ИНФОСИСТЕМЫ ДЖЕТ

# Угрозы и тенденции рынка информационной безопасности. Защита от атак «нулевого» дня

Юрий Черкас,
руководитель направления инфраструктурных ИБ-решений
Центра информационной безопасности
компании «Инфосистемы Джет»

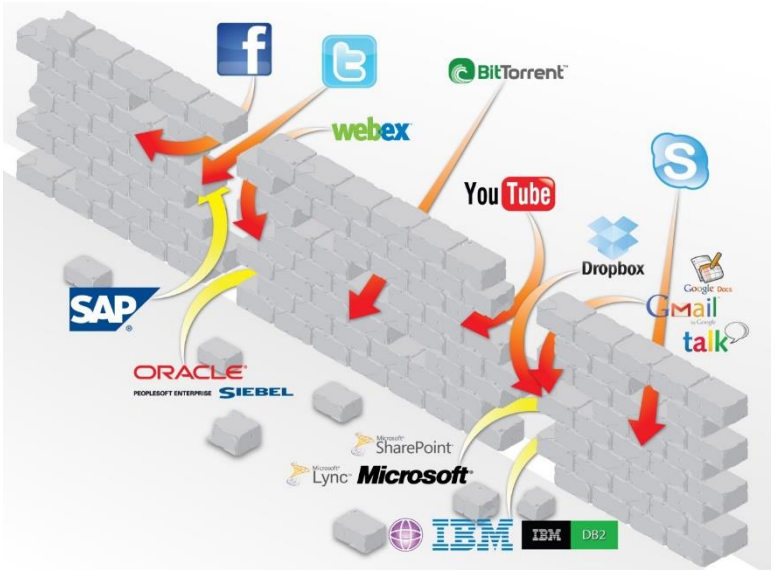
ИНФОСИСТЕМЫ ДЖЕТ


*Конфуций*
*551 – 479 г. до н.э.*

*«Изучайте прошлое, если хотите предсказать будущее»*

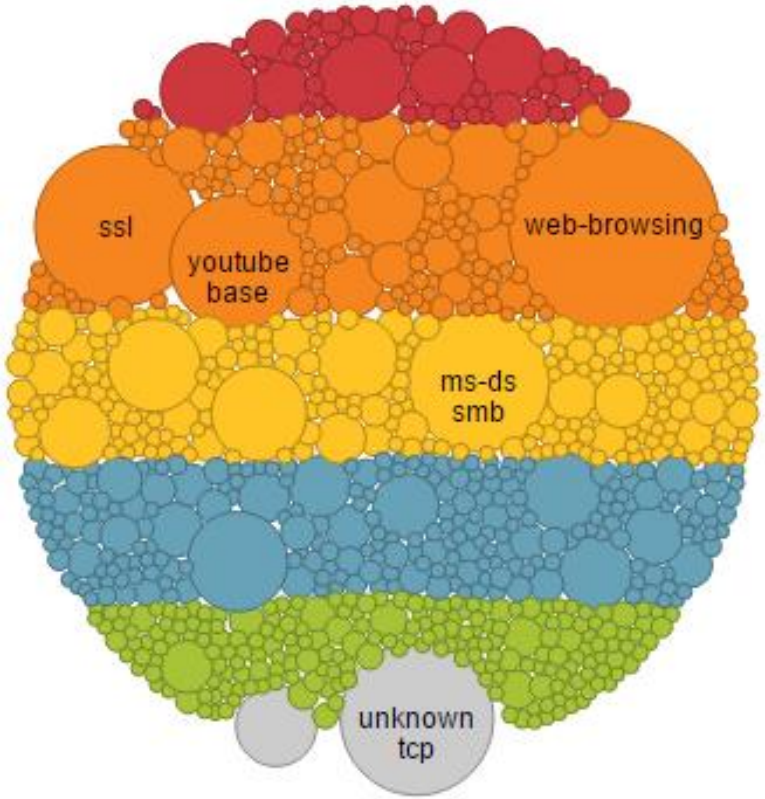
# Как изменилась сеть?

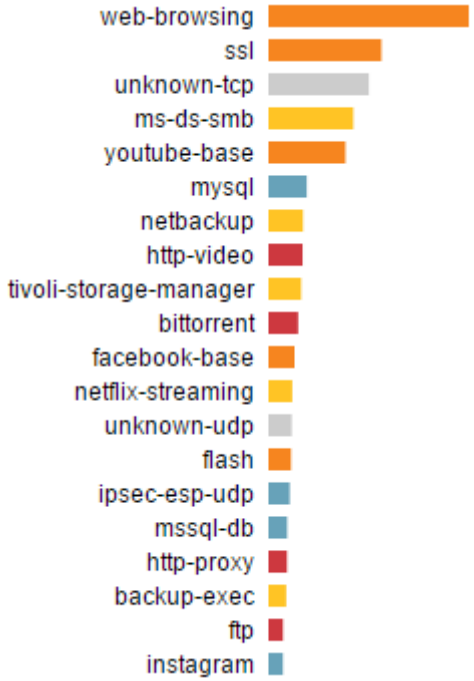
- Использование мобильного доступа (при помощи VPN, смартфонов, планшетов и т.п.) размывает понятие «периметра»
- Динамичное развитие корпоративных систем и бизнес-приложений требует постоянного изменения правил фильтрации на МЭ
- Фильтрация на основе IP-адреса, протокола и порта становится неэффективной и требуется контроль конкретных приложений и пользователей



