radware

CASE STUDY: **SAAS PROVIDERS**

Leading Cloud Computing Provider Partners with Radware for Behavioral-Based DDoS Mitigation

THE CHALLENGES

This leading enterprise SaaS provider experienced several attacks and needed to strengthen its security to protect both its own data and customers' data.

THE SOLUTION

The SaaS provider purchased Radware DefensePro, configured in an out-of-path deployment mode, in addition to DefenseFlow and Radware professional services to assist with implementation and customization.

WHY RADWARE

Radware's machine-learning capabilities were able to accurately distinguish between good and bad traffic and mitigate any attacks within seconds and without creating false positives.

BENEFITS

The cloud SaaS provider uses Radware's unique machine-learning capabilities to mitigate threats in real time versus relying on rate-based mitigation strategies. Additionally, DefensePro is able to mitigate burst attacks, one of the customer's major concerns.

This cloud computing company is a leading provider of various business, commercial and social networking solutions and services, all delivered via the SaaS delivery model. Its services are configured and integrated with various third-party platforms and leading enterprise applications.

THE CHALLENGES

The rapid growth of SaaS companies underscores the power and flexibility that this service model delivers; however, the distributed nature of the model and the potential damage as a result of a successful attack invite an increased risk of cyberattacks. Attacks against SaaS providers can be the result of hackers targeting valuable customer data or competitors targeting the SaaS provider, or even the provider hosting a customer who becomes a target. Regardless of the motives, the impact on these attacks can be catastrophic for an SaaS business and its customers.

This leading enterprise SaaS provider experienced several attacks and needed to strengthen its security to protect both its own data and customers' data. The company was concerned about availability of its services and meeting contractual SLAs.

The company was also concerned about its risk of attack exposure due to rapid growth and expansion, which included the acquisition of new companies. This SaaS provider would adopt the increased risk of attack of the acquired companies, some of which were attacked frequently.

An example of this occurred several years earlier when the SaaS provider acquired a digital email marketing platform that serviced thousands of customers, had strict SLA requirements and required SSL attack detection and mitigation capabilities. The SaaS provider evaluated several DDoS mitigation vendors, including Radware, NETSCOUT Arbor and F5. The SaaS provider preferred Radware's behavioral-based DDoS protection capabilities and SSL attack prevention solution. These capabilities were put to the test while the SaaS provider was visiting Radware's headquarters. The email marketing platform experienced a 13-hour, 7.5Gbps volumetric attack that Radware's solution automatically identified and mitigated with the assistance of Radware's Emergency Response Team.

> "We suffered an attack that made our firewall fail over, but then the DefensePro kicked in and mitigated the attack within 18 seconds."
>
> *— Information Security Manager for the Marketing Cloud, commenting on the aforementioned attack*

The SaaS provider's existing cybersecurity solution was Akamai's Prolexic cloud-based DDoS protection service, which provided protection from volumetric attacks but did not leverage behavioral-based detection and automated mitigation capabilities to defend against burst and other multivector and zero-day attacks.

The SaaS provider had several requirements:

- Integration of new company acquisitions into its existing SaaS platform
- High availability and satisfaction of strict SLAs (99.999%) for thousands of customers
- SSL attack detection and mitigation for its systems
- Low false positives and fast detection
- Mitigation of flood and burst attacks, as well as automated mitigation responses to bot activity
- Minimal network latency
- Partnership with a leading DDoS mitigation provider that has proven expertise and technology

With these technical capabilities defined, the SaaS provider began evaluating a series of DDoS protection solution vendors.

THE SOLUTION

The SaaS provider tested a number of vendors, including Radware and A10. Radware's DefensePro, an on-premise DDoS mitigation appliance, and DefenseFlow, a cybersecurity orchestration solution, were tested in addition to A10's One-DDoS Protection solution. Testing revealed that Radware's behavioral-based mitigation capabilities, implemented via an out-of-path deployment, provided more accurate detection and mitigation than A10's capabilities did. In several tests, A10's rate-based mitigation techniques dropped legitimate traffic while Radware's machine-learning capabilities were able to accurately distinguish between good and bad traffic and mitigate any attacks within seconds and without creating false positives.

The SaaS provider purchased Radware DefensePro, configured in an out-of-path deployment mode, and DefenseFlow in addition to Radware professional services to assist with implementation and customization. It also opted for a Radware resident engineer to be part of its on-site security team at its main global data centers. Radware was also selected for other various reasons.

- DefensePro's out-of-path deployment architecture was a key competitive differentiator. Because networks can be sensitive to latency and points of failure caused by adding a DDoS mitigation device, DefensePro devices can be configured out-of-path instead of in-line. Only network traffic that requires inspection is diverted to the mitigation device, which receives a copy of the traffic to be scanned for attacks. This eliminates latency and additional risk of failure. Once an attack is detected, only the relevant traffic is diverted through the device, and the attack is prevented in seconds. "Clean" traffic is allowed to flow through the network freely.
- DefenseFlow collects measurements and statistics from various network elements and applies behavioral algorithms for accurate detection without generating false positives. It uses behavioral detection and mitigation mechanisms for fast and accurate mitigation.

BENEFITS

The cloud SaaS provider was able to leverage DefensePro's unique machine-learning capabilities to detect traffic anomalies against network behavioral fingerprinting and automated signature creation to mitigate threats in real time versus relying on rate-based mitigation strategies or "blackholing." As an additional benefit, DefensePro is able to mitigate burst attacks, one of the customer's major concerns.

To benefit from Radware's expertise with service installation and day-to-day solution monitoring and management, the customer elected to purchase additional assistance from Radware's professional services team and have a resident engineer on-site to assist the SaaS provider's operations team with daily operations and maintenance. The SaaS provider is pleased with the results of its partnership with Radware and will tailor its implementation as its business requirements evolve.

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.