

# Управление сетевой безопасностью на основе намерений

Алексей Андрияшин, Технический директор

20.09.2018

**SECURITYDAY**

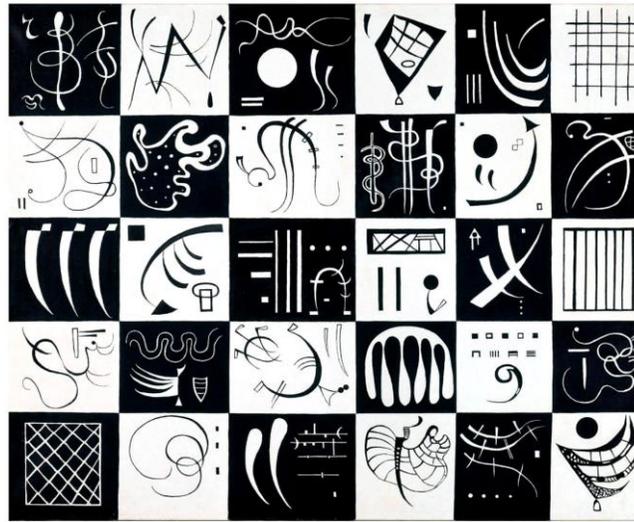
# Мир сильно изменился...

## Облачные вычисления



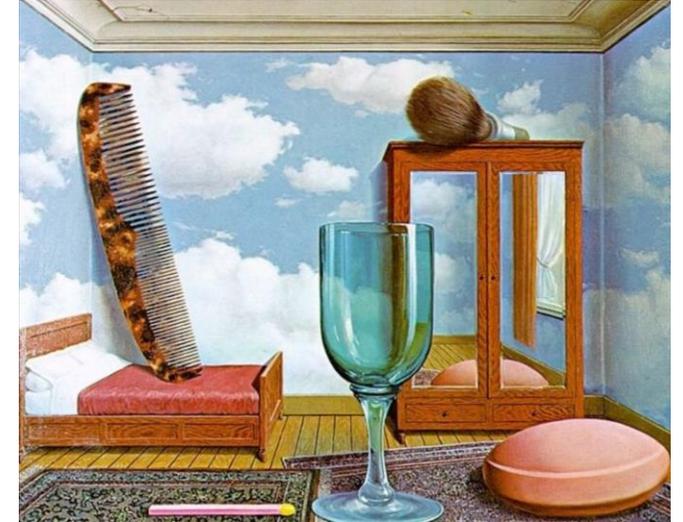
Облака, 1880-е, А.М. Васнецов

## Виртуализация



«Thirty» 1937 г. В. Кандинский

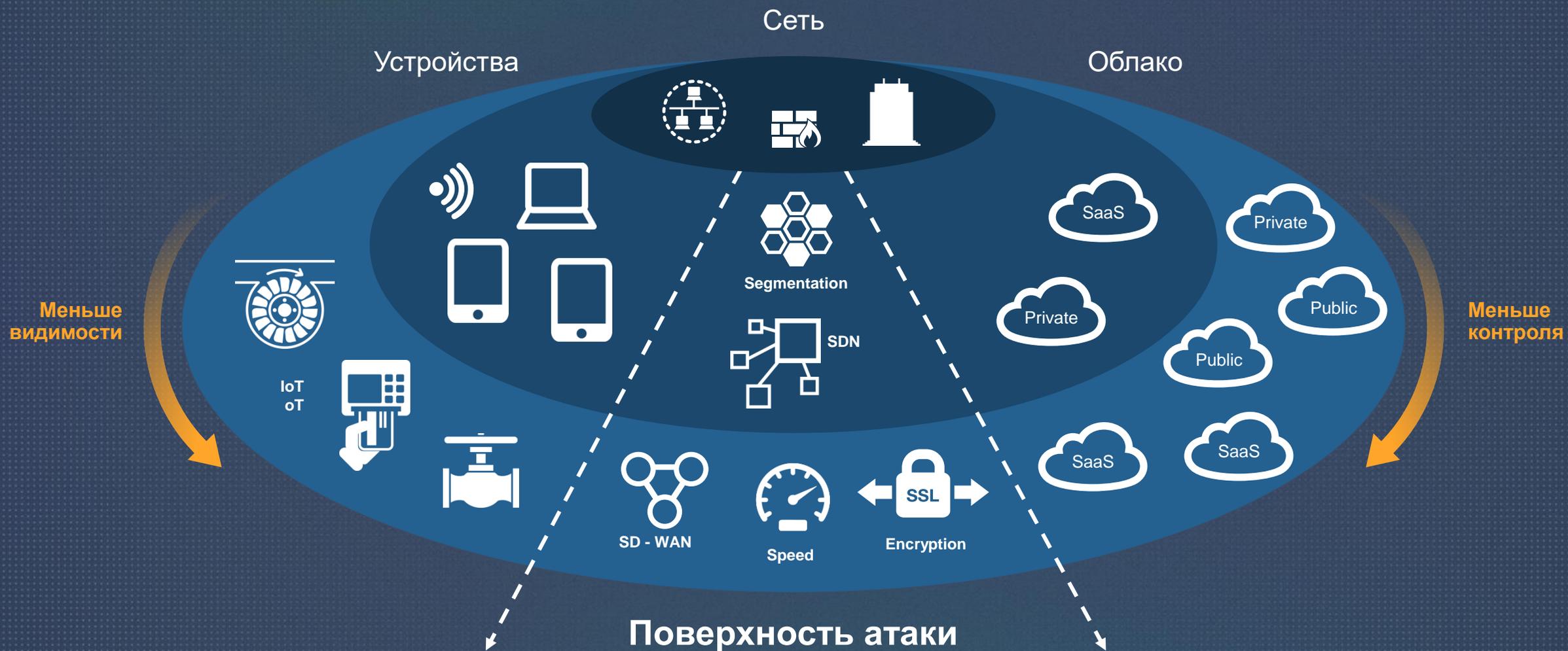
## Интернет вещей, IoT



«Личные ценности» 1937 г., Р. Магритт

...и продолжает меняться

# ЦИФРОВАЯ ТРАНСФОРМАЦИЯ ЗНАЧИТЕЛЬНО РАСШИРЯЕТ ПОВЕРХНОСТЬ АТАКИ

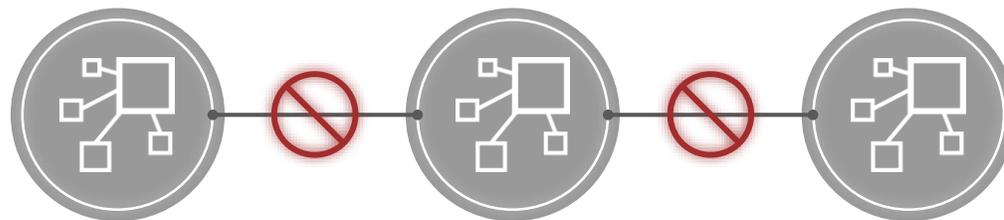


# Как много производителей могут обеспечивать высокий уровень защиты?

ОРКЕСТРАТОР 1

ОРКЕСТРАТОР 2

ОРКЕСТРАТОР N



## МНОЖЕСТВО ПОДСИСТЕМ УПРАВЛЕНИЯ

Skill Set



Appliance



Appliance



Appliance



SaaS



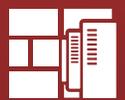
SaaS



IaaS

Form Factor

