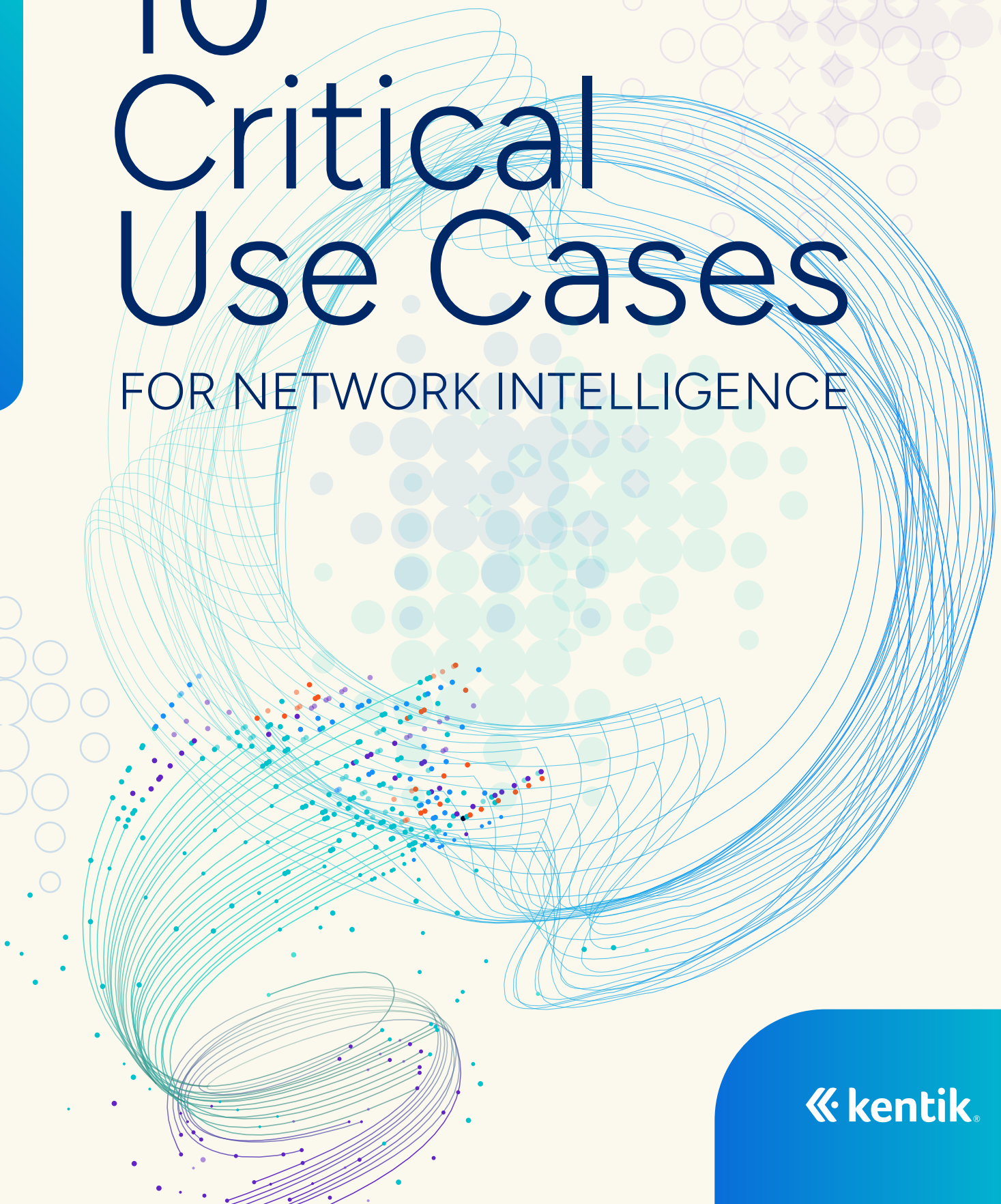
10 Critical Use Cases

FOR NETWORK INTELLIGENCE



kentik®

Table of Contents

Introduction

In today's fast-paced digital landscape, the network is no longer just an IT utility; it has become the central nervous system of every modern business. Yet, as infrastructures grow more distributed and complex, spanning diverse cloud regions, on-prem data centers, and countless applications, gaining accurate control has become an immense challenge. Traditional monitoring and even early observability solutions, while valuable, often leave network teams reacting to problems after they've already impacted users, relying on heroic efforts and deep, hard-won expertise to pinpoint elusive root causes.

