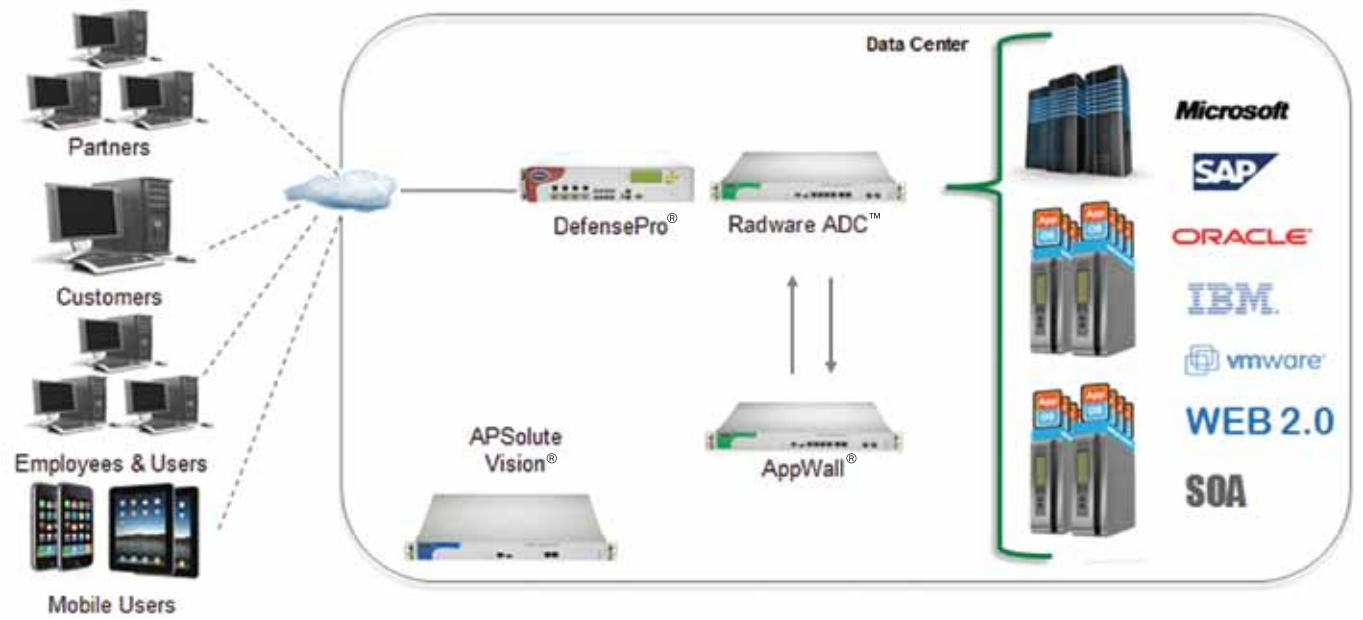
# RADWARE ATTACK MITIGATION SYSTEM:

## Комплексная защита и отказоустойчивое ускорение доставки приложений




Radware AMS — портфель решений для борьбы с современными многоцелевыми атаками, направленными на сетевое оборудование, серверы и приложения. Данный комплекс состоит из:

- **DefensePro®:** борьба с DDoS (поведенческий и сигнатурные алгоритмы очистки) с автоматическим распознаванием и блокированием атаки
- **Alteon®:** аппаратное ускорение SSL, оптимизация (кеширование, компрессия, мультиплексирование) и балансировка трафика для повышения отказоустойчивости сервисов и скорости их доставки потребителю
- **AppWall®:** фаервол уровня приложений (WAF) для гранулярной очистки Web-трафика от атак на прикладной уровень (SQL-injection, Cross Site Scripting, Slow Rate Attack и пр.)
- **APSolute Vision®:** система централизованного управления и анализа событий (SIEM)
- **Специализированная тех.поддержка быстрого реагирования –** ERT (Emergency Respond Team) для оперативной помощи по отражению атаки в реальном времени

Платформа Radware AMS консолидирует отдельные инстументы обнаружения атак и технологии противодействия на различных сетевых уровнях, обрабатывая зловредный трафик с помощью интеллектуальных методов. Это позволяет в режиме реального времени идентифицировать и блокировать действия ботов и хакеров, маскирующиейся под обычные транзакции приложений, и не ограничивать деятельность легитимных пользователей

# DefensePro®

## Защита от DDoS


Система **DefensePro®** объединяет в одном решении классический IPS и автоматическую защиту от DDoS атак, работающую без вмешательства оператора при отражении атаки. Отличительными особенностями являются высочайшая производительность (атака может достигать 25,000,000 пакетов в секунду, и автоматически отбивается в течение 18 секунд!) и отсутствие ущерба работе легитимных пользователей.

**DefensePro®** – это специализированная мультипроцессорная платформа со встроенными высокопроизводительными сетевыми процессорами со специализированными ASIC и FPGA для аппаратного ускорения обработки сетевого трафика.

