

# Ключевые ингредиенты хорошего WAF

Александр Шахлевич

RSD Russia&CIS

Все больше приложений

Все больше возможностей продать  
информацию..

Web  
Apps



Customer  
portal



Mobile  
Apps



Web Services  
or APIs



DARK WEB

WikiLeaks

Bitcoin

Все больше  
информационных хранилищ

Все больше различных  
субъектов доступа

Structured

ORACLE

Microsoft  
SQL Server

IBM DB2

Unstructured

NFS



Windows  
Server

Big Data



mongoDB

cloudera



SaaS



Office 365

Knowledge  
Workers



Customers



Contractors

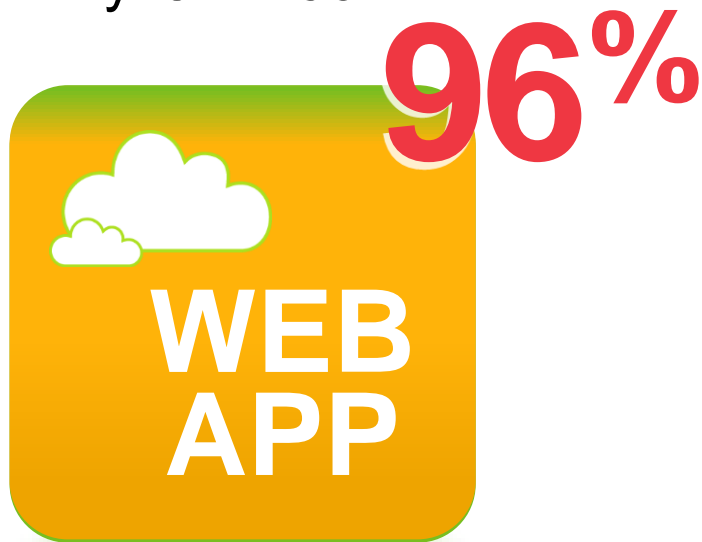


Privileged  
Users

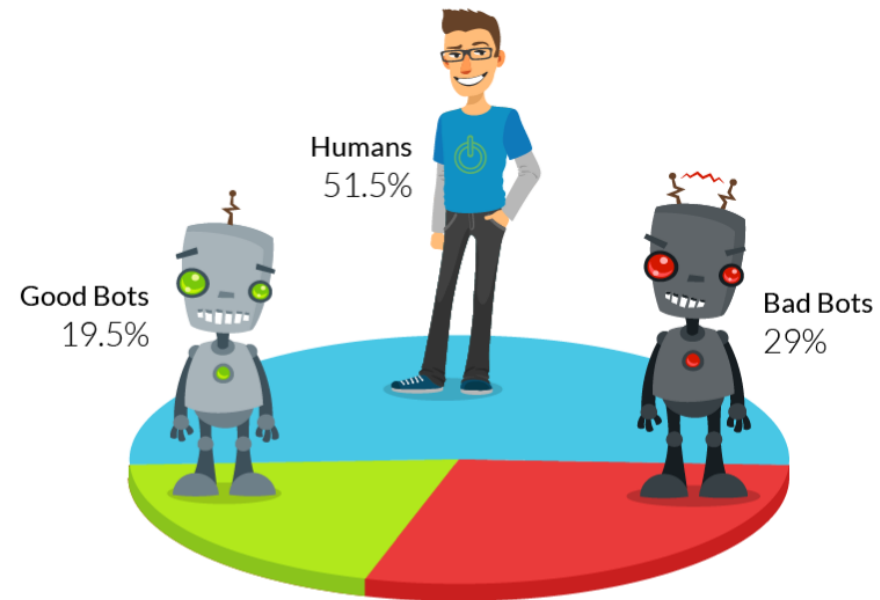


# Практически у любого сайта есть уязвимости

**96%** веб-приложений  
имеют те или иные  
уязвимости.



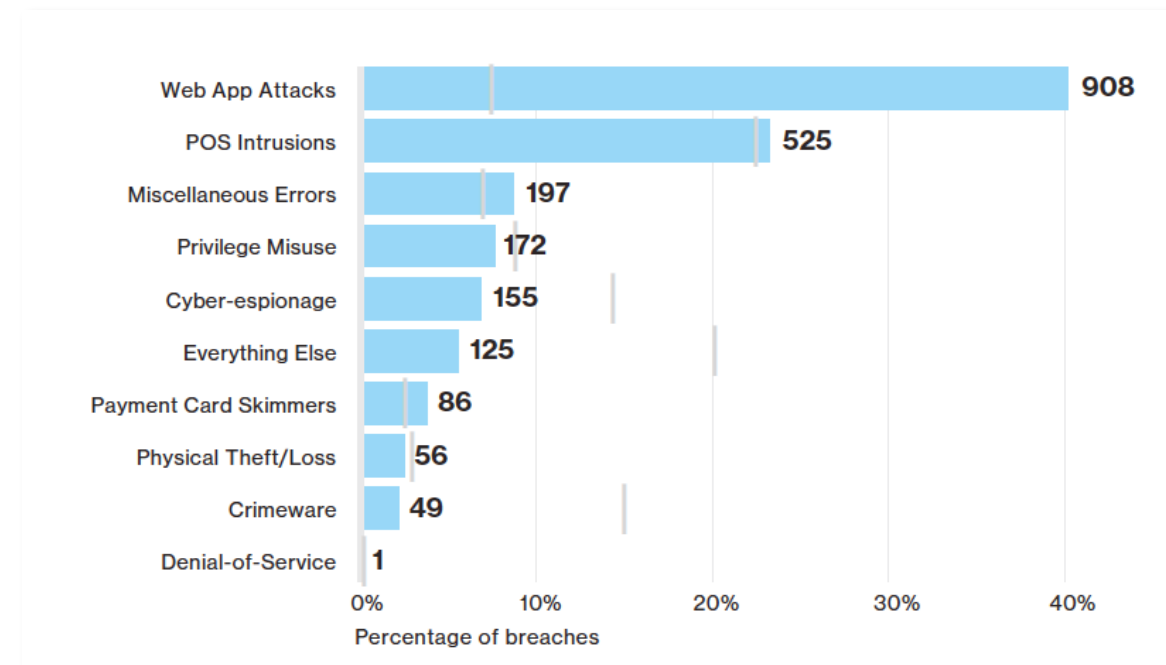
Около половины трафика генерируется  
средствами автоматизации.



