kentik

Case Study

PenTeleData Keeps DDoS at Bay With Kentik Detect

Category

Communications Service Provider: voice, video, data, and Internet.

Challenge

DDoS defense with outmoded detection appliances.

Solution

Kentik Detect for accurate detection and automated mitigation via Radware DefensePro.

Result

30+ percent increase in protection accuracy; fewer service-threatening disruptions.

Upgrade enables accurate detection and automated mitigation

As the scale and sophistication of Distributed Denial of Service attacks continues to accelerate, first-generation DDoS defense solutions fall further behind. That leaves online businesses without adequate protection, vulnerable to potentially severe interruptions in service and revenue. One company that's been keenly aware of this risk is PenTeleData, a leading provider of voice, video, data, and Internet services with more than sixty points of presence in Pennsylvania and New Jersey. Having dealt with the shortcomings of legacy DDoS protection tools, PenTeleData decided to update defenses and extend better protection to subscribers. To do so, PenTeleData turned to Kentik, applying the extended anomaly detection, alerting, and mitigation triggering capabilities built into Kentik Detect.

PenTeleData®

> *"As a network-based business, the ability to use a single tool to find, remediate, dig into, and truly understand not just DDoS but all other manner of operational and planning issues makes it much easier to do our job, which at the end of the day is to deliver excellent service."*
>
> - Brian Mengel, CTO of PenTeleData

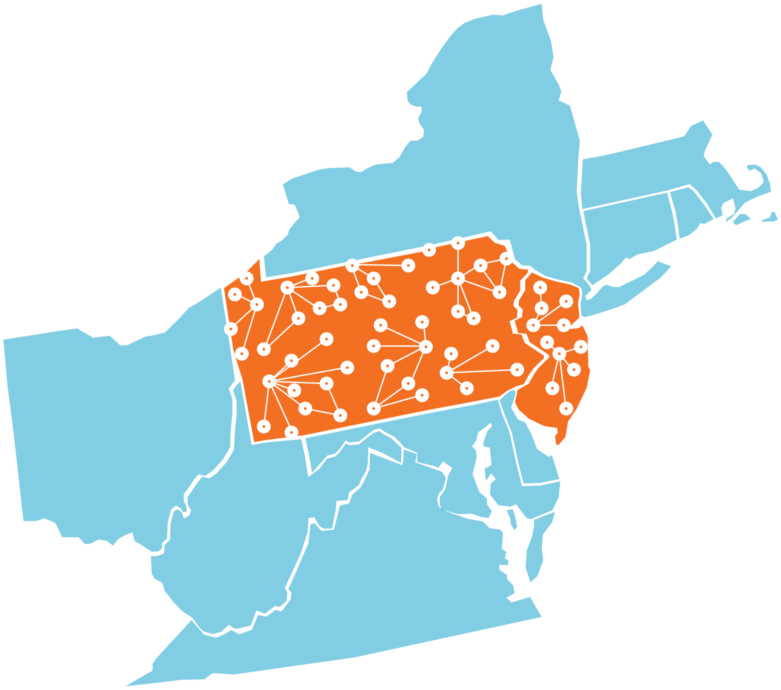
DDoS Detection

Automated DDoS Mitigation

Big Data Analytics

Situation

Founded in 1994, PenTeleData is a strategic partnership of local cable and telephone companies, including Service Electric Cable TV and Communications, Service Electric Broadband Cable, Service Electric Cablevision, Ironton Telephone, and Blue Ridge Communications. The PenTeleData partnership has invested more than $300 million in fiber optic infrastructure, operating nearly 10,000 miles of fiber optic cabling. PenTeleData serves customers in all facets of life, from home to business, including sectors such as banking, healthcare, education, government, retail sales, and the wireless industry.



Prior to Kentik, PenTeleData depended on an appliance-based DDoS detection system. With the limited compute and memory capabilities typical of legacy designs, the system suffered from severe constraints on its baselining capabilities, which forced PenTeleData to rely on overly broad, simple rate-based DDoS detection policies. Since individual IPs weren't baselined with sufficient granularity, a steady stream of DDoS attacks were missed by these policies, impacting subscribers as well as the service network itself.

"Our Network Control Center (NCC) was continuously dealing with attack traffic that hadn't been detected or mitigated and threatened to degrade service," says Frank Clements, Engineering Manager at PenTeleData. "Aside from the risk to our service quality, we were losing a lot of staff time that would have been better spent on more productive projects."