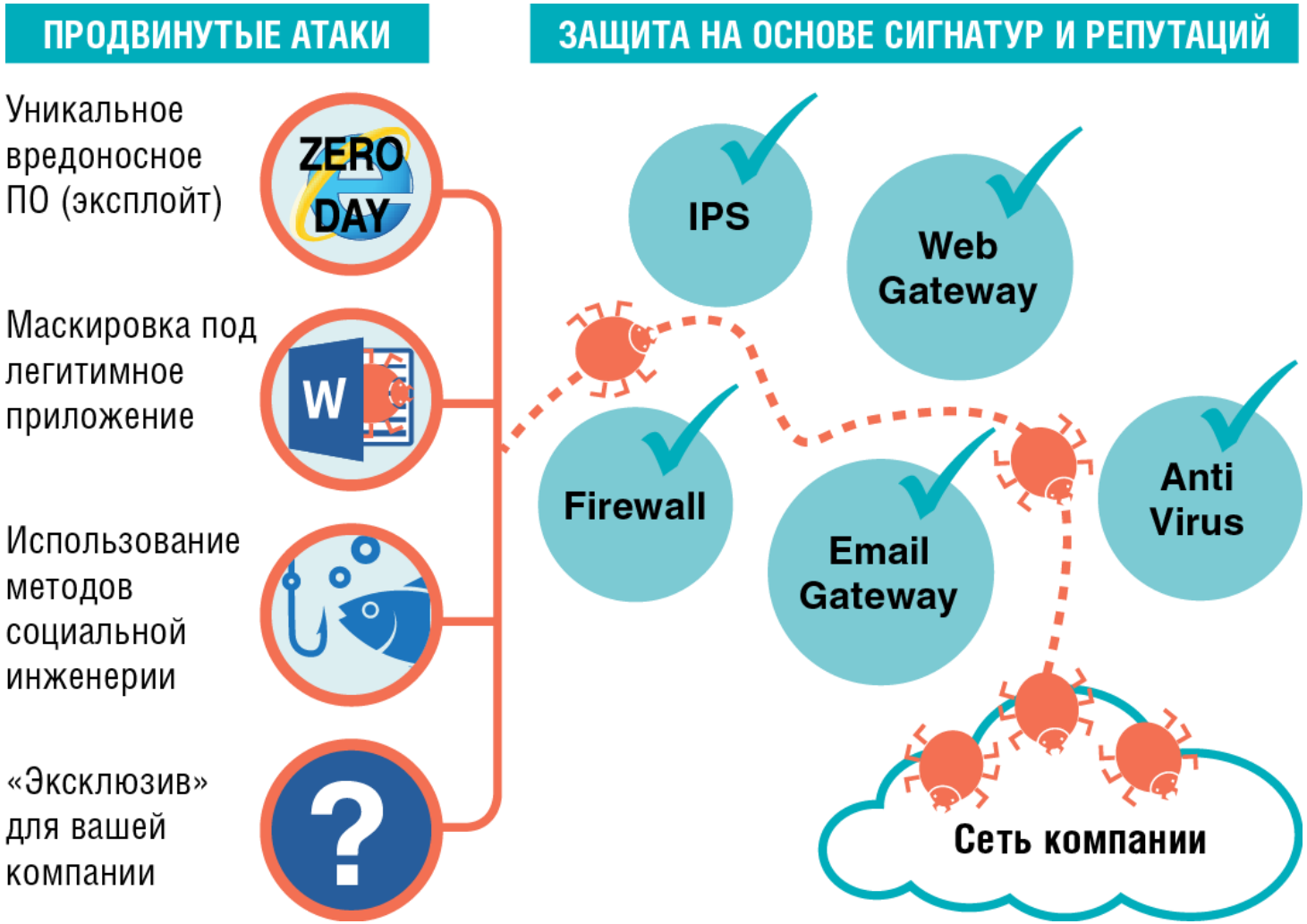
# От IP-адресов и портов к приложениям

## А Вы знаете все свои приложения в сети?



# Как изменились атаки?

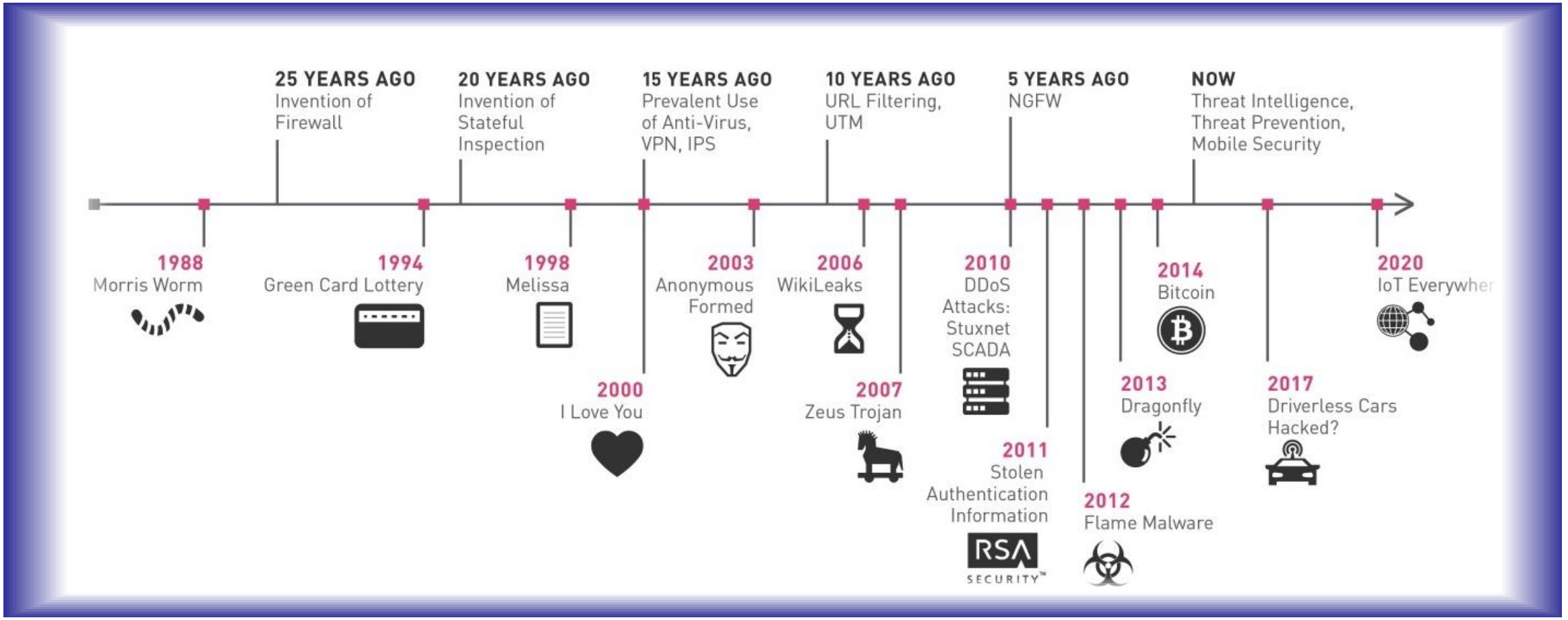



**Техники обхода стали доступным инструментом**

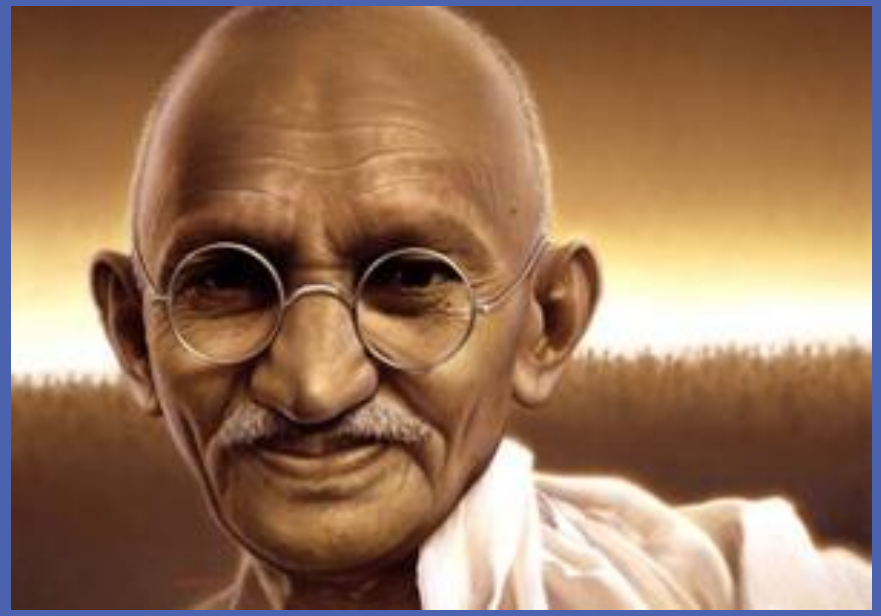
**Вирус для конкретного пользователя – это не фантастика!**