**60%** из этого трафика  
является вредоносным.

# Веб-приложения – врата к данным

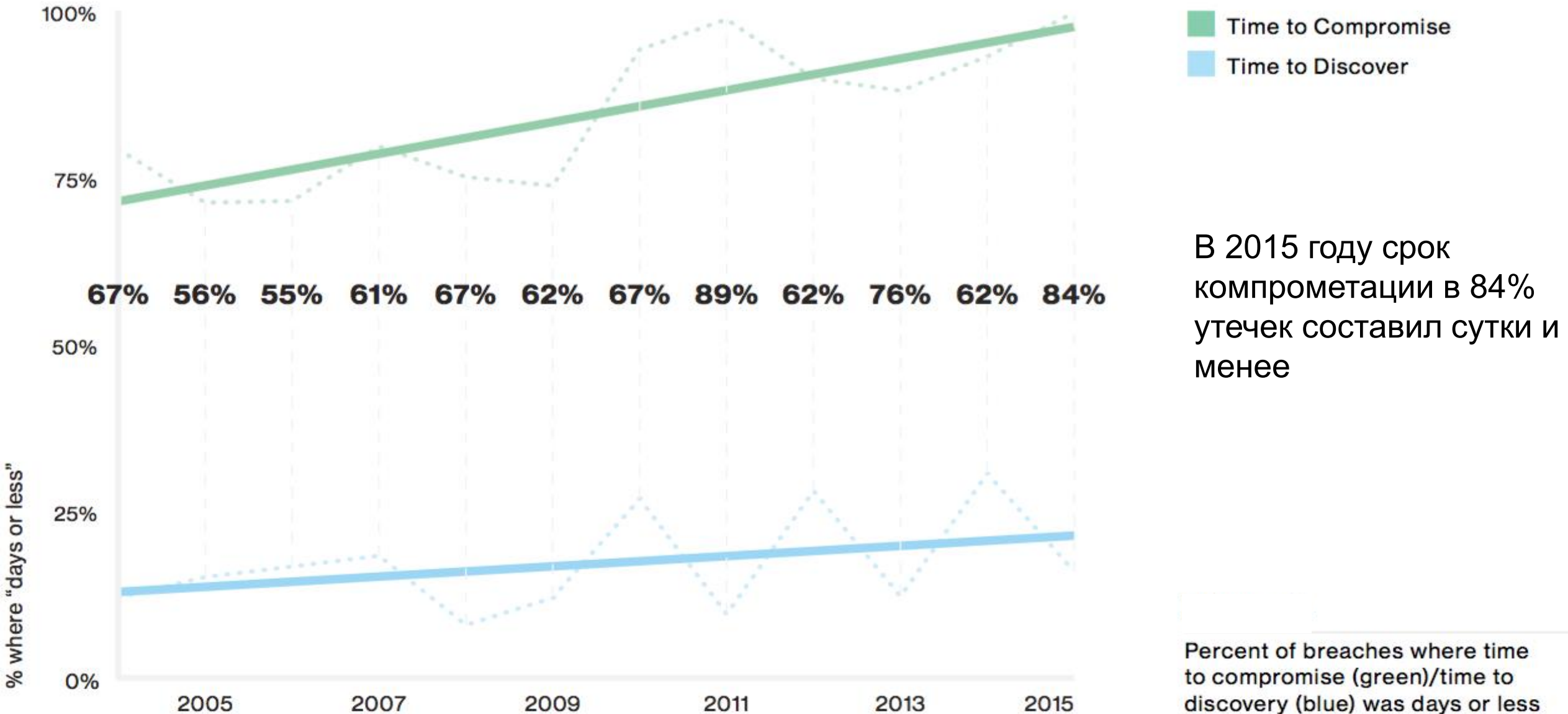
- 85% успешных атак можно описать всего 10 основными паттернами
- 40% подтвержденных утечек были связаны с уязвимостями веб-приложений
- 95% подтвержденных утечек были финансово мотивированы



Source: 2016 Verizon Data Breach Investigation Report

*Lastly we want to thank AsTech Consulting, **Imperva**, and WhiteHat Security for scan data and mind melds around web application security.”*

# Скорость компрометации систем возрастает



Crimeware	Cyber-espionage	Denial of Service	Everything Else	Stolen Assets	Misc. Errors	Card Skimmers	Point of Sale	Privilege Misuse	Web Apps
			1%	<1%	1%	<1%	95%	1%	1%
	7%		17%	17%	27%			3%	30%
				3%			47%		50%
1%	<1%	<1%	2%	<1%	2%	9%		4%	82%
3%	3%		11%	19%	22%		7%	32%	3%
1%	3%		4%		25%		1%	11%	57%
3%	47%		3%				3%	24%	21%
4%	19%		25%	4%	15%			21%	13%
12%	16%		4%	9%	37%			13%	9%
1%	1%		4%		1%	3%	64%	2%	26%

Incident patterns by industry  
minimum 25 incidents (only  
confirmed data breaches)

Accommodation (72), n=282

Educational (61), n=29

Entertainment (71), n=38

Finance (52), n=795

Healthcare (62), n=115

Information (51), n=194

Manufacturing (31-33), n=37

Professional (54), n=53

Public (92), n=193

Retail (44-45), n=182

# Ключевые системы и задачи по отраслям

Отрасль	Критичные системы
Финансовые компании	<ul style="list-style-type: none"><li>• АБС</li><li>• ДБО</li><li>• Процессинг</li><li>• Платежные системы</li><li>• Онлайн-сервисы</li><li>• Корпоративные ресурсы</li></ul>
Страховые, онлайн ритейл	<ul style="list-style-type: none"><li>• Личный кабинет пользователя</li><li>• Онлайн-сервисы</li><li>• Корпоративные ресурсы</li><li>• Логистика</li></ul>
Телеком	<ul style="list-style-type: none"><li>• Биллинг</li><li>• Корпоративные ресурсы</li><li>• Личный кабинет пользователя</li><li>• Услуги хостинга</li><li>• Облачные услуги</li></ul>
Госкомпании	<ul style="list-style-type: none"><li>• Корпоративные ресурсы</li><li>• Госуслуги</li><li>• СМЭВ</li><li>• ГАСУ</li></ul>
ТЭК и промышленность	<ul style="list-style-type: none"><li>• SCADA</li><li>• Система учета добычи\выработки</li><li>• ERP</li><li>• CRM</li><li>• Корпоративные ресурсы</li></ul>

# Что такое OWASP Top 10?

## OWASP Top 10

The OWASP Top Ten is a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

We urge all companies to adopt this awareness document within their organization and start the process of ensuring that their web applications do not contain these flaws. Adopting the OWASP Top Ten is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code.

