radware

Cloud DDoS Protection Service — Protecting Microsoft Azure-Hosted Applications

WHITE PAPER

SHARE THIS WHITE PAPER

TABLE OF CONTENTS

CHALLENGES WITH CLOUD ADOPTION

Today's enterprises cannot ignore the cost savings and flexibility offered by public cloud solutions. With increased pressure on IT departments to deliver results with a minimal budget, the migration of applications and services to the cloud continues. Organizations are increasingly adopting cloud-based services and hosting their applications on a mix of public, private and hybrid cloud environments.

While the economical and operational advantages of the cloud are evident, there is also added complexity in securing this new network infrastructure. As the traditional enterprise perimeter dissolves, organizations are facing more distributed network infrastructures that split across multiple cloud providers and the organizations' private networks. While some applications have migrated to or have been deployed in the cloud, others are still in transition or remain on-premise.

The level of protection from cyberthreats and, specifically, DDoS attacks across these different hosting environments varies and is dependent on the varying degree of protection offered by different vendors.

MORE THAN NETWORK-LAYER ATTACKS

Organizations are specifically challenged by their ability to protect public cloud-hosted applications from today's dynamic and sophisticated application-layer and SSL-based DDoS attacks. With the growth of internet of things (IoT) enabled devices and the emergence of DDoS-as-a-service tools, attackers are launching massive application-layer DDoS attacks that can either bring down or create prohibitive costs for web applications that are hosted on public clouds. As organizations are using more encrypted traffic, SSL-based DDoS attacks have also grown in frequency. According to Radware's *2017–2018 Global Application & Network Security Report*, organizations are experiencing greater impact due to growth in the following trends:

- **Application-layer (L7) attacks** — Application attacks have become the preferred DDoS vector (more than 64% in 2017) as one in every five attacks exceeds 1 Gbps.
- **SSL DDoS floods** — As internet traffic is becoming more and more encrypted, SSL-based attacks have become the primary application security concern (see Figure 1).

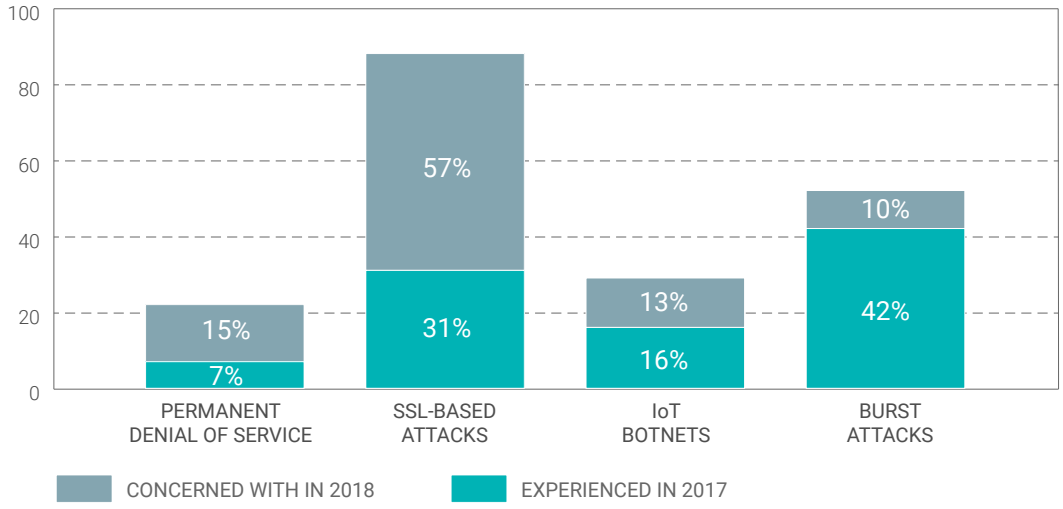

Figure 1: Emerging DDoS Attack Vectors

Yet existing DDoS protection solutions for applications hosted on public clouds provide very limited protection, if any, against DDoS attacks. Public cloud providers that offer DDoS protection only focus on network-layer DDoS protection and lack any protection from application-layer and SSL-based DDoS attacks.

