About Radware

Global Leader of Application Delivery and Application Security Solutions

ADC Solutions
• L4-L7 Server Load Balancing
• Application Acceleration
• SSL Offloading

Global Leader of Application Delivery and Application Security Solutions

Attack Mitigation System
• DDoS attacks Protection
• Intrusion Prevention
• Web Application Protection

WAF
IPS
Anti-DoS

and Application Security Solutions

Leverage SDN & NFV to create:
• More intelligent application delivery and security services
• Easier and abstracted operation of complex services
• Lower solution costs
• Higher scalability
• Simpler implementations

Enabling a smarter network.
Radware in the NFV Ecosystem

1. Virtualize
2. Disaggregate
3. Automate
4. Extend

- NFV Management and Orchestration
- Orchestration
- NFVish: Enable on-demand right-size protection
- SDNish: Global view of the network: Enable tailored mitigation strategy
- DefenseFlow Client
- Radware Virtual Anomaly Detector
- Radware Cyber Security Controller

- Or-Vnfm
- Vi-Vnfm
- Or-Vi
- EMS 1
- EMS 2
- EMS 3

Execution reference points:
Main NFV reference points
Other reference points

Virtual Computing
Virtual Storage
Virtual Network
Virtualisation Layer
Virtualisation Manager(s)
VNF Manager(s)
Orchestrator
VNF 1
VNF 2
VNF 3
Service, VNF and Infrastructure
Description
Or-Vi
Or-Vnfm
Vi-Vnfm
Os-Ma
Se-Ma
Ve-Vnfm
Nf-Vi
Vn-Nf
Vl-Ha
Introducing DefenseFlow

DefenseFlow leverages Radware’s patented *behavioral* technologies to provide attack mitigation as a native network service.

DefenseFlow collects and analyzes various security telemetries and based on this information provides various intelligent security actions.

DefenseFlow together with DefensePro provide a comprehensive and *network wide* security solution that copes with today’s and tomorrow’s security challenges.
Infrastructure Protection

DefenseFlow
Radware Security Control Plane

Service Provider Infrastructure

The Internet

DefensePro
Scrubbing Center

Tenant 1

Tenant 2
Infrastructure Protection: Provisioning

Protect critical infrastructure resources

DefenseFlow
Radware Security Control Plane

Service Provider Infrastructure

The Internet

DefensePro Scrubbing Center

PO

PO

Tenant 1

Tenant 2

DefenseFlow
Radware Security Control Plane

Start statistics collection

PO
Infrastructure Protection: Peace Time Learning

DefenseFlow
Radware Security Control Plane

Baseline of correct network behavior is created
Infrastructure Protection: Detection

- Select best mitigator and provision mitigation strategy
- Redirect suspicious traffic
- Attack detected

Service Provider Infrastructure

DefenseFlow
Radware Security Control Plane

Tenants:
1. Tenant 1
2. Tenant 2

DefensePro
Scrubbing Center

The Internet

PO

PO
Infrastructure Protection: Mitigation

Service Provider Infrastructure

DefenseFlow
Radware Security Control Plane

The Internet

DefensePro
Scrubbing Center

Tenant 1

Tenant 2

PO

PO
Managed Security Services Provider (MSSP):
- Offer to customers on-demand, low cost, zero-effort DDoS protection
MSSP: Self-served Tenant Protection Provisioning

DefenseFlow
Radware Security Control Plane

The Internet
Service Provider Infrastructure
DefensePro Scrubbing Center

Tenant 1
Request protection
Tenant 2
PO

DefenseFlow is a part of the Radware Security Control Plane, providing self-served tenant protection provisioning. The diagram illustrates the flow of protection requests and the integration with openstack.
DefenseFlow Client
- Behavioral detection: statistics and/or data based
- Lightweight: can run as a VM or container on several platforms (x86, Cisco’s ISR, …)
- Designed to integrate with CPE or in vCPE service chain (in tap mode)
MSSP: Attack Signaling

DDoS Open Threat Signalling (DOTS)

The Internet

Service Provider Infrastructure

DefensePro
Scrubbing Center

DefenseFlow
Radware Security Control Plane

Under Attack,
Help please

Attack Signaling
Attack on: IP#1,
Attack Type: SYN Flood
Attack Risk: High
Attack BW: x Mbps
Traffic baselines: y Mbps
TBD
MSSP: Mitigation

Select best mitigator and provision mitigation strategy

Redirect suspicious traffic

DefenseFlow
Radware Security Control Plane

The Internet

Service Provider Infrastructure

Tenant 1

Tenant 2

DefensePro
Scrubbing Center

PO
MSSP: Mitigation

Service Provider Infrastructure

DefenseFlow
Radware Security Control Plane

The Internet

DefensePro
Scrubbing Center

Tenant 1

PO

Tenant 2
MSSP: Perimeter-less Protection: Follow the PO

DefenseFlow
Radware Security Control Plane

PO moved!!

Cloud Provider

The Internet

Service Provider Infrastructure

DefensePro
Scrubbing Center

Tenant 1

Tenant 2

Cloud Provider

The Internet
**Summary**

**Network as a Sensor**
- Network infrastructure and router resources as “Attack Detectors”

**Best of breed detection and mitigation**
- Accurate behavioral detection with shortest time to detect – Less than 10 seconds!
- Broadest detection ability – From network to application layer attacks detection
- Less latency and non-intrusive compare other cloud services

**Monetization of protection resources**
- Offer Protection as a Service

**On-demand, right-sized protection**
- Network service rather than “on premises” security, Zero management at the customer premises
- Cost-efficient service: consumption based service

**Virtual perimeter protection**
- New distributed DDoS posture across multiple perimeters

**Follow (drive) standards**
- IETF DOTS
- ETSI NFV