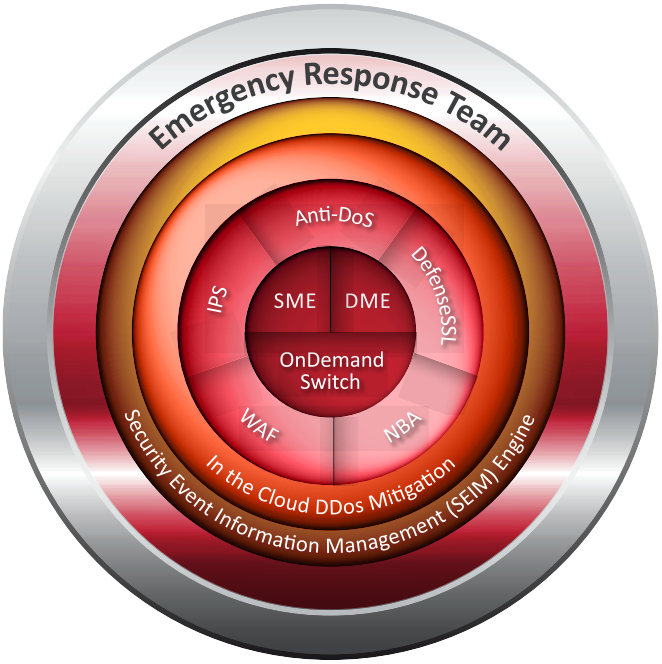
radware

Radware's Attack Mitigation Solution

Protect Online Businesses and Data Centers Against Emerging Application & Network Threats - Whitepaper



SHARE THIS WHITEPAPER

Table of Contents

Understanding the Threat Landscape

In the past, everything enterprises protected – data centers, applications, and databases - resided in the perimeter. Organizations had to secure the perimeter in order to keep assets protected. Yet today, as organizations adopt cloud technologies to improve overall efficiency and expand business opportunities, they face a more distributed network infrastructure and are required to protect assets beyond the perimeter.

Organizations of all sizes are struggling to finance costs associated with cyber-attack prevention and mitigation. Cyber-attacks that cause network, server and application downtime and/or service degradation can lead to reduced revenues, higher expenses and damaged reputations.

Cyber-attacks reached a tipping point in terms of quantity, length, complexity and targets. As cyber threats grow and expand to new targets, even organizations with by-the-book security programs can be caught off guard.

The Evolution of Attackers' Motivation

As cyber-attacks continue to threaten organizations, attacker's motivations evolve. Richard Clarke, a former Special Advisor of Cybersecurity, defines the four main motivations for cyber-attack - **CHEW**:

- **C**ybercrime-the notion that someone is going to attack you with the primary motive being financial gain from the endeavor.
- **H**acktivism- attacks motivated by ideological differences. The primary focus of these attacks is not financial but rather to persuade or dissuade certain actions or "voices."
- **E**spionage - straightforward motive to gain information on another organization in pursuit of political, financial, capitalistic, market share or some other form of leverage.
- **W**ar (Cyber) - the notion of a nation-state or transnational threat to an adversary's centers of power via a cyber-attack. Attacks could focus on non-military critical infrastructure or financial services or more traditional targets, such as the military-industrial complex.

Attacks can be driven by one or more of these motives and attackers can vary from script kiddies, members of organized crime, to governments.

Attacks Are Longer, More Complex and Continuous

Attackers are deploying multi-vector (e.g., different types) attack campaigns that target all layers of the victim's IT infrastructure including the network, server and application layers. Attackers are more patient and persistent - leveraging "low & slow" attack techniques that misuse the application resource rather than resources in the network stacks. They also use more evasive techniques to avoid detection and mitigation including SSL-based attacks, changing the page request in a HTTP page flood attack and more.

Years ago, DoS attacks targeted mostly the network through SYN, TCP, UDP and ICMP floods. From 2010-2012 there was an increase in more sophisticated application level attacks and SSL encryption-based attacks. Recently, a specific type of DoS attack—the amplification reflective flood—has not only revived network attacks but also given them an edge over counterparts that target applications. Reflective attacks, including those using DNS, NTP, and CHARGEN, started heating up in 2013 and remained a persistent threat throughout 2014. The rise in reflective attacks has contributed to crowning the Internet pipe as the major failure point in enterprise security.

The length of an attack indicates another new trend in DDoS attacks -constant attacks. The graph below from Radware's 2014-2015 Global Application & Network Security Report highlights the rise in continuous attacks in which attackers continuously and constantly attack the same organization.

