
radware
Обзор решений Radware
NETWELL

О компании Radware

Лидер в сегментах
Application Delivery и
Защита от DDoS

Награда
«Отличие в облачной безопасности», 2017

Оборот более **>$250M**
Более 1.000 сотрудников
Усиленная команда в РФ/СНГ

NETWELL

Лидер рынка защиты от атак

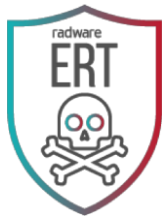
Финансы	Корпорации, Ритейл, Онлайн	Операторы связи
7/14 крупнейших бирж **12/22** коммерческих банков	**1/5** топ-брендов в каждой вертикали	**3/7** топ облачных провайдеров **6/10** операторов

NETWELL

Продуктовый портфель Radware

Аналитика и защита от современных атак

Фид активных атак ERT



Облачный сервис детектирования 0-day

Управление и мониторинг

Портал для MSSP

Система управления

Модуль отчетности

Control Plane

vDirect
Оркестрация и автоматизация

DefenseFlow
Защита от DDoS для SDN

Data Plane

DefensePro
Защита от DDoS

AppWall
WAF и WCO

Alteon ADC и SSL


radware
ADC, WCO, WAF.
Защищенная доставка приложений
NETWELL

Линейка Alteon

Виртуальные

Alteon D-VA

Alteon D-Cloud

Alteon NFV

От 1 Mbps до 200 Gbps

Физические

Alteon D-5208	Alteon D-6024	Alteon D-6420	Alteon D-8420	Alteon D-8820
24 vADCs	30 vADCs	80 vADCs	100 vADCs	>100vADCs

От 6 Gbps до 200 Gbps, логические vADC: от 1 до 100

Для любого ЦОДа от небольшого устройства до облака

NETWELL

Alteon D-Lineup

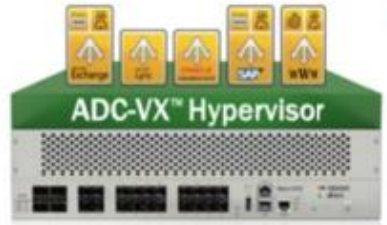
Alteon 4208

6 - 12 Gbps

Alteon 5208

6 - 26 Gbps

1 - 24 vADCs



Alteon 6420
Alteon 6024

30 - 80 Gbps

1 – 64 vADCs

Alteon 7220
Alteon 7612

160 - 200 Gbps

1 - 64 vADCs

Alteon 8420

100 - 160 Gbps

1 - 100 vADCs

Licensing model

- **Deliver**

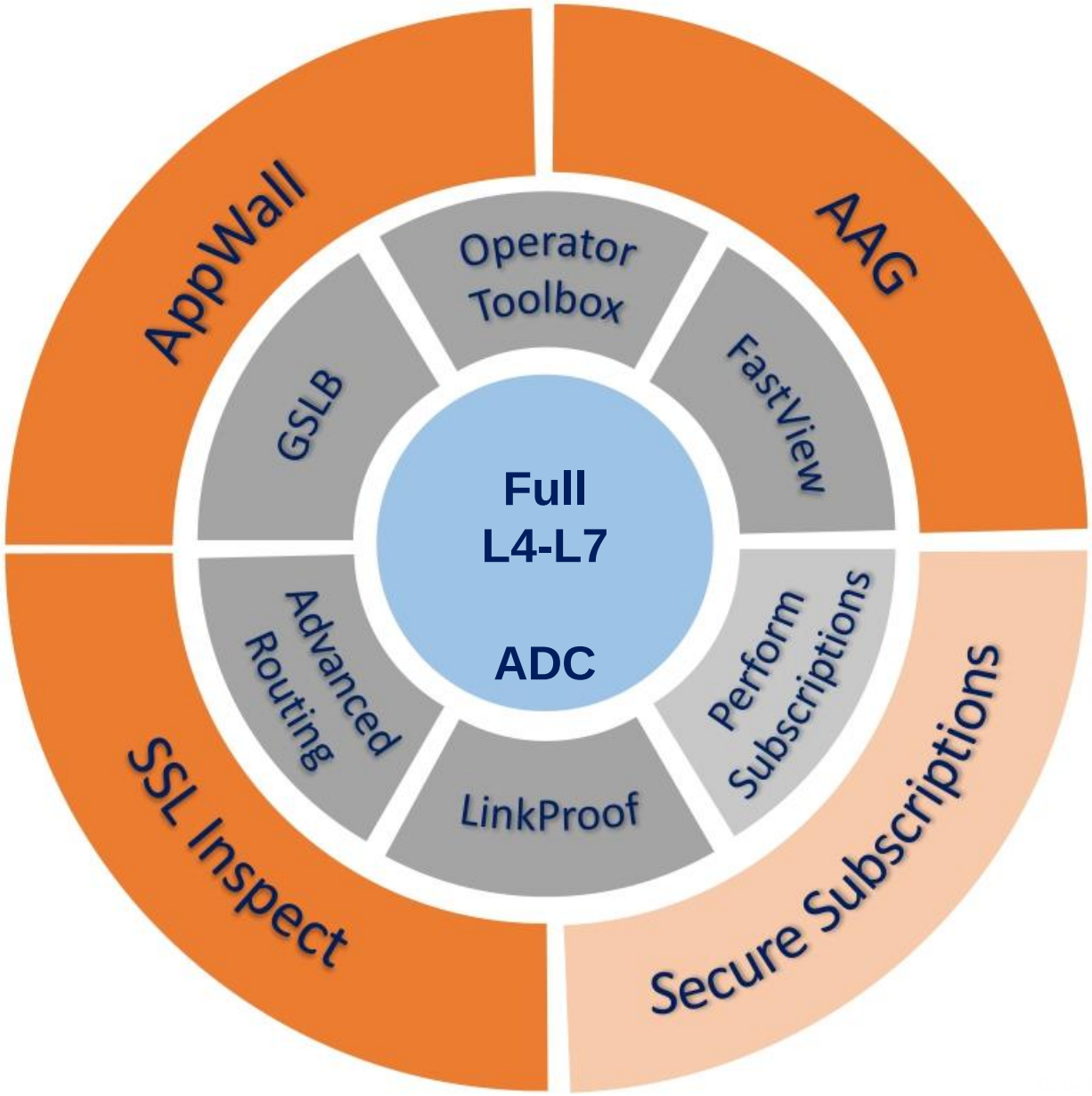
Fully featured L4-L7 ADC with market leading flexibility and performance

