radware

Attack Mitigation Service Brochure

Protecting Enterprises Against Cyber-Attacks with Always-On, Hybrid DDoS Protection Service

Radware's Attack Mitigation Service Integrates On-Premise Detection & Mitigation with Cloud DDoS Protection Service and 24x7 Emergency Response Team Support

The Age of the Integrated Hybrid Solution

Today's standard defense technologies, including DDoS protection, IPS, anomaly & behavioral analysis, SSL protection and WAF, are often provided in point solutions. These systems are almost never integrated and require dedicated resources consisting of IT managers and security experts to maintain and synchronize. Radware's Attack Mitigation Service combines the requisite technologies for making your business resilient to cyber-attacks with on-premise systems and the ability to scale on demand with a cloud-based scrubbing center. The service integrates fully-managed on-premise detection and mitigation with cloud-based DDoS protection service.

Radware's Attack Mitigation Service includes the following three components:

1. Radware's DDoS mitigation device - DefensePro - deployed on-premise for real-time detection and mitigation of cyber attacks.

2. Radware's Hybrid Cloud DDoS Protection Service - only activated upon volumetric attacks that aim to saturate the Internet pipe.

3. Radware's ERT Premium - an extended set of managed services that includes on-premise device management and 24x7 monitoring, detecting, alerting and mitigating DDoS attacks.
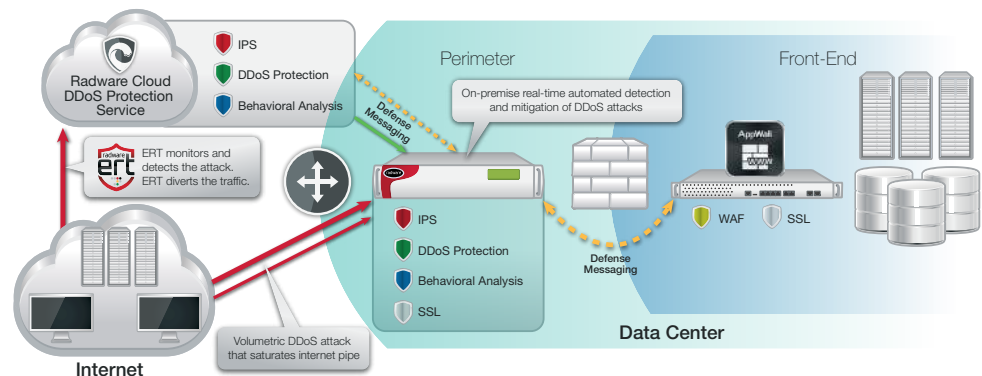

Figure 1: Attack Mitigation Service: Scalable Hybrid Network Defense

Always-On DDoS Protection

Radware's on-premise defense component ensures that the data center is protected by providing accurate real-time detection and mitigation of multi-vector DDoS attacks, which is not possible using only a cloud-based DDoS solution. In cases of volumetric attacks that threaten to saturate the Internet pipe, mitigation is moved to the cloud. This enables a smooth transition between mitigation options and assures immediate protection with no disruption gaps and without the addition of scrubbing center latency.

According to Radware's Emergency Response Team (ERT), it is only in 15% of attacks that the pipe is at risk of being saturated. These hybrid protection capabilities ensure that traffic is not diverted unless it is absolutely necessary. As a result, the organization is fully protected and time to mitigation is measured in seconds.

Monitor. Analyze. Report.

Radware's Attack Mitigation Service includes active monitoring and health checks on the protected service or application. In addition, the service includes pipe saturation monitoring and customer notification when there is a risk for saturation and action is required.

Figure 2: Attack Mitigation Service Portal Dashboard

Ongoing reports regarding all attacks that were mitigated by the service (automatically mitigated or invoked) are available for viewing on a web-based service portal. When Radware's ERT is involved in mitigating an attack, a full post attack analysis report is provided to the customer.

Single Point of Contact for DDoS Attack Mitigation

Radware's Attack Mitigation Service also includes 24x7 ERT support for hands-on attack mitigation assistance from a single point of contact. The ERT provides expertise needed during prolonged, multi-vector attacks. This includes working closely with customers to decide on the diversion of traffic during volumetric attacks, assisting with capturing files, analyzing the situation and ensuring the best mitigation options are implemented. The ERT's experience with fighting widely known attacks in the industry provides best practice approaches to fight each and every attack.

