Radware Attack Mitigation Architecture

For Carriers, Service Providers & Cloud Providers

One Architecture. Double the Protection. Half the Cost.

Csinos Tamás, CISSP

Country manager, Clico Hungary

October 19, 2023


ARISTA
ARMIS®
Cryptshare®
CLOUDIAN
CYBERARK
DIGI
ENTRUST
exabeam
Fidelis Cybersecurity
Forcepoint
FORESCOUT
GREYCORTEX
illumio
imperva
Infinera
IronNet
ivanti
JUNIPER driven by Mist AI
MICROSENS
netskope
nextsense
opengear A DIGI COMPANY
paloalto NETWORKS
radware
RAPID7
Recorded Future®
rubrik
COMMSCOPE® RUCKUS®
SailPoint
SCIRGE
SentinelOne™
THALES
tufin
VECTRA

Carrier Market Leading Solutions

5 of the World's Top 10 Telcos &
3 of the Top 7 Cloud Service Providers
use Radware's Attack Mitigation Solutions

Carrier & Service Provider Challenges

59% of enterprise customers said DDOS attacks are becoming harder to stop

Multi-vector attacks have increased 41% YoY

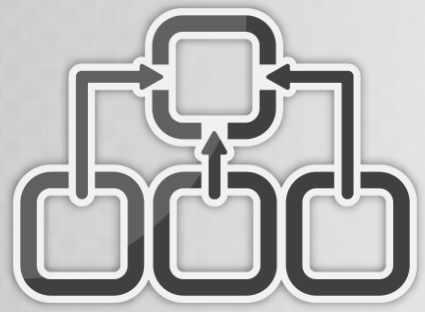
Shift from volumetric to application attacks

