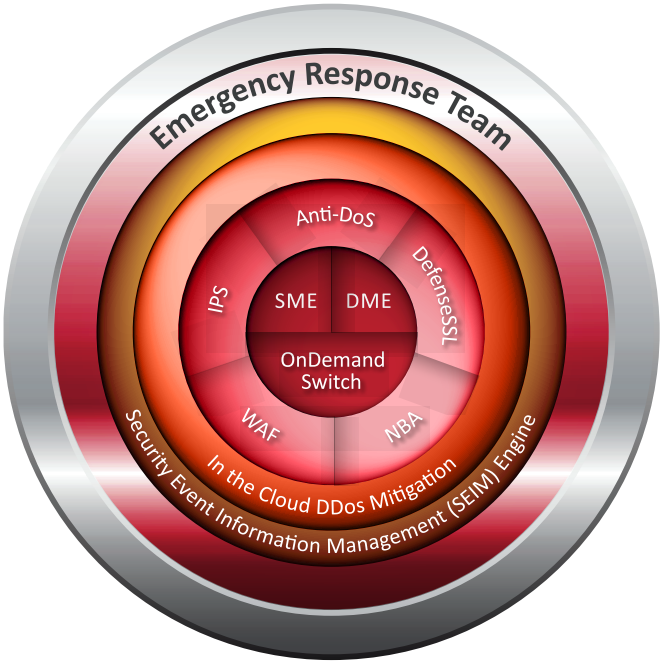
radware

Attack Mitigation Solution

Technology Overview - Whitepaper



SHARE THIS WHITEPAPER

Table of Contents

Understanding the Threat Landscape

In the past, every asset enterprises protected – data centers, applications, and databases - resided within a secure network perimeter. Today, as organizations adopt cloud technologies to improve overall efficiency and expand business opportunities, they face a more distributed network infrastructure and are required to protect assets beyond the perimeter.

Organizations of all sizes are struggling to finance costs associated with cyber-attack prevention and mitigation. Cyber-attacks that cause network, server and application downtime and/or service degradation can lead to reduced revenues, higher expenses and damaged reputations.

Cyber-attacks have reached a tipping point in terms of quantity, length, complexity and targets. As cyber threats grow and expand to new targets, even organizations with by-the-book security programs can be caught off guard.

The Evolution of Attackers' Motivation

As cyber-attacks continue to threaten organizations, attacker's motivations evolve. Richard Clarke, a former Special Advisor of Cybersecurity, defines the four main motivations for cyber-attack - **CHEW**:

- **C**ybercrime – the notion that someone is going to attack you with the primary motive being financial gain from the endeavor.
- **H**acktivism – attacks motivated by ideological differences. The primary focus of these attacks is not financial but rather to persuade or dissuade certain actions or "voices."
- **E**spionage – straightforward motive to gain information on another organization in pursuit of political, financial, capital market share or some other form of leverage.
- **W**ar (Cyber) – the notion of a nation-state or transnational threat to an adversary's centers of power via a cyber-attack. Attacks could focus on non-military critical infrastructure or financial services, or more traditional targets, such as the military-industrial complex.

Attacks can be driven by one or more of these motives and attackers can vary from script kiddies, members of organized crime, to governments.

Attacks Are Longer, More Complex and Continuous

Attackers are deploying multi-vector (e.g., different types) attack campaigns that target all layers of the victim's IT infrastructure, including the network, server and application layers. Attackers are more patient and persistent, leveraging "low & slow" attack techniques that misuse the application resources rather than resources in the network stacks. They also use more evasive techniques to avoid detection and mitigation including SSL-based attacks, changing the page request in a HTTP page flood attack, and more.

Years ago, DoS attacks mostly targeted the network through SYN, TCP, UDP and ICMP floods. From 2010-2012 there was an increase in more sophisticated application level attacks and SSL encryption-based attacks. Recently, a specific type of DoS attack—the amplification reflective flood—has not only revived network attacks but also given attackers an edge over their counterparts who target applications. Reflective attacks, including those using DNS, NTP, and CHARGEN, started heating up in 2013 and remained a persistent threat throughout 2014. The rise in reflective attacks has contributed to the crowning of the Internet pipe as the major failure point in enterprise security.

The length of an attack indicates another new trend in DDoS attacks -constant attacks. The graph below from Radware's 2014-2015 Global Application & Network Security Report highlights the rise in contstant attacks, those in which attackers continuously and constantly attack the same organization.

The simplicity of launching such cyber-attacks and the variety of attack tools available are reasons why more organizations are suffering from increased attacks, such as DDoS. The question is no longer about preventing attacks. The attacks are happening. It is about detecting and mitigating attacks.

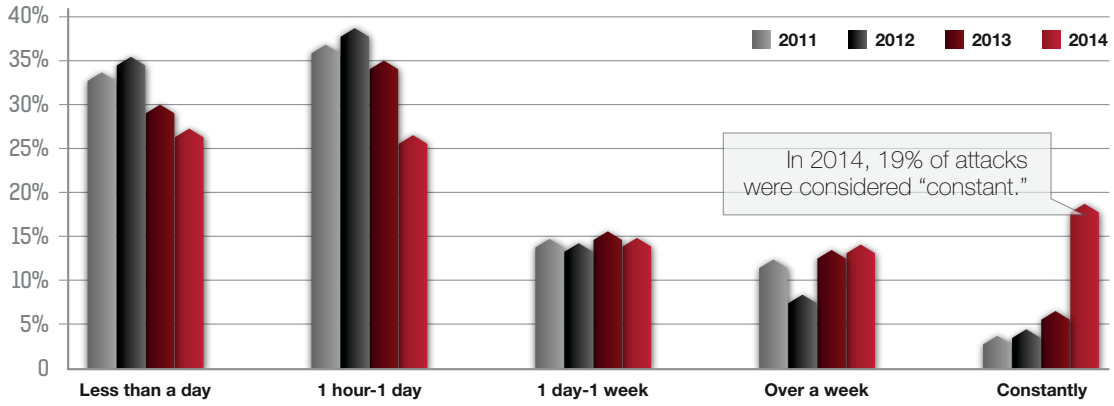


Figure 1: Attack durations year by year, as presented in the Radware Global Application & Network Security Report 2014-2015.

Network-Based Threats and Risks

The network-based layer of threats includes attacks that misuse network resources. One of the most effective methods to exploit IP infrastructure weaknesses is the Distributed Denial of Service (DDoS) attack.

DDoS attacks typically involve breaking into hundreds or thousands of machines across the Internet. This break-in process can be performed "manually" or automatically by using worms and other malware that either propagate on their own, or can be downloaded by the unaware client and then infect every vulnerable host. After a successful break-in, the attacker, or the malware acting on behalf of the attacker, installs specific DDoS tools or a specific bot, allowing the attacker to control all these "burgled" machines to launch coordinated attacks on victim sites.

Network attacks typically exhaust network stack resources, router and switch processing capacity, and/or misuse bandwidth resources, all of which disrupt the victims' network connectivity. The number of DDoS attacks significantly increased in 2014, reaching volumes which were so high that they saturated the ingress link from the organization to the service provider. This is typical of reflection attacks which are transported over UDP due to the session less nature of the protocol. UDP allows attackers to utilizing open network resources as tools to launch high volume attacks on a chosen victim.

In addition to the DDoS flood threat, the network layer threats include the "traditional" exploit-based operating system attack vectors. Each common network infrastructure product—routers, switches, and firewalls—has a list of known vulnerabilities. If any of these vulnerabilities are being exploited, the product can be compromised, risking the entire IP infrastructure and putting business continuity at high risk.

Server-Based Threats and Risks

Server-based threats can be clearly divided into two groups: TCP/IP stack weaknesses exploitation, and application level attacks.

TCP/IP Stack Weaknesses

These types of threats include attack vectors that misuse the resources of the transport layer in a way that can disturb, deny, or bring down TCP connections, and the application transaction(s) that go with them, for example, HTTP transactions, FTP files downloads, or MAIL messages. It's easy to exhaust the TCP resources of a server through several attack vectors, such as TCP SYN flood attacks and TCP established connection floods. The latter, although very easy to generate, cannot be effectively detected and prevented by most existing security products. This attack can bring down, or seriously damage, the operation of servers by consuming large amounts of server TCP resources. This misuse of TCP resource attacks are not necessarily large scale attacks, and are therefore difficult to detect and prevent by most security solutions.

As in the case of network based attacks, the TCP/IP stack threats also include the "traditional" operating system attack vectors. Each of the common operating systems has a list of known vulnerabilities. If any of these vulnerabilities are exploited, the server can be compromised, which risks the service as well.

Server Applications Level Attacks

The vulnerabilities that are associated with this layer of threats can be divided into two families:

a. Vulnerability-based server application threats. This family includes both known and zero-minute attacks.
b. "Non-vulnerability-based" server application threats.