# Check Point Security Report 2015

## Эволюция malware и типы атак:



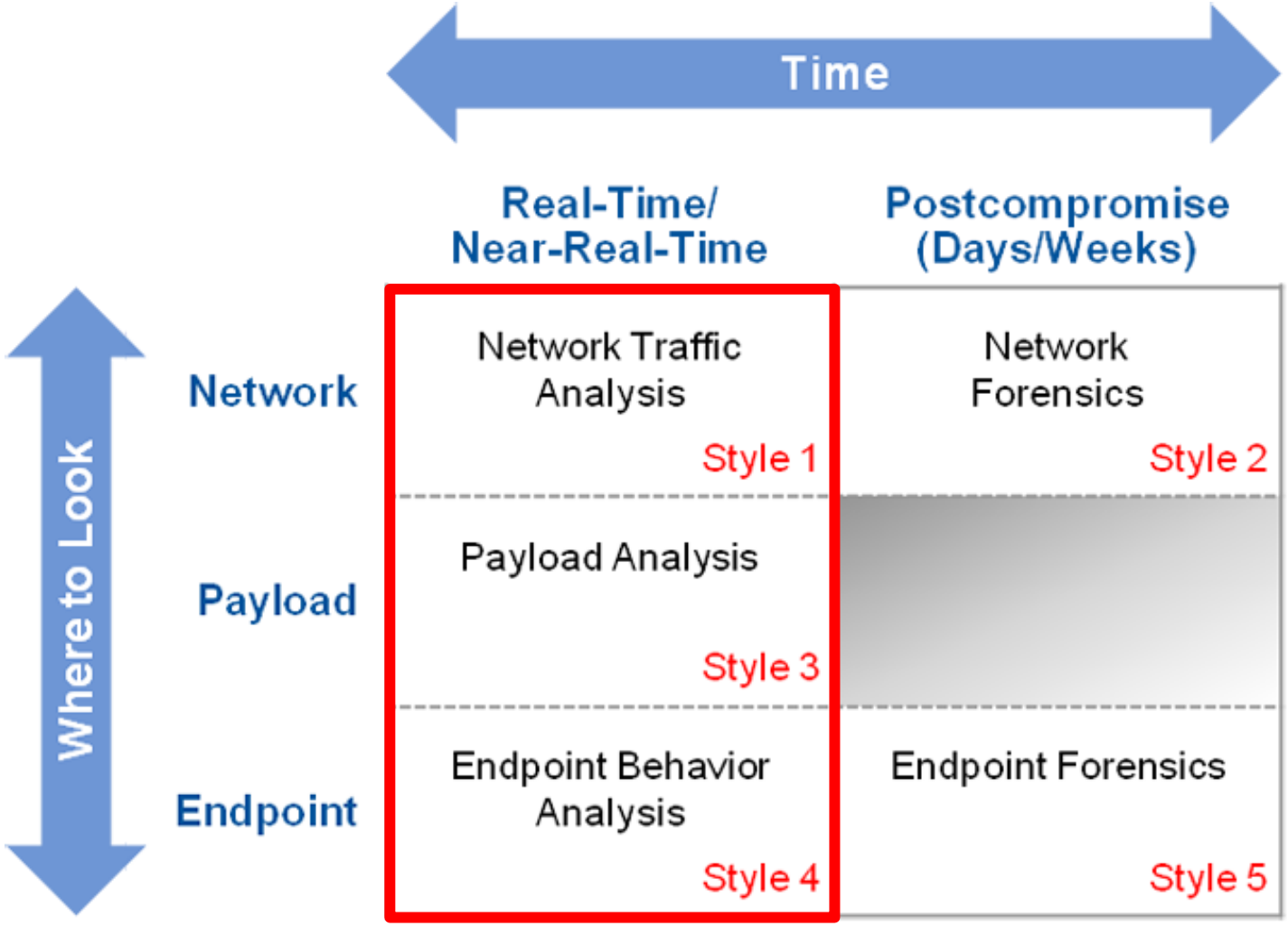
ИНФОСИСТЕМЫ ДЖЕТ



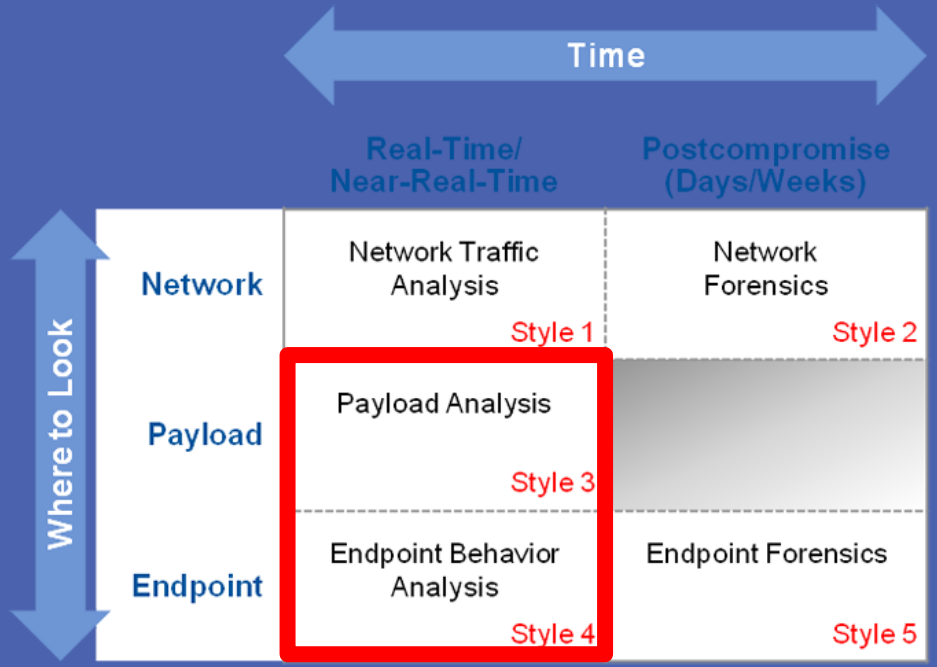
*Махатма Ганди*
*1869 – 1948 г.*

*«Будущее зависит от того, что мы делаем в настоящем»*

# Защита от APT по Gartner




**Gartner выделяет 5 стилей защиты**




ИНФОСИСТЕМЫ ДЖЕТ

# Style 3-4

# Песочницы или Style 3


## Песочница (Sandbox)

### ДИНАМИЧЕСКИЙ АНАЛИЗ

- Обнаружение изменений реестра
- Обнаружение сетевых коммуникаций
- Обнаружение активности процессов
- Обнаружение изменений файловой системы

