

SOFTPROM



**RAPID7**

# RAPID7 INSIGHT PLATFORM. USE CASE

Subhan Sharifov  
Head of Information Security Department  
at Bank of Baku



**SECURITY FORUM**  
BAKU ♥ APRIL 23

# Продуктовая линейка



InsightVM  
InsightAppsec  
InsightIDR (SIEM + XDR  
+ honeypots )  
InsightCloudSec  
InsightConnect (SOAR)

Metasploit

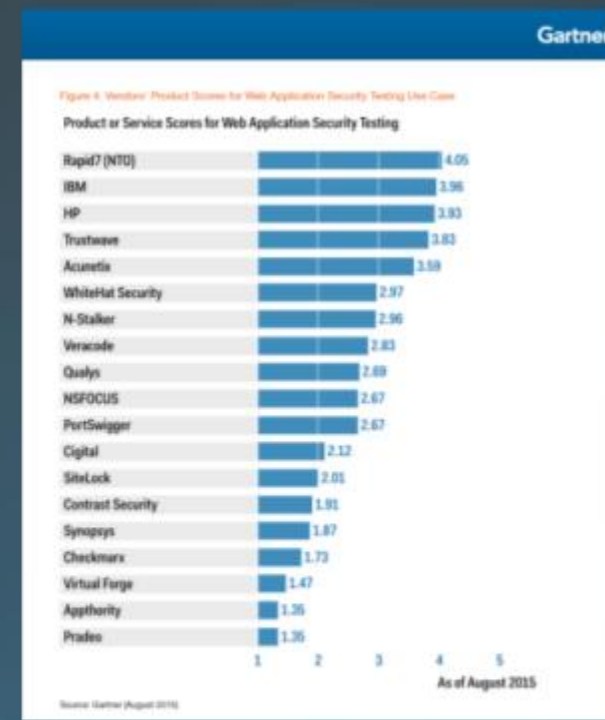
# Отраслевое лидерство



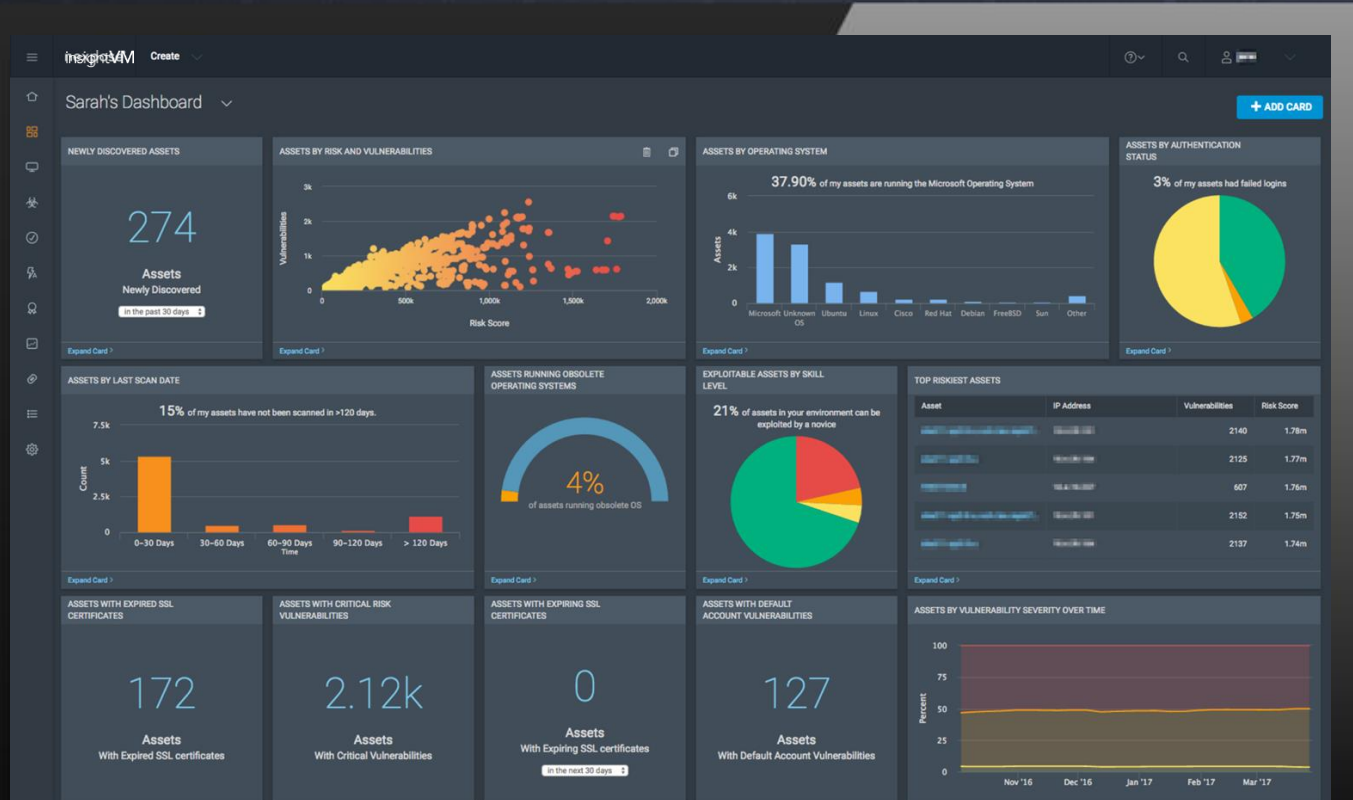
SIEM Magic Quadrant  
- Gartner



Vulnerability Risk Management  
- Forrester Wave



Critical Capabilities for  
