



Radware Attack Mitigation Solution (AMS)

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

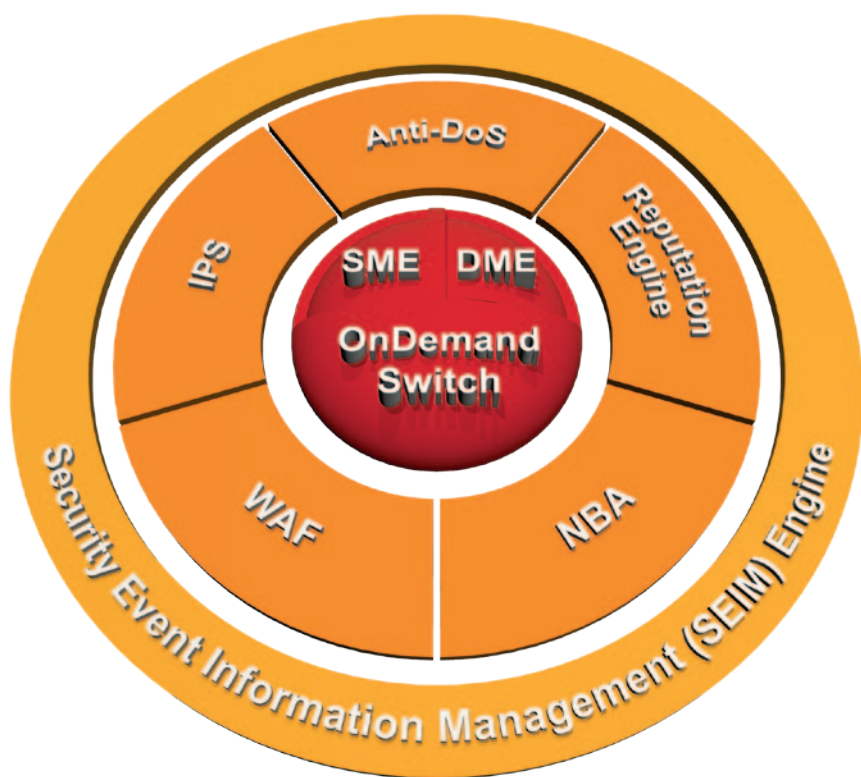


Table of Contents

Abstract.....	3
Understanding Online Business Security Threats	3
Radware Attack Mitigation System.....	6
AMS Product Portfolio	9
Summary: the Radware Business Advantage	9

Abstract

This paper reviews the changing threat landscape and how it impacts online businesses that use Internet access to generate revenue or support their productivity. It maps the required security modules to fight emerging attack campaigns, and then introduces Radware Attack Mitigation System – the AMS. Along with the AMS introduction, a more detailed description of the AMS building block is provided.

Understanding Online Business Security Threats

Introduction

Today, online businesses and data centers face multiple types of attacks that hit every layer of the IT infrastructure:

- The **network layer** is targeted with volumetric network flood attacks, network scans, and network intrusions, aiming to consume or misuse networking resources.
- The **server layer** is targeted by port scans, SYN flood attacks, and low & slow DoS attack tools, which aim to misuse the server resources.
- The **application layer** is targeted with a wide variety of attacks from application vulnerability exploitations, application misuse attacks and application DDoS attacks, and web application attacks.