UNCOMPROMISED DDOS PROTECTION FOR APPLICATIONS

Radware's fully managed Cloud DDoS Protection Service protects applications deployed across physical data centers, public cloud environments or both. It is a unified DDoS protection solution that delivers a consistent security policy, an automated DDoS attack mitigation life cycle and a portal for visibility and control. It includes an experienced emergency response team (ERT) and focal point for premise and cloud-based protection, agnostic to the public cloud hosting platform.

This best-of-breed Cloud DDoS Protection Service defends network and server assets by diverting traffic to Radware's globally dispersed, 3.5 Tbps scrubbing centers for cloud-based mitigation during a DDoS attack. Featuring full automation and minimal latency, the service protects against DDoS attacks covering Layers 3–4 and Layer 7. It ensures that only clean traffic is forwarded to the original computer in order to fully safeguard it.

In addition to its robust DDoS protection offering for premise and private cloud-based applications, Radware's Cloud DDoS Protection Service now protects applications hosted on public clouds. Complete with the widest protection against the full breadth of DDoS attacks with real-time mitigation and no added latency in peacetime, it eliminates any manual human actions.

Figure 2: Scrubbing Center Global Network

RADWARE DDOS PROTECTION SERVICE FOR AZURE-HOSTED APPLICATIONS

With sophisticated multivector cyberattacks becoming commonplace, a large percentage of Azure's customers now require more advanced and comprehensive DDoS detection and mitigation capabilities to protect mission-critical, cloud-based assets. Azure customers require protection from a wide array of Layer 7 attacks, advanced persistent denial-of-service (APDoS) multivector assaults, volumetric attacks and SSL-based DDoS assaults.

Radware's Cloud DDoS Protection Service provides the most advanced SLA-committed solution for protecting Azure Virtual Networks. Offered either as On-Demand or Always-On deployment models, the service leverages its best-in-class core technology to rapidly and effectively mitigate DDoS attacks. It harmonically integrates with Microsoft Azure to fully automate the attack life cycle from detection to diversion through mitigation and monitoring. It utilizes Microsoft Azure's API to sync and interact with an organization's virtual private cloud (VPC), and its automation achieves a significantly lower time to mitigation while minimizing the customer's total cost of ownership.

SOLUTION KEY ADVANTAGES

There are several core advantages that are only available with Radware solutions, including:

- **Widest attack coverage including application-layer and SSL-based DDoS attack protection:** Radware's Cloud DDoS Protection Service provides Azure customers with the most advanced attack detection and mitigation capabilities to fully protect applications from all forms of DDoS attacks and protect against zero-day attacks, such as Burst, Dynamic IP and others. No other DDoS protection service, including Azure DDoS prevention solution, can reach this breadth of attack coverage.

Category	Radware Cloud DDoS Protection Service	
Network attacks	• SYN floods • TCP floods • TCP out-of-state floods (e.g., ACK floods, RST floods) • Volumetric DDoS • Amplification and reflection attacks (DNS, NTP, CHARGEN, Memcached, SSDP, etc.)	• UDP floods • Fragmented UDP floods • ICMP floods • TCP connection floods • Behavioral
Encrypted SSL/TLS-based attacks	• SSL negotiation floods • Encrypted web attacks	
Application floods	• HTTP flood attacks • DNS flood attacks • DNS randomized domain name attacks • Mail and spam flood attacks • Network and port scanning • Behavioral	• HTTPS floods • SIP flood attacks • Brute force attacks • Malware propagation
Known attacks and tools	• Application vulnerabilities and exploits • Network infrastructure vulnerabilities • Anonymizers	• OS vulnerabilities and exploits • Worms, bots, trojans and spyware • Protocol anomalies

Figure 3: Attack vectors covered by Radware's Cloud DDoS Protection Service

- **Real-time mitigation with highest accuracy of protection:** Radware is the only vendor to offer out-of-path behavioral-based cloud DDoS protection that can accurately detect Layer 3–7 DDoS attacks and automatically generate attack signatures for mitigation.