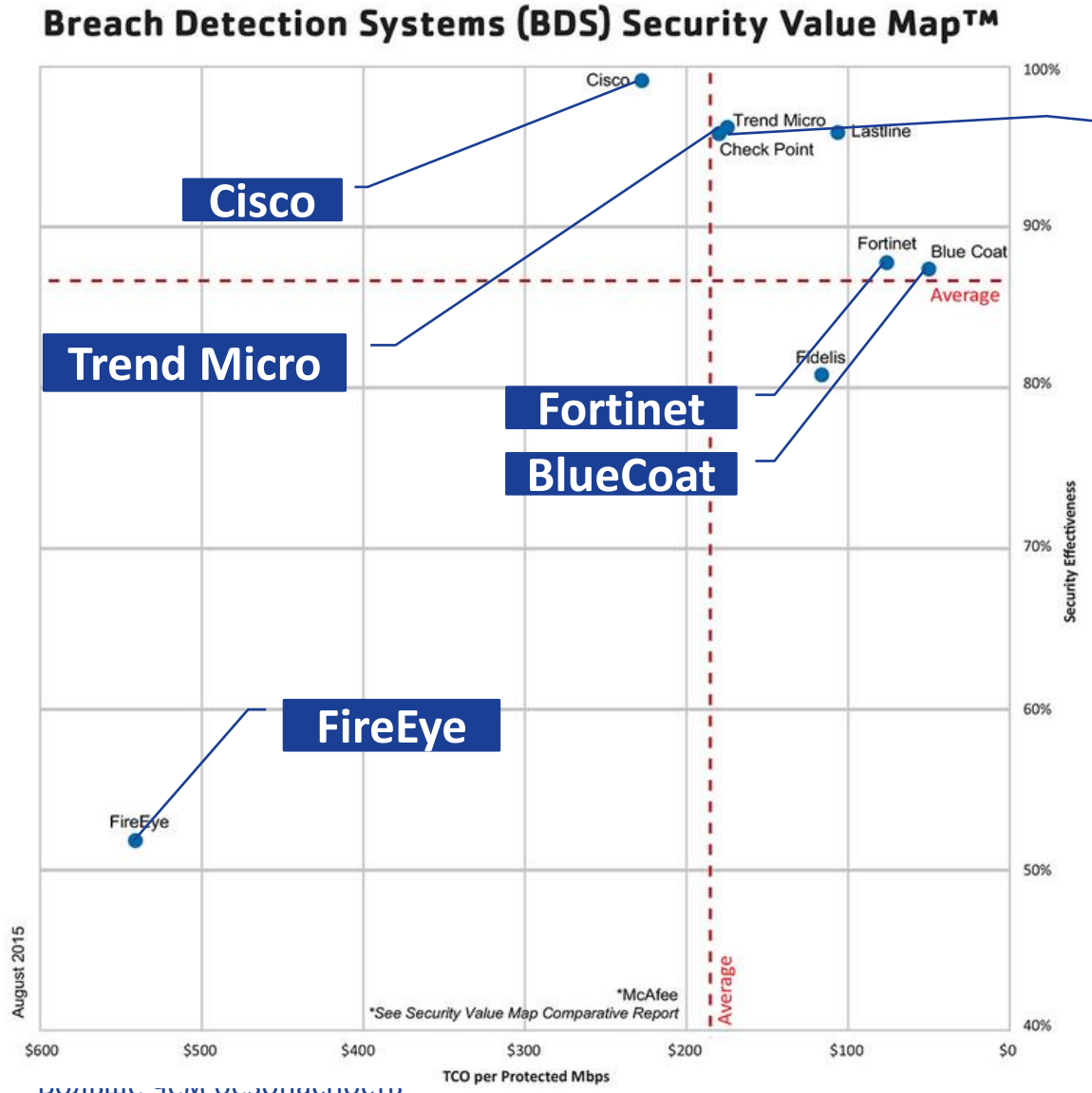
### СТАТИЧЕСКИЙ АНАЛИЗ

- Распаковка
- Анализ деассемблированного кода
- Анализ пассивного кода
- Обнаружение скрытых логических путей

