Neutralize DDoS attacks. Analyze incidents. Catch botnets.

Cyber attacks have evolved significantly over the last several years. Not only are attacks more frequent, but the approaches used by attackers are more sophisticated and subtle. To offset these challenges, your attack detection also needs to evolve. Malicious traffic detection needs to be more intelligent, and capable of quickly mitigating different types of attacks. Attack mitigation needs to be automated, and should provide organizations with a way to analyze the effectiveness of the mitigation and track its impact on users.

Many of our customers rave about how Kentik helps them detect and automate the mitigation of DDoS attacks. Kentik Protect is a SaaS offering and provides customers the benefit of advanced DDoS defense and malicious traffic detection without the delays, capital investment, and ongoing costs of building and maintaining their own threat detection system.

> *"You want to look at traffic volumes, but with Kentik we also can look at source IPs, AS numbers, and other metrics to see if it's a distributed attack. This is so easy to do in Kentik; you simply add the source IP address dimension to the analysis.*

> *With some security tools, it's already too late when you get a notification. But with the DDoS filters in Kentik turned on, we get notified immediately.*

Booking.com

Key benefits

- Eliminate false positives and negatives
- Investigate attacks in detail
- Enable turn-key, vendor-neutral protection
- One platform for detection, mitigation, and investigation
- Create and differentiate "clean pipe" services
- See the impact of rejecting RPKI-invalid routes before activation
- See the origin and impact of botnets and threat traffic

Key capabilities

- Accurate and flexible anomaly and DDoS detection
- Integrated automation with mitigation providers
- Native RTBH/Flowspec support
- Ad-hoc forensic analytics on years of network traffic
- Easy integration via JSON APIs
- Accurate real-time threat intelligence service
- White-label My Kentik Portal, enabling DDoS-as-a-service and threat analysis with network analytics

DDoS detection and mitigation

Kentik Protect is the industry's most accurate DDoS and network anomaly detection solution, offering field-proven accuracy gains of 30 percent in attack recognition. How does it work?

Understand incident details and causes. Drill down into forensic analytics in real time or retroactively.

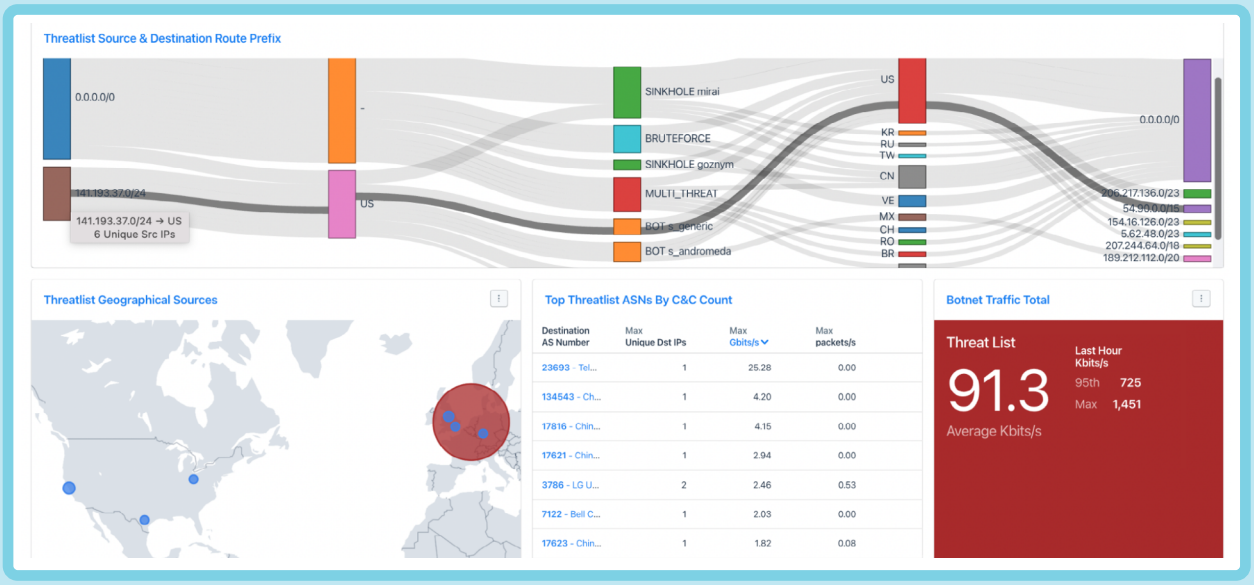
- It ingests and unifies, in real time, massive volumes of NetFlow, sFlow, IPFIX and BGP data, network performance metrics, and SNMP device and interface data.
- It applies the scale-out power of the Kentik Network Observability Cloud to network-wide scanning of billions of rows of data using multi-dimensional criteria and adaptive baselining.
- It automates hybrid mitigation via standards-based BGP Flowspec and remote-triggered black hole (RTBH), as well as integrations with mitigation solutions from leading vendors, including Cloudflare, A10, Juniper and Radware.
- It enhances the ability to investigate and understand attacks with deep ad-hoc traffic analysis, flexible dashboarding, botnet detection, and network performance monitoring.

