

Switch Partners with Radware to Secure the World's Largest Colocation Data Centers and to Protect Its Customers From Attack

Business Need

Switch's award-winning Tier IV Gold SUPERNAP data centers are the highest-ranking colocation data centers in the world. To maintain its 100% guaranteed uptime for customers that leverage these data centers, Switch needed to implement a market-leading cyber security solution to safeguard its data centers and to offer the solution to its subscribed DDoS customers.

Why Radware's Solution

Switch deployed Radware's Attack Mitigation System (AMS) to protect its SUPERNAP data centers and customers from all forms of DDoS attacks. AMS was selected for its ability to detect and mitigate a wide array of cyber assaults and because it was the most scalable attack mitigation solution on the market.

Solution

Radware's AMS is a real-time, behavioral-based cyber security solution that protects an organization's applications and networks against known and emerging threats, including DDoS, Internet pipe saturation, attacks on login pages, low and slow and encrypted assaults, CDNs and SSL-based flood attacks.

Benefits

AMS defends Switch's SUPERNAP data centers from all forms of network and application attacks and is backed by Radware's cloud scrubbing network in the event of a volumetric attack. This allows Switch to maintain business continuity for its customers and has allowed it to offer AMS to its subscribed DDoS customers.



Overview

Based in Las Vegas, Nevada, Switch's award-winning Tier IV Gold SUPERNAP data centers are the highest-ranking colocation data centers in the world and are maintained by the highest-rated mission critical operations teams. With more on-net, independent cloud providers than any other physical cloud gateway, SUPERNAP connects thousands of clients and providers in the most cost-efficient and technologically secure environment worldwide. SUPERNAP is the recognized world leader in colocation design, development and mission critical operations with clients ranging from sophisticated startups to Fortune 100 powerhouses.

Challenges

Switch's SUPERNAP data centers required protection from all forms of DDoS threats via a security solution that provided a wide breadth of protection, thereby allowing the company to maintain 100% uptime and business continuity for its customers, even in the face of an attack. The new solution would need to be capable of mitigating DDoS attacks of up to 300Gbps and 220 million packets-per-second from a single device.

“As the world’s best colocation data center provider, we want to provide our customers with the highest quality cyber-attack protection available today... With Radware’s Attack Mitigation System, we can maintain business continuity for our customers even in the face of a volumetric attack.”

- *Chris Donnelly, Executive Vice President of Connectivity at Switch*

The Solution

After conducting an evaluation of various solution providers, Switch selected Radware’s AMS, as it was the most scalable attack mitigation platform on the market and provided defense from the widest array of attack vectors.

With Radware’s Attack Mitigation System, Switch can detect, mitigate and scrub nearly every type of cyber-attack with precision and accuracy. Automated attack mitigation allows Switch to mitigate multiple attack vectors simultaneously without their customers experiencing a disruption.

The AMS is a behavioral-based real-time signature technology that detects and mitigates emerging network attacks in real time, such as zero-minute attacks, DoS/DDoS attacks, and application misuse attacks—all without the need for human intervention and without blocking legitimate user traffic.

Benefits

AMS now defends Switch’s SUPERNAP data centers from attack and is capable of detecting and mitigating all forms of network and application attacks, low and slow, and encrypted attacks. It has allowed Switch to maintain business continuity for its customers even in the face of volumetric cyber-attacks. AMS is backed by the added capacity of Radware’s cloud scrubbing service network, which is used to cleanse attack traffic in the event of a volumetric attack. In addition, AMS will be offered to Switch’s subscribed DDoS customers.