**Классификация и решение, принятие мер**

**Имитация распаковки и запуска файлов на пользовательских компьютерах**

# SVM от NSS Labs (August 2015)




Check Point

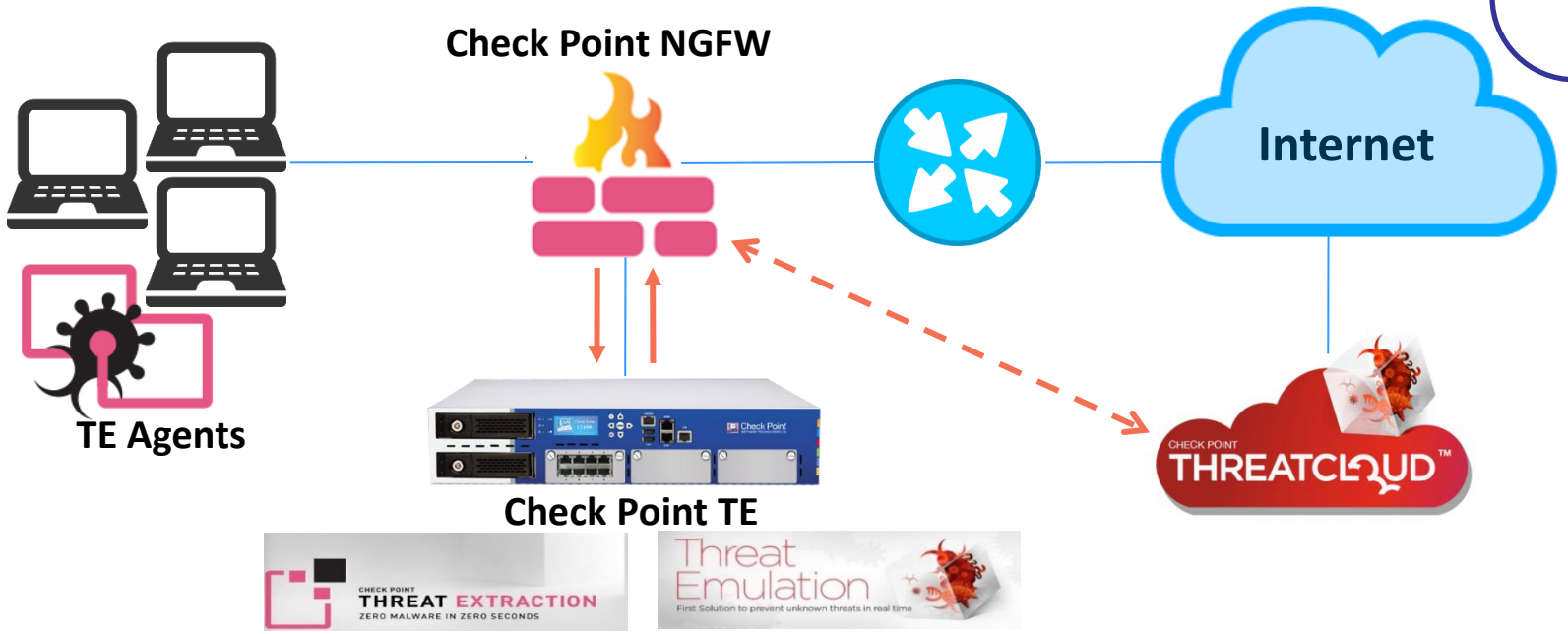
NSS LABS
WE MAKE SECURITY A SCIENCE

- Check Point
- Trend Micro
- FireEye
- Lastline
- Fortinet
- Blue Coat
- Cisco

# Check Point SandBlast

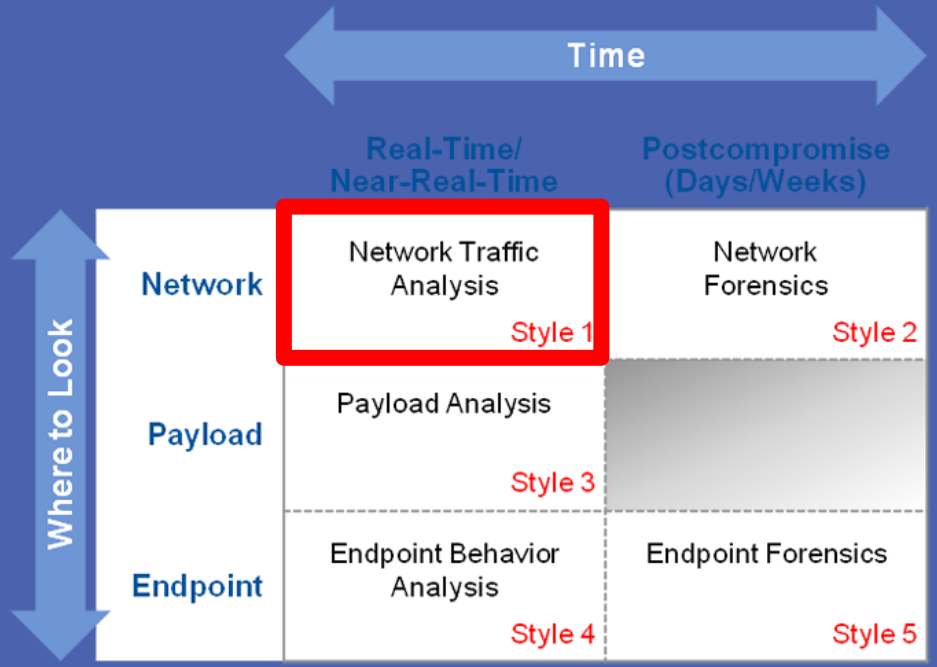
## 2 варианта реализации:

- локальное устройство SandBlast
- облачный сервис




## 2 технологии:

- **Threat Emulation** – эмуляция файлов
- **Threat Extraction** – удаление опасного содержимого в документах Office и PDF

