radware

Smart Network. Smart Business.

Attack Mitigation Service

Fully Managed Hybrid (Premise & Cloud) Cyber-Attack Mitigation Solution - Whitepaper

SHARE THIS WHITEPAPER

Table of Contents

Abstract

In an era where cyber-attacks have become main-stream and a permanent tactic in perpetrating cybercrime, social protests and cyber war, organizations need to implement a security solution which can overcome a litany of emerging risks.

Cyber Attack Complexity: Attacks are becoming more sophisticated and increasing in severity as they bypass traditional cloud and CDN protection services to target an organization's IT infrastructure and critical applications. The diagram below from Radware's 2014-2015 Global Application & Network Security Report highlights the varied and tenacious nature of today's attack landscape.

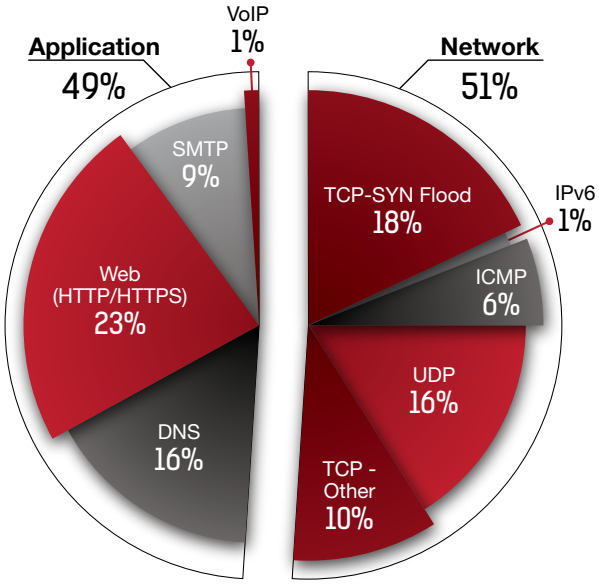

Figure 1: Network vs Application Attacks

Recent Worldwide Regulatory Efforts

Regulatory Pressures: Recently, the world has seen a dramatic rise in the necessary requirements to onboard cyber-attack defenses including six noteworthy efforts:

- Effort #1: National Institute of Standards and Technology's Cyber Security Framework (US)
- Effort #2: Office of the Superintendent of Financial Institutions (OSFI) Memorandum (Canada)
- Effort #3: Federal Financial Institution's Examiner Council (FFIEC) Joint Statement on DDoS Cyber Attacks, Risk Mitigation and Additional Resources (US)
- Effort #4: Securities & Exchange Commission Cyber Exams (US)
- Effort #5: Office of the Comptroller of the Currency (OCC) Guidance (US)
- Effort #6: National Credit Union Administration (NCUA) Risk Alert (US)

Evolving Information Technology (IT) Trends: For the past twenty years technologies have accelerated the fight in information security to thwart a threat landscape that is focused on attacking newly-minted, automated processes that are designed to make businesses more efficient, effective and faster. These technologies were largely based on assumptions in which businesses and customers related to one another. Over the past 36 months these assumptions have dissipated and the following three trends have been the most disruptive to new security models:

- The Great Cloud Migration: Enterprise IT is dissolving
- Internet of Things(IoT): Rise of things communicating with each other
- Software Defined Networking (SDN): Software which shifts the paradigm of routing and networking

Effective & Nimble Security Teams: If there is one permeating, unending lesson learned on how to survive cyber-attacks, it is that modern day security teams need to be agile and crafty in combatting attacks. They need to provide better service and procurement options from partners and technology providers alike.

Although these trends are powerful and warrant individual whitepapers, this paper highlights the most recent technical cyber-attack trends and how these trends are effectively addressed with a fully-managed, mitigation solution from end-to-end. This paper demonstrates how relying solely on cloud or on-premise, distributed denial of service (DDoS)/ cyber-attack mitigation solutions will only provide a partial solution and how modern responses need to leverage automated detection and wise mitigation that is specialized and unique. To further illustrate the superior defense model for these issues, this solution paper introduces Radware's Attack Mitigation Service that is based on a combination of premise-based cyber-attack protection technology and a robust cloud-delivered scrubbing solution.

Introduction

Cyber-attacks have become so rampant that nearly every online business, financial service, government agency, or critical infrastructure is likely a target. There are numerous reasons why cyber-attackers strike, and most organizations will face a dizzying array of attacks.

As cyber-attacks reach a tipping point in terms of quantity, length, complexity and targets, even organizations with by-the-book security programs can be caught off guard.

In the 2014-2015 Global Application & Network Security report Radware surveyed security leaders to understand business concerns related to cyber-attacks. We asked which type of cyber-attack would cause the greatest harm to respondent's organizations. Although DDoS was the most-cited threat type (46%), its lead is narrow. As you can see in the diagram below, all of the threat types are fairly well represented - suggesting that the threat landscape varies depending on each organization's industry and business concerns.

