radware

Smart Network. **Smart** Business.

Mitigating the DoS/DDoS Threat

Why You Need On-Premises Security Solution in Conjunction with Anti-DoS Managed Service - Whitepaper

Table of Contents

Abstract....3

DDoS is Growing and Evolving....3

DDoS Layers of Attack: the Protection Challenges....5

The Radware Approach to Fight the DDoS Threat....7

Summary....9

Abstract

In the era of fast-growing cyber-hacktivism where DDoS attacks are the preferred weapon of mass disruption, a closer look is required for emerging attack campaigns.

Attackers are getting sophisticated. There are frequent DDoS attack campaigns that disembark directly at the victims' IT infrastructure, bypassing managed DDoS protection services.

This paper highlights recent DDoS attacks trends and why they are successful; it then shows why relying on managed DDoS protection services provides a partial solution against the DDoS threat. This paper also introduces Radware DDoS protection solution and establishes the need for an on-premises security solution in addition to the managed DDoS service.

DDoS is Growing and Evolving

Introduction

Cyber-hacktivism has become so prevalent that every online business, financial service, government agency, or critical infrastructure is likely a target. Financially motivated attackers are still a threat, however their activity is not on the news since just recently, they have received much less publicity.

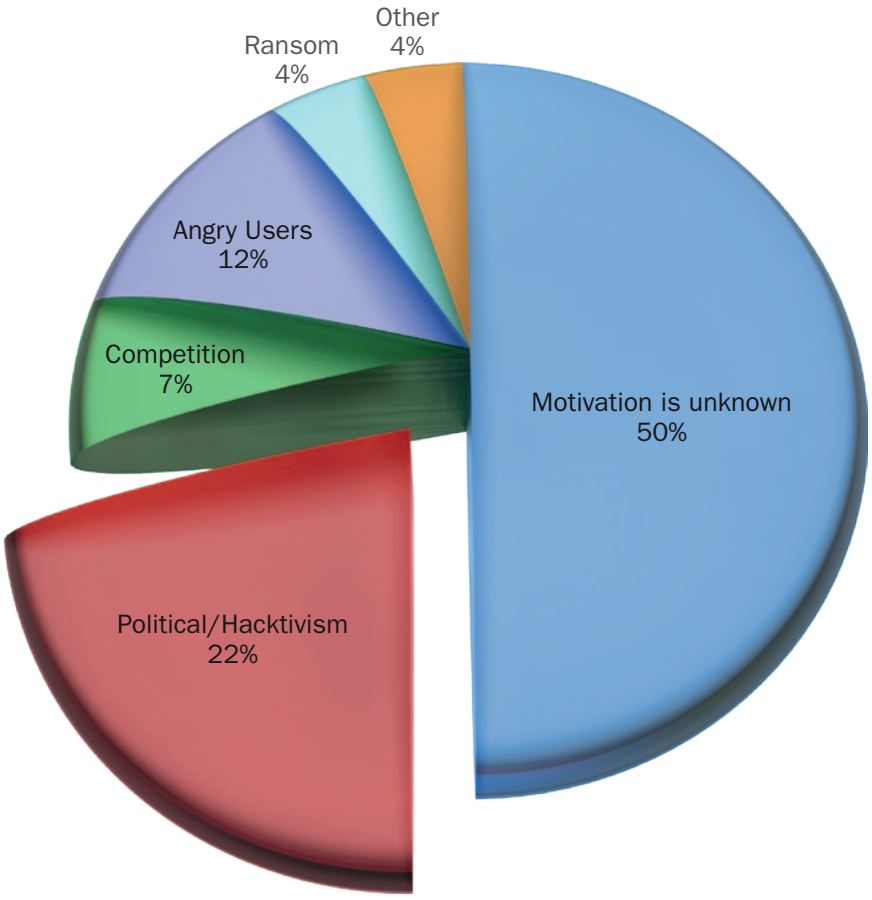

Figure 1: Radware Security Survey 2011: While the "unknown motivation" is still prominent the most prominent motivation is by far political hacktivism