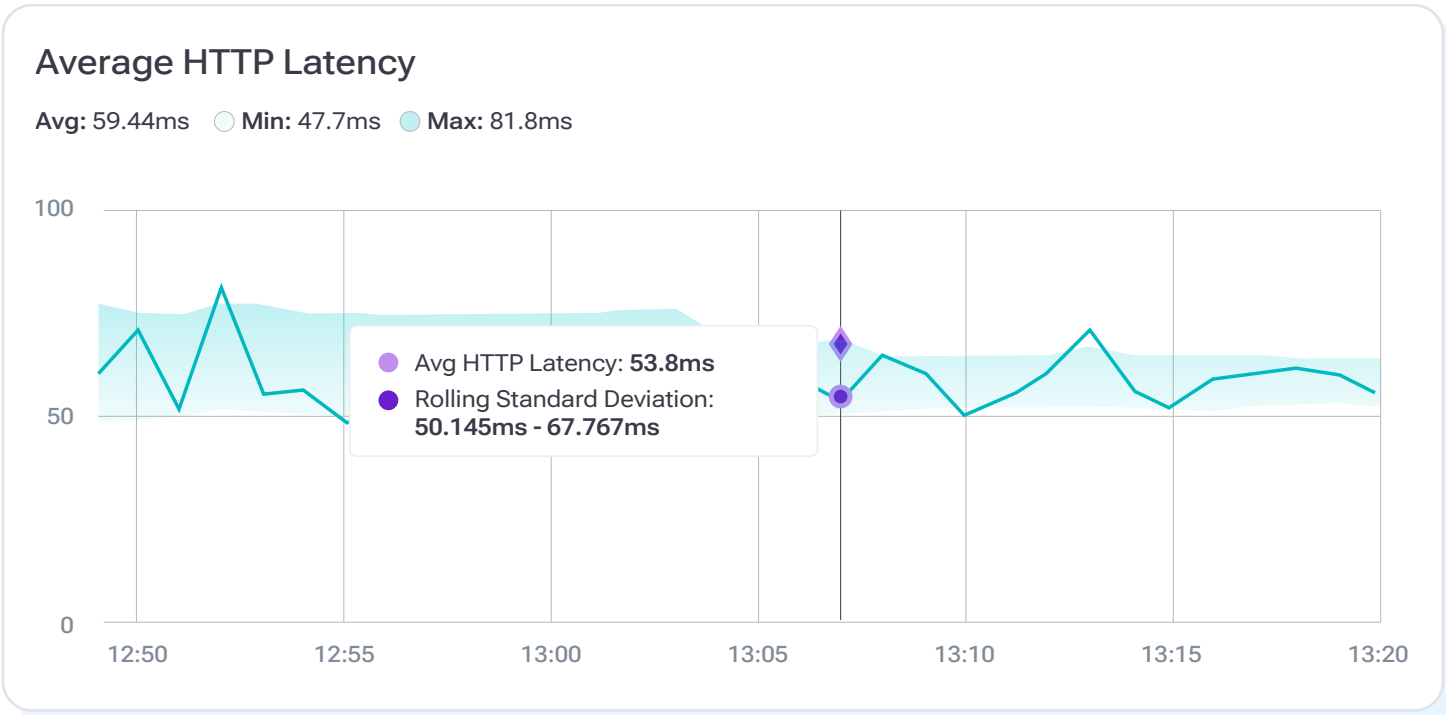
What if you could transcend this reactive cycle? What if your network could actively inform you of impending issues, reveal hidden patterns, and guide you toward optimal performance and cost efficiency before a single customer is affected? This is the transformative power of network intelligence. By combining high-fidelity telemetry with advanced AI, network intelligence provides a holistic, contextualized view that empowers engineers to move from firefighting to strategic foresight. This ebook will dive into **10 critical use cases** that demonstrate how network intelligence is not just an evolution, but a fundamental shift in how organizations will build, manage, and secure their digital foundations.