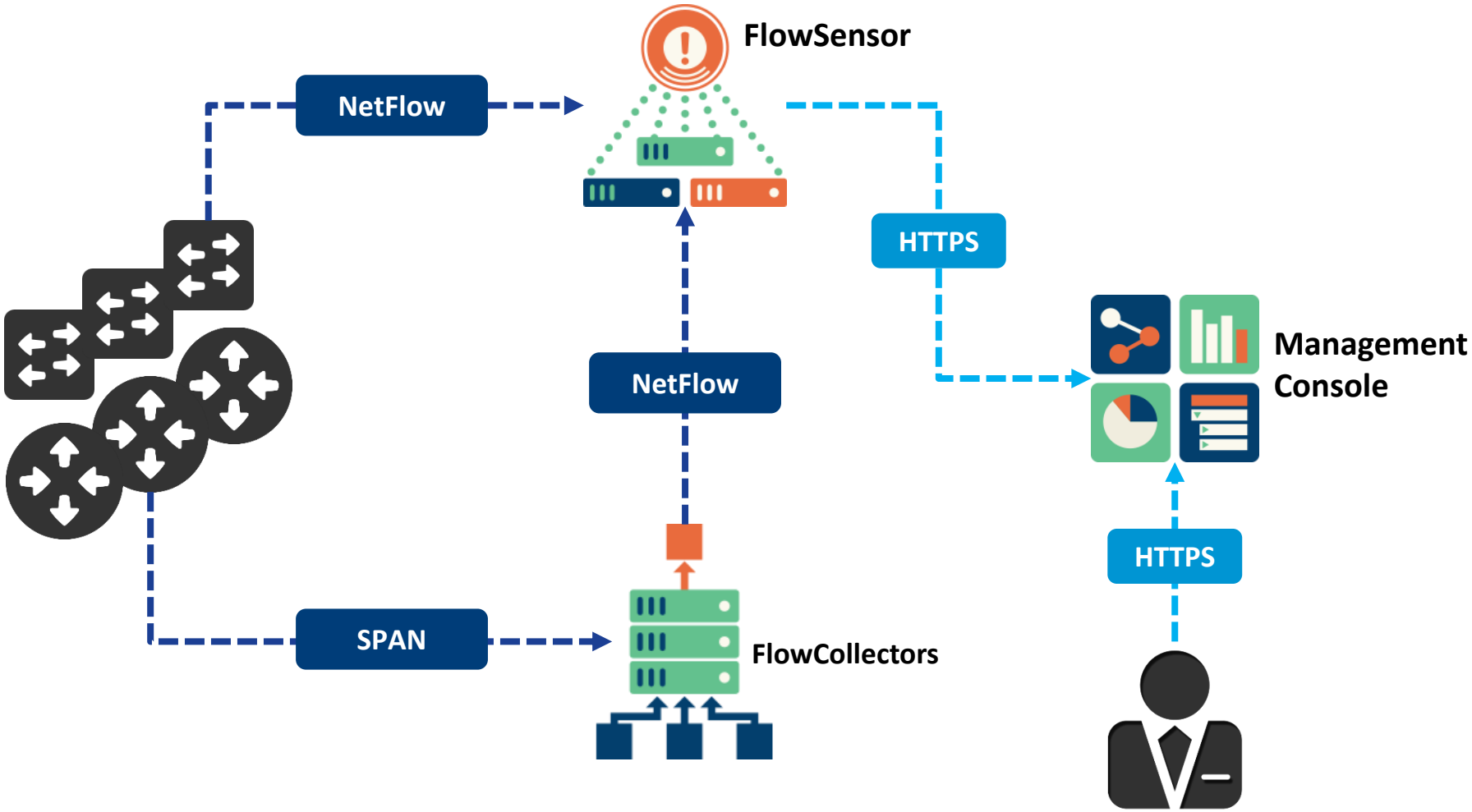



ИНФОСИСТЕМЫ ДЖЕТ

# Style 1

## Network Traffic Analysis

# Компоненты и дизайн NBA-решения



# Как работает NBA

# Но есть и другой подход

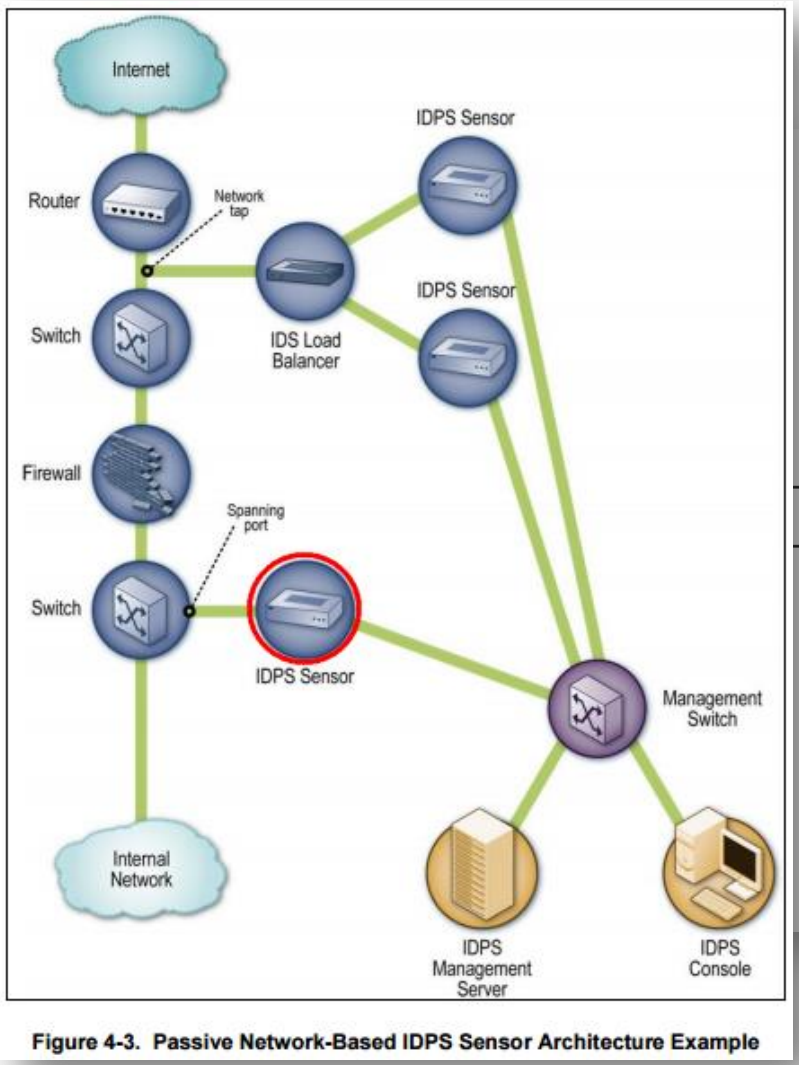



**Figure 4-3. Passive Network-Based IDPS Sensor Architecture Example**

**NIST Special Publication 800-94**

Guide to Intrusion Detection and Prevention Systems (IDPS)