Large increase in encrypted attacks

High profile public attacks targeting carriers & service providers

The Pillars of Attack Mitigation

Attack Mitigation Pillars



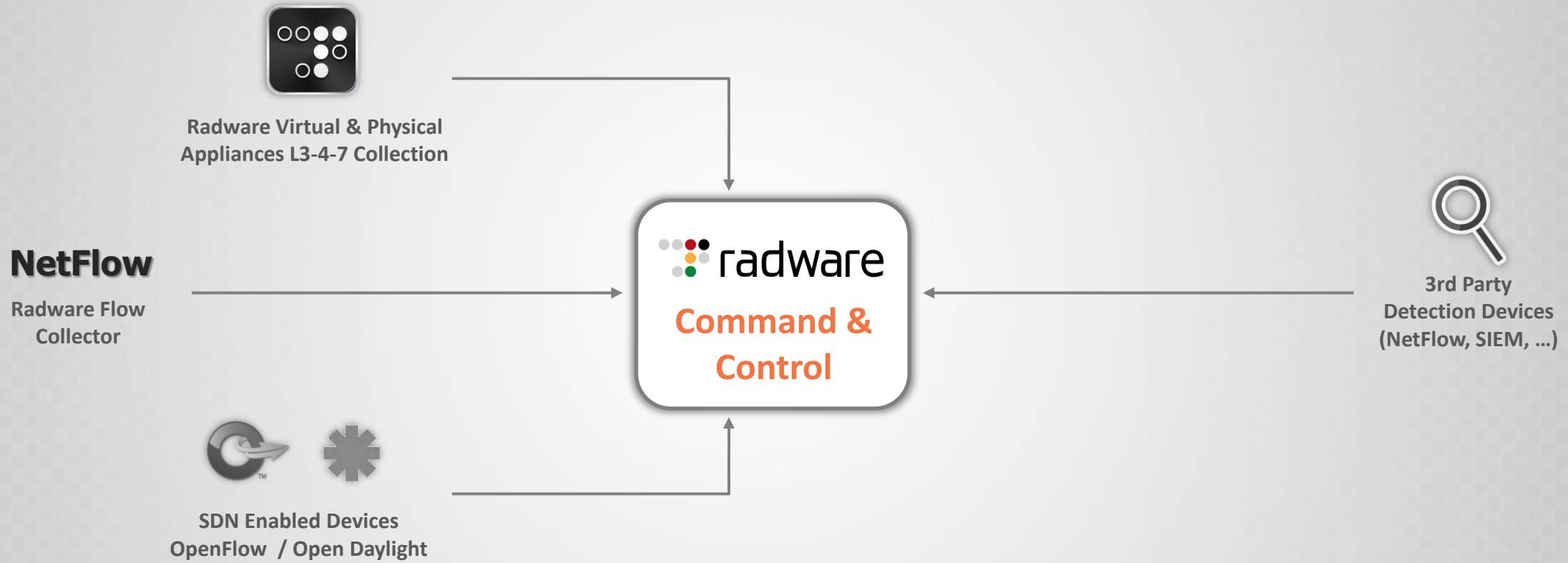
Collection

Detection

Mitigation

Operation

Robust Data Collection



Multi-source collection ensuring **100% attack coverage**

Attack Mitigation Pillars

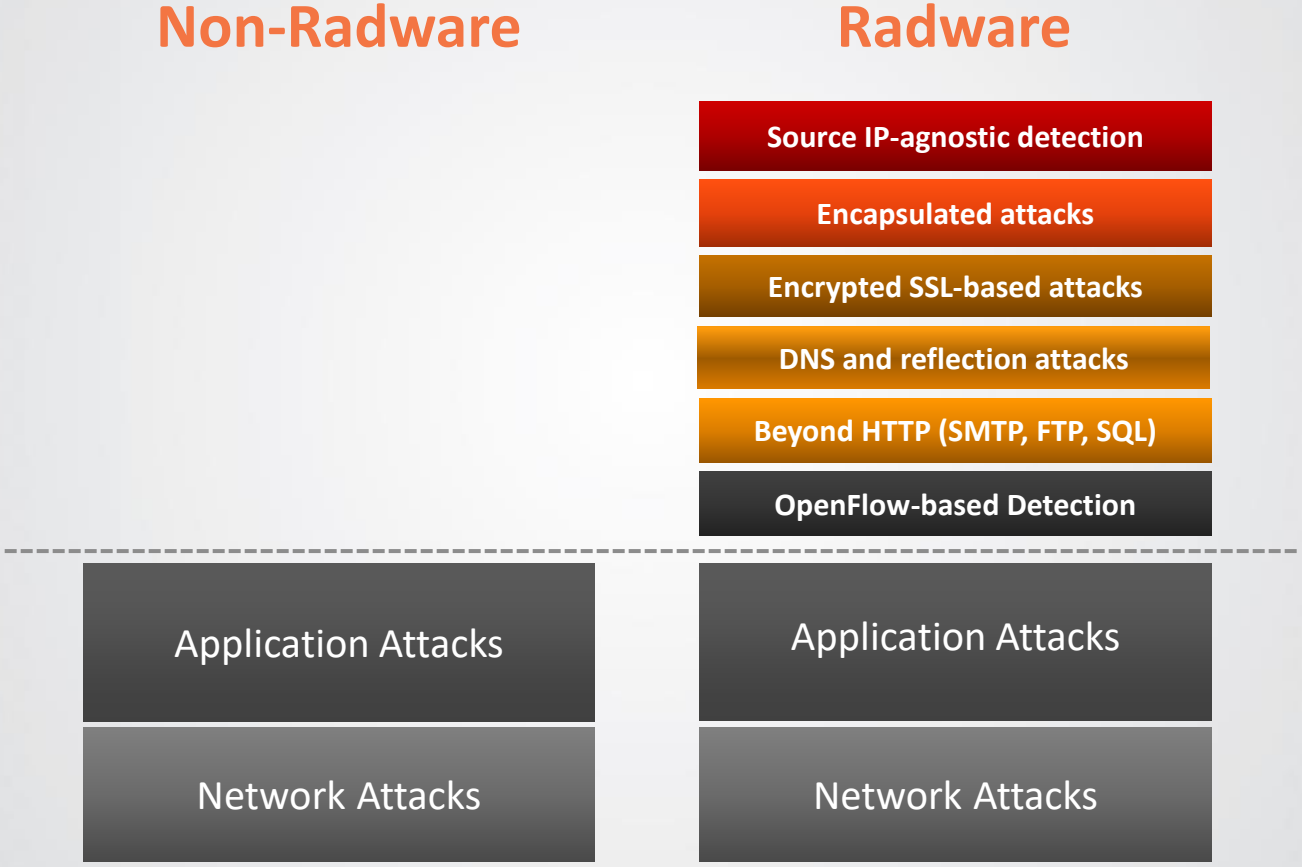
Collection

Detection

Mitigation

Operation

How Can You Protect From Something You Don't See?



