radware

Cloud vs. On-Premise Security

Striking a Balance for Optimal Protection

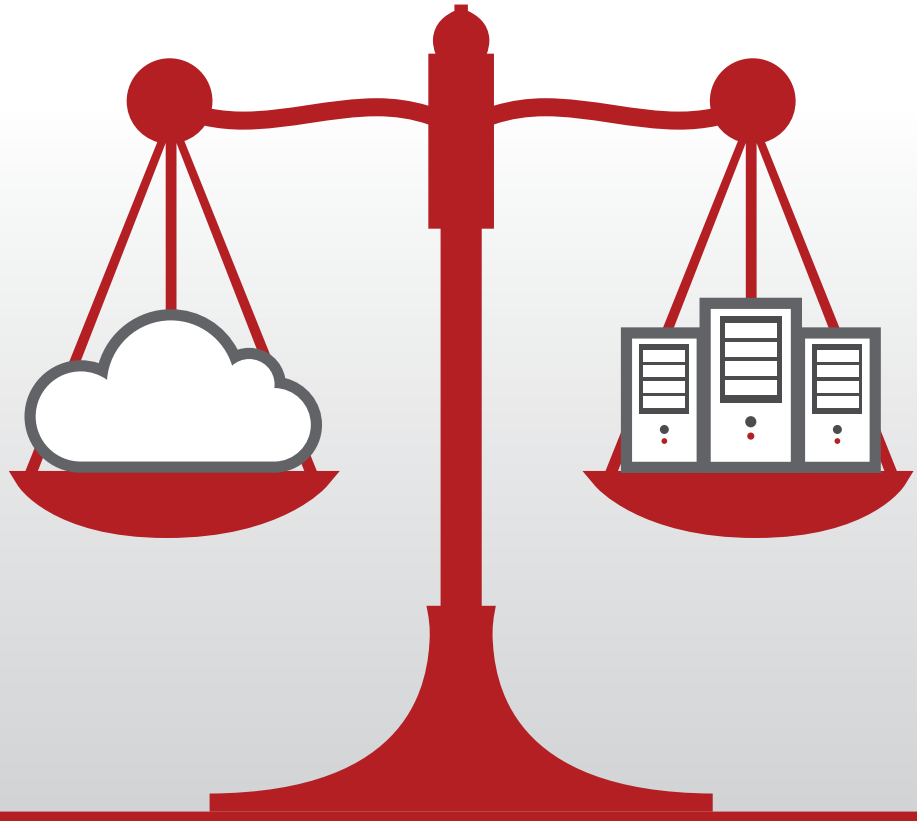
Cloud vs. On-Premise Security

Striking a Balance for Optimal Protection

Introduction

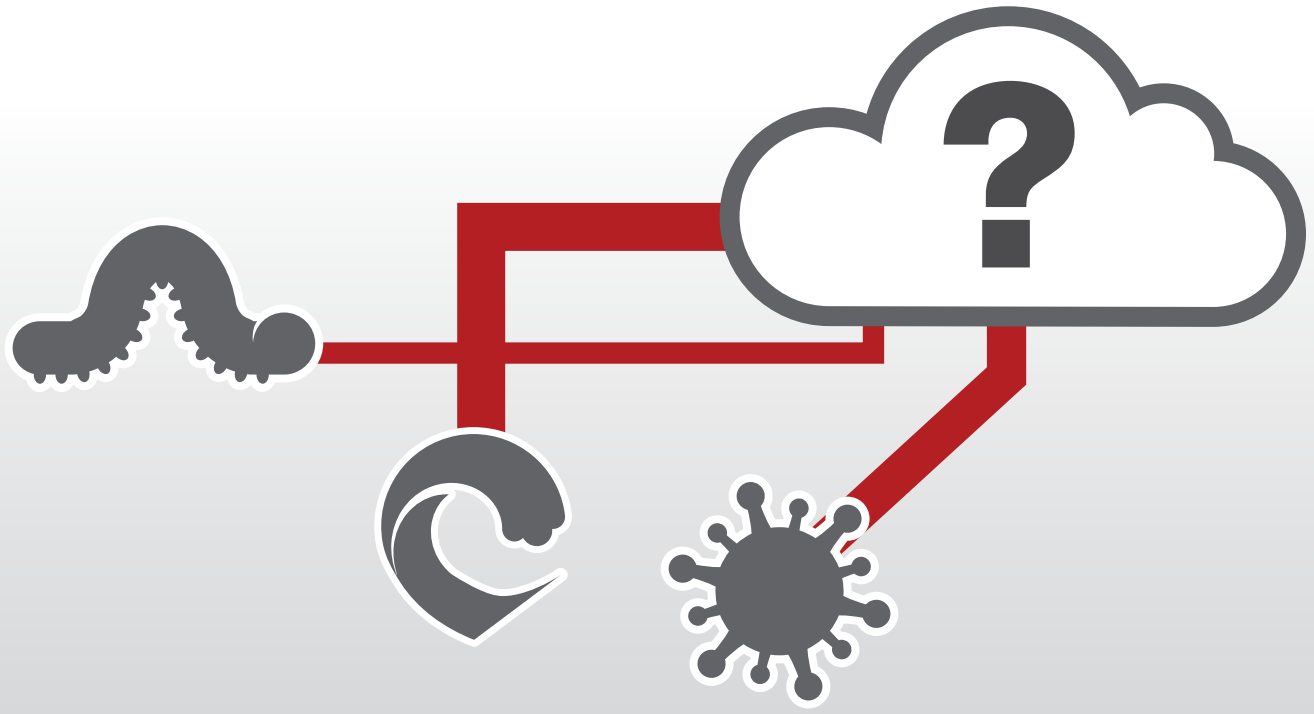
There is an important trend in security that looks to cloud-based resources to help mitigate the rise in virulent cyber-security threats. It is driven in part by the same motives spurring a shift in moving applications, computing and storage functions to the cloud; namely cost effectiveness and reduction in infrastructure management complexity. However, the movement to cloud often creates its own infrastructure management challenges. And in the case of security, it can lead to less than ideal architectures for managing the growing array of threats.