Your Peace of Mind with a Fully Managed Service

Radware's Attack Mitigation Service comes with ERT Premium – an extended set of services that includes 24x7 monitoring and blocking of DDoS attacks with:

- On-premise device configuration and management
- Network statistics and attacks' situational awareness available on an online portal
- Real-time attack mitigation with direct "hot-line" access to the ERT
- Preemptive attack intelligence to provide managed customers early warnings of attacks
- ERT post attack forensic analysis and recommendations
- A fully dedicated and proactive technical account manager
- Quarterly review of forensics reports and security configurations to provide recommendations
- Ongoing periodical configurations, reports and recommendations

Robust Global Cloud Network

With over 2Tbps of mitigation capacity spread strategically across scrubbing centers around the world for when volumetric attacks threaten to saturate customers' link capacity.

Attack Vectors

Over 100 attack vectors on the network and application layers are detected and mitigated including:

- Large volume network attacks
- SYN floods
- HTTP floods
- Brute force
- Session attacks
- Low and slow
- SSL encryption
- BGP table attacks
- Invasive scans

Service Considerations

Complexity and length of attacks drain resources – outsource attack mitigation to experts

Cost-effective monthly service fee with:
- Guaranteed SLA throughout term of the agreement
- On-premise equipment can be leased
- Reports covering all attacks that were mitigated are available on the service portal

Benefits

Most comprehensive attack mitigation coverage:
- Non-volumetric, low & slow attack protection
- Encrypted SSL attack protection
- Multi-vector attack detection & mitigation

Shortest time to protection – active mitigation within seconds with real-time, always-on protection

Most professional security service available:
- Service and attack mitigation infrastructure fully monitored and managed by Radware's team of experts
- 24x7 Emergency Response Team (ERT) support – single point of contact of trained security experts with the wide experience and deep knowledge of threats, attack tools, intelligence and mitigation technologies
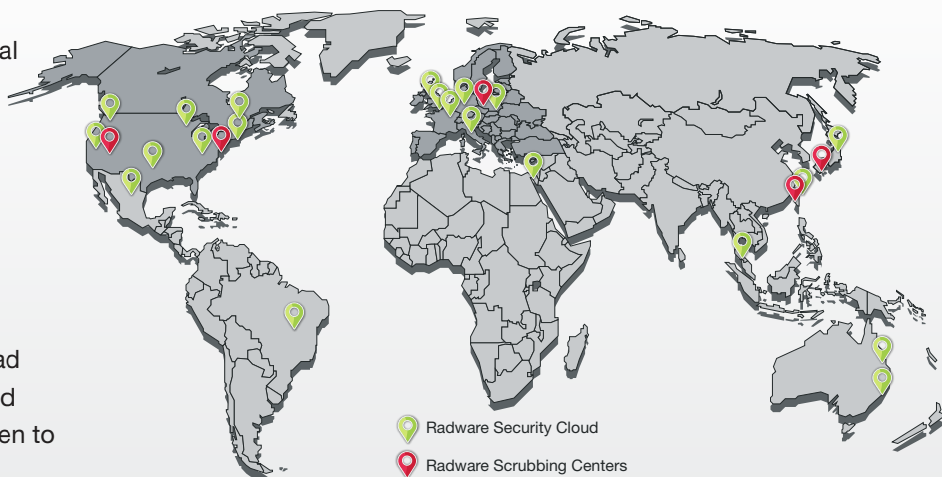- High availability and low latency – global network of attack scrubbing centers

Radware Security Cloud
Radware Scrubbing Centers

Figure 3: Radware's Global Cloud Security Network

Radware's Attack Mitigation Service

Provides the most comprehensive attack mitigation coverage that includes:

End-to-end service and protection: A hybrid DDoS protection solution leaving the ownership, monitoring and mitigation with the service provider

Widest security coverage including multi-vector attack detection and mitigation, handling attacks at the network layer, server-based attacks, malware propagation and intrusion activities

Minimal time to mitigate with mitigation starting on-premise in real time and no protection gap when traffic is diverted to the cloud

Flexibility with a full OPEX based DDoS attack mitigation service subscription

Single point of contact and extensive managed services by battle proven security and DDoS experts

About Radware

Radware® (NASDAQ: RDWR), is a global leader of application delivery and cyber security solutions for virtual, cloud and software defined data centers. Its award-winning solutions portfolio delivers service level assurance for business-critical applications, while maximizing IT efficiency. Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis on DDoS attack tools, trends and threats.

Certainty Support

Radware offers technical support for all of its products through the Certainty Support Program. Each level of the Certainty Support Program consists of four elements: phone support, software updates, hardware maintenance, and on-site support. Radware also has dedicated engineering staff that can assist customers on a professional services basis for advanced project deployments.

Learn More

To learn more about how Radware's integrated application delivery & security solutions can enable you to get the most of your business and IT investments, email us at info@radware.com or go to www.radware.com.