- **Perform**

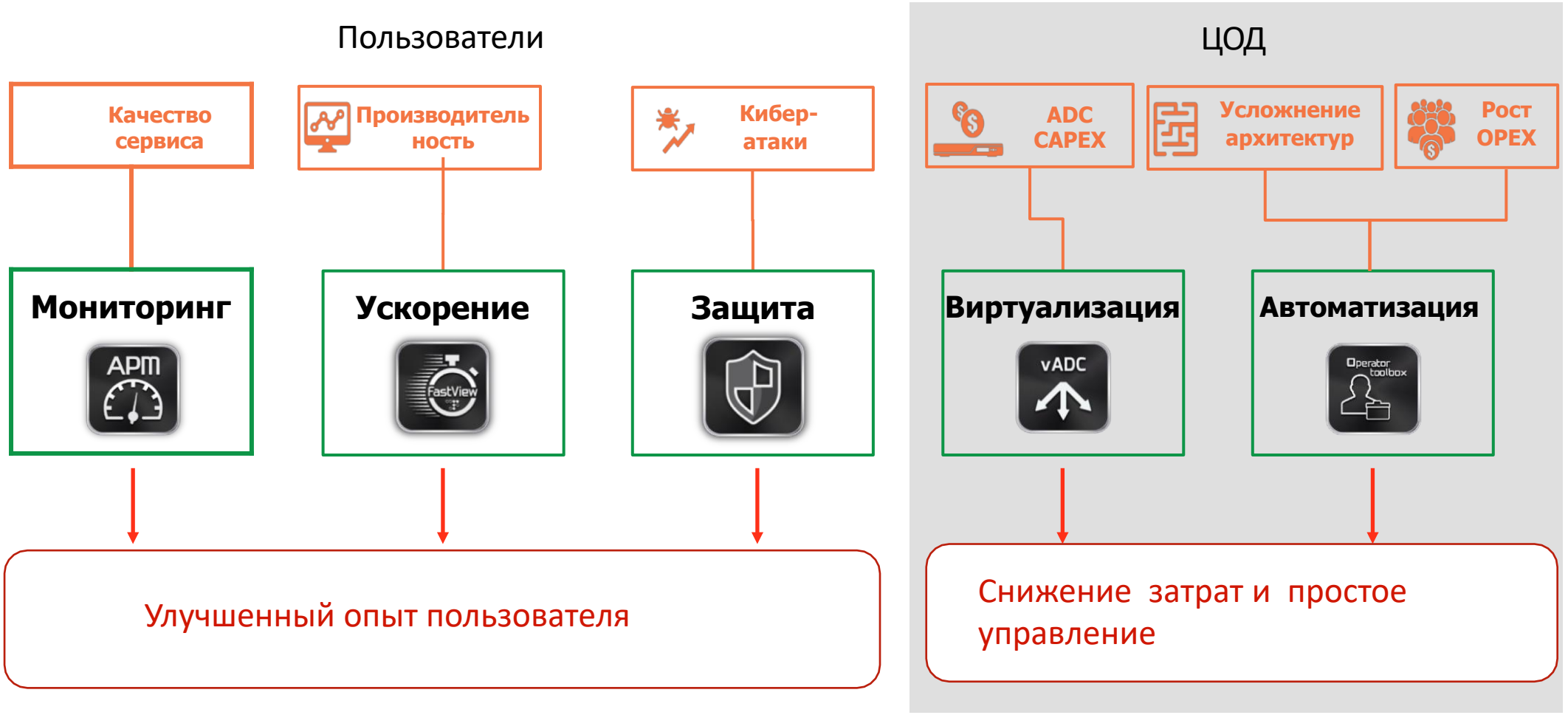
Performance boosting features for application delivery acceleration and SLA assurance as well as enhanced operational efficiency

