

Networking and security professionals face a constant challenge in understanding, managing, and protecting IT and service infrastructures that are far flung, dynamic, and virtual. The problems only get greater as application complexity increases and cloud becomes a daily reality. Kentik® and Palo Alto Networks® work together to provide insightful telemetry and advanced, automated analytics for improving visibility, optimizing network efficiency and protective policy, and providing the operational and security intelligence needed to keep users, partners, and customers safe and productive.

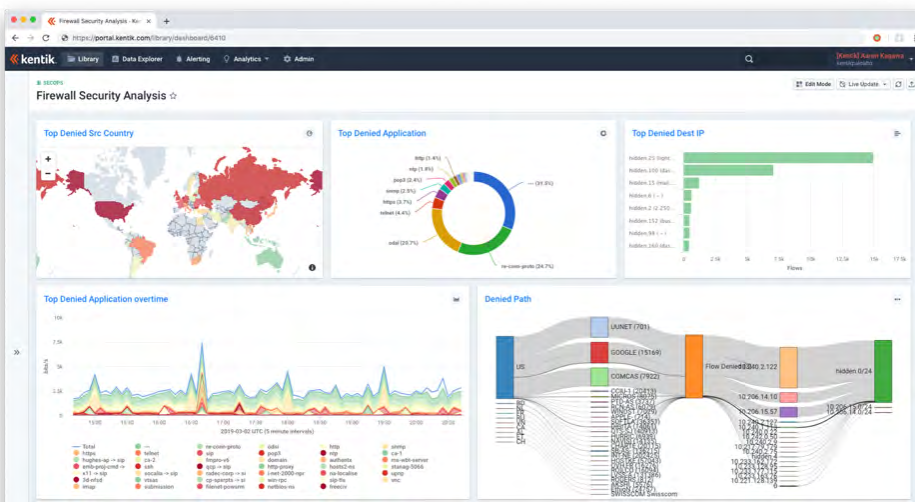
## Use Case #1: Extending Network and Application Visibility

### CHALLENGE

Establishing an end-to-end view of network and application traffic across geographically and topologically diverse infrastructures

### SOLUTION

Add IPFIX data from Palo Alto Networks firewalls into Kentik's traffic monitoring and analytics. Locations that have a Palo Alto Networks firewall present can now contribute telemetry, helping network operations and application support teams to better understand which applications are active across the infrastructure and who is using them, from data center to branch to cloud.



## Benefits

Expanded end-to-end network traffic visibility for improved recognition of user and application activity across private, hybrid, and multi-cloud infrastructures

Correlated views of multi-site traffic patterns for identifying and responding to coordinated attack activity

Clear identification of accepted and rejected traffic flows, including source and destination IPs and application markers

Rich data store for fast incident investigation and forensic analysis

Detailed composition and trending views for capacity planning and traffic engineering



## Use Case #2: Traffic Pattern Recognition and Response

### CHALLENGE

Recognizing coordinated attack patterns across multiple locations

### SOLUTION

Use Kentik's ability to provide centralized visibility for large and geographically broad deployments of Palo Alto Networks firewalls, so that common patterns of legitimate and illegitimate network traffic can be recognized, common sources identified, and actions taken to mitigate ongoing impact to network availability and proficiency.

