radware

Radware's Attack Mitigation Solution

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

WHITE PAPER

SHARE THIS WHITE PAPER

TABLE OF CONTENTS

Cyber Security Reaching a Tipping Point

Hacking used to require a distinct set of skills and capabilities. These days, attack services are bought and sold via marketplaces on the Clearnet and Darknet—a phenomenon that is closing the gap between skilled and amateur hackers, fueling an exponential increase in threats.

Thanks to the growing array of online marketplaces, it's now possible to wreak havoc even if you know virtually nothing about computer programming or networks. As attack tools and services become easier to access, the pool of possible attackers—and possible targets—is larger than ever. While many hacktivists still prefer to enlist their own digital "armies," some are discovering that it's faster and easier to pay for DDoS-as-a-Service than to recruit members or build their own botnet. Highly skilled, financially-motivated hackers can be invaluable resources to hacktivists seeking to take down a target.

By commoditizing hacktivist activities, hacking marketplaces have also kicked off a dangerous business trend. Vendors are now researching new methods of attack, incorporating more efficient and powerful vectors into their offerings. Some marketplaces offer a rating system so users can provide feedback on the tools. Ultimately, this new economic system will reach a steady state—with quality and expertise rewarded with a premium.

Tools of the Trade

Denial-of-service (DoS) attacks have come a long way since the days of LOIC and other GUI-based tools. Today, hackers are abandoning "old school" GUI and script tools, opting to pay for attacks via stresser services. They no longer need to acquire technical expertise or tools; instead, they can simply engage attack services to launch an attack.

Many notorious distributed denial-of-service (DDoS) groups—including Lizard Squad, New World Hackers and PoodleCorp—have entered the DDoS-as-a-Service business, monetizing their capabilities by renting their powerful stresser services. Groups sometime use their tools against high-profile targets to showcase and promote their attack services. As the point of entry becomes easier to cross, novice attackers may carry out larger, more sophisticated assaults. For just $19.99 a month, an attacker can run 20-minute bursts for 30 days using a number of attack vectors, such as DNS, SNMP and SSYN, and slow GET/POST application-layer DoS attacks.

Most tools offer basic TCP, UDP and HTTP attack vectors with slight variations. Some enable the attacker to customize payload options—including packet size, randomized data, threads and sockets per thread—in the tools. HTTP attacks are a popular vector. When an operation is underway, hackers can easily bypass mitigation solutions and overwhelm server resources with simple POST/GET floods that appear to be legitimate traffic.

What Motivates Attackers?

According to Radware's 2016-2017 Global Application & Network Security Report, the year 2016 saw an explosive rise in extortion threats, which eclipsed most other types of cyber-attacks. The primary motivations—political/hacktivism and competition—have remained consistent in recent years. For the fifth consecutive year, political hacktivism holds the second spot in the survey, accounting for twenty-seven percent of known attack motivations, with competition retaining the number four position at twenty-six percent.

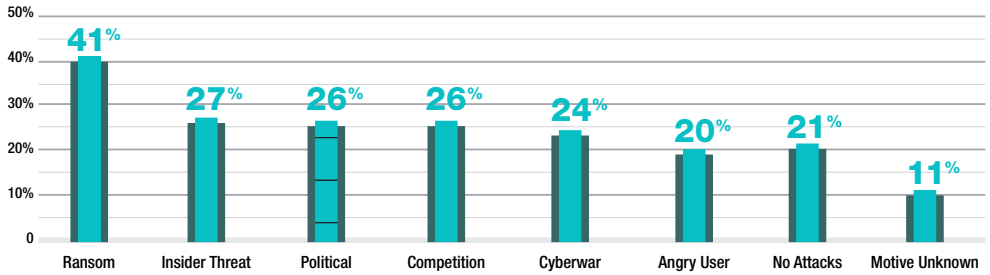


Figure 1: Which motives are behind any cyber-attacks your organization experienced?
Source: 2016-207 Global Application & Network Security Report

New Attacks Types Threaten Organizations

Preparing for "common" DDoS attacks is no longer enough. As attack tools are becoming more sophisticated and easily available, hackers are constantly evolving and finding new attack types and threats to breach existing mitigation technologies.