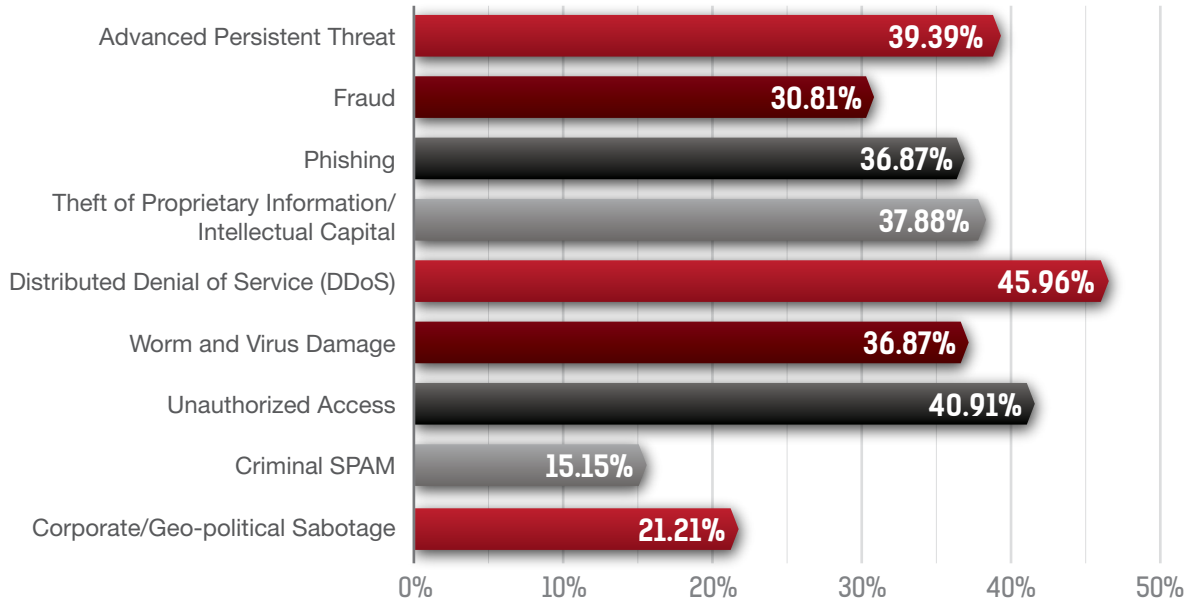

Figure 2: Attacks that will cause most harm to businesses

Attackers Are Getting Sophisticated

- Organizations that rely solely on a 'one-size-fits-all' in-the-cloud managed security or on-premises security solution cannot withstand current coordinated attack campaigns. Attackers are deploying multi-vulnerability attack campaigns that target all layers of the victim's IT infrastructure including networks, servers and application layers.
- Attackers are also patient and persistent - leveraging "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 attack and more.
- In 2014, a number of Radware ERT customers experienced very long attacks with 19% of major attacks reported considered "constant" by the targeted organization. Many have reported week-long and even month-long attacks in previous years - but never more than 6% reported experiencing constant attacks.
- The Internet pipe has been identified as the number-one failure point in 2014 and reflective attacks represent 2014's single largest DDoS "headache".

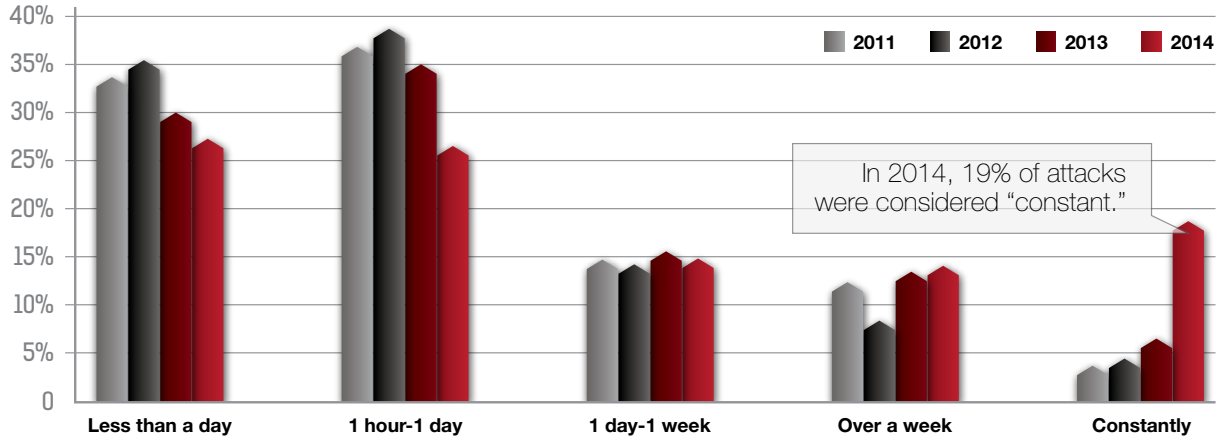

Figure 3: YoY attack durations

Cyber-Attacks: Attacks Come in Vectors / Layers

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 2013 shows that attackers are getting sophisticated and manage to bypass the service provider and hit businesses directly. The following illustrates how the most successful organizations have designed their defenses to effectively repel modern cyber-attacks. The strategies they leveraged require three distinct levels of protection.