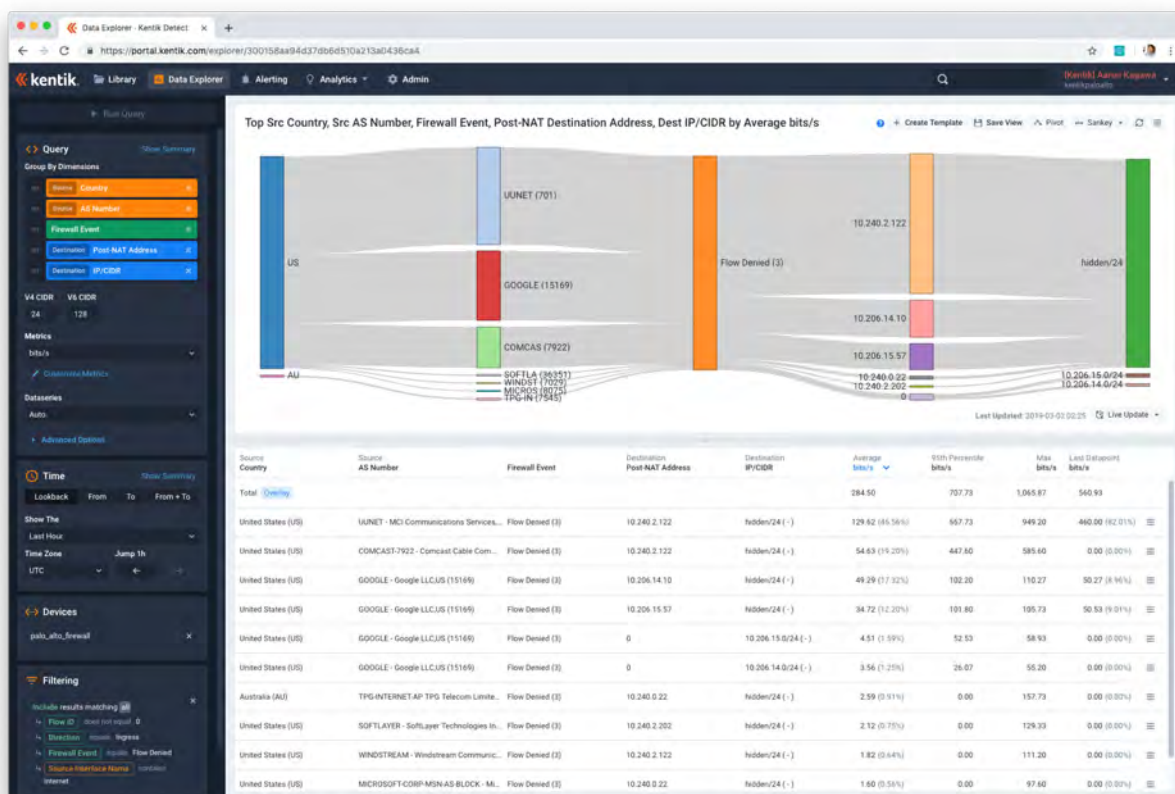
## Use Case #3: Firewall Policy Verification and Tuning

### CHALLENGE

Recognizing business intent and assessing policy impact across a global infrastructure

### SOLUTION

Analyze denied and accepted traffic flows. View traffic in Kentik by flow accept or deny status to reveal who is driving traffic that is getting denied, what the traffic is, in what volume, and from where.



## Use Case #4: Integrating Forensic Analysis

### CHALLENGE

Understanding the full scope of activity of a particular application, user, or network node, when an operational incident or security threat dictates deeper investigative workflows.

### SOLUTION

Add flow data from Palo Alto Networks firewalls into the Kentik data store, for access to a full resolution historical store of activity to mine and explore.

## Use Case #5: Network Capacity Planning

### CHALLENGE

Recognizing resource exhaustion at remote sites

### SOLUTION

Send flow data records to Kentik, to monitor maximum peak activity and growth trends in traffic traversing Palo Alto Networks firewalls, to ensure that sufficient capacity is available for continuous protection.



**ABOUT KENTIK** | Easily the world’s most powerful network insight and analytics for the cloud-native world, 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](http://www.kentik.com).

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

**ABOUT PALO ALTO NETWORKS** | We are the global cybersecurity leader, known for always challenging the security status quo. Our mission is to protect our way of life in the digital age by preventing successful cyberattacks. This has given us the privilege of safely enabling tens of thousands of organizations and their customers. Our pioneering Security Operating Platform emboldens their digital transformation with continuous innovation that seizes the latest breakthroughs in security, automation, and analytics. By delivering a true platform and empowering a growing ecosystem of change-makers like us, we provide highly effective and innovative cybersecurity across clouds, networks, and mobile devices.

Find out more at [www.paloaltonetworks.com](http://www.paloaltonetworks.com).