

Top Layer's IPS Increases Performance and Enables Significant Traffic Flow Improvements for University of Miami

The University of Miami is home to over 15,400 undergraduate and graduate students from around the world, with another 11,000 faculty and employees serving the campus population. Its Leonard M. Miller School of Medicine campus consists of 45 acres within the 100-acre University of Miami/Jackson Memorial Medical Center complex and includes the Miami VA Medical Center and two University-owned hospitals - the University of Miami Sylvester Comprehensive Cancer Center and Anne Bates Leach Eye Hospital, home to the top-ranked Bascom Palmer Eye Institute. Miller School of Medicine faculty conducts more than 2,000 research projects in basic science and clinical care.

Protecting a Hospital and a Medical School in a Single Network

Each August, more than 15,400 students converge on the campus of the University of Miami as classes start, though at the Leonard M. Miller School of Medicine, network activity does not see a seasonal surge as seen at other universities nationwide. Traffic at the Miller School of Medicine remains consistently high year-round because it serves the role of both medical school *and* hospital, with no time off between classes. Because of the nature of the dual-purpose facility, the Miller School of Medicine has unique requirements for network security: it demands highly-available and reliable performance while providing both open access to students and dedicated protection of patient data and proprietary research information.

The University of Miami, and the Miller School of Medicine specifically, continuously seek to learn about, evaluate and deploy new technologies to strengthen the security of its network and ensure protection of its data. In doing so, the Miller School of Medicine sought to upgrade its intrusion prevention solution (IPS) from the outdated device sitting on its network to a third generation purpose-built IPS appliance.

Replacing Outdated First-Generation Technology with Modern Third-Generation Solutions

In late 2007, Vijay Haripal, Information Security Manager at the Miller School of Medicine, had begun evaluating options to strengthen the network security of the University school and hospital. As security threats evolved and became more cunning and sophisticated,

Vijay knew the TippingPoint IPS currently in his network would not be able to provide adequate protection to his changing network needs and the changing security threat landscape that has evolved over recent years. According to Vijay, "At the same time, we started hearing more and more about Top Layer Security's capabilities beyond its strong Distributed Denial-of-Service (DDoS) protection history and that its award winning technology was protecting customers from all types of malicious content, undesired access and botnet-based attacks. As new threats beyond simple worms and rate-based threats have emerged in recent years, Top Layer Security has kept up, evolving and enhancing its technology to help its customers face these new challenges."

In addition, their local Top Layer Secure Circle Partner Program reseller supported replacement of the TippingPoint IPS appliances, as its capabilities were outdated and limited in the protection that it could deliver. For instance, because the appliance relied on signature-based rules protection, even minorly-altered attacks would get through. The Miller School of Medicine engaged in an extensive evaluation of the current solutions on that market that were the most viable over the long-term. In addition to Top Layer Security's IPS 5500 solution, Vijay and his team evaluated, the new TippingPoint 2400E and Reflex Security's IPS solution. However, Reflex's technology was not mature enough, TippingPoint's 2400E was still signature-based and when put inline too often went into Layer 2 fallback.

The Miller School of Medicine ended up evaluating the TippingPoint IPS and the Top Layer IPS 5500 in parallel on the network in front of data centers to compare traffic and behavior, with the entire Top Layer Security rule set active, including: signatures, protocol anomaly protection, application usage awareness, deep-packet inspection and firewall. "The Top Layer solution was performing at 28-35% capacity maybe peaks to 50% once in a while, which was quite impressive. This sealed the deal, and we then left the Top Layer IPS 5500 in the network to replace the TippingPoint 2400 we used previously," stated Vijay. "We have never seen a performance hit since putting Top Layer inline, proving to us that Top Layer's ASIC-based architecture and inline protection mechanisms were truly built for high-performance networks, and not just marketed that way."

Shaping Traffic while Ensuring A+ Protection across the University Network

The University has parallel networks for redundancy and for fail-over reasons. To maximize protection, Vijay purchased several more Top Layer IPS 5500s and positioned them on both sides of the network, in front of and behind the firewalls to provide added protection. The outside IPS 5500s were tuned to enable more server-protection rules; the inside IPS 5500s tuned for more virus/DDoS protection – essentially, the outside appliances serve as filter for the inside counterparts. Because of this flexibility in tuning and deployment configuration, the Miller School of Medicine is better able to shape traffic to its specific operational needs. “The architecture of Top Layer IPS that uses ASIC processors and CPUs runs more efficiently and effectively than competing solutions. Because of this design, Top Layer’s solution is able to process traffic faster and better, therefore increasing performance and enabling significant traffic flow improvements.”

In addition, The Miller School of Medicine has Top Layer’s ProtectionCluster enabled with the four IPS 5500 appliances in place, to make use of additional processing horsepower and load-balancing, in case needed. “However, we haven’t needed the additional horsepower yet, but is certainly nice to have,” added Vijay.

The University of Miami has a diverse network, requiring high-performance due to various sectors it serves. For instance, the university has a high-speed computing facility connected to Internet2, a large research community, students, doctors, faculty, staff etc. that all have different computing needs, so any type of inline device needs to take this into consideration when deployed on the University of Miami network. “Top Layer gave us the flexibility to identify which rules to apply to which networks. Internet pipe comes from the main University of Miami campus and traffic goes

between the campuses as well as to the Internet,” added Vijay. “Specifically, the University of Miami Medical Center and the University of Miami share a network and we’re able to carve out segments that each entity owns, and create specific rules for traffic between the campuses and to deal with external threats. This capability within the Top Layer IPS was a big deciding factor; our previous IPS was too generic, while Top Layer enabled us to get very granular.

Lessons Learned: Moving Beyond Signatures and the Value of Executive Involvement

Vijay’s team realized the fundamental issues with relying too heavily on signature-based protection, and because Top Layer’s architecture also examines the actual protocol of attack as well as traffic behavior and characteristics, it performed much, much better with variants of attacks. “Top Layer notices what is ‘abnormal’ and the solution showcased these great defense capabilities against the attacks that our team threw at it during the testing phase.” In addition, testing was not conducted in an evaluation network; it was tested on the production network with no performance impact once installed. “Granularity and fine-tuning is key to managing the network, and Top Layer excelled in these areas,” added Vijay.

“In addition, Top Layer’s senior engineer and executive team were highly-engaged and visited on-site to discuss their technology roadmap. We felt very involved in the future of the Top Layer technology, as they listened to our needs and shared where their roadmap would be heading,” added Vijay. “Top Layer’s philosophy of treating customers like partners is greatly appreciated; they have remained extremely hands-on even after the deployment. Lastly, Top Layer has shared real numbers regarding the solution’s performance and there have been no promises that haven’t been delivered, which is rare.”

About Top Layer Security

Top Layer is dedicated to its role as the leading global provider of Network Intrusion Prevention Systems (IPS), developing and bringing to market network security infrastructure solutions that help commercial and government organizations protect their critical on-line assets from the losses and risks associated with cyber threats. Top Layer is headquartered in Massachusetts, USA with sales and services support worldwide.