Application Security Testing  
- Gartner



## COLLECT



Автоматический сбор, мониторинг и анализ всей вашей сети на предмет новых и существующих рисков.

## PRIORITIZE



Выйдите за пределы только CVSS-методов, чтобы помочь вам **сосредоточиться** на наиболее важных уязвимостях, так же как это делает злоумышленник.

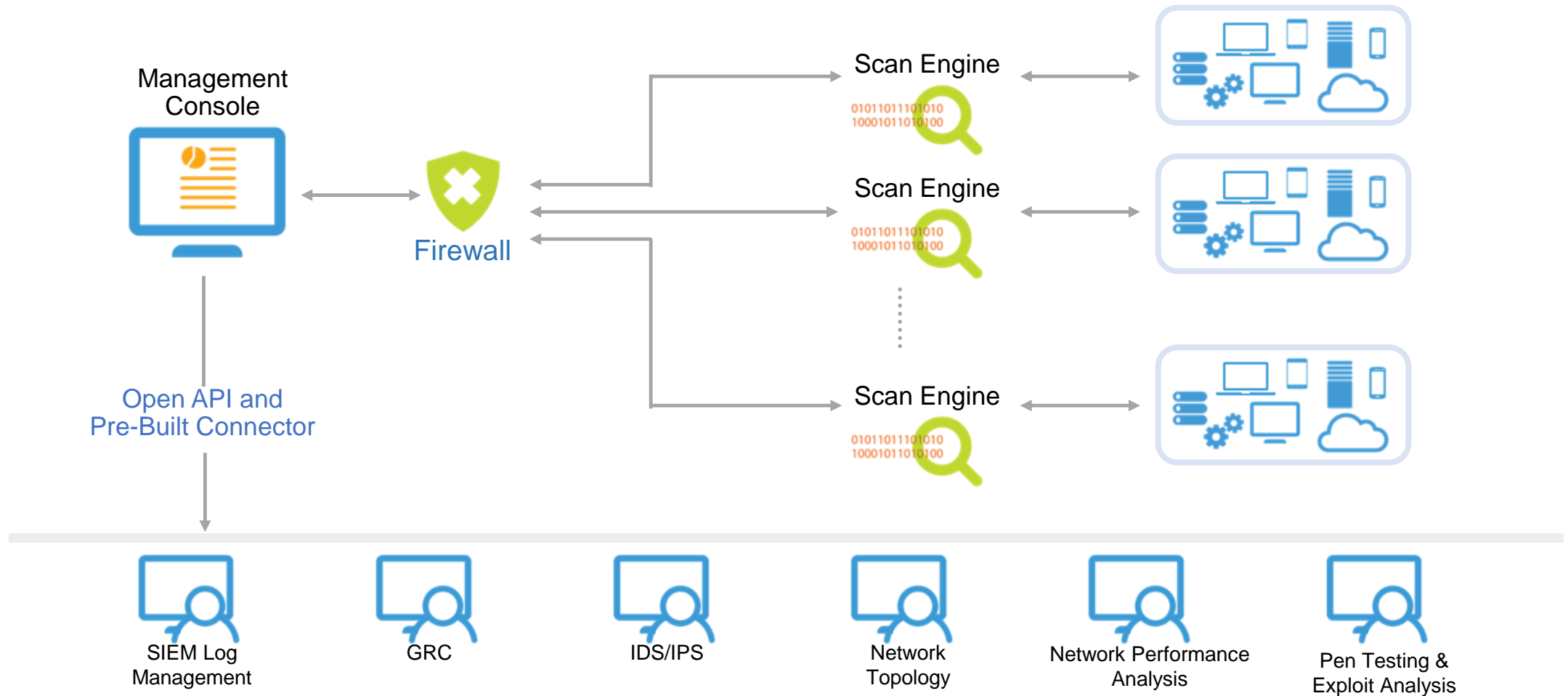
## REMEDiate



Оптимизируйте рабочий процесс исправления (устранения **уязвимостей**), чтобы сделать его вашим лучшим другом и **отслеживать прогресс** в режиме реального времени.