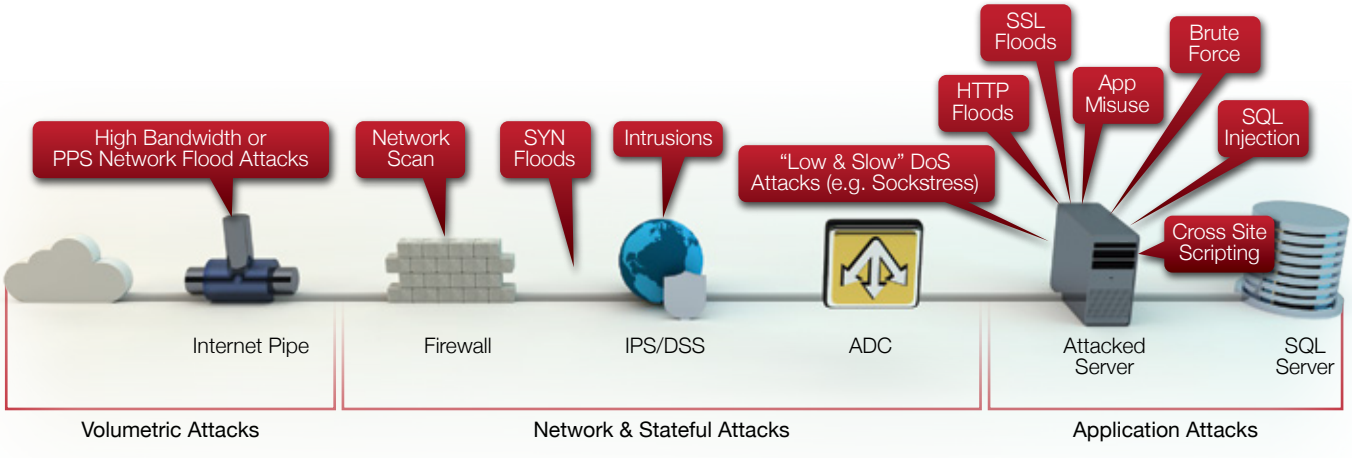

Figure 4: Levels of Protection

First Layer of Defense: The Perimeter Protection

Even though the notion of a "perimeter" is abstract today, the reality is that it exists, even if it's distributed and multi-layered. Given that the perimeter does exist in a distributed and abstract way, the perimeter needs to be protected for threats entering your organization's most valued assets. In this layer there are six categories which need protection. They are illustrated below and highlighted in the following list:

> **Did you know?**
> The perimeter is where, according to a three year trend analysis, 85% of all cyber-attacks focus and only 15% of the attacks are volume-oriented requiring cloud scrubbing solutions.

1. **Envelope Attacks**: Detection and mitigation of attacks aimed at overloading your technology devices and logic themselves (this area is often missed by traditional security inspection tools).
2. **Directed Attacks**: Exploit (e.g., CVE / CVSS) vulnerabilities are a concept well known by modern security teams.
3. **Intrusions**: Typically referred to as hackers who have leveraged an entry technique such as a misconfiguration (e.g., someone left a virtual door open) and are running chaotic in an environment.
4. **Localized volume attacks**: Virtual and multi-tenant technologies aimed at optimizing and gaining efficiency from technology spending has increased the probability to have micro-DDoS attacks – or something called localized volume. This is the concept that one virtual instance or one tenant in a modern day intra-data-center environment (e.g., no external sources) can attack one another with both volume and non-volume attacks.
5. **Low & Slow Attacks**: An attack that is pervasive, but non-volume, however it has the same effect of exhausting resources as volume attacks and the tactic employed for perpetrating the attack stretches attacks over a long period of time.
6. **SSL Floods**: Encrypted SSL DoS and DDoS attacks consume more CPU resources during 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.

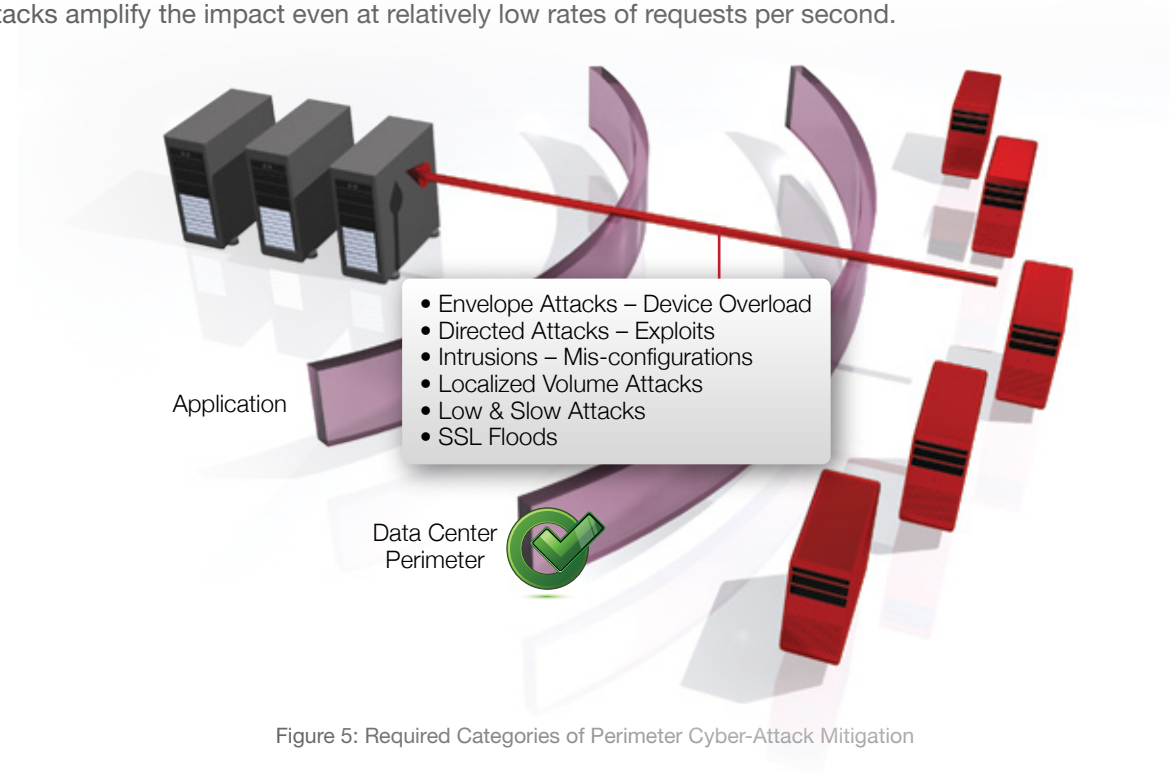

Figure 5: Required Categories of Perimeter Cyber-Attack Mitigation

Six different detection and mitigation models must be operational at all perimeter technologies – whether it is located inside an enterprise or cloud service delivery model.