- **Secure**

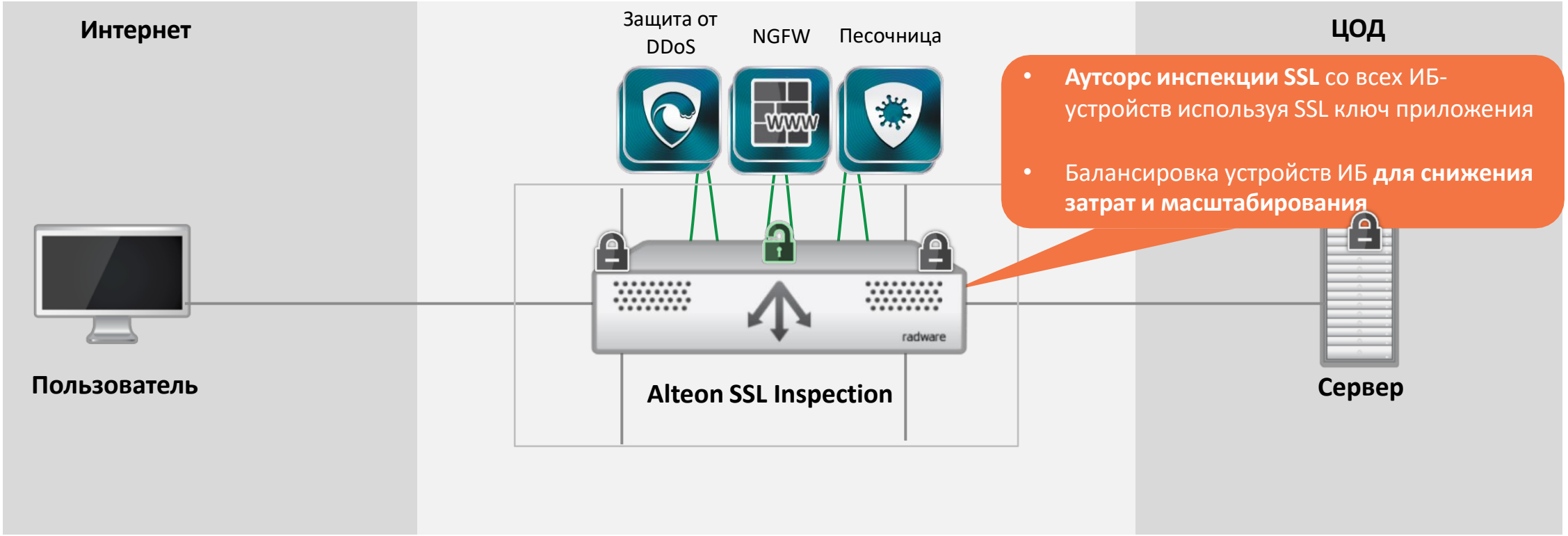
Comprehensive application protection and secure web access for ensuring safe inbound and outbound connectivity



Пять постулатов Alteon



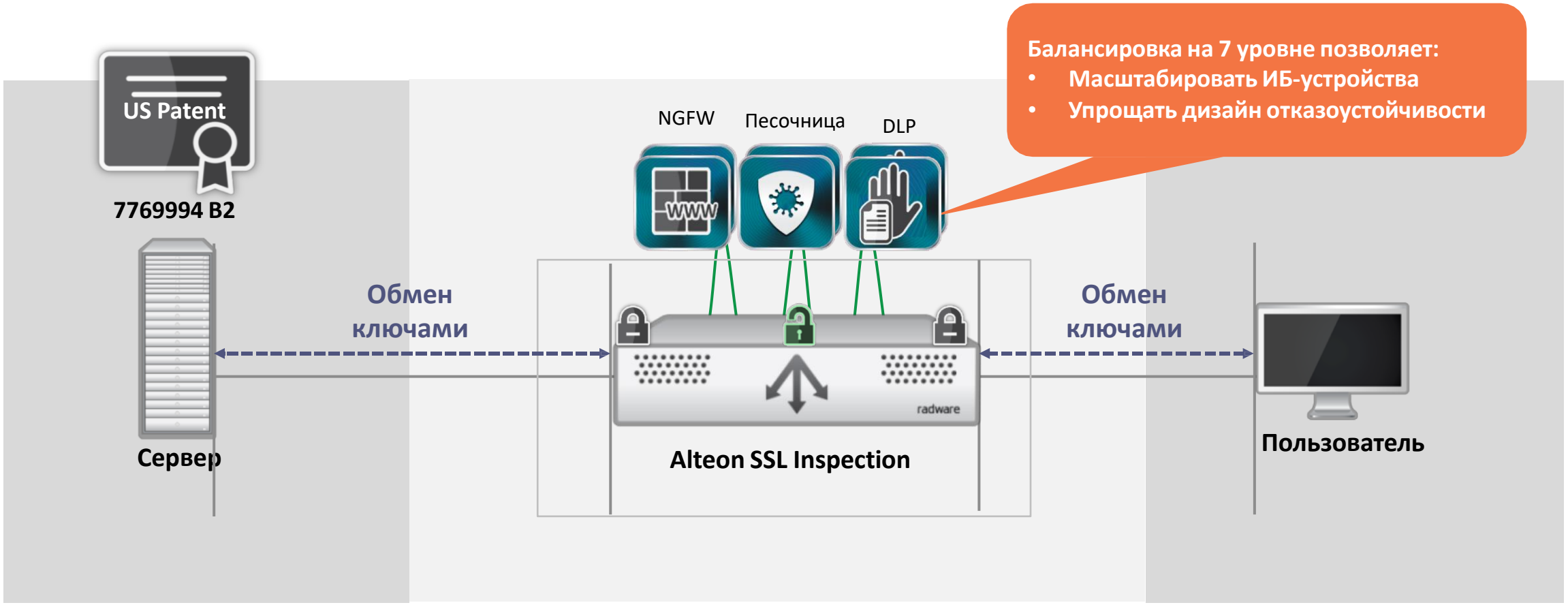
Сервис расшифровки входящего SSL



√ Защита зашифрованного трафика без снижения производительности
√ Оптимизация затрат на ИБ-решения