Radware can protect against **x2 of attacks**

Radware Detection Elements

Real-time attack mitigation device providing layer 4-7 multi-attack coverage

DefensePro

Real-time attack mitigation device providing layer 4-7 multi-attack coverage

DefenseFlow

Network-wide attack detection and cyber command and control

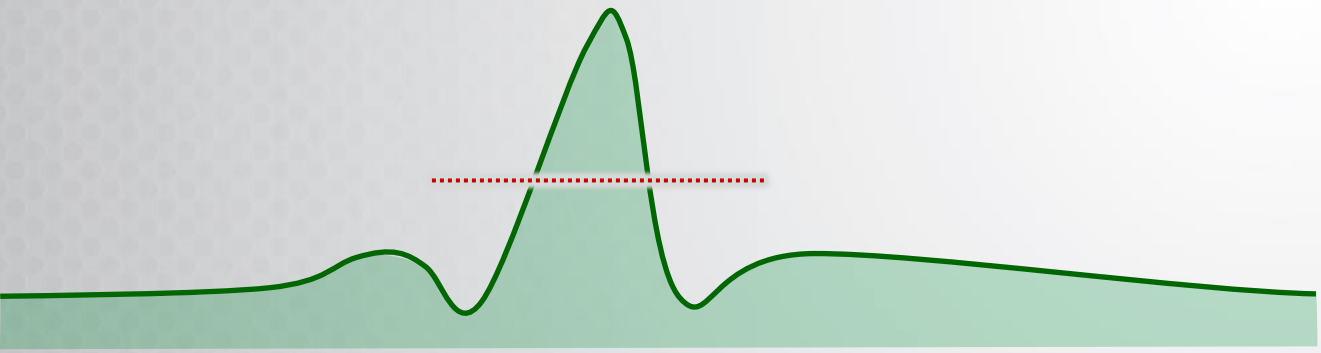
AppWall

Web Application Firewall (WAF) providing full coverage of OWASP top-10 threats

Behavior-Based vs. Rate-Based Detection

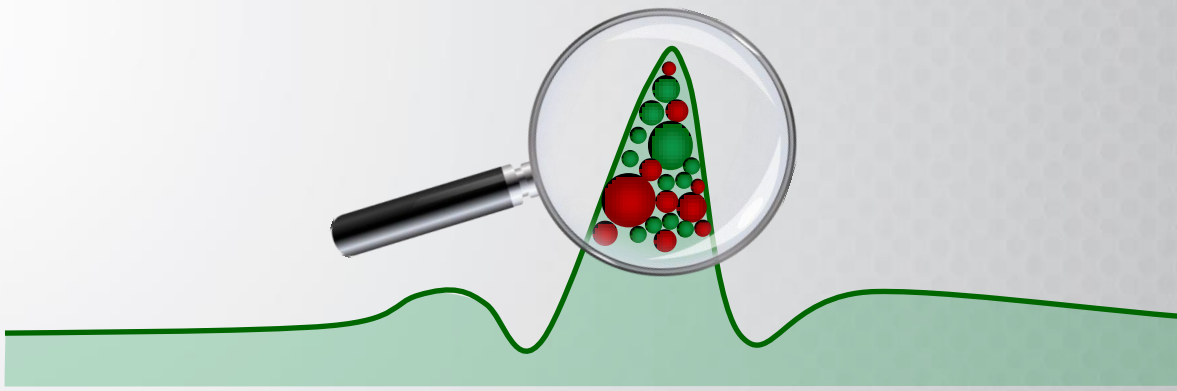
Non-Radware

Rate-Based Detection



Radware

Behavior-Based Detection



To prevent service-level impact of legit traffic

Attack Mitigation Pillars

Collection

Detection

Mitigation

Operation

Beyond Primitive Source IP Blocking

Non-Radware

Source IP Address Only

X.X.X.X

Radware

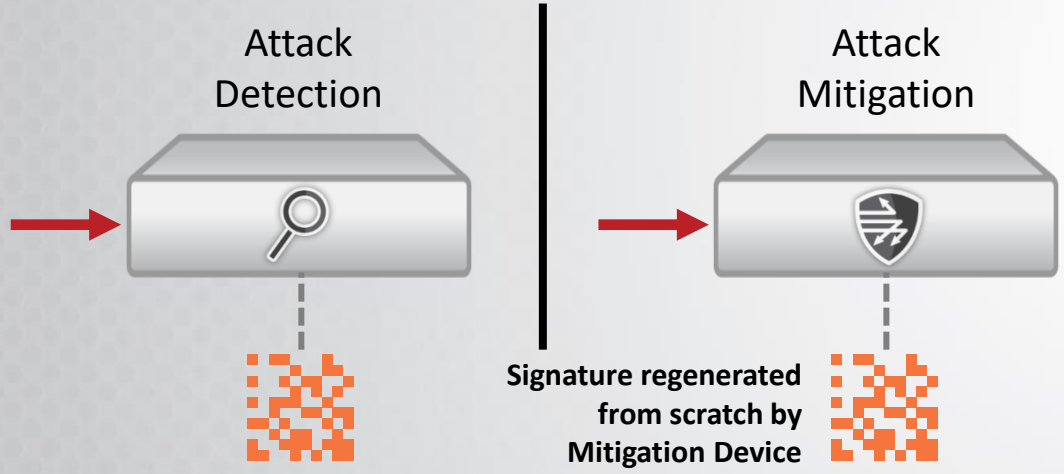
Signature with multiple parameters

Smart traffic blocking based on Real-Time Signature incorporating **multiple parameters** comparing to primitive source IP address blocking