In the image above, telemetry such as latency and packet loss are measured over time and compared to a dynamically created rolling baseline of normal behavior. These metrics can then be correlated with each other in a time series to show how a spike in one relates to a spike in another.

01 Correlate diverse data to provide contextualized network visibility

Network intelligence ingests high-volume telemetry and enriches the data with relevant business information to identify correlations and provide contextually relevant insights.

By combining these disparate signals into a single, contextualized narrative, network intelligence provides engineers with holistic visibility, allowing them to see not just that packets are dropping, but also which business service, customer segment, or revenue stream is affected. This accelerates incident response, reduces the mean time to resolution between network, application, and security teams, and helps engineers understand what is impacted to prioritize triage activity.



In the image above, notice that the system programmatically created a rolling standard deviation using Z-scores to determine what "normal" HTTP latency is over a given timeframe. That way, when HTTP latency deviates significantly, the system can measure the delta, flag it as an anomaly, and send an alert.

02 Identify traffic patterns, seasonality, baselines, and benchmarks

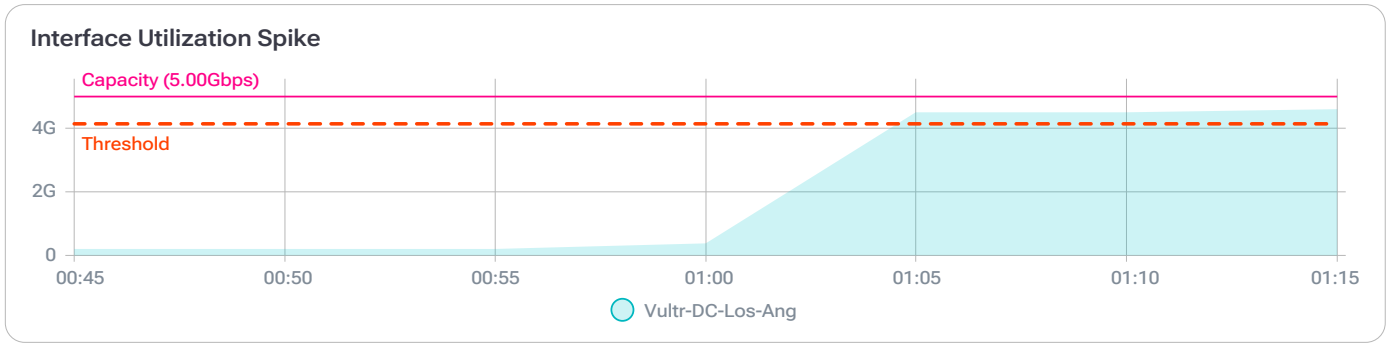
Network intelligence continuously analyzes network data to learn the normal rhythm of traffic. From hourly bursts from backup jobs, lunchtime video spikes, and quarter-end ERP surges, Kentik establishes dynamic baselines and benchmarks that adapt to growth while still flagging anomalies, as well as providing alerts on performance against service-level agreement (SLA) targets.

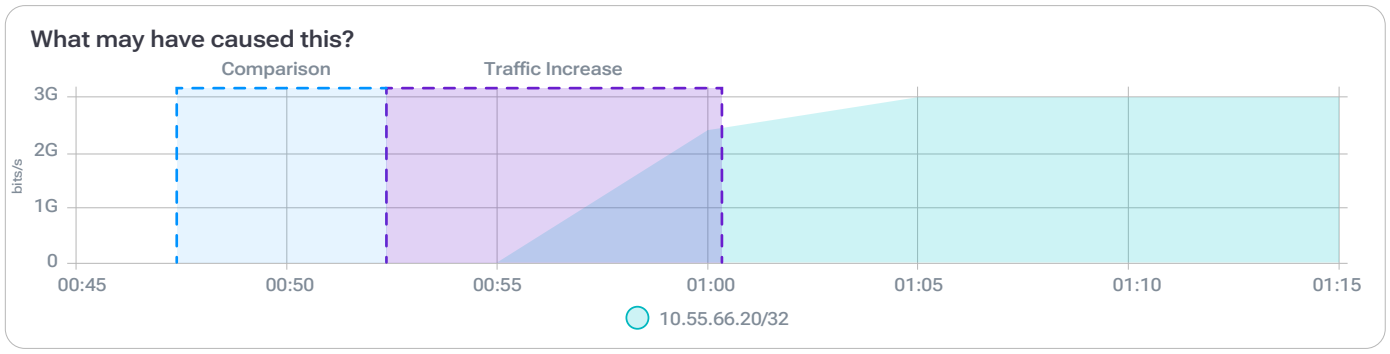
With AI, network intelligence models those cycles as seasonality patterns that update as the environment evolves. Engineers can identify what's normal and what's anomalous, thereby improving their ability to make sense of network data in relation to the business's needs.