# Гибкая и масштабируемая архитектура Nexpose

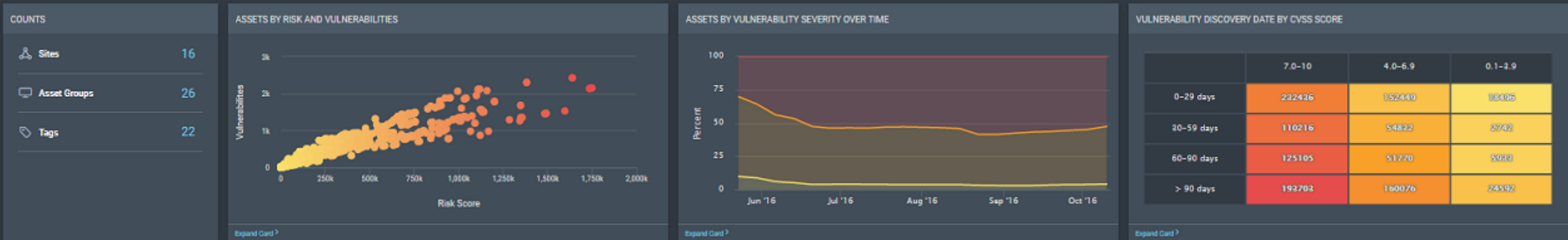


ОСНОВНЫЕ ОТЛИЧИЯ КОТОРЫЕ ЕСТЬ  
ТОЛЬКО IVM – но нет в NEXPOSE!

# Liveboards – New Generation Reporting

Отслеживайте риски в реальном времени

Daily Metrics ▾

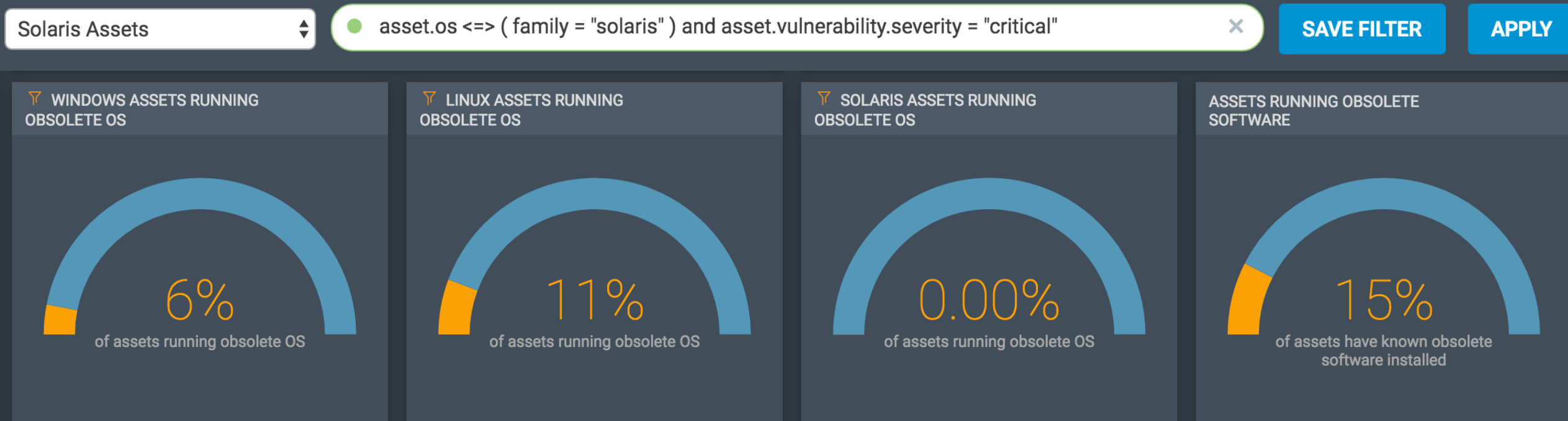


Моментальная аналитика данных сканирования.

Визуализация результатов анализа в интерактивных карточках позволяющих моментально реагировать на изменения в инфраструктуре

# Liveboards – New Generation Reporting

Отчеты больше не нужны



Глубокий анализ данных  
Интеллектуальная система фильтров  
Находите быстро то что важно!



# Remediation Workflows



Мгновенная реакция на риск.

Автоматические  
создание проектов

Контроль выполнение  
заданий

Автоматическое  
распределение заданий.