- **IoT Botnets** have earned their "right" as one of the top threats for organizations given the dramatic increase in the use of Internet of Things (IoT) devices to create powerful botnets. Most notable is the Mirai botnet, used to carry out one of the largest DDoS attacks in history in 2016. This botnet utilized 60+ factory default credentials found on BusyBox-based IoT devices and created the most powerful botnet to date. Mirai introduced new and sophisticated attack vectors including the Generic Routing Encapsulation (GRE) Flood Attack and DNS Water Torture Attack. With additional botnets being uncovered, including Hajime and BrickerBot, it is clear that the impact botnets will have in cyber security has just begun.

- **DNS Attacks** occur because DNS is a critical infrastructure component for any organization. While organizations and service providers take security measurements to protect the DNS infrastructure, attackers are generating more sophisticated attacks. Sophisticated attackers take advantage of the DNS protocol behavior to generate more powerful attacks–including DNS Water Torture and DNS Recursive attacks. Mitigating these attacks requires tools that can learn and gain a deep knowledge of the DNS traffic behavior.

- **Burst Attacks and Advanced Persistent Denial-of-Service (APDoS) Campaigns** include short bursts of high-volume attacks in random intervals as well as attacks that can last weeks, involving multiple vectors aimed at all network layers simultaneously. These type of attacks have a tendency to cause frequent disruptions in a network SLA, preventing legitimate users from accessing services.

- **SSL/Encrypted Attacks** are on the rise, with ten percent year-over-year growth1. Attackers use SSL protocols to mask and further complicate attack traffic and malware detection in both network and application-level threats. Many security solutions use a passive engine for SSL attack protection, meaning they cannot effectively differentiate encrypted attack traffic from encrypted legitimate traffic while only limiting the rate of request.

- **Layer 7 Application Attacks** These attacks come in two varieties: application DoS attacks that target resource exhaustion by using the well-known Hypertext Transfer Protocol (HTTP), as well as HTTPS, DNS, SMTP, FTP, VOIP and other application protocols that possess exploitable weaknesses, allowing for DoS attacks. Much like attacks targeting network resources, attacks targeting application resources come in a variety of flavors, including floods and "Low and Slow" attacks.

- **Ransom DDoS Attacks** or RDoS are one form of ransom-based attacks. RDoS are where perpetrators send an email threatening to attack an organization—rendering its business, operations or capability unavailable—unless a ransom is paid by the deadline. These attacks have grown in number every year since 2010 and typically come in the form of a volumetric DDoS attack. RDoS attacks are particularly insidious because they do not require the attacker to hack into the target's network or applications.

- **Reflection/Amplification Attacks** take advantage of a disparity of request and response ratios in certain technical protocols. For instance, the attacker could use a router as an amplifier, taking advantage of the router's broadcast IP address feature to send messages to multiple IP addresses in which the source IP (return address) is spoofed to the target IP. At high rates, these responses have generated some of the largest volumetric DDoS attacks to date.

- **Telephony DoS (TDoS) Attacks** involve launching a high volume of calls against the target network, tying up the system from receiving legitimate calls. In recent years, these attacks have targeted various businesses and public entities, including the financial sector and other public emergency operations interests.

- **Dynamic Content and CDN-based Attacks** are happening because organizations often use Content Delivery Network (CDN) providers to support global site and application performance. The problem is that CDNs provide a particularly insidious cover for attacks as organizations cannot block traffic coming from the CDN's IP addresses. Malicious actors have made an art form out of spoofing IP addresses to not only obfuscate their identity but also to possibly masquerade as seemingly legitimate users based on geolocation or positive reputational information about IP addresses they are able to compromise. Dynamic content attacks further exploit CDN-based protection by overloading origin servers with requests for non-cached content that the CDN nodes simply pass along.

What It Takes to Stay Protected

Integrated Solution to Protect from Multi-Vector Attacks
To fight evolving threats, organizations need to implement the most sophisticated security solutions to protect against new threats and emerging attacks types. Attackers are deploying multi-vector attack campaigns by increasing the number of attack vectors launched in parallel. To target an organization's blind spot, different attack vectors target different layers of the network and data center. Even if only one vector goes undetected, then the attack is successful and the result is highly destructive.

To effectively mitigate all types of DDoS attacks, multiple protection tools are needed.