Interface Utilization Spike

We detected a **2140.3% increase** in bandwidth on TenGigabitEthernet4 and found the causes were **Src IP/CIDR**: 10:55.66.20 **Src Port**: 33222.

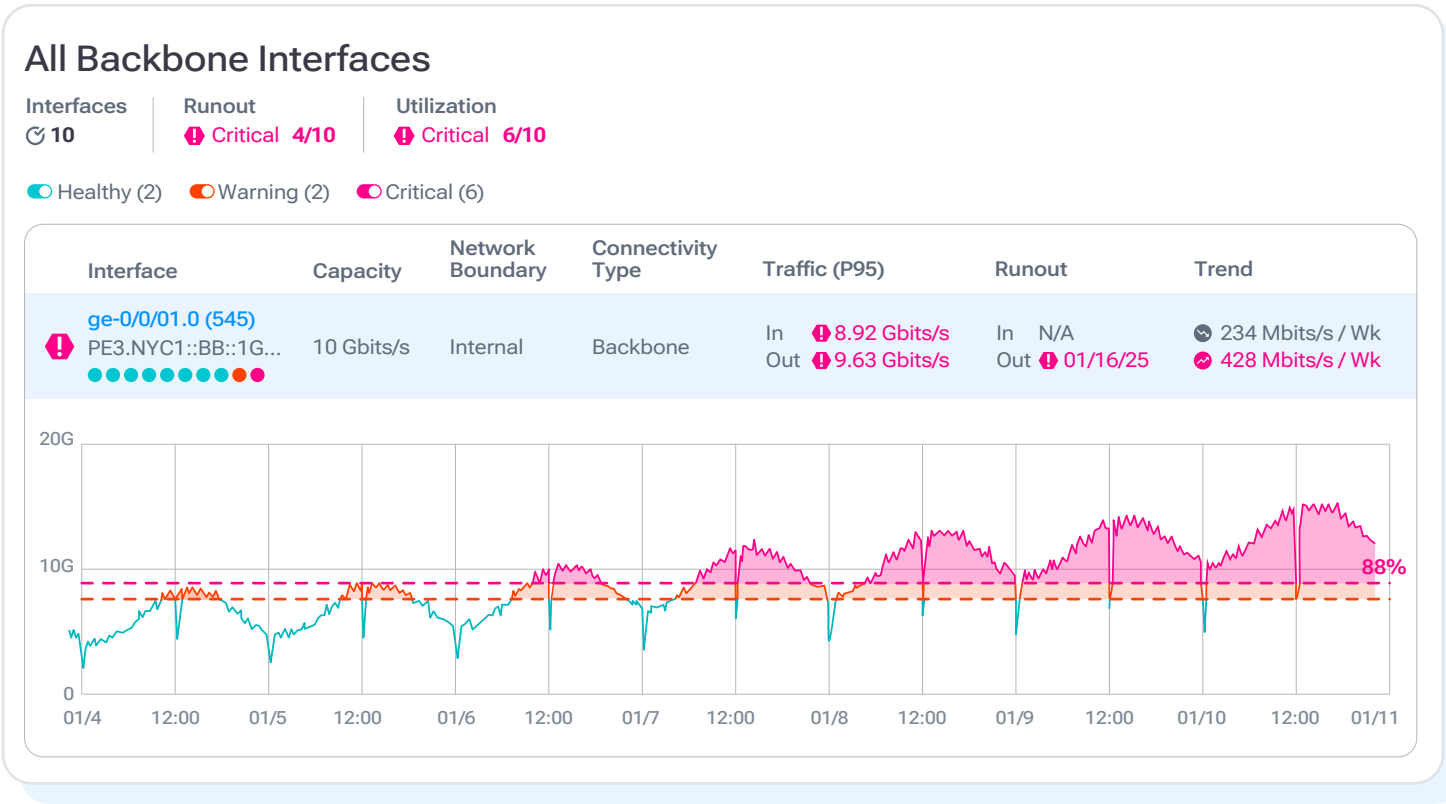
Device	Interface	Capacity
WAN-ROUTER	TenGigabitEthernet4	5.00 Gbps