*Recommendations of the National Institute of Standards and Technology*

**Karen Scarfone**
**Peter Mell**

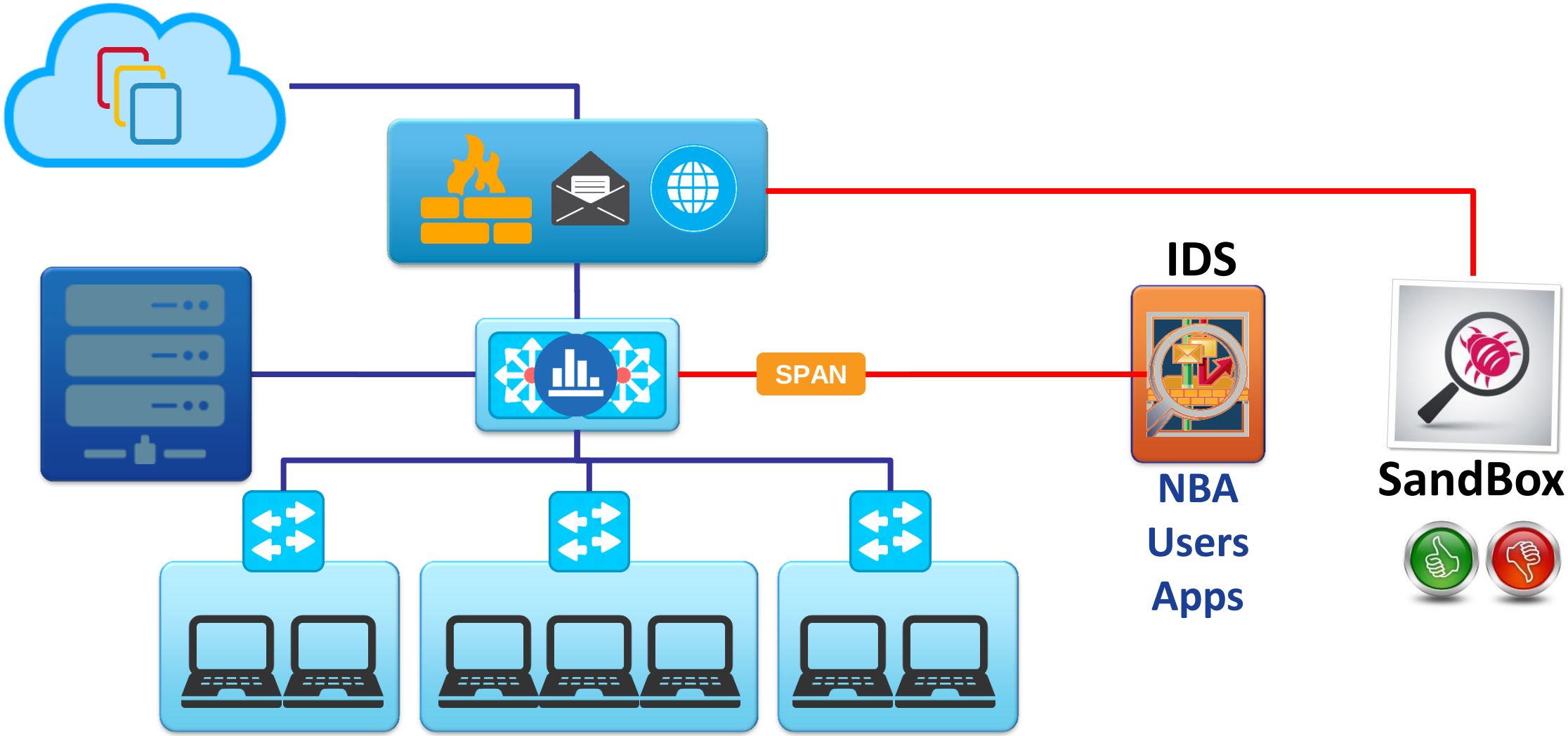
**COMPUTER SECURITY**

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2007

**В 9 из 10 случаев IDS во внутреннем сегменте отсутствует**

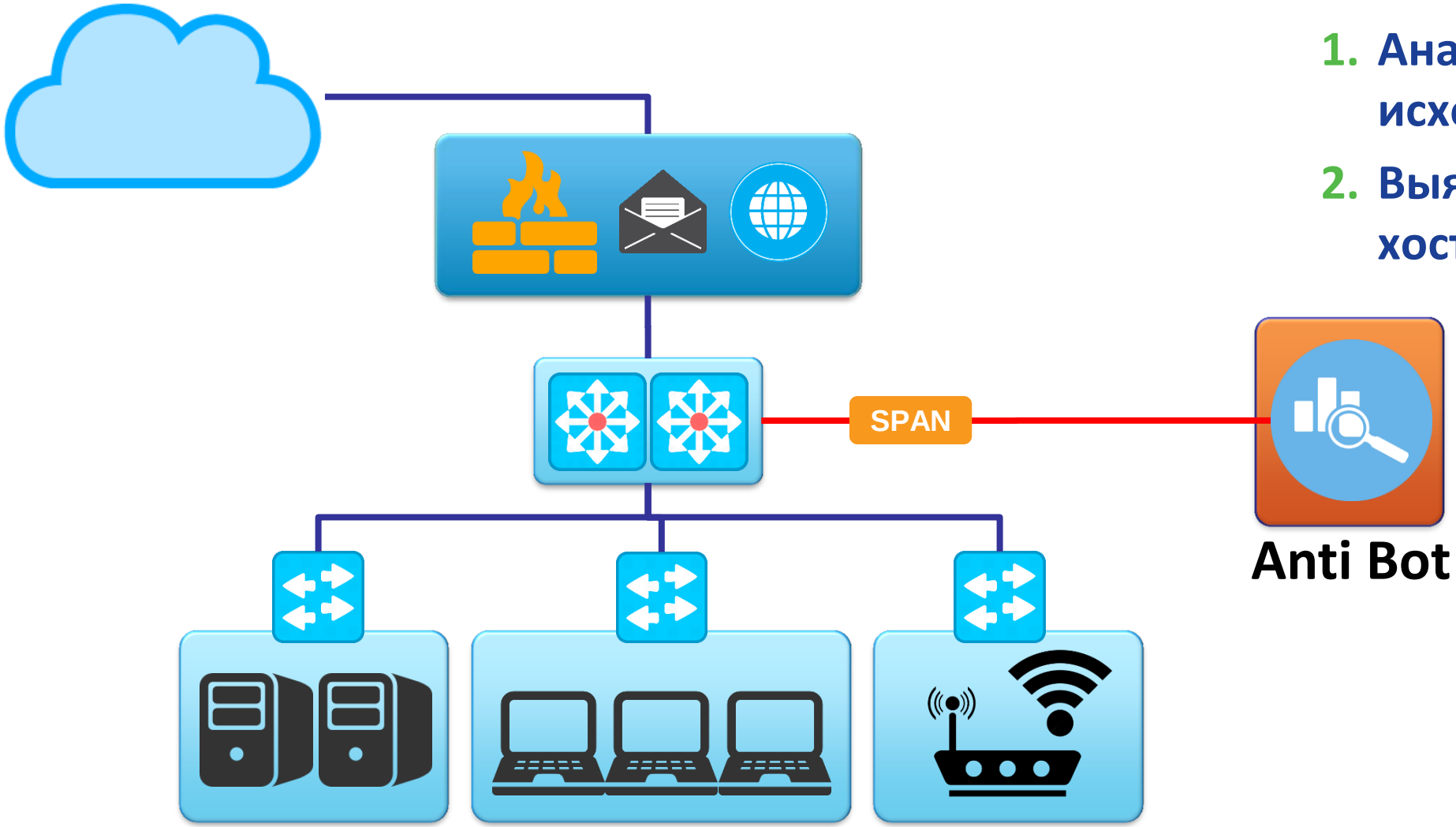
# NBA – это не только NetFlow



ИНФОСИСТЕМЫ ДЖЕТ

# Style 1`

# Выявление ботов



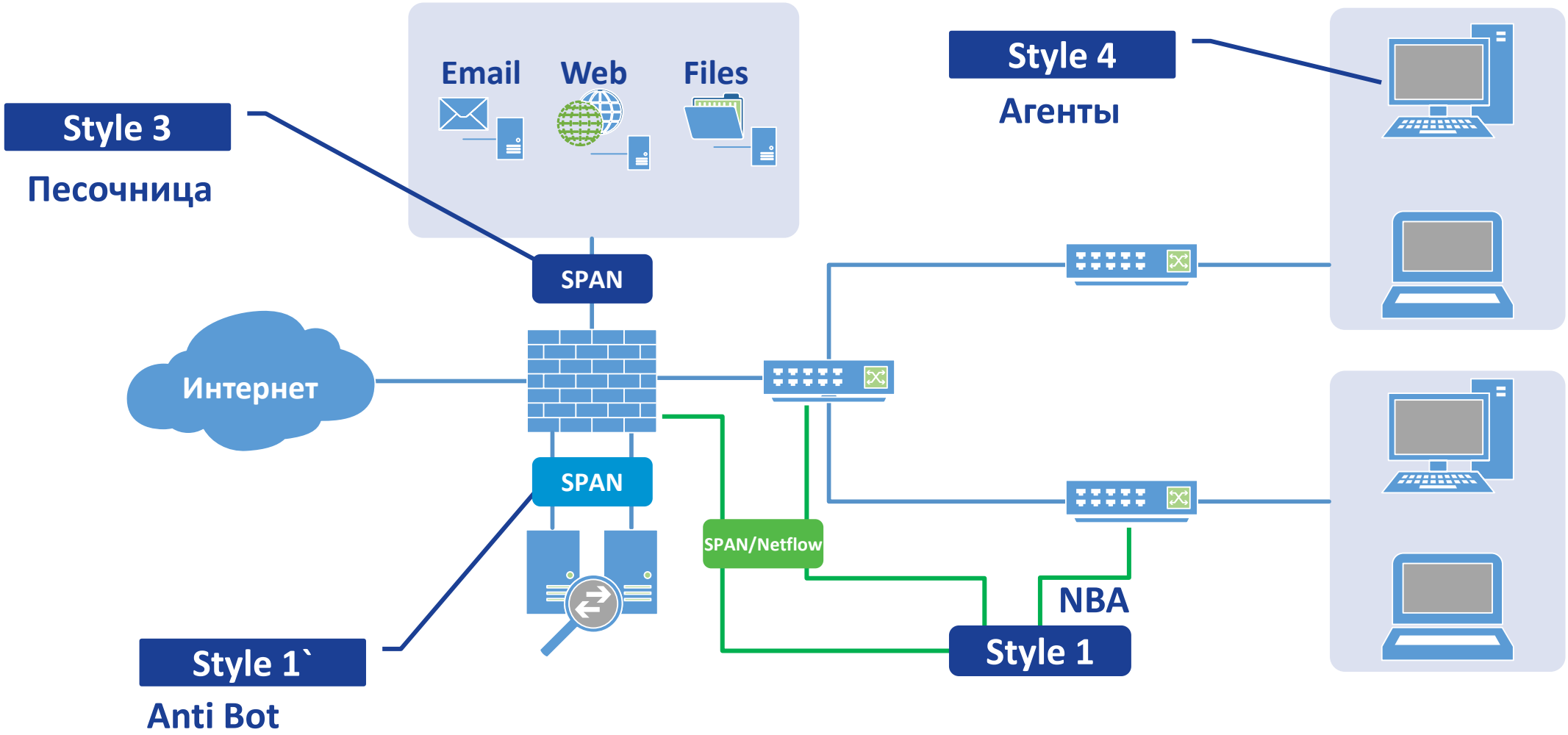

1. Анализ входящего и исходящего трафика