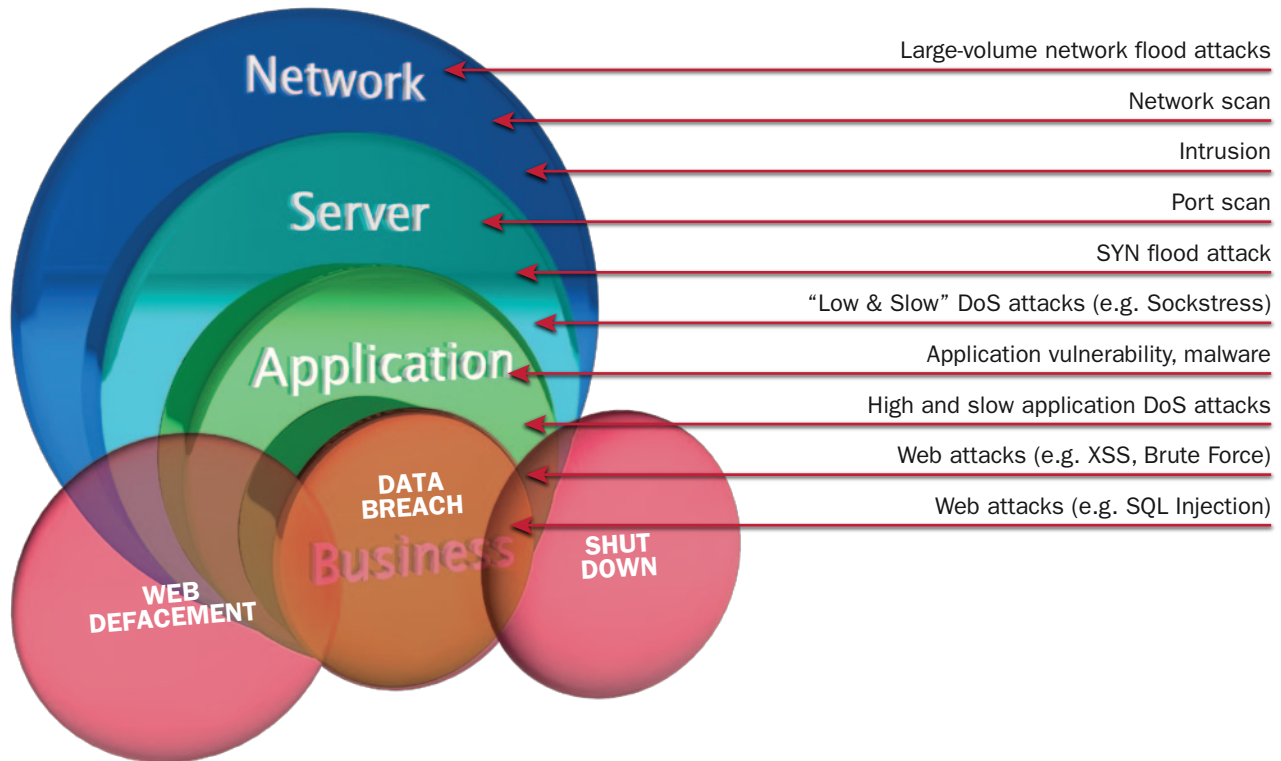


Figure 1 – Attackers target every layer of the IT infrastructure

The result of such attacks can vary from data breach and web defacement, all the way to service shut down.

Cyber-hacktivism Spikes

2010 and 2011 were record years for the most active periods of cyber-hacktivism in the history of cyber threats. Moreover, given the current efficacy of hacktivists attacks, such as WikiLeaks revenge attacks (December 2010), South Korea DDoS attacks (March 2011), Operation Megaupload (January 2012), which include a new concept of attacks we define as a multi-vulnerability attack campaign, we believe this will only serve to encourage even more actors to enter the picture, and spawn a vicious cycle of future malicious activity.

Reassessing the Risk of Cyber Attacks

No one can say for certain how all of this will play out, however given the increased frequency, directed attacks, and effectiveness of the techniques, we can safely assume the following:

- **Cyber attacks go mainstream for activists and for financially motivated criminal organizations.** Attackers' motivation has evolved from publicity and vandalism. They are now looking for financial gain or protest without going out of their homes.
- **Reassessing the risk** – your organization is likely a target. For example, eCommerce sites, which were the prime target for financially motivated attackers, become now also targets for hacktivism.
- **Cyber weapons of mass disruption deploy multi-vulnerability DoS & DDoS attacks.** This turns traditional network security measures useless, as they typically can detect and defend only some of the attack vectors.
- **The need for complementing security technologies.** Mitigating multi-vulnerability and multi-vector attacks requires more than one security technology in place. It is critical to add behavioral analysis technologies on top traditional signature detection and rate-based protection.
- **Architecting the perimeter for attack mitigation.** Deployment of complementing network security technology requires rethinking of perimeter security.
- **Counterattacks are needed!** Defense mitigation strategies are also evolving and now include active counterattack strategies.