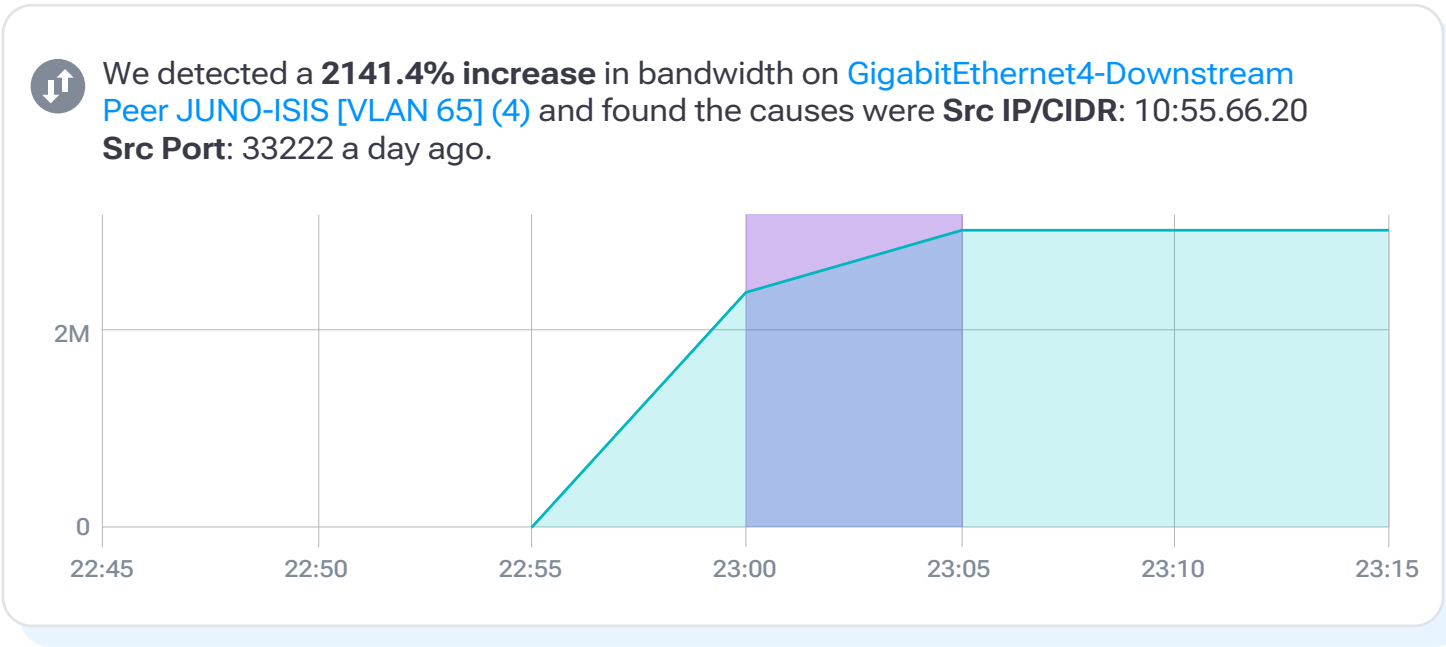
03 Intelligent traffic engineering

Network intelligence turns raw telemetry into an always-on, traffic-engineering brain. Machine-learning models monitor latency, jitter, loss, and link utilization in real time, predict congestion before it occurs, and suggest adjustments to mitigate issues. Kentik can also assist with capacity planning, which in terms of traffic engineering involves understanding which links to drain for maintenance when utilization is predictably low, and when to shift bulk data transfers to off-peak circuits, as well as how to optimize throughput from existing infrastructure without incurring the expense of over-provisioning. The business experiences faster page loads, more stable SaaS performance, fewer outages, and a lower transit bill, all of which contribute to higher customer satisfaction and a healthier bottom line.