Cyber attacks have become the weapon of choice for hacktivists seeking to leverage the impact of conflicts and social protests. Recent examples are the Anonymous group joining the Occupy Wall Street protesters to launch cyber attacks on major financial institutions in New York, attacking Sony®,, and other companies affiliated with the copyright industry for revenge as part of Operation Mega-upload. In addition, the Nightmare group works with the hacker "0xOmar" to escalate their cyber war against Israel,

Attackers are getting sophisticated

An analysis of cyber attacks throughout 2011-2012 by Radware's Emergency Response Team (ERT), notes that companies that relied only on a 'one-size-fits-all' in-the-cloud managed security, or on-premise security solutions alone, could not withstand the coordinated attack campaigns. The Radware ERT review of the attack traffic from multiple reported cases shows that:

- Attackers are deploying multi-vulnerability attack campaigns, targeting all layers of the victim's IT infrastructure. This includes the network, servers, and application layers.
- Attackers who previously used distributed denial of service (DDoS) attack tools that focused on networks have now developed new DDoS tools focusing on applications.
- Attackers are using "low & slow" attack techniques that misuse the application resource rather than resources in the network stacks.
- Attackers are using evasion techniques to avoid detection and mitigation including SSL based attacks, changing the page request in a HTTP page flood attacks and more.

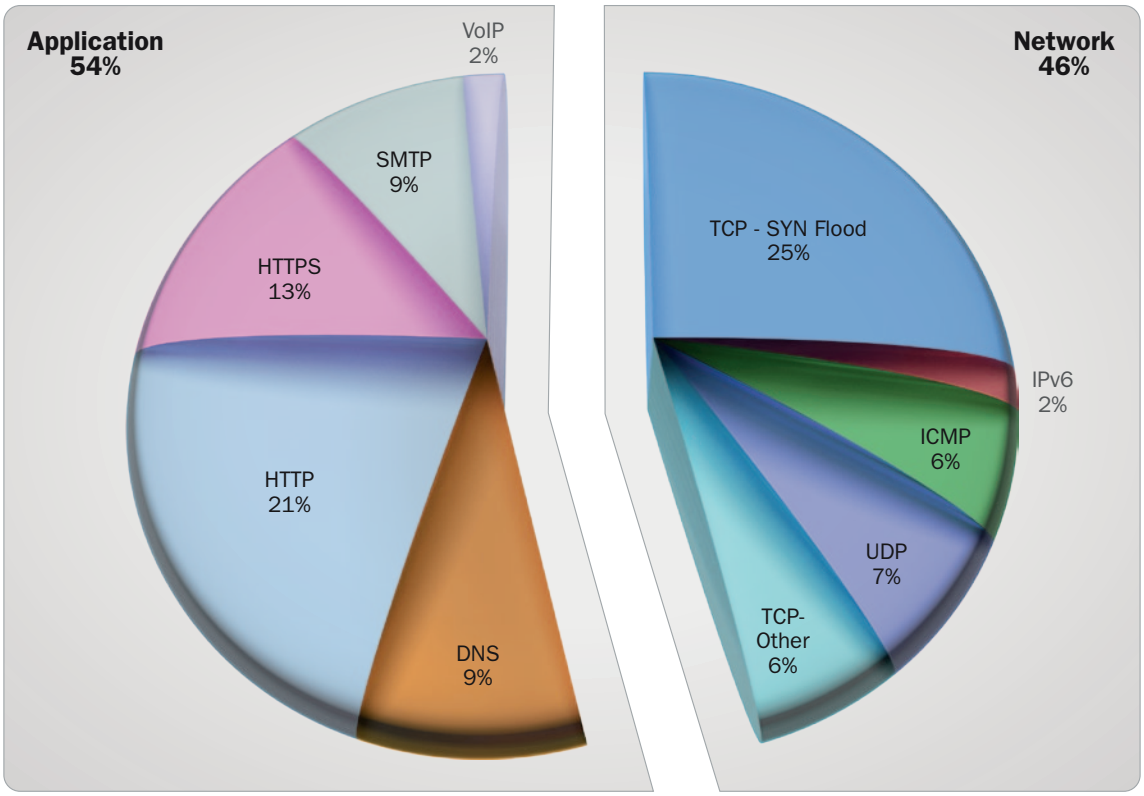

Figure 2: Radware Security Survey 2011: Attack count by type and bandwidth

As a result, small to medium online businesses, financial services, data centers, and enterprises find themselves with limited capabilities and knowledge to fight against emerging network security threats. While the common practice of organizations is relying on DDoS protection from their service provider, the recent wave of attacks in 2012 shows that attackers are getting sophisticated and manage to bypass the service provider and hit businesses directly. This aises the need to build secured network architecture that combines in-the-cloud DDoS protection and on-premise DDoS protection.

