

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

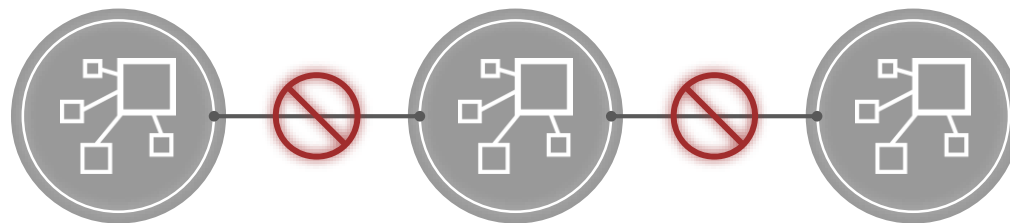


Как много производителей могут обеспечивать высокий уровень защиты?

ОРКЕСТРАТОР 1

ОРКЕСТРАТОР 2

ОРКЕСТРАТОР N



МНОЖЕСТВО ПОДСИСТЕМ УПРАВЛЕНИЯ

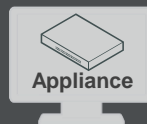
Skill Set



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**

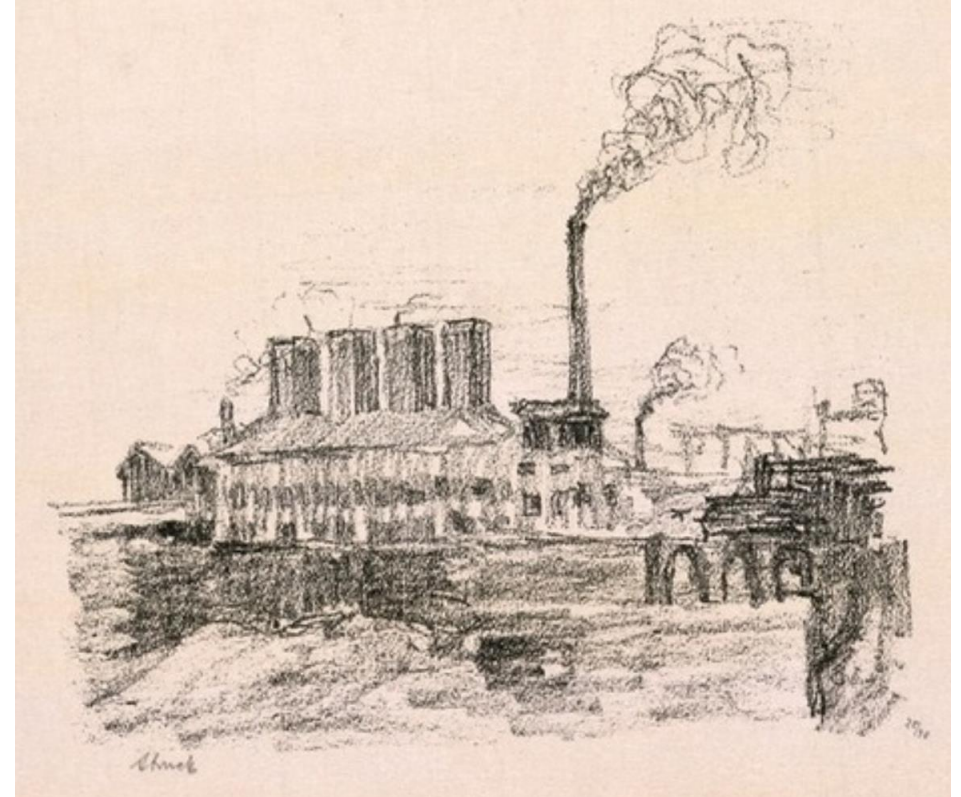
- <https://www.infosecurity-magazine.com/webinars/the-time-for-intentbased-security/>