Vulnerability-based Server Application Threats

Vulnerability-based server application threats are the more traditional type of attacks that are based on a previously known vulnerability of application software—they are defined as the known attacks. When a new vulnerability is discovered, an attacker can exploit it before the security company or the software vendor is ready with an attack signature protection or, alternatively, with a software patch that "fixes" the newly discovered vulnerability. While the protection or the software patch is developed, the system is exposed, and any attack during this time period is defined as a "zero-minute"[1] attack. New application vulnerabilities are discovered every day, which adds up to thousands of new vulnerabilities every year.

Representative categories of known and zero-minute server application attacks include:

- Buffer-overflow vulnerability types – A design flaw where a process attempts to store data beyond the boundaries of a fixed-length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may result in erratic program behavior, a memory access exception, program termination (a crash), incorrect results or, especially if deliberately caused by a malicious user, a possible breach of system security.

- SQL injection vulnerabilities – A technique that exploits a security vulnerability occurring in the database layer of an application. The vulnerability is present when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements, or user input is not strongly typed, and thereby unexpectedly executed. A successful SQL Injection can result in information disclosure or even full database denial of service.

- XSS - Cross Site Scripting – A type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users. Examples of such code include HTML code and client-side scripts. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy. Vulnerabilities of this kind have been exploited by powerful phishing attacks and browser exploits.

1 In the past these types of attacks were defined as "zero-day" attacks, but now that the time to exploit the newly discovered vulnerabilities has been shrinking down to a less than a day, these attacks are now defined as "zero-minute" attacks.

- Rootkits – A program designed to take fundamental control of a computer system, without authorization by the system's owners and legitimate managers. Rootkits help intruders gain access to systems while avoiding detection. Rootkits exist for a variety of operating systems, such as Microsoft Windows, Mac OS X [2] [3], Linux, and Solaris.

- Worms – A self-replicating computer program. It uses a network to send copies of itself to other computers and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms almost always cause harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

- Evasion Techniques – A technique which threatens the capability of static signature-based technologies to handle vulnerability attacks is evasion. Attackers use various encoding, fragmentation, obfuscation and polymorphism techniques to evade detection by signature based systems. This technique utilizes the infinite number of options to encode a message to the server in order to send the attack message in a format that will not be detected by a signature.

"Non-vulnerability-based" Server Application Threats

Non-vulnerability based threats aim to exploit weaknesses in the servers' application that cannot necessarily be defined as vulnerabilities. They can be typified by a sequence of "legitimate" events that are used to break authentication mechanisms (also referred to as "server cracking"), scan the application for existing vulnerabilities (e.g. vulnerability scanning) that are usually followed by a successful exploitation and could be used for taking control of the server's application operations. More sophisticated non-vulnerability application attacks include well-chosen repeated sets of legitimate application requests that misuse the server's CPU and memory resources, creating a full or partial denial of service condition in the application.

Non-vulnerability based threats aim to exploit weaknesses in the servers' application that cannot necessarily be defined as vulnerabilities.

These emerging server application threats, which look like legitimate application requests, are generally not associated with unusually large traffic volumes. This allows hackers to integrate well with wholly legitimate forms of communications, and comply with all application rules, so that in terms of traffic thresholds or known attack signatures, they are below the radar of existing network security protections.

These non-vulnerability-based server application attack vectors include attack tools, such as: application scanners, brute-force and dictionary tools (called "crackers"), and application session-based flood tools and bots. All of these attack tools can be integrated into and infect a legitimate client machine that will generate all of the previously mentioned server-based threats.

Bots targeting Web applications are a complex threat for many site operators. Advanced bots dramatically complicate the mitigation process using techniques such as mimicking user behavior, dynamically changing the source IP addresses, operating behind anonymous proxies and CDNs and more. The various bots aim to achieve different goals, where the most common ones are web scraping, Web application DDoS, brute force attacks for password cracking, and clickjacking.

However, not only bots can target web applications to achieve these goals. A collective community of human users can introduce similar challenges in detection and mitigation of these attacks, possibly making it even more difficult to detect and mitigate.

The following illustration describes the relationships between threat types that were discussed:

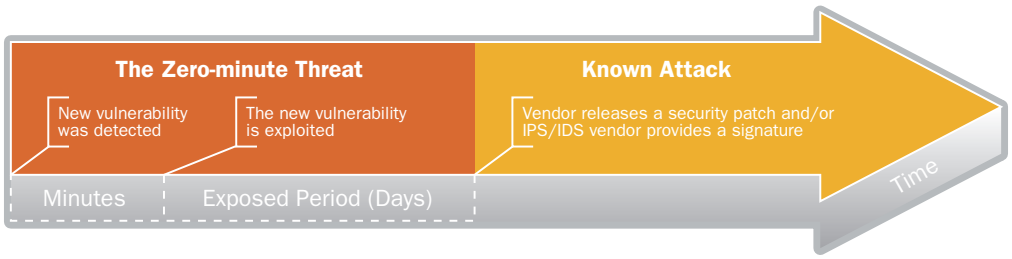


Figure 2 – Vulnerability-based attack lifecycle

Figure 3 – Non-vulnerability based attack lifecycle

The focus of the vulnerability-based attacks life cycle (Figure 2) is the early discovery stage: hackers try to exploit newly discovered application vulnerabilities while the security vendors scramble to provide a signature to protect against it, hence the cat-n-mouse play between hackers and vendors.

The non-vulnerability threats define a new playground: security vendors cannot respond proactively by securing newly discovered vulnerabilities, or use signature protection as the attack traffic interacts well into legitimate traffic patterns.

Protection from Multi-Vector Attacks

In order to fight evolving threats, organizations need to implement the most ample security solutions to fully protect against new threats and all types of attacks.

To target an organization's blind spot, attackers are deploying parallel, multi-vector attack campaigns by increasing the number of attack vectors launched in parallel and targeting 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 and the low and slow attacks.
- **SSL protection** to protect against encrypted flood attacks.
- **Web Application Firewall (WAF)** to prevent web application vulnerability exploitations.

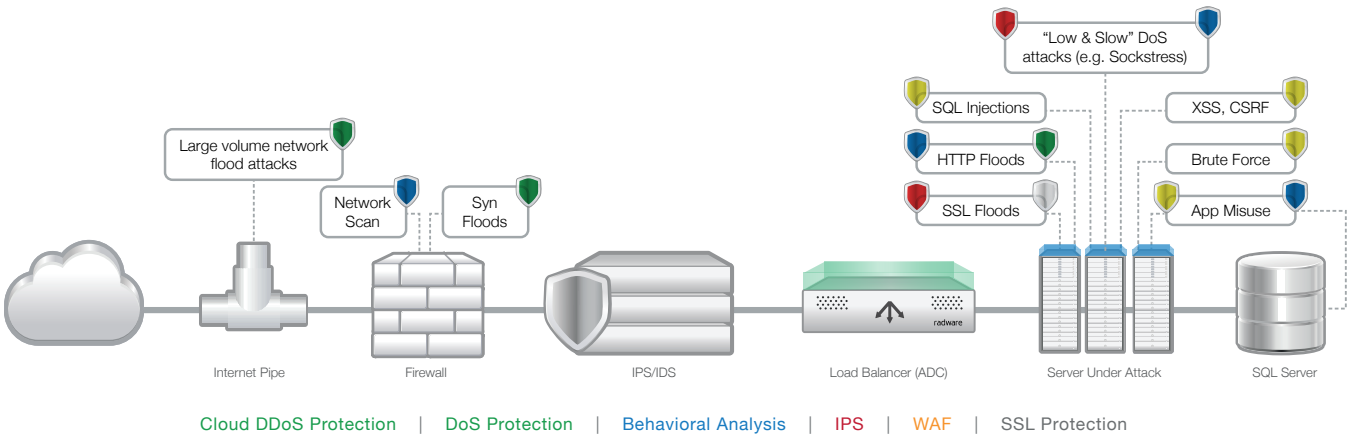


Figure 4: Attack vectors and the technology tools used to detect and mitigate

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 hybrid attack mitigation solution 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 cloud-based volumetric attack scrubbing.

The solution was designed to help organizations best mitigate attacks by offering a single-vendor security solution that combines detection and mitigation tools. Radware's solution provides maximum coverage, accurate detection and shortest time to protection.