## Translation Efforts

The OWASP Top 10 has been translated to many different languages by numerous volunteers. These translations are available as follows:

- All versions of the OWASP Top 10 - 2013
- All versions of the OWASP Top 10 - 2010
- Information about the various translation teams

## What is the OWASP Top 10?

The OWASP Top 10 provides:

- A list of the 10 Most Critical Web Application Security Risks

And for each Risk it provides:

- A description
- Example vulnerabilities
- Example attacks
- Guidance on how to avoid
- References to OWASP and other related resources

OWASP Top 10 - 2010 (Previous Version)	OWASP Top 10 - 2013 (Current Version)
A1-Injection	A1-Injection
A3-Broken Authentication and Session Management	A2-Broken Authentication and Session Management
A2-Cross Site Scripting (XSS)	A3-Cross-Site Scripting (XSS)
A4-Insecure Direct Object Reference	A4-Insecure Direct Object References
A6-Security Misconfiguration	A5-Security Misconfiguration
A7-Insecure Cryptographic Storage - Merged with A9 -->	A6-Sensitive Data Exposure
A8-Failure to Restrict URL Access - Broadened into -->	A7-Missing Function Level Access Control
A5-Cross Site Request Forgery (CSRF)	A8-Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9-Using Components with Known Vulnerabilities
A10-Unvalidated Redirects and Forwards	A10-Unvalidated Redirects and Forwards
A9-Insufficient Transport Layer Protection	Merged with 2010-A7 into 2013-A6



<b>OWASP Top 10 – 2010 (Previous)</b>	<b>OWASP Top 10 – 2013 (New)</b>
<b>A1 – Injection</b>	<b>A1 – Injection</b>
<b>A3 – Broken Authentication and Session Management</b>	<b>A2 – Broken Authentication and Session Management</b>
<b>A2 – Cross-Site Scripting (XSS)</b>	<b>A3 – Cross-Site Scripting (XSS)</b>
<b>A4 – Insecure Direct Object References</b>	<b>A4 – Insecure Direct Object References</b>
<b>A6 – Security Misconfiguration</b>	<b>A5 – Security Misconfiguration</b>
<b>A7 – Insecure Cryptographic Storage – Merged with A9 →</b>	<b>A6 – Sensitive Data Exposure</b>
<b>A8 – Failure to Restrict URL Access – Broadened into →</b>	<b>A7 – Missing Function Level Access Control</b>
<b>A5 – Cross-Site Request Forgery (CSRF)</b>	<b>A8 – Cross-Site Request Forgery (CSRF)</b>
<b>&lt;buried in A6: Security Misconfiguration&gt;</b>	<b>A9 – Using Known Vulnerable Components</b>
<b>A10 – Unvalidated Redirects and Forwards</b>	<b>A10 – Unvalidated Redirects and Forwards</b>
<b>A9 – Insufficient Transport Layer Protection</b>	<b>Merged with 2010-A7 into new 2013-A6</b>

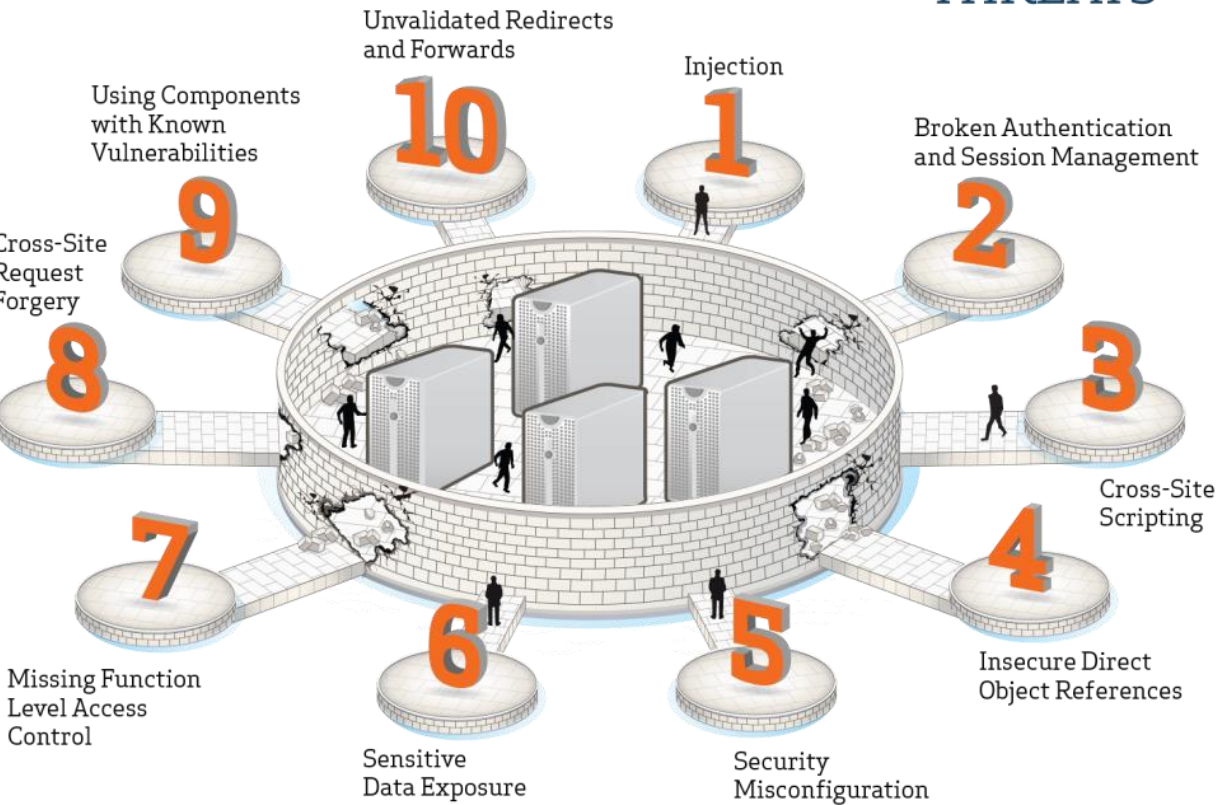
# Table of Contents

---

- [Top 10 2017](#)
- [Introduction](#)
- [Release Notes](#)
- [Risk](#)
- [Top 10](#)
  - [A1-Injection](#)
  - [A2-Broken Authentication and Session Management](#)
  - [A3-Cross-Site Scripting \(XSS\)](#)
  - [A4-Broken Access Control](#)
  - [A5-Security Misconfiguration](#)
  - [A6-Sensitive Data Exposure](#)
  - [A7-Insufficient Attack Protection](#)
  - [A8-Cross-Site Request Forgery \(CSRF\)](#)
  - [A9-Using Components with Known Vulnerabilities](#)
  - [A10-Underprotected APIs](#)