For information security professionals and organizations where strong security is the core requirement, it is critical to consider the common shortcomings of these cloud-only architectures (both on-demand and always on models) and understand the benefits of leveraging cloud and other deployment models.



Why Cloud Isn't ***Always*** the Answer

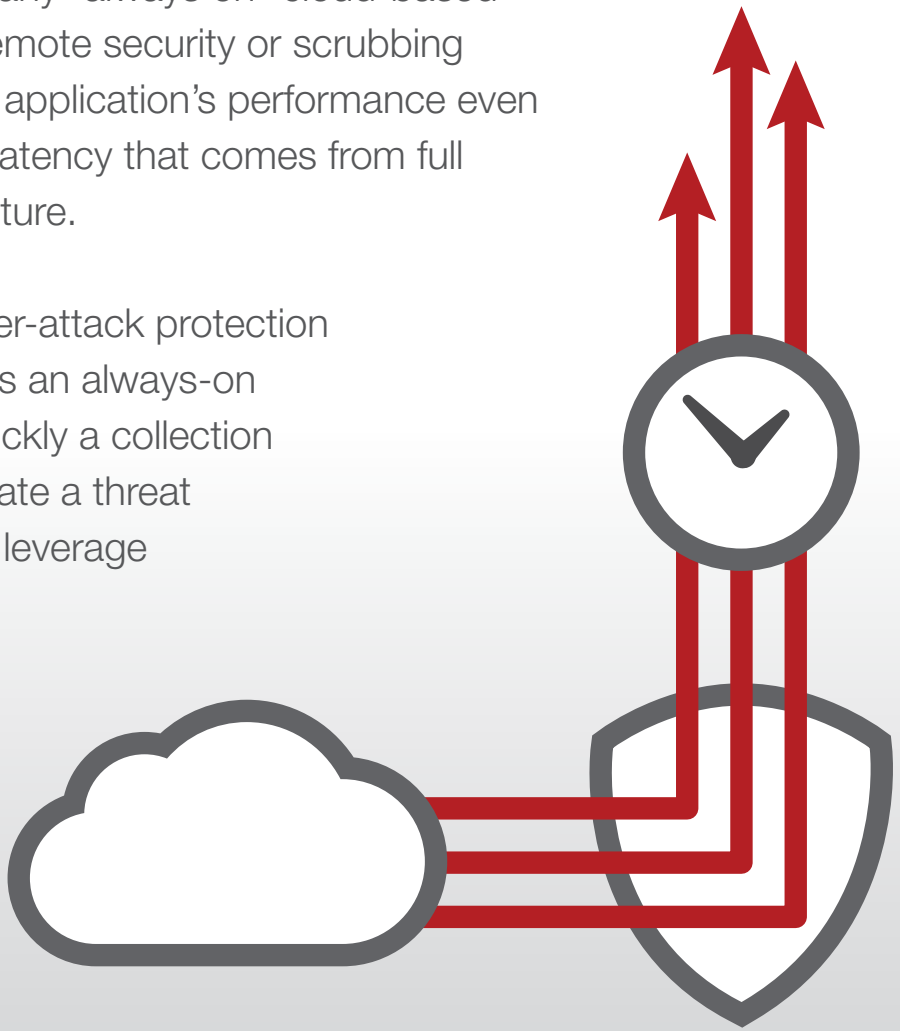
Influenced by today's headlines of mega-sized attacks, some organizations mistakenly conclude that the cloud is the best solution for complete cyber-threat management. While cloud-based resources, such as third-party scrubbing centers, play an important part in a comprehensive security strategy, there are some inherent limitations that make it less than optimal for teams looking for complete protection.