NETWELL

Сервис расшифровки исходящего SSL



√ Аутсорс обработки SSL

√ Упрощение внедрения
√ Снижение затрат

√ Снижение латенности

NETWELL

AppWall. Web Application Firewall (WAF)

- **Комплексная защита веб-приложений**
- **Адаптивные автоматические методы**
- **Гибкие режимы внедрения**
- **Уникальная защита от ботов**

Комплексная защита веб-приложений

Терминация TCP, разбор HTTP

- Evasions
- Сплиттинг HTTP-ответов (HRS)
- Инъекции, закодированные в URL / Base 64 / UTF-8
- Сигнатуры на нормализованном трафике

ICSA labs CERTIFIED WEB APPLICATION FIREWALL

Сигнатуры и правила

- Cross site scripting (XSS)
- SQL injection, LDAP injection, OS commanding

Web Application Security Consortium

Защита от утечек

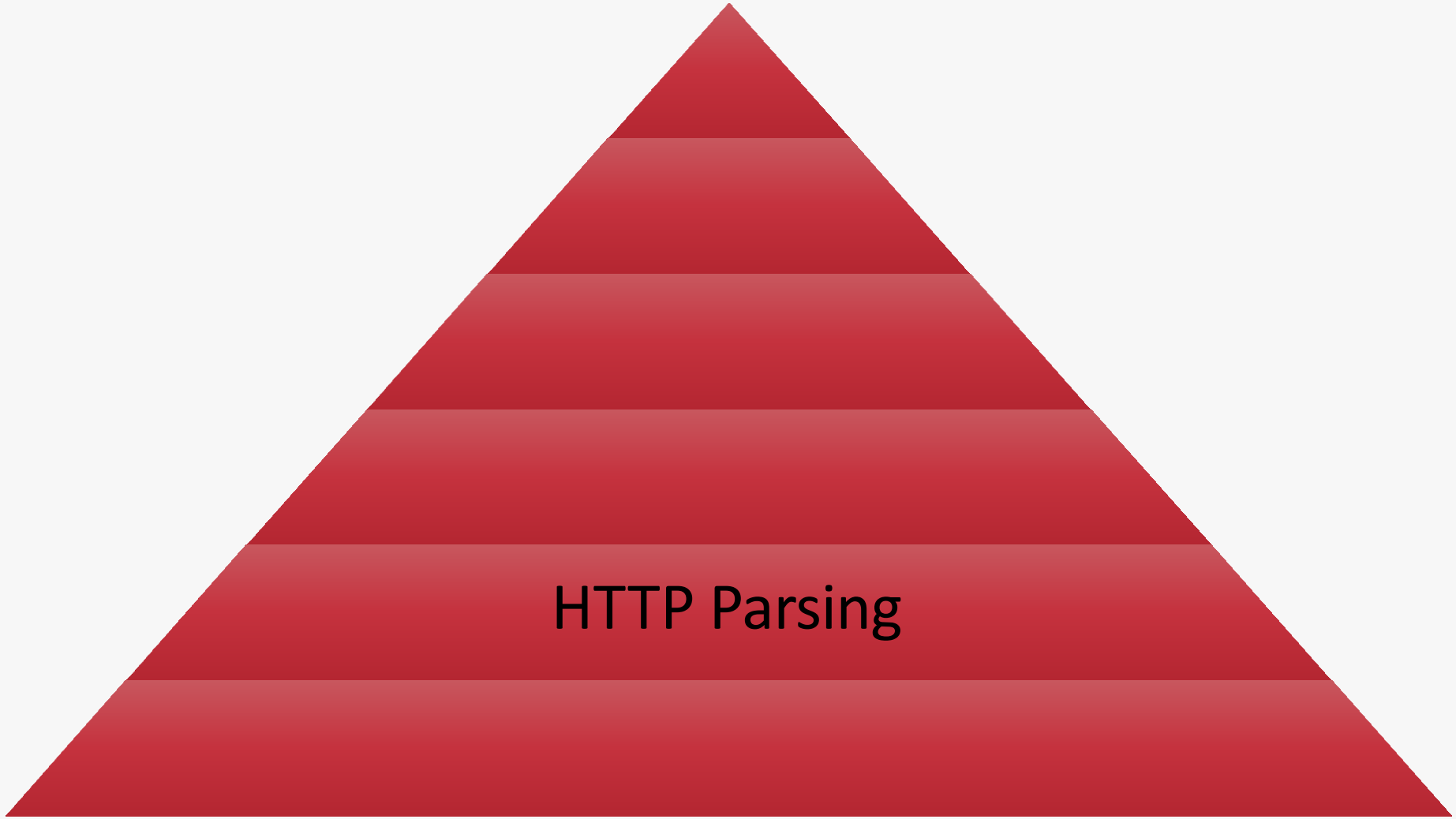
- Номер кредитных карт (CCN)
- Social Security (SSN)
- Регулярные выражения

OWASP The Open Web Application Security Project
OWASP Top 10 - 2013
The Ten Most Critical Web Application Security Risks