Win 7 Enterprise SP1 Dynamic Remediations

PROJECT OVERVIEW (BETA)  

2143 Solutions 14 Unknown Solutions 2 Pending Verification

Update Status

Remediation Solutions (0 of 2143 selected)

Solutions	Assets Affect...	Vulnerabil...	Risk Redu...	Status
<input type="checkbox"/> Upgrade to the latest version of Adobe Flash Player for Windows	30	818	8,229,084	Open
<input type="checkbox"/> Upgrade to the latest version of Google Chrome	75	495	5,841,998	Awaiting Verificati...
<input type="checkbox"/> Configure SMB signing for Windows	616	2	986,285	Awaiting Verificati...
<input type="checkbox"/> Upgrade to the latest version of Oracle Java	4	621	456,654	Open
<input type="checkbox"/> MS15-115: Security Update for Windows 7 for x64-based Systems (KB3097877)	42	33	394,383	Open
<input type="checkbox"/> Upgrade to the latest version of Adobe AIR	2	540	380,381	Open
<input type="checkbox"/> Upgrade to the latest version of PHP	10	153	352,337	Open
<input type="checkbox"/> MS16-120: October, 2016 Security Only Quality Update for Windows 7 for x64-based S...	47	26	292,453	Open
<input type="checkbox"/> MS16-001: Cumulative Security Update for Internet Explorer 10 for Windows 7 for x64-...	15	27	208,214	Open
<input type="checkbox"/> MS16-001: Cumulative Security Update for Internet Explorer 8 for Windows 7 for x64-b...	31	29	196,309	Open

PROJECT NAME Win 7 Enterprise SP1 Dynamic Remediations

DESCRIPTION Remediate vulnerabilities on aging OSes

CREATED ON Tue, Sep 27, 2016

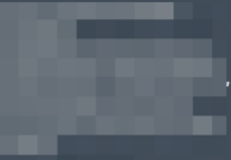
ASSETS AFFECTED 788

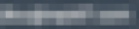
TOTAL REMEDIATIONS 2143

PROGRESS 47%

REMAINING TIME 3 months

DUE ON Sat, Feb 4, 2017

ASSIGNEES 

OWNER 

Go beyond understanding risk: Get to the fix.