The simplicity of launching such cyber-attacks and the variety of attack tools available are reasons why more organizations are suffering from increased attacks, such as DDoS. The question is no longer about preventing attacks. The attacks are happening. It is about detecting and mitigating attacks.

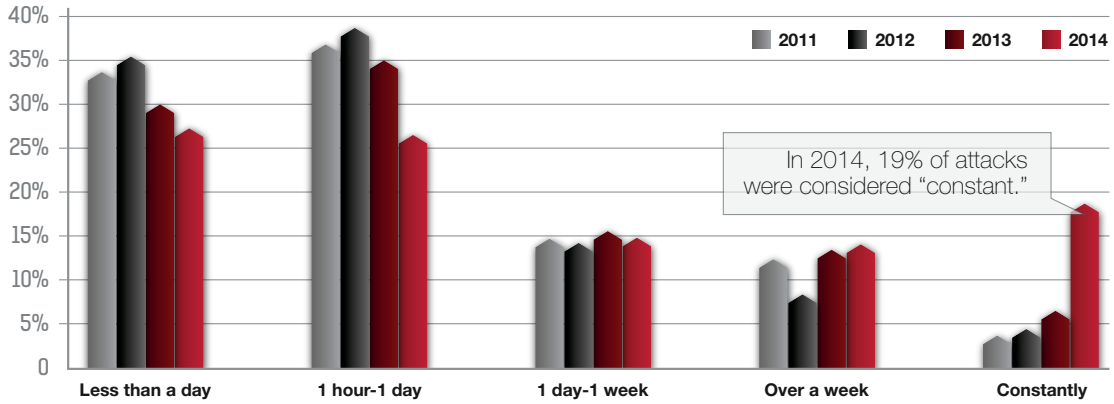


Figure 1: Attack durations year by year, as presented in the Radware Global Application & Network Security Report 2014-2015.

Protection from Multi-Vector Attacks

In order to fight evolving threats, organizations need to implement the most adequate security solutions to fully protect against new threats and all types of attacks.

Attackers are deploying multi-vector attack campaigns by increasing the number of attack vectors launched in parallel. In order to target an organization's blind spot, different attack vectors target different layers of the network and data center. Even if only one vector goes undetected then the attack is successful and the result is highly destructive.

To effectively mitigate all types of DDoS attacks, multiple protection tools are needed.

- **Cloud DoS protection** to mitigate volumetric attacks that threaten to saturate the Internet pipe.
- **DoS protection** to detect and mitigate all types of network DDoS attacks.
- **Behavioral Analysis** to protect against application DDoS and misuse attacks. Those attacks are harder to detect and appear like legitimate traffic so they can go unnoticed without a behavioral analysis tool.
- **Intrusion Prevention System (IPS)** to block known attack tools and the low and slow attacks.
- **SSL protection** to protect against encrypted flood attacks.
- **Web Application Firewall (WAF)** to prevent web application vulnerability exploitations.

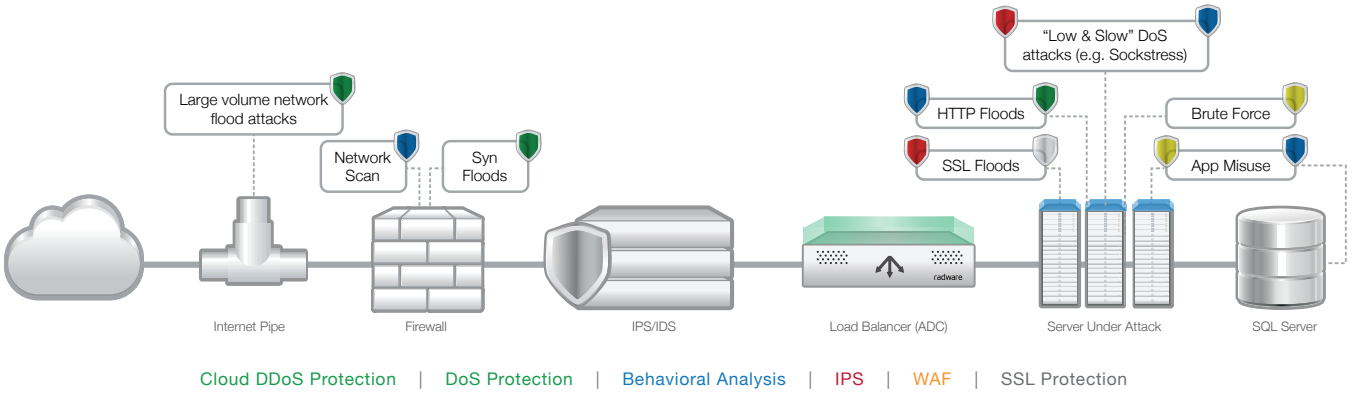


Figure 2: Attack vectors and the technology tools used to detect and mitigate

Radware Attack Mitigation 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 hybrid attack mitigation solution combines the requisite technologies for making businesses resilient to cyber-attacks with on-premise systems and the ability to scale on demand with a cloud based scrubbing center. It is a hybrid attack mitigation service that integrates on-premise detection and mitigation with cloud-based volumetric attack scrubbing.

