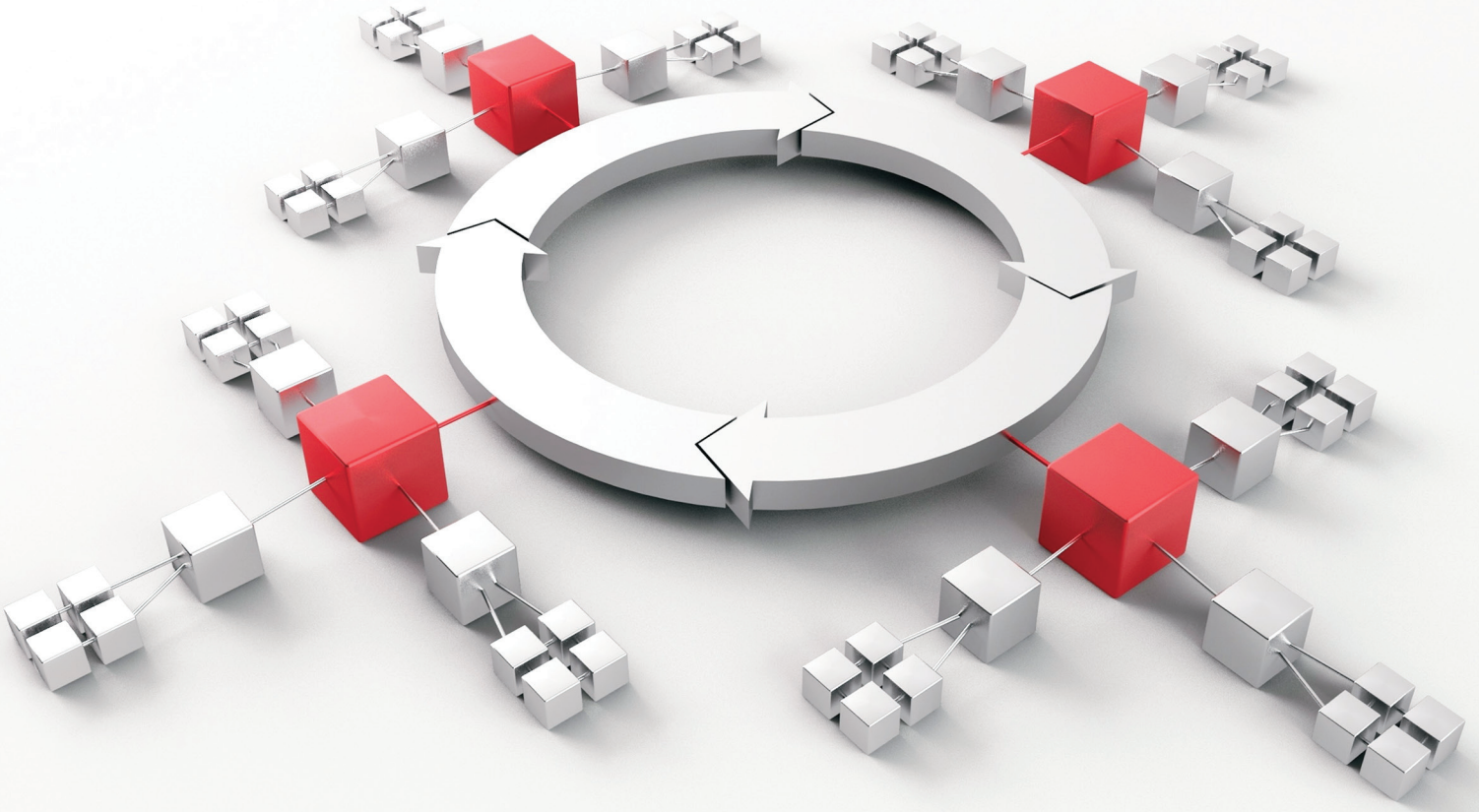

radware

SHARE THIS BROCHURE

Attack Mitigation Solution

Attack Mitigation Solution

Protect Enterprises Against Cyber Attacks with Always-On DDoS Attack Detection and Mitigation

Radware's attack mitigation is a hybrid solution integrating on-premise detection and mitigation with cloud-based volumetric attack scrubbing and 24x7 Emergency Response Team (ERT) support.