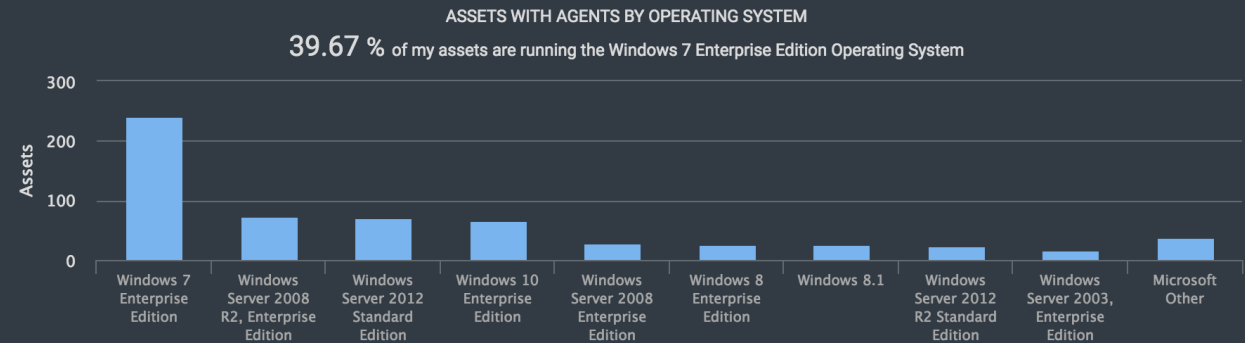
# Agents

- Хосты за пределами сети

- Часто выключаемые хосты

- Хосты которые нельзя сканировать

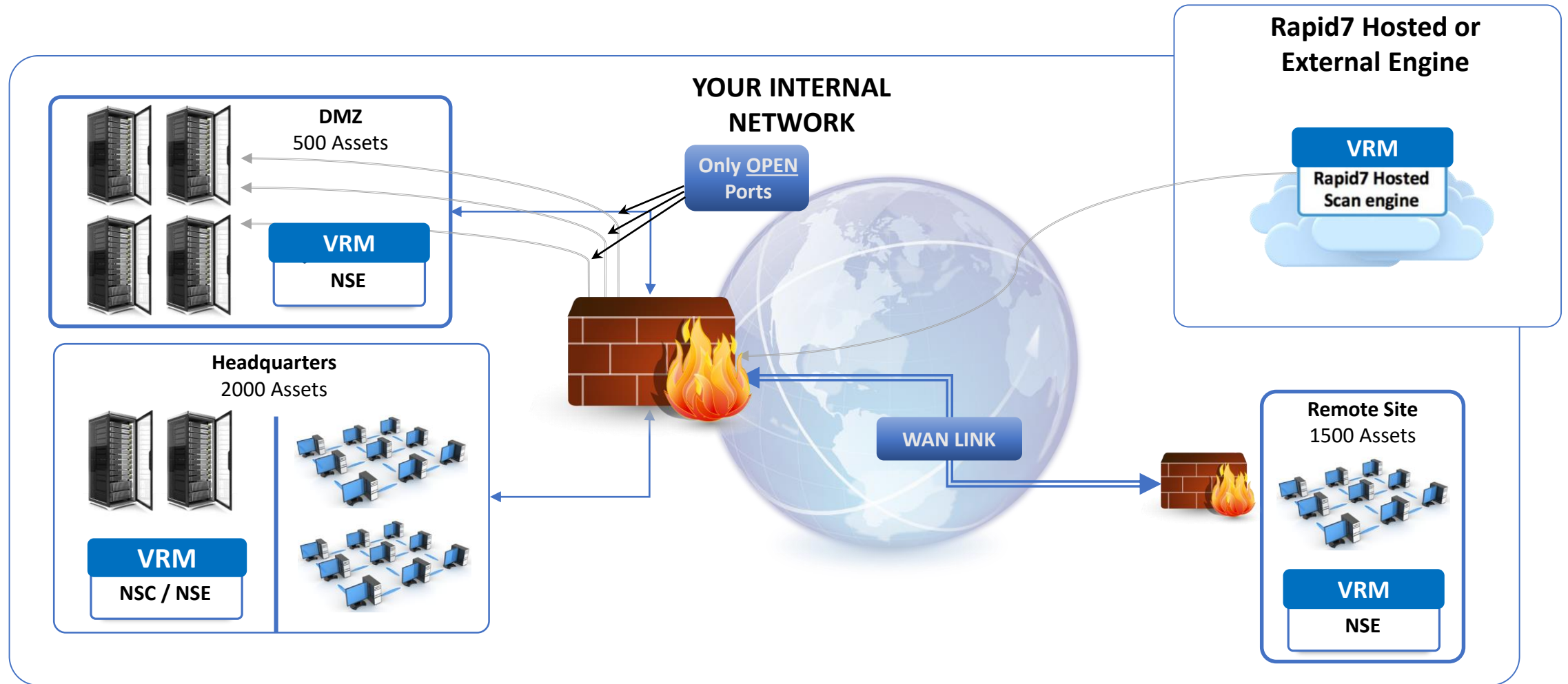
610 Agents	579 Success	31 Error	0 Without Agents	610 Using old version
------------	----------------	-------------	---------------------	--------------------------



(0 of 610 selected)

IP Address	Asset Name	Operating System	Agent status	Time since last assessment	Risk Score	Version
192.168.1.1	xp6-pr-japanese	Microsoft Windows XP Professional SP2	Online	20 minutes ago	696.48k	Oct 24, 2016
192.168.1.2	xp6-pro-chinese	Microsoft Windows XP Professional SP2	Online	35 minutes ago	695.06k	Oct 24, 2016

# Рекомендуемые виды Сканирования (Internal & External Scans)



# Автоматизация – ключ к эффективности

- Автоматическое обнаружение хостов и динамические сканы
- Динамическая группировка хостов
- Сканирования по расписанию
- Адаптивный мониторинг безопасности и Автоматическая реакция на триггеры
- Workflow **Orchestration (IVM)**
- Ticketing integration
- Restfull API
- Интеллектуальная методика оценки рисков
- Эффективная, многоуровневая отчетность

The screenshot displays the Rapid7 API documentation for the **ASSET** endpoint. On the left, a navigation menu lists various API endpoints under the **ASSET** category, including `Assets`, `Asset Search`, `Asset`, `Asset Databases`, `Asset Files`, `Asset Services`, `Asset Service`, `Asset Service Configurations`, `Asset Service Databases`, `Asset Service User Groups`, `Asset Service Users`, `Asset Service Web Applications`, `Asset Service Web Application`, `Asset Software`, `Asset Tags`, and `Asset Tag`. The main content area shows the **ASSET** endpoint details:

**ASSET**  
Resources and operations for managing assets. Assets can be created under the...

**Assets**  
`GET` `/api/3/assets`

Returns all assets for which you have access.

**PARAMETERS**

Query Parameters

- `page`: integer <int32>  
Default: `0`  
The index of the page (zero-based) to retrieve.
- `size`: integer <int32>  
Default: `10`  
The number of records per page to retrieve.
- `sort`: Multiple query params of string  
The criteria to sort the records by, in the format: `property[,ASC]` using multiple sort query parameters.

# Структурированные решения по исправлению (Remediation)

- Выберите из различных типов решений для исправления.
- Отчет об **основных** исправлениях показывает единственное лучшее решение для каждого актива.
- Получите доступ к **полному набору** применимых решений в портлете Remediations.

## REMIATIONS

### BEST SOLUTIONS

### APPLICABLE SOLUTIONS

### SOLUTIONS BY VULNERABILITY

2017-05 Security Only Quality Update for Windows 7 for x64-based Systems (KB4019263)  
 2017-06 Security Only Quality Update for Windows 7 for x64-based Systems (KB4022722)  
 2017-07 Security Only Quality Update for Windows 7 for x64-based Systems (KB4025337)  
 2017-08 Security Only Quality Update for Windows 7 for x64-based Systems (KB4034679)  
 April, 2017 Security Only Quality Update for Windows 7 for x64-based Systems (KB4015546)  
 Configure SMB signing for Windows  
 Configure the minimum password length control