Second Layer of Defense: Application Layer of Protection

The next layer of defense is defined at the 'transaction-oriented' or application-layer. This layer provides numerous areas of concern and in this layer the complexity of detection and mitigation rises and the need for premise-based technology becomes paramount. There are seven categories which need protection in this layer and are illustrated below and highlighted in the following list:

> **Did you know?**
> The most important part about the protection layer is that none of the following techniques can be comprehensively protected by any perimeter technology.

1. **Web Attacks**: Exploit (e.g., CVE / CVSS) vulnerabilities are a concept well known by modern security teams and are frequently called OWASP-type of attacks for the well-known standard in defining how to secure web applications.
2. **Application Misuse or Business Logic Attacks**: These attacks focus on disabling application code or logic which can lead to misuse and cause adverse effects. Recent examples of such attacks are on application search engine queries or the ability to enter numerous requests into an input field(s).
3. **Application or Connection Floods**: These attacks generate complete sessions and target application resources. Examples are HTTP Get, Post flood attacks, or DNS flood attacks. These floods are most often misunderstood and need to be handled exclusively by cloud scrubbers. However, there are many types which actually require, at a minimum, premise based detection. Examples of these are dynamic HTTP floods with randomized sources.
4. **Brute Force**: Brute force attacks are a category generally not covered by most traditional security tools including firewalls or IPS'. This category has become an Achilles' heel for modern security environments as they seek coverage for a technique that requires behavioral algorithms to determine when someone is authenticating whether or not an attempt is to lock out an account maliciously.
5. **Directory Traversals**: Traversals of directories is a session-oriented attack which allows an attacker to perpetrate availability-based attacks once in an authentic session. This type of an attack evades all perimeter detection technologies and must monitor user behavior inside of a session/transaction.
6. **Injections**: Injections (e.g., SQL, LDAP, XML, JSON, etc.) are a heinous attack type and have risen over the years to represent the second most prevalent type of effective attacks. Like the Traversal-category of attacks, this vector evades perimeter detection and requires intra-session or intra-transaction monitoring nestled close to the targeted application for detection.
7. **Scraping and API Misuse**: A rising attack technique involves web scraping and API misuse which masquerade as 'good bots' conducting 'good information gathering or other duties', however have malicious or unintended consequences. These attacks require great intimacy with the offending application to handle competently.

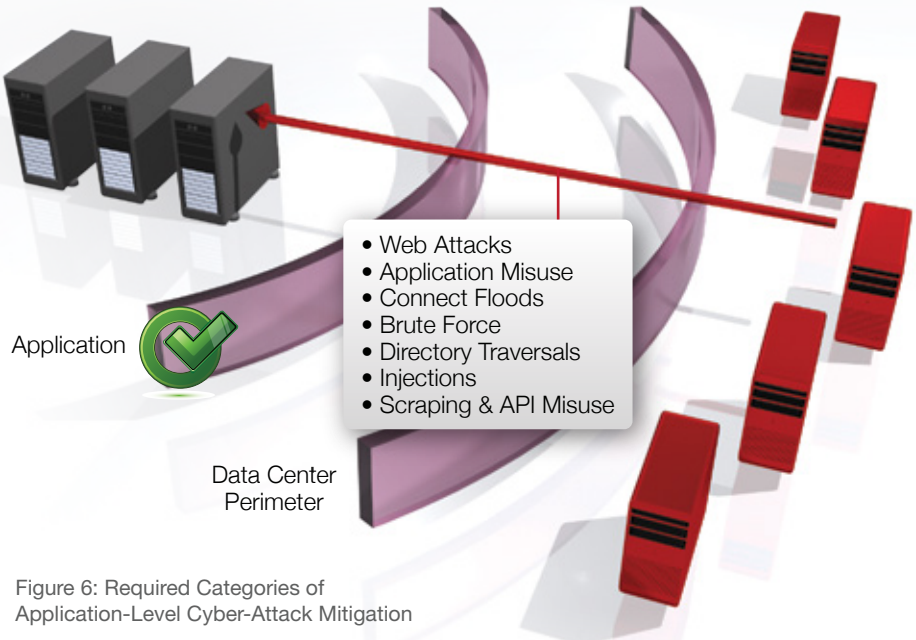

Figure 6: Required Categories of Application-Level Cyber-Attack Mitigation

Seven different detection and mitigation models must be operational at all application-level technologies – whether it is located inside an enterprise or in a cloud service delivery model.

This raises the need to build secured network architecture that combines in-the-cloud DDoS protection and on-premise DDoS protection.

Third Layer of Defense: Volume- Layer of Protection

The next layer of defense is defined at the 'volume threat'. 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 application floods such as HTTP, SIP, SMTP, FTP and more. In this layer there are seven categories which need protection. They are illustrated below and highlighted in the following list:

> Did you know?
> Not only is cloud scrubbing ineffective against all volume based attacks, but it is not the domain of ISPs alone.

1. **SYN Floods**: A form of denial-of-service attack in which an attacker sends a succession of **SYN** requests to a target's system in an attempt to consume enough server resources to make the system unresponsive to legitimate traffic.
2. **Network Volume other than SYN**: Leveraging techniques other than SYN type of techniques, these malicious attacks attempt to make server or network resources unavailable by using architectures or protocols which have an inherent imbalance between a technical request and reply. Examples of these are reflections and amplification attacks most notably on UDP protocols, but also CDN XFF and NTP infamous attacks.
3. **Application Floods (HTTP)**: These attacks generate complete sessions and target the application resources. Examples are HTTP Get, Post flood attacks, or DNS flood attacks. The simple versions of these attacks can be best handled via cloud scrubbers.