## МНОЖЕСТВО ПРОИЗВОДИТЕЛЕЙ



# Изучение намерений



- Максимальное **исключение** уязвимостей
- Предотвращение угроз **до** их возникновения
- **Адаптация** к изменениям
- Мгновенная **классификация** угроз
- Устойчивое состояние **защищенности**
- Отсутствие **недопустимых** рисков

Minority Report, 20th Century Fox (North America), DreamWorks Pictures (International), 2002

# Предпосылки развития IBNS

- Облачные технологии
- Микросегментация
- DevOPS
- SDN/SDS/SDDC/SDx
- Большие данные
- Agile
- IoT

Политики устройств безопасности быстро устаревают и **теряют актуальность**

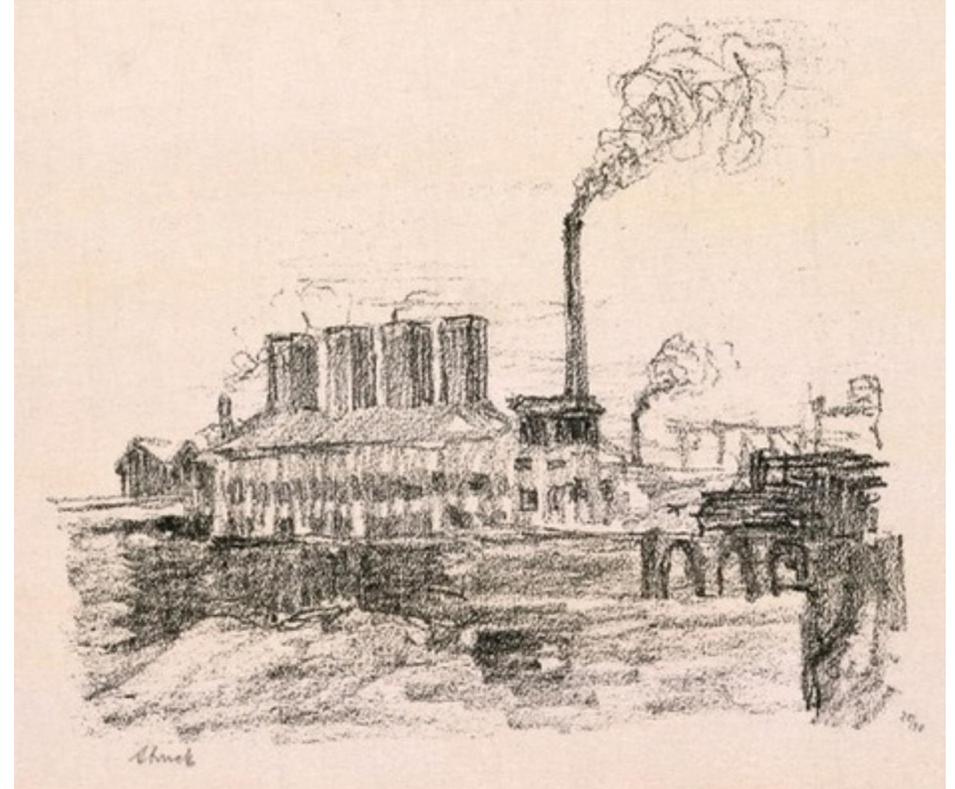
- <https://www.infosecurity-magazine.com/webinars/the-time-for-intentbased-security/>



«Сын человеческий» (1964), М.Рене

# Гибридные технологии

- Безопасность должна учитывать гибридный принцип построения корпоративных сетей:
  - » SDN (software-defined networking,)
  - » SD-WAN (software-defined, WAN)
  - » Hybrid WAN