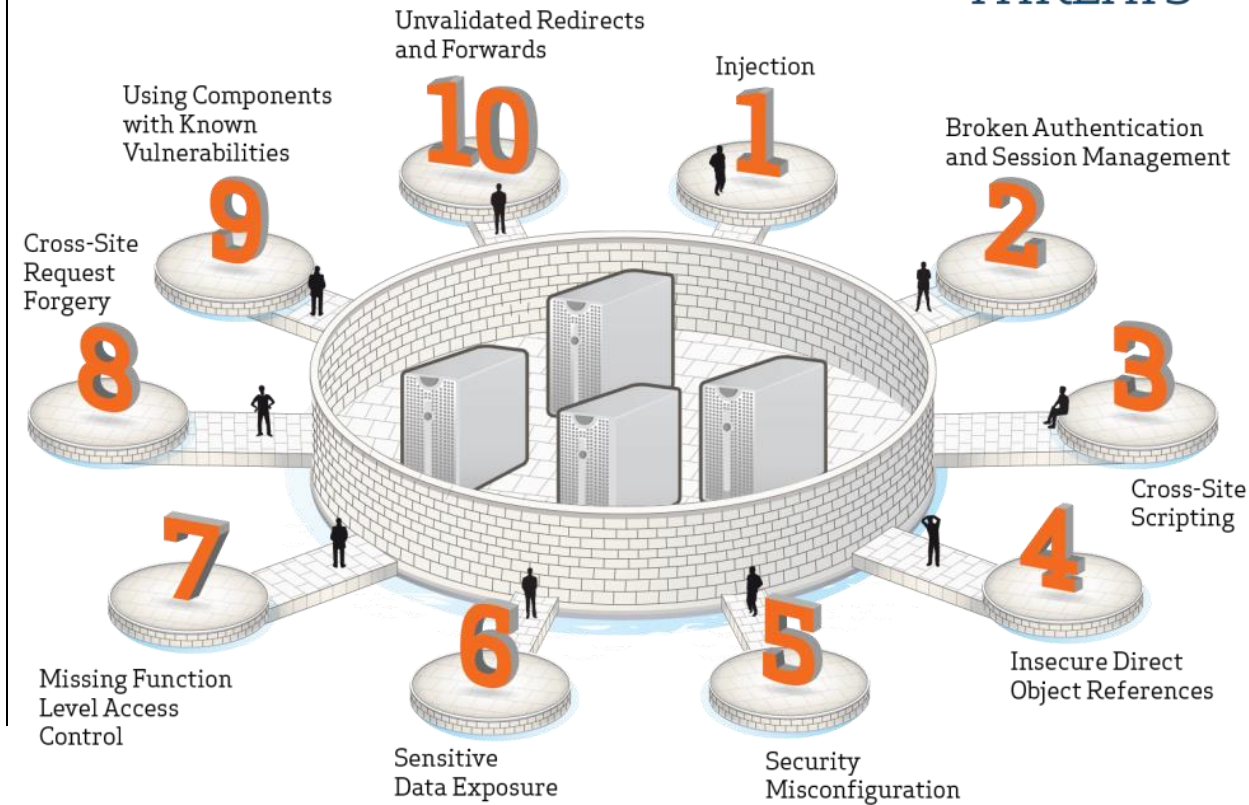
# NEXT GENERATION FIREWALLS

BLOCK  
**<40%**  
OF THE OWASP  
TOP TEN  
THREATS



# WEB APPLICATION FIREWALLS






















BLOCK  
**100%**  
OF THE OWASP  
TOP TEN  
THREATS






OWASP Top 10 (for 2013)

# ОСНОВНЫЕ ОТЛИЧИЯ WAF ОТ IPS&NGFW

Figure 2. Main Differences Between WAF, IPS and NGFW

	Web Application Firewall	Intrusion Prevention System	Next-Generation Firewall
Multiprotocol Security			
IP Reputation			
Web Attack Signatures			
Web Vulnerabilities Signatures			
Automatic Policy Learning			
URL, Parameter, Cookie, and Form Protection			
Leverage Vulnerability Scan Results			

 = good to very good     = average or fair     = below average

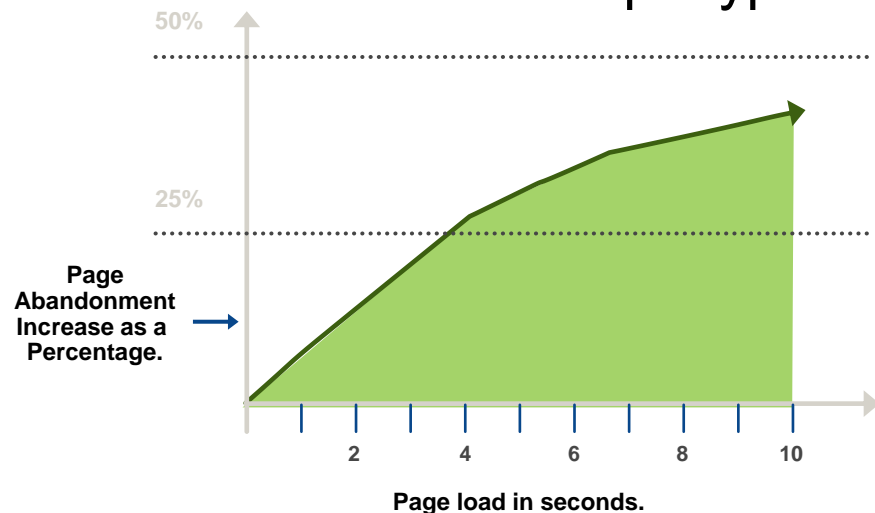
IP = Internet Protocol

# Ключевые проблемы для бизнеса

- Упущенная выгода в связи с простоем сайта
- Ущерб репутации
- Конкурентная борьба\кража информации
- Штрафы и регуляторные меры (PCI, СТО БР ИББС, SOX)

# Дополнительные задержки при загрузке страниц напрямую влияют на выручку компании

Задержки при загрузке сайта влияют на повышение оттока посетителей с ресурса



В соответствии с отчетом Aberdeen Group **1-секундная** задержка в отклике приводит к следующим показателям:



Fewer Page Views



Decrease in Customer Satisfaction



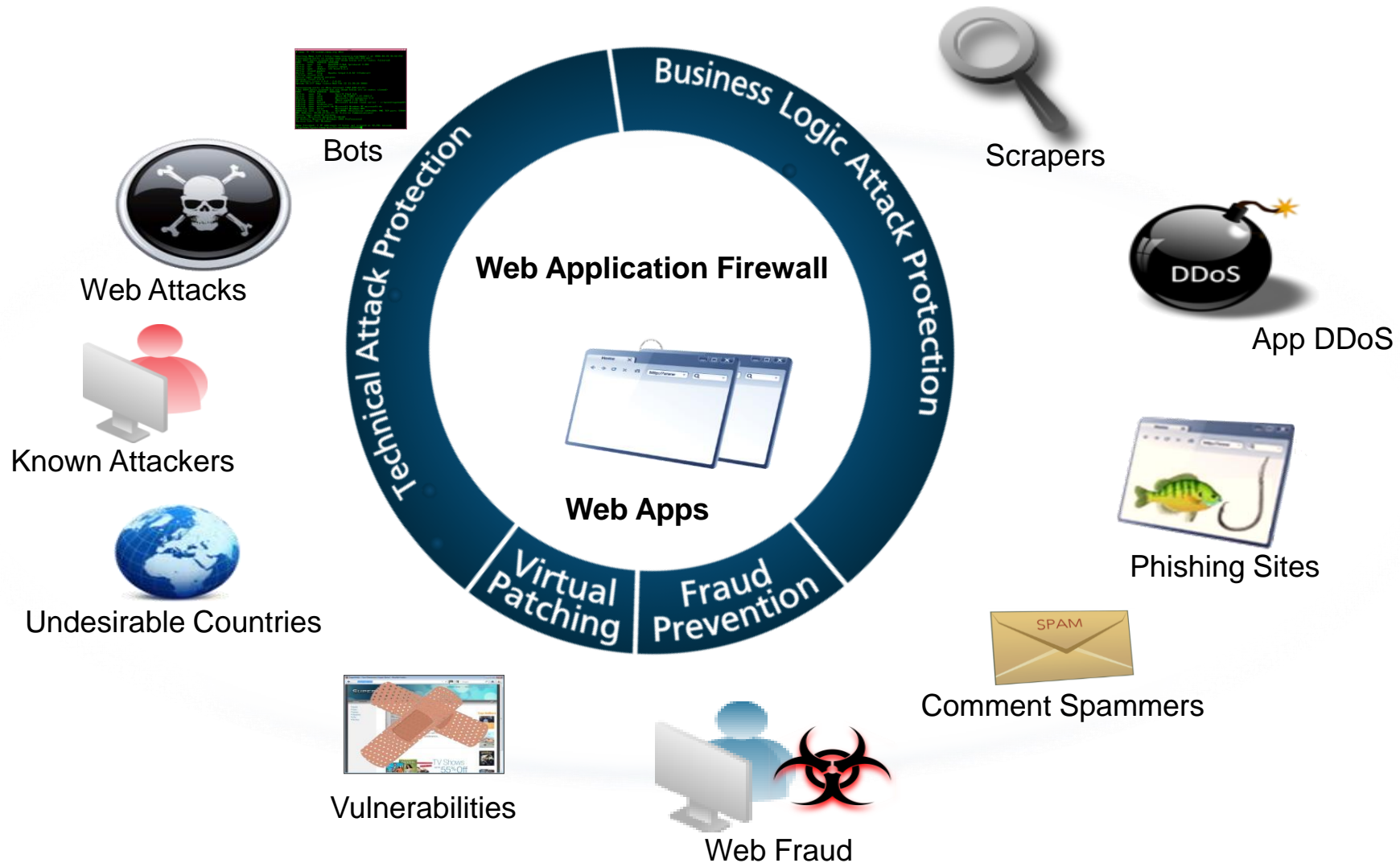
Loss in Conversions

# Как на веб-сервис смотрят различные подразделения?

Маркетинг\продажи	ИТ	Безопасность
Удобство для клиентов	Простота использования	Обеспечение защиты от атак на веб-сервис
Статистика (прозрачность действий пользователей)	Прозрачность действий пользователей при работе с сервисом	Прозрачность действий пользователей при работе с сервисом
Отсутствие ложных срабатываний	Отсутствие ложных срабатываний	Отсутствие ложных срабатываний
Обеспечение защиты от атак на веб-сервис	Обеспечение защиты от атак на веб-сервис	Контроль и кастомизация решения
Простота использования	Контроль и кастомизация решения	Простота использования