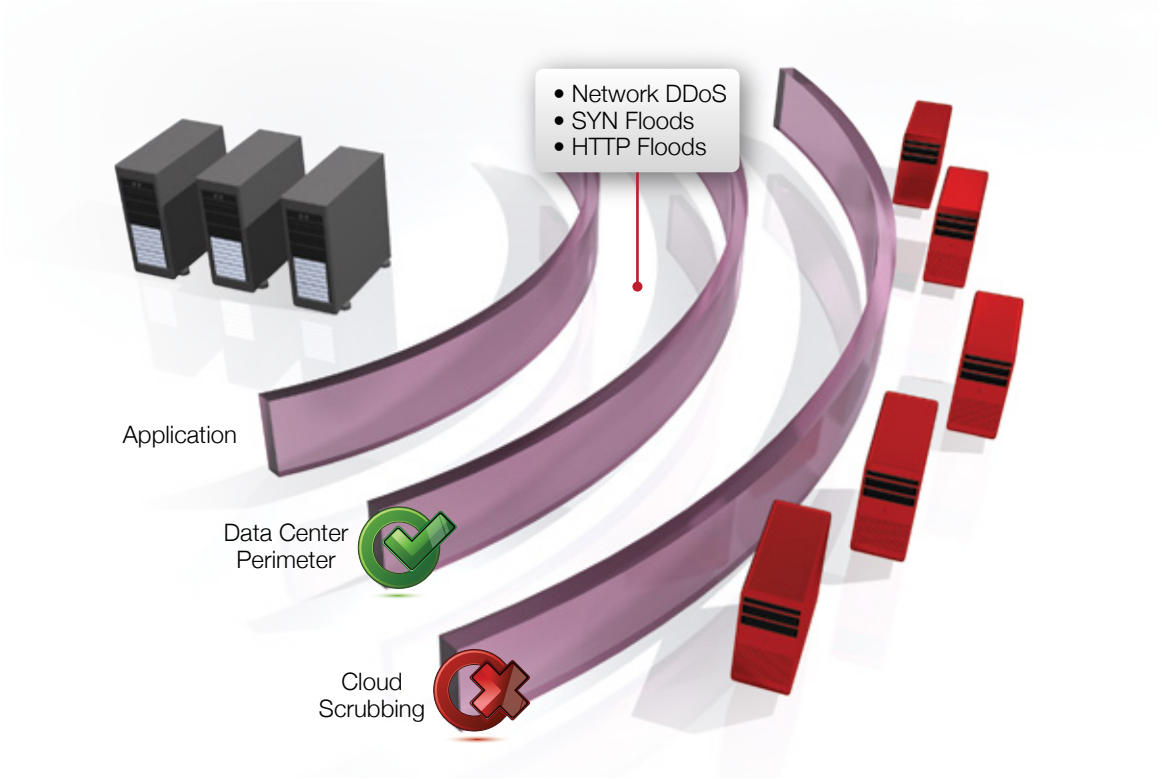

Figure 7: Required Categories of Perimeter Cyber-Attack Mitigation

Three different detection and mitigation models must be operational at all perimeter technologies – whether it is located inside an enterprise or cloud service delivery model.

Fourth Layer of Defense: Wise and Effective Cyber Warriors

The next layer of defense is defined at the people layer – often called layer eight in the OSI stack as an acknowledgement to the importance of administration, configuration, and overcoming unforecastable attack techniques and types. Of all the cyber-attack mitigation tools, the people layer is perhaps the most underestimated, misunderstood and under evaluated.

> **Did you know?**
> The most effective way to mitigate an attack is with quick and high quality detection. Most cloud scrubbing solutions rely on people/customers to notify them about the nature of an attack. This low-quality approach exacerbates effective mitigation.

DDoS Layers of Attack: Protection Challenges

Where Current Mitigation Solutions Fail

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 2011-2013 shows that attackers are getting sophisticated and manage to bypass the service provider, hitting businesses directly.