«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

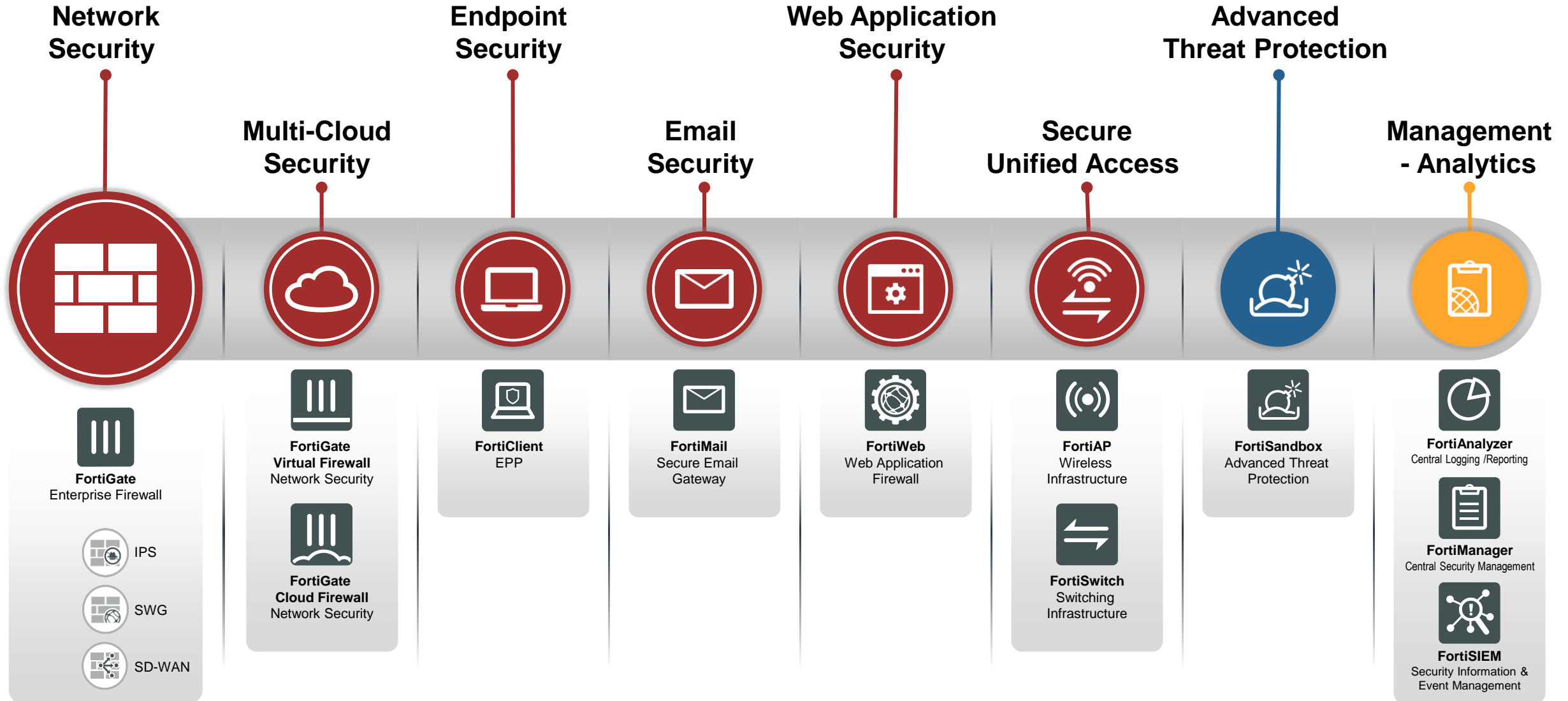
Ключ к построению IBNS

- 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

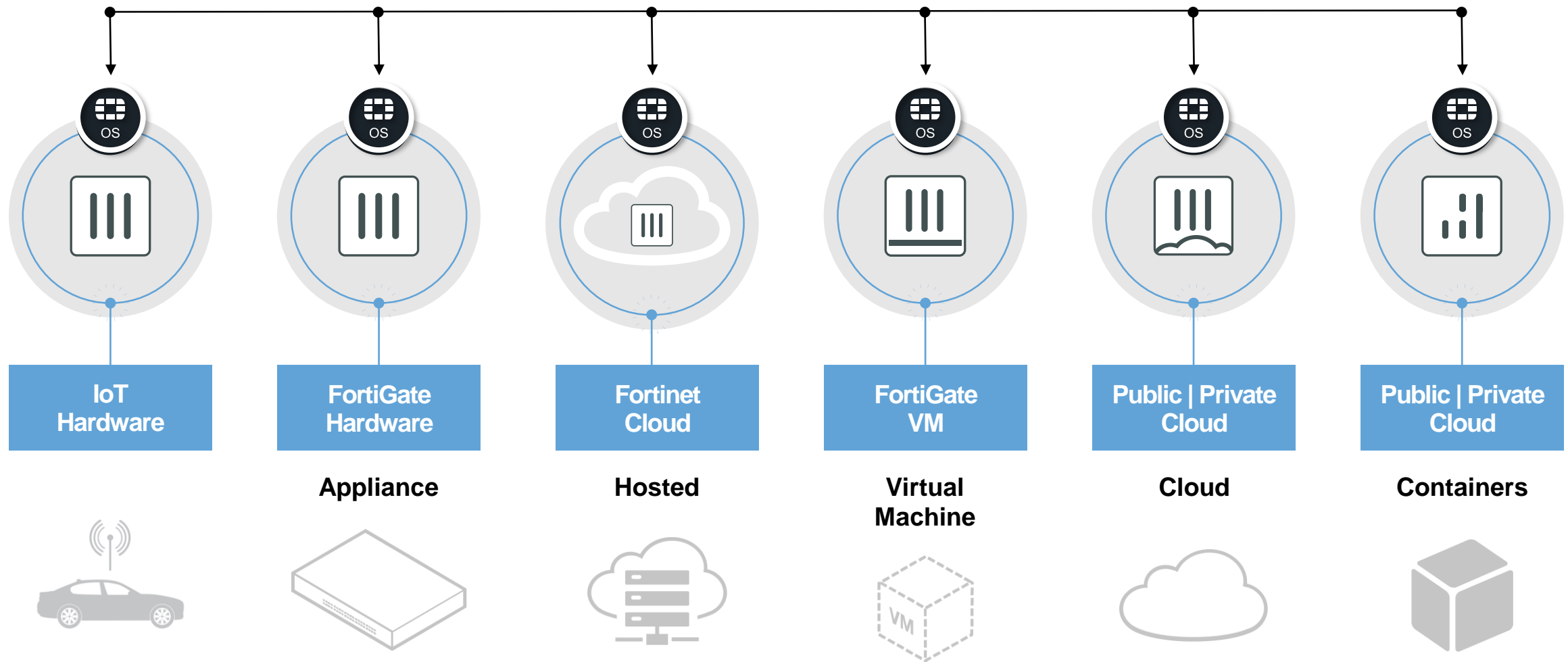