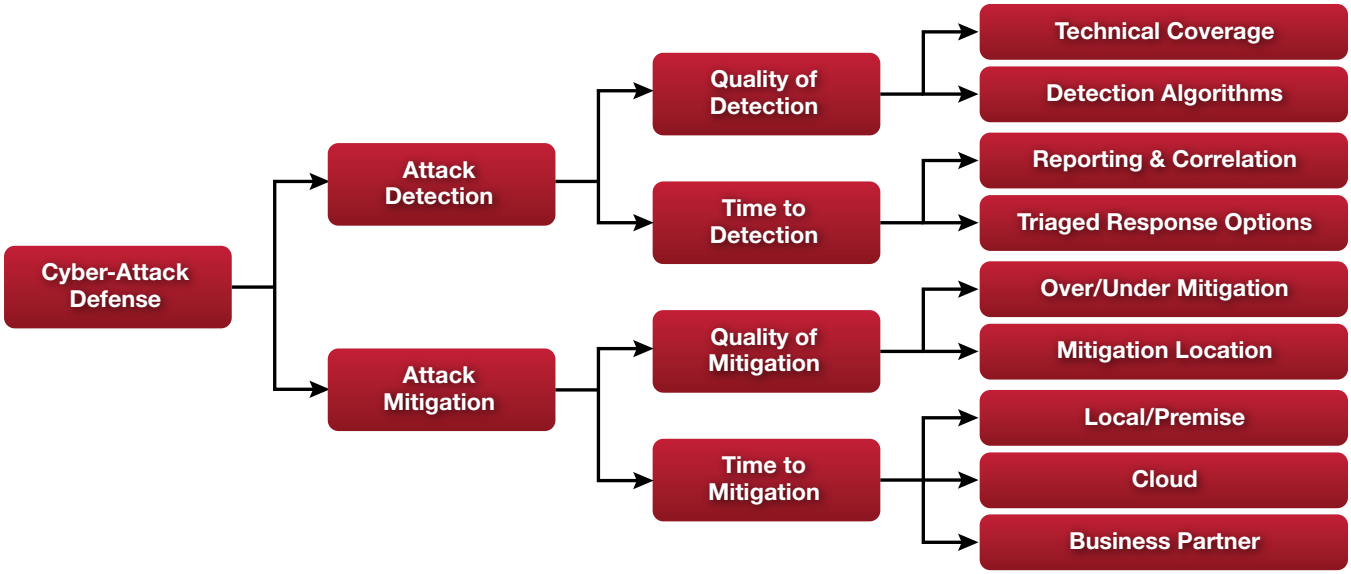


Figure 5: Comprehensive cyber-attack protection with detection & mitigation

Widest Attack Coverage, Including SSL-Based Attacks

Radware's attack mitigation solution offers a multi-vector attack detection and mitigation solution by 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, SSL based attacks, and more. As the solution analyzes the traffic, it builds traffic baselines that are customized for the deploying organization.

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.

Radware's on-premise protection is comprised of 5 modules, which are all optimized for online business and data center protection, and designed for data center and carrier deployments.

DoS Protection – protection 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 – the network behavioral analysis module prevents application resource misuse and zero-minute malware spread. Protection against attacks, including:

- 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

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 – the web application firewall 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

The network behavioral analysis (NBA) module in Radware's attack mitigation platform 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. By implementing patent-protected behavioral analysis technology, Radware's attack mitigation solution can detect attacks in a very short timeframe with minimal false positives.

Always-On Protection and Shortest Time to Mitigation

Radware's 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 saturate, is traffic diverted to Radware's 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- the time to mitigation is measured in mere seconds. Moreover, in the event of an attack that requires the traffic to be diverted to the cloud-scrubbing center, the protection continues with no disruption or gaps.

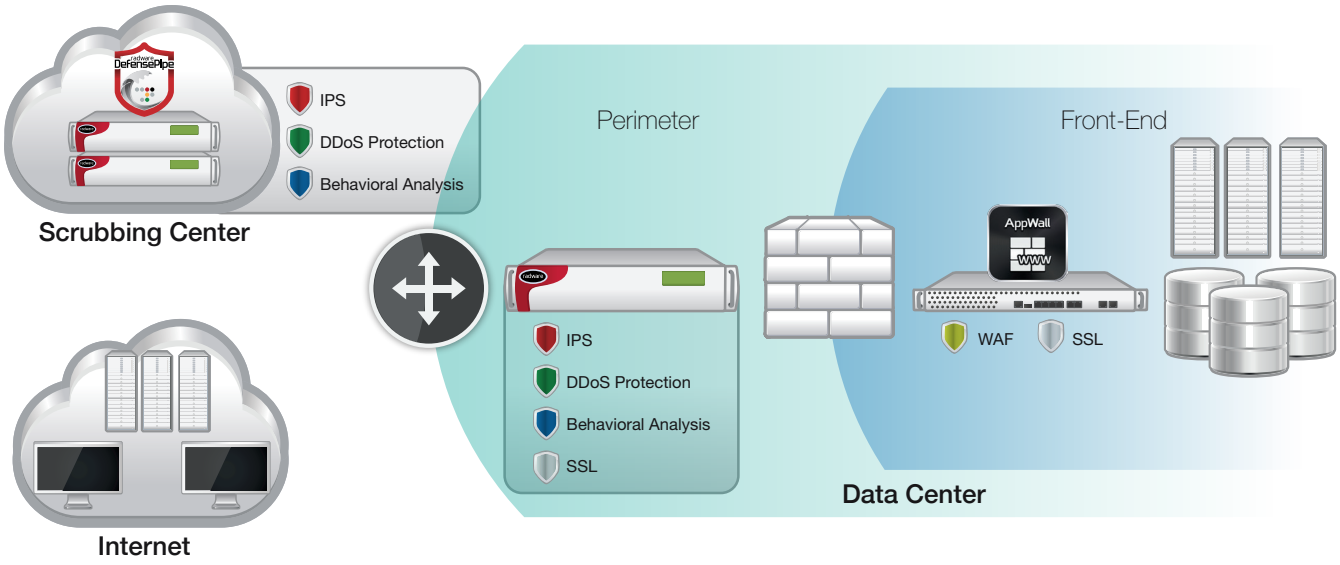


Figure 6: Radware Hybrid Attack Mitigation Solution

Protection Against Web Application Attacks

Radware's Web Application Firewall (WAF) provides complete protection against web application attacks, web application attacks behind CDNs, advanced HTTP attacks (slow loris, dynamic floods), brute force attacks on login pages, and more.

A messaging mechanism enables Radware's WAF to signal Radware's perimeter attack mitigation device when a web application attack is detected, blocking it at the perimeter and protecting the rest of the network.

As organizations migrate to the cloud, Radware also offers a cloud-based WAF service to protect cloud-based applications from Web-based attacks. Radware's Hybrid Cloud WAF offering provides a fully managed enterprise grade WAF that protects both on-premise and cloud-based applications, using a single technology solution. Unlike existing WAF solutions that integrate dual technologies that result in a gap between protection coverage and quality, Radware's single technology approach makes migrating applications to the cloud safer and more secure.

Monitor. Analyze. Report.

Radware's 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 system mitigated attacks (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

Radware's attack mitigation solution is complemented by the Emergency Response Team (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, assists with capturing files, analyzes the situation and ensures the best mitigation options are implemented.

Radware's Attack Mitigation Brain: Technology Overview

As discussed in the previous section, the main security technologies deployed in Radware's attack mitigation solution are:

- Automatic real-time signatures technology – Detects and prevents the non-vulnerability and zero-minute attacks without the need for human intervention.
- Deterministic signature-based technology – Detects and prevents known attack vulnerabilities.

NBA & Anti DoS Modules Technology Overview

Three main patented technologies are responsible for Radware's network and application behavior analysis, and for the Anti-DoS modules:

- Fuzzy Logic expert detection and real time signature generation technology
- Advanced action escalation technology
- SSL DDoS Protection

Fuzzy Logic and Real-Time Signature Technology

The real time signatures technology is an adaptive, multi-dimension decision engine that deploys Fuzzy Logic technology for accurate attack detection and mitigation. The technology consists of three modules that work together to create Radware's unique advantage in the Attack Mitigation market:

1. The Fuzzy Logic module – A multi-dimension decision engine that detects attacks in real time.
2. Automatic real-time signature generation module – Once an attack has been detected, this module creates on-the-fly attack signatures.
3. Closed-feedback modules – Responsible for optimizing the real-time signature during the attack-blocking stage, and removing the signature once attack is over.

Fuzzy Logic Module - Adaptive Multi-Dimension Decision Engine

Radware's Fuzzy Logic module is the main engine that drives decisions regarding traffic, users, and application behavior. This engine collects traffic characteristic parameters and assigns them an anomaly weight according to an adaptive fuzzy membership function. It then correlates these parameter weights and produces real time decisions represented by a "degree of attack" (or anomaly) value. Based on the degree of attack, the system is able to introduce counter-measures that actively mitigate a perceived threat.

Radware's Fuzzy Logic algorithm overcomes traffic analysis difficulties that Internet communications usually present. The algorithm provides a simple way to draw definite conclusions from vague, ambiguous, or imprecise

information. Difficulties such as incomplete knowledge or noisy signals (a common occurrence when dealing with Internet traffic), are smoothly handled by the Fuzzy Logic algorithm. Radware chose Fuzzy Logic over other traditional analysis and approximation methods due to the large amount of CPU and memory resources that these more traditional methods consume.