Shortest Time to Mitigate via Synchronized Operation

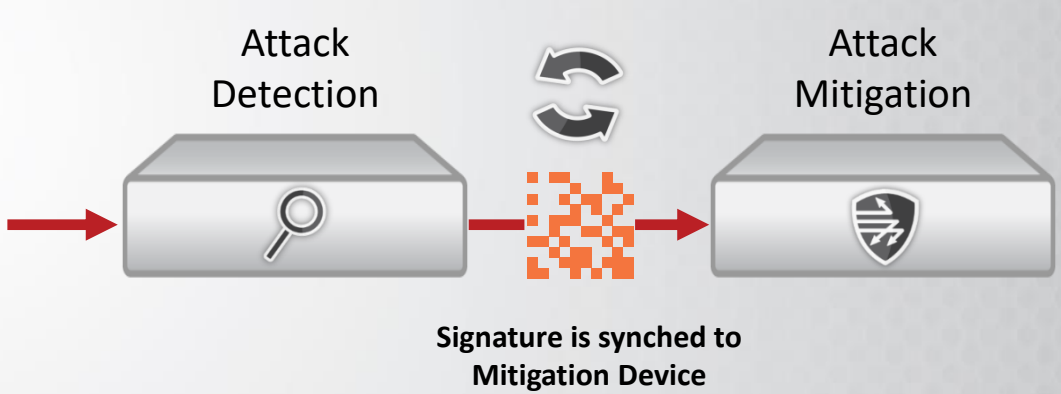
Non-Radware

Non-Synchronized Operation



Radware

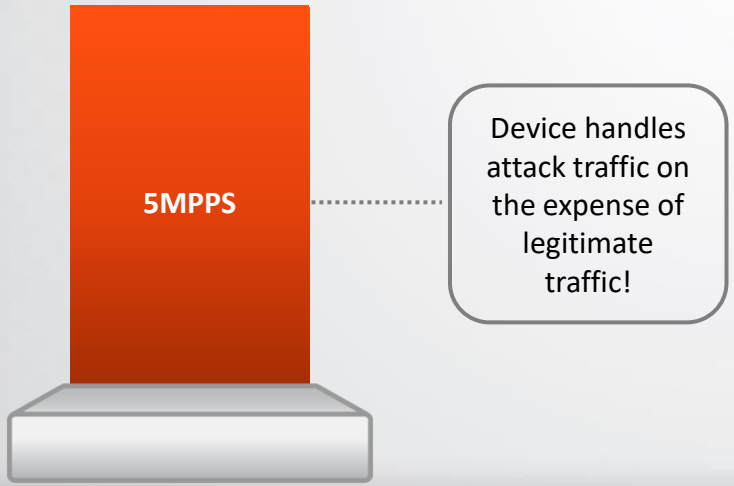
Synchronized Operation



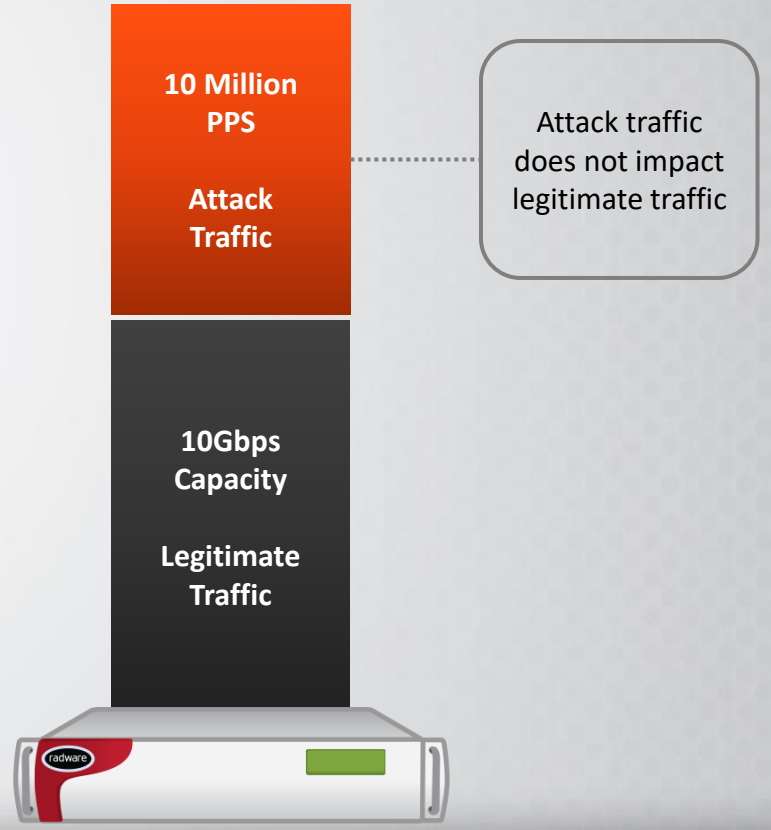
Radware synchronized operation = **real-time** mitigation engagement