- **Cloud DoS Protection** to mitigate volumetric attacks that threaten to saturate the Internet pipe.
- **DoS Protection** to detect and mitigate all types of network DDoS attacks.
- **Behavioral Analysis** to protect against application DDoS and misuse attacks. Those attacks are harder to detect and appear like legitimate traffic so they can go unnoticed without a behavioral analysis tool.
- **Intrusion Prevention System (IPS**) to block known attack tools as well as Low and Slow attacks.
- **SSL Protection** to protect against encrypted flood attacks.
- **Web Application Firewall (WAF)** to prevent web application vulnerability exploitations.

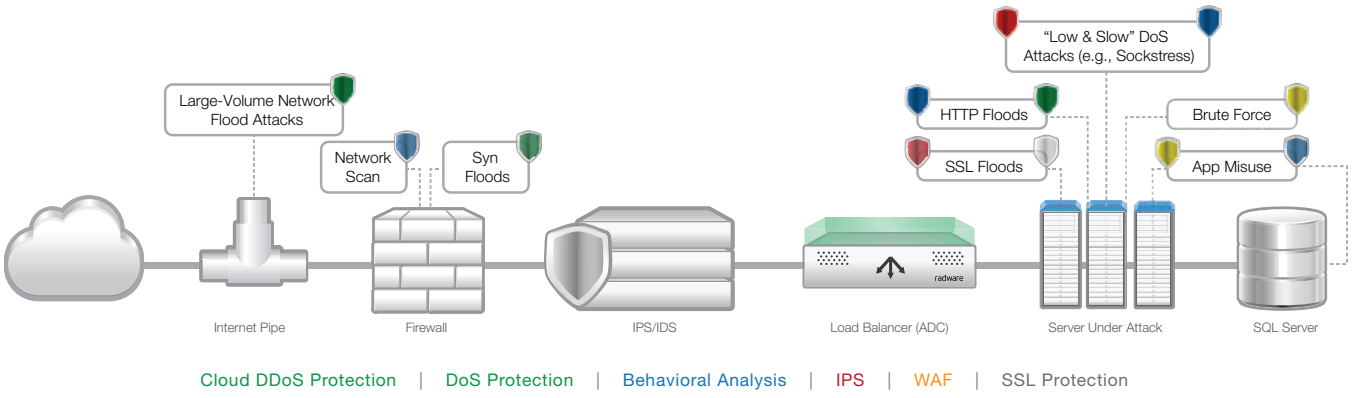


Figure 3: Attack vectors and the technology tools used to detect and mitigate

Algorithms and Automation
Automation is at the core of a successful attack mitigation solution. To withstand the evolving threat landscape, organizations need to have the right algorithms in place to shorten the time to mitigation, overcome hacker sophistication and automatically respond to attacks.

Attacks are becoming completely automated and more sophisticated, making it difficult to defend against them manually. New techniques like Burst Attacks and Advanced Persistent Denial-of-Service (APDoS) demand advanced detection and mitigation and underscore the need for automation.

Most organizations rely on a collection of solutions that require manual intervention. Multi-vector attacks demand a hybrid solution – integrating cloud-based with on-premise protection – to guard both networks and data centers. According to Radware's *2015 – 2016 Global Application & Network Security Report*, only 41% of respondents have a hybrid DDoS mitigation solution in place.

Information security problems have been largely defined by nefarious bots usurping the controls of modest and imperfect security departments. When it comes to detection quality and mitigation speed, humans are simply unable to match highly crafted automated bots. Malicious bots have proven effective—exacting steep tolls on careers, finances and, even the existence of companies themselves. In the end, the only successful defense is to deploy a powerful set of good 'bots' focused on rooting out and eradicating the hordes of bad bots.

Radware Attack Mitigation Solution

Today's standard defense technologies including DDoS protection, IPS, anomaly & behavioral analysis, SSL protection and WAF 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 attack mitigation solution (AMS) 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 center. It is a hybrid attack mitigation service that integrates on-premise detection and mitigation with cloudbased volumetric attack scrubbing. The solution was designed to help organizations mitigate attacks you can detect and offers a security solution that combines detection and mitigation tools from a single vendor. This solution provides maximum coverage, accurate detection and shortest time to protection.