2. Выявление зараженных хостов-ботов

# А в чем идея решения?

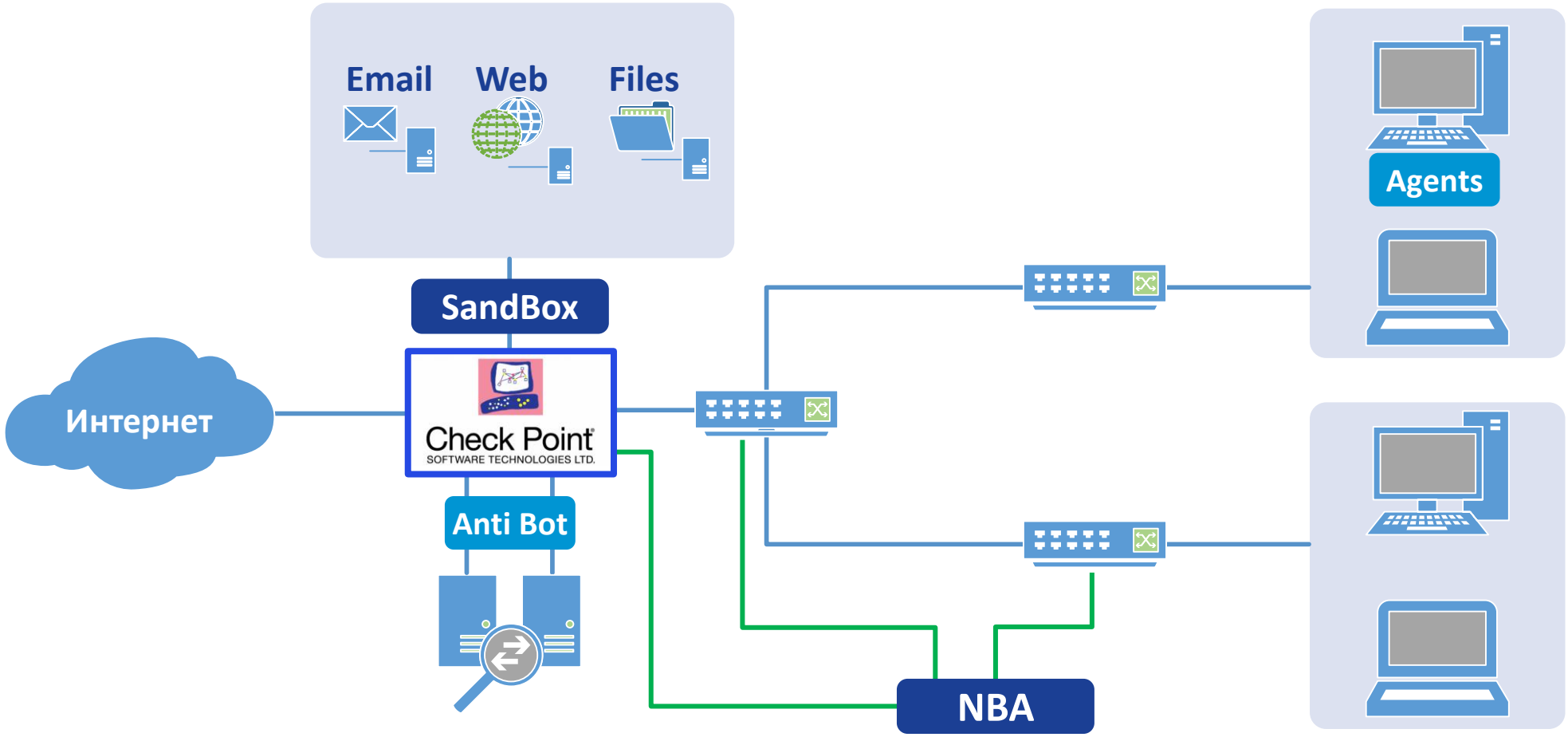
## Интеллектуальная защита от современных атак – это:

1. **Удобно, развлекательно и «прикольно»**
   - Новая полезная «игрушка» в руках службы ИБ
2. **Полезно и выгодно**
   - Возможность показать свою значимость перед руководством
3. **Эффективно и остро необходимо**
   - Альтернативы нет

# Пример сочетания стилей защиты



# Или…



ИНФОСИСТЕМЫ ДЖЕТ


# Let’s Just Try!