04 Capacity Planning

Network intelligence analyzes real-time and historical telemetry, including flow records, interface counters, application response times, and cloud-billing data, to learn demand cycles, detect long-term growth trends, and simulate "what-if" scenarios, such as a new SaaS rollout or a marketing-driven traffic surge. By forecasting when and where links will become saturated or how much burst bandwidth a cloud interconnect requires, network intelligence enables engineers to schedule upgrades months in advance, right-size circuits, renegotiate carrier contracts, and shift traffic to off-peak paths when necessary. This data-backed precision prevents latency issues and SLA breaches, trims capex by avoiding overprovisioning, and provides more predictable opex budgets.

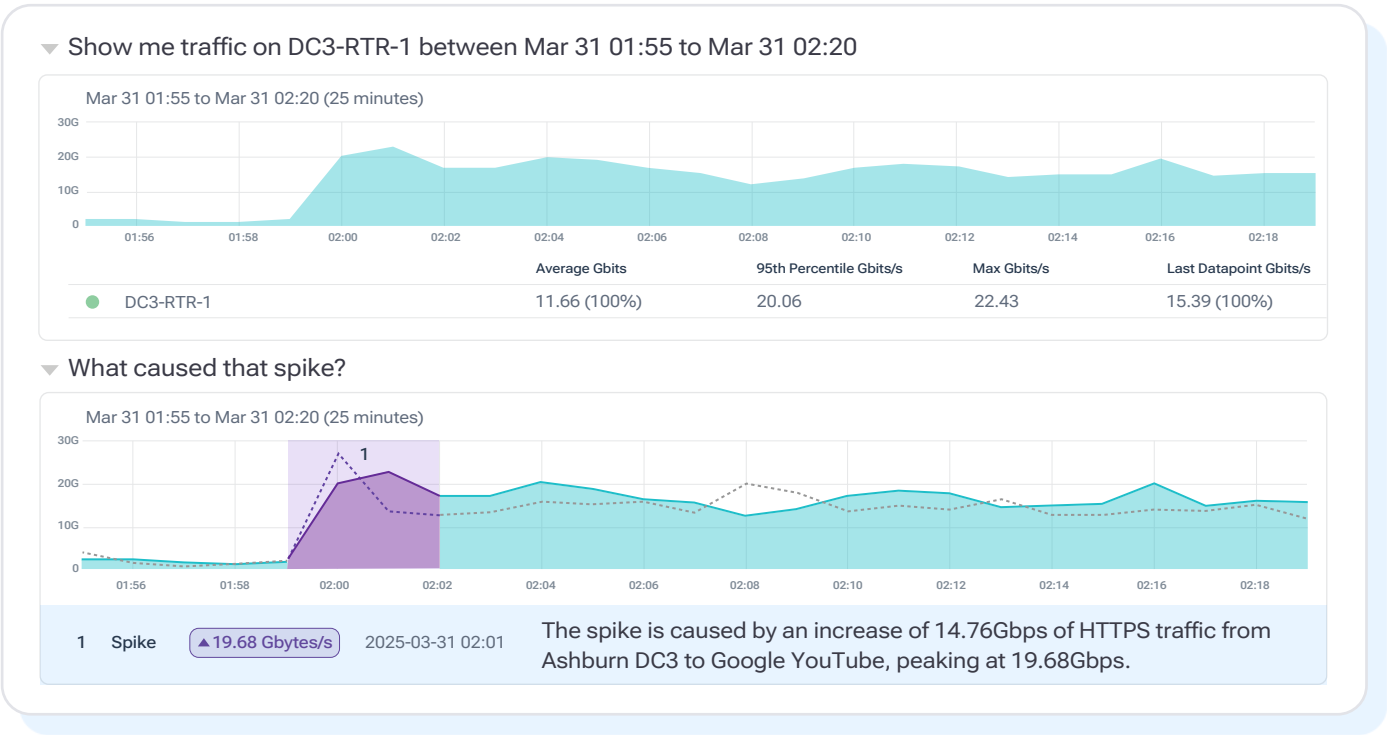


Network telemetry is ingested over time to determine typical behavior for the network. When a change occurs, the system is able to dynamically identify, as opposed to using static thresholds, if it falls outside of the normal range and therefore out of SLA.

