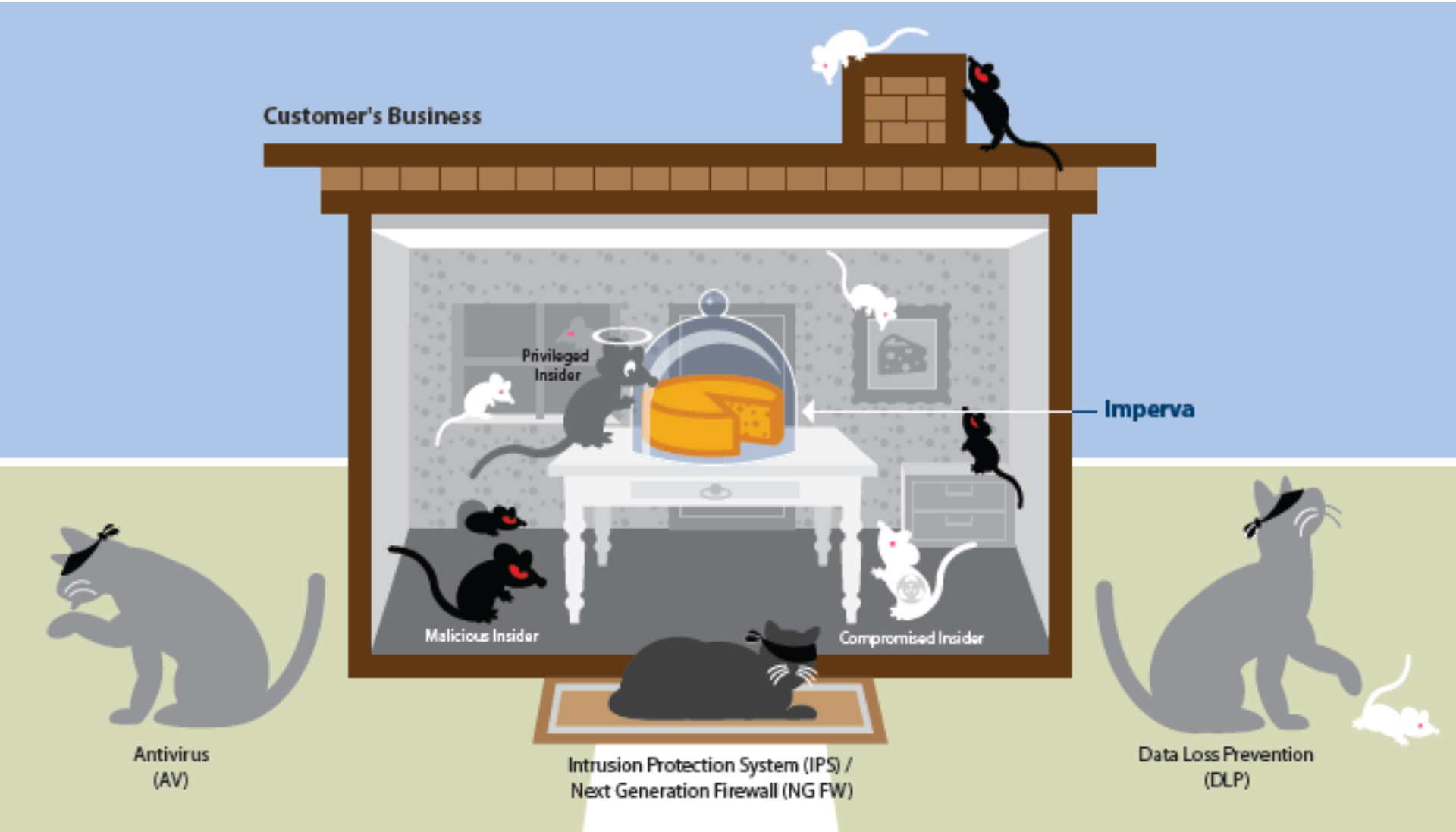
Персональные данные, финансовая информация