The solution was designed to help organizations mitigate attacks you can detect and offers a security solution that combines detection and mitigation tools from a single vendor. Radware's solution provides maximum coverage, accurate detection and shortest time to protection.

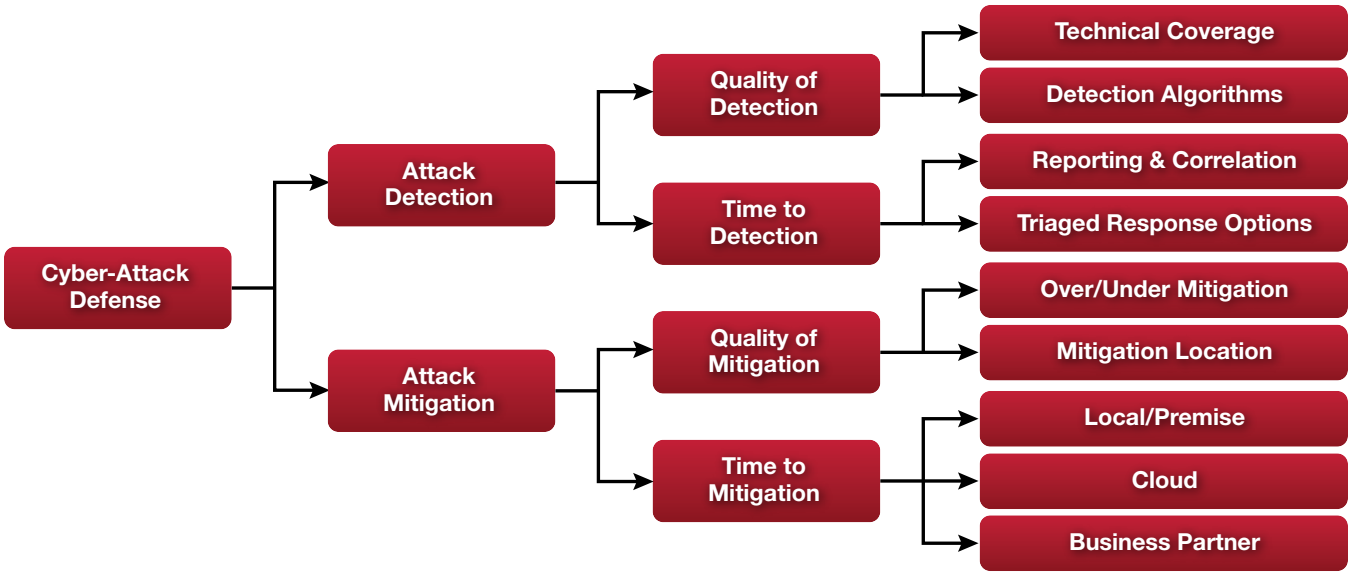


Figure 3: Comprehensive cyber-attack protection with detection & mitigation

Widest Attack Coverage, Including SSL-Based Attacks

Radware's attack mitigation solution offers a multi-vector attack detection and mitigation solution, handling attacks at the network layer, server based attacks, malware propagation and intrusion activities. The solution includes protection against volumetric and non-volumetric attacks, SYN Flood attacks, Low & Slow attacks, HTTP floods, SSL based attacks and more. As the solution analyzes the traffic, it builds traffic baselines that are customized for the deploying organization.

The solution mitigates SSL-based attacks using challenge-response mitigation techniques. SSL decryption and challenge response mechanisms are enforced only on suspicious traffic. The result is the lowest latency SSL mitigation solution in the industry, as legitimate traffic is not affected by the mitigation efforts.

Radware's on-premise protection is comprised of 5 modules; all optimized for online business and data center protection, and designed for data center and carrier deployments.

