European Manufacturer Turns To Radware To Build A Custom Security Solution

BUSINESS NEED

A well-known European manufacturing company required protection for its complex, globally-distributed network comprised of data centers, remote offices and cloud-hosted applications in preparation of a high-profile sponsorship event. Each asset type had radically different requirements and faced different threat profiles. Traditional DDoS mitigation vendors did not have the flexibility or scope to offer full, cost-effective protection for all asset types.

SOLUTION

Radware implemented a combination of cloud and premise-based DDoS and WAF solutions. The data centers were protected with a hybrid DDoS solution, combining a premise-based appliance with scalable cloud protection; the cloud-based applications were protected using an 'always-on' cloud service and cloud WAF; and non-critical remote sites were protected with Radware's on-demand cloud DDoS service.

WHY RADWARE

Radware is the only DDoS mitigation provider which develops its own mitigation technology and implements it via its own globally distributed cloud scrubbing network. As a result, Radware was the only provider who could tailor its offering specifically to the needs of the customer.

BENEFITS

With the flexibility provided by Radware, the enterprise manufacturing company was able to safeguard all assets in its network leveraging Radware's high-quality DDoS and WAF protections. Radware's security services blocked several major attacks during the high-profile event, with no impact on availability or performance of any assets.

This European manufacturing company was facing a dilemma: how best to protect its worldwide operation against DDoS and application attacks. As a well-known household brand, the customer's network was both globally distributed and complex. Different infrastructure assets had different requirements under various operational scenarios, resulting in each asset requiring different protection coverage.

The problem, however, was that most vendors did not support this level of granularity in their product offerings. Most vendors were constrained by their limited offering set – usually only cloud-based or only hadware-based – and even some of the 'hybrid' DDoS vendors had surprising limitations in the scope of coverage they could offer. Moreover, the company's previous security vendors suffered a major breach the previous year.

Perplexed, the customer turned to Radware, who was the only security provider able to offer the breadth and depth of protection along with the granularity required by the customer's elaborate use case.

CHALLENGES

The organization's network and data center infrastructure was as diverse and complex as it was far flung.

1. **Four globally distributed data centers** running mission-critical applications. Each data center runs a wide array of mission-critical services. These data centers require constant protection against both volumetric and non-volumetric DDoS attacks with minimal latency and cannot afford any interruption to service.
2. **150 cloud applications** hosted on a large public-cloud provider. Even though the organization still maintained a network of physical data centers, it also had a large set of applications running in the cloud atop public cloud providers. These applications were constantly exposed so they needed continuous protection against both DDoS attacks and application vulnerabilities.
3. **Three-dozen remote sales offices** spanning the globe. The offices were part of the company's global IT network, and while not mission-critical to the extent that the on-premise data centers or cloud-applications were, still required first-rate protection.

An evaluation of the DDoS mitigation market quickly revealed a massive hurdle: no vendor could perfectly address the protection needs of all asset types.

Cloud-based DDoS vendors offered, naturally, an all-cloud solution. While this worked well for cloud-based applications, it introduced an unacceptable level of latency to the mission-critical applications in the physical data centers.

DDoS equipment manufacturers , on the other hand, offered premise-based devices or hybrid solutions which combine a physical device with an expandable cloud service. While this was appropriate for protection of the four data centers, this quality of protection was not required for the remote sites and the cost would have been exorbitant. Moreover, it could not provide protection for the cloud-based applications.

Some vendors offered a combination of several approaches, but even they could not do so with a single unified solution. Rather, they would have had to integrate multiple vendors and/or technology stacks.

THE SOLUTION: RADWARE TAILORS A BESPOKE SOLUTION

Radware was able to satisfy the needs of the customer via the breadths of its offering, which could tailor specifically to the needs of the customer's elaborate network topology.

- **Hybrid DDoS protection for the four global data centers** using Radware's DefensePro DDoS appliances together with Radware's Cloud DDoS Protection Service. This approach allows for constant, high-quality protection against both volumetric and non-volumetric attacks with minimal latency.
- **Always-On protection for the 150 cloud applications** by providing constant, uninterrupted cloud-based protection for all online assets. In addition, the customer deployed Radware's Cloud Web WAF Service to provide protection against application attacks.
- **On-Demand protection for the 36 remote sites.** These offices were not considered mission-critical, so a cloud-based on-demand service could provide effective protection without leading to exorbitant cost.

