kentik

PhoenixNAP Adds Global Network Visibility and Automates DDoS Attack Mitigation with Kentik

phoenixNAP GLOBAL IT SERVICES

CATEGORY

- Data center and IT service provider

CHALLENGE

- Appliance-based network tool provided limited visibility in DDoS threats

SOLUTION

- Kentik Detect® for global network visibility and security

RESULTS

- Optimized network visibility
- Automated DDoS mitigation
- Significant cost-savings

Overview

Today's data center and IT service provider market is competitive. For the providers targeting the mid-market, the competition is even greater. Vendors compete and stretch limits to help buyers do more without risking affordability or performance. Some service providers meet demands by choosing legacy network technologies that fit within budgets but ultimately don't provide the visibility, scale, or security their customers require. The leading service providers are changing the game by investing in software-as-a-service (SaaS)-based network analytics to provide high-reliability, speed, and scale, without hidden costs or increased security risks. That's why phoenixNAP turned to Kentik.

Situation

PhoenixNAP is a data center and IT services provider that offers infrastructure-as-a-service (IaaS) solutions to mid-market companies. Founded in Arizona, phoenixNAP runs its own network backbone, connecting their Arizona facility to three international points-of-presence (POPs) in the Netherlands, Singapore, and Serbia. The company now offers bare metal servers, cloud, hardware leasing, and colocation services across the globe.

Mid-market companies worldwide come to phoenixNAP because its solutions are built to meet evolving technology demands without straining budgets or jeopardizing performance. So when phoenixNAP noticed an increase in distributed denial-of-service (DDoS) attacks targeting the mid-market, the IaaS provider knew it needed to ensure its data center systems were highly distributed and scalable. PhoenixNAP wanted to make certain that the increase in attacks wouldn't threaten its network or, in turn, the performance, availability, or security of its customers.

"As we observed the increasing scale of DDoS attack-attempts on our network, we knew the appliance-based DDoS detection tool we were using wouldn't be able to scale as quickly as we needed," said Ian McClarty, president of phoenixNAP. "We needed an innovative, cost-effective, scalable solution capable of providing real-time visibility to support all of our customers across the globe."

Solution

> "We needed an innovative, cost-effective, scalable solution capable of providing real-time visibility to support all of our customers across the globe."
>
> *- Ian McClarty, President, phoenixNAP*

The appliance-based tool phoenixNAP was using to alert on DDoS attacks allowed the company to see how traffic was coming into its network. However, the tool provided only siloed visibility to specific network segments where appliances were deployed. To improve security and performance, phoenixNAP decided to move away from the appliance-based approach and began evaluating SaaS-based solutions to expand visibility pervasively across their entire network.

The phoenixNAP team previously demoed Kentik's network traffic intelligence platform, Kentik Detect®. By the time the team re-architected to move away from appliances, Kentik's capabilities matched precisely what phoenixNAP required in a new DDoS solution.

"In finding a new solution, we wanted to ensure we had eyes on our whole network," said Danny Fuentes, director of information systems at phoenixNAP. "In the first few days of deploying Kentik, we knew we made the right decision. Kentik provides the granular, single-pane-of-glass visibility we needed."

Results

> "In the first few days of deploying Kentik, we knew we made the right decision. Kentik provides the granular, single-pane-of-glass visibility we needed."
>
> *- Danny Fuentes, Director of Information Systems, phoenixNAP*

With Kentik Detect, phoenixNAP realizes the following benefits of network traffic intelligence:

OPTIMIZED NETWORK VISIBILITY

With deeper network visibility from Kentik, phoenixNAP has a new view of its network traffic, both in real-time and historically via Kentik's 90-day full forensic data retention capabilities. The provider can quickly identify whether an alert is caused by a network performance issue, misconfiguration, or DDoS attack. The team also leverages Kentik Detect's Custom Dimensions feature, which allows phoenixNAP to map its business data onto network data for instant context – to understand not only IP addresses, interfaces, ports and protocols, but also gain instant context on which customers, categories, and service names were affected to inform faster decision-making about response.

"For less than the support costs of our previous appliance-based tool, Kentik provides us with a far-stronger solution that powers a new level network visibility, scale, and security for our customers."

- Ian McClarty, President, phoenixNAP

AUTOMATED DDOS MITIGATION

With Remote Triggered Black Hole (RTBH), Kentik Detect is the first layer of DDoS defense automation for phoenixNAP. RTBH allows phoenixNAP to automatically drop malicious traffic, prevent collateral damage to adjacent customers, and dramatically improves initial response time to attacks. Kentik's BGP route injection also allows the phoenixNAP team to steer traffic toward multiple layers of more advanced filtering to protect the attacked customer.

SIGNIFICANT COST-SAVINGS

With its previous appliance-based DDoS attack detection tool, phoenixNAP was paying over $100,000 per year on support and maintenance costs. Because Kentik Detect is a SaaS-based solution with included support and no future appliance refresh costs, phoenixNAP has seen – and will continue to see – significant cost savings.

Key Takeaways

"For less than the support costs of our previous appliance-based tool, Kentik provides us with a far-stronger solution that powers a new level network visibility, scale, and security for our customers," said McClarty.

"With Kentik in place, we have full visibility into our network traffic."

- Danny Fuentes, Director of Information Systems, phoenixNAP

"We now know immediately if we have a security or performance problem. We know when there are spikes or drops in traffic for a client, and we can quickly investigate to understand the cause. We can tie network traffic events to specific carriers or infrastructure components, and ultimately, better support our customers," added Fuentes. "With Kentik in place, we have full visibility into our network traffic."

ABOUT KENTIK

Kentik is the network traffic intelligence company. Kentik turns network traffic – billions of digital footprints – into real-time intelligence for both business and technical operations. Network operators, engineers, and security teams use Kentik to manage and optimize the performance, security, and potential of their networks and their business. To learn more about Kentik and its award-winning solutions, visit www.kentik.com.

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