“Нью Йорк, Фабрика”, Г. Штрук

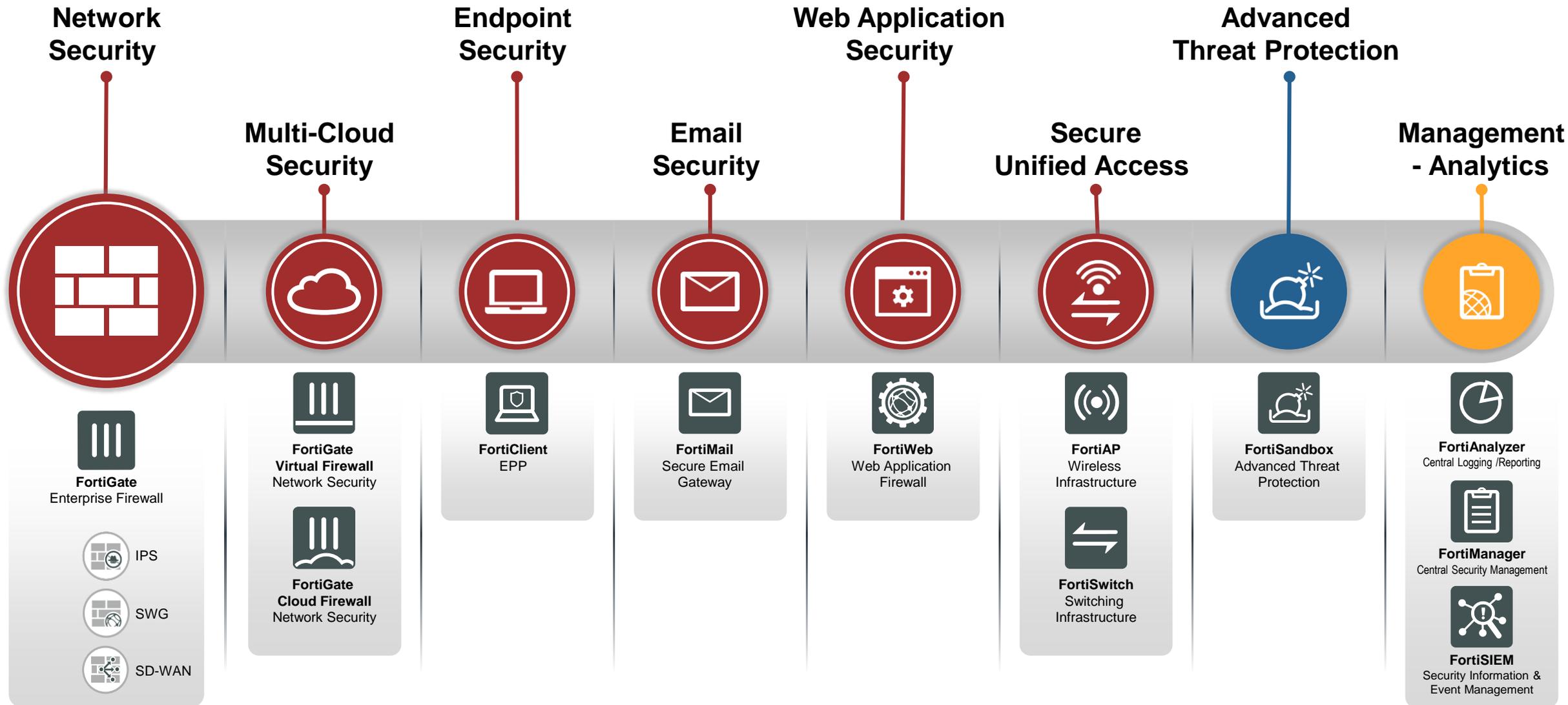
# Ключ к построению IBNS

- Определение желаемого уровня защищенности
- Автоматизация процессов для минимизации ручного описания правил, обеспечивающих необходимый уровень безопасности:
  - » в распределённом окружении
  - » в сетях с высокой сегментацией
  - » при высокой мобильности пользователей и устройств