- **No added latency in peacetime:** Radware's On-Demand Cloud DDoS Protection Service monitors traffic and diverts traffic for mitigation only upon detection of an attack. It provides organizations with a zero-latency solution in peacetime with automatic detection and mitigation capabilities.

- **No hidden traffic costs:** Protecting applications from application-layer and SSL-based flood attacks means that organizations don't have to pay for the attack traffic that reaches their applications using service credits. Radware's Cloud DDoS Protection Service provides a more cost-effective model for protecting applications everywhere.

- **Unlimited mitigation capacity:** Radware's Cloud DDoS Protection Service provides Azure customers with unlimited attack traffic capacity as part of the legitimate traffic service mode.

- **Maximal customer control:** Customers with Azure-hosted applications can customize their service and choose between automatic, manual or API-based programmatic diversion methods based on their technical and organizational requirements. It uses Radware's service for asset protection across various locations and environments, whether on other public cloud environments or on-premise, using the same seamless technology across the board.

- **Deployment Flexibility:** Radware's Cloud DDoS Protection Service can be deployed in two deployment modes:

  - **Always-On Cloud DDoS Protection Service** is for applications hosted on public clouds where traffic is constantly routed through Radware's cloud scrubbing centers and provides real-time attack detection and mitigation.

  - **On-Demand Cloud DDoS Protection Service** is for applications hosted on public clouds and includes remote monitoring of applications, automatic detection of a DDoS attack, proactive customer alerts, and automatic diversion to Radware's cloud scrubbing centers for real-time mitigation once an attack is detected.

- **Fully managed security service:** Radware's Cloud DDoS Protection Service is a fully managed, 24x7 service provided by Radware's Emergency Response Team (ERT) — a dedicated group of security experts who assume full responsibility to configure and update protection as well as actively monitor, detect, alert and mitigate attacks in real time.

AZURE APPLICATION ATTACK LIFE CYCLE MANAGEMENT

Radware's Cloud DDoS Protection Service for Azure applications automatically protects critical assets through their entire attack life cycle. The diagram below illustrates the various stages where the solution safeguards Azure applications.