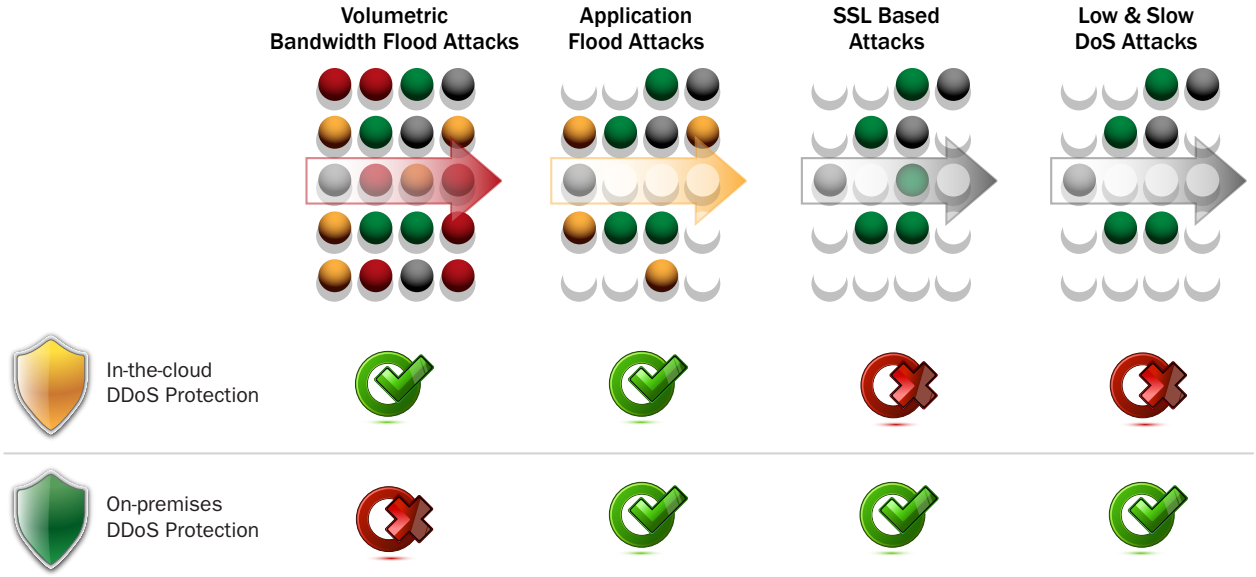

Figure 8: Where current mitigation solutions fail to protect against DDoS attacks

In-the-cloud DDoS protection is effective against volumetric bandwidth attacks. Some providers offer protection against application DDoS flood attacks depending on the equipment they use for detection and mitigation. However, service providers don't have visibility into SSL encrypted traffic and cannot block SSL-based attacks. Furthermore, low & slow attacks typically go undetected by service providers as they are low rate attacks that run under detection thresholds.

To summarize, in-the-cloud DDoS protections are effective in cleansing a high volume of DDoS flood attacks. Deploying an on-premise DDoS protection solution provides complete protection against application DDoS flood attacks, SSL-based attacks, and low & slow attacks. On-premise 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-premise solution useless.

Point of Failure

In 2011, Radware started surveying security leaders about the point of failures in DDoS attacks. Every year, the results have been largely consistent: Points of failure are divided among three main entities. The most obvious, of course, is the server that is under direct attack. However, the Internet pipe itself becomes a point of failure when it gets saturated, and the firewall—a stateful device—often fails even sooner than the server.

In our 2014 survey, we found that the Internet pipe has increased as a point of failure. In fact, it has the dubious honor of being the number-one failure point—most likely because of the increase in User Datagram Protocol (UDP) reflected amplification attacks.

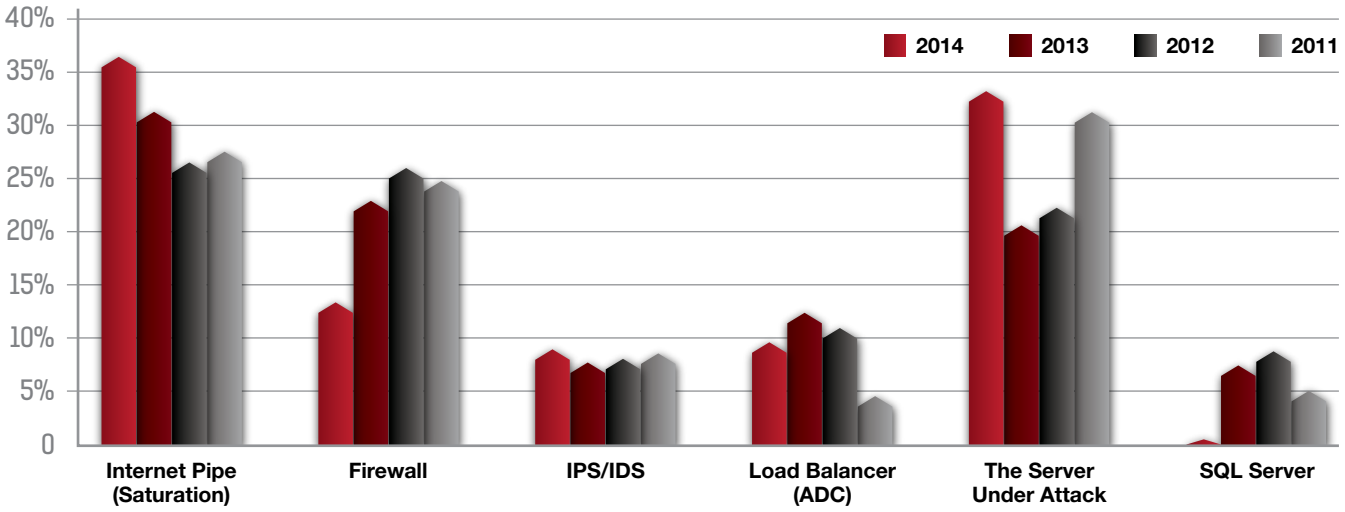

Figure 9: Which service or network elements are (or have been in the bottleneck) of DoS?

Introducing Attack Mitigation Service

Cyber-attacks have become omnipresent with motives spanning the mundane cybercrime, exotic cyber-espionage, ominous cyber war or the unpredictable hacktivism. Organizations can no longer take the "it's not going to happen to me" approach and need a more proactive and comprehensive improved strategy.

Cyber-attacks today are not like the one's of old. Attackers are using sophisticated methods to bring down datacenters and organizations' web presence, and often use multiple attack-vectors in the same attack-campaign. In addition, the simplicity of launching cyber-attacks and the variety of attack tools are reasons why more organizations suffer from more cyber-attacks such as DDoS.

Did you know?
Only one company partners with you for end-to-end defense. It's not outsourced and there are no separate delivery partners. Radware brings you the world's only end-to-end fully managed hybrid cyber-attack mitigation solution.

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.