Risks of Redirection

The motivation to quickly move potentially malicious traffic away from networks and application infrastructure to an outside resource is logical, but comes with some implications that warrant consideration. First, many “always on” cloud-based resources require full-time redirection of ***all*** traffic to remote security or scrubbing centers. This can introduce non-trivial latency into the application’s performance even during peacetime. Many applications require minimal latency that comes from full management of the security and application infrastructure.

Another overlooked risk of cloud-only security for cyber-attack protection is the collateral risk. For providers delivering customers an always-on option only in the cloud, it’s important to note how quickly a collection of attacks targeting a growing customer base can create a threat against all customers. Alternatively, organizations that leverage cloud resources in conjunction with on-premises components incur none of these risks at peacetime and are able to better detect attacks that can be mitigated without having to swing traffic.

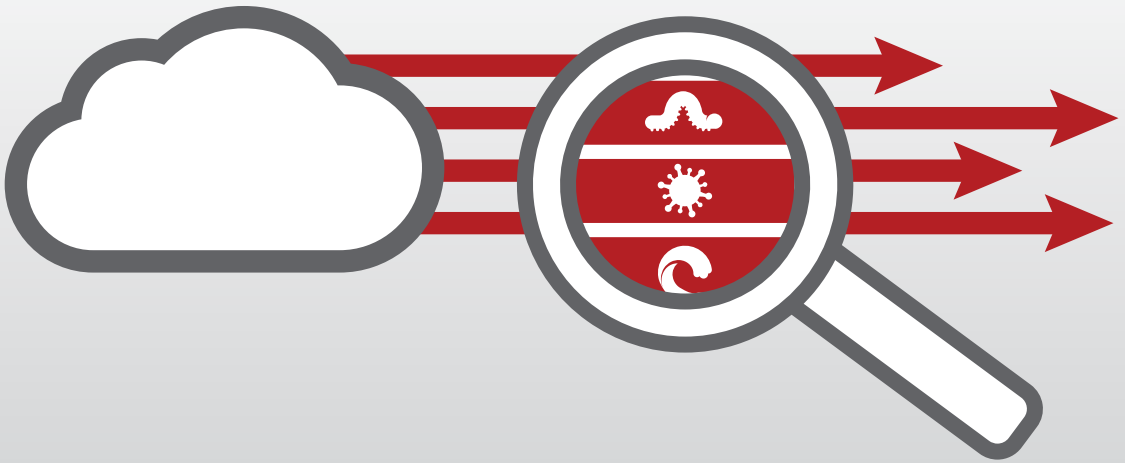


Detection in the Cloud

Speed and accuracy are top priorities of service providers looking for cyber-attack protection. For providers offering cloud only services, there are some challenges to ensure timely and accurate attack detection. Many solutions on the market are very specific about the various attack vectors its technology can block, but are generally less specific about how well it identifies and isolates these attacks from legitimate traffic. Over mitigation becomes a common problem with many solutions that cannot use a full view into normal traffic patterns to detect anomalies that warrant further inspection for potential malicious intent.