DDoS Layers of Attack: the Protection Challenges

DDoS Layers of Attack

From the point of view of a service provider, DDoS attacks can be partitioned into four dimensions as shown in Figure 3:

- **Volumetric bandwidth flood attack** – Attackers flood the victim with a high volume of packets, consuming networking equipment resources or bandwidth resources. These are network DDoS flood attacks such as SYN flood attacks (high packet-per-second attacks), large UDP packet floods (bandwidth attacks), ICMP floods, and more.

- **Application DDoS flood attacks** – These attacks generate complete sessions and target the application resources. Examples are HTTP Get or Post flood attacks, or DNS flood attacks.

- **SSL based attacks** – Encrypted SSL DoS and DDoS attacks consume more CPU resources during the encryption and decryption of the content than processing of a clear text. As a result, encrypted application DoS & DDoS attacks amplify the impact, even at relatively low rates of requests per second.

- **Low & slow DoS attacks** – Low & slow application DDoS attacks exploit application implementation weaknesses and design flaws. Examples are Slowloris, a tool that allows a single machine to take down another machine's web server with minimal bandwidth, and Circle cache-control (Circle-CC), which floods a website by scanning the site across multiple pages systematically.

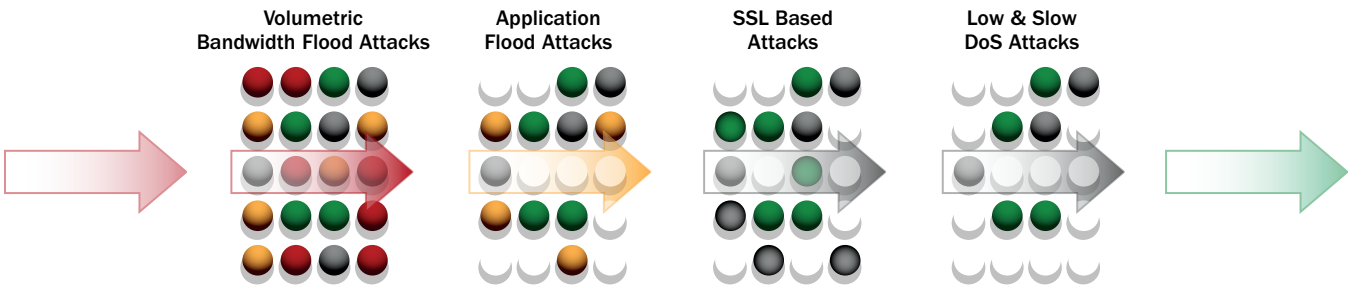

Figure 3: DDoS layers of attacks, from high volume to low volume attacks

Where Current Mitigation Solutions Fail

As mentioned in the introduction, online businesses, financial services, data centers, and enterprises find themselves with limited capabilities and knowledge to fight against emerging network security threats. The common practice of organizations is to rely on DDoS protection from their service providers. However, the recent wave of attacks in 2012 shows that the attackers are getting sophisticated and manage to bypass the service provider and hit businesses directly, as shown in Figure 4.