Attack Mitigation Service Description

Attack Mitigation Service is a sophisticated network-based cyber-attack mitigation solution. Attack Mitigation Service uses the same Radware AMS elements such as DefensePro, an on premise defense component and DefensePipe, a cloud-based scrubbing center, in a hybrid architecture with a simple subscription pricing model. The service includes Radware's Emergency Response Team (ERT) service that provides 24x7 security support services for customers facing a DoS attack or a malware outbreak. Attack Mitigation Service customers can also subscribe for the ERT Premium manage option – an additional package of security and operational support services that allow customers to fully outsource the monitoring and management of the Attack Mitigation Service to Radware's team of security experts.

Attack Mitigation Service is designed to ensure the availability of an organization's internet connectivity – which given the unique and often unpredictable nature of the cyber-threat landscape – is increasingly susceptible to assaults from commercially or ideologically motivated attackers.

Attack Mitigation Service is the industry's first hybrid solution that harnesses on-premise detection and mitigation technologies in conjunction with cloud-based volumetric attack scrubbing measures to ensure that all forms of attack are dealt with optimally – and internet connections never reach saturation. Information about the attack is shared between the organization's Attack Mitigation System infrastructure (DefensePro) and Radware's cloud-based (DefensePipe) scrubbing center service resulting in real-time, comprehensive attack mitigation that safeguards on-line operations.

It has been designed to leverage all AMS technologies including protection at the three levels covered above such as:

- Perimeter Layer: A set of security modules including: Denial-of-service (DoS) protection, Network Behavioral Analysis (NBA), Intrusion Prevention System (IPS), and Reputation Information to protect you against the world's most heinous attacks.
- Application Layer Security Risk Management
- Application or Transaction Layer
- Cloud Layer
- People Layer: ERT consists of knowledgeable and specialized security experts who provide 24x7 instantaneous services for customers facing DoS attacks in order to restore network and service operational status. These experienced cyber warriors are aided with their ability to have panoramic views of the unfolding attacks through Radware's built-in SEIM that collects and analyzes events from all modules to provide enterprise-view situational awareness.

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

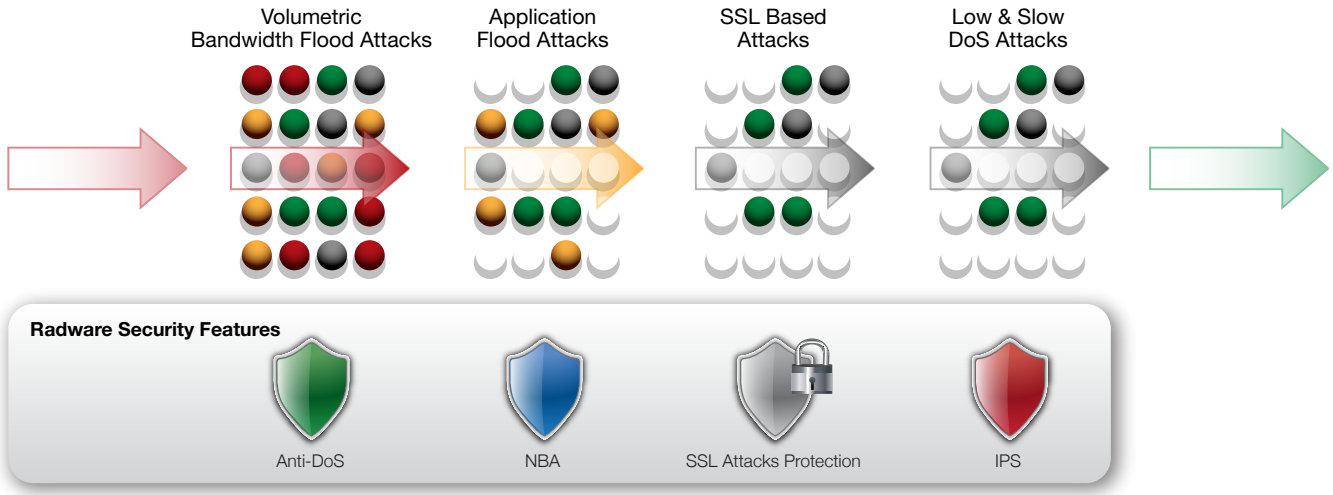

Figure 10: Mapping Radware AMS protection modules according to the DDoS layers of defense

- **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 attack 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.
- **ERT management**: Ability to have experienced operators handle cyber-attacks of all types and seamlessly escalate issues to R&D and vendor-owned service centers. Radware's ERT is the foundation around our Attack Mitigation Service and is designed to provide 24x7 attack mitigation support services for customers facing and/or experiencing a DoS attack or a malware outbreak. Often these attacks require immediate assistance.

  The ERT provides expert assistance in support of a client organizations security personnel in order to help them prepare for and defend their operations against an attack. The ERT is staffed by experienced security specialists that have vast knowledge of network threats, detection and mitigation, and in-depth operational knowledge of Radware's AMS products and technologies. In addition, the ERT takes every customer engagement, and simulates the same scenario internally for further analysis and proactive implementation of defense techniques for other customers that may face similar security threats.

End-to-End Mitigation Solution

It is clear that an effective mitigation approach against cyber-attacks of all types, including the omnipresent DDoS threat, requires both in-the-cloud protection and on-premise protection. AMS is the best fit in the industry against the DDoS threat and can be deployed in all locations and managed, maintained and upgraded by experts from the vendor supplying the equipment.