Solution

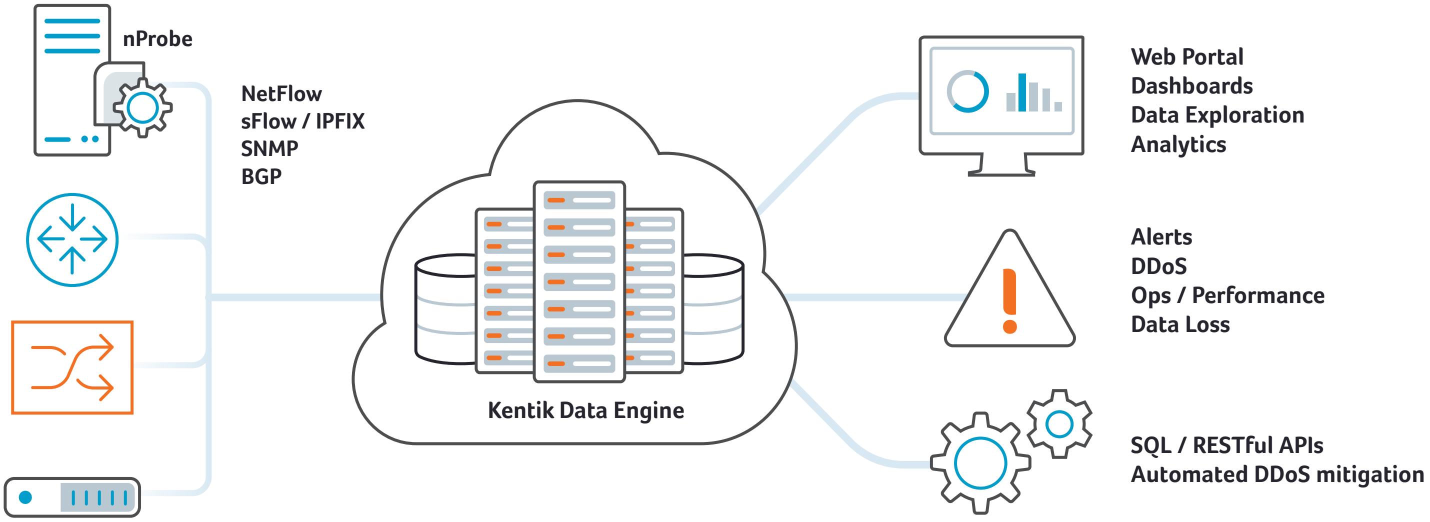
PenTeleData had been an early adopter of Kentik Detect, using the industry's only big data-based network visibility solution since 2014. In May 2016 PenTeleData was the first to deploy Kentik Detect's newly enhanced DDoS functionality. Among the enhancements is a set of integrations with leading providers of mitigation solutions, so that Kentik Detect can automatically trigger a mitigation response when the network is under attack.

Kentik also substantially enhanced its alerting system to enable more sophisticated policies for anomaly detection. The new system includes an auto-adaptive baselining capability that continuously monitors millions of individual IP addresses (IPs), recognizes and focuses on the IPs that are currently the top traffic receivers, automatically baselines their traffic patterns, and measures anomalies in their traffic.

At PenTeleData, the Kentik alerting system is configured such that when an attack is detected, Kentik Detect signals PenTeleData's Radware DefenseFlow platform, which then activates mitigation via either Radware DefensePro appliances or Cloud DDoS Protection Service. The end-to-end system has been in full production, automatically detecting and mitigating DDoS attacks, since June 2016.

Results

Pairing Kentik Detect with Radware mitigation has proven to be transformative for PenTeleData's DDoS defenses. The company has experienced a greater than 30 percent improvement in catching and stopping DDoS attacks of varieties that the previous solution missed. In addition to fewer false negatives, NCC personnel also noticed far fewer false positives, which has saved countless hours of wasted work and stress.



"When we first deployed Kentik Detect, we started seeing attacks that weren't being caught by our previous DDoS defense solution," Clements says. "Once we set Kentik Detect to automatically trigger mitigation via our Radware DefenseFlow platform, the constant pattern of interrupts and firefighting really quieted down."

As important as DDoS protection is to PenTeleData, their use of Kentik Detect isn't limited to a single use case. Kentik Detect offers PenTeleData a comprehensive, silo-free platform for insights into all aspects of network operations, ranging from availability and performance to planning and peering.

"Kentik Detect has become a trusted source of visibility for our teams," says Brian Mengel, CTO of PenTeleData. "As a network-based business, the ability to use a single tool to find, remediate, dig into, and truly understand not just DDoS but all other manner of operational and planning issues makes it much easier to do our job, which at the end of the day is to deliver excellent service."

Learn more about DDoS Protection with Kentik Detect.
Contact us at sales@kentik.com to request a demo . Or visit www.kentik.com to sign up for a free trial.