Н. Ключник "Ключи", 2014

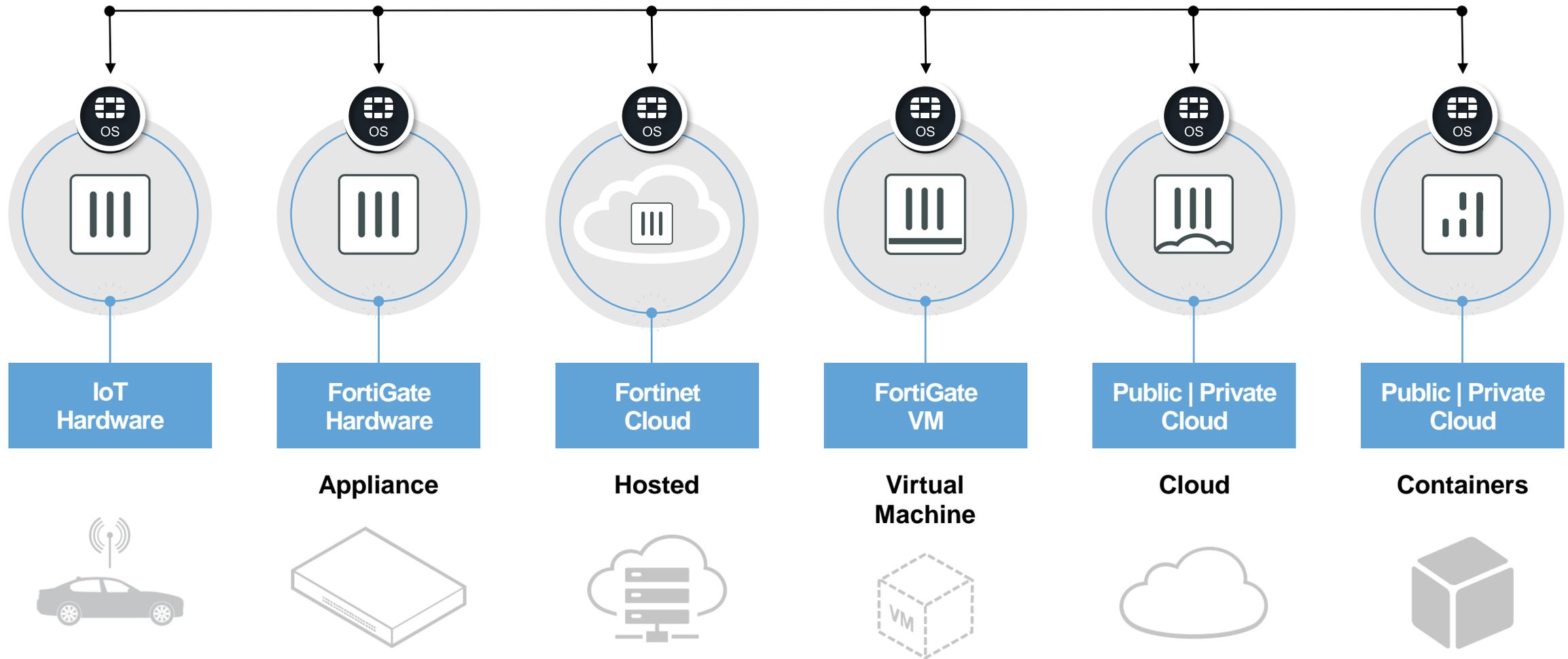
# 2018 Fortinet – Фабрика безопасности



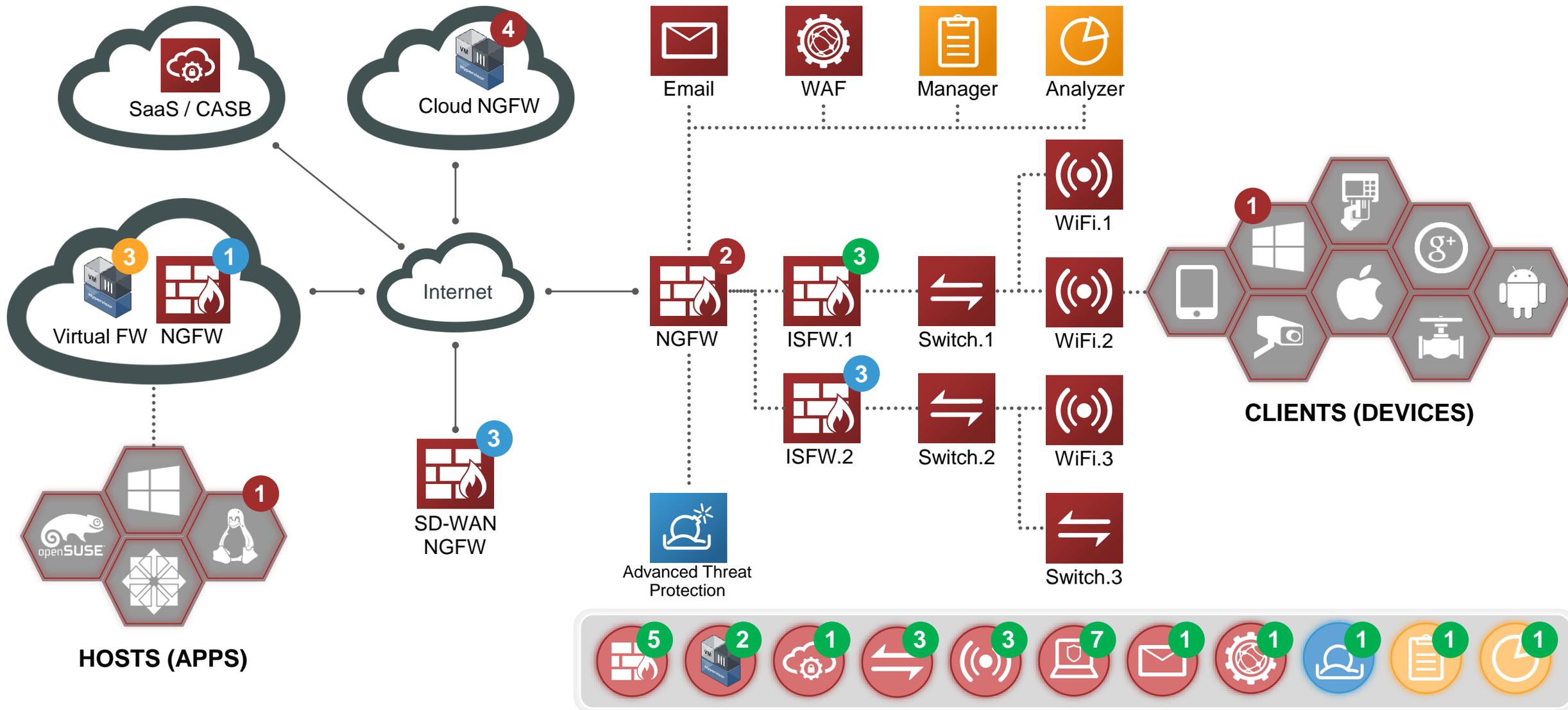
# Адаптивная архитектура безопасности

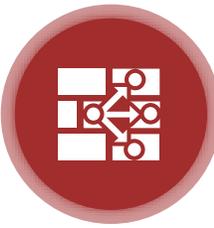
## Оборудование + Программное обеспечение + Сервисы