The solution provides organizations with a complete, integrated solution to protect their networks and applications. This full architecture includes:

- A real-time DDoS detector and mitigator located at the edge of the data center to protect against application and network attacks. This mitigator can function as the central point for any mitigation of any detected event in automated fashion.
- A Web Application Firewall located next to the applications to detect business and application attacks.
- Patented SSL attack mitigation that provides the lowest latency, most efficient SSL attack protection with the widest coverage from SSL-based DDoS attacks.
- A Cloud DDoS Protection Service needed in case floods are bigger than network or application capacity in the data center.
- Emergency Response Team with battle-proven security experts.
- Full automation of the attack lifecycle and synchronized messaging to improve detection and mitigation response and accuracy.

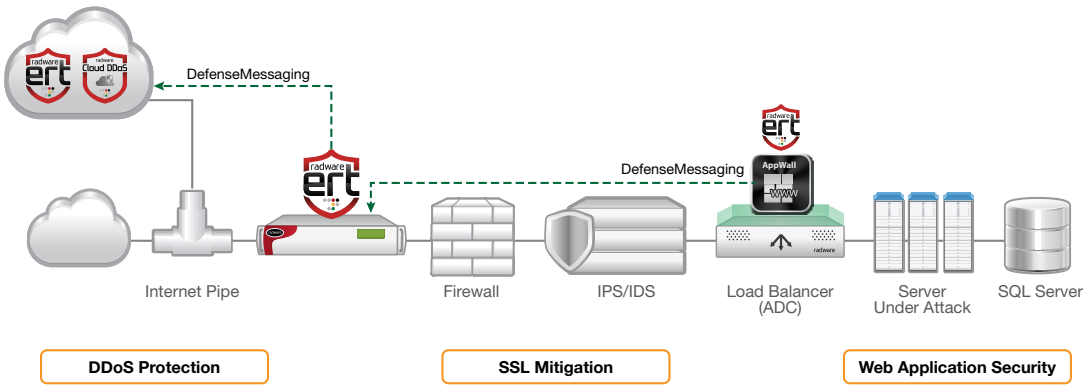


Figure 4: Radware's Attack Mitigation Solution

At the core of the solution are patent-protected algorithms for behavioral-based detection, real-time signature creation and auto policy generation that automate the attack lifecycle process and deliver a high degree of protection from the most dynamic, sophisticated attacks with minimal impact on legitimate traffic.

Multi-Vector Attack Coverage with Advanced IoT Botnet Protection

The solution offers a multi-vector attack detection and mitigation solution, handling attacks at the network layer, server-based attacks, malware propagation and intrusion activities. The solution includes protection against volumetric and non-volumetric attacks, SYN flood attacks, Low & Slow attacks, HTTP floods, SSLbased attacks, Burst attacks, and more. As the solution analyzes the traffic, it builds traffic baselines that are customized for the deploying organization.

The solution provides the industry's most advanced, automated protection from fast-moving threats from recent IoT-based attacks such as Mirai. It is uniquely built to overcome both the complexity and scale of today's sophisticated IoT-based botnets. Radware DDoS protection includes first-in-class behavioral-based algorithms to protect from known and unknown DNS flood attacks in the most cost-effective way and includes an innovative positive DNS security model to protect from DNS Water Torture Attacks.

Radware on-premise protection is comprised of five modules; all optimized for online business and data center protection as well as designed for data center and carrier deployments.

DoS Protection – protects from all types 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 (network behavioral analysis) – 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

- 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

SSL Attack Mitigation – provides protection from SSL-based DDoS attacks.

- Uniquely mitigates floods that are directed to HTTPS pages
- Provides unlimited SSL decryption and encryption capabilities
- Operates in symmetric and asymmetric environments

WAF – prevents all type of web server attacks such as:

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

High Accuracy of Detection and Mitigation
Radware's attack mitigation solution employs patented behavioral-based detection and real-time signature creation algorithms. These algorithms create baselines of normal network, application, and user behavior and use these baselines to notice abnormal traffic and accurately detect attacks. When a new, previously unknown zero-day attack is detected, the solution creates a signature in real time that uses the attack characteristics and starts blocking the attack immediately within 18 seconds. By implementing patent-protected behavioral analysis technology, the attack mitigation solution can detect known and unknown attacks in a short timeframe, with minimal false positives.