## Top 25 Remediations by Risk

March 31, 2017 2:33:06 PM PDT

### Top Remediations Report



Remediation	Assets	Vulnerabilities			Risk ▼
1. MS16-144: December, 2016 Security Only Quality Update for Windows Server 2008 R2 for x64-based Systems (KB3205394)	2	152	208	22	76,064

# Отчет на основе действий. Эффективность и резу

## Top 25 Remediation

Top Remediation

### Applying

25

Remediation

#### Remediation

1. MS16-144: December Quality Update for Windows Server 2012 (KB3205408)
2. MS16-144: December Quality Update for Windows Server 2012 (KB3205400)
3. MS16-142: November Quality Update for Windows Server 2012 (KB3197876)
4. MS16-142: November Quality Update for Windows Server 2012 (KB3197873)
5. MS15-128: Security Update for Windows Server 2012 (KB3109098)
6. 2018-01 Security Update for Adobe Flash Player for Windows Server 2012 Systems (KB4056887)

## 6. 2018-01 Security Update for Adobe Flash Player for Windows Server 2012 for x64-based Systems (KB4056887)

### Remediation Steps

Download and apply the patch from: <http://support.microsoft.com/help/4056887> <http://support.microsoft.com/help/4056887>

### Assets

Name	IP Address	Site
2012-AD	10.4.26.39	Toronto - Full Audit
2012-AD.vuln2012ad.vuln.lax.rapid7.com	10.4.26.39	Los Angeles - Full Audit - Full CIS Windows
2012-AD.vuln2012ad.vuln.lax.rapid7.com	10.4.26.39	Los Angeles - Full Audit
2013-LYNC-FE.vuln.lax.rapid7.com	10.4.22.210	Los Angeles - Full Audit
2013-LYNC-FE.vuln.lax.rapid7.com	10.4.22.210	Los Angeles - Full Audit - Full CIS Windows
EXCHG2016-U.exchg2016ad.vuln.lax.rapid7.com	10.4.31.210	Toronto - Full Audit
exch2013cu7-u.vuln2012ad.vuln.lax.rapid7.com	10.4.19.73	Los Angeles - Full Audit
exch2013cu7-u.vuln2012ad.vuln.lax.rapid7.com	10.4.19.73	Los Angeles - Full Audit - Full CIS Windows
exchg2013-a-u.vuln2012ad.vuln.lax.rapid7.com	10.4.24.228	Los Angeles - Full Audit
exchg2013-a-u.vuln2012ad.vuln.lax.rapid7.com	10.4.24.228	Los Angeles - Full Audit - Full CIS Windows
exchg2013-b-u.vuln2012ad.vuln.lax.rapid7.com	10.4.22.64	Los Angeles - Full Audit
exchg2013-b-u.vuln2012ad.vuln.lax.rapid7.com	10.4.22.64	Los Angeles - Full Audit - Full CIS Windows
exchg2013-u.vuln.lax.rapid7.com	10.4.31.216	Los Angeles - Full Audit - Full CIS Windows



# Политики соответствия (стандарты)

## Визуализация

“Мне нужно быстро увидеть свое состояние соответствия для всех политик.”

### Policies

272 Policies

148  
Scanned Policies

36  
Policies with Increased Compliance

112  
Policies with Decreased Compliance

78%  
Overall Compliance

☐
🗑️
✎
📷
📄
📺

Policies (0 of 272 selected)

Search

	Policy Name	Category	Source	Assets Passed	Assets Failed	Rule Compliance	Compliance Trend
<input type="checkbox"/>	DISA STIG Windows 2008 R2 Domain Controller Mission Support Sensitive (Version 1, Revision 11)	DISASTIGS	Built-in	1237 of 1636	399 of 1636	<div style="width: 77.15%; background-color: #4caf50;"></div> 77.15%	▲ 0.01%
<input type="checkbox"/>	DISA STIG Windows 2008 R2 Domain Controller Administrative Classified (Version 1, Revision 11)	DISASTIGS	Built-in	1237 of 1636	399 of 1636	<div style="width: 77.15%; background-color: #4caf50;"></div> 77.15%	▲ 0.01%
<input type="checkbox"/>	CIS Microsoft Windows Server 2008 R2 Level One Domain Controller v3.0.0	CIS	Built-in	1064 of 1422	358 of 1422	<div style="width: 76.54%; background-color: #4caf50;"></div> 76.54%	▼ 9.88%
<input type="checkbox"/>	CIS Microsoft Windows Server 2008 R2 Level One Member Server v3.0.0	CIS	Built-in	1064 of 1422	358 of 1422	<div style="width: 76.48%; background-color: #4caf50;"></div> 76.48%	▼ 9.87%
<input type="checkbox"/>	USGCB 1.3.3.1 - Internet Explorer 8	USGCB	Built-in	1136 of 1636	500 of 1636	<div style="width: 70.5%; background-color: #4caf50;"></div> 70.5%	▲ 0.63%
<input type="checkbox"/>	USGCB 1.2.1.0 - Internet Explorer 8 (deprecated)	USGCB	Built-in	1136 of 1636	500 of 1636	<div style="width: 69.71%; background-color: #4caf50;"></div> 69.71%	▲ 0.54%
<input type="checkbox"/>	CIS Windows 7 Level One v2.1.0.2	CIS	Built-in	999 of 1611	612 of 1611	<div style="width: 69.5%; background-color: #4caf50;"></div> 69.5%	▼ 5.9%