Additionally, cloud-based resources are trying to detect attacks by monitoring sample traffic flows from existing network monitoring tools, such as Netflow data. Typically, these solutions are simply detecting traffic patterns that exceed established rates and thresholds, rather than looking deep into the traffic for behavioral patterns that may signal an attack.

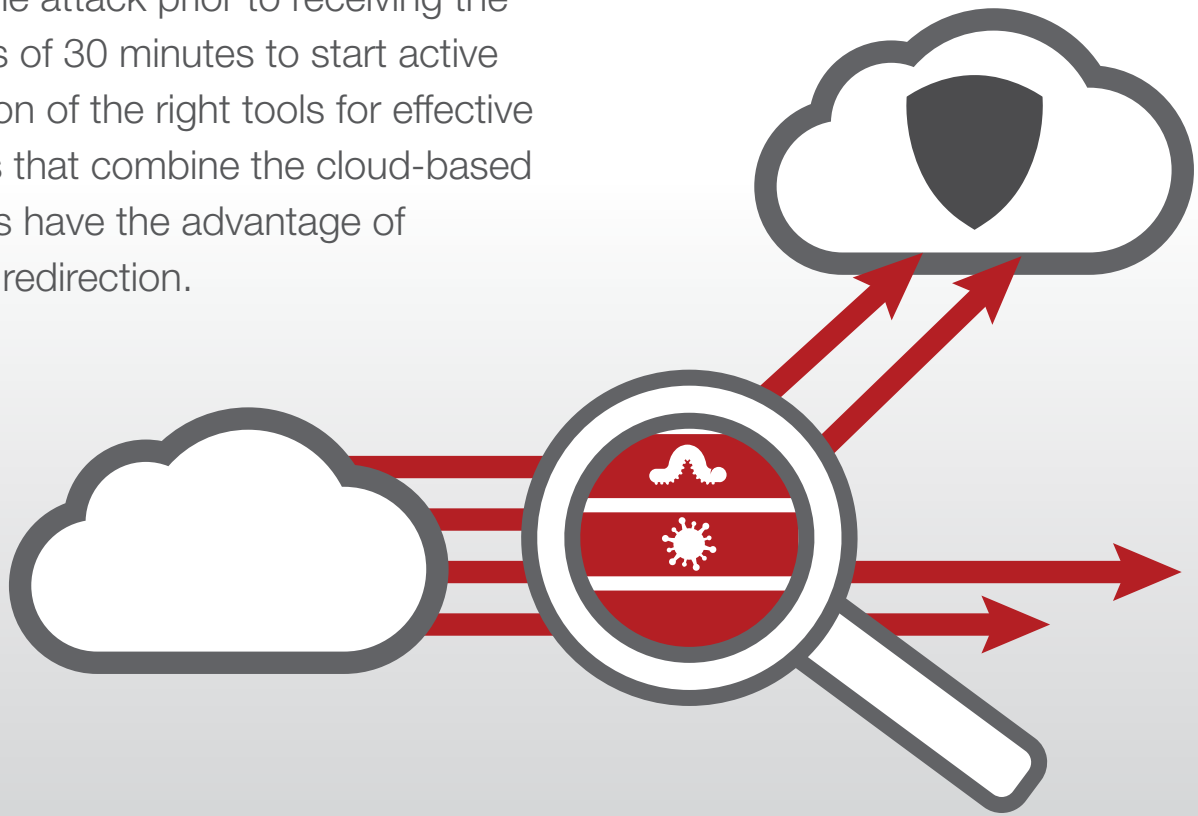
In the end, many cloud-only solutions leave the end customer with the burden of detection and having to make a trade-off between low thresholds for mitigation and low false positive rates.



Lack of On-Premises Limits Cloud View

There are very specific cyber-attack protection strategies that have proven to be more successful than others in defending against increasingly sophisticated adversaries. There is a focus on minimizing 'time to mitigation', the period of time it takes mitigation resources to fully understand the nature of an attack and apply the appropriate defense tactics. Many cloud-based defense offerings support a swing or redirection of traffic from the target resources to a scrubbing center for mitigation. However, without proper visibility into the attack prior to receiving the traffic, these services can take upwards of 30 minutes to start active mitigation and even longer for application of the right tools for effective protection. Conversely, hybrid solutions that combine the cloud-based resources with on-premise components have the advantage of attack visibility in advance of this traffic redirection.