Сервисы безопасности FortiGuard



# Фабрика безопасности (топология)





## Поддержка приложений

Видимость более чем 3500 приложений

Управление трафиком приложений для соблюдения SLA

## Сетевая гибкость

Динамический выбор маршрута соответствующего SLA

Отказоустойчивость подключений на уровне ISP

## Несколько ISP

Независимый транспорт с поддержкой Ethernet, 3G/4G

Объединение нескольких интерфейсов в один логический SD-WAN

## Эффективное управление

Один клик для подключения нескольких филиалов к центру обработки данных

Минимальное количество ресурсов для подключения удаленной точки

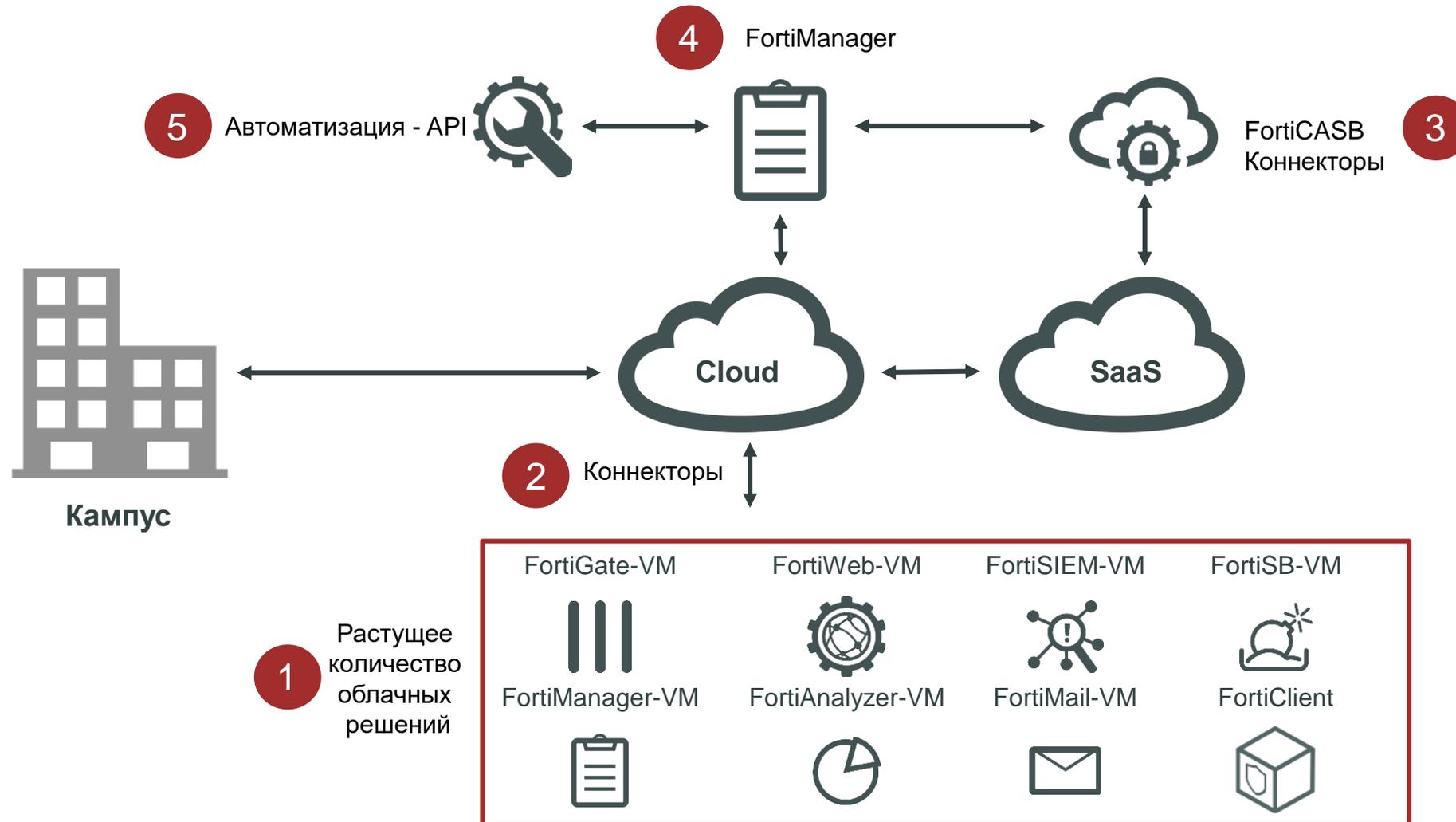
## Проверенные решения

Проверено NSS Lab и многими сторонними компаниями

Высокая производительность, обеспеченная аппаратными Security Processor

# Облачные решения Fortinet

Коннекторы

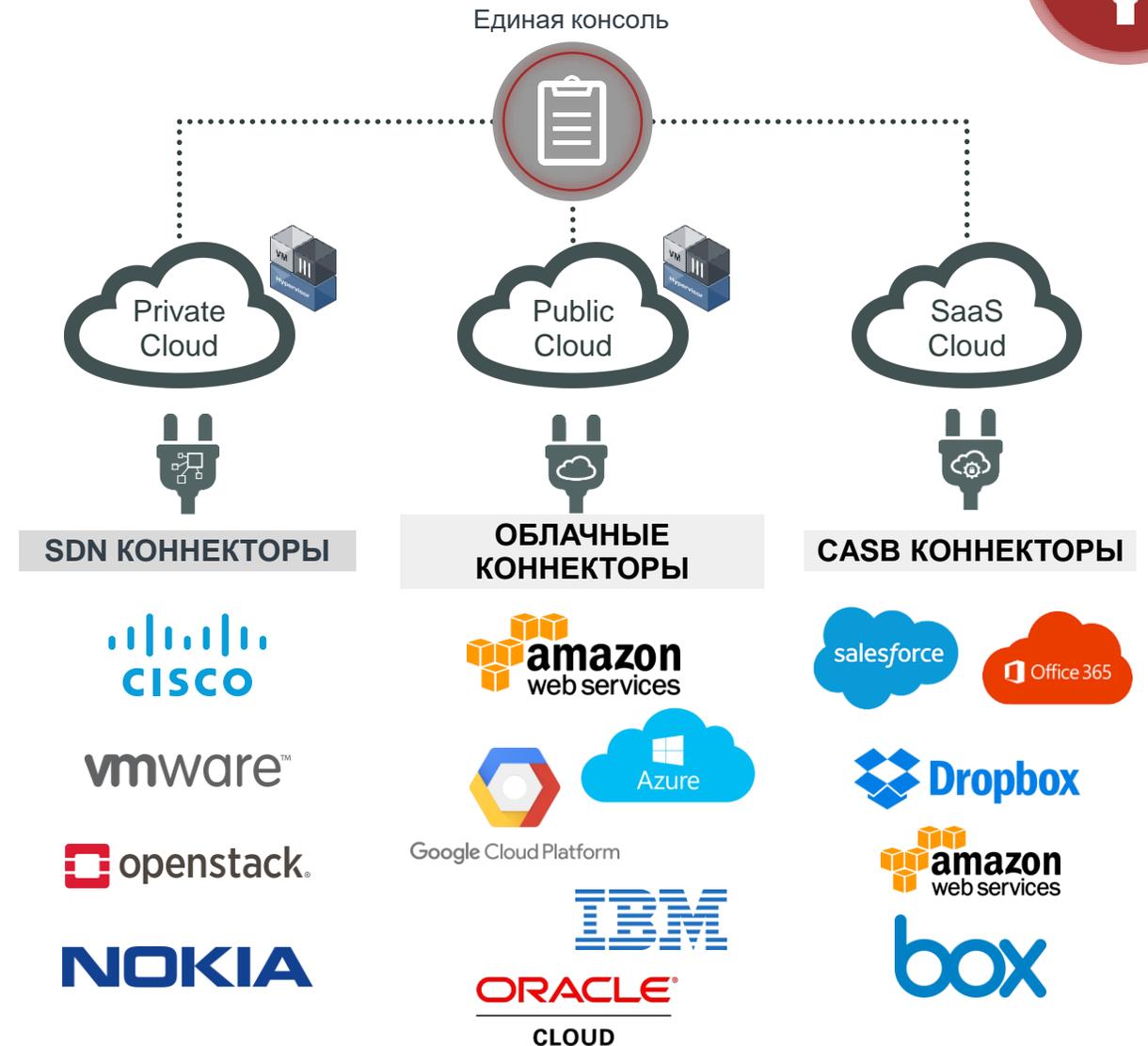
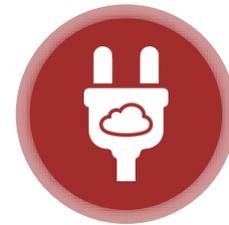


# Облачные коннекторы



Virtual Security	Cloud Security	API
Applications	Applications	Applications
Data	Data	Data
O/S	O/S	O/S
Virtualization	Virtualization	Virtualization
Servers	Servers	Servers