DATA CENTER PROTECTION	PUBLIC CLOUD PROTECTION	PROTECTING REMOTE GLOBAL OFFICES
4 DATA CENTERS	**150 APPS ON PUBLIC CLOUD**	**36 REMOTE LOCATIONS**
Hybrid Cloud DDoS Protection Service	Always-On Cloud DDoS Protection Service + Cloud WAF Service	On-Demand Cloud DDoS Protection Service

Providing service across all protection layers, Radware's Emergency Response Team (ERT) provided managed services for both premise-based and cloud components, as well as attack-time SOC support in times of need, giving the customer a single point-of-contact.

By mixing-and-matching different service offerings and matching the protection model to the business needs, the customer was able to achieve high-quality, cost-effective protection for all their assets. It also afforded them flexibility to modify their offering in the future should their network topology change.

TESTING DEFENSES UNDER FIRE

Shortly after deploying Radware's cloud security services, the company sponsored a major international sporting event. High-profile events naturally attract attention – both from customers and hackers. The company received a number of attack ransom emails in the months leading up to the event.

Once the event started, the company experienced an immediate uptick in attacks. In particular, there were massive attack spikes during the opening weekend of the event, as well as during the quarter-finals round. Interestingly, such large spikes were not observed during the semi-finals and finals.

Over the course of one month, Radware successfully blocked four major DDoS attacks and over 175,000 web application attacks. During this time, the customer reported zero false-positives and zero false-negatives, which means that no legitimate user traffic was blocked. The massive attack campaign had no impact of the availably or performance of the customer's applications.

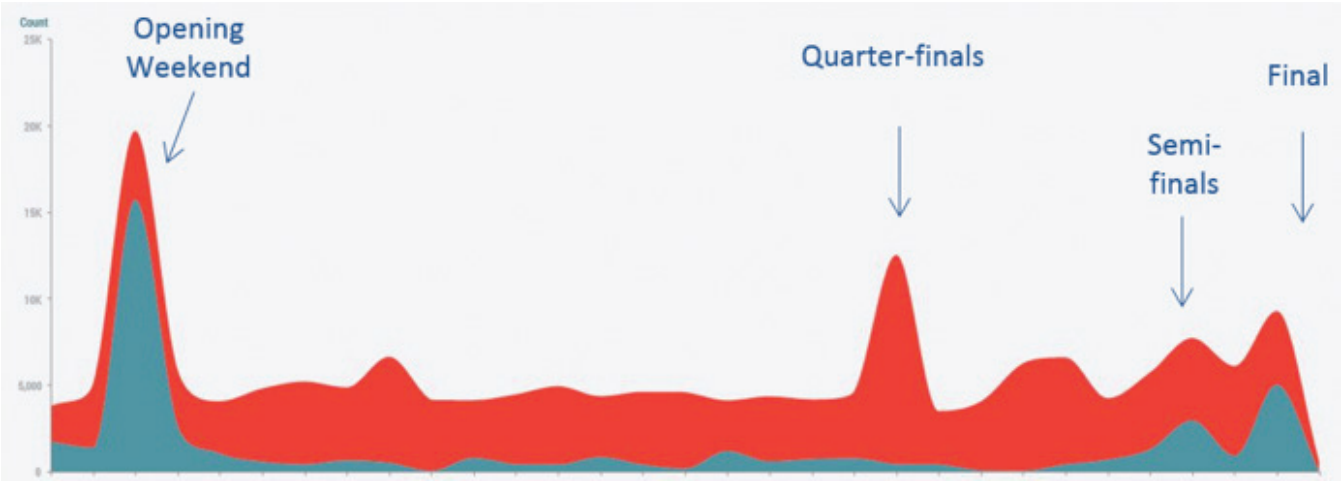

Figure 1: Attack traffic display from Radware Cloud Security management console showing spikes throughout the event

BENEFITS: SAME TECHNOLOGY AT EVERY LEVEL, SINGLE PANE OF GLASS

Selecting Radware's solution afforded the organization a number of key benefits:

- **Best Protection:** The combination of multiple protection models for different asset types allowed for optimal DDoS protection across all assets.
- **Single Pane of Glass:** Radware provides a unified Cloud Security portal which gives security administrators visibility and control over all assets, both cloud-based and on-premise.
- **Single Point of Contact:** Rather than having multiple support contacts for different services, Radware's ERT provides customers with a single focal point and single business process to implement for all of their support and assistance needs.
- **Future Proof:** Radware's flexible solution supports future migration of assets to the public cloud using the same technology and same support structure at every level and for every asset.