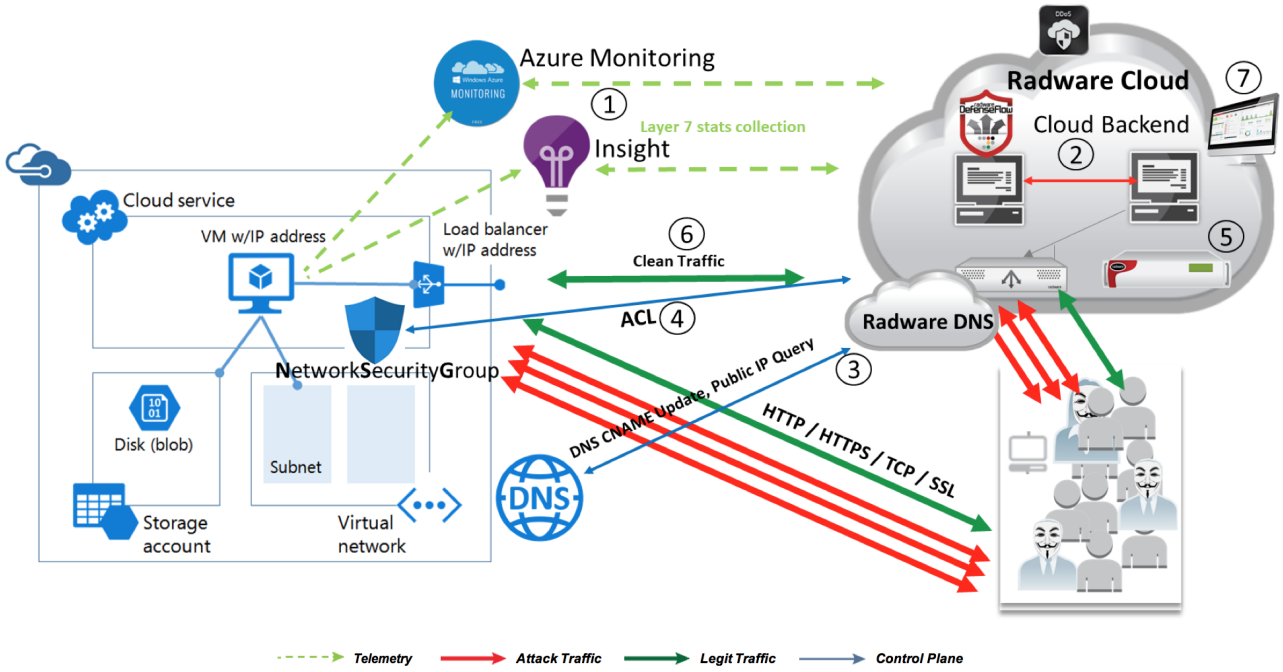

Figure 4: Cloud DDoS Protection for Microsoft Azure — Solution Architect

Stage 1: Azure Metric Monitoring

Radware's Cloud DDoS Protection Service collects Azure Monitor and Insights telemetries from the load balancer to automatically detect behavioral and volumetric DDoS attacks. The required setup is performed only during onboarding and does not require any ongoing technical intervention.

Stage 2: Out-of-Path Detection

Radware's out-of-path behavioral-based cloud DDoS protection can accurately detect Layer 3–7 DDoS attacks and automatically generate attack signatures for mitigation. The detection triggers a series of predefined events including traffic diversion initiation and alerts.

Stage 3: Diversion

Once an attack is detected, Radware's Cloud DDoS Protection Service diverts the traffic to scrubbing centers for cloud mitigation. The service triggers the diversion automatically by configuring the customer's DNS service. (Any external DNS services are supported for a fully managed diversion.) Radware updates the DNS record to point to the scrubbing center, and by doing so, traffic is sent to the scrubbing center. Diversion can be done to one, multiple or all of the scrubbing centers (using Anycast) as needed. Scrubbed traffic is returned to the organization's VPC via reverse proxy.

Step 4: Security Access Enforcement

In order to ensure that direct attacks on Azure's IP addresses are eliminated, Radware replaces an organization's existing network security group for inbound traffic with a new security group that ensures only clean traffic from the scrubbing center is allowed in the virtual network. This provides ACL blocking and ensures that the application is not directly attacked.

Step 5: Attack Mitigation

Operated by Radware's ERT, its globally dispersed scrubbing centers provide over 3.5 Tbps of real-time mitigation capacity. The mitigation is performed by Radware's award-winning DefensePro mitigation devices which leverage our patented behavioral technology to autogenerate signatures for DDoS attacks in real time. Known attack tools are automatically mitigated by harnessing a vast, customizable signature bank and challenge-based remedies.

Step 6: Clean Traffic Return

While the attack traffic is being cleansed, only legitimate traffic is routed back to the protected asset.

Step 7: Real-Time Reporting

Radware's Cloud DDoS Protection Service provides a web-based portal for full visibility and control of the attack life cycle process. The portal includes a real-time, customizable widget dashboard as well as a reporting tool and administrative and configuration screens. Customers can monitor attacks as they happen and analyze the attack vectors, attack volume, target, source and more (see Figure 5).

Step 8: Cool Down and Diversion

When the attack subsides, Radware recommends a cool-down period in which traffic remains diverted by a default for up to four hours in order to provide a quick protection in case a secondary attack is launched. After the cool-down period is over, Radware's ERT experts deactivate the diversion. The diversion can also be self-deactivated by the user programmatically via the web UI, REST API or using BGP over GRE commands.