Networking	Networking	Networking

Коннекторы



# Сервисы безопасности FortiGuard

FortiGuard



## Baseline Protection

- IP Reputation
- Internet DB
- Certificate & Domain White List
- Application Control
- Antispam



+

## Threat Protection

- Antivirus
- Intrusion Prevention



## Unified Protection

- Web Filtering
- Antivirus
- Intrusion Prevention



## Enterprise Protection

- Virus Outbreak Service
- Content Disarm & Reconstruction
- FortiSandbox Cloud
- Web Filtering
- Antivirus
- Intrusion Prevention



Industrial Security Service



Security Audit Service

# Адаптивный анализ защищенности

Security Rating



# Агенты безопасности и защита конечных точек

Поддержка хостов и конечных точек

Fabric Agent



# Автоматизация процессов ИБ

Автоматизация



System  
Events



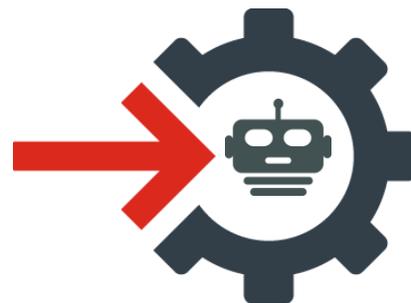
Threat  
Alerts



User & Device  
Status



External  
Inputs



Notification



Reports



Quarantine



Adjust  
Configuration

ТРИГГЕРЫ

АВТОМАТИЗАЦИЯ

ДЕЙСТВИЯ

Автоматизация процессы безопасности с использованием триггеров для выполнения соответствующих действий