The Fuzzy Logic algorithm processes many parameters, determines their degree of anomaly, and correlates between them to reach conclusions in real time. Using Fuzzy Logic as a decision engine, Radware's AMS can perform more in-depth traffic analysis and come to conclusions quicker than any other traditional method.

The Fuzzy Logic module includes adaptive capabilities and the sensitivity of the module is being continuously tuned to match the characteristics of the protected network. The adaptive algorithms include IIR (Infinite Impulse Response) filters that continually average traffic parameters and shape the Fuzzy Logic membership functions accordingly.

These capabilities allow Radware's IPS module to continuously establish normal behavior baselines according to the date and the time of day, and depending on the behavior of the protected site.

For each required protection type, the Fuzzy Logic decision collects and learns traffic parameters required to best characterize the threat that should be identified and mitigated.

Typically, the Fuzzy Logic decision engine uses two categories of traffic behavioral parameters to generate a degree of attack:

- **Rate-based** behavioral parameters such as packet rate, Mbps, connection rate, application request rate, and application response rate.

- **Rate-invariant** behavioral parameters such as protocol breakdown, TCP flag distributions, ratio between inbound and outbound traffic, application request/response ratio, connections distribution, URL hits, probability functions, and more.

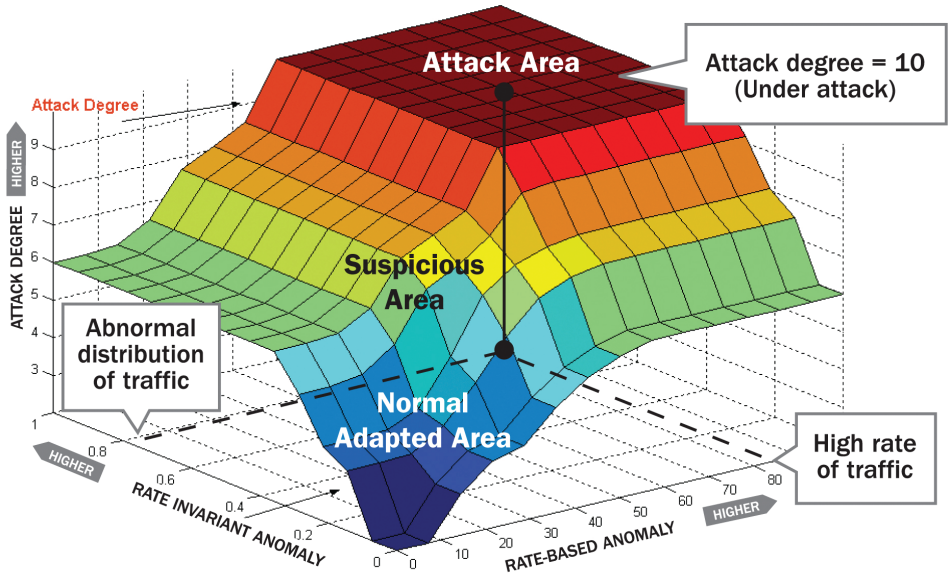


Figure 7: Fuzzy Logic Decision Surface

The XY plane shows the fuzzy input rate-based input and rate-invariant inputs).
The z-axis represents the degree of attack (or anomaly).

The Fuzzy Logic decision surface (illustrated in Figure 7), shows a correlation between both rate-based and rate- invariant behavioral parameters, before generating a degree of attack. Although, in reality, the Fuzzy Logic engine correlates between multiple behavioral parameters (for clarity the figure illustrates a two-dimensional decision surface).

Elimination of False Positives - In order to eliminate false positive decisions and misdetections, the Fuzzy Logic engine correlates between both rate and rate-invariant parameters. To illustrate this point, consider the frequent legitimate behavior of an unexpected mass crowd entering a news website. This behavior immediately causes rate-based behavioral parameters to significantly increase, thus making it look like an anomaly. If the detection engine relies only on rate-based behavioral parameters, this completely legitimate behavior will be flagged as an attack, and will be blocked. However, because rate-invariant parameters will remain unchanged (within certain boundaries) during such legitimate mass crowd behavior, an engine that intelligently correlates between both rate-based and rate-invariant parameters, such as Radware's Fuzzy Logic, will not flag this legitimate event as an attack and prevent blocking of legitimate users.

The Fuzzy Logic module is an adaptive expert system that requires minimal human intervention to configure rules or thresholds. A system that relies upon manually-tuned thresholds and rules produces wildly disparate detection quality, and mostly depends on the individual skill level of the system administrator.

Automatic Real-Time Signature Generation Module

In cases where the attack is unknown (zero-minute threat), it is a challenge to block the attack without simultaneously blocking legitimate traffic.

A known attack is usually characterized by a well-defined content signature that can be used to remove the threat in a surgical manner. However, in the case of zero-day or non-vulnerability based threats, no signature exists and therefore the security technology that detects the anomaly is based on behavioral analysis. In order to block the attack, the system should also be capable of characterizing it in a very precise way. In other words, the behavioral-based technology should have the capability of automatically creating an attack signature.

Radware utilizes probability analysis and closed-feedback loop technology in order to create an attack signature that characterizes the ongoing anomaly without the need for a human research vulnerability group. When the Fuzzy Logic decision module detects an anomaly, the system activates the automatic attack signature generation mechanism in order to find characteristic parameters of the ongoing anomaly. Radware developed a probability theory, a unique patented implementation method that distinguishes between expected and unexpected repetition of parameters. These parameters were studied (statistically) according to the network environment, and the automatic signature generation mechanism flags unexpected values as "possible" pieces of the attack signature that represents the ongoing detected anomaly.

The following parameter types as well as others are analyzed by the automatic signature creation module:

- Packet checksums
- Source IP address
- SIP URL's (for VoIP anomalies)
- TTL (Time to Live)
- TCP sequence numbers
- DNS Qname
- Packet Identification number
- Ports numbers
- DNS query ID (identification number)
- ToS (Type of Service)
- HTTP URL's
- Fragment offset
- TCP Flags
- Packet size
- Destination IP address
- DNS Qcount

Once the values of these parameters are flagged as "abnormal", the system transits into a signature optimization state that activates a closed-feedback loop mechanism.

Closed-Feedback Module

The closed-feedback module is responsible for creating the narrowest, but still effective, signature rule. Each one of the above parameter types can include multiple values, detected by the automatic signature generation mechanism. The closed-feedback module "knows" how to tailor these values through AND/OR logical relationships. The more "AND" logical relationships types that are constructed between different values and parameter types, the more accurate and narrow the blocking signature rule is considered to be.

In order to create the logical relationship rules between the detected signature values, the closed-feedback module uses the following (but not limited to) feedback cases:

- **Positive feedback**: The traffic anomaly was reduced by using the blocking signature rules created by the module. The system continues to use the same action, and tailors more attack characteristic parameters (i.e., signature types and values) through as many "AND" logical relationships as possible.

- **Negative feedback**: The degree of traffic anomaly was not changed, or was increased. The system stops using the last blocking signature rules and continues to search for more appropriate ones.

- **Attack stopped feedback**: If the attack stops, then the system will stop all countermeasures immediately (i.e., remove the signature rule).

The main advantage of the system described above is the ability to detect statistical traffic anomalies, create an accurate attack signature based on heuristic protocol information analysis in real-time, and mitigate the attack.

Advanced Action Escalation Technology

This mechanism works in conjunction with the real-time signature and closed feedback modules.

The main idea behind this escalation approach is to first detect suspicious users through the real time signature generation module, and second, to start and activate a set of actions beginning with the most "gentle" one that will have negligible, if any, impact on the legitimate user. Based on a closed-feedback loop, the system will decide if escalating to a more aggressive action is required.

The approach aims to minimize the impact on the human user experience while presenting a more accurate and adaptive response to the artificial users, like a bot. This automatic process allows the system to automatically tune the counter-measure's actions based on the detected level of risk. This dynamic action per level of risk also improves the protection system resistance against reverse engineers.

Radware's attack mitigation action escalation allows the system to adapt its action to the ongoing risk, which provides automatic risk management as intended by the network and application security expert (an expert system that emulates the human security expert's decision process in real time).

Advanced Action Escalation Process

At this stage, the system starts to enforce counter measure actions in order to accurately mitigate the attack. Actions apply to the suspicious users only (those that match the RT signature).

As mentioned before, the advanced action escalation technology is designed to minimize the impact on the human user experience, while presenting a more accurate and adaptive response to the uses behind the detected threat.