# Комплексная защита от веб-угроз

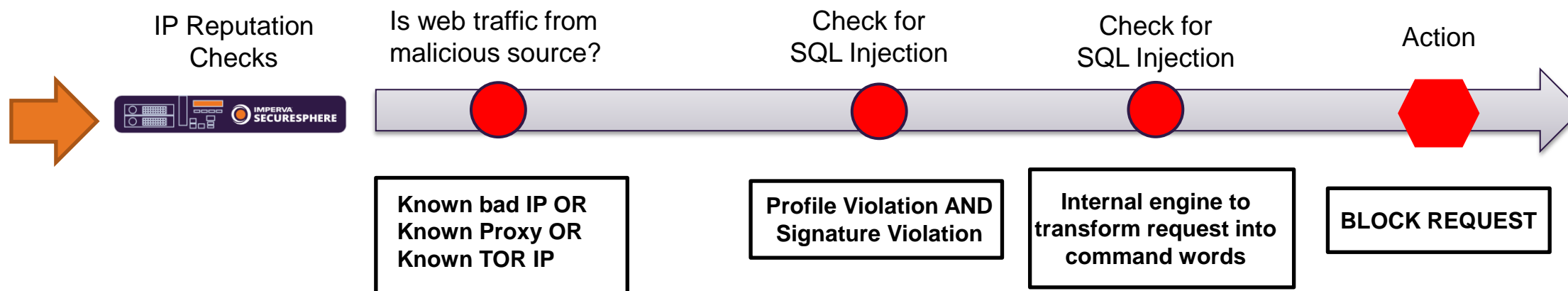




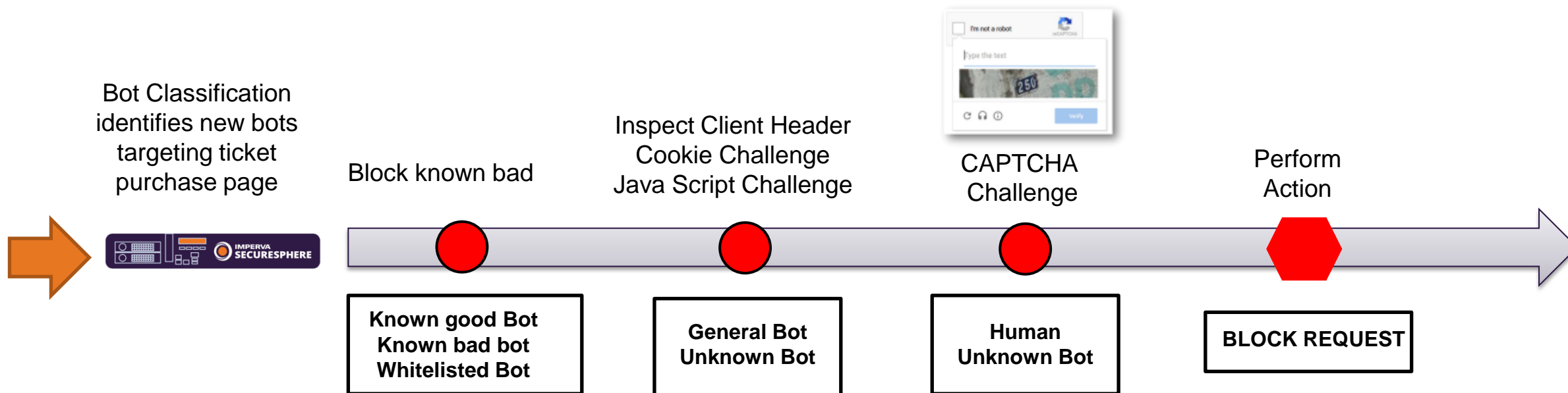
# Как должна строиться защита веб-приложения



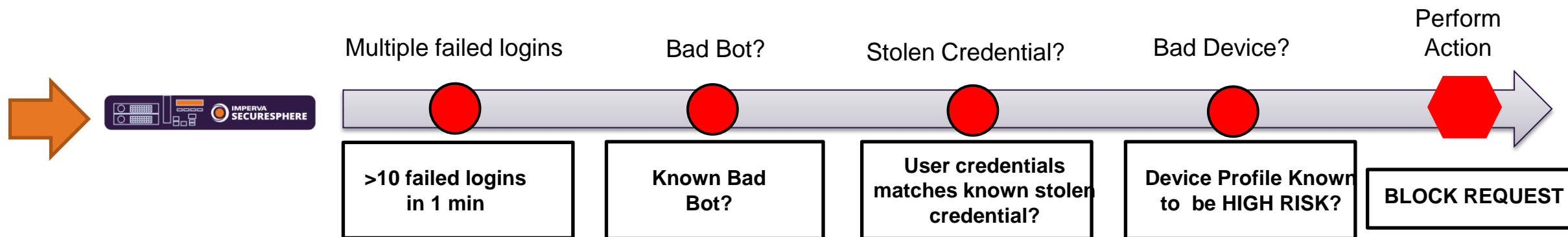
# Корреляция: защита от SQL-инъекций с вредоносных IP