**DefensePro®** со встроенным IPS содержит также высокопроизводительный контекстный процессор для аппаратного ускорения сигнатурного анализа сетевых пакетов.

Обработка сетевого трафика осуществляется поэтапно с использованием различных механизмов защиты. При этом суммарное время задержки сетевого пакета для всех линеек DefensePro не превышает 60 микросекунд.

**Встроенные механизмы защиты:**

- Behavioral DDoS Protection
- TCP SYN Flood Protection
- Connection Limit
- HTTP Mitigator
- Behavioral Server-Cracking Protection
- Bandwidth Management
- Signature Protection
- Stateful Inspection
- Anti-Scanning Protection
- Stateful Firewall (ACL)

**Доступные действия:** Drop packet, reset (source, destination, both), suspend (source, src port, destination, dest port or any combination), Challenge-Response for HTTP and DNS attacks

**Режим инсталляции:** In-line; SPAN Port Monitoring; Copy Port Monitoring; local out-of-path; Out-of-path mitigation

**Туннелирование протоколов:** VLAN Tagging, L2TP, MPLS, GRE, GTP

Одно из достоинств **DefensePro®** – это возможность лицензионного увеличения производительности по мере необходимости без замены оборудования, остановки услуги и без какой-либо переконфигурации устройства.

| Свойства | DefensePro® x06 | | | DefensePro® x16 | | | DefensePro® x412 | | | DefensePro® x420 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 506 | 1006 | 2006 | 1016 | 2016 | 3016 | 4412 | 8412 | 12412 | 10420 | 20420 | 30420 | 40420 |
| Пропускная способность, Гбит/сек | 0.5 | 1 | 2 | 1 | 2 | 3,6 | 4 | 8 | 12 | 10 | 20 | 30 | 36 |
| Число конкурентных сессий | 2 000 000 | | | 2 000 000 | | | 4 000 000 | | | 8 000 000 | | | |
| Отражаемая DDoS атака, пак/сек | 1 000 000 | | | 5 000 000 | | | 10 000 000 | | | 25 000 000 | | | |
| Инспектируемые порты | | | | | | | | | | | | | |
| 10/100/1000 | 4 | | | 12 | | | 8 | | | - | | | |
| GE (SFP) | 2 | | | 4 | | | 4 | | | - | | | |
| 10GE (XFP) | - | | | - | | | 4 | | | 20 | | | |
| 40GE (QSFP) | - | | | - | | | - | | | 4 | | | |

# AppWall®

## WAF, защита веб-сервисов

Radware **AppWall®** – это фаервол уровня приложений, защищающий веб-сервисы и обеспечивающий соответствие требованиям PCI DSS путем отражения веб-угроз и уязвимостей. Он предотвращает кражу данных и неавторизованные изменения важной корпоративной и пользовательской информации.

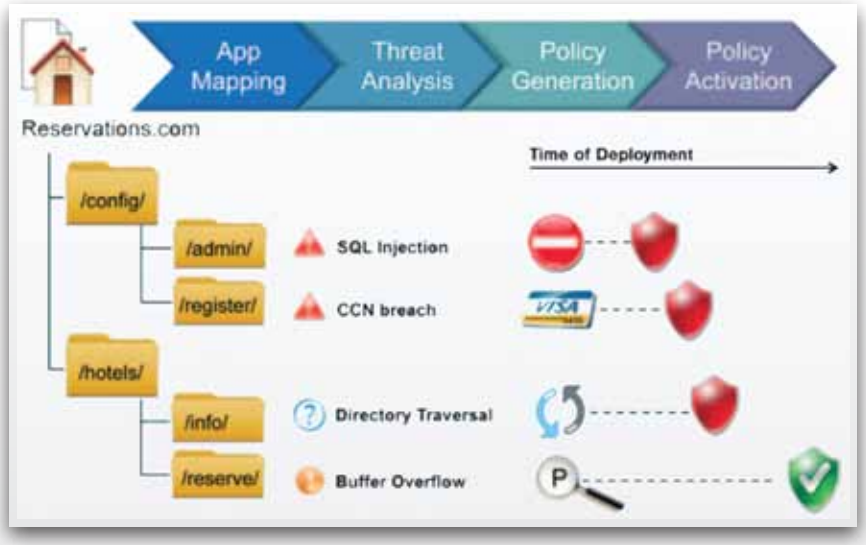
Наличие автоматического сканирования и генерации политики, а также возможность применения Позитивной (запрещено все, кроме явно разрешенного) и Негативной модели (разрешено все, что явно не запрещено) для разных частей одного приложения выгодно отличают Radware AppWall от конкурентов.