# Политики соответствия (стандарты)

## Отчетность

### Быстрые исправления, и для политик также!

Top Policy Remediations with Details

September 12, 2016 14:39:23 GMT

Policy Remediations with details



Policy Name	Rule Name	# Assets	Rule Compliance
CIS Microsoft SQL Server 2008 R2 Database Engine v1.2.0	1.1. Install the Latest SQL Server Service Packs and Hotfixes	506	↑ 3.448 %
CIS Microsoft SQL Server 2008 R2 Database Engine v1.2.0	1.2 Install on dedicated single-function member servers	506	↑ 3.448 %
CIS Microsoft SQL Server 2008 R2 Database Engine v1.2.0	2.1. Set the 'Ad Hoc Distributed Queries' Server Configuration Option to 0	506	↑ 3.448 %
CIS Microsoft SQL Server 2008 R2 Database Engine v1.2.0	2.2. Set the 'CLR Enabled' Server Configuration Option to 0	506	↑ 3.448 %

Rule Breakdown Summary

March 9, 2016 10:13:51 PST

10.4.25.14 w2k8-cis-c.vuln.lax.rapid7.com Microsoft Windows Server 2008 Enterprise Edition SP2

92.24 % Compliant

2 Scanned Policies with 580 Rules

535 of 580 Rules Passed

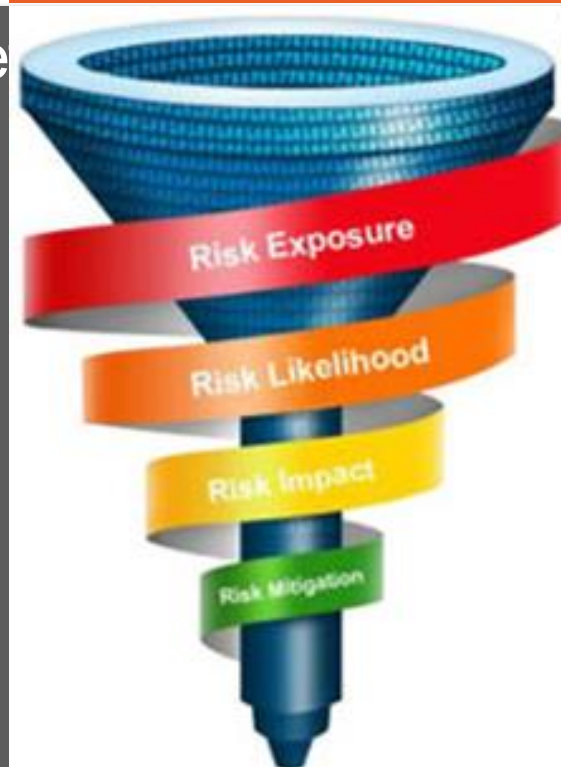
Policy Breakdown	Rules	Passed	Failed
CIS Windows 2008 Domain Controller Level One v2.1.0.1	295	40	
Computer Configuration > Windows Settings > Security Settings > System Services	78	22	
1.1.1.1.1. Set 'Function Discovery Resource Publication' to 'Manual'			
1.1.1.1.10. Set 'UPnP Device Host' to 'Disabled'			
1.1.1.1.100. Set 'IKE and AuthIP IPsec Keying Modules' to 'Automatic'			
1.1.1.1.11. Set 'System Event Notification Service' to 'Automatic'			
1.1.1.1.12. Set 'Windows Color System' to 'Manual'			
1.1.1.1.13. Set 'Active Directory Domain Services' to 'Automatic'			

# Приоритезация. RealRisk

Rapid7 Risk Score (шкала от 0 до 1000) отображае

- > CVSS Score (from 0 to 10)
- > Как давно известна эта уязвимость
- > Как давно эта уязвимость в нашей сети
- > Наличие эксплойтов и malware
- > Насколько легко эксплуатируется
- > Информация с Rapid7 Labs
- > Пользовательский контекст (Критичность актива)

## Visibility



## Prioritization

## ACTIONS

Featured by



# Адаптивная безопасность

Реагируйте автоматически.

Узнавайте о новых рисках сразу после их появления.

Актуализируйте список хостов без необходимости дополнительной инвентаризации.