# Корреляция: защита от активности ботов



# Корреляция: защита от кражи аккаунта

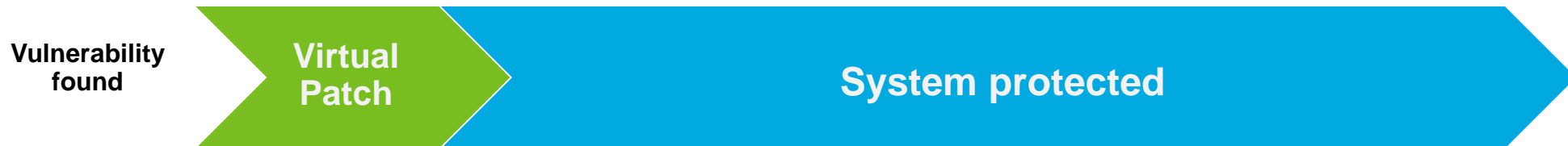


# Virtual Patching: быстрая и эффективная защита веб-приложений

- **116 дней:** среднее время исправления уязвимости



- С помощью систем WAF вы можете сократить срок со **116 дней до 0-5 дней**

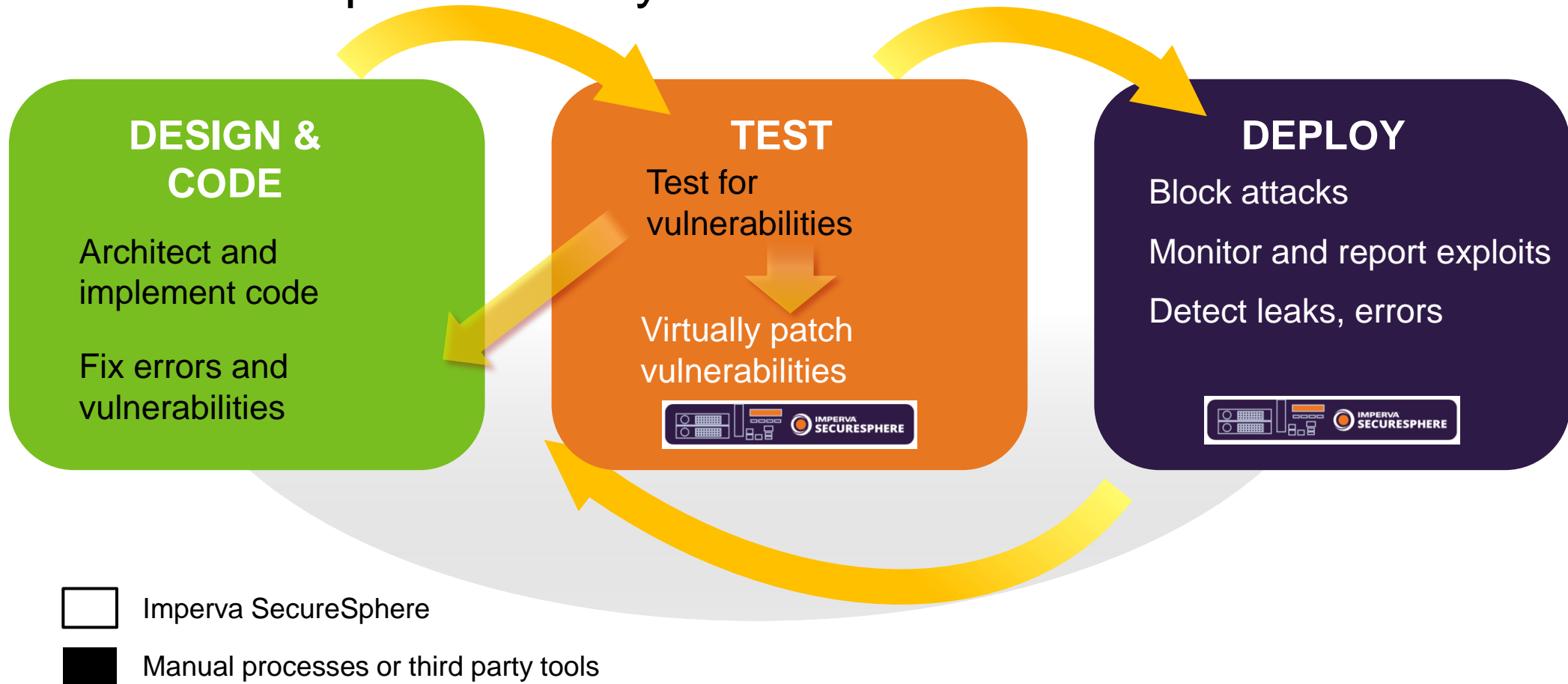


- Можно закрывать уязвимости, даже не найденный сканнерами

<sup>1</sup> [WhiteHat Website Security Statistics Report](#), Winter 2011

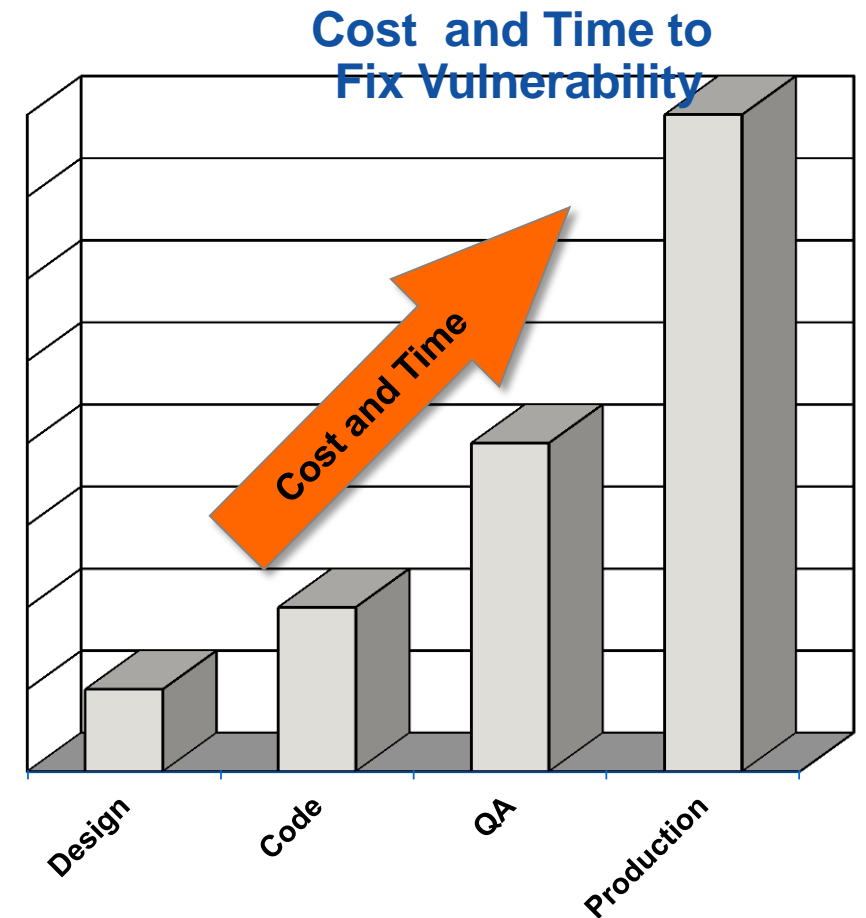
# Virtual Patching: оптимизация цикла разработки

## Software Development Lifecycle



# Уязвимости в продуктивной среде могут стоить дорого

- Цена увеличивается в течении жизненного цикла системы
- Многие уязвимости находят уже только после перевода в продуктив
  - Сложность инфраструктуры
  - Новые атаки и уязвимости
- Цена = Стоимость отладки и тестирования + Риск компрометации
  - Цена повышается с каждой фазой разработки
  - Есть риск атаки системы до стадии продуктива
  - Риск срочного обновления без тщательного тестирования
  - **\$4,000** в среднем стоимость каждого фикса<sup>1</sup>



<sup>1</sup> Dark Reading Article, "The Cost of Fixing an Application Vulnerability"

# Как посчитать ROI для WAF?

Параметр	Основание для расчета
Вероятность совершения атаки\утечки	Verizon DBIR, другая аналитика, для финансовой отрасли – 82%
Стоимость утечки	Оценка доступных через веб-сервисы активов и их критичности, примем за \$500 000 для финансовой отрасли.
Вероятность реализации DDoS прикладного уровня	На данный момент в мире примерно 50%\50% распределение DDoS атак между атаками на L3\L4 и атаками прикладного уровня. Общую вероятность реализации DDoS атак можно взять из отчета Forrester, для финансовых организация этот показатель составляет 74%, итого вероятность - 37%.
Стоимость простоя сервиса	На основании опыта или из усредненных отраслевых показателей. Примем в среднем за \$100 000\час для финансовой отрасли.
Стоимость исправления уязвимостей	На основании опыта или из усредненных отраслевых показателей. Примем в среднем за \$150 000\год для финансовой отрасли.
Годовая стоимость инженера ИБ	\$40 000