Логика

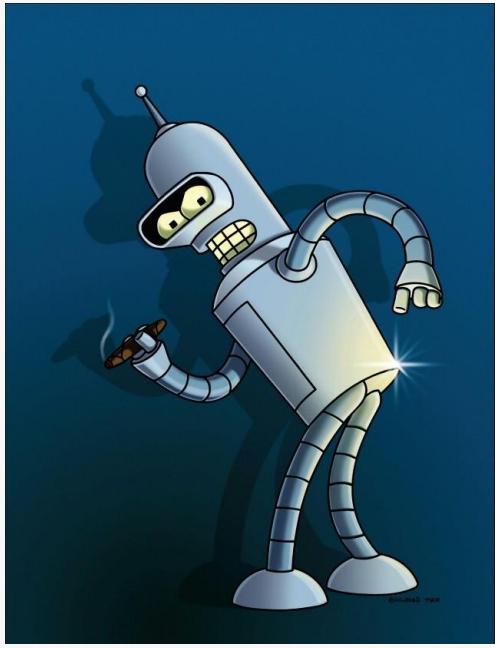
- Поведение пользователей
- Инспекция параметров и защита сессий
- Ролевая политика и контроль доступа на 7 уровне

Защита API

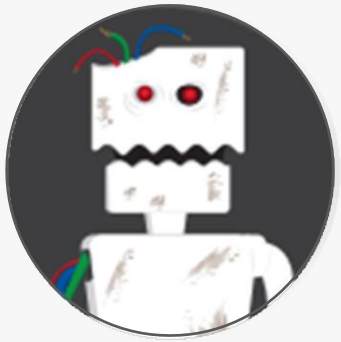


Примерно 30% веб-трафика создают

Плохие боты



Хакерские боты



Вирусные / вредоносные боты

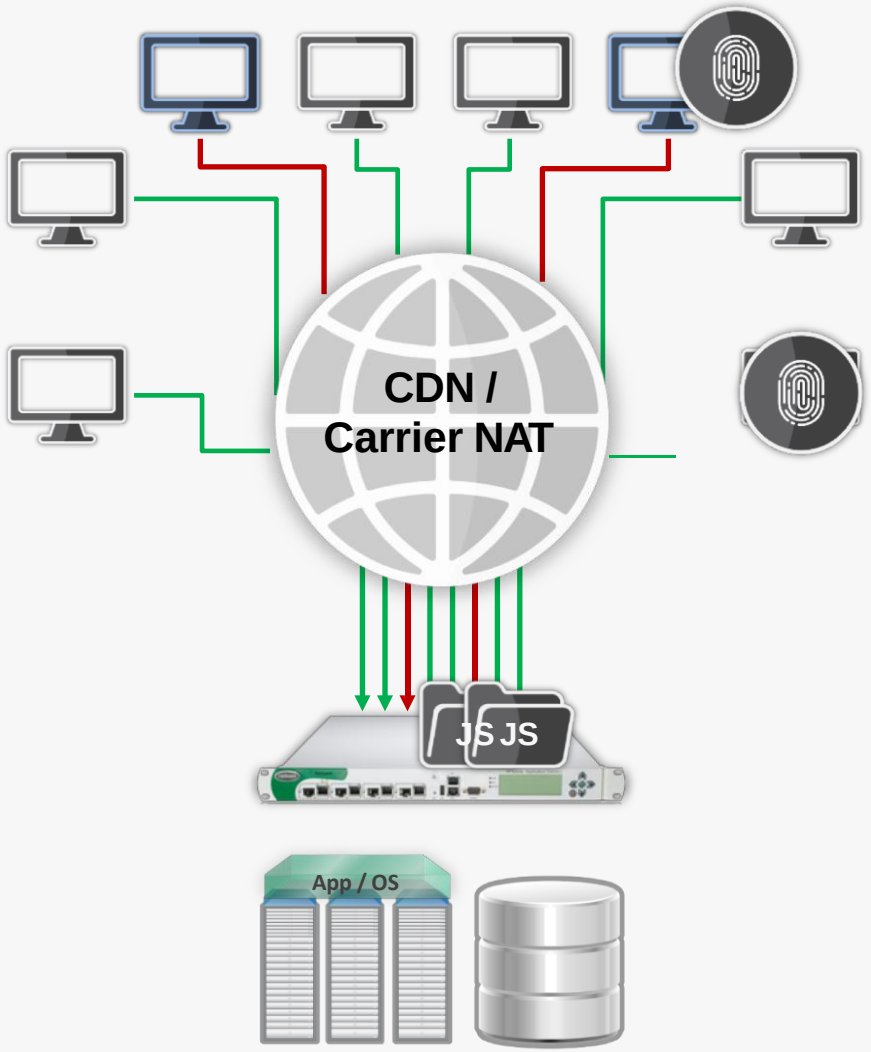
Загрузчики

Спамботы

NETWELL

Генерация отпечатка устройства – лучший способ защиты

- **Фингерпринтинг позволяет**
  - Отслеживать активность со временем
  - Оценивать репутацию устройства
- **И защищает от:**
  - Скрейпинга веб-сайтов
  - Брут-форс атак
  - Динамического HTTP-флада



NETWELL

Пример отпечатка устройства


radware
Anti-DDoS
Защита от атак на сети
NETWELL

Линейка DefensePro

Виртуальное устройство

DefensePro VA

Inspection Ports:
2x 10G vNIC
BW: 200M-20G
Mitigation BW: 20G
PPS: Up to 950K/vCPU

SSL in-the-box

Филиал / СМБ

DefensePro 6

Inspection Ports:
8x Copper, 2x1/10G
BW: 200M-2G
Mitigation BW: 6G
PPS: 3M
Size: 1U