DoS Protection – protects from all types of network DDoS attacks including:

- UDP flood attacks
- SYN flood attacks
- TCP flood attacks
- ICMP flood attacks
- IGMP flood attacks
- Out-of-state flood attacks

NBA – the network behavioral analysis module prevents application resource misuse and zero-minute malware spread. Attacks protected include:

- HTTP page flood attacks
- DNS flood attacks
- SIP Flood attacks
- Brute force attacks
- Network and port scanning
- Malware propagation

IPS – This module protects against:

- Application vulnerabilities and exploits
- OS vulnerabilities and exploits
- Network infrastructure vulnerabilities
- Malware such as worms, Bots, Trojans and Drop-points, Spyware
- Anonymizers
- IPv6 attacks
- Protocol anomalies

SSL Attack Mitigation – provides protection from SSL based-DDoS attacks.

- Uniquely mitigates floods that are directed to HTTPS pages
- Provides unlimited SSL decryption and encryption capabilities
- Operates in symmetric and asymmetric environments

WAF – the web application firewall prevents all type of web server attacks such as:

- Cross site scripting (XSS)
- SQL injection
- Web application vulnerabilities
- Cross site request forgery (CSRF)
- Cookie poisoning, session hijacking, brute force

High Accuracy of Detection and Mitigation

The network behavioral analysis (NBA) module in Radware's attack mitigation platform employs patented behavioral-based real-time signature technology. It creates baselines of normal network, application, and user behavior. When an anomalous behavior is detected as an attack, the NBA module creates a real-time signature that uses the attack characteristics, and starts blocking the attack immediately. By implementing patent-protected behavioral analysis technology, Radware's attack mitigation solution can detect attacks in a very short timeframe with minimal false positives.

Always-On Protection and Shortest Time to Mitigation

Radware's on-premise attack mitigation device ensures that the data-center is constantly protected. It provides always-on full protection against multi-vector DDoS attacks. Only in cases of volumetric attacks, where the organization's internet pipe is about to saturate, is traffic diverted to Radware's cloud-based scrubbing center, clearing attack traffic before it reaches the Internet pipe. This enables smooth transition between mitigation options.

The always-on protection ensures that the organization is fully protected and time to mitigation is measured in seconds. Moreover in case of an attack that requires the traffic to be diverted to the cloud-scrubbing center, the protection continues with no disruption or gaps.

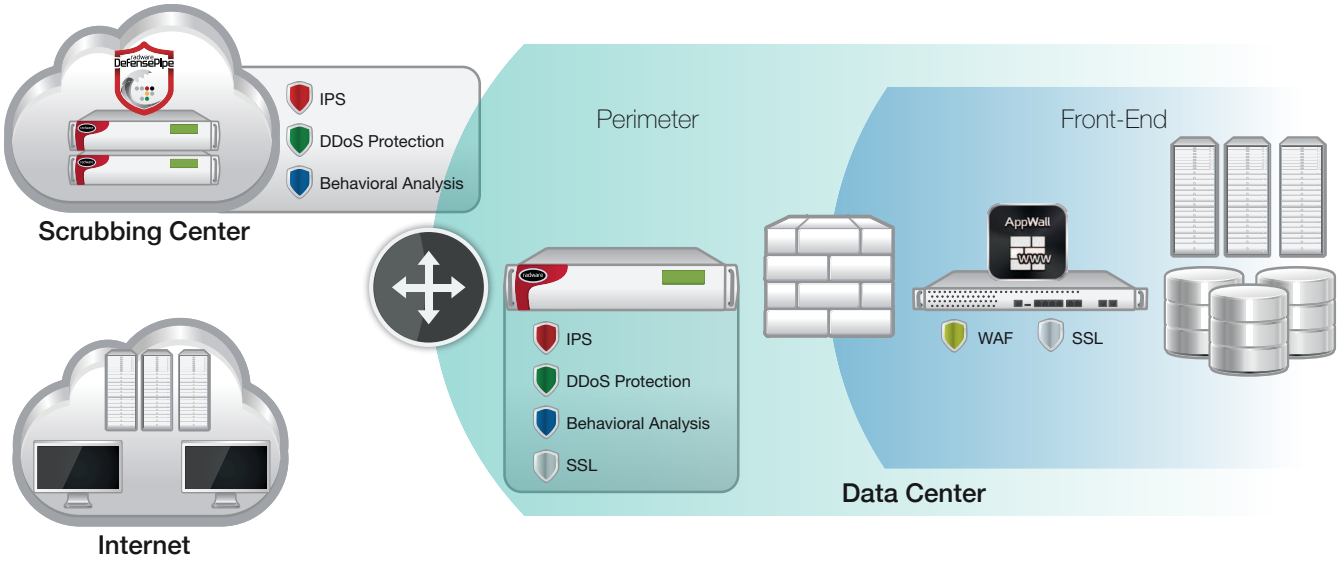


Figure 4: Radware Hybrid Attack Mitigation Solution

Protection Against Web Application Attacks

Radware's Web Application Firewall (WAF), provides complete protection against: web application attacks, web application attacks behind CDNs, advanced HTTP attacks (slowloris, dynamic floods), brute force attacks on login pages and more.