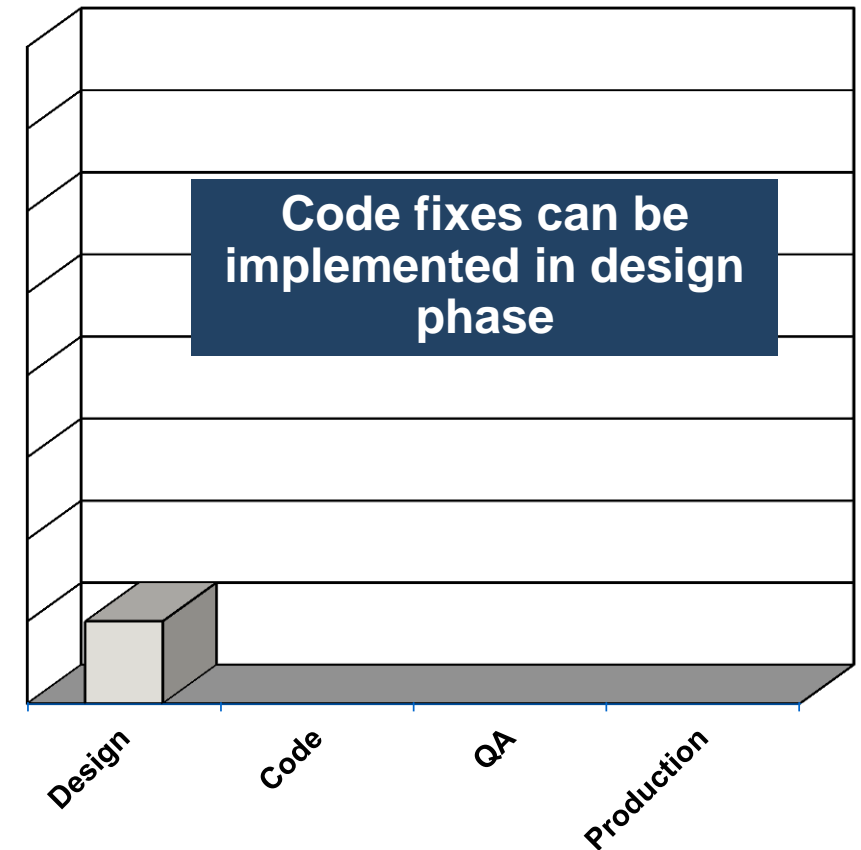
# Расчет ROI от внедрения WAF в финансовой отрасли

Параметр	1 год	2 год	3 год	4 год	5 год
Потенциальный риск от утечки	\$410 000	\$410 000	\$410 000	\$410 000	\$410 000
Потенциальный риск от DDoS прикладного уровня	\$37 000	\$37 000	\$37 000	\$37 000	\$37 000
Стоимость устранения уязвимостей	\$150 000	\$150 000	\$150 000	\$150 000	\$150 000

Параметр	1 год	2 год	3 год	4 год	5 год
Стоимость владения системой WAF на 1 Гб\с	\$150 000	\$25 000	\$25 000	\$25 000	\$25 000
Стоимость устранения уязвимостей	\$75 000	\$75 000	\$75 000	\$75 000	\$75 000

# Исправляйте уязвимости тогда, когда хотите!

- Мгновенная защита с WAF
  - Может заблокировать угрозу еще задолго до исправления\устранения уязвимости
- Сокращение расходов с устранением угрозы
  - Исправление уязвимостей по своему расписанию, а не по требованию злоумышленников
  - Забудьте об экстренных фикса и циклах тестирования
- Никаких дополнительных расходов
  - Никаких изменений в приложение или инфраструктуру
  - Адаптивное обучение

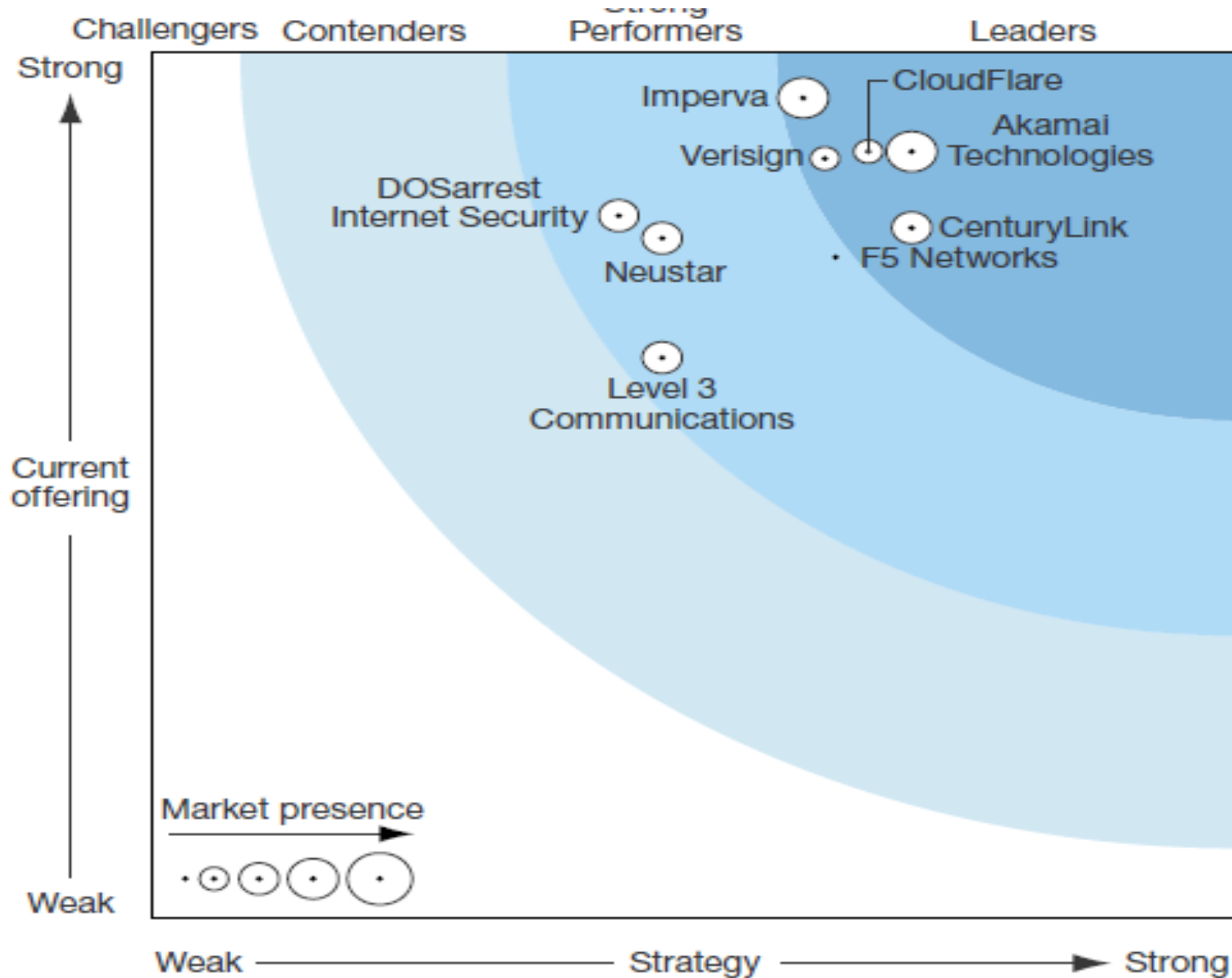


# Gartner MQ for Web Application Firewalls 2014\2015\2016



Imperva SecureSphere WAF – третий год подряд единственный ЛИДЕР в области межсетевых экранов для web-приложений по мнению Gartner

# Forrester Wave for DDoS Protection '15



# Вопросы?