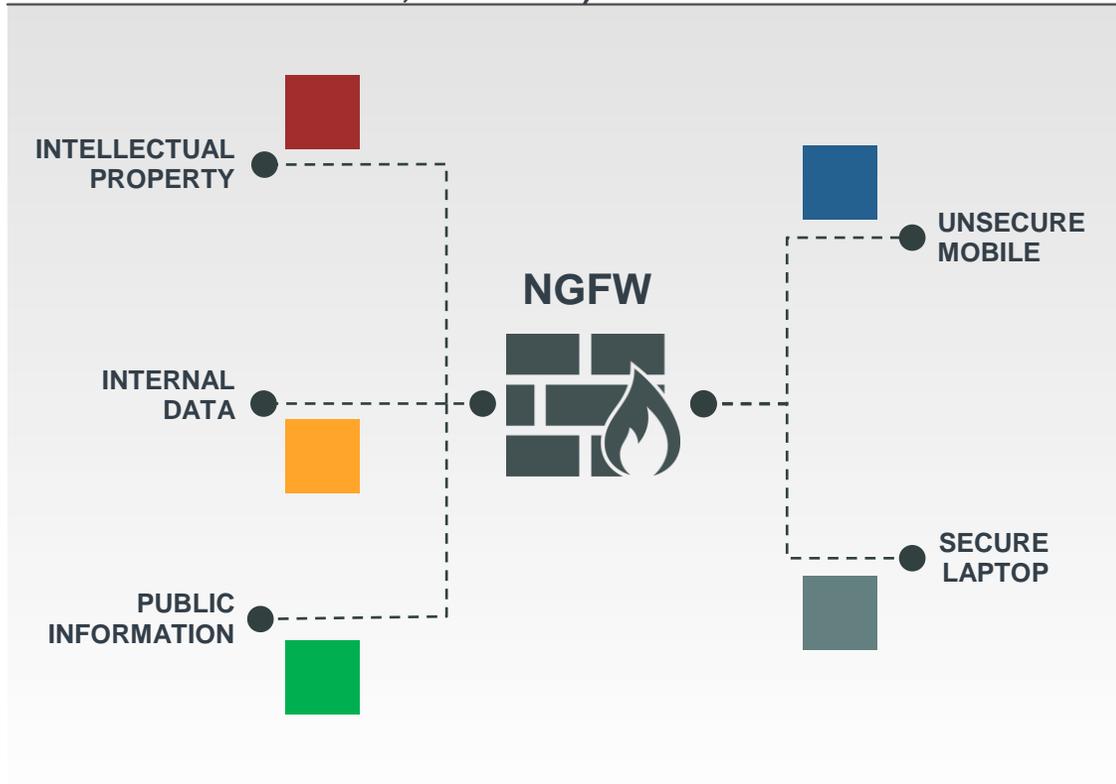
# Безопасность на основе намерений (IBNS)

## Бизнес логика при реализации политик безопасности

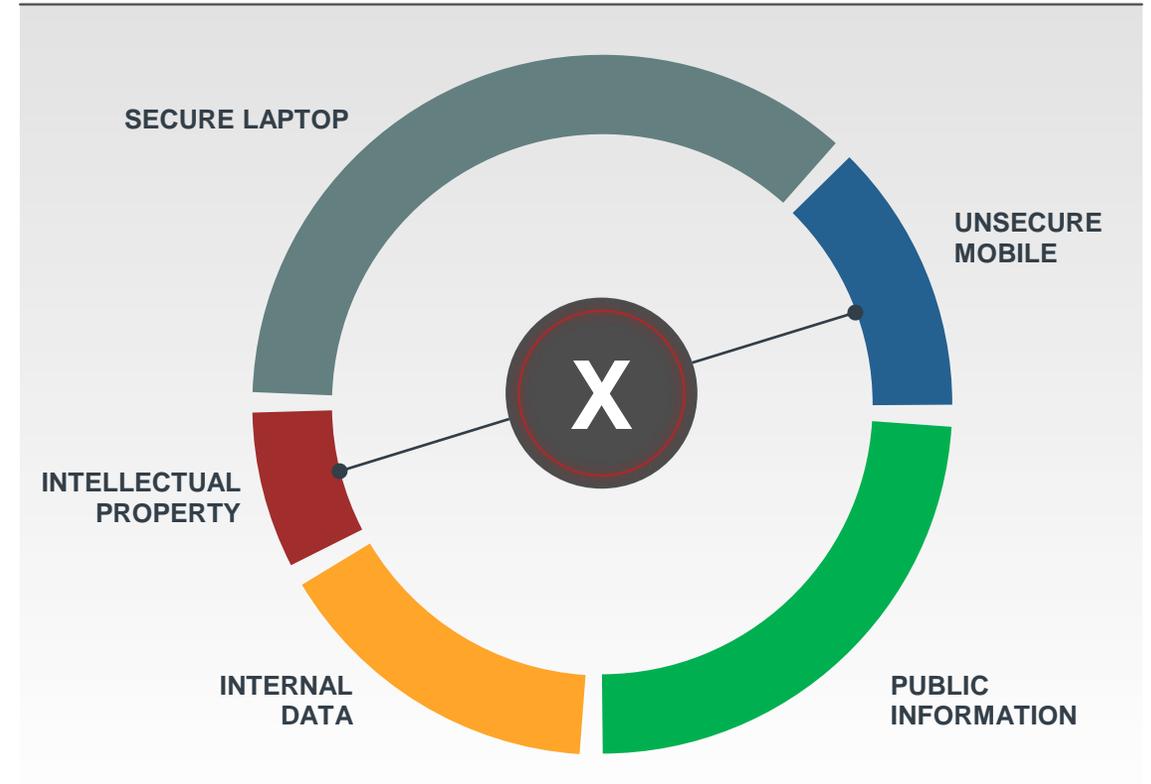
Тегирование



ТЕГИРОВАНИЕ (УСТРОЙСТВА, ИНТЕРФЕЙСЫ, ОБЪЕКТЫ)



ГЛОБАЛЬНАЯ ПОЛИТИКА



## УПРАВЛЕНИЕ

## Удобство мониторинга и отчетности



## ОТЧЕТЫ БЕЗОПАСНОСТИ

Новые шаблоны отчетов для менеджмента / С-уровня и аудиторов



**Prepare**

Figure 4: Network Topology

Figure 17: Summary of Changes

**Protect**

Pro-2 Change Control - Security

Overview

This category provides awareness to all changes made. The information will list the overall number of changes, includes the zone name, date/time of the change, user comments.