The action escalation mechanism will initiate a set of actions, beginning with the most "gentle" one (e.g., a syn cookie) that will have negligible, if any, impact on the legitimate user (in case the user was accidently matched to the RT signature. Based on the closed-feedback loop mechanism, the system will decide if an escalation into a "stronger" action is required. The following is a more specific example for this mechanism:

a. The mitigation engine only intercepts the sessions which originate at the suspicious source and replies back with a "weak" challenge option. A weak challenge can be considered a redirect HTTP command that forces real browsers to re-initiate their requests automatically. A simple bot will fail to respond correctly;

b. If the suspicious source responds correctly but continues to generate suspicious activities, it means a more advanced tool is behind the operation. If not, then the suspicious flags that were raised were probably false alarms and the human user will be able to continue his activity on the site;

c. The mitigation engine raises the level of the challenge to include some customized JavaScript that forces the suspicious user to download and process the object. Most of the advanced bot tools will fail to respond correctly, and will be blocked;

d. In case the user responds correctly and suspicious activities are still identified, then the system can either generate a rate limit rule or a full blocking rule. In any case, the action will apply only to users who match the RT signature.

The main benefit of this process is that it allows an accurate mitigation process with minimal impact on the user experience. It also presents an adaptive response aimed at dealing with the dynamic nature of behavior types that today's and tomorrow's attackers may choose to use. Finally, most actions described above do not require the human user to go through any disruptive tests.

An illustration of the closed-feedback loop mitigation process can be seen in Figure 8 below:

The above actions show how Radware's attack mitigation solution is used against HTTP-based attacks. Other mitigation options will be used if other types of attack are detected (e.g., UDP based attacks, DNS attacks etc), but the goal is to follow the closed-feedback loop and action escalation mechanism, which ensures minimal impact on the user experience while maintaining a high level of effectiveness in mitigating the emerging threats.

Deterministic Security Technology Modules – IPS Module Technology Overview

Until now, we have described Radware's behavioral-based engine, however, even today, many threats simply violate stateful protocol rules, applications rules, or are exploiting known application vulnerabilities. These threats can be precisely removed through a pre-defined attack signature that was the developed by vulnerability research groups, or by enforcing deterministic protocol compliancy rules. For these purposes, the following deterministic security technology is deployed in DefensePro:

A security device that combines IPS signature-based approaches with advanced behavioral technology will have an advantage over signature-based technology alone.

Security Update Subscription - Radware's Security Operations Center (SOC)

For the more deterministic threat types, such as known application vulnerability exploitation attacks in which a signature is already available, Radware's attack mitigation solution provides a proactive security update service that automatically downloads recent attack signatures to the system's attack database. Radware's on-premise attack mitigation device – DefensePro - inspects the traffic and compares each packet in real time to the signatures in the database. Radware's hardware-accelerated string match engine is used for this purpose.

Radware's 24x7 Security Operations Center (SOC) provides subscribers with an automated, weekly delivery of new attack signature filters as well as emergency and custom delivery of signatures. This ensures that networks and applications are fully protected from current known vulnerabilities.

Radware's SOC comprises of a group of security experts that constantly monitor networks and applications for vulnerabilities, participate in security forums and discussion groups, and deploy honey pots to discover new attacks. Radware's SOC performs research for the newly discovered vulnerabilities and attacks which result in a weekly signature database update. In the case of an urgent attack situation, an update will be issued on the same day. Each signature database update is fully tested on real customers' networks, utilizing devices deployed as beta staging. The signatures are tested against real world traffic to eliminate false-positives.
For more information on latest threats SOC resources, please visit the Radware security site:
http://security.radware.com/

Radware's vulnerability-based attack database includes the following attack categories:

- **Known Attack Tools** – Protection against known availability attack tools which generate an abnormal signature or anomalous traffic behavior.
- **Web servers** – Protection against attacks targeting common web server application including IIS and Apache. The attack signatures protect against application level vulnerabilities, SQL injection and cross-site scripting.
- **Mail servers** – Protection against POP3, IMAP, and SMTP protocol vulnerabilities and mail application vulnerabilities.
- **DNS** – Service protection against DNS protocol and DNS server applications vulnerabilities.
- **FTP** – Service protection against FTP vulnerabilities.
- **Databases** – Protection for database servers such as Oracle and SQL.
- **Telnet and FTP** – Protection against Remote access protocol vulnerabilities and FTP/Telnet server implementation vulnerabilities.
- **SIP** – Protection for SIP servers, proxies, and IP phones against SIP protocol violations preventing shut downs, denial of service, and malicious takeovers.
- **Network malware protection** – Protection against worms, Trojan horses, spyware, and backdoor attacks.
- **Botnets protection** – This protection includes a solution to detect and block known communication control channel of the botnets.
- **Infrastructure vulnerabilities protection** – Protection for router and switch operating systems' vulnerabilities including Cisco, 3Com, Juniper, and more.
- **Anonymizers** – Prevention from users within a given network to use anonymizers.
- **Phishing** – Detection and prevention of malicious attempts to redirect users into phishing dropping points for known and legitimate e-commerce and banking sites.
- **IPv6 attacks** – Protecting against IPv6 protocol vulnerabilities.
- **SSL-Based Attacks** – Protection against encrypted, SSL-based attacks.

Hardware Architecture "Tailored" for Attack Mitigation

Each layer and module of defense in Radware's attack mitigation solution is supported by hardware architecture that was designed to maximize the protection performance.

DME – DoS Mitigation Engine

The DME is a dedicated network processor that was optimized to perform L3 and L4 filtering operation at a rate of 12 Million PPS.

SME – String Match Engine

The String Match Engine is a hardware ASIC-based component that supports the IPS module. The solution is capable of multi-gig L7 (application layer), and deep packets for full content inspection. This includes inspection of attack signatures that span across multiple packets (i.e., support cross packet inspection), or inspection attack signatures that can only be written through regular expressions in order to avoid false positive or false negative events.

Multi-purpose CPU's

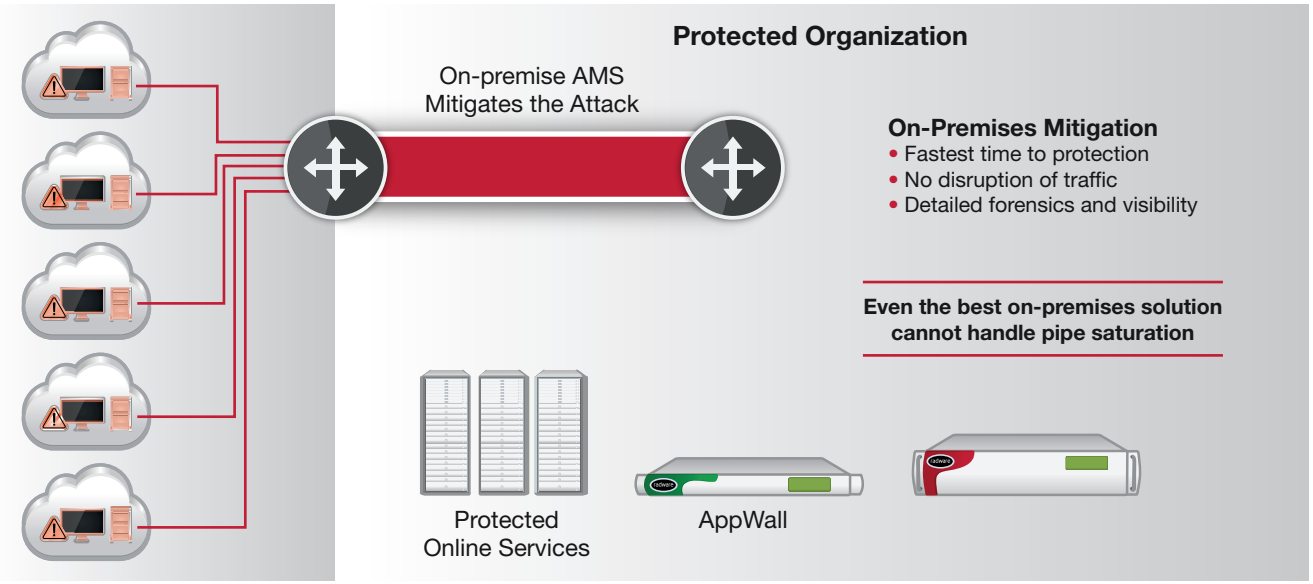
The other protection layers and network-based operations are performed by multi-purpose CPUs, which provide the required flexibility and scalability for the more standard operations, such as stateful and statistical analysis, and are part of the behavioral analysis modules.

The main advantage of Radware's attack mitigation hardware architecture is its ability to completely separate the mitigation tasks, each one in a different dedicated hardware component, thus preventing internal resource "cannibalization" that typifies other attack mitigation products. Mitigating the multi-million PPS L3-4 DDoS attack is done solely by the DME hardware component, while attacks that need to be mitigated through DPI (Deep Packet Inspection) utilizes the L7 Regex acceleration ASIC. At the same time, legitimate traffic that should continue to be processed by the stateful analysis modules and feed the statistical analysis modules in the system is being processed by the multi-purpose (multi-cores) CPU's.

