

Kentik Delivers Network Automation & Security for OSHEAN



CATEGORY

- Research and Education Network (REN) Operator

CHALLENGE

- In need of a scalable, centralized network defense service for DDoS, capable of best serving all of its members as a whole, rather than each member institution having to defend itself

SOLUTION

- Fast, accurate, and automated DDoS detection and analytics from Kentik

RESULTS

- Automated DDoS mitigation to stop more than 300 volumetric DDoS attacks from affecting its member networks in less than one year

Overview

Research and Education Network (REN) operators must provide ultra-fast, reliable network performance for their members while fending off cyber attacks — all within tightening budgets. Analytics and automation are becoming critical tools to help these operators tackle network management and security challenges under given staff and dollar constraints. That is why Rhode Island-based OSHEAN, Inc. turned to Kentik.

Challenge

OSHEAN is a non-profit coalition of 160 members consisting of universities, K-12 schools, libraries, hospitals, government agencies, and other non-profit organizations. With more than 600 miles of fiber, OSHEAN's goal is to deliver carrier-class optical transport, advanced IP-based networking, and innovative cloud solutions to its member institutions and the communities they serve.

As digital transformation initiatives proliferate among many of its members, OSHEAN's network has expanded dramatically. Alongside that, security threats, like distributed denial-of-service (DDoS) attacks, were increasing on its membership. OSHEAN President and CEO David Marble, together with a team of staff and selected members, decided that building a centralized network defense service for DDoS would best serve OSHEAN's members as a whole, rather than each member institution having to defend itself.

The OSHEAN technical team previously handled DDoS attacks in a reactive, brute-force manner, by manually recognizing attacks (sometimes because of a member phone call). The team would then blackhole, or drop, the assumed-malicious traffic. As a result, the targeted member's network would experience an outage for the duration of an attack. In many instances, that meant the members' operating heartbeat — including classes, research projects, hospital operations, and government services — would temporarily stall. Mitigating attacks this way was a manually intensive process, consuming significant staff time at all hours of the day and night.

A large, light blue, stylized quotation mark graphic is positioned to the left of the quote text.

“Deployment of Kentik’s platform was fast and easy, and we quickly learned Kentik’s solution would provide us with much more than just DDoS traffic detection.”

— David Marble, OSHEAN President and CEO

As OSHEAN began to look for a new DDoS defense architecture, the team found that many of the solutions on the market were either appliance-based or service-based. Appliance models required significant capital and had scaling issues while the service-based solutions lacked features and automation potential. OSHEAN decided to split the problem into an analytics/detection component and a mitigation component and build the service chaining in-house. As a result, the team decided on a cloud-based scrubbing solution to handle the DDoS mitigation piece and set out to find the front-end network analytics system needed to understand all of OSHEAN’s traffic and detect potential incidents.

Solution

At several events for the research and education community, OSHEAN continued to hear about Kentik and the company’s fast, accurate, and automated DDoS detection and analytics capabilities.

“As a SaaS-based network visibility platform, Kentik’s solution was instantly appealing. We knew it wouldn’t require the costly infrastructure-management overhead of the appliance-based products out there,” said Marble. “Deployment of Kentik’s platform was fast and easy, and we quickly learned Kentik’s solution would provide us with much more than just DDoS traffic detection.”

Results

With Kentik’s SaaS-based network analytics platform, OSHEAN has implemented a fully automated security mitigation architecture with numerous benefits.

With Kentik's real-time analytics solution and an automated service chain, OSHEAN prevented more than 300 volumetric attacks from affecting its members' networks in less than one year.

Automated DDoS Mitigation


The Kentik platform detects attacks using both historical profiling and attack signatures. Using Kentik's Restful API, OSHEAN developers stitched the detection trigger into its routing infrastructure to reroute the affected member traffic to the cloud-based scrubbing service, which then returns clean traffic. The network operations team then sends an informational email to the affected member organization with the Kentik analytics attack report attached. With Kentik's real-time analytics solution and an automated service chain, OSHEAN prevented more than 300 volumetric attacks from affecting its members' networks in less than one year.

"We were hesitant to consider a fully-automated DDoS mitigation approach. Initially, we had team members approving each mitigation because we thought there would be false positives," said Marble. "After a few weeks with Kentik, we began to trust the detection completely, and full automation is now easy and essential for us. We no longer have to sit around waiting for the next attack to happen. It's also great for our members, who typically don't even know they've been attacked, except for the email they receive saying an attack was attempted and resolved."

Cost and Performance Insights


With Kentik, OSHEAN has deep visibility into their members' traffic, including which content and cloud payloads that members access most frequently. OSHEAN uses these analytics to optimize caching and peering for that content, inform members of their own application usage, and make internal design decisions for its network topology.

"With Kentik we were able to see, for example, when one of our member universities was doing a huge data transfer from the east to the west coast over a commodity route. With Kentik's granular, detailed UI, we took a snapshot of what we were seeing and advised the university network team to move the traffic over to the research-optimized portion of the network for better performance at a lower cost," added Marble.

A light blue graphic element consisting of a large, stylized quotation mark shape, partially enclosing the text.

“For anyone considering
Kentik, I’d say to just go for it.”

— David Marble, OSHEAN
President and CEO

A network diagram in the top right corner of the page, showing a complex web of white lines connecting various nodes on a dark blue background.

OSHEAN has also integrated Kentik’s network traffic insights into their self-service web portal provided to member organizations. IT managers can now get quick answers to common traffic questions like top talkers, top applications, bandwidth utilization, latency, and top destinations without engaging OSHEAN’s customer support team.

Policy Enforcement Intelligence

“One of our K-12 member institutions distributed 4,000 Chromebooks to students. Using Kentik analytics, we observed a huge spike in traffic associated with the application Twitch, a video gaming platform,” said Marble. “We realized many students were watching videos, during and outside of the classroom, which was not part of their curriculum. The insight allowed this member to write better acceptable-use policies and implement on-going monitoring.”

Key Takeaways

“In our field, it’s not just about delivering bandwidth anymore. Delivering mission-critical content with security sets the tone. We can provide additional value to members by defending their networks and deeply understanding priority traffic behavior to drive down cost and improve performance. That’s why Kentik’s solution is so powerful for us,” said Marble. “For anyone considering Kentik, I’d say to just go for it.”

A network diagram in the bottom left corner of the page, showing a complex web of white lines connecting various nodes on a dark blue background.

ABOUT KENTIK

Easily the world’s most powerful network insight and analytics for the cloud-native world, Kentik® uses real-time traffic analysis, uniquely enriched with application, routing, and internet context to power the network operations of leading enterprises, cloud, and communication service providers (CSPs). Kentik’s SaaS platform is built on a patented big data engine to deliver modern network analytics that is both powerful and easy to use. Kentik is based in San Francisco — learn more at www.kentik.com.

Products from Kentik have patents pending in the US and elsewhere.