2018 Fortinet – Фабрика безопасности



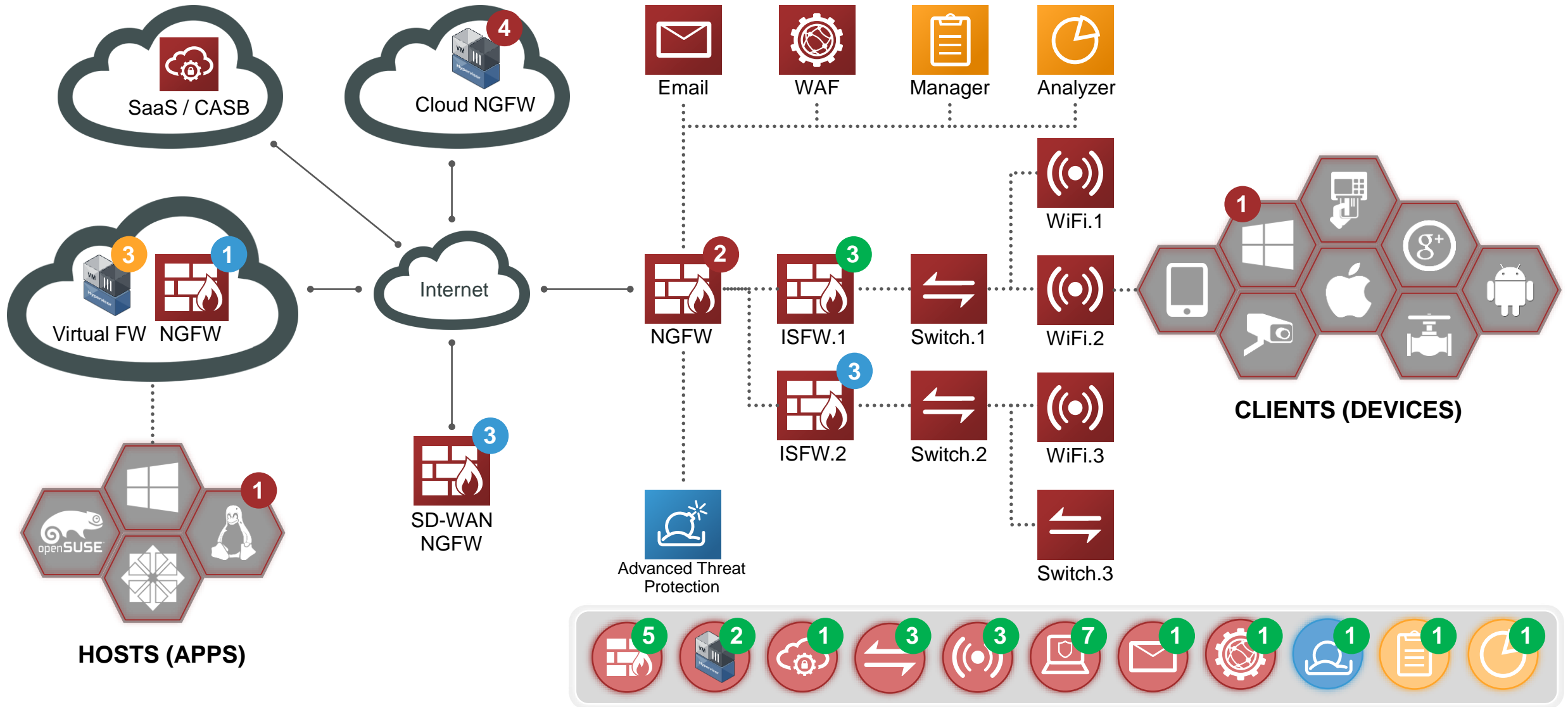
Адаптивная архитектура безопасности

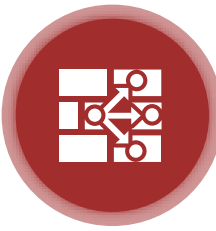
Оборудование + Программное обеспечение + Сервисы

