Radware DDoS Protection Market Impact Report

Leading CSPs Adopting Machine Learning and Automation

EXECUTIVE SUMMARY

Radware, a global leader in security and application delivery solutions with a long track record of success in the enterprise market, has been penetrating the communication service provider (CSP) market and now counts 50% of the top 25 Tier-1 global CSPs as security customers.

The threat and potential impact from network DDoS attacks is changing. Attacks are increasingly sophisticated and variable in order to avoid detection and mitigation. Although volumetric attacks remain common, application-specific attacks and targeted, short-burst, high-intensity attacks are increasing in frequency. Automation leveraging massive botnets and software algorithms with morphing vectors means that the attacks, much like a biological virus, continuously mutate.

Radware is utilizing a unique combination of machine-learning algorithms and closed-loop automation to detect and mitigate DDoS attacks without intervention by a security analyst. Attacks that typically required at least 30 minutes of analysis followed by manual infrastructure configuration changes can now be detected and mitigated in less than 30 seconds. Zero-day attacks—those that have never been seen before—are being identified and thwarted with machine-learning algorithms that track and analyze multiple parameters for detection and mitigation. The result is a dramatic leap in efficiency and lower operations costs realized across many CSPs' deployments, benefiting not only the CSPs but also their enterprises, mobile and residential customers.

Automated DDoS protection is also transforming CSPs' security operations and streamlining operator' workflows. Because they are no longer directly involved in mitigating every DDoS event in real time, security analysts are able to move from a reactive to a proactive posture and focus on hardening the network to prevent future threats.

Key Points

- Global Tier-1 CSP success: 50% of top 25 now use Radware DDoS solutions
- Machine-learning, automation provide unique benefits for CSPs
  - Mitigate in seconds
  - Identify zero-day threats
  - Detect nonvolumetric attacks and subscale threats consuming network infrastructure
- Dramatic improvement in automated DDoS protection efficiency
  - 99.58% effective always-on detection/mitigation
  - 95.8% effective on-demand detection/mitigation
- Transform security operations
  - Eliminate troubleshooting bottlenecks
  - Alleviate shortage of skilled security analysts
  - Free analysts to be more proactive to prevent future attacks and threats

DDOS ATTACKS INCREASING IN SCALE AND SOPHISTICATION

DDoS attacks are the scourge of the Internet, disrupting e-commerce, business continuity and consumer applications serving hundreds of millions of users globally. The negative impact of service outages is substantial, resulting in lost revenue, lower productivity, schedule delays, frustrated users and inconvenience for all affected. Explosive growth in consumer IoT has enabled hackers to exploit poorly secured devices and create vast botnets for unleashing massive scale volumetric attacks. The dark web is now a ready source of turnkey automation tools for bad actors to easily launch many different types of attacks.

Radware's Tier-1 service provider customers are seeing increasingly sophisticated and automated attacks, characterized by continuously morphing vectors that complicate both detection and mitigation. State-supported actors and well-funded criminals are exploiting DDoS attacks for extortion, data theft, espionage and cyber warfare.

Volumetric and resource exhaustion attacks are being combined with targeted application-level attacks, masking the goal of infiltrating private networks to install ransomware or steal data. Radware reports an increase in short-burst, high-intensity attacks that typically last only a few minutes but may recur over a period of days or weeks.