Dedicated Hardware to Fight Attacks

Non-Radware



Radware



Attack Mitigation Pillars

Collection

Detection

Mitigation

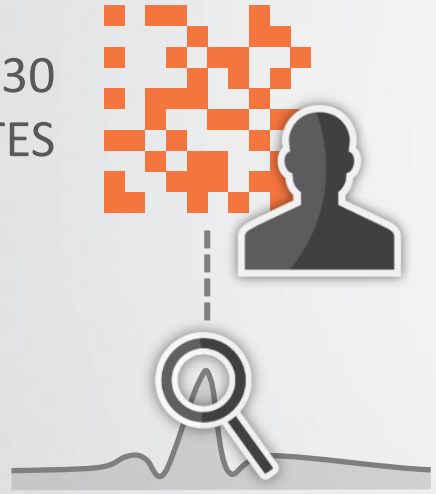
Operation

Real-Time Signature Generation vs. Manual

Non-Radware

Manual Signature Generation

30
MINUTES



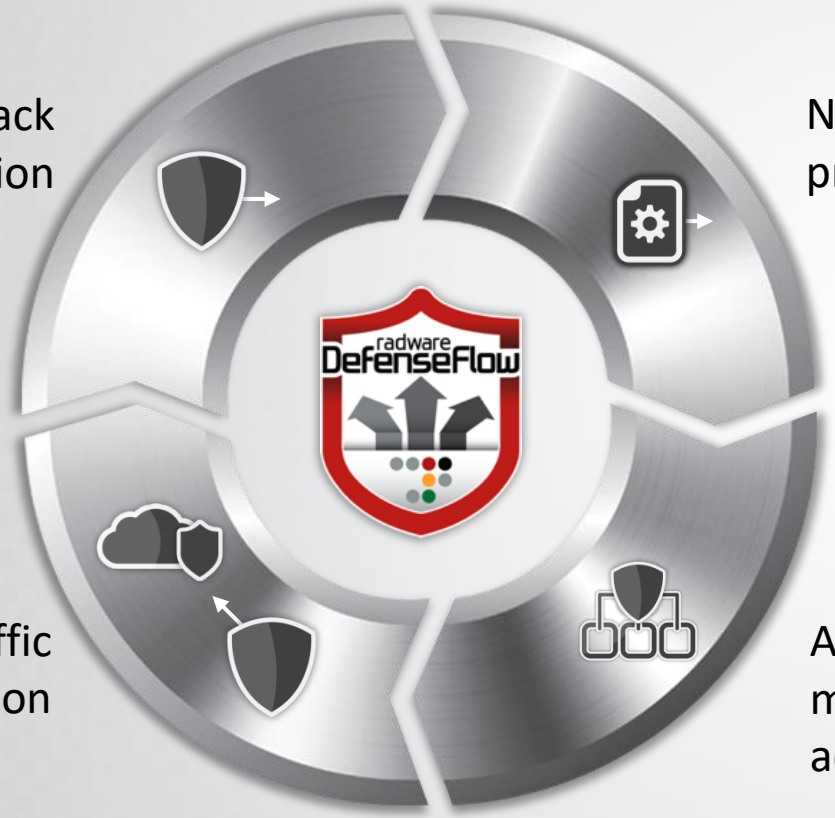
Radware

Real-Time Signature Generation

18
SECONDS

Manual signature creation can take up to **30 minutes.**
Radware Real-Time Signature is generated in **up to 18 seconds.**

Complete & Automatic Attack Lifecycle Management



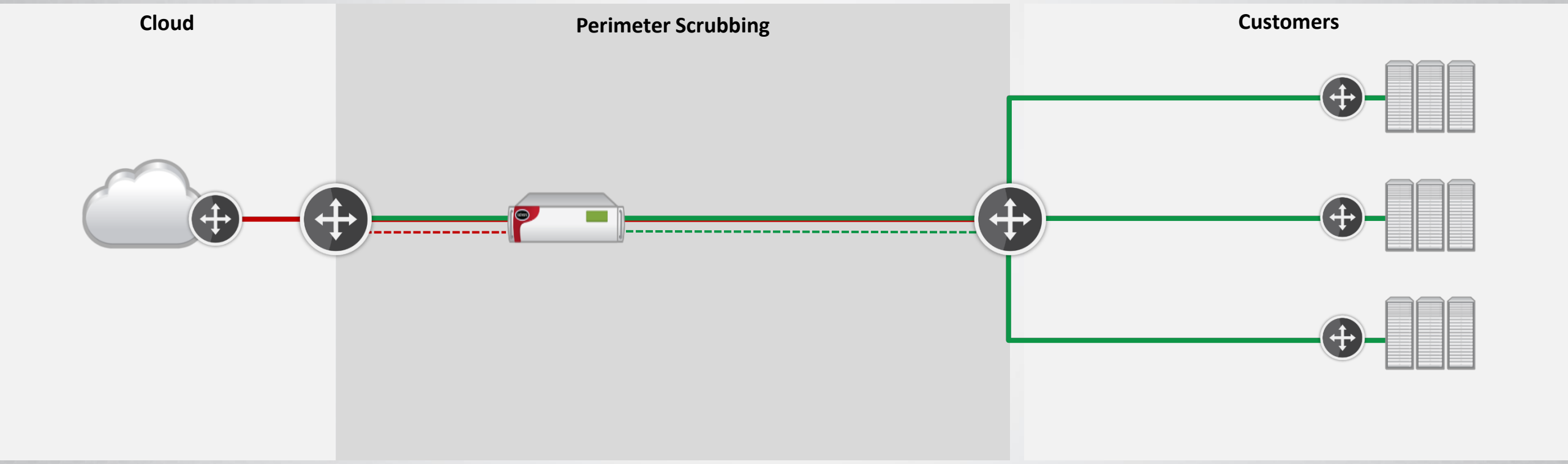
- **Lower TCO**
- **Less dependency on HR**

Radware Protection In-Action

Deployment Architectures

1. **Inline Perimeter**
2. Scrubbing Center (NetFlow-based Protection)
3. Hybrid Attack Mitigation
4. Top-of-Rack
5. Peak Protection

Inline Perimeter Infrastructure Protection



Unique Value:

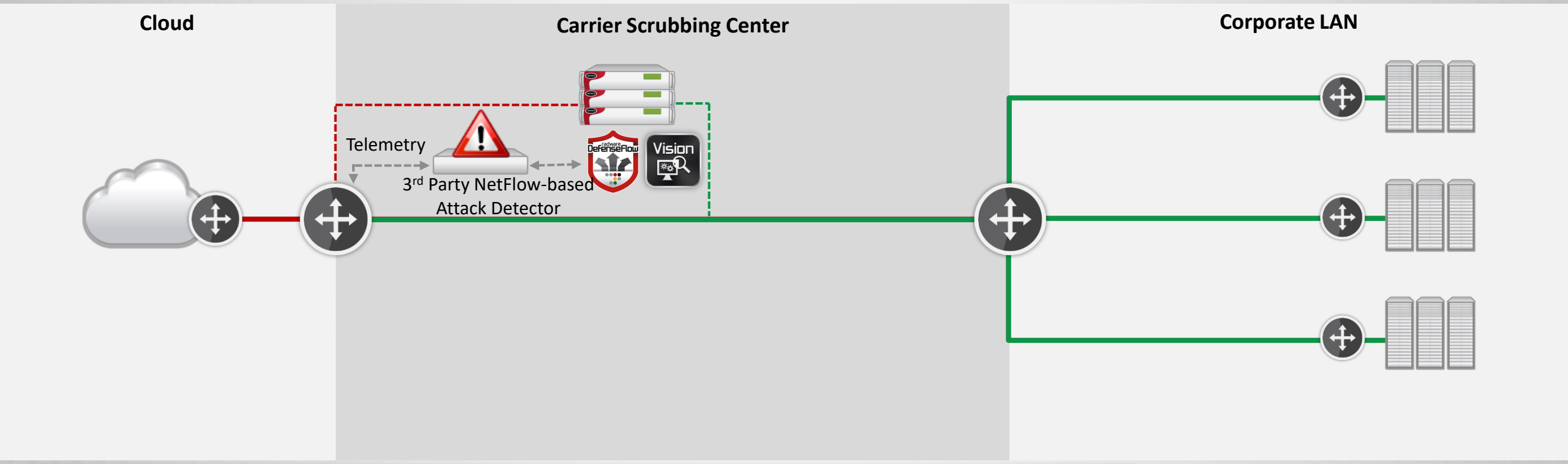
- Optimal level of protection, providing immediate detection and mitigation of Layer 2-7 attacks
- Permits a scalable customer offering - leveraging the same device for infrastructure protection
- Simple - does not require any diversion of traffic or changes to the network