Organizations are challenged by an evolving threat landscape that reduces revenues, increases expenses and damages reputations. Today's cyber-attackers use sophisticated methods — often multiple attack-vectors in the same attack campaign — to bring down datacenters and organizations' web presence. The simplicity of launching such cyber-attacks and variety of attack tools available are reasons why more organizations are suffering from increased attacks, such as DDoS.

The Age of the Integrated Hybrid Solution

Today's standard defense technologies including DDoS protection, IPS, anomaly & behavioral analysis, SSL protection and web application firewalls (WAFs) 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 service.

Attack Mitigation Solution

By protecting enterprises against known and emerging network and application threats in real-time, Radware's layered approach is designed to help organizations mitigate attacks that can be detected and offer 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.

Radware's attack mitigation solution offers a multi-vector attack detection and mitigation solution, handling network layer and server based attacks, malware propagation and intrusion activities. Complete with anti-DoS, network behavioral analysis, SSL defense, IPS, WAF and in-the-cloud DoS mitigation in one integrated system, the solution is supported on dedicated hardware designed to fight multiple attack vectors simultaneously.

To mitigate network attacks that threaten to saturate the Internet pipe, Radware's attack mitigation solution includes a cloud based DDoS scrubbing service that works in sync with on premise attack mitigation devices.

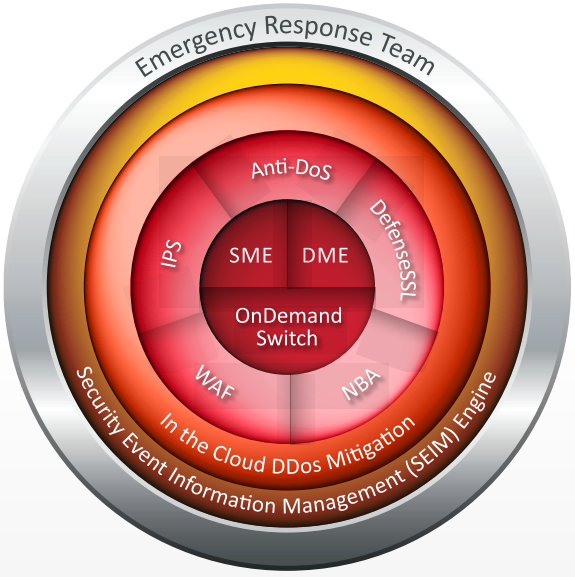

Figure 1: Radware's Attack Mitigation System

Enhanced with a central monitoring and reporting system, the solution provides on-going unified situational awareness of the network and applications using a single security event information management (SEIM) engine for all components.

During long lasting attack campaigns where the system cannot mitigate all attack vectors out of the box – Radware provides the support of its Emergency Response Team – a team of security experts that provide 24x7 real-time security service to help customers restore operational status under attack.

Always-On DDoS Protection with Optimal Attack Mitigation

Radware's on-premise attack mitigation device ensures the datacenter is constantly 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.

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 where attack traffic is cleared before it reaches the company's Internet pipe. This enables a smooth transition between mitigation options assuring immediate protection with no disruption gaps and without adding the scrubbing center latency.

Only 15% of DDoS attacks handled by Radware's ERT saturated the Internet pipe[1]. 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.