Интеллектуальная собственность, конкурентные преимущества

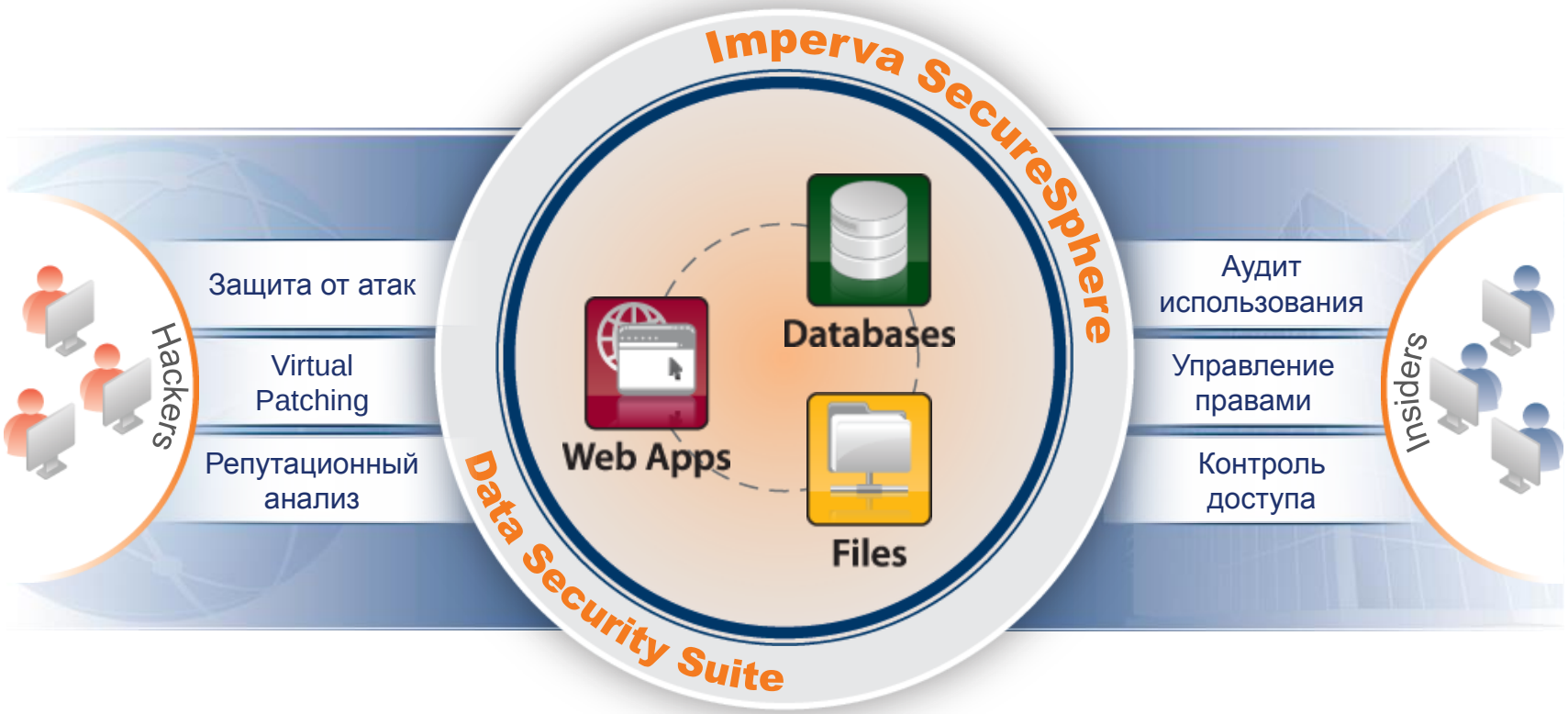
IMPERVA

Подход Imperva

- Защитите то, что действительно ценно!



Комплексный портфель решений



IMPERVA

Imperva SecureSphere

- Комплексное решение для защиты данных
- Простота развертывания и администрирования
- Соответствие стандартам информационной безопасности, в том числе ФСТЭК №17, 21
- Собственный исследовательский центр