Attackers Deploy Multi-vulnerability Attack Campaigns and Raise the Mitigation Bar

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 the 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 because if one attack vector hits the target, the result is destructive. The attackers' assumption is that even if their victims deploy multiple protection tools, there are blind spots in their perimeter network security architecture and therefore are exposed to a few of the attack vectors.

Radware believes that there is a clear need to complement existing network security technologies, such as firewalls and network IPS, in order to protect businesses against existing and future attacks.

Mapping Security Protection Tools

Going back to the threat landscape, we can now better understand and map the required protection tools to fully safeguard an online business or data center. To fully protect against all type of attacks that target the IT infrastructure, you need:

- DoS protection to fend off volumetric network DDoS flood attacks.
- Network Behavioral Analysis (NBA) to detect and prevent zero-day and non-vulnerability based attacks, where the attackers are replicating real user’s behavior to misuse application resources.
- Intrusion Prevention System (IPS) to detect and protect against known application vulnerability exploits.
- IP reputation to prevent financial fraud attacks, social attacks such as phishing, and malware contamination.
- Web Application Firewall (WAF) to protect against web application attacks.

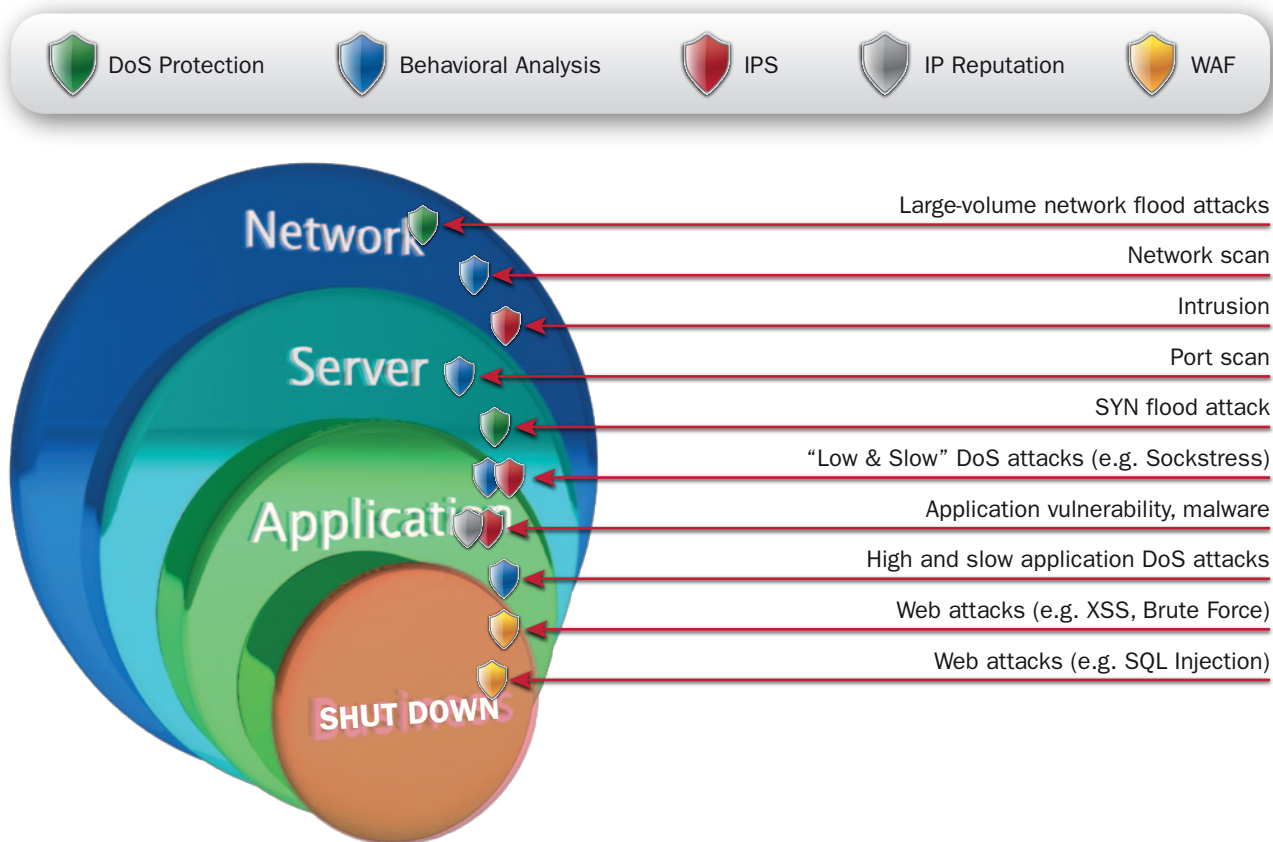


Figure 2 – Mapping security protection tools according to the threat landscape

An integrated approach is required to make sure there are no blind spots in perimeter and application security, and to save on deployment, management, and integration costs.

Radware Attack Mitigation System

Introduction

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 and 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) collects and analyzes 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.

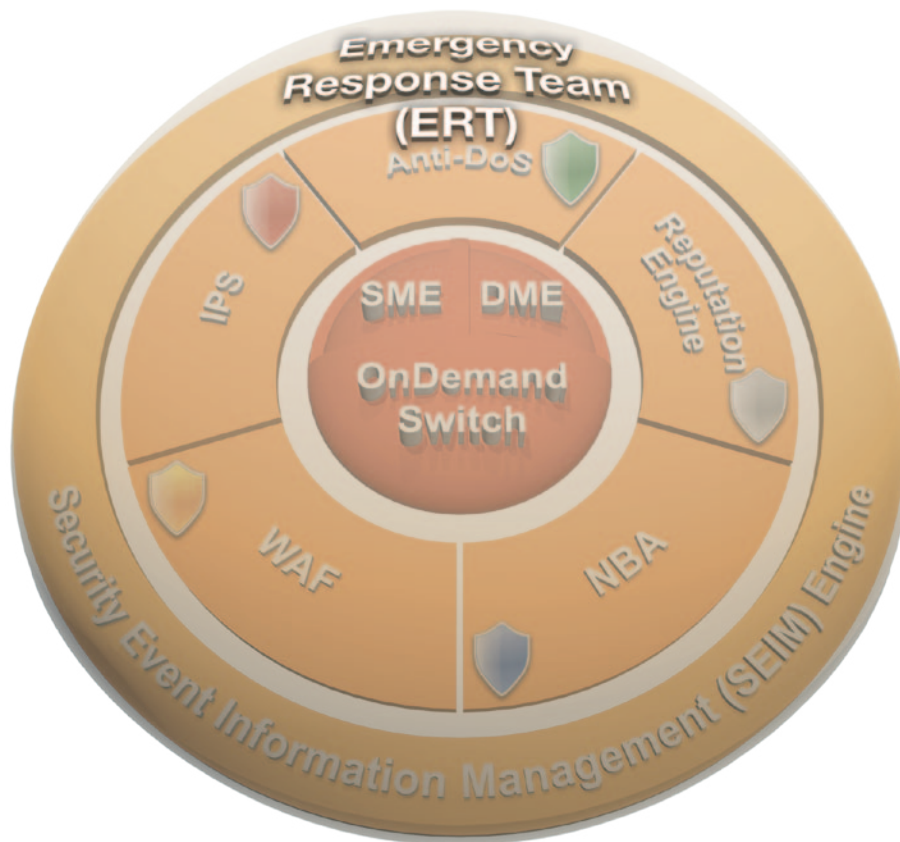


Figure 3 – AMS offers the complete set of protection modules and services for online businesses and data center protection

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

AMS Protection Modules

AMS is comprised of five protection modules, all optimized for online business and data centre protection, and designed for data center and carrier deployments:

DoS Protection – Prevent all type 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
-

Reputation Engine – Protects against financial fraud, Trojan & phishing attack campaigns. This feature is based on third party real-time IP reputation feeds.

