

DreamHost Protects Service Performance and Brand Reputation with Network Traffic Intelligence and Security Automation from Kentik



CATEGORY

- Web hosting provider

CHALLENGE

- Brand reputation and operational overhead were threatened by DDoS attacks
- Open source monitoring tool and commercial appliances did not scale to detect and mitigate DDoS attacks in real time

SOLUTION

- Kentik Detect for network traffic intelligence and security

RESULTS

- Real-time operational visibility benefiting both technical and business operations
- Powerful network troubleshooting capabilities
- Security automation

Overview

Hosting providers are in a highly competitive market, driven by their ability to deliver the fastest, most reliable internet connectivity. Customers won't hesitate to change providers if their host is unable to meet stringent performance and security requirements. On top of that, providers face an uphill battle in actively monitoring their vast network traffic to ensure they do not support malicious users, who purchase hosting services to carry out costly distributed denial-of-service (DDoS) attacks. These malicious users cost providers plenty, both in transit overage fees and in brand damage. To gain network visibility and stay ahead of these threats without straining operational overhead, hosting provider DreamHost turned to Kentik.

Situation

DreamHost is a Los Angeles-based web hosting provider and domain name registrar that has hosted enterprise and consumer sites since 1997. Hosting more than 1.5 million sites with over 400,000 customers, DreamHost continues to grow after 20 years in business because it delivers an excellent customer experience via always-on, fast and secure access to its hosting services. The hosting provider is committed to providing top network performance and security that allows its customers to own their digital presence while maximizing their digital privacy.

To support network operations and DDoS defense, DreamHost built its own open source network traffic monitoring tool, combined with commercial DDoS detection appliances. However, as the hosting provider's customer base grew, it realized that driving the best customer experience would require deeper insights into potential network issues and automated defense against DDoS attacks. At the same time, a larger customer base meant DreamHost needed a solution capable of monitoring a massive volume of network traffic in real time to ensure abuse was not happening on its servers. Specifically, DreamHost needed to be certain that new customers were not buying web servers to launch outbound UDP flooding attacks.

“We knew immediately Kentik was the only solution that we could instantly implement to address our traffic intelligence and security needs while handling the sheer volume of network traffic we see.”

—James Gomez, Senior Network Engineer, DreamHost

As a type of denial-of-service attack, UDP floods can cause hosting providers to violate transit contracts with their telecommunications providers. These contract overages result in companies having to pay their transit providers by gigabit or megabit above the contract allotment, costing thousands of dollars per incident. The attacks can also cause a hosting company to be blacklisted by transit providers and damage their brand reputation severely.

With the size of its network and sheer volume of traffic, DreamHost understood the enormous challenges of building its own next-generation network intelligence solution to ensure uptime and security, while continuing to give its customers the highest level of service.

Solution

“We push about 40 to 50 gigabits per second (Gbps) of network traffic from our IP edge,” said James Gomez, senior network engineer at DreamHost. “When we started considering our options for a new network management solution, we realized it would require a lot of different types of software. We typically adopt things from the open-source community, but we knew there was a real lack of tooling and challenge with ease of adoption for this specific effort. To do the amount of NetFlow capture, collection, and analysis for the size of network traffic we manage, we came to a quick realization that we needed an always-on solution that was both secure and production ready.”

“Fortunately, we quickly found Kentik and its SaaS offering,” added Gomez. “We knew immediately Kentik was the only solution that we could instantly implement to address our traffic intelligence and security needs while handling the sheer volume of network traffic we see.”

DreamHost deployed Kentik Detect, and from day one, the hosting provider was able to leverage the rich intelligence from their network traffic to improve and optimize their services.



“When it comes to detecting DDoS attacks, we could not find another solution capable of providing the speed and accuracy that Kentik provides us.”

– James Gomez, Senior Network Engineer, DreamHost

Results

With Kentik, DreamHost has achieved the following results:

ELIMINATION OF ABUSE

Kentik helps DreamHost to quickly find and mitigate abuse on its networks, stopping UDP flood attacks before they cause outages. Finding the attacks and shutting them down fast saves DreamHost thousands of dollars annually as the company is able to avoid high transit contract overages. It also preserves DreamHost’s strong brand reputation and always-on services.

DDOS PROTECTION

Through Kentik’s integration partnership with A10 Networks, DreamHost leverages Kentik’s SaaS solution to automate DDoS detection and mitigation triggering to stop attacks in real time, before they can cause harm to the network. Kentik’s solution combined with A10’s advanced DDoS mitigation capabilities enable DreamHost to quickly escalate suspect traffic through progressively tougher countermeasures to minimize the impact on its legitimate traffic.

With deeper visibility into its network traffic and automated alerts and triggering, DreamHost reduces the time it takes to mitigate attacks, ensuring higher service quality to its customers. In addition, increased automation saves money by eliminating the time that network experts previously spent on triaging alerts and manually triggering mitigation.

“We have anywhere from 10 to 20 mitigations going each day, which required a lot of the team’s focus. Automating the process with help from Kentik has greatly reduced our need for manual interactions, which ultimately saves us time and money. When it comes to detecting DDoS attacks, we could not find another solution capable of providing the speed and accuracy that Kentik provides us,” said Gomez.

CROSS-DEPARTMENTAL NETWORK VISIBILITY

More than 20 members of the DreamHost operations team regularly use Kentik for network visibility and security automation. DreamHost's engineering team used the Kentik API to provide user-friendly question and answer tools for extended operations personnel, eliminating a critical information bottleneck around network intelligence.

DreamHost expects even more of its TechOps team will soon begin to use the solution as the company further leverages Kentik's powerful APIs. "We're quickly integrating Kentik deeper into TechOps process and workflows," added Gomez.

Key Takeaways

With Kentik, DreamHost gained real-time operational visibility, powerful network troubleshooting capabilities, and security automation that impact both technical and business operations. As a result, DreamHost has been able to significantly increase network uptime while reducing the amount of resources the hosting provider spends dealing with network issues.

"Kentik gives us better introspection into our network, and it's a great solution for us," said Gomez.

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.