PCI Security Standards Council Member

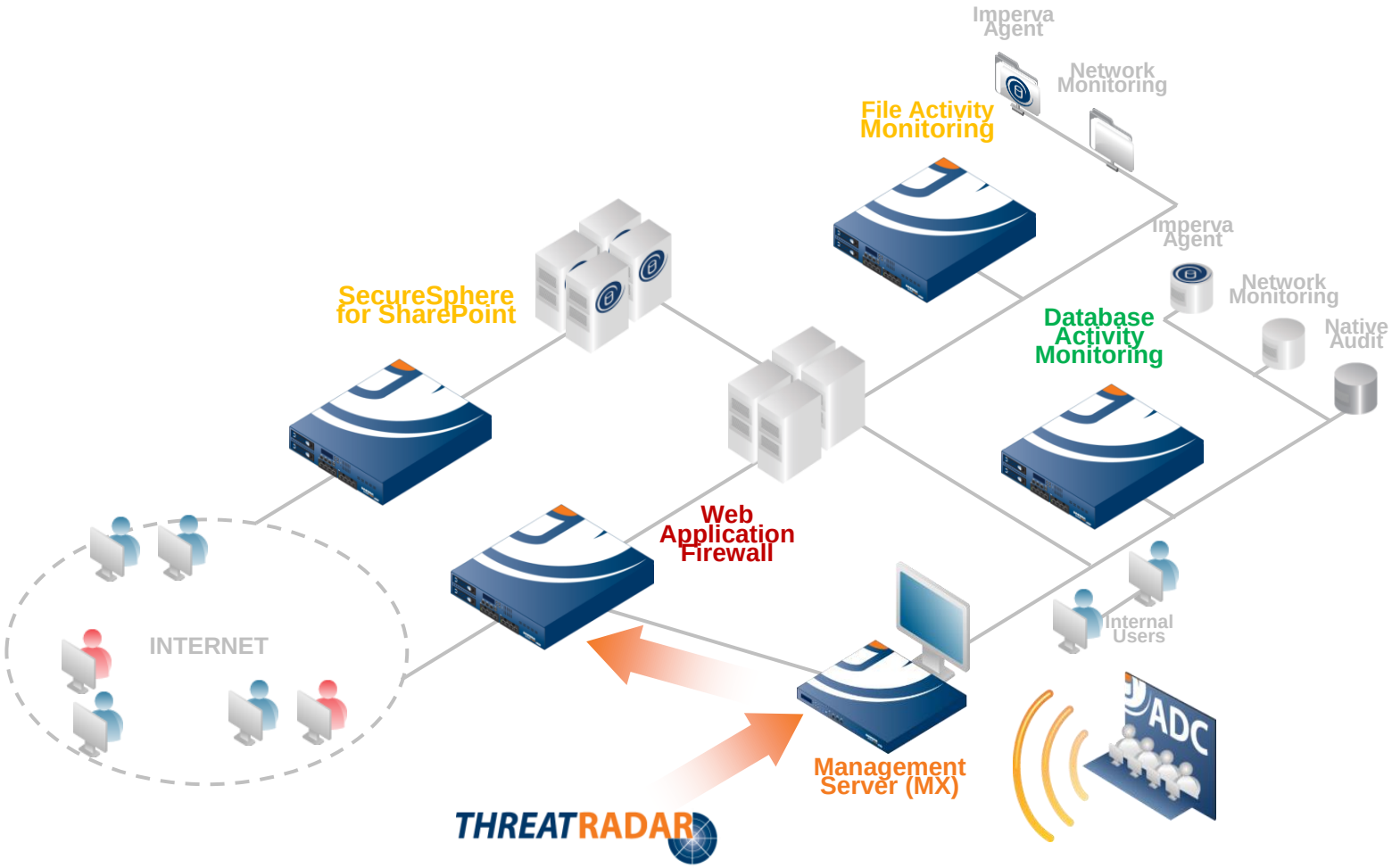
Sybase IQ

ORACLE Microsoft IBM MySQL

SYBASE TERADATA Raising Intelligence Informix

IMPERVA

Архитектура решения



Imperva дополняет имеющуюся инфраструктуру

- Специализированные решения для SAP, OEBS, PeopleSoft, SharePoint

- Интеграция со сторонними производителями:
  - Vulnerability Scanning
  - SIEM
  - DLP
  - Fraud Management
  - Endpoint Protection
  - Cloud