WAF – The web application firewall prevents all types of web server attacks, such as:

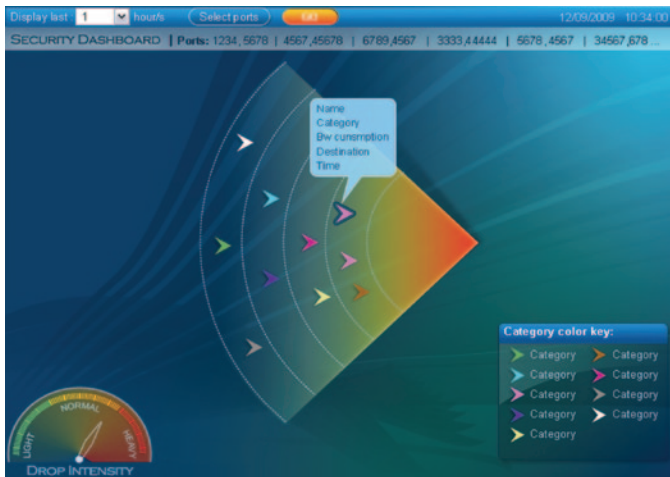
- Cross site scripting (XSS)
- SQL injection
- Web application vulnerabilities
- Cross site request forgery (CSRF)
- Cross site request forgery (CSRF)
- Cookie poisoning, session hijacking, brute force

Cutting-edge Security Technologies

Radware AMS uses multiple technologies to provide complete attack protection for online businesses, data centers, and networks:

- The **DoS Protection** module is based on several technologies: signature detection, behavioral based real-time signatures, and SYN cookies mechanism that challenge new connections prior to establishing a new session with the servers.
- The **Network Behavioral Analysis (NBA)** module 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. In case of DDoS attacks, it injects the real-time signature into the DME hardware, offloading the main CPUs from the excessive unwanted traffic.

- The **Intrusion Prevention System (IPS)** module is based on stateful static signature detection technology, with periodic signature updates and emergency updates, in case of a newly discovered high risk attacks.
- The **Reputation Engine** offers real-time anti-Trojan and anti-phishing service, targeted to fight against financial fraud, information theft, and malware spread.
- The **Web Application Firewall (WAF)** offers patent-protected technology to create and maintain security policies for the widest security coverage with the lowest false positives and the lowest operational effort. The WAF auto policy generation module analyzes the security related attributes of the protected web application and derives the potential threats in the application. The web application is mapped into application zones, each with its own common potential threats. It then generates granular protection rules per zone, and sets a policy-in-blocking mode once it has completed an optimization process that minimizes false-positives while maintaining best security coverage.



Security Risk Management

Best-of-breed Reporting and Forensics Engine

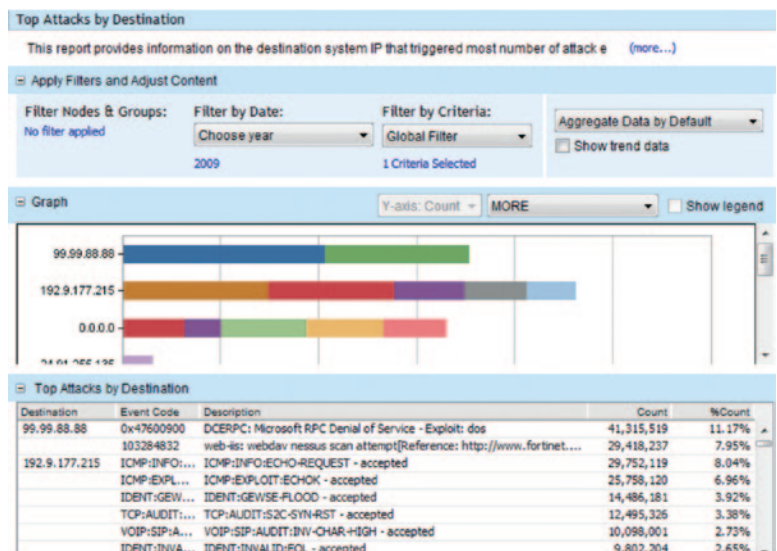
Built-in Security Information Event Management (SIEM) system provides an enterprise-wide view of security and compliance status from a single console. Data from multiple sources is collected and evaluated in a consolidated view of dashboards and reports. These views provide extensive, yet simple, drilldown capabilities that allow users to easily drill into information to speed incident identification, and provide root cause analysis, which improves collaboration between NOC and SOC teams, and accelerates the resolution of security incidents.

