Smart Network. **Smart** Business.

radware

Attack Mitigation System

Attack Mitigation System

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

Emerging Network Threats Require Multiple Protection Tools to Secure Your Business

Data center and network security managers face an increasing threat landscape including network downtime, application downtime, application vulnerability, information theft, authentication defeat, malware spread, web application attacks and web defacement.

Recent attacks show that attackers are using new techniques known as multi vulnerability attack campaigns. During this the attackers set the Botnet (or instruct their fans, as in the case of Anonymous group operations) to launch several attack types in parallel, targeting multiple vulnerability points of the victim's IT infrastructure such as the network, servers and the application layers. Multi-vulnerability attack campaigns are highly destructive even though each attack vector is well known (examples are: UDP flood targeting the network bandwidth resources; SYN flood targeting the server resources; HTTP Get flood targeting the web application resources). The victim is at high risk as even if one attack vector hits the target - the result is destructive. The attackers' assumption is that even if their victims deploy multiple protections tools, there are blind spots in their perimeter network security architecture and therefore is exposed to a few of the attack vectors.

Additionally, zero-minute malware spread attacks; Trojan installs and botnet based attacks are not prevented by standard network and application security deployments.

In order to combat the increasing threat landscape, security managers are required to deploy multiple detection and protection tools including: Intrusion Prevention Systems (IPS), DoS Protection, Network Behavioral Analysis (NBA), IP reputation tools and Web Application Firewall (WAF).

Attack Mitigation System: Protect Your Application Infrastructure Against Known and Emerging Network & Application Threats in Real Time

Protecting the application infrastructure requires deployment of multiple prevention tools. Radware's Attack Mitigation System (AMS) is a real-time network and application attack mitigation solution that protects the application infrastructure against network & application downtime, application vulnerability exploitation, malware spread, information theft, web service attacks and web defacement.

Radware's Attack Mitigation System contains three layers:

- Protections layer – a set of security modules including: **Denial-of-service (DoS) protection, Network Behavioral Analysis (NBA), Intrusion Prevention System (IPS), Reputation Engine and Web Application Firewall (WAF)** - to fully safeguard networks, servers and applications against known and emerging network security threats
- Security risk management - built-in **Security Event Information Management (SEIM)** collecting and analyzing events from all modules to provide enterprise-view situational awareness
- **Emergency Response Team (ERT)** consisting of knowledgeable and specialized security experts who provide 24x7 instantaneous services for customers facing a denial-of-service (DoS) attack in order to restore network and service operational status

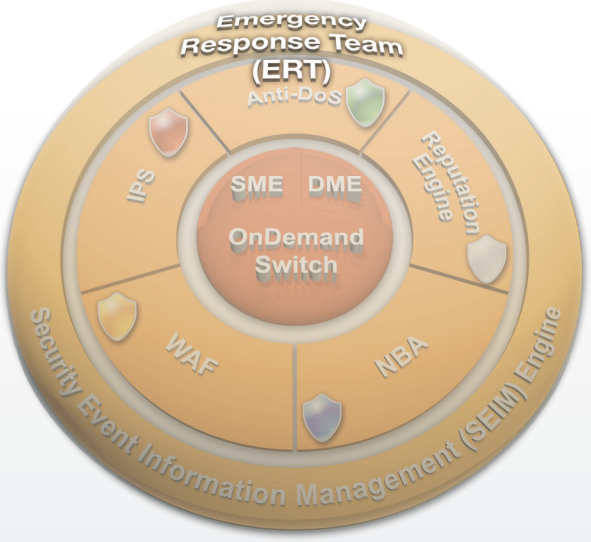

Figure 1 – AMS offers the complete set of protection modules and services for online businesses and data center protection

The synergy of multiple protection modules at part of one system enables more effective protection against attackers who seek to compromise the business assets systematically when compared to stand alone solutions deployment, while providing unified reporting and compliance.

Built-in Security Event Information Management (SEIM) Providing Real-Time Identification, Prioritization and Response to Cyber Attacks

Built-in Security Event Information Management (SEIM) system provides an enterprise-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 drill into information to speed incident identification and provide root cause analysis, improving collaboration between NOC and SOC teams, and accelerating the resolution of security incidents.

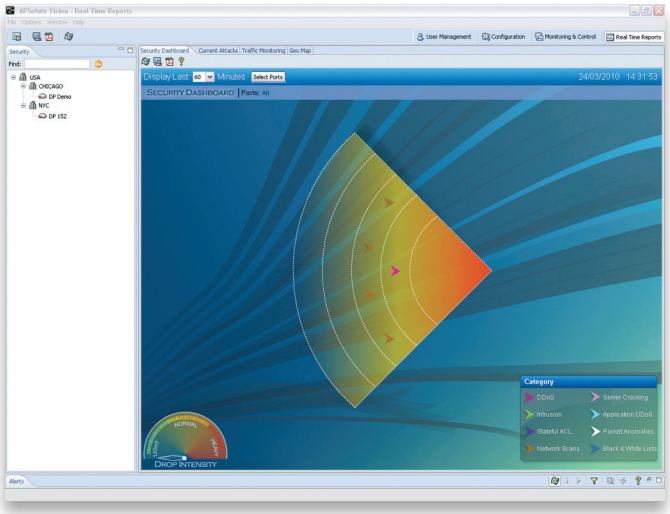

Figure 2 - The real time sonar view allows you to see current attacks in your network. High risk attacks are located closer to the sonar transmitter. The side meter indicates the drop intensity of attack traffic.

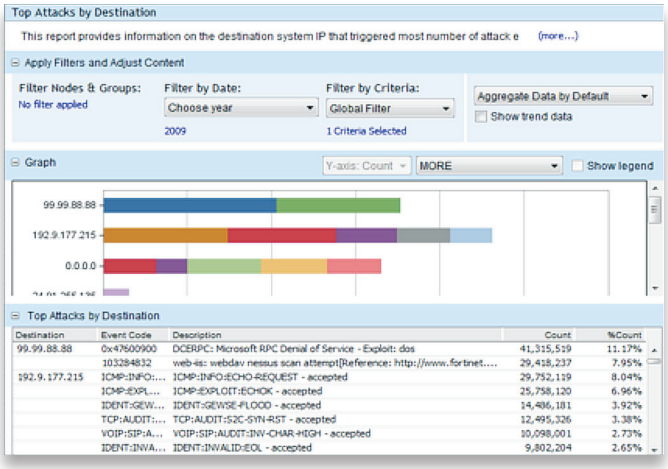

Figure 3 – example of Top Attacks Report based on correlation of events collected from multiple sources

Business Value

Maintain business Continuity of Operations (COOP) even when under attack

- Full protection of data center and on-line business applications against known and emerging network threats
- Maintain excellent user response time even when under volumetric attacks
- Emergency response team (ERT) to assist customers under high risk attacks

Reduces OpEx of security management

- Business centric security situational awareness with Radware integrated SEM – reducing complexity and increasing security assurance
- Integrated security solution – avoiding blind spots and huge saving on tools integration

Reduces CapEx of security tools

- Multiple security tools in a single, integrated solution

Radware AMS is based on the following Radware products:

DefensePro
Network & Server Attack Prevention Device

AppWall
Web Application Firewall (WAF)

APSolute Vision
Management and Security Reporting & Compliance

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.

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.