Radware's security solution is fueled by a powerful detection algorithm that:

- Considers all attack probabilities, not just volumetric.
- Uses a behavioral engine to generate multivector representations.
- Employs advanced active challenges to verify good versus bad traffic.

Radware looks at multiple parameters of the traffic using a behavioral engine. This behavioral engine analyzes multiple IP parameters within TCP (connection oriented) and UDP (connectionless) flows, as well as ICMP (router discovery) and IGMP (IP multicast) messaging. Radware also measures different parameters on HTTP and DNS traffic, detecting attacks trying to target the server. By looking at both the rates and the ratio of these different parameters, Radware creates a multi-vector mathematical representation of the normal or baseline traffic flows, which is then compared to incoming flows to detect attacks.

For example, in case of TCP or UDP, Radware determines the difference between a flash crowd or heavy traffic that follows the normal traffic ratios for a particular network (therefore good traffic) and an attack, which would have different ratios as shown in Figure 4.

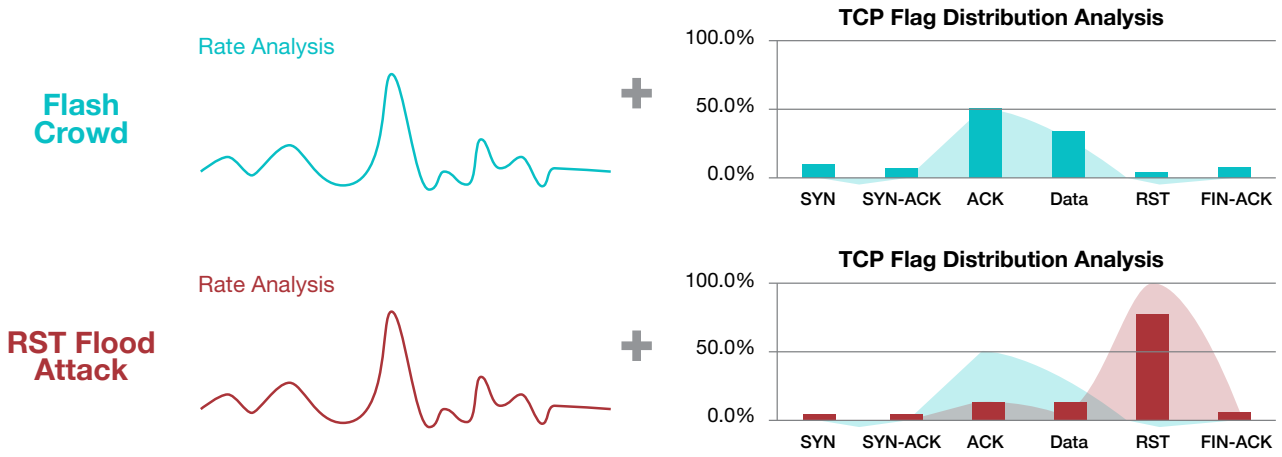


Figure 4: Radware's advanced algorithm can determine whether traffic is an acceptable flash crowd where the TCP flag distribution indicates a normal traffic or an RST attack flood indicated by very high TCP RST and a low number of TCP ACK flags that needs to be mitigated.

Always-On Protection and Shortest Time to Mitigation
The Radware on-premise attack mitigation device ensures that the data center is constantly protected. It provides always-on full protection against multi-vector DDoS attacks. Only in cases of volumetric attacks, where the organization's Internet pipe is about to be saturated, is traffic diverted to the Radware cloud-based scrubbing center, clearing attack traffic before it reaches the Internet pipe. This enables smooth transition between mitigation options.

The always-on protection ensures that the organization is fully protected and time to mitigation is measured in seconds. Moreover, in case of an attack that requires the traffic to be diverted to the cloud-scrubbing center, the protection continues with no disruption or gaps.

Smart SSL Attack Mitigation
As part of the solution, Radware offers a patent-protected SSL attack mitigation solution that supports all common versions of SSL and TLS and protects from all types of encrypted attacks — including TCP SYN floods, SSL Negotiation floods, HTTPS floods and Encrypted Web Attacks.

Radware's SSL solution is deployed using Radware-patented SSL DDoS protection technology that enables the SSL decryption agent to be deployed out-of-path and triggered only when suspicious activity starts. The solution mitigates SSL-based attacks using challenge-response mitigation techniques. 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.