**Полная защита от ТОП-10 угроз веб-приложениям (по классификации OWASP):**

- A1-Injection
- A2-Cross Site Scripting (XSS)
- A3-Broken Authentication and Session Management
- A4-Insecure Direct Object References
- A5-Cross Site Request Forgery (CSRF)
- A6-Security Misconfiguration
- A7-Insecure Cryptographic Storage
- A8-Failure to Restrict URL Access
- A9-Insufficient Transport Layer Protection
- A10-Unvalidated Redirects and Forwards

**Защита от атак на веб-сервисы:**

- XSS
- SQL injection
- OS command injection
- LDAP injection
- SSI injections
- XPath injection
- Sensitive information leakage (e.g. CCN, SSN custom defined)
- Application DOS
- CSRF
- Parameter tampering
- From field manipulation
- Session hijacking
- Cookie poisoning
- Application buffer overflow
- Brute force
- Access to predictable resource locations
- Unauthorized navigation
- Web server reconnaissance
- Directory\path traversal
- Forceful browsing
- HotLink
- HTTP response splitting
- Evasion and illegal encoding
- XML validation
- Web services methodrestrictions and validation
- HTTP RFC violations
- HTTP request format and limitation violations (size, unknown method, etc.)
- Use of revoked hr expired client certificate
- File upload violations




**Адаптивная генерация политики –** AppWall® самостоятельно анализирует атрибуты защищаемых веб-сервисов и обнаруживает потенциальные угрозы, разделяя приложение на зоны безопасности. На основе этих данных автоматически предлагается соответствующая политика защиты для каждой из зон, минимизируя ложные срабатывания (False-positive) при одновременном обеспечении наиболее полной защиты.

# Alteon®

## ADC, ускорение доставки приложений

**Коммутаторы приложений Alteon® –** широко применяемое решение для оптимизации трафика приложений. Для таких приложений, как Oracle, MSExchange, SharePoint, WEBSphere нагрузка на сервера снижается в 2-3 раза, а потребность в пропускной способности - на 60-90%. Оборудование Alteon включает следующий богатый функционал:

- **Балансировка нагрузки** между серверами приложений с помощью мониторинга серверов и глубокого анализа трафика на 4-7 сетевом уровне позволяет снизить расходы за счет сокращения потребности в серверной мощности
- **Акселерация приложений** происходит за счет снятия со всех серверов нагрузки, напрямую не связанной с самим приложением (динамическое кэширование, TCP/HTTP мультиплексирование, HTTPS-шифрование, TCP оптимизация, сжатие трафика и т.д.), что позволяет высвободить до 70-80% мощности для работы с приложением
- **Глобальная балансировка (GSLB)** нагрузки между несколькими ЦОД, прозрачно для пользователей.

Оборудование Alteon реализует концепцию “on-demand” – пропускная способность и дополнительные функции расширяются на лицензионной основе по мере необходимости и без остановки сервиса.

| | Alteon® 4408 | Alteon® 4416 | Alteon® 5224 | Alteon® 5412 | Alteon® 10 000 Chassis |
|---|---|---|---|---|---|
| Пропускная способность, Гбит/сек | 0.5, 1, 2, 4 | 1, 2, 4 | 1, 2, 4, 8, 12, 16 | 8, 12, 16, 20 | 20, 40, 60, 80 |
| SSL CPS (соединений в секунду) | 500 – 2 000 | 500 – 2 000 | 500 – 2 000 | 500 – 4 000 | 25 000 – 100 000 |
| SSL CPS (connection per second) для XL - ревизии оборудования | 5 000 – 12 500 | 5 000 – 20 000 | 10 000 – 35 000 | 10 000 – 50 000 | 50 000 – 200 000 |
| Сжатие трафика, Гбит/сек | 0.1 – 2.3 | 0.1 – 2 | 0.1 – 3.2 | 0.1 – 6.2 | 3 - 20 |
| Поддержка виртуализации ADC-VX | 1 | 1 | 24 | 28 | 256 |
| Инспектируемые порты | 2 x 1GbE SFP<br>6 x 1GbE RJ45 | 4 x 1GbE SFP<br>12 x 1GbE RJ45 | 2 x 10 GbE SFP+<br>16 x 1 GbE SFP<br>8 x 1GbE RJ45 | 4 x 10GbE XFP<br>4 x 1GbE SFP<br>8 x 1GbE RJ45 | 15 x 10GbE/1GbE<br>8 x 1GbE RJ45 |

Поддерживается маршрутизация (OSPF, RIP, RIP II, BGP). Для модели Alteon® 5224 доступна опция заводской комплектации FIPS-сертифицированного HSM модуля Cavium.

Программный Alteon VA® поддерживает различные гипервизоры (VMware ESX/ESXi, KVM, Open XEN, Microsoft Hyper-V) и лицензируется по полосе: 1Мбит/сек, 0.2 – 0.5 и 1 Гбит/сек.

Виртуальные разделы (ADC-VX) используют механизм изоляции сбоев, не позволяющий никакому сбою в одном блоке vADC распространиться на соседние vADCs. Процессорное время гарантировано.