Complete Alignment with Enterprise Compliance Requirements and Regulations

The SIEM provides complete alignment with the enterprise’s compliance, regulations, and business processes, providing compliance and audit professionals with a complete picture of compliance across the enterprise. It ensures the appropriate separation of duties, collection of information, configuration, and operation auditing mandated by business processes, regulations, and information security standards (PCI-DSS, SOX, HIPAA, etc).

Full Alert Lifecycle Management

The SIEM provides IT managers with a rich set of tools to manage all the alerts (availability, performance, security, and more), within their infrastructure. Alerts are managed from the moment they surface (identification stage), through ticket opening, analysis, resolution, and verification until the problem is resolved and summarized.



Emergency Response Team (ERT)

Radware AMS delivers the best attack coverage in the industry for online businesses and data centers. We deliver the widest out-of-the-box protection set.

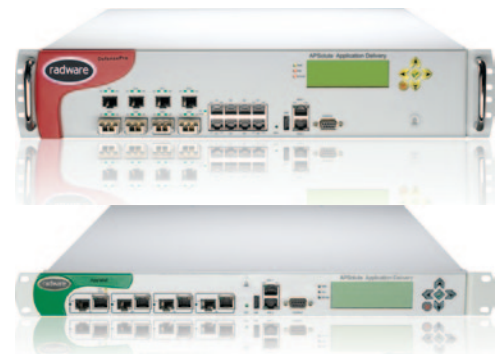
Yet, as attackers are getting more sophisticated by the day, there is a chance that they will launch a new form or type of attack for which the AMS may not be triggered out-of-the-box. For those cases, which are not frequent, the user is required to perform the analysis of the attack traffic and configure protection rules manually.

On the other hand, not all users have the skills or the experience in applying security rules in real-time when under attack. That's why we established Radware's Emergency Response Team (ERT) to provide customers with 24x7, security expert services for hands-on attack mitigation assistance to help successfully defend their network against cyber attacks.

AMS Product Portfolio

The Radware AMS is based upon the following product portfolio:

- **DefensePro**
Delivers anti-DoS, NBA, IPS, and Rep. Engine protection modules.
- **AppWall**
Radware Web Application Firewall (WAF).
- **APsolute Vision**
Radware Management solution that includes the advanced Security Information Event Management (SIEM) for security reporting, forensics, alerting, and compliance management.



Summary: the Radware Business Advantage

Cyber activists and financially motivated attackers are getting sophisticated. They deploy multi-vulnerability attack campaigns making mitigation nearly impossible. No single tool or solution is effective against the broad range of attacks that target every layer of the IT infrastructure – the network layer, the servers layer, and the applications layer.

With the Radware Attack Mitigation System, online businesses, data centers, and service providers can assure their online presence and maintain productivity thanks to the following solution benefits:

- Radware AMS is the only solution that can truly defend against emerging cyber attack campaigns that target all IT infrastructure layers.
- The Emergency Response Team (ERT) offers rapid assistance to customers under attack, and ensures their business is up at all times.
- AMS offers the lowest cost OpEx and CapEx solution in the industry.

© 2012 Radware, Ltd. All Rights Reserved. Radware and all other Radware product and service names are registered trademarks of Radware in the U.S. and other countries. All other trademarks and names are the property of their respective owners.