Deployment Architectures

1. Inline Perimeter
2. **Scrubbing Center (NetFlow-based Protection)**
3. Hybrid Attack Mitigation
4. Top-of-Rack
5. Peak Protection

Use Case 1 – 3rd Party NetFlow-Based Attack Detection

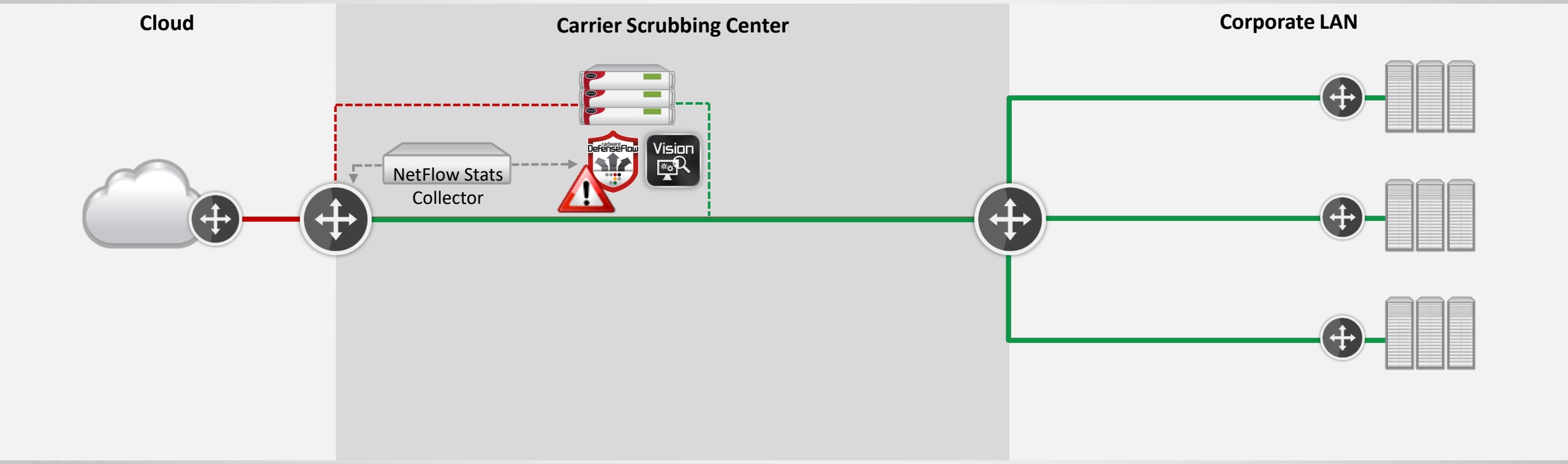
Tier 1: Infrastructure and Volumetric Protection (with 3rd party telemetry device)



Flow based telemetry used to detect network layer attacks from peering edges while high capacity Mitigation Center is used to protect infrastructure

Use Case 2: NetFlow-Based Attack Detection

Tier 1: Infrastructure and Volumetric Protection (with DefenseFlow as detector)



Flow based telemetry used to detect network layer attacks from peering edges while high capacity Mitigation Center is used to protect infrastructure

Unique Value:

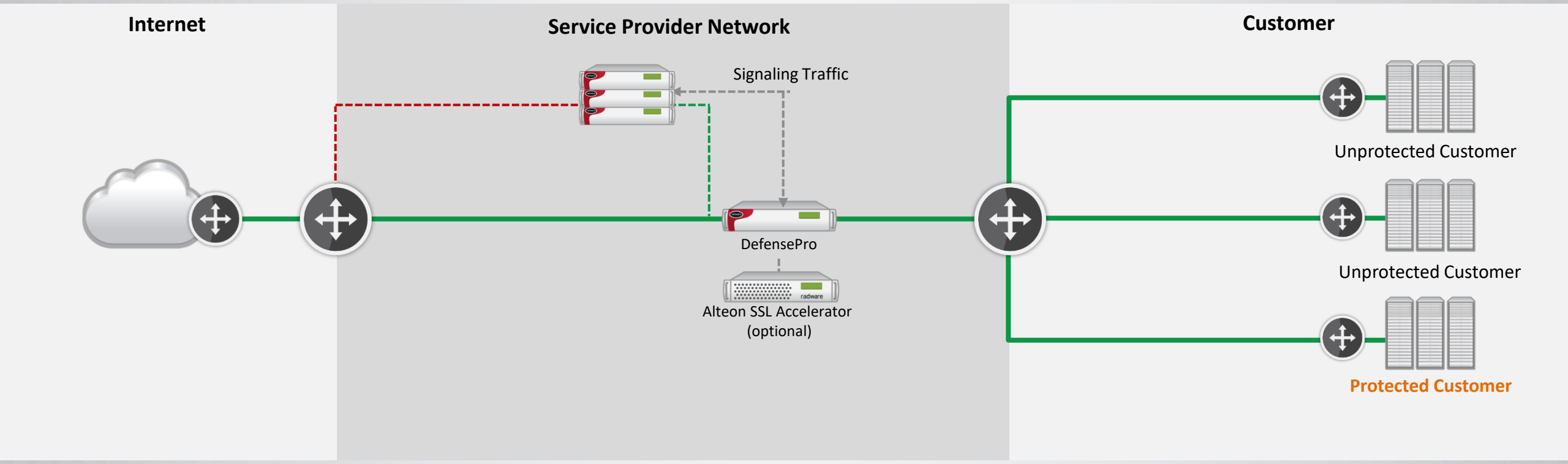
Radware Behavioral Technology delivers the fastest time to mitigation and mitigation accuracy in Out-Of-Path Infrastructure Protection

