kentik

Viasat Taps Kentik for Real-Time Visibility of Critical Broadband Networks

Viasat

CATEGORY

- Broadband provider

CHALLENGE

- Legacy tools not capable of incorporating traffic variations correctly, producing high volume of false positives and false negatives

SOLUTION

- Real-time monitoring and investigation insights from Kentik

RESULTS

- Accurate baselining for faster security investigations
- Powerful APIs for data customization and automation
- Out-of-box accessibility and ease of use for cross-department ROI

Overview

Today's broadband providers share a common goal: to deliver fast, always-on, secure connectivity to customers. To execute on that goal, providers operate some of the largest, most complex networks. Satellite-based providers who serve hard-to-reach customers have an additional challenge: managing high infrastructure costs on a price-per-bit basis. Visibility into their network performance and security is critical. Any network downtime, or even just the presence of unnecessary traffic, can result in significant financial loss for both the providers and their customers. That's why high-speed satellite broadband provider Viasat turned to Kentik.

Situation

Viasat is a global provider of high-speed satellite broadband services and secure networking systems. In business for more than 30 years, Viasat has launched two satellites into orbit, acquired two additional satellites, and supported everything from military communications, marine vessels, and Wi-Fi for passengers onboard airplanes.

With more than 4,500 employees across 26 offices worldwide, Viasat's vision is centered on making sure "affordable, secure and, above all, high-quality connections are available even in the hardest-to-reach places." To make good on that vision, Viasat requires real-time visibility into its network traffic for optimized broadband performance and security.

While Viasat was previously using several commercial tools to monitor network traffic and alert to incidents, the legacy tools weren't capable of incorporating normal daily or weekly traffic variation into their detection algorithms, producing a high volume of both false positives and false negatives. With a continuous stream of traffic anomalies like denial-of-service attacks, Viasat knew it needed a fast, accurate, real-time network traffic analytics platform to prevent outages and cost exposure from carrying unnecessary traffic across expensive satellite links.

Solution

At NANOG, a conference for network operators, the Viasat team met Kentik and learned of Kentik Detect®, the SaaS-based modern network analytics platform. With Kentik Detect's ability to provide network visibility both in real-time and historically via its 90-day full forensic data retention capabilities, it was the solution Viasat was looking for.

"When we deployed Kentik, we quickly gained live security monitoring and security investigation insights," said Alex Kitthikoune, network administrator for Viasat.

> "When we deployed Kentik, we quickly gained live security monitoring and security investigation insights."
> *— Alex Kitthikoune, Network Administrator*

Results

Kentik Detect provides Viasat with the following benefits:

Accurate Baselining for Faster Security Investigations

With Kentik's baselining capabilities, Viasat can set policies that trigger alarms based on comparisons of its current network traffic against historical traffic patterns. This allows Viasat to fingerprint network abuse and attacks and instantly offload or quickly investigate live traffic when alerted to a pattern of potentially malicious traffic. Using baselining from Kentik, Viasat has identified more than 1,700 attacks and similar incidents, and has prevented over 60 Terabytes of malicious or unnecessary traffic from traversing their satellites. This has saved the Viasat team a significant amount of time they would have otherwise spent manually hunting for incidents or investigating to determine whether each could be a false positive or an actual issue. Eliminating the unwanted traffic has also had a measurable impact on customer experience, and reduced cost by slowing network traffic growth.

> "With such good visibility from Kentik, we're able to offload traffic that's malicious in nature with a much greater degree of accuracy."
> *— Alex Kitthikoune, Network Administrator*

"With such good visibility from Kentik, we're able to offload traffic that's malicious in nature with a much greater degree of accuracy," said Kitthikoune.

kentik

> "The way Kentik displays and visualizes traffic and the intuitive UI make it easy for our teams to pick up anomalies and drill into investigations."
> *— Lee Chieffalo, Senior Network Engineer*

Powerful APIs for Data Customization and Automation

"With Kentik's powerful APIs, we can automatically import our internal threat and IP reputation data," said Lee Chieffalo, senior network engineer at Viasat. "In combination with Kentik's built-in IP reputation data, we can tag potentially malicious traffic flows and automatically detect, for example, whether there are scanners or brute-force attacks coming in from over the internet. We also use Kentik's APIs for closed-loop automation so that network actions, like blocking a malicious IP, automatically silence further alarms."

Out-of-the-Box Accessibility & Ease of Use for Cross-Department ROI

Only three of Viasat's security team members attended training for Kentik Detect at the time of the company's deployment. Yet, because Kentik's platform was designed with accessibility and an easy-to-use user interface (UI) in mind, Viasat found that many of its teams were able to leverage and gain insights from the platform instantly, without spending time and holding up resources dedicated to training. Now nearly 10 security team members, 40 people in Viasat's Network Operations Center, and 20 NetOps and security employees from the Viasat Government team use Kentik Detect.

"The way Kentik displays and visualizes traffic and the intuitive UI make it easy for our teams to pick up anomalies and drill into investigations," said Chieffalo. "Using Kentik's built-in sharing tools, our security team can quickly direct our network team to what they're looking at, and the network team can instantly view the same issue and data. With that kind of collaboration, the teams can more quickly triage and resolve both network and security incidents, which has led to an overall reduction in our mean-time-to-investigate (MTTI) and mean-time-to-resolve (MTTR)."

> “Kentik has allowed us to remove a substantial amount of abusive and malicious traffic from our network, with a huge measurable impact on our bottom line.”
>
> *— Alex Kitthikoune, Network Administrator*

Key Takeaways

“With the high cost-per-bit of satellite infrastructure, bandwidth is a precious resource for us. Kentik has allowed us to remove a substantial amount of abusive and malicious traffic from our network, with a huge measurable impact on our bottom line,” said Kitthikoune.

“Our overall experience with Kentik Detect on our network has been great. Kentik is so much faster than legacy tools and its baselining capabilities are a strong value-add for us,” added Chieffalo.

ABOUT KENTIK

Easily the world’s most powerful network insight and analytics, Kentik® uses real-time flow analysis, uniquely enriched with application, routing, and internet context to power the network operations of leading enterprises and 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.