Just getting an alert that traffic patterns have changed is not enough. Kentik Protect allows you to quickly double-click from an alert into an advanced Data Explorer query. This is powerful because you can dive into the details of an attack, filter down, and compare across time frames. Most legacy application-based DDoS detection systems cannot do this because they only aggregate data.

Kentik Protect also incorporates a feature that allows you to determine the impact of rejecting RPKI-invalid traffic. This feature gives you an intimate understanding of the impact on your traffic globally if you were to reject RPKI-invalid statuses.

Threats and botnets

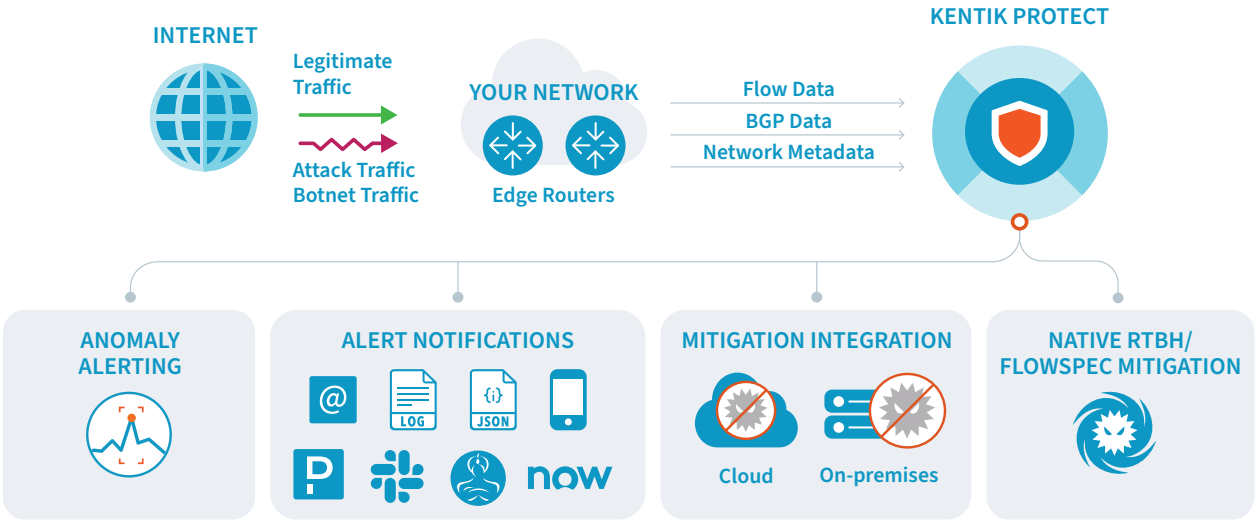
Kentik helps you find traffic from infected or compromised hosts by enriching flow records with IP reputation data from Spamhaus. The result is two dimensions, Botnet Command and Control and Threat List Host, which are then used to identify threats to your network, such as botnet command and control servers, malware distribution points, phishing websites, spam sources, and more.



Partial view of the Kentik Botnet & Threat-feed Analysis dashboard. Identify and analyze botnet and threat-feeds — their size, impact, and origin. Included for all customers at no additional cost.

We make these threats known to you via the Botnet & Threat-feed Analysis dashboard. The panels illustrate the extent to which traffic on your network is associated with known risks.

Kentik end-to-end DDoS and attack protection



"Kentik is our global standard for detecting DDoS attacks. There isn't a single minute in the day that we're not attacked somewhere, so it's crucial for us to have a reliable service to detect attacks and trigger mitigation measures."

GoDaddy

Summary

The Kentik Network Observability Cloud delivers the industry's most accurate and automated DDoS detection against various types of DDoS attacks (volumetric, application, etc.), botnet, and threat attack traffic, giving security and operations teams full forensics capabilities across months of raw data.

ABOUT KENTIK | Kentik is the network observability company. Our platform is a must-have for the network front line, whether digital business, corporate IT or service provider. Network professionals turn to the Kentik Network Observability Cloud to plan, run and fix any network, relying on our infinite granularity, AI-driven insights and ridiculously fast search. Market leaders like IBM, Box, and Zoom rely on Kentik for network observability. Visit us at kentik.com and follow us at @kentikinc.

Revised 20220906