Risk

Not implementing change control processes can result in unauthorized manner and could increase potential for risk.

Recommendations

Review each change in this report and cross-reference documented and approved by management. If you do one, it can be a simple document outlining the change how to record the change, how will the change effect it how will the change be implemented if approved instead.

Figure 17: Summary of Changes

**Review Sections**

Quick View

This section provides a quick view into the aggregate severity level of findings for each functional area allowing you to prioritize your focus. Below is a description of risk levels.

Function	Score
Prepare	High (Score 4.5)
Protect	High (Score 4.5)
Detect	High (Score 4.5)
Respond & Recover	High (Score 4.5)

High - Significant impact to information and services  
Medium - Some impact to information and services  
Low - Minimal impact to information and services

**Situation Awareness Report Sections**

The following is a brief description of each functional area and its importance to a strong security posture.

<b>Prepare</b>	If you don't know what is on your network how can you begin to adequately protect it. The Prepare functional area is focused on assisting with continuous understanding your other environment and critical areas. This includes providing awareness of your cyber assets such as endpoints and servers, applications including SaaS, network topology and user accounts accessing security devices.
<b>Protect</b>	Once you have a good understand of your other environment you can now start to protect your other assets. The Protect functional area is focused on assisting you with the continuous protection of your cyber assets allowing you to limit or reduce the potential impact of a cybersecurity event. This includes providing awareness of your baseline security configuration, change control, vulnerabilities and remediation efforts and remote access to external cyber assets.
<b>Detect</b>	As the attack surface increases so does the volumes of threats making it important to detect events in a timely manner and understand the potential impact. The Detect Functional area is focused on assisting you with continuous monitoring to understand threats detected against your network. This includes providing awareness on your data flows, top attack targets, top malware detected, security events and compliance violations and ensuring log integrity.
<b>Respond &amp; Recover</b>	As evasion techniques continue to increase in sophistication it is becoming more important to not only quickly identify threats, but also respond to and recover from them. The Respond/Recover functional area is focused on assisting you with responding to and recovering from an identified breach within your network. This includes providing continuous awareness of unknown threats identified within the network and containment of those threats.

**Recover**

Count Opened vs Closed by Date

Number of incidents opened vs closed by day for the last 7 days.

Incidents By Severity

44

Critical High Medium Low

Containment

Awareness of the containment status for identified breaches within the network. The information will include the associated information including potential victims host name, Mac and IP address, the zone the breach is in, status of the breach and the time it occurred.

Capabilities can result in drastically reduced ability to perform adequate incident triage and return increase the impact damage of a breach to critical systems and sensitive data. It could also legal and compliance liabilities which could result in fines and reputation loss.

УПРАВЛЕНИЕ

# Удобство мониторинга и отчетности



## ВИДЖЕТЫ ДЛЯ МОНИТОРИНГА

Дополнительные виджеты мониторинга в FAZ



### Ransomware Activities in Your Network

Last 2 Years

- This Year
- Last Year
- Last 2 Years
- Last 3 Years
- Last 4 Years

2016 2017

### Vulnerable to WannaCry

**John Smith**

- jsmith
- johnsmith
- J\_Smith

- Windows 10 professional
- IP Address: 172.16.79.215
- MAC Addresses: 94:57:a5:e3:d2:a5
- FortiClient Telemetry @ : Connected

### WannaCry

**10** Vulnerable Hosts  
14 Total Hosts

**Description:** WannaCryptor!tr is a generic detection that utilizes exploits identified in Microsoft Windows SMB Server (4013389)

<b>Type:</b> Ransomware, Trojan	<b>AV Signature:</b>	<b>Vulnerability Criteria:</b>
<b>Severity:</b> Critical	W32/CVE_2017_0147.A!tr	XP 10
<b>CVE ID:</b> CVE-2017-0144, CVE-2017-0145, CVE-2017-0147	W32/Farfli.ATVE!tr.bdr	Vista Server 2008/R2
<b>Patch:</b> Microsoft 17-010	W32/Filecoder_WannaCryptor.B!tr	7 Server 2012/R2
<b>IPS Signatures:</b> MS.SMB.Server.SMB1.Trans2...	W32/Filecoder_WannaCryptor.D!tr	8/8.1/RT 8.1 Server 2016
	W32/Gen.DKT!tr	
	W32/Gen.DLG!tr	
	W32/GenKryptik.1C25!tr	

### Malware Activities

**12** Ransomware Incidents

- Exploits blocked by IPS
- Botnet C2 blocked by AV
- Malicious websites access blocked by Web Filter
- Malicious email attachments blocked by AV
- Outbound Tor traffic blocked by App Control

**russia@fortinet.com**

The logo for FERTINET is displayed in a bold, white, sans-serif font. The letter 'F' is stylized with three horizontal bars. The letters 'E', 'R', 'T', 'I', 'N', and 'E' are solid. The final 'T' is also solid. A registered trademark symbol (®) is located to the right of the final 'T'. The background is a solid blue color with a complex, white, geometric pattern of overlapping lines and rectangles, creating a sense of depth and structure.

**FERTINET®**