SSL in-the-box

ЦОД / Корпоративный уровень

DefensePro 20

Inspection Ports:
24x1/10G
BW: 2G-12G
Mitigation BW: 20G
PPS: 25M
Size: 2U

SSL in-the-box

Крупные компании и платформы MSSP

DefensePro 60

Inspection Ports:
24x1/10G
BW: 10G-40G
Mitigation BW: 60G
PPS: 25M
Size: 2U

SSL in-the-box

Операторы связи и облаков

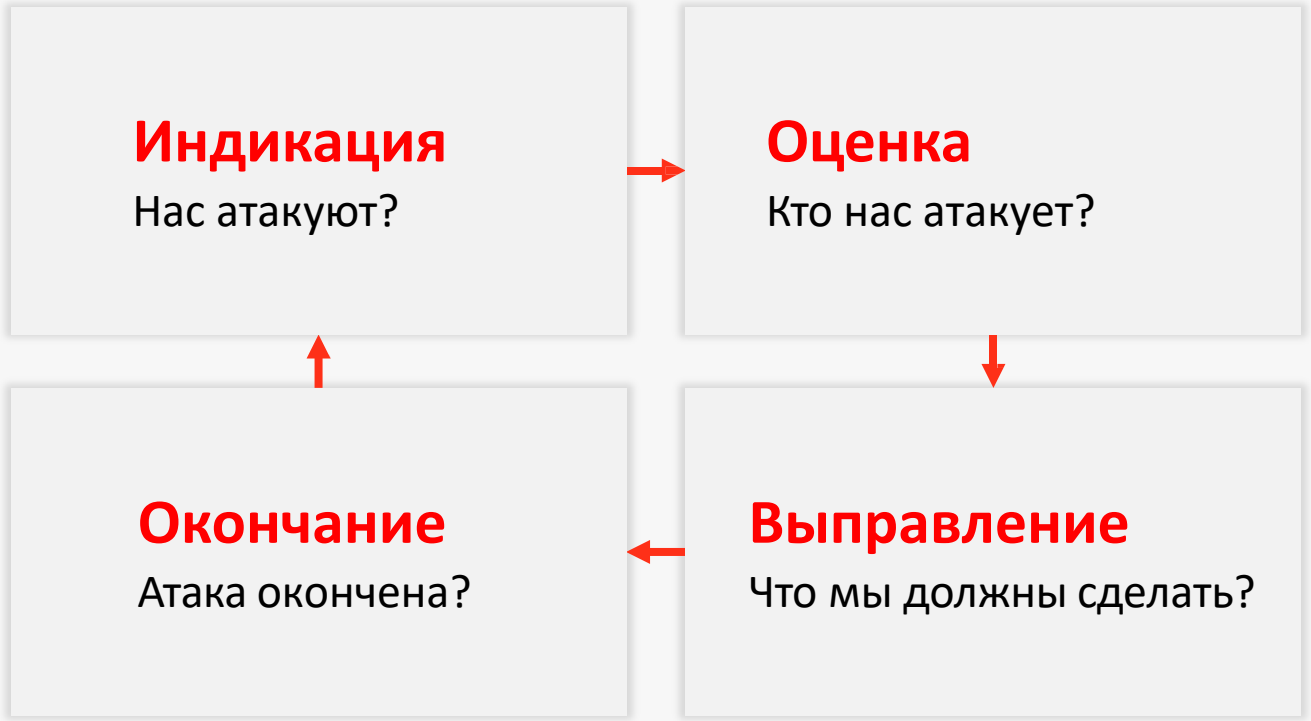
DefensePro 200

Inspection Ports:
20x10G, 4x40G, 4x100G
BW: 80G
Mitigation BW: 200G
PPS: 330M
Size: 2U

DefensePro 400

Inspection Ports:
20x10G, 4x40G, 4x100G
BW: 160G
Mitigation BW: 400G
PPS: 330M
Size: 2U

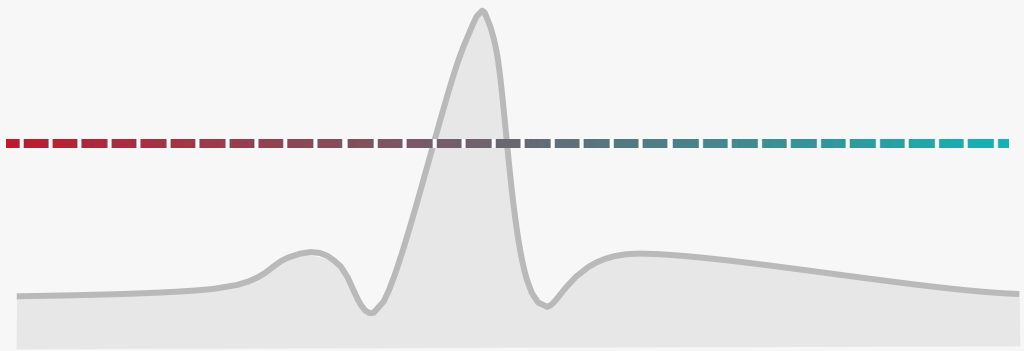
Поведенческий анализ и обучение DefensePro