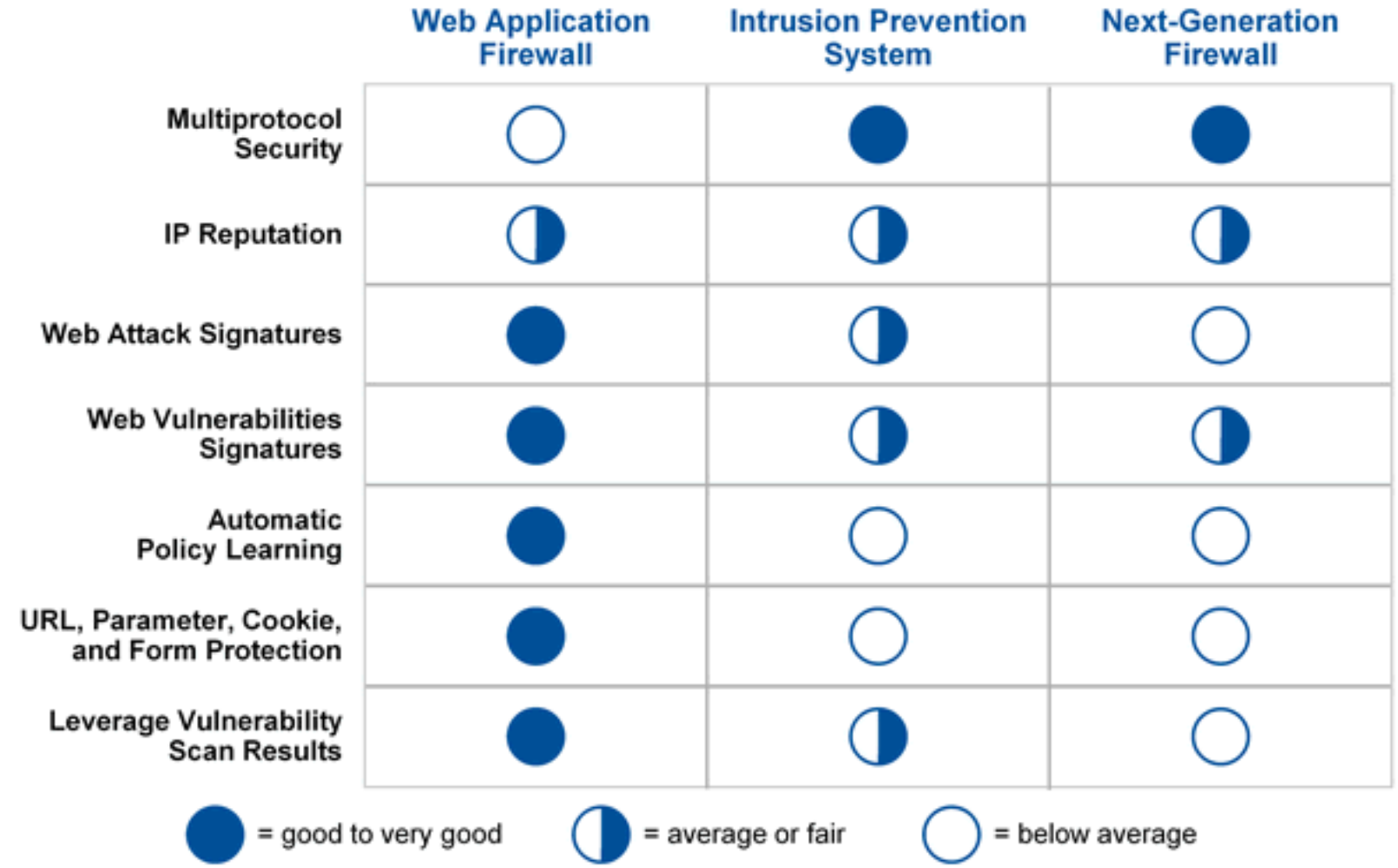
Позиционирование на рынке

ТОП-10 угроз OWASP, 2013

1) Injection
   - Защита от SQL, LDAP, Xpath и OS injection
2) Broken Authentication and Session Management
   - Защита и контроль процесса аутентификации и пользовательских сессий
3) Cross-Site Scripting (XSS)
   - Сигнатурные и поведенческие механизмы защиты
4) Insecure Direct Object References
5) Security Misconfiguration
6) Sensitive Data Exposure
   - Контроль возвращаемой информации
7) Missing Function Level Access Control
8) Cross-Site Request Forgery (CSRF)
   - Корреляционные политики безопасности
9) Using Components with Known Vulnerabilities
   - Технология Virtual Patching
10) Unvalidated Redirects and Forwards

Две проблемы.. Два решения!

Figure 2. Main Differences Between WAF, IPS and NGFW



IP = Internet Protocol

Source: Gartner (February 2014)

Концепция WAF Testing Framework (WTF)

- Инструмент для определения реальной эффективности IPS\NGFW\WAF при защите от веб-атак
- Комбинация легитимного и вредоносного трафика
- Оценка двух параметров:
  - Good traffic being blocked (False Positives)
  - Bad traffic being overlooked (False Negatives)
- Дает наглядное представление о балансе между безопасностью и непрерывностью бизнеса
- **Скачивание и тестирование – бесплатно!**

DB Security

Подходы к аудиту доступа к СУБД

- Два распространенных подхода

1. Встроенные возможности СУБД по аудиту (Native Audit)
   - Различные варианты с использованием самописных скриптов\анализаторов и\или интеграция с SIEM

2. Использование внешних решений для аудита
   - «Наложенные» решения, например Imperva

Почему Native Audit?