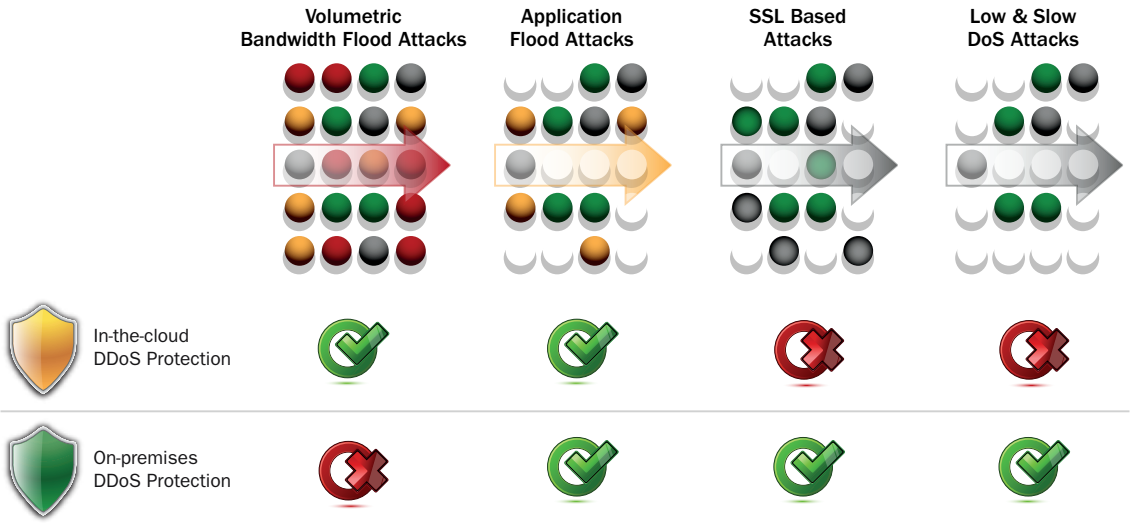

Figure 4: Where current mitigation solutions fail to protect against DDoS attacks

In-the-cloud DDoS protection is effective against the volumetric bandwidth attacks, and some providers also offer protection against application DDoS flood attacks, depending on the equipment they are using for detection and accurate mitigation. However ,the service providers has no visibility into SSL encrypted traffic and cannot block SSL based attacks; furthermore, the low & slow attacks typically will go undetected by the service providers as they are low rate attacks that run under the detection thresholds.

To summarize, in-the-cloud DDoS protections are effective in cleansing a high volume of DDoS flood attacks.

Deploying an on-premises DDoS protection solution provides complete protection against the application DDoS flood attacks, SSL based attacks, and the low & slow attacks. On-premises DDoS protection can detect and mitigate volumetric attacks as well, however the physical location at the business perimeter network rather than the carrier link, offers limited effectiveness: attackers that flood victims with a large volume of traffic achieve Internet link saturation, which renders the on-premises solution useless. Figure 5 shows that 27% of customers participating at the Radware survey reported that their service was denied due to overload of the Internet link.

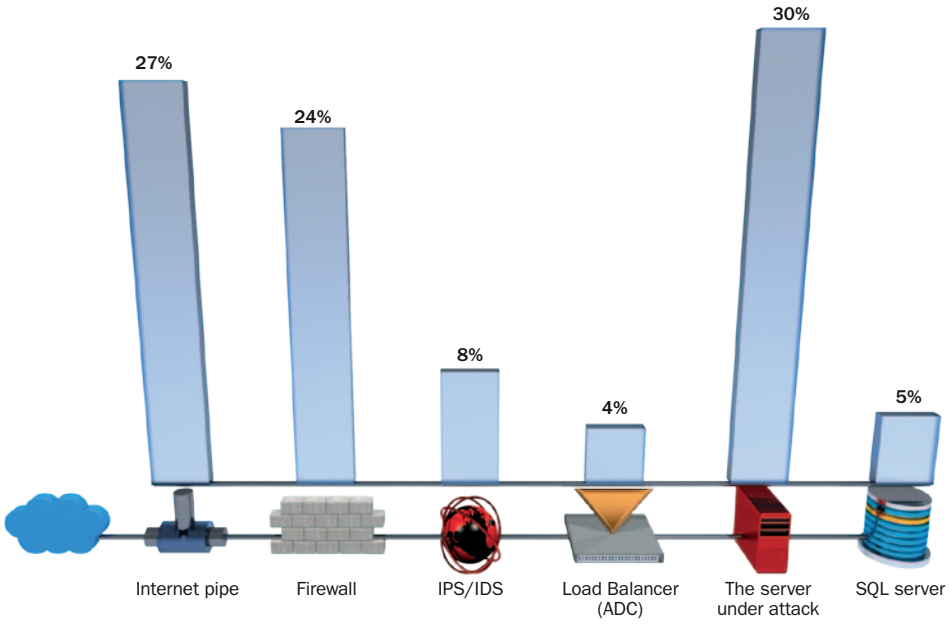

Figure 5: Which services or network elements are (have been the bottleneck) of DoS?