This hardware architecture provides higher and more predictable performance figures than other attack mitigation systems.

Radware's Cloud Scrubbing DDoS Mitigation Service (DefensePipe)

When a high volume attack threatens to saturate the organization's Internet link to their service provider, even the most sophisticated on-premise attack mitigation system will not be able to mitigate it because the problem is at the service provider's side.



Radware's cloud scrubbing service, DefensePipe, is based on a network of data centers built by Radware and provides cloud-based protection against pipe saturation DDoS attacks. It is delivered as part of Radware's attack mitigation solution - the industry's first hybrid attack mitigation solution, and is enabled only when the service provider's link is at risk. All threats which are not related to pipe saturation are stopped immediately and most accurately by the on-premises attack mitigation device.

Radware's Cloud Scrubbing Service includes several key elements:

- Identical Technology to CPE – Radware's cloud scrubbing data centers are equipped with high capacity attack mitigation devices which are identical to the on-premise attack mitigation devices (CPE). This enables high technological integration between the cloud and CPE and results in the fastest cloud mitigation time and accuracy.
- Defense Messaging Information Sharing – The cloud receives 3 types of information messages from the CPE:
  - Traffic Statistics and Protection Baselines - including the required configuration and learned behavioral statistics required to activate mitigation with the same level of information available to the CPE inline protection modules.
  - Attack Alerts - which provides Radware's Emergency Response Team (ERT), and the customer, a single view for full situational awareness of the detection status in the cloud and CPE.
  - Health Check - from the cloud to the CPE is generated continuously. The application response time is measured such that the cloud monitoring system is aware of the application performance status at all times and can activate with complete independence in the CPE.
- ERT Monitoring – Radware's cloud scrubbing service offering includes Radware ERT monitoring of the customer environment and engagement on pipe saturation risk such that when a high volume attack starts, a Radware ERT security expert is already in contact with customer operatives and traffic is already diverted to the cloud.

Traffic Diversion Capabilities

Radware's cloud scrubbing service supports several traffic diversion options, including the use of BGP or DNS diversion techniques to enable safe, hands free and secure traffic diversion to the cloud. BGP diversion is pre-setup such that the diversion procedure is independent in the availability of the CPE network or personnel resources. Secure failover DNS diversion allows for customers who do not own an Autonomous System Number, to divert their traffic to Radware's cloud while eliminating vulnerability to direct attacks on the protected IP address.

Global Network of Scrubbing Centers

The ever-expanding network of scrubbing centers has a global footprint, allowing for the optimal routing path towards the protected organization while also having the capacity to mitigate the largest attacks recorded to date.

The Web Application Firewall Module

Radware's WAF module secures web applications and enables PCI compliance by mitigating web application security threats and vulnerabilities. It prevents data theft and manipulation of sensitive corporate and customer information.

The WAF module provides protection against the following web application attacks:

- **Full coverage out-of-the-box of OWASP top-10 threats** – Including injections, cross site scripting (XSS), cross site request forgery (CSRF), broken authentication and session management, and security mis-configuration.
- **Data leak prevention** – Identifying and blocking sensitive information transmission, such as credit card numbers (CCN) and social security numbers (SSN).
- **Zero-day attacks prevention** – positive security profiles limit the user input only to the level required by the application to properly function, thus blocking zero day attacks. Positive security profiles are a proven protection against zero-day attacks.
    a. **Protocol validation** –enables HTTP standards compliance to prevent evasion techniques and protocol exploits.
    b. **XML and Web services protection** – offers a rich set of XML and web services security protections, including XML validity check web services method restrictions, XML structure validation to enforce legitimate SOAP messages, and XML payloads.
    c. **Web application vulnerabilities** – signature protection offers the most accurate detection and blocking technology of Web application vulnerability exploits. Radware WAF's negative security profiles offer comprehensive attack protection.
    d. **Normalization and Decoding** – HTTP traffic is decrypted, normalized and decoded such that the content is interpreted as the HTTP application will have interpreted it. Encoding capabilities include SSL, percent encoding, base64, HEX, and more. This enables the WAF to prevent attacks even when encryption, decoding, and obfuscation are used in order to evade common detection systems.

Radware's WAF module is based on positive and negative security policies:

- Positive security policies are based on behavioral analysis technology. The security technology learns what the possible inputs per each web page are and what the typical values per each input field are. It then locks the policy to the allowed ranges of values.
- Negative security policies are based on static signature detection technology. The WAF module stores a signature file that covers thousands of known application vulnerabilities and exploits that are checked against every user transaction. Once a signature match is found – the session is terminated and the attack is blocked.

Activity Tracking

The Activity Tracking module counts the HTTP transaction rate to the defined application scope (domain/folder/page) per user per second. Once reaching the threshold, a security page is returned instead of the requested resource.

The Activity Tracking module can be set to one of two tracking modes:

- **IP-based tracking**. This is a non-intrusive functionality which is available both in Passive and Active modes. Thus supported both in an inline AppWall Gateway deployment mode and in Out-of-Path Monitor mode.
- **Device Fingerprint-based tracking**. This is an intrusive functionality which is available only in Active mode and supported only in an inline Gateway deployment.

While IP-based tracking offers the value of non-intrusive activity tracking and detection capabilities, device fingerprint-based tracking offers IP-agnostic source tracking. AppWall can detect sources operating in a dynamic IP environment and activity behind a sNAT (source NAT), such as an enterprise network or proxy. Even if the bot dynamically changes its source IP address, its device fingerprint does not change. AppWall tracks the device activity and correlates the source security violations across different sessions over time.

Device fingerprint technology employs various tools and methodologies to gather IP-agnostic information about the source, including running a JavaScript on the client side. The device fingerprint uniquely enough identifies a web tool entity by a combination of the operating system and the browser attributes. Once the JavaScript is processed, an AJAX request is generated from the client side to AppWall with the device fingerprint information.

When Activity Tracking is set to IP-based tracking, it can be correlated with the IP blocking module. Once a source IP reaches a configured threshold, the source IP is blocked (either Layer 3 or Layer7).

To prevent scenarios where AppWall mistakenly detects search engine bots (Google, Yahoo, etc) as malicious bots, there is a mechanism in AppWall that detects and verifies legitimate search engine bots by running a reverse-DNS lookup process to verify their source and to excluded them from the list of tracked sources.

Auto Policy Generation

The WAF module offers patent-protected technology to create and maintain security policies for the widest security coverage with the lowest false positives and lowest operational effort. The WAF module uses a four step flow to create and maintain security policies:

Step 1 – Application mapping
The WAF model learns the web application and maps the application pages into application zones or paths. For example, admin pages are allocated into an admin application path, dynamic content pages are allocated into another application path, registration pages into a third application path, etc. The application mapping is performed passively or actively using an embedded web crawler.

Step 2 – Threat Analysis
Once the WAF module has completed the application learning and mapping, it performs a risk analysis per each application path. The result of the risk analysis is an association of relevant web threats per path. For example, an admin path should be protected against attacks that aim to steal user information, create false user accounts or tamper with user account data; the dynamic application-path should be protected against buffer overflow attacks that could lead to remote code execution, unexpected application behavior, and full system compromise.

Step 3 – Policy Generation
In this step, the WAF module automatically generates granular security policies per each application path. Typically, admin paths and static pages paths will be assigned with negative security policies, while dynamic content application-paths will be assigned with positive security policies.

Step 4 – Policy Activation
The last step is used to optimize the security policies to maintain maximum coverage while reducing false-positives and improve the system performance. The WAF module optimizes the negative security policies (based on application vulnerability signature detection technology), by learning what attacks the application-path is vulnerable to, and removes unnecessary signatures. The result is full-attack coverage while reducing false-positives due to non-relevant signatures. For the positive security policies, the WAF module performs the parameter inspection and learning per field in every application page. Once learning is completed it locks the learned values, and any parameter value exceeding the learned ranges will be detected as an attempt to attack the application.