Deployment Architectures

1. Inline Perimeter
2. Scrubbing Center (NetFlow-based Protection)
3. **Hybrid Attack Mitigation**
4. Top-of-Rack
5. Peak Protection

Network-Based Hybrid Attack Mitigation

Inline Real-Time Protection with On-Demand Scrubbing

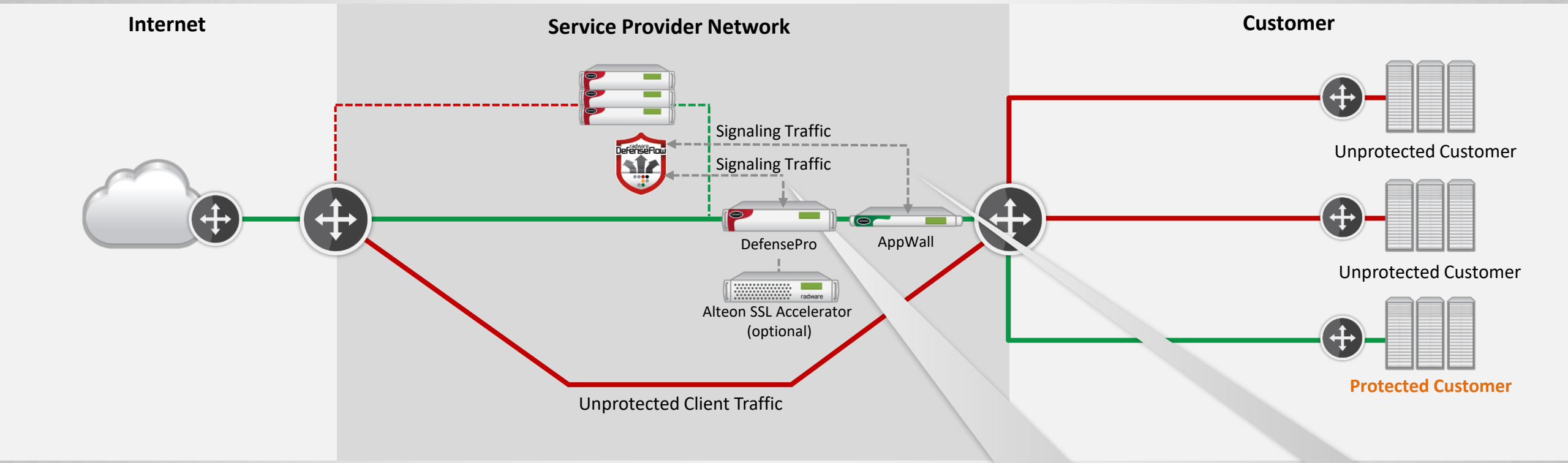


Unique Value:

- Deeper level protections enable real-time protection for the fully array of both network and application attacks
- Signaling to cloud-based scrubbing for volumetric attacks
- Best long-term return on investment and supports over subscription of network based components

Network-Based Hybrid Attack Mitigation

Customer Applications Inline Real-Time Protection



Unique Value:

- Immediate mitigation of application and network attacks
- Widest security coverage
- Signaling to Tier 1 for volumetric attacks

DC Applications protected by advanced inline detection with signaling to activate higher tier mitigation when necessary