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

Проблемы Native Audit и решений, работающие на его базе

- **Потеря производительности на уровне 15-20%**
- Сложность администрирования
- «Слепа» в трёхзвенной архитектуре
- Отсутствие контроля привилегированных пользователей и администраторов
- Отсутствие сильных механизмов противодействия атакам
- Нет единого средства для гетерогенных сред

Сопряженные расходы

- Дополнительные расходы при использовании Native Audit

Затраты на Hardware и Software

Дополнительные СХД

Человеческие ресурсы

Пример

Модель применения	Аудит всей активности
Инфраструктура	7 DB Servers (7 Oracle)
Текущее решение	Using Native Database Auditing
Расчетный период	1 год

Затраты на Hardware и Software

Просадка производительности серверов СУБД при использовании Native Audit составляет **~15%**(1)

(1) Based on industry metrics and Vendor Guidelines, “Cost Effective Security and Compliance with Oracle Database 11g Release 2 Whitepaper, March 2011”

Hardware and Software

	Native Auditing
Просадка производительности при использовании Native Audit (1)	15%
Кол-во аппаратных ресурсов, выделенных на аудит, шт (2)	1,05
Стоимость аппаратных ресурсов, за сервер	~ $8,000
Стоимость ПО, за сокет\процессор	$14,000
Среднее количество процессоров на сервер	12
Стоимость ПО и аппаратных ресурсов для реализации функций аудита	**$184.800** (1,05 x 8,000) + (1,05 x 12 x 14,000)

(1) Additional database software and servers to overcome performance degradation due to native audit

(2) All prices are list prices

Хранение результатов аудита

Средняя цена СХД за GB составляет **$0.50**

Реальная стоимость СХД

	Native Audit	SecureSphere
Audit Level	Full Auditing (1)	Audit All(2)
Data written per day	5320 GB	120 GB
Compressed data per day	216 GB	6 GB
Yearly additional audit data	78 840 GB	2190 GB
Recurring cost of storage per year (additional audit data X price per GB)	**$ 39 900**	$ 1 095

(1) 300 queries per sec with query size of 25 kilobytes for native audit
http://msdn.microsoft.com/en-us/library/dd392015%28v=sql.100%29.aspx
(2) 1 query per sec with query size of 1 kilobyte for privileged user auditing

IMPERVA

Ручной труд

Средняя зарплата администратора СУБД в России составляет $25 000

(1) Note that salary cost does not include benefits portion which is estimated to be around 30% of salary

Человеческие ресурсы

	Native Audit	SecureSphere
Implementation and Training	0 FTE	.~1 FTE
Administration Costs	.~3 FTE	.~2 FTE
Auditing Costs	.~7 FTE	~.1 FTE
Total FTE count	~ 1 FTE	~0.4 FTE
Recurring Cumulative Operational Costs	$ **25,000**	$ 16,000

FTE = Инженер на полную ставку

Итоговая таблица

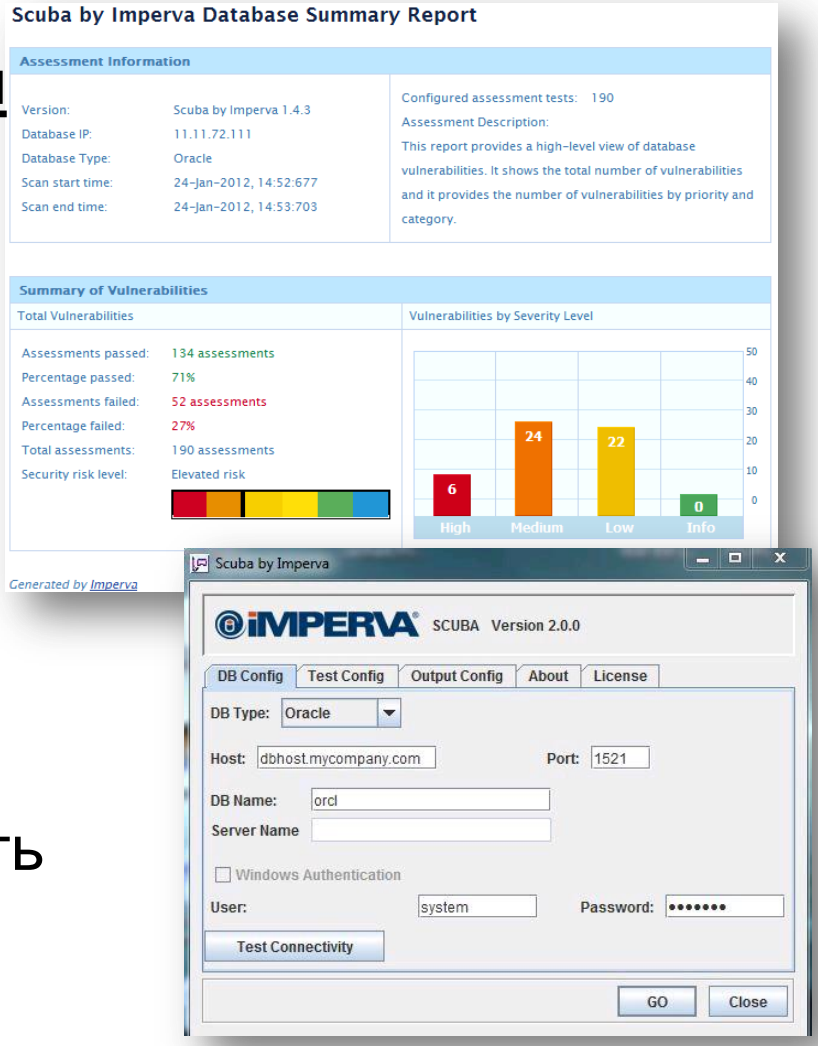
	Native Audit	SecureSphere	Savings/Investment
 HW/SW	$184 800	$ -	Стоимость ресурсов: ПО и серверов
 Storage	$39 900	$ 1 095	Ежегодные расходы
 Labor	$ 25 000	$ 16 000	Ежегодные расходы
 SecureSphere	$ -	$ 154 000	Разовые вложения
	$249 700	**$171 095**	TCO