Note: In an Always-On deployment topology, the traffic is continuously diverted, hence steps 3 and 8 are irrelevant.

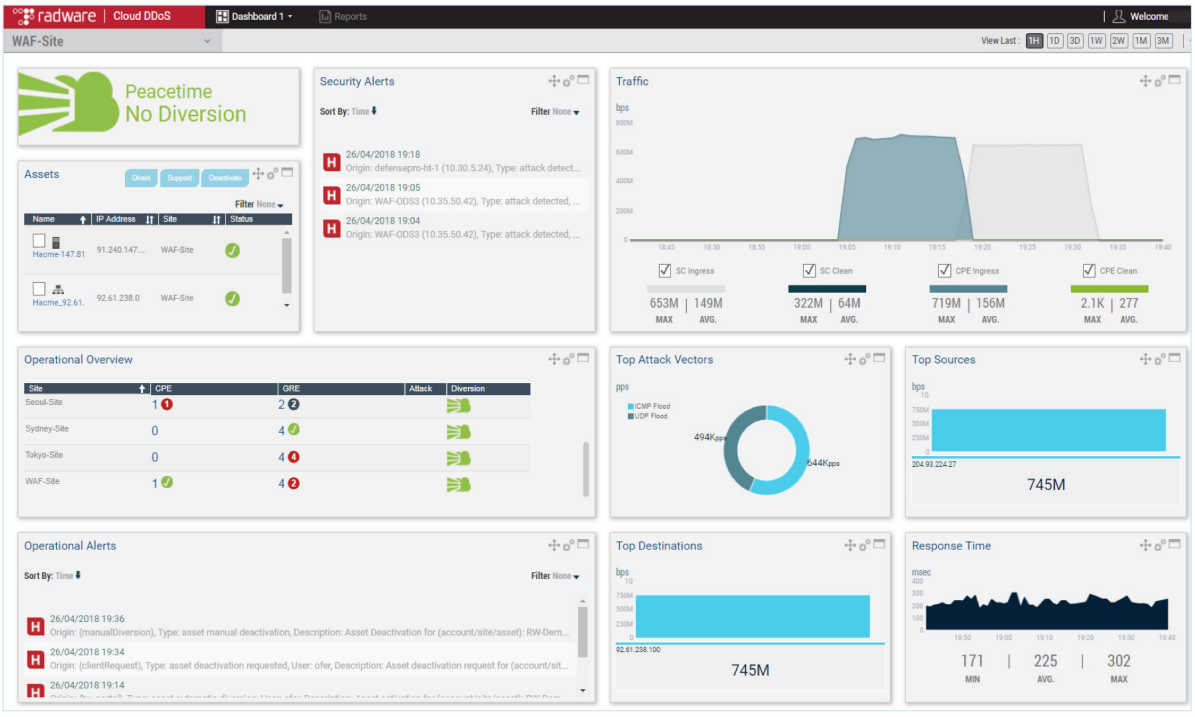

Figure 5: Cloud DDoS Protection Portal

CONCLUSION

Whether it's an on-premise data center or a cloud-hosted application, Radware's flexible Cloud DDoS Protection Service offers a variety of deployment methods (Hybrid, On-Demand or Always-On) as well as multiple detection and diversion methods and customized security policies for precise mitigation.

Customers hosting applications on Microsoft Azure can rely on it to provide fully automated multilayered protection from DDoS attacks on network and application layers; and from volumetric and nonvolumetric attacks as well as full coverage of SSL-based DDoS attacks as part of a service that integrates harmonically with an organization's Azure Virtual Networks.

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.

Certainty Support

Radware offers technical support for all of its products through the Certainty Support Program. Each level of the Certainty Support Program consists of four elements: phone support, software updates, hardware maintenance and on-site support. Radware also has dedicated engineering staff that can assist customers on a professional services basis for advanced project deployments.

Learn More

To learn more about how Radware's integrated application delivery and security solutions can enable you to get the most of your business and IT investments, email us at info@radware.com or go to www.radware.com.