It is the only solution that supports asymmetric deployment environments where only ingress traffic flows through the solution. This capability is crucial in cloud-based deployments such as within scrubbing centers or service providers, and multi-homed deployments.

The SSL mitigation solution also works to maintain user data confidentiality by performing the HTTPS validation with independent certificate management. This means that once a user is validated as legitimate, the HTTPS session resumes with the customer's certificate, which is unknown to Radware. As a result, user data remains fully encrypted and confidential and customer certificate management remains unchanged. This also removes operational dependencies between the service provider and the organization when keys are changed. In addition, the solution allows usage of wildcard certificates to reduce operational complexity when required to protect a large number of subdomains.

Protection Against Web Application Attacks
Radware's WAF is an ICSA Labs-certified and PCI-compliant WAF that 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.

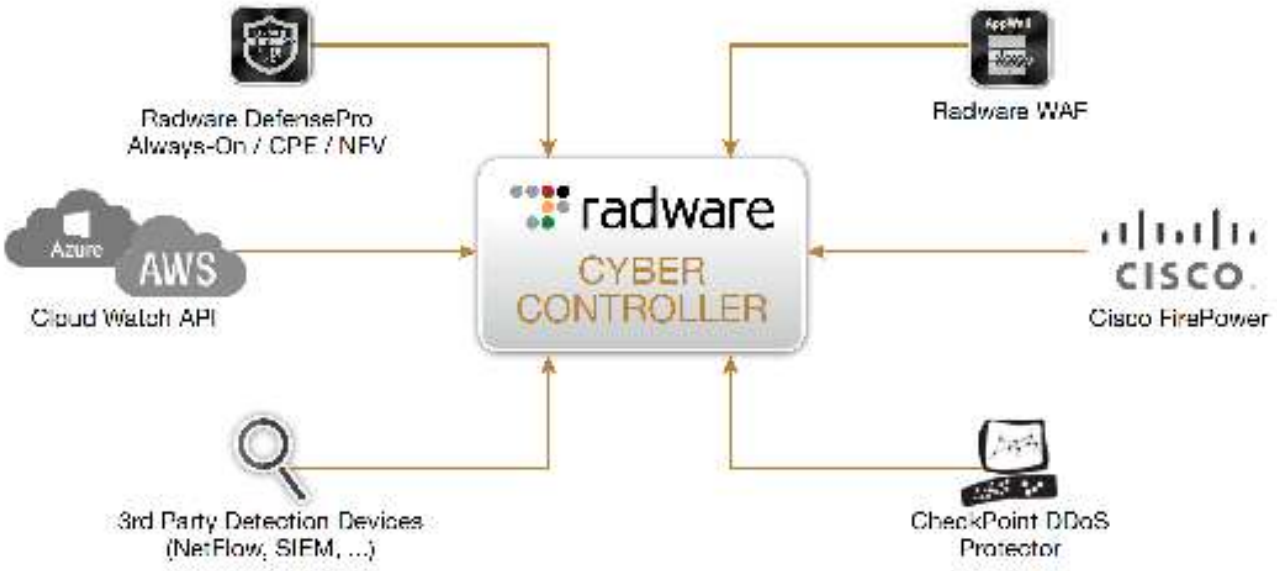
By using both negative and positive security models, the WAF solution delivers comprehensive and accurate security coverage of known and unknown web application threats including out-of-the-box coverage of all OWASP Top-10 threats. It also supports a unique machine-learning auto policy generation algorithm that provides the best tool for automatically generating security policy for the secured web application. A messaging mechanism enables the Radware WAF to signal Radware's perimeter attack mitigation device when a web application attack is detected to block it at the perimeter, protecting the rest of the network.

Radware also offers its WAF technology in a cloud-based WAF service to protect cloud-based applications from web-based attacks. The Cloud WAF Service offering provides a fully managed enterprise grade WAF that protects both on-premise and cloud-based applications, using a single technology solution. This service is based on the same technology as the on-premise WAF, allowing Radware to offer its positive security model and fingerprinting capabilities to its cloud customers.

Integrated, Synchronized Solution
At the core of the solution is DefenseMessaging — a unique messaging capability that synchronizes traffic statistics, attack information, floating policies and baselines across the various elements of the solution to create a truly integrated system.