Уникальная технология поведенческого обнаружения DDoS

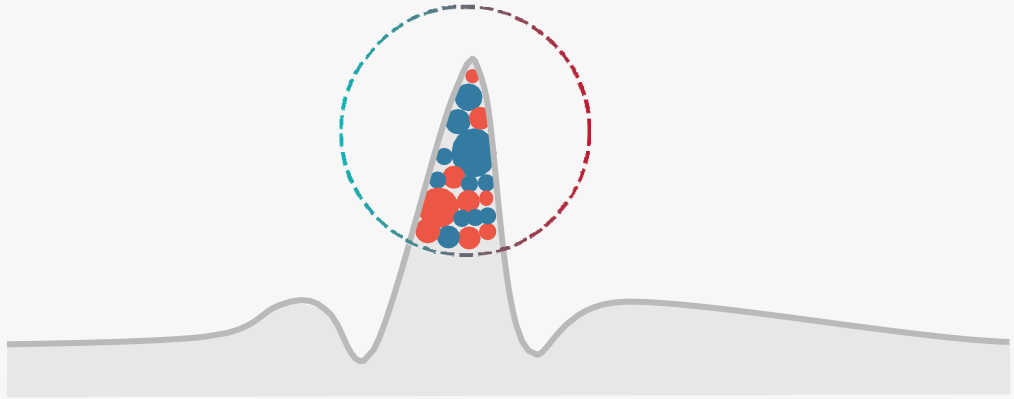
Не Radware

Детект то полосе



Radware

Детект по поведению



Повышенная защита с минимальными ложными срабатываниями

NETWELL

Генерация сигнатур в реальном времени

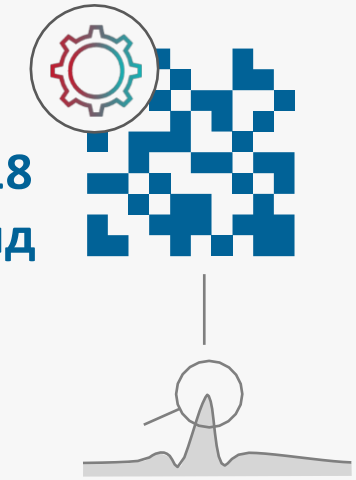
Не Radware

Сигнатуры вручную

30 мин – 4 часа

Radware

В реальном времени



До 18 секунд

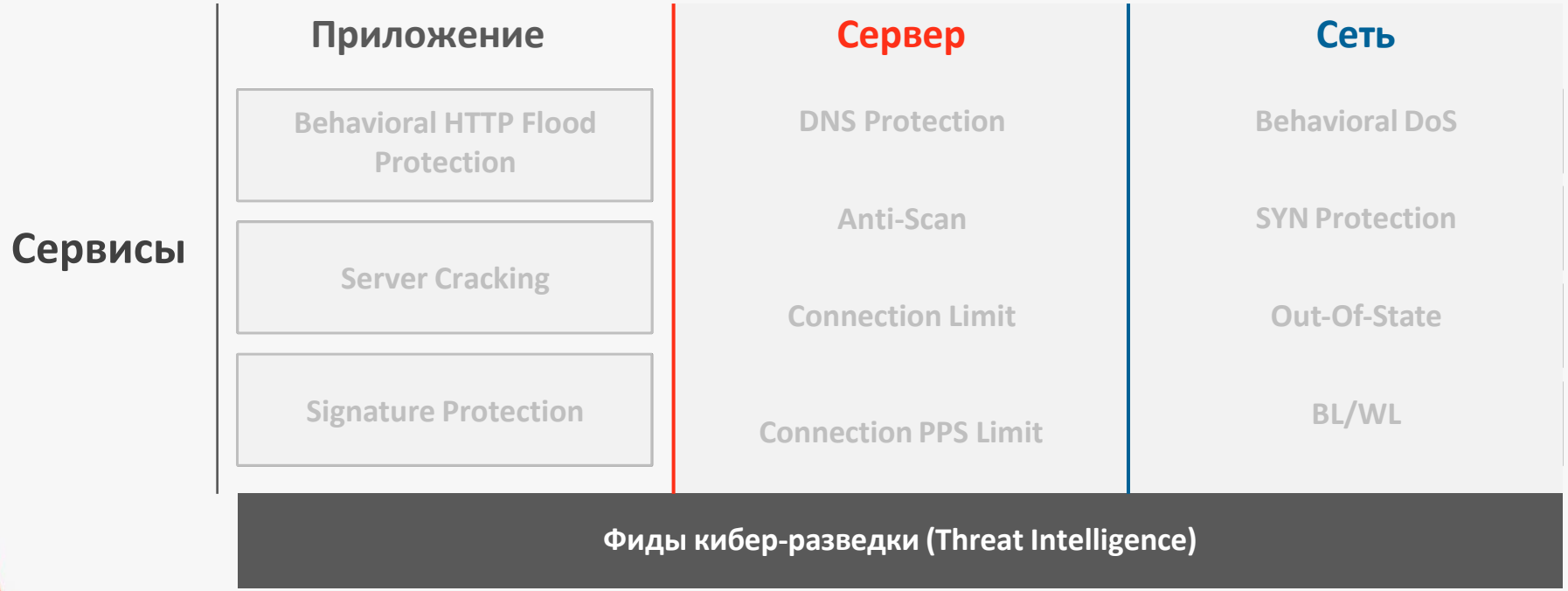
Автоматическое создание сигнатур в реальном времени

Защита от 0-day DDoS-атак за секунды

NETWELL

Слои защиты DefensePro

- Защита по поведению
- Запрос/Ответ
- Контроль доступа
- Известные уязвимости / инструменты / злоумышленники