⚠ Attack Vectors

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

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

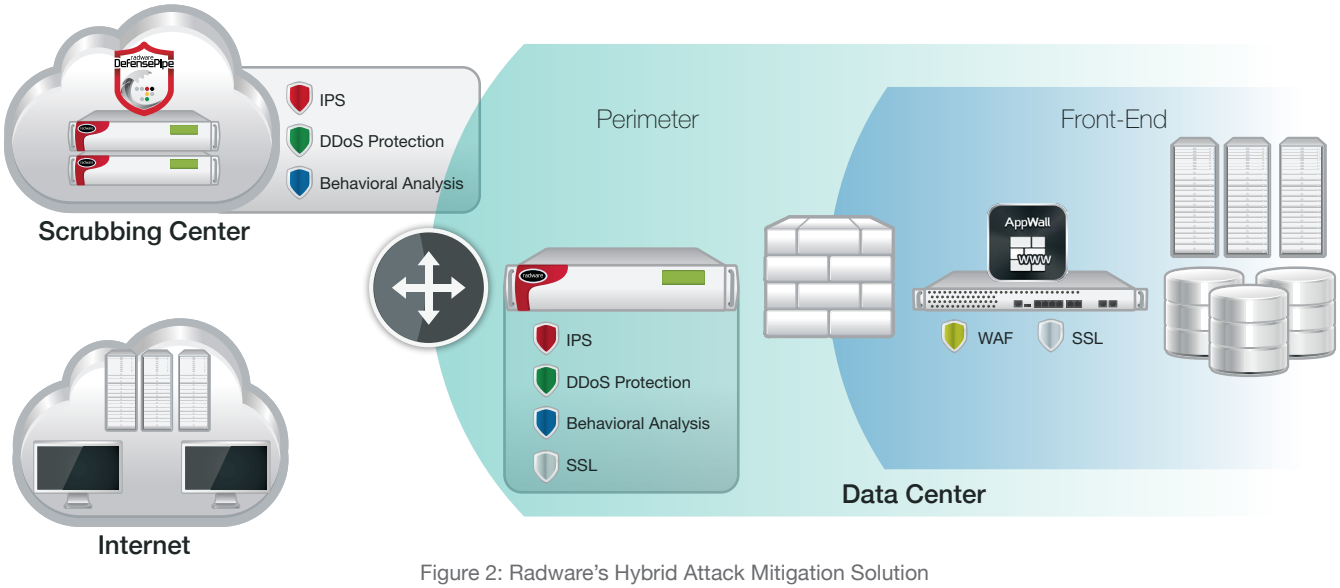

Figure 2: Radware's Hybrid Attack Mitigation Solution

Monitor. Analyze. Report.

Radware's attack mitigation solution includes active monitoring and health checks on the protected service or application. In addition, the system performs pipe saturation monitoring and customers are notified when there is a risk for saturation and action is required.

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. 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 solution 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 the most widely known attacks in the industry provides best practice approaches to fight each and every attack.

[1] Radware's Emergency Response Team (ERT).

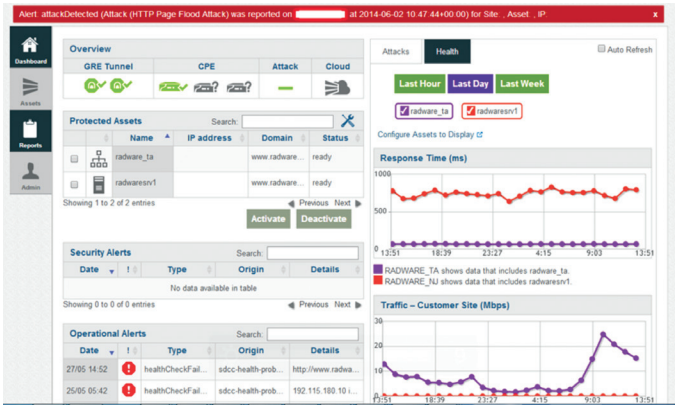

Figure 3: Portal Dashboard

"Radware's attack mitigation solution mitigates both known and new forms of attacks while allowing legitimate business traffic to be handled as normal, so the business continuity of our hosted cloud customers is preserved even while under attack."

Nathaniel Kemberling, CTO, Brinkster

"Radware's attack mitigation solution fits perfectly within our secure cloud hosting architecture. The ability to stop a variety of multi-level attacks at the edge of our networks in North America and Europe empowers FireHost to provide the best protection in the industry."

Chris Drake, Chief Executive Officer, FireHost

Web Applications – Detect. Signal. Block.

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 and needs to be blocked at the perimeter, protecting the rest of the network.

Mitigating the SSL Threat

Radware's SSL mitigation solution is unique in the industry. It mitigates SSL encrypted flood attacks at the network perimeter. The solution mitigates SSL-based attacks using challenge-response mitigation techniques and 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.

Benefits

- Hybrid solution with widest security coverage and shortest time to mitigation – immediate mitigation on-premise and traffic diversion only upon pipe saturation
- Single point of contact – ERT fights the attack during the entire campaign, no other vendors involved
- Integrated reporting system including on-premises and cloud-based mitigation reports
- Available as a fully-managed service with flexible payment models (CAPEX or OPEX-based subscription)

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.

Radware encourages you to join our community and follow us on Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube and the Radware Connect app for iPhone®.

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.

PRD-AMS-BR-03-2015/03 - US