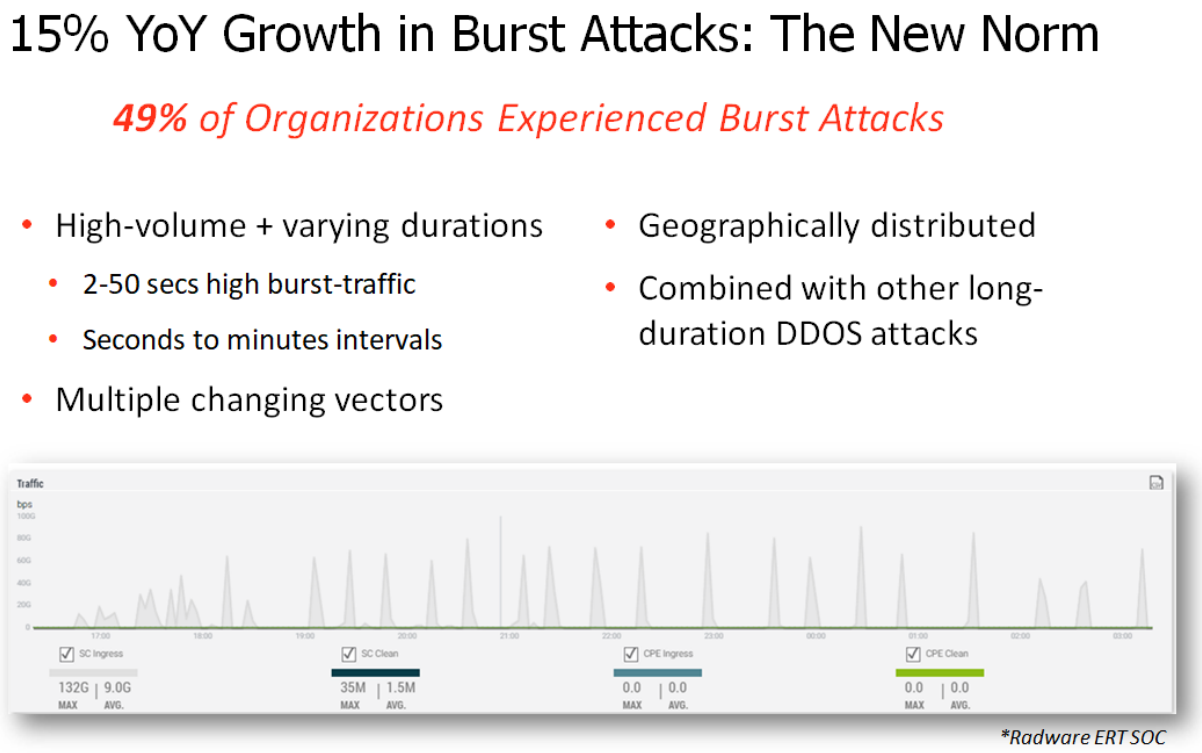

Figure 1. Short-Burst, High-Intensity DDoS Attacks

The adoption of cloud-based business and consumer applications adds complexity by expanding the attack surface to a wide array of targets: ISPs, broadband providers, CDNs, gaming providers, mobile operators, SaaS providers, digital enterprises, hosting providers, public cloud services and enterprise SD-WANs. Emerging industrial IoT infrastructure and edge computing clouds are also potential targets.

Migration to 5G exposes mobile networks to security threats from a wide variety of smart devices that can be hijacked to launch attacks, and using gigabit speed 5G connections, fewer devices are needed to launch sizable volumetric attacks. This puts a new generation of mission-critical 5G applications, such as autonomous vehicles, smart cities, industrial IoT and digital health, at risk.

SERVICE PROVIDER DDOS PROTECTION SOLUTIONS UNDER STRAIN

Since the first large-scale DDoS attacks occurred nearly two decades ago, network operators and vendors have evolved well-known methods for detecting and mitigating against attacks. However, because of the growing complexity, scale and frequency of attacks, these methods require considerable expense in terms of bandwidth and infrastructure costs. Service provider security operations centers are under constant strain and hiring has increased to keep pace with the growing array of threats, although a global shortage of security engineering talent results in most teams being understaffed.

DDoS attacks do not have to be massive in scale to inflict serious damage. Subscale attacks can bleed off compute, memory and network resources slowly over time. In one service provider's network, Radware identified over $6.4 million of core network infrastructure consumption attributed to a single lightweight subscale DDoS attack vector. The customer's existing DDoS protection solution was focused on volumetric attacks and blind to the subscale network activity.

Technically adept attackers are utilizing automation to launch attacks that strike fast and can quickly escalate, leaving overworked security analysts little time to react. Randomized, multivector attacks are more complex to detect and mitigate, taxing the ability of operations staff to respond in time to prevent service outages. Radware's DDoS protection solution reflects the reality that automated attacks require automated detection and mitigation in addition to human expertise.

RADWARE A LEADER IN DDOS PROTECTION FOR SERVICE PROVIDERS

Less than seven years ago, with service providers worldwide struggling to defend against more sophisticated and frequent attacks, Radware[1] entered the market with an automated DDoS protection solution based on machine learning and behavioral analytics. Since then, the company has emerged as a leading provider of DDoS protection solutions to service providers (CSPs) across North America, Europe and Asia.