NETWELL


radware
Seculert AMS и ERT Feed
Защита от современных 0-day атак
NETWELL

Облачный сервис
Radware Cloud Malware Protection Service

Детектирует
0-day вредоносы на основе машинного обучения

Проверяет
вашу защиту от актуальных сейчас атак

Блокирует
новые угрозы на основе интеграций

Сообщает
об активности вредоносов в вашей в виде алертов и менеджерских отчетов

NETWELL

Базовая технология

Современная технология машинного обучения, созданная ведущими аналитиками

70+ алгоритмов анализа поведения

Уникальная технология песочницы

Детекция аномалий коммуникации

Сообщество пользователей

Данные собираются с крупного пула корпоративных заказчиков Radware

> 2 млн. пользователей

Компании всех размеров

Разные отрасли

Массивные объемы данных

Технологии и масштабы внедрений Radware позволяет видеть новые атаки и вредоносы сразу при их появлении

Более 2 млрд. коннектов в день

100.000 вредоносных семплов в день

30 млн. профилей вредоносов в БД

www.radware.com

NETWELL

Алгоритм работы сервиса

NETWELL

Пример. Radware первым обнаружил Nymaim

Технология машинного обучения Radware обнаружила вредонос **Nymaim** на основе анализа исходящего HTTP/S трафика:

<table>
<tr><td rowspan="2">Алгоритмы коммуникативного поведения</td><td>1. Похож на вредонос:
Коммуникации похожи на вредоносные по многим векторам</td><td>3. Периодичность:
Паттерн коммуникации ~10 мин между запросами</td><td>5. Детект спуфинга хоста:
Ненормальные коммуникации как будто бы настоящих сайтов</td></tr>
<tr><td>Подозрительно:

bepqh.php?ootaj=5476067166608&snyrt=8431723538236482&afuwnfhd=lbbimn&wicckkl=hwrjwcz&imamiy=25809456648867803074&yqrpq=cskfmagusm&vxyo=deu</td><td>07/31/2016 23:13:20 GET
07/31/2016 23:03:07 GET
07/31/2016 22:53:07 GET
07/31/2016 22:43:06 GET</td><td>Сокрытие реального хоста:
nylon.com – не настоящая цель

POST/wcras.php?spadx=bajwheosn&oude=0566…
HTTP/1.1
Host: nylon.com
Cache-Control: no-cacheContent-Type: application/x-www-form-urlencoded</td></tr>
<tr><td rowspan="2">Алгоритмы поведения URL</td><td>2. Возраст домена:
Молодые домены</td><td>4. Насыщенность сайта:
Низкая насыщенность каждого домена (мало HTML-объектов)</td><td rowspan="2">ВЕРДИКТ – 0-DAY ВРЕДОНОС</td></tr>
<tr><td>http://hzkxoab.com < менее года
http://lkihbdov.com < менее года</td><td>http://hzkxoab.com – низкая
http://lkihbdov.com – низкая</td></tr>
</table>

NETWELL

Автоматический пен-тестинг

- Проверьте уязвимость к активным вредоносам, которые используются в атаках сейчас
- Проактивно тестируйте ваши средства защиты, не подвергая себя риску
- Запуск симуляции в браузере
- Немедленные результаты

NETWELL

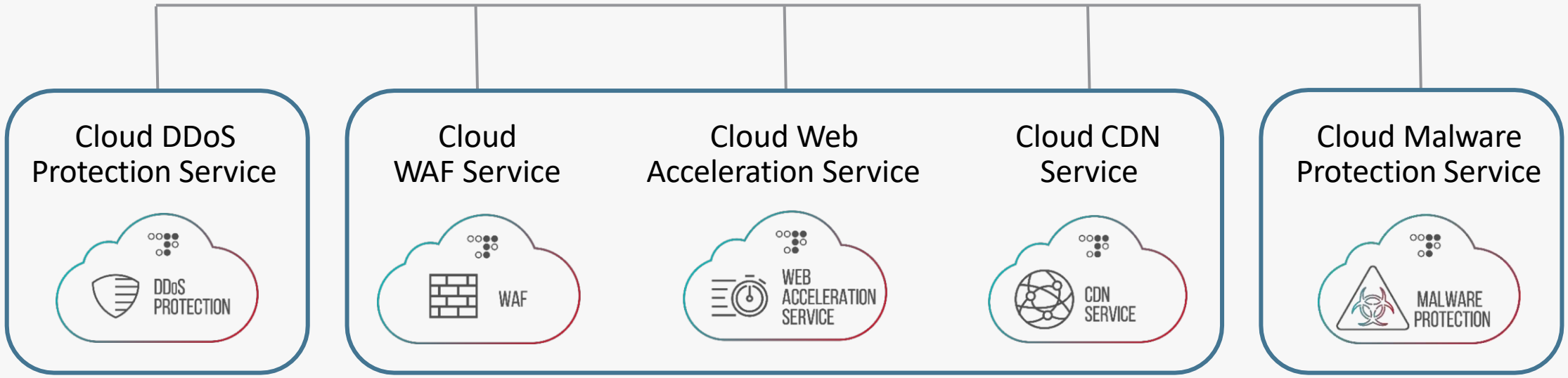

radware
Облачный портфель Radware
NETWELL

Облачные сервисы Radware

Управляемые **корпоративные облачные сервисы**

защищают от современных атак

и **оптимизируют** работу приложений



Защита инфраструктуры

Защита приложений

Защита от 0-day угроз

Спасибо за внимание!

- Контактная информация:

- Алексей Пироженко
- apirozhenko@netwell.ru
- +7.915.098.89.08 (telegram, WhatsApp)

- Геннадий Соколов
- gsokolov@netwell.ru
- +7.985.279.99.38 (telegram, WhatsApp)

radwar

NETWELL