Advanced hybrid solutions go a step further by supporting deep defense messaging between premise and cloud to share a full footprint of the attack and knowledge of already proven mitigation tactics for defense.



Most Effective Architecture for Trending Threat Vectors

One undeniable fact about the cyber-security threat landscape is that the attacks are rapidly evolving in order to stay ahead of many security technologies and thereby evade detection. The unending race between malicious actors and security professionals largely defines the risk profile of organizations and industries. To better defend against these powerful and dynamic threats, organizations need a thoughtful architecture to stay one step ahead.

There are two particular recent threat types that are trending and creating significant challenges for protection from cloud-only security solutions: Low & Slow attacks and SSL encrypted attacks.

Low & Slow attacks leverage targeted resource exhaustion, going after specific design flaws or vulnerabilities of a server or application with a relatively small amount of malicious traffic, eventually causing it to crash. “Low and slow” attacks mostly target application resources (and sometimes server resources). By nature, they are very difficult to detect because they involve connections and data transfers that appear at a normal rate. This creates significant challenges for cloud-only solutions that are either monitoring Netflow data levels or are engaged only when overall traffic rates exceed pre-determined thresholds.

Most Effective Architecture for Trending Threat Vectors

The use of SSL/TLS in applications to encrypt traffic and secure end-to-end data transit is on the rise. Many businesses now have a high majority of traffic and transactions occurring through encrypted sessions. The use of encrypted traffic in cyber-attacks is also on the rise, creating significant challenges for many security technologies in terms of computing and capacity, as well as simple visibility into the traffic for attack detection. Most attack mitigation technologies do not inspect SSL traffic, as it requires decryption of the traffic. HTTPS Floods—encrypted HTTP traffic floods are now frequently participating in multi-vulnerability attack campaigns. Compounding the impact of "normal" HTTP Floods, encrypted HTTP attacks add several other challenges, such as the burden of encryption and decryption mechanisms.

Cloud-only security solutions require end customers to share private keys and certificates in order to support decryption and inspection of potentially malicious traffic. This compromises the overall security posture of the customer and in many cases will violate compliance with certain security standards.

Where Cloud Fits into a Complete Architecture

Cloud-based security, much like cloud computing in general, is designed to reduce the complexity of virtualization and computing resource management away from the end user. In this regard, cloud-based resources should have a significant and meaningful role in a modern security architecture. The availability of cloud-based resources can support the need for organizations to tap into massive levels of capacity and computing power in order to defend against large attacks. It can also be leveraged to align with the ongoing migration of applications into cloud hosting environments.

With these two opportunities as a focus, here are two specific security architectures that capitalize on the benefits of cloud-based resources: hybrid attack protection and cloud security supporting application migration.

Hybrid Attack Protection

There is no longer debate over the ideal security architecture for providing protection from the wide array of threat vectors related to denial of service attacks. Leading analysts agree that the best solution is hybrid attack protection, a combination of on-premise and cloud-based mitigation technology that delivers immediate mitigation of non-volumetric attacks with the availability of additional mitigation resources in the event an attack threatens to saturate the Internet pipe. The market also agrees, with over one-third claiming to have implemented hybrid solutions and over half planning to do so by the end of 2015[1].

There are many benefits to a hybrid protection model. Primary among them is that it supports a “detect where you can, mitigate where you should” approach that ensures effective attack detection through visibility into all traffic, immediacy of mitigation, and outside volumetric support. However, not all hybrid solutions are created equal. Organizations should look very closely at the accuracy of detection and attack vectors covered in on-premises technologies. Expertise and capacity of cloud-based resources that defend against large volumetric attacks that require redirection to scrubbing centers should be considered. Single-vendor hybrid solutions that utilize identical technologies and teams for both on-premises and cloud-based protection have many benefits and advantages.

1 Global Application & Network Security Report 2014-2015, Radware
2 IDC Technology Spotlight, Sponsored by Radware, Optimizing DDoS Mitigation Using Hybrid Approaches, March 2015

IDC

Volumetric-based attacks remain the most common, more advanced hybrid attacks that include application layer and encrypted traffic and is spurring the growth of hybrid defense solutions. It integrates Layer 3 and Layer 7 on-premise detection devices with cloud signaling to mitigate DDoS attacks both in the cloud and on-premise. This represents a newer and more comprehensive approach that a number of organizations are beginning to consider[2].