App Mapping → Threat Analysis → Policy Generation → Policy Activation

SHORTEST TIME TO PROTECTION

Only **1 week**
For known attacks

50% FASTER than other leading WAFs

BEST SECURITY COVERAGE

Auto threat analysis
No admin intervention

OVER 150
Attack vectors COVERED

LOWEST FALSE-POSITIVES

~0 False positives

THROUGH

Auto-optimization of out-of-box rules

SECURITY ASSURANCE

Automatic detection of web application changes ensuring security

THROUGHOUT THE APPLICATION'S DEVELOPMENT LIFECYCLE

POST-DEVELOPMENT PEACH OF MIND

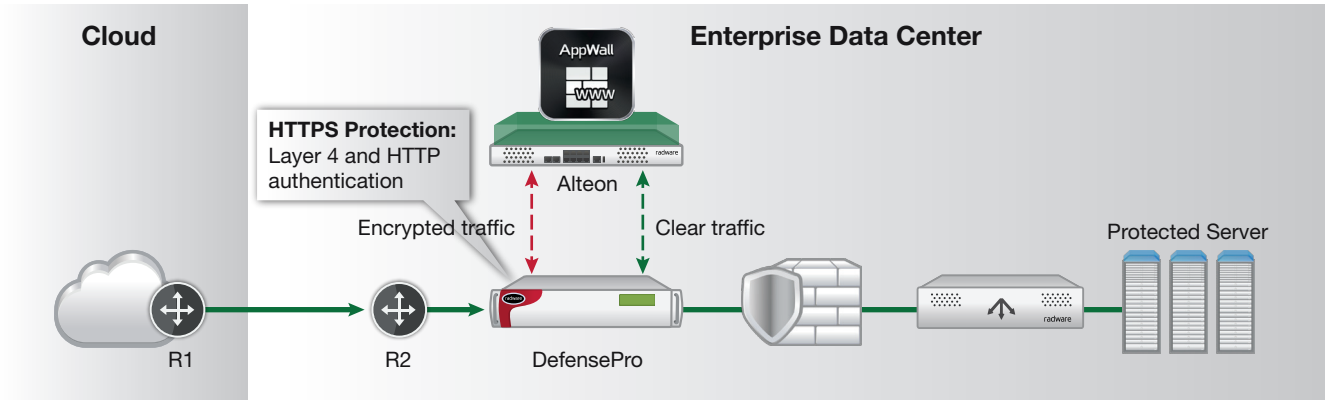
Radware SSL Attack Mitigation

Provisioning of encrypted applications involves three infrastructure layers. Each of the layers is vulnerable to a different set of attacks and is therefore optimally protected by a different set of tools. Any breakage in the toolset or a failure to protect one of the layers breaks the entire chain:

- The TCP Layer is vulnerable to network infrastructure and server attacks which are described in the previous sections. It is important not to expose the system to such attacks while trying to protect from other layers' threats.
- The SSL Layer is inherently vulnerable to session saturation and renegotiation attacks due to the protocol structure which requires more compute resources from the server than from the client in any session creation. Moreover it is vulnerable to SSL related protocol anomaly attacks and implementation vulnerabilities.
- The Encrypted Application Layer is vulnerable to application layer floods, application protocol and non-vulnerability attacks and application vulnerabilities as described above.

Off-Path Unique SSL Deployment

Radware's SSL solution is deployed using Radware-patented SSL DDoS protection technology which enables the SSL decryption agent to be off-path and triggered only when suspicious activity starts. This unique deployment model enables a solution which introduces zero latency in peace time and minimal latency under attack – only on the first session per each client. The deployment also doesn't require Radware to act as the SSL termination point and may be supported in asymmetric deployment environments where ingress only traffic flows through the solution.



DefensePro – Deployed inline as a perimeter security device. Connected to both data-path and Alteon.

Alteon – Deployed in parallel to DefensePro without direct access to the network. Connected to DefensePro with two physical ports.

AppWall – Deployed within Alteon physical appliance in OOP mode, with a copy of traffic for deep analysis.

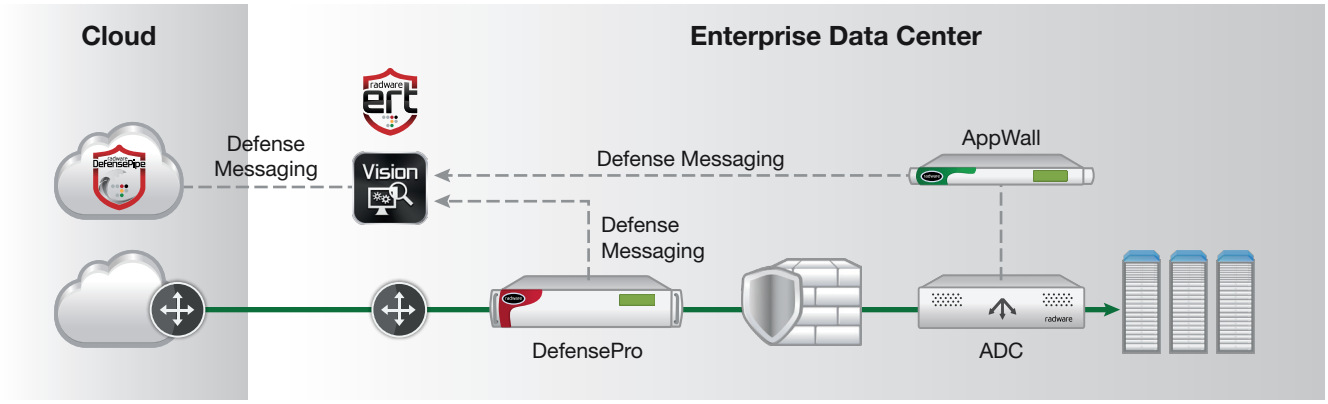
Complete SSL Protection

Radware's SSL mitigation solution includes the following components:

- TCP Attacks Protection includes Radware behavioral network protection described above, TCP state saturation attacks protection, TCP challenge response mechanisms and TCP vulnerabilities and anomalies protection.
- SSL Vulnerabilities Protection includes SSL renegotiation attacks protection, state and session saturation protections, and SSL vulnerabilities protection signatures.
- Encrypted Challenge Response Technology includes protection from HTTP floods and botnets. The HTTP challenge includes the capability to thwart advanced tools, ones which are able to overcome standard challenge response mechanisms.
- Encrypted Applications Signature Protections are applied to application traffic and protect from known attack tools and application vulnerabilities.
- Encrypted web application protection enables negative security while it applies decryption, normalization and decoding of application traffic – thus enabling complex known attacks protection. Positive security is applied by learning normal application behavior and patterns and enables zero-day web application protection.

A Truly Integrated System – Defense Messaging

Defense Messaging is a communications method developed by Radware which enables the different elements in Radware's attack mitigation solution to operate as a single system. This capability allows Radware's solution to apply the optimal detection technology deployment and maintain the ability to mitigate attackers at high performance and then push attackers to the perimeter of the network. There are several cases in which this capability becomes crucial to the successful mitigation of complex and multi-vector attacks.



The following table describes the different messaging types and the actions they trigger in the receiving module:

Threat	Source	Destination	Message Type	Action
Encrypted/ Encoded/ Obfuscated HTTP Attacker	WAF	DefensePro	Misbehaving L3 IP	Dynamic black list
CDN/Proxy Originating Attack	WAF	DefensePro	Misbehaving L7 IP (X-Forwarded-For/True-Client-IP)	Dynamic L7 signature
DNS Violation	Alteon	DefensePro	Misbehaving L3 IP	Dynamic black list
SSL Violation	Alteon	DefensePro	Misbehaving L3 IP	Dynamic black list
Link Saturation	DefensePro	DefensePipe	Link Utilization	Traffic diversion
Any	DefensePro	DefensePipe	Attack Alerts	Reporting and situational awareness
Link Saturation	DefensePro	DefensePipe	Configuration and Baselines Update	Baseline and configuration update
Link Saturation	DefensePipe	Protected Assets	Health Check	Traffic diversion

Radware's Application and Security Management System (APSolute Vision)

Security Management, Monitoring, Reporting, and SIEM Engine

Radware's management system, APSolute Vision, provides a highly available, single point-of-access for network and security administrators to centrally manage distributed Radware devices and monitor the health, real-time status, historical security trends, performance, and security of enterprise-wide application delivery infrastructures. Available as both a hardware appliance and a virtual appliance, the system consolidates the monitoring and configuration of several Radware devices across multiple data centers. By removing the need for deploying management appliances in multiple data centers, it reduces IT CAPEX and OPEX, and simplifies data center management.

APSolute Vision continuously monitors the system and will send an alert if there is any degradation of business continuity or performance across the entire infrastructure. It provides the following benefits:

- Up-to-date information, and improved business continuity service.
- Effective application delivery and security capacity planning.
- Shorter time frame required to resolve business continuity issues.
- Minimized impact of service downtime on the enterprise's business.

Radware's application and security management system is a specifically tailored unified management and monitoring application for application delivery and network security devices. It supports all aspects of management: initial device setup, ongoing maintenance, SSL certificate management, reporting, forensics, workflow automation, interoperability via REST API and more. It also provides central storage of vital device information, allowing IT managers to easily find hardware platform details, software versions, serial numbers, and more. This eliminates manual tracking of critical device information and reduces errors.