Radware developed patented algorithms that can detect attacks more quickly and accurately than rudimentary threshold-based techniques, including zero-day attacks that have not been seen previously. Radware applies policy-based automation to mitigate attacks without operator intervention, reducing the total cycle time from initial attack to mitigation to under 30 seconds. This is a breakthrough for CSPs that previously had to manually troubleshoot zero-day attacks, resulting in costly and indeterminate network outages that take hours to resolve.

Most CSP customers have deployed Radware to augment an existing volumetric DDoS protection solution while capitalizing on Radware's ability to detect and block attacks in real time to minimize their impact. Despite substantial prior investments in DDoS protection, Radware penetrated the top tier of the CSP

[1] Source: *Radware Global Application & Network Security Report 2017-2018.*

market by delivering a solution that complements these investments and the associated security operations teams' workflows.

As evidence of its growing success in the CSP DDoS protection market, Radware has penetrated 50% of the top 25 global Tier-1 CSPs. Partnerships have played a key role in the company's success in this demanding market with leading vendors, notably Cisco and Nokia, integrating Radware's DDoS protection solutions with their offerings.

AUTOMATION DRIVEN BY MACHING LEARNING AND BEHAVIOR ANALYTICS

Radware supports the DDoS protection lifecycle with an automated solution enabled by machine learning and behavioral analytics. Radware's multivector DDoS detection algorithms monitor the rate of different types of traffic flows and track key parameters associated with each flow. Behavioral analytics examines the distribution of key parameters to identify anomalous patterns that characterize malicious flows. Using this method, Radware's algorithms detect a wide variety of attacks, including low and slow application layer attacks and zero-day attacks for which there are no previously known signatures, eliminating the need to manually troubleshoot these.

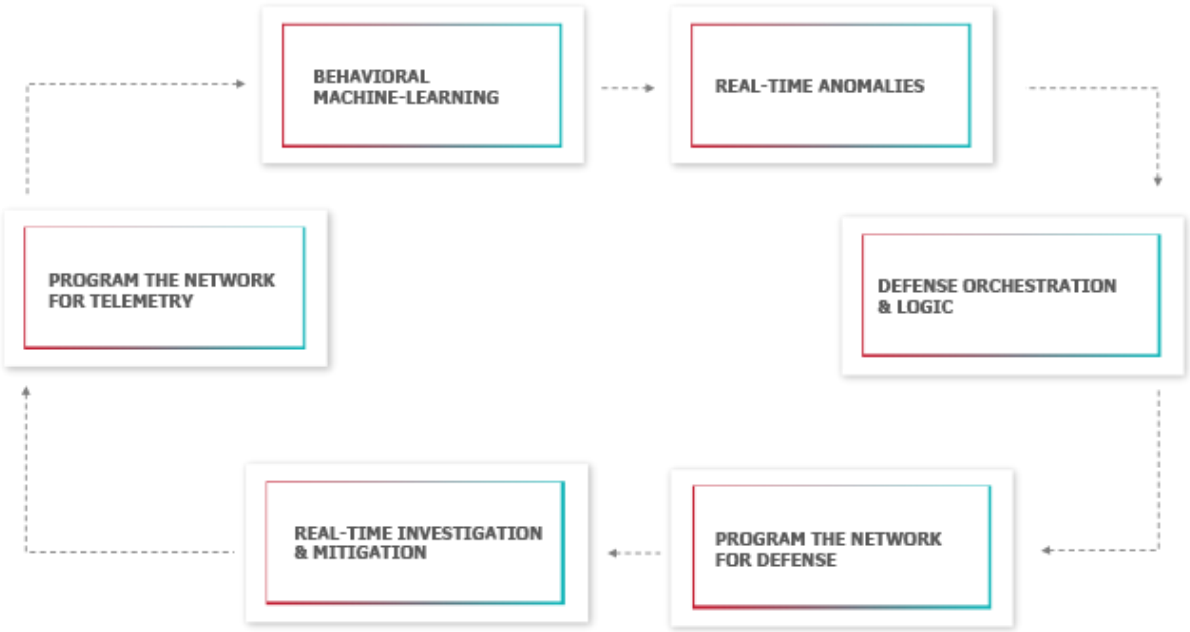

Figure 2. DDoS Protection Automation Lifecycle

Radware's detection solution also includes advanced challenge/response mechanisms to determine if suspect traffic flows originate with legitimate users versus hijacked hosts in a botnet. Challenges directed to originating hosts enable Radware to pinpoint the source of attacks to specific sessions or users, enabling more efficient mitigation mechanisms.