Все цены приведены в соответствии с рекомендованными производителями

IMPERVA

Сканирование уязвимостей БД и технология Virtual Patch, Scuba by Imperva

- **Свободно распространяемая** утилита для сканирования уязвимостей и конфигураций БД, включая информацию по установленным обновлениям
- Отчеты предоставляют наглядную информацию по актуальным угрозам.
- Регулярное обновление ПО Scuba гарантирует актуальность встроенных в сканер проверок



Вопросы?

- Шахлевич Александр
- RSD Russia

- Alexandr.Shakhlevich@imperva.com

Новые документы ФСТЭК, приказы №17, 21

- Меры по защите информации:
  - Идентификация и аутентификация субъектов доступа
  - Управление доступом субъектов доступа к объектам доступа
  - Ограничение программной среды
  - Защита машинных носителей информации
  - Регистрация событий безопасности
  - Антивирусная защита
  - Обнаружение (предотвращение) вторжений
  - Контроль (анализ) защищённости ПДн
  - Обеспечение целостности ИС и ПДн
  - Обеспечение доступности ПДн
  - Защита среды виртуализации
  - Защита технических средств
  - Защита ИС, её средств , систем связи и передачи данных
  - **Выявление инцидентов**
  - **Управление конфигурацией ИС и системы защиты ПДн**

IMPERVA

Меры по обеспечению безопасности информации

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности	Уровни защищенности ПДн\Классы защищенности ИС				Соответствие продуктов Imperva (*в части защиты веб-приложений, СУБД и файловых серверов)
		4	3	2	1	
II. Управление доступом субъектов доступа к объектам доступа						
УПД.1	Управление учетными записями пользователей, в том числе внешних пользователей	+\+	+\+	+\+	+\+	Полное соответствие. Специальный компонент User Right Management для интеграции с контроллером домена. Возможность настройки ролей в самой системе.
УПД.2	Реализация необходимых методов, типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+\+	+\+	+\+	+\+	
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС	+\-	+\+	+\+	+\+	
УПД.5	Назначение минимально необходимых прав и привелегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС	+\-	+\+	+\+	+\+	
УПД.6	Ограничение неуспешных попыток входа в ИС	+\+	+\+	+\+	+\+	
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя ИС	-\-	-\-	-\-	-\-	
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификаии	-\+	+\+	+\+	+\+	
УПД.13	Реализация защищённого удалённого доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+\+	+\+	+\+	+\+	

Меры по обеспечению безопасности информации, продолжение

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности	Уровни защищенности ПДн\Классы защищенности ИС				Соответствие продуктов Imperva (*в части защиты веб-приложений, СУБД и файловых серверов)
		4	3	2	1	
V. Регистрация событий безопасности						
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени	+\+	+\+	+\+	+\+	Большой набор предустановленных фильтров, возможность написания пользовательских политик, втсроенная отчетность, защищенное хранение данных аудита.
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	+\+	+\+	+\+	+\+	
РСБ.7	Защита информации о событиях безопасности	+\-	+\+	+\+	+\+	
VII. Обнаружение вторжений						
СОВ.1	Обнаружение вторжений	-\-	-\-	+\+	+\+	Модуль Web Application Firewall и Database Firewall
СОВ.2	Обновление базы решающих правил	-\-	-\-	+\+	+\+	
VIII. Контроль (анализ) защищённости ПДн						
АНЗ.1	Выявление, анализ уязвимостей ИС и их устранение	-\-	+\+	+\+	+\+	Встроенный сканер уязвимостей СУБД, интеграция модуля WAF с внешними сканерами уязвимостей
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ	-\-	+\+	+\+	+\+	
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализация правил разграничения доступа, полномочий пользователей в ИС	-\-	-\+	+\+	+\+	