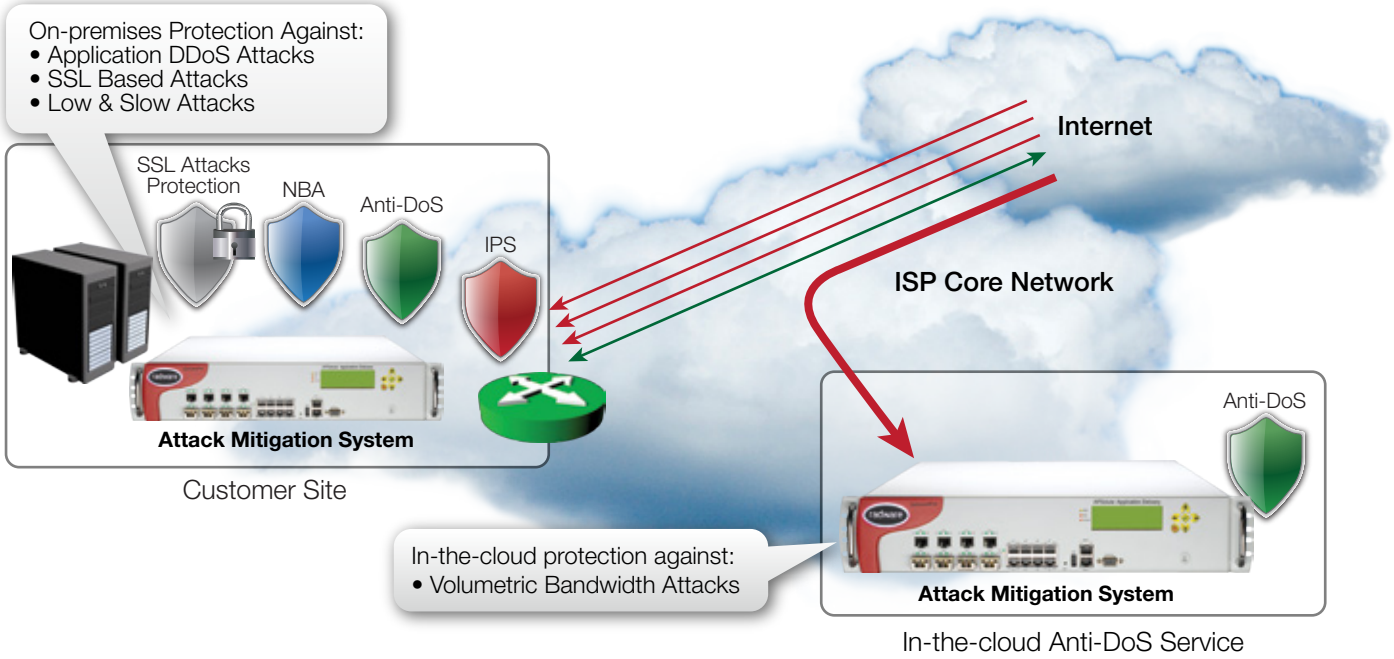

Figure 11: Radware end-to-end mitigation solution fighting the DDoS threat

- **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. It handles volume attacks of all types which would threaten saturation of your internet pipe or cloud service delivery.

- **On-premises protection**: AMS is deployed at the business perimeter network to fend-off all type of DDoS attacks: 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.

The way this service works is to have a one stop shop – built around easy technology deployment and service levels.

Radware's ERT Premium Service

Radware's Attack Mitigation Service comes with ERT Premium – an extended set of services that includes 24/7 monitoring, blocking of DDoS attacks and provides:

- Network statistics and attacks' situational awareness available on an online portal
- Real-time attack mitigation with direct "hot-line" access to the ERT
- ERT post-attacks forensic analysis and recommendations
- Quarterly review of forensic reports and security configurations
- On-going periodical configurations, reports and recommendations

Summary

Cyber-attacks, such as DDoS, are so prevalent in today's environment that no online business or organization can afford to ignore them. Attackers have become too sophisticated and can easily launch multi-vulnerability attack campaigns, making detection and mitigation nearly impossible.

Organizations that used to rely on their service provider's DDoS protection service (in-the-cloud) find that these attacks are bypassing their provider's protection layer and directly affecting business. Organizations have also found that they need to deploy premise-based technologies for comprehensive attack detection and mitigation.

However, they have been stymied with the following:

- Complexity in effectively and quickly managing and mitigating cyber-attacks
- Complexity of managing technology
- Complexity of managing various vendors
- Sticker shock of the various solutions - no pricing flexibility
- Struggle to provide comprehensive and integrated reports

Radware has introduced Attack Mitigation Service to address all of the issues listed above in one simple, easy to procure solution which is both comprehensive and fully managed. We have seen that businesses that deployed AMS on premise in conjunction with DDoS protection at the service provider were able to survive and maintain their business operations in spite of large-scale, high-volume multi-vulnerability attack campaigns. When AMS is deployed on both sides (on premise and at the service provider), organizations achieved the best protection when properly managed and maintained.

Attack Mitigation Service delivers the following solution benefits:

- Easy to deploy and maintain (fully outsourced)
- Comprehensive technology:
  - 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 low & slow DoS attacks.
  - End-to-end deployment of AMS is the best solution to fight the DDoS threat at all layers, mitigating all attack vectors in seconds.
  - When deployed on-premise, an online business has full control of its security solution and can be assisted by the ERT when attack mitigation expertise is required.
- Attack Mitigation Service offers the lowest cost OPEX and CAPEX solution to fight cyber-attacks and can be delivered either in a low monthly charge, on an annual basis or all up front.
- Superior panoramic visibility leading to world-class compliance and reporting. Let Radware do the hard work in demonstrating compliance and cyber-attack effectiveness and leave your IT security and management to focus on more business-oriented activities.