Cloud Security Supporting Application Migration

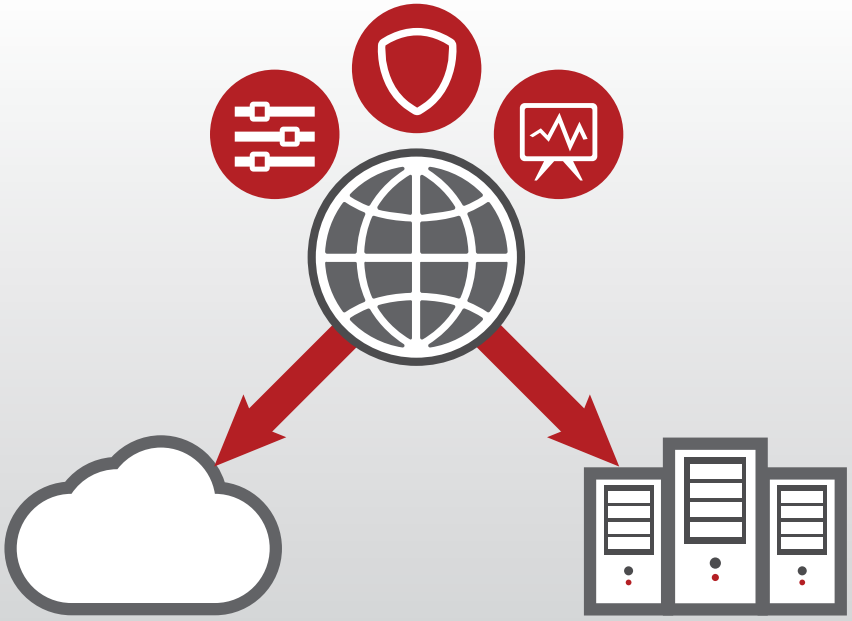
The migration of applications and computing resources into the cloud is well underway and rapidly accelerating. However, because of legacy business processes; legal, compliance, or resiliency reasons, complications from management and loss of real-time visibility, most businesses will not be able to completely eliminate IT infrastructure and rely solely on the cloud. As a result, organizations may evolve into a hybrid hosting environment, with applications and resources spread across multiple cloud hosting providers as well as its own data centers.

This hybrid hosting environment creates many challenges for security teams:

- Different operating environments (premise, cloud, hosting, managed, collocated, etc.)
- Ability to detect threats in one location and react in real time
- Crafting the right security rules in one location and automate policies throughout the entire IT and application infrastructure regardless if internally owned or operated
- Orchestrating changes to the affected systems quickly and universally. Making changes manually to all the necessary devices can take some time and be prone to mistakes

Cloud Security Supporting Application Migration

Cloud-only application solutions (cloud based WAF) have proven ineffective in supporting an efficient means of managing policies across hybrid hosting environments. Nonetheless, cloud plays a key role in the ideal architecture for these challenges: hybrid cloud WAF protection. These technologies offer a single vendor solution, with fully integrated management and reporting, to protect both cloud-based and on-premise applications. It provides both visibility and control in disaggregated application delivery environments to provide comprehensive detection and mitigation of attacks, as well as simplifying security policy orchestration and automation. Finally, the most advanced of these solutions enable worldwide mitigation of threats detected in the cloud via signaling to on-premise security devices.



Conclusion

With the increased focus and attention on headline-grabbing volumetric attacks, the focus on outside cloud-based resources for protection is understandable. But organizations need to keep in mind that these types of threats represent only a small percentage of overall attack volume; roughly 10-15% based on the attacks Radware mitigates on behalf of customers.

The best strategy for protection from today's advanced threats is an architecture that effectively leverages cloud-based resources for attacks exceeding internal resources and capacity, balanced with on-premises technology for immediate detection and mitigation of non-volumetric threats.

About Radware

Radware (NASDAQ: RDWR), is a global leader of application delivery and application security solutions for virtual, cloud and software defined data centers. Its award-winning solutions portfolio delivers service level assurance for business-critical applications, while maximizing IT efficiency. Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, 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: Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis on DDoS attack tools, trends and threats.