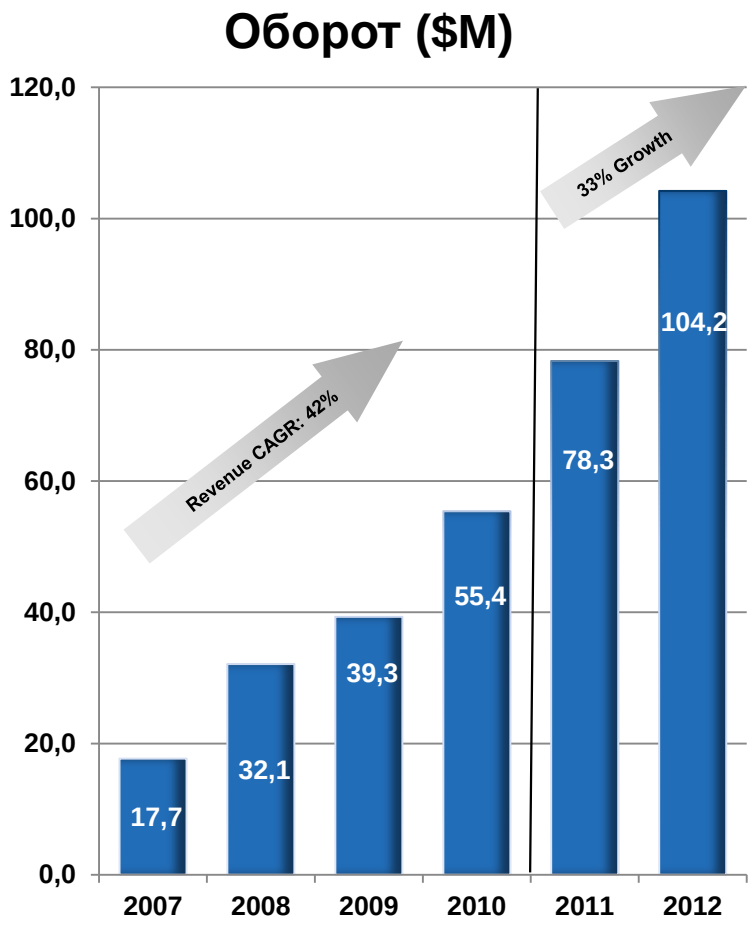
Требования регуляторов

- 1) PCI DSS Compliance

	PCI DSS 2.0 Requirements	Imperva Solutions for PC DSS
6.6	Protect public-facing Web applications	SecureSphere Web Application Firewall
7	Restrict access to cardholder data to business need to know	User Rights Management for Databases and Files
8.5	Identify and disable dormant user accounts	User Rights Management for Databases and Files
10	Monitor all access to cardholder data	SecureSphere Database and File Activity Monitoring
11.5	Deploy file integrity monitoring software	SecureSphere File Activity Monitoring

- 2) 382-П – есть аналитика
- 3) СТО БР ИББС – есть аналитика

Обзор Imperva



Миссия

Защита бизнес-приложений и конфедециальных данных от современных атак и утечек

Сегмент рынка

Безопасность бизнеса, безопасность данных

Мировое присутствие

- Основана в 2002
- Глобальное присутствие, штаб-квартира в США
- 450+ сотрудников
- Заказчики в 60+ странах

Наши заказчики

2,200+ заказчиков продуктов Imperva; тысячи клиентов облачных сервисов

- 8 из топ 10 глобальных телеком. провайдеров
- 5 из топ 10 американских коммерческих банков
- **6 из топ 10 российских банков**
- **2 из 3 российских мобильных операторов**
- 4 из топ 5 глобальных производителей hardware
- 200+ государственных заказчиков