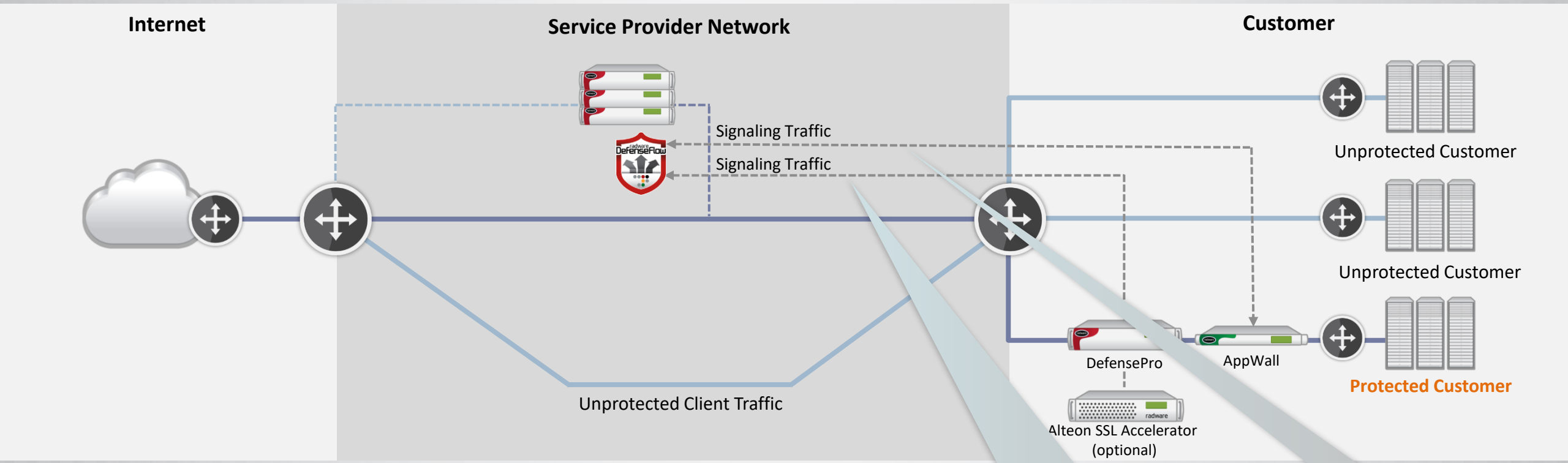
Web applications protected by advanced web tier protection

Deployment Architectures

1. Inline Perimeter
2. Scrubbing Center (NetFlow-based Protection)
3. Hybrid Attack Mitigation
4. **Top-of-Rack**
5. Peak Protection

Top-of-Rack (TOR)

Tenant Application Inline Protection

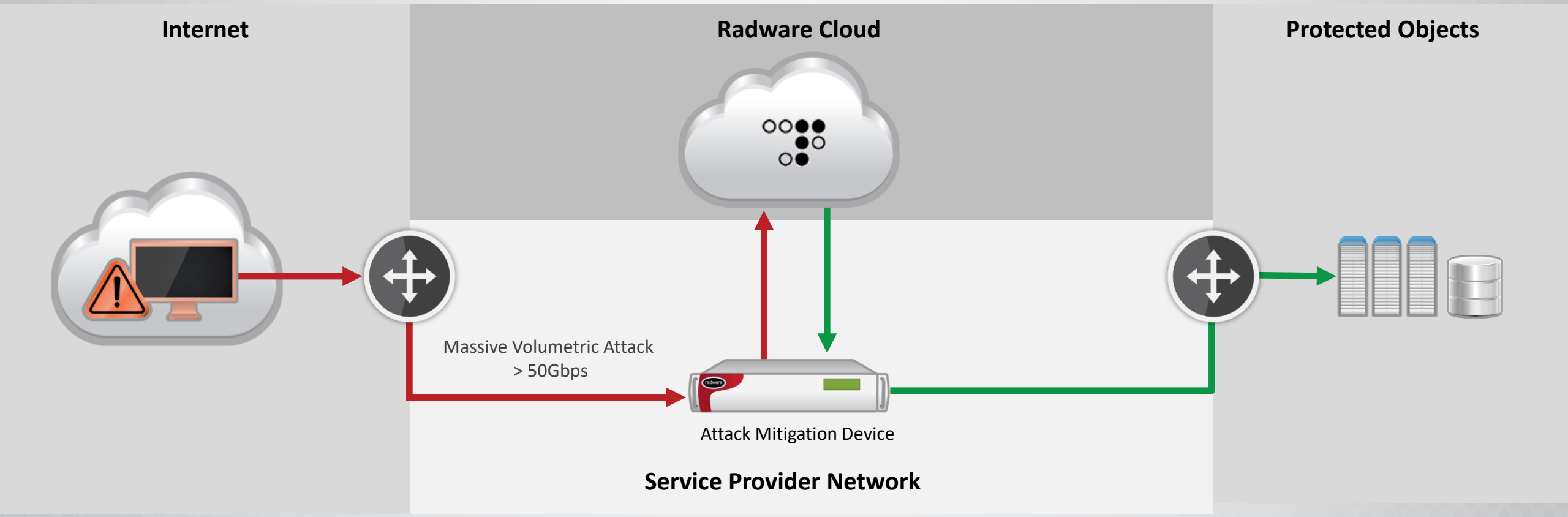


Unique Value: Dedicated hardware and resources per customer with full integration to Tier 1 mitigation

Deployment Architectures

1. Inline Perimeter
2. Scrubbing Center (NetFlow-based Protection)
3. Hybrid Attack Mitigation
4. Top-of-Rack
5. **Peak Protection**

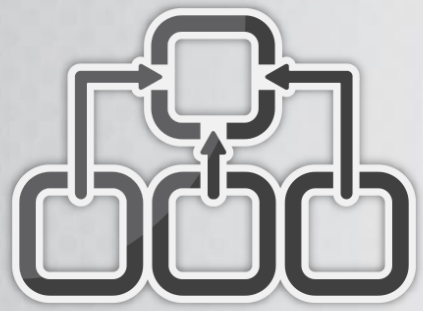
Radware Cloud DDoS Peak Protection Service



On demand infrastructure protection from very large DDoS attacks (>50Gbps).

Summary

Attack Mitigation Pillars



Collection

Detection

Mitigation

Operation

radware

Every second counts

CLICO