The pace of attacks is growing fast and furiously, outstripping the ability of security operations teams to react in time. Radware blocks attacks using automated, policy-driven mitigation that utilizes data plane

platforms that span dedicated DDoS appliances, firewalls, application delivery controllers and cloud-based scrubbing centers.

Realizing the significant operational efficiencies of security automation does require a shift in operators' mindset and significant trust in the new DDoS protection solution. Consequently, CSP customers have typically deployed Radware in parallel to existing solutions, which either remain installed or serve as a backstop as they gain full confidence in Radware.

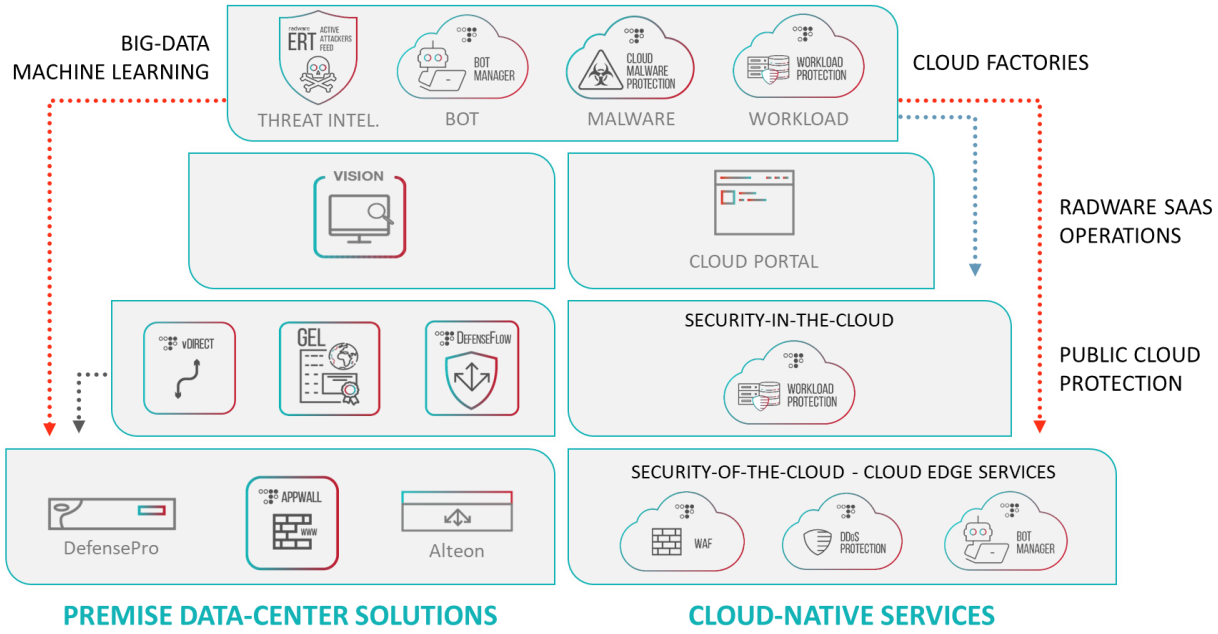

Figure 3. The Big Picture: Radware Architecture for Automated Mitigation

Radware shared some anonymized statistics with ACG. At most CSPs, prior to deploying Radware it could take up to 30 minutes or longer to respond to a DDoS attack, first alerting the security operations center to the attack and then having analysts manually investigate the attack profile to initiate the appropriate mitigation response. With Radware's automated solution, this cycle time has been reduced to under 30 seconds.