The Radware Approach to Fight the DDoS Threat

Introducing Radware Attack Mitigation System (AMS)

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). These modules 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)** - Consists 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

Fighting the DDoS threat is based on multiple AMS protection modules:

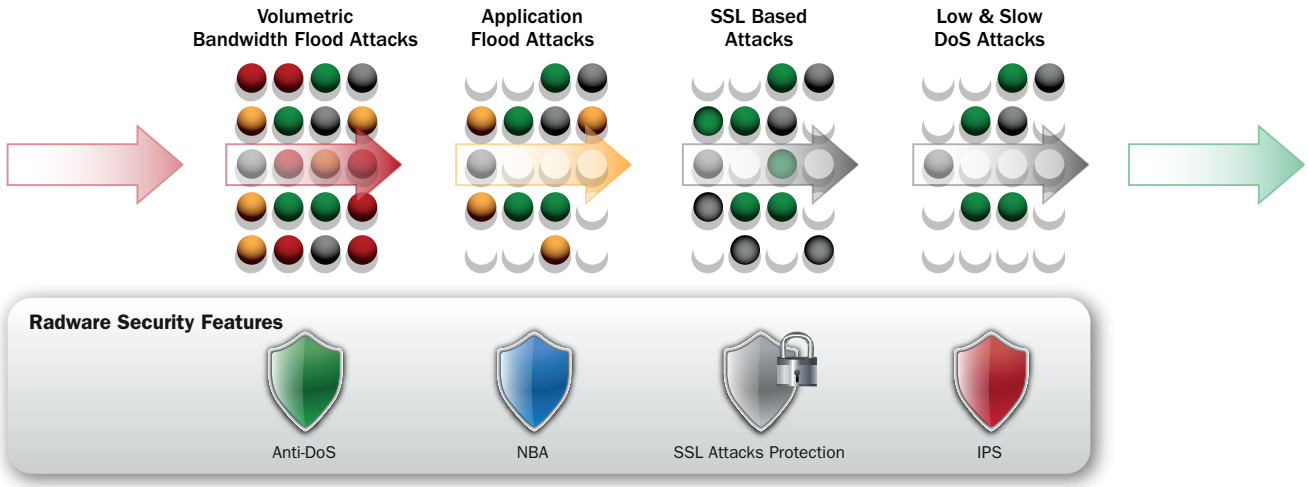

Figure 6: Mapping Radware AMS protection modules according to the DDoS layers of defense

- **Anti-DoS** – This module protects against all types of network flood attacks including UDP floods, SYN floods, TCP floods, ICMP floods, and out-of-state flood attacks.

- **NBA** – The NBA module detects application misuse attacks and protects against HTTP page and post flood attacks, DNS flood attacks, SIP flood attacks, and more.

- **SSL attacks protection** – In conjunction with Radware SSL accelerator, AMS detects and prevents SSL encrypted attacks, including application flood attacks and vulnerability based attacks.

- **IPS** – This module deploys deep packet inspection to detect and mitigate low & slow attack tools such as Slowloris, Sockstress, and others.

End-to-end Mitigation Solution

At this stage, it is clear that an effective mitigation approach against the DDoS threat requires both in-the-cloud protection and on-premises protection. Radware AMS is the best fit in the industry against the DDoS threat and can be deployed in both locations:

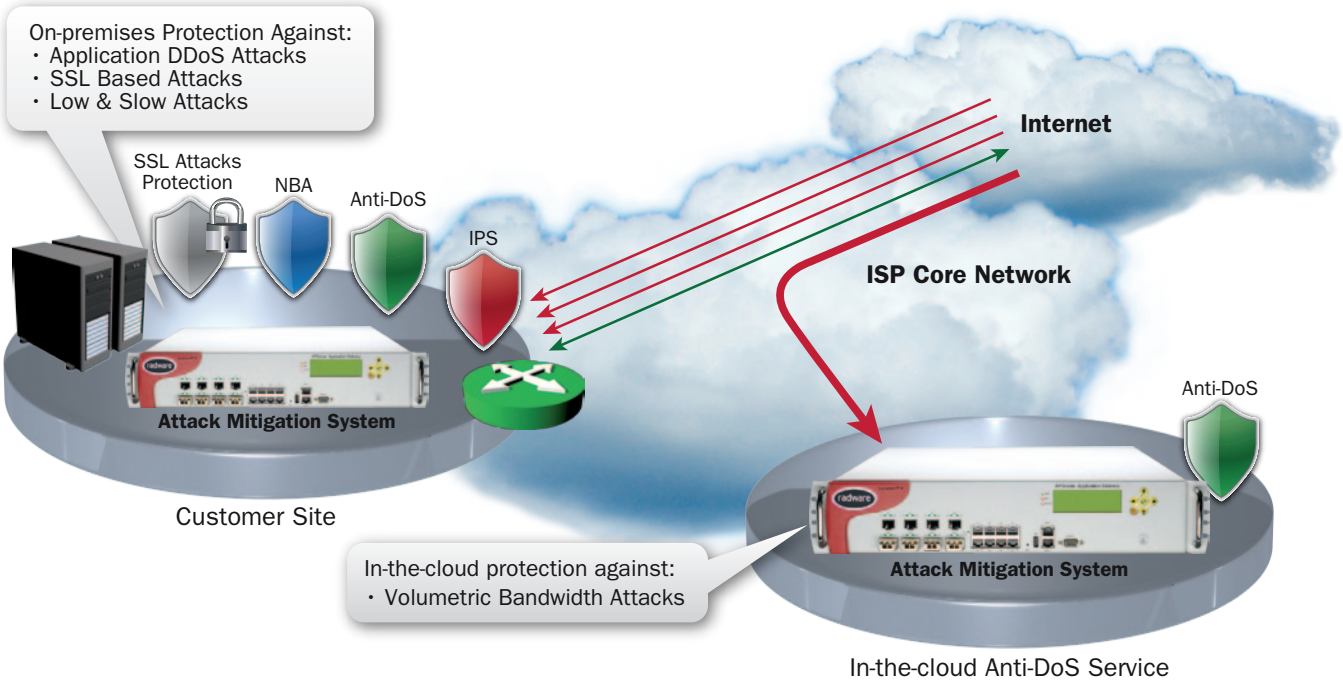

Figure 6: Radware end-to-end mitigation solution fighting the DDoS threat

- **In-the-cloud protection:** AMS is used to remove the volumetric bandwidth attacks to avoid the risk of link saturation. This is the first line of defense against DDoS attacks.

- **On-premises protection:** AMS is deployed at the business perimeter network to fend-off all type of DDoS attacks: the low & slow attacks, SSL based attacks, application flood attacks, and leakage of network flood attacks that managed to go undetected or unprotected in-the-cloud.

Only end-to-end mitigation deployment (in-the cloud AND on-premises protection), enables businesses to fully protect their IT infrastructure against evolving DDoS attacks.

Summary

DDoS attacks are prevalent and no online business or organization can ignore them anymore. Attackers are getting sophisticated and launch multi-vulnerability attack campaigns, which makes detection and mitigation nearly impossible.

Organizations that used to rely on their service provider's DDoS protection service (in-the-cloud), find that the attacks hit their business, bypassing the provider's protection layer.

In recent attack cases, we have seen that businesses that have deployed Radware AMS on premises in conjunction with DDoS protection at the service provider were able to survive and maintain their business operations in spite of large scale, large volume multi-vulnerability attack campaigns. When AMS is deployed on both sides (on premises and at the service provider), they have achieved the best protection.

Radware AMS delivers the following solution benefits:

- Radware AMS is the only solution that can truly protect against all type of DDoS attacks including volumetric DDoS flood attacks, application flood attacks, SSL based attacks, and the low & slow DoS attacks.
- End-to-end deployment of Radware AMS is the best solution to fight the DDoS threat at all layers, mitigating all attack vectors in seconds.
- When deployed on-premises, the online business has full control of its security solution and can be assisted with Radware ERT when attack mitigation expertise is required.
- Make sure your service provider deploys Radware AMS or that the service provider can remove the volumetric attacks with any other solution they deploy.
- AMS offers the lowest cost OpEx and CapEx solution to fight DDoS attacks.