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

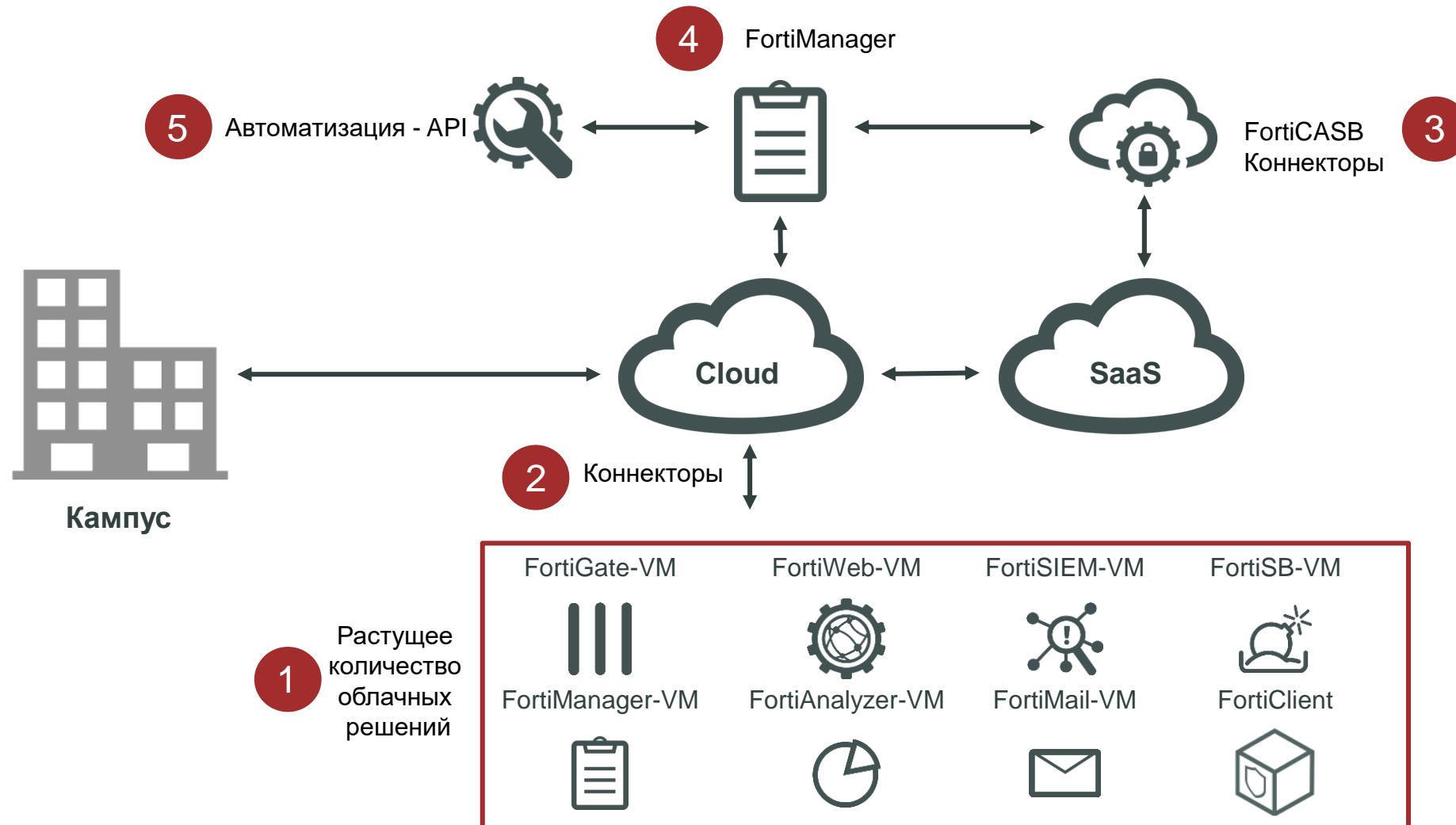
Проверенные решения

Проверено NSS Lab и многими сторонними компаниями