Ключевые международные заказчики

Government

Media/Telco

Technology

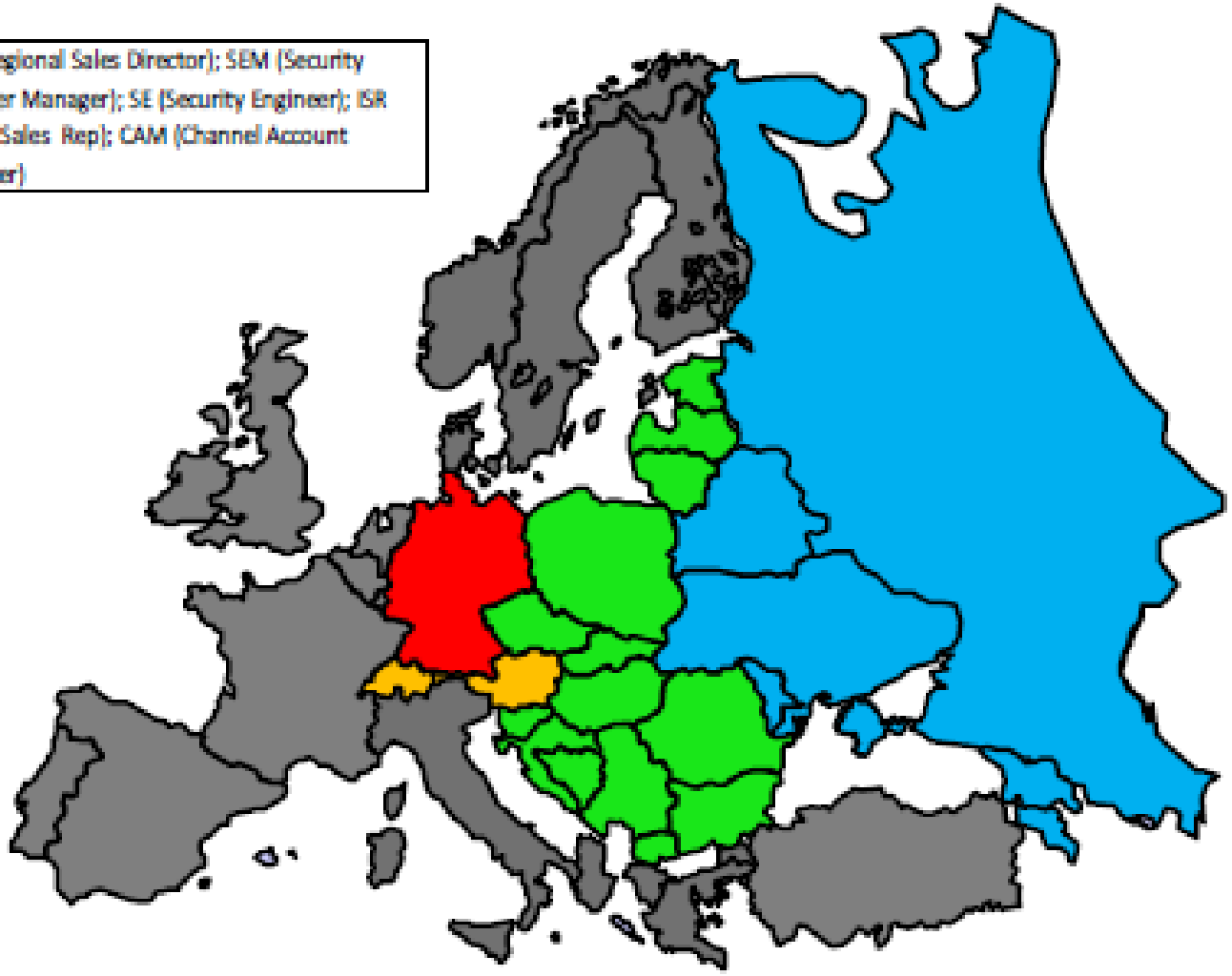
Other

Ключевые факторы успеха

- Лидирующее решение в области защиты данных
- Возрастающая потребность в новых решениях для защиты корпоративных приложений от современных угроз
- Масштабируемая бизнес-модель и активное развитие продуктовой линейки
- Обширный пул разнопрофильных заказчиков
- Эффективная канальная модель продаж
- Успешный вывод целого ряда новых продуктов на рынок
- Сильная команда специалистов

Представители в России и СНГ

RSD (Regional Sales Director); SEM (Security Engineer Manager); SE (Security Engineer); ISR (Inside Sales Rep); CAM (Channel Account Manager)



Russia & CIS 1
RSD **Johan Nordstrom** +46 709 982 898 Johan.Nordstrom@imperva.com
SE **Pavel Kovalev** +7 915 040 2168 Pavel.Kovalev@imperva.com
SE **Konstantin Solodilin** (38063) 270-0110 Konstantin.Solodilin@imperva.com

Russia & CIS 2
RSD **Alexandr Shakhlevich** +79150005847 alexandr.shakhlevich@imperva.com
SE **Pavel Kovalev** +7 915 040 2168 Pavel.Kovalev@imperva.com
SE **Konstantin Solodilin** (38063) 270-0110 Konstantin.Solodilin@imperva.com