The screenshot displays the 'Automated Actions' dashboard in the Nexpose interface. At the top, it shows '200 Automated Actions' with a breakdown: 3 Running, 15 Queued, 2 With Errors, and 5 With Failures. The overall execution rate is 85.75%. Below this, there are buttons for 'Create Automated Action' and 'Copy Automated Action'. The main section is a table titled 'Automated Action Activities Over Time (0 of 200 selected)', showing activities from August 16 to August 22. The table includes columns for the action name, status (On/Off), and daily activity counts. A sidebar on the right shows 'Known assets - Aus\_AWS' with 'ACTIVITY DETAILS (16)', listing specific events like '3 known assets available' at 1:22 PM on Aug 22.

Automated Action	On/Off	Tue, Aug 16	Wed, Aug 17	Thu, Aug 18	Fri, Aug 19	Sat, Aug 20	Sun, Aug 21	Mon, Aug 22
Known assets - Aus_AWS	On	3	2	2	2	0	0	2
Known assets - Aus_DHCP	On	2	1	1	0	2	0	1
Known assets - Bos_AWS	On	1	2	1	0	0	0	1
Known assets - Bos_DHCP	Off	1	2	1	0	0	0	1
New assets - Aus_DHCP	On	0	2	1	0	0	0	1
New assets - Bos_DHCP	On	0	1	1	0	0	0	1
New Critical Vulnerabil...	Off	2	1	0	0	0	0	0
New released vulns - Aus	Off	1	1	0	0	0	0	0

# Безопасность на основе оценки рисков

Старая модель :  
**Prevention-Based Security**



Новая модель :  
**Risk-Based Security**

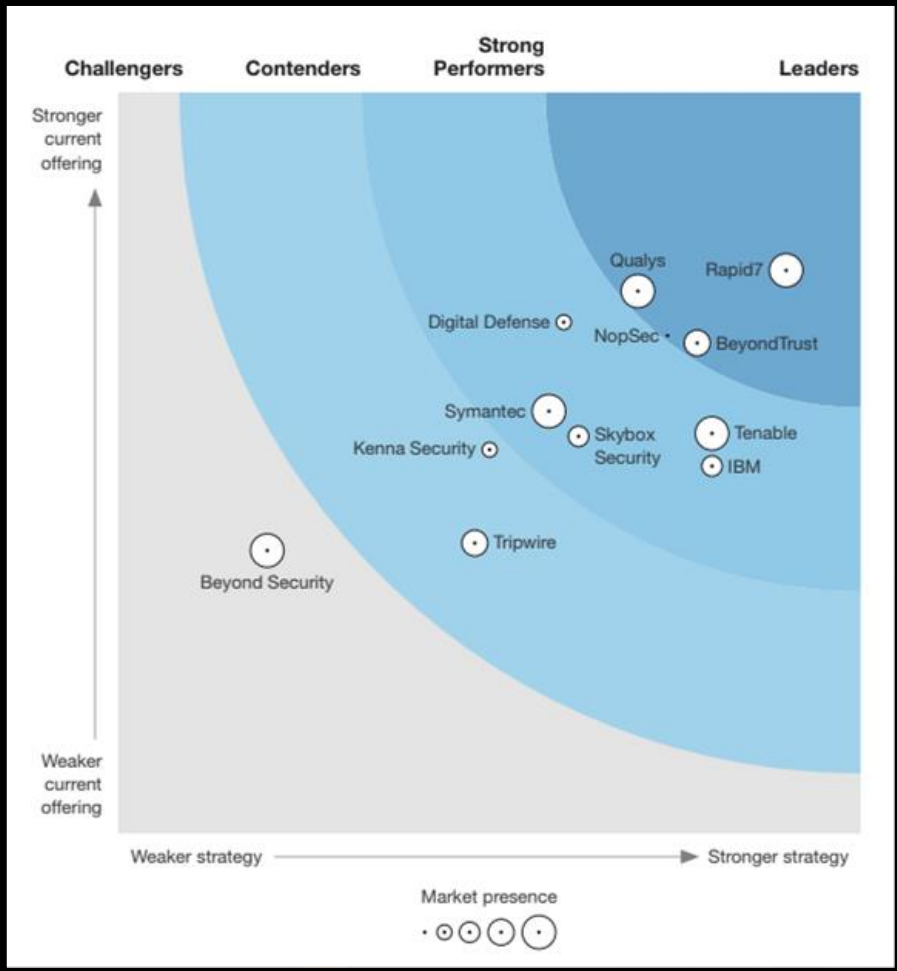


К 2020,

# 60%

средств корпоративной информационной безопасности будет выделено на **быстрое обнаружение и реагирование** по сравнению с менее чем 20% в 2016 году.

- Gartner: "Special Report: Cybersecurity at the Speed of Digital Business", May 26, 2016



“Rapid7 уже реализовал то, как VRM будет выглядеть в будущем”

- Forrester Wave for Vulnerability Risk Management, Q1 2018

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.



Гибкая и масштабируемая архитектура

Множество вариантов разворачивания

Автоматизация

Динамические сканы

# THANK YOU

New Generation Reports

Сканирование мобильных устройств

Агенты

Не только логи

Vulnerability Validation