Высокая производительность, обеспеченная аппаратными Security Processor

Облачные решения Fortinet

Коннекторы

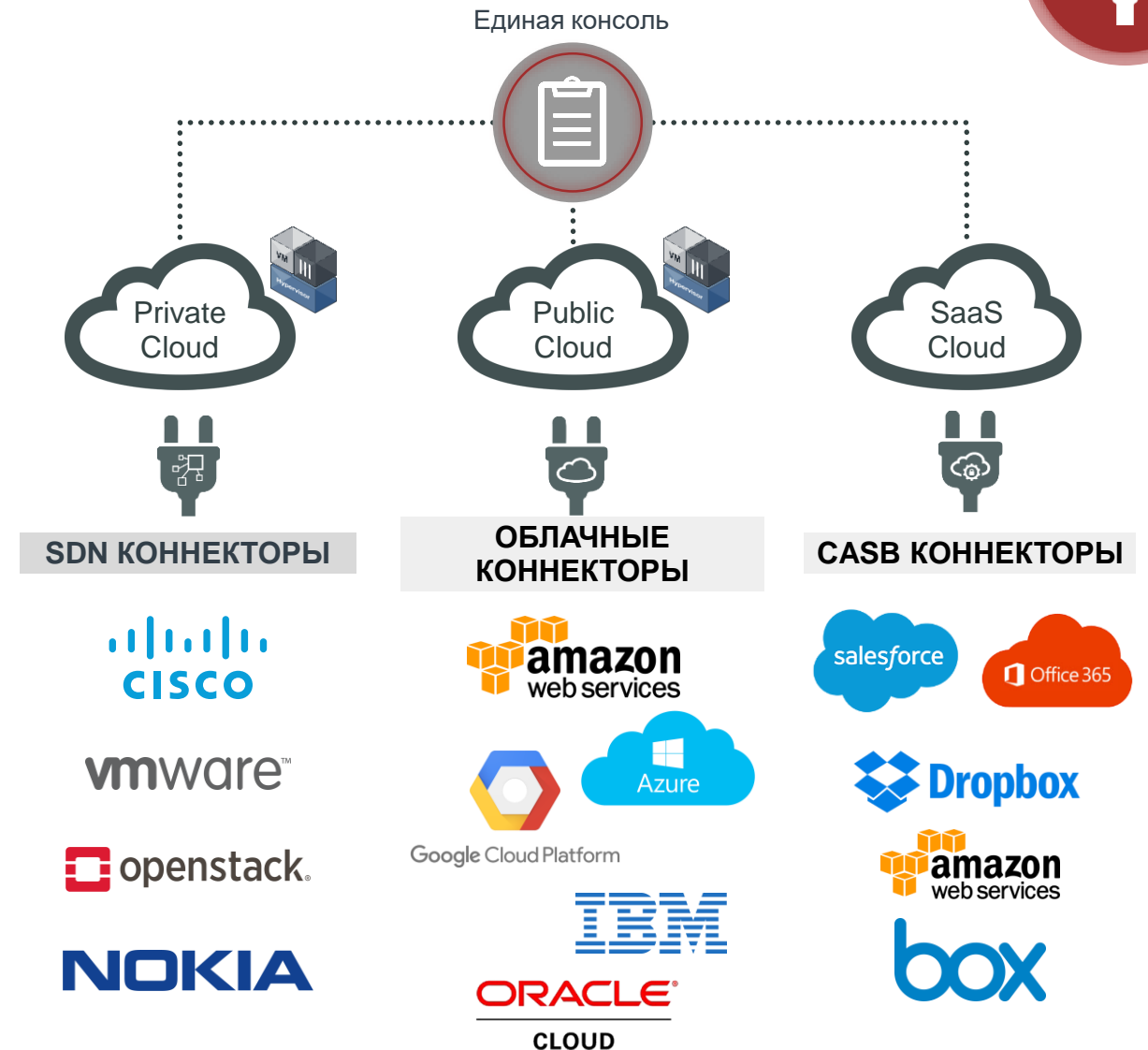
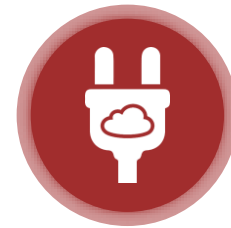