A messaging mechanism enables Radware's WAF to signal Radware's perimeter attack mitigation device when a web application attack is detected in order to block it at the perimeter, protecting the rest of the network.

As organizations migrate applications to the cloud, Radware also offers a cloud-based WAF service to also protect cloud-based applications from web-based attacks. Radware's Hybrid Cloud WAF offering provides a fully managed enterprise grade WAF that protects both on-premise and cloud-based applications, using a single technology solution. Unlike existing WAF solutions that integrate dual technologies that result in a gap between protection coverage and quality, Radware's single technology approach makes migrating applications to the cloud safer and more secure.

Monitor. Analyze. Report.

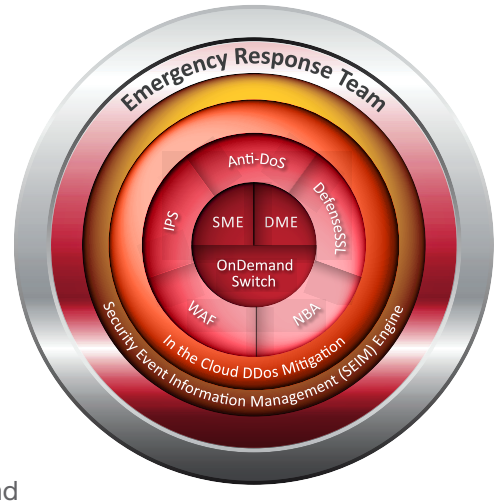
Radware's solution includes active monitoring and health checks on the protected service or application, providing an organization-wide view of security and compliance status from a single console. Ongoing reports regarding all attacks that were mitigated by the system (automatically mitigated or invoked) are available for viewing on a web-based service portal. The built-in Security Event Information Management (SEIM) system provides an organization-wide view of security and compliance status from a single console. Data from multiple sources is collected and evaluated in a consolidated view of dashboards and reports. These views provide extensive, yet simple drilldown capabilities that allow users to easily obtain information to speed incident identification and provide root cause analysis, improving collaboration between NOC and SOC teams, and accelerating the resolution of security incidents.

24x7 Security Experts

Radware's attack mitigation solution is complemented by the Emergency Response Team (ERT), providing 24x7 support for hands-on attack mitigation assistance from a single point of contact. With the necessary expertise in mitigating prolonged, multi-vector attacks, the ERT works 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.

Summary: Wider, Faster, Broader Protection

DDoS attacks cause organizations to lose revenues and increase expenses. Attackers are more sophisticated and use multi-vulnerability attack campaigns. Radware's attack mitigation solution offers a hybrid, multi-layered mitigation solution with the broadest attack mitigation. Radware's hybrid solution provides the shortest time to mitigation, stopping multi-vulnerabilities DDoS attacks instantly, resuming revenues flow.



Hybrid solution that offers the widest protection coverage

- On-premise perimeter attack mitigation device detects and mitigates the full range of attacks including network and application layer attacks, SSL-based attacks, and low & slow attacks.
- Cloud scrubbing service mitigates volumetric attacks that are beyond the Internet pipe capacity.

Highest Accuracy of Detection and Mitigation

- Minimal false positives with patent-protected behavioral analysis technology.
- Real-time signatures and selective challenge-response mechanism for high mitigation accuracy.

Shortest Mitigation Response Time

- All attacks are detected on-premise in real-time. No need to wait for traffic diversion to start mitigation.
- Protection starts in seconds – shortest time to protect in the industry.
- Dedicated hardware guarantees best quality of experience to legitimate users.
- Traffic is diverted only as a last resort.

Complete Solution from a Single Vendor

- Radware's Emergency Response Team security experts fight the attack during the entire campaign.
- Single point of contact. No need to work with multiple vendors or services.
- Available as a fully managed service for simple, easy deployment.
- Integrated reporting with historical reporting and forensic analysis.

About Radware

Radware (NASDAQ: RDWR), is a global leader of application delivery and application security solutions for virtual and cloud data centers. Its award-winning solutions portfolio delivers full resilience for business-critical applications, maximum IT efficiency, and complete business agility. 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.