While each one of the elements has its own role and operates individually to provide best-of-breed protection in its own domain, DefenseMessaging enables them to operate as a single system that provides optimal detection and mitigation capabilities — giving the organization more visibility and control in protecting its critical assets. The importance of such a capability is most apparent in scenarios where complex, multi-vector attacks are launched on an organization, targeting multiple services that are located at different parts of the network.

Automation of the Attack Lifecycle
For the more sophisticated, larger scale networks, such as those employed by service providers and carriers, Radware offers a cyber-control application designed to collect input from distributed detection elements in the network and then aggregate, correlate and analyze in the context of the protected service. This supports a workflow-based model with an orchestrated and automated flow per protected customer that includes service provisioning, DDoS attack defense, detection criteria and attack mitigation.



Monitor. Analyze. Report.
The Radware solution includes active monitoring and health checks on the protected service or application, providing an organization-wide view of security and compliance status from a single console. 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. The built-in Security Event Information Management (SEIM) system provides an organization-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 obtain information to speed incident identification and provide root cause analysis, improving collaboration between NOC and SOC teams, and accelerating the resolution of security incidents.

24x7 Security Experts and Fully Managed Services
Radware's attack mitigation solution is complemented by the ERT, providing 24x7 support for hands-on attack mitigation assistance from a single point of contact. With the necessary expertise in mitigating prolonged, multi-vector attacks, the ERT works closely with customers to decide on the diversion of traffic during volumetric attacks, assisting with capturing files, analyzing the situation and helping ensure the best mitigation options are implemented.

The ERT also offers an extended set of security and operational support services that allow customers to fully outsource the monitoring and management of their organization's security, including on-premise device management, to Radware security experts. ERT Premium is a managed service designed to proactively prevent emergencies, neutralize security risks, and safeguard operations from irreparable damages, thus assuring SLA and business continuity.

Summary

Widest, Automated, Real-Time Protection
DDoS attacks cause organizations to lose revenue and increase expenses. Attackers are more sophisticated and use multi-vulnerability attack campaigns. The solution offers a hybrid, multi-layered mitigation solution with the broadest attack mitigation.

This hybrid solution provides the shortest time to mitigation, stopping multi-vulnerabilities DDoS attacks instantly, resuming revenue flow.

Radware's attack mitigation solution is based on patent-protected algorithms for behavioral-based detection, real-time signature creation and auto policy generation that automate the attack lifecycle process. It delivers a high degree of protection from the most dynamic, sophisticated attacks with minimal impact on legitimate traffic. These algorithms provided in an integrated, single vendor solution offer organizations the most automated, multivector attack mitigation solution:

- **Hybrid DDoS Attack Prevention & Protection** – Integrating Radware on-premise, real-time DDoS protection solution, DefensePro, with Hybrid Cloud DDoS Protection Service for volumetric attack protection.
- **Unmatched Web Application Security** – Through WAF, AppWall, or Cloud WAF Service, Radware offers full web security protection including OWASP Top-10 coverage, advanced web attack protection and zeroday web attack protection.
- **Minimal-Latency SSL Attack Mitigation Solution** – A patent-protected mitigation solution supports all common versions of SSL and TLS and protects from all types of encrypted attacks — including TCP SYN floods, SSL Negotiation floods, HTTPS floods and Encrypted Web Attacks.
- **Full Suite of Cloud Security Services** – Full range of cloud WAF and DDoS protection solutions that can provide organizations optimal cloud protection services to meet the unique needs of their networks and applications.
- **Centralized Management & Reporting** – Providing a single pane of glass to manage and monitor all security components in a collaborative and consistent way.

About Radware

Radware® (NASDAQ: RDWR) is a global leader of cybersecurity and application delivery solutions for physical, cloud and software-defined data centers. Its award-winning solutions portfolio secures the digital experience by providing infrastructure, application and corporate IT protection and availability services to enterprises globally. Radware's solutions empower more than 12,500 enterprise and carrier customers worldwide to adapt quickly to market challenges, 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: Radware Blog, LinkedIn, Facebook, Twitter, SlideShare, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis of DDoS attack tools, trends and threats.

PRD-AMS-Solution-WP-06-2018/27-US