Real-Time Threat Identification, Prioritization, and Response

Radware's management system provides an enterprise-wide view of security and compliance status from a single Web-based console. Data from multiple devices is collected and evaluated in a consolidated view of dashboards and reports. These reports—viewable from a secure portal or exported in HTML, PDF, CSV, etc.—provide extensive, yet simple, drilldown capabilities that allow users to easily access information in order to expedite incident identification and provide root cause analysis. This improves collaboration between NOC and SOC teams, and accelerates the resolution of security incidents.

The system provides real-time monitoring and alerts on policy violations, non-standard processes, rogue applications, potential financial fraud, identity theft and cyber-attacks. Intuitive visualization allows rapid resolution and focusing on urgent issues. For example, the Current Attack Table View presents visualizations that represent attacks by frequency, category, severity, etc.

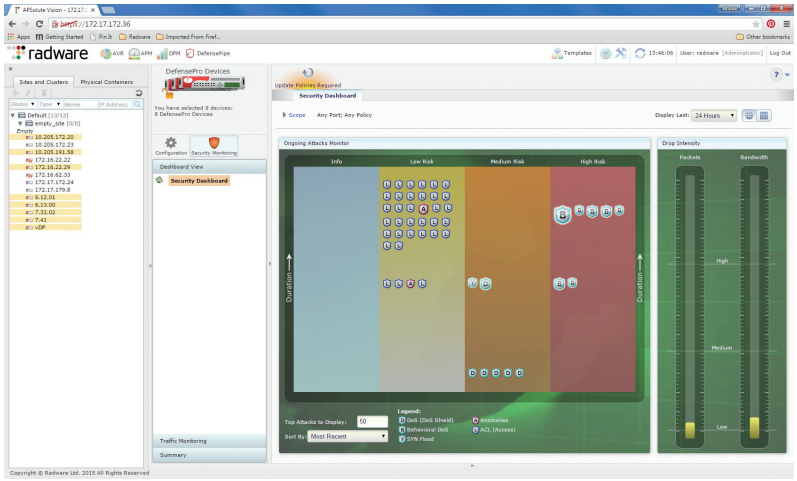


Figure 12: The real-time dashboard view allows you to see current attacks in your network. High risk attacks are located closer to the red risk zone. The drop intensity meters indicate the packet and bandwidth drop rate of attack traffic.

Per User Dashboards and Report Customization

Radware's management system allows users to fully customize real-time security dashboards and historical security reports. This allows for security trend detection and ensures a complete network security view at-a-glance, both of which provide the specific information needed to take action and reduce the amount of drill-downs required to access information. Security data can be exported into HTML, CSV and PDF formats and can be provided as comprehensive reports.

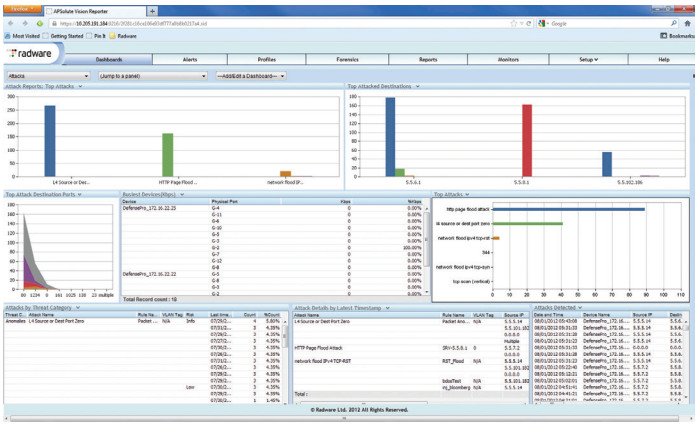


Figure 13: The security dashboard displays multiple attack reports in a single view, customizable per user.

Advanced Security Forensics Engine

Radware's application and security management system provides an easy-to-use search engine that allows users to quickly sort through large volumes of archived log, vulnerability, and attack data. Forensics analysis helps users isolate attack vectors, investigate security breaches and position appropriate defenses in place by detecting anomalies, identifying policy violations, and displaying a chronological order of malicious activity.

Flexible Role-Based Access Control (RBAC)

Customer's data center / network operations and security teams may consist of different user roles requiring different access levels to the security event information and reporting. For example, SOC and security admins need fine-grain level of security events data, but top-level management prefers a high-level trend summary, while specific service / app / tenant owners must gain access only to policies and events related to their tenant.

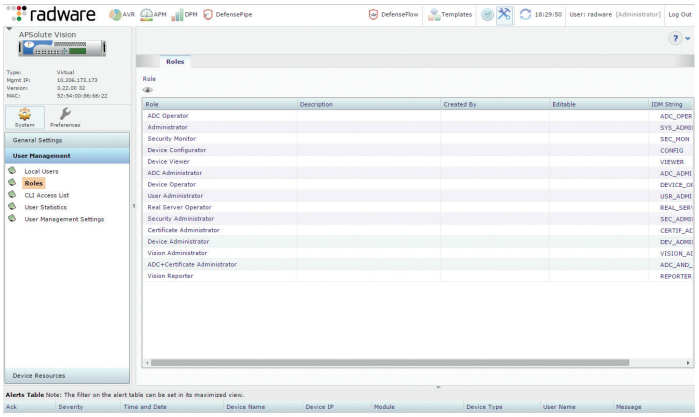


Figure 14: APSolute Vision Role Management Page

APSolute Vision provides a complete role-based access control (RBAC) approach which allows for the assignment of different users with different authorization levels. APSolute Vision's RBAC capabilities extend to scope (devices / sites / clusters), role (features available to a specific user e.g. configuration, monitoring, scheduling, etc.), as well as protection policy level authorization. In addition, the solution allows for integration with external user repository systems including RADIUS and TACACS+ in order to apply RBAC on customers' existing user entities.

Complete Alignment with Enterprise Compliance Requirements and Regulations

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

Through enhanced role-based access and logging capabilities, the system ensures all actions across the application delivery and security infrastructure are logged and performed only by authorized personnel.

Radware's management system segregates statistical and performance data to support job-specific views, dashboards, analysis, and reporting. While executives may desire a view of high-level summary reports, IT professionals can easily drill down into more complex monitoring, reporting, and forensics detail.

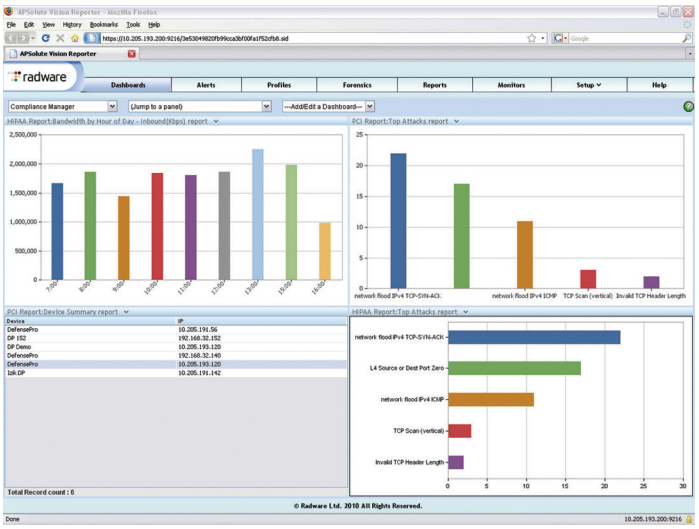


Figure 15: Create job specific dashboards, such as a compliance manager dashboard containing compliancy information on different regulations.

Summary: Wider, Faster, Broader Protection

Cyber activists and motivated attackers are more sophisticated and initiating multi-vulnerability attack campaigns that make mitigation very difficult. No single protection tool is fully effective against the broad range of attacks that can target every layer of the IT infrastructure – the network layer, the server layer, and the application layer. With Radware's Attack Mitigation Solution, online businesses, data centers, and service providers can ensure the security of their online presence and maintain productivity, along with the following solution benefits:

Hybrid Solution Offering the Widest Protection Coverage

- On-premise perimeter attack mitigation device detects and mitigates the full range of attacks, including network and application layer attacks, SSL-based attacks, and low & slow attacks.
- Cloud scrubbing service mitigates volumetric attacks that are beyond the Internet pipe capacity.

Highest Accuracy of Detection and Mitigation

- Minimal false positives with patent-protected behavioral analysis technology.
- Real-time signatures and selective challenge-response mechanism for high mitigation accuracy.

Shortest Mitigation Response Time

- All attacks are detected on-premise in real-time. No need to wait for traffic diversion to start mitigation.
- Protection starts in seconds – shortest time to protect in the industry.
- Dedicated hardware guarantees best quality of experience to legitimate users.
- Traffic is diverted only as a last resort.

Complete Solution from a Single Vendor

- Radware's Emergency Response Team security experts fight the attack during the entire campaign.
- Single point of contact. No need to work with multiple vendors or services.
- Available as a fully managed service for simple, easy deployment.
- Integrated reporting with historical reporting and forensic analysis.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.

© 2015 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.