05 SLA violation prediction

A network intelligence pipeline closely monitors real-time network telemetry. It feeds that data through ML models that learn how latency, loss, and jitter typically behave for each path, application, or customer. Those models output a probability of SLA breach minutes or even hours before the threshold is crossed, allowing operators to open tickets or trigger automation.

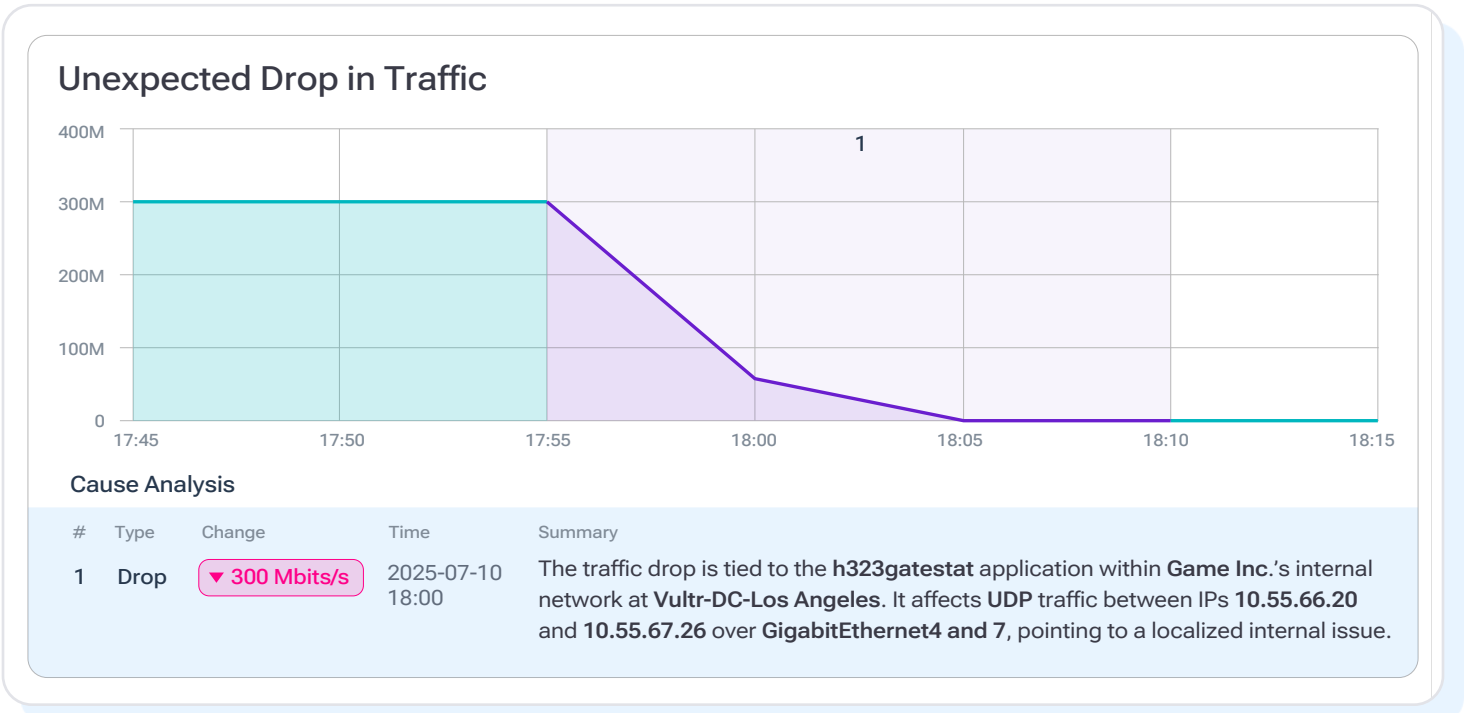
Running continuous synthetic tests enables an intelligence platform to correlate predicted spikes with real-world hop-by-hop measurements. This transforms abstract risk into concrete remediation steps. Service providers already use this proactive approach to manage contract penalties by identifying where performance is deviating, initiating reroutes, or adding capacity before customers experience a slowdown.



06 Troubleshoot connectivity and performance issues

Network intelligence enables the continuous synthesis of network telemetry data into a searchable context, helping engineers understand traffic flow and where it breaks down. With that foundation, Kentik Journeys turns troubleshooting into an interactive dialogue. Every natural