In one example, a global Tier-1 service provider encounter over 130,000 attacks in just five days. When installed in an always-on detection and mitigation mode with the ability to establish a baseline and observe peace-time traffic, Radware was able to auto-mitigate over 99.5% of all attacks. In an on-demand Tier-1 application where traffic was only sent to Radware on an ad-hoc or as-needed basis without the benefit of peace-time visibility and baselining, the effectiveness of Radware's automated solution was still measured to be 95.8%.

False positives, or blocking of legitimate user traffic, are a potential side effect of all DDoS protection solutions. In both scenarios the basis for measuring mitigation effectivity is blocking less than 1% of legitimate user traffic while leaking less than 1% of malicious traffic that should have been blocked. The

integrated feedback loop in Radware's automated solution enables it to continuously learn and adapt. In developing a real-time signature and parameterization for mitigation, the algorithm measures the effectiveness in blocking malicious flows (compare pre-mitigation to post-mitigation traffic) while not impacting legitimate ones. If the algorithm determines that a mitigation parameter is ineffective (example, not blocking malicious traffic or is blocking legitimate traffic), it removes it from the mitigation signature and reoptimizes in a continuous process.

These metrics provide a clear view as to how machine learning and automation can enhance the effectiveness of human analysts in the face of increasingly sophisticated and frequent attacks. With skilled analysts in short supply across the industry and the sheer number of attacks increasing, improving the efficiency of each analyst is an added motivation for service providers to adopt an automated approach to DDoS protection. Security analysts can spend less time on the front lines reacting to events and more time proactively analyzing security risks and protecting the network against other threats.

SERVICE PROVIDER DEPLOYMENT SCENARIOS

Radware reports that its CSP customers install DDoS protection first and foremost to defend their networks from attack, especially high-bandwidth links into the network core and primary data centers. Radware views 5G networks and next-generation cloud transformation as greenfield opportunities for automated protection solutions to ensure the availability and performance of new, high-speed, mission-critical applications.

The expanding network perimeter requires operators to manage protection across potentially thousands of ingress points. Radware is often installed to augment an existing DDoS protection solution, so the company recently developed a traffic filter generation feature that operators can use to automatically apply the appropriate filters to existing threat mitigation platforms protecting this multitude of ingress points, complementing existing security operations tools and workflows.

For managed security service providers (MSSP) serving hundreds of clients, it is prohibitively expensive and time-consuming to insert expert analysts into routine DDoS attack detection and mitigation workflows for each client. Radware's automated, multitenant platform is well-suited for these managed service offerings and has been successfully deployed at scale at a leading Tier-1 SP. It also features a user portal that MSSPs can deploy for their clients to gain visibility into network traffic as attacks are detected and offending flows are blocked.

Tier-1 CSP customers are keenly aware of the myriad of evolving threats targeting their networks and services. They rely on Radware to be nimble in quickly developing new solutions to new threats. In addition to rapidly mitigating attacks, Tier-1 CSPs are pushing for ways to prevent attacks from occurring in the first place. Radware supports this effort by providing customers with a real-time threat feed that disseminates information about new attacks so that CSPs can be proactive and take protective measures.

Service providers' network transformation hinges on virtualization and software-defined, cloud-based infrastructure. Radware is well-positioned for this change with a DDoS protection solution that is packaged in multiple form factors, including an appliance, a VNF or a VM that installs on a customer's server. The choice of form factor depends on the deployment environment and performance requirements; however,

once installed, Radware's software is configured and managed using the same UI and management tools, regardless of form factor.

CONCLUSION

Rapid DDoS attack detection and mitigation ensures service availability and performance while helping to root out insidious security threats masked by attacks. Radware's success in the CSP market demonstrates the effectiveness of applying machine learning, behavioral analytics and automated mitigation to DDoS protection. The accuracy and precision of Radware's detection and mitigation mechanisms allow legitimate traffic to continue to flow during attacks while abusive flows from offending sources are blocked, ensuring service availability when under attack. In addition to reduced time-to-mitigation, Radware's CSP customers are seeing both a decrease in false positives and an increase in the effectiveness of mitigating malicious traffic. Radware's automated DDoS protection solution is also helping to improve the efficiency and overall effectiveness of CSPs' security operations teams and the value they offer to end customers.

Authorship: This paper was authored by ACG Research which is solely responsible for its contents.

Sponsorship: Radware, January 2019.