Облачные коннекторы



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



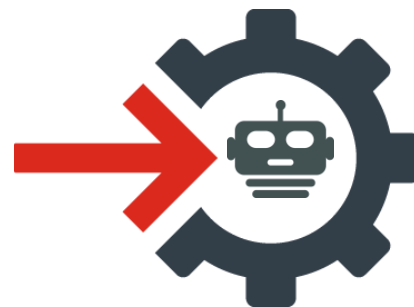
Threat
Alerts



User & Device
Status



External
Inputs



Notification



Reports



Quarantine



Adjust
Configuration

ТРИГГЕРЫ

АВТОМАТИЗАЦИЯ

ДЕЙСТВИЯ

Автоматизация процессы безопасности с использованием триггеров для выполнения соответствующих действий

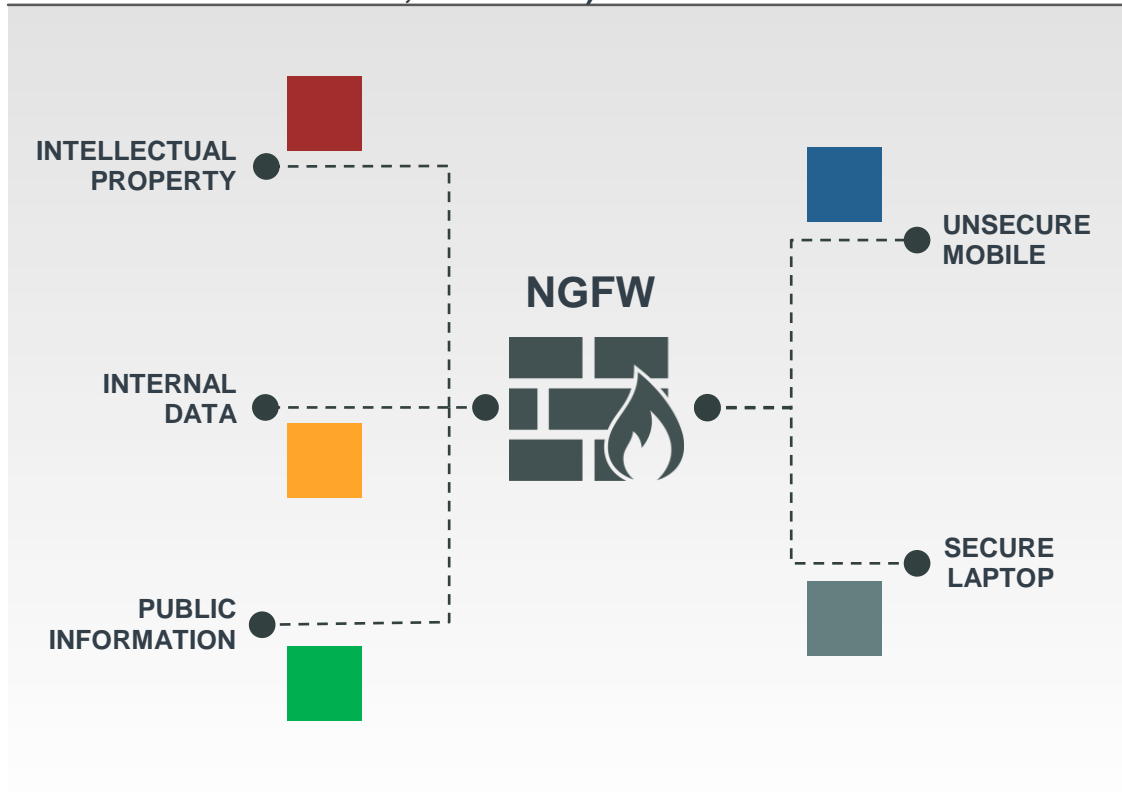
Безопасность на основе намерений (IBNS)

Бизнес логика при реализации политик безопасности

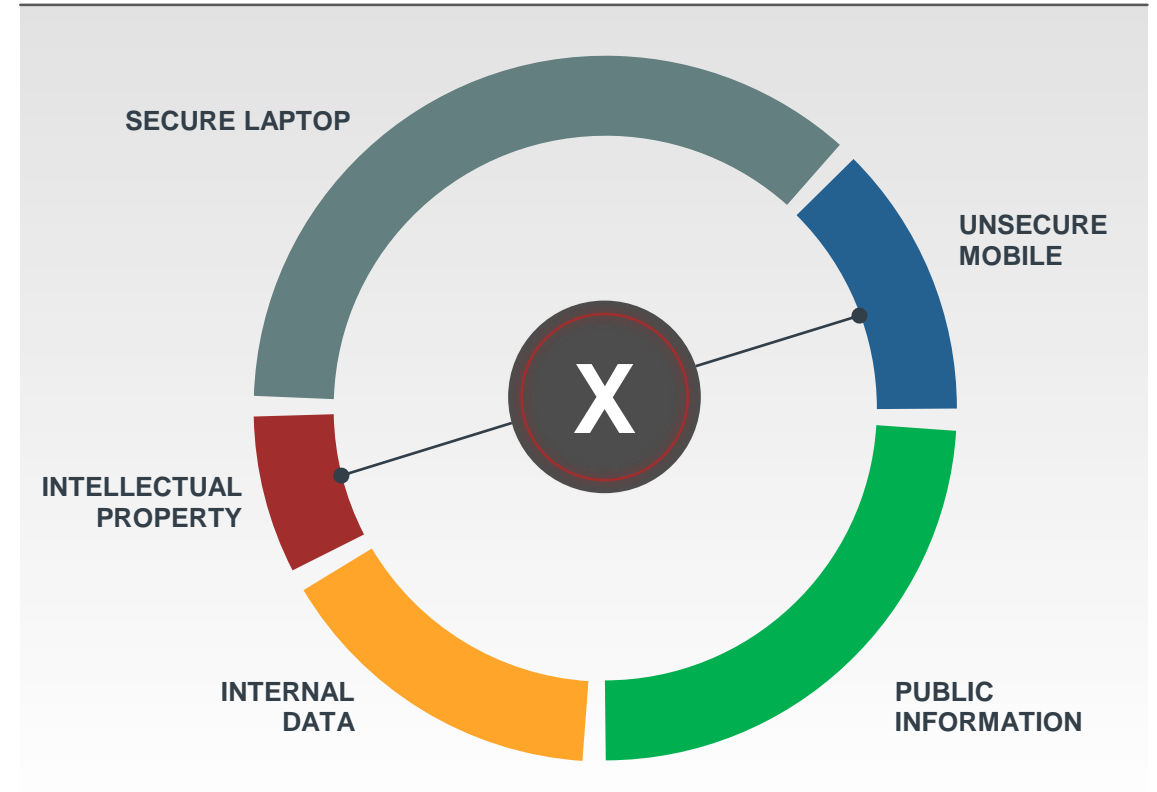
Тегирование



ТЕГИРОВАНИЕ (УСТРОЙСТВА, ИНТЕРФЕЙСЫ, ОБЪЕКТЫ)



ГЛОБАЛЬНАЯ ПОЛИТИКА



УПРАВЛЕНИЕ

Удобство мониторинга и отчетности



ОТЧЕТЫ БЕЗОПАСНОСТИ

Новые шаблоны отчетов для менеджмента / C-уровня и аудиторов



Prepare

Figure 4: Network Topology

Figure 17: Summary of Changes

Prep-2 Application Inventory

Overview

The category provides awareness to the operating systems and applications that reside on the endpoints installed on the network. The charts below show the top 5 operating systems and top 5 applications of Microsoft systems. For a complete detailed list of applications please see Appendix.

Risk

No ability to determine operating systems and software on the network will drastically reduce the risk address vulnerabilities and will increase the potential for system compromise, downtime and data loss.

Recommendations

Review the operating systems and applications installed to ensure they are authorized to exist on the network. If you do not have an authorized list of applications use this information to identify unauthorized applications. Review the operating systems and applications installed to ensure they are authorized to exist on the network. If you do not have an authorized list of applications use this information to identify unauthorized applications. This will help your attack surface and help reduce the overall risk of a breach.

Protect

Pro-2 Change Control - Security

Overview

This category provides awareness to all changes made to the network. 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 changes being made to the network in an unauthorized manner and could increase potential for system compromise, downtime and data loss.

Recommendations

Review each change in this report and cross-reference documented and approved by management. If you do not have a simple document outlining the change how to record the change, how will the change effect the network, how will the change be implemented if approved instead of implemented as is.

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 3.5)
Detect	High (Score 2.5)
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.

Prepare	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.
Protect	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.
Detect	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.
Respond & Recover	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.

Legend: Outlook, IFA, Twitter, Gmail, Microsoft SaaS, Dropbox

Recover

Count Opened vs Closed by Date

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

Legend: Opened, Closed

Incidents By Severity

Legend: 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.

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

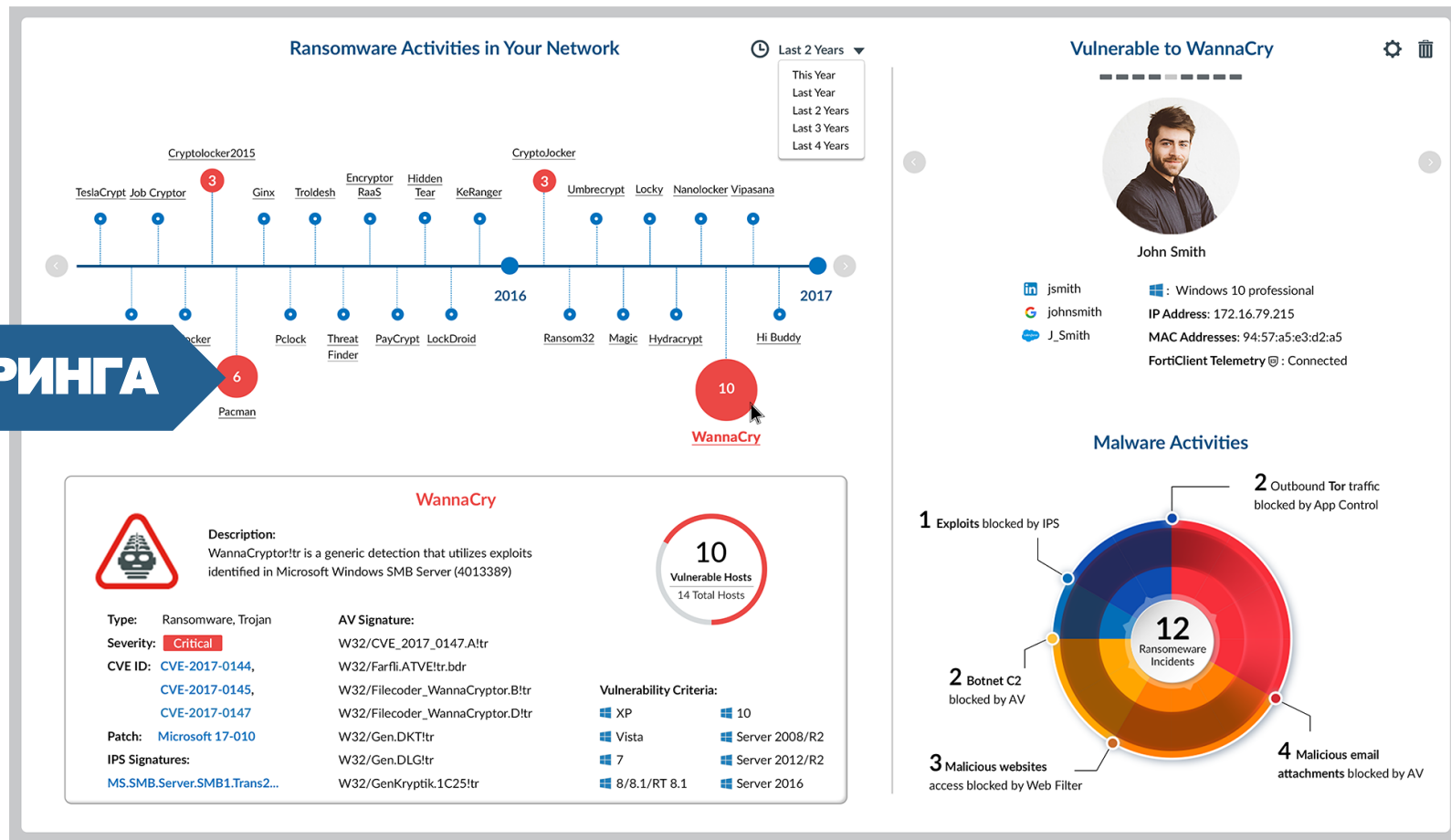
УПРАВЛЕНИЕ

Удобство мониторинга и отчетности



ВИДЖЕТЫ ДЛЯ МОНИТОРИНГА

Дополнительные виджеты мониторинга в FAZ



russia@fortinet.com

The logo for FERTINET is centered on a dark blue background. The word "FERTINET" is written in a bold, white, sans-serif font. The letter "E" is stylized with three horizontal bars. A registered trademark symbol (®) is located at the end of the word. The background features a complex, white, isometric wireframe pattern of overlapping rectangular and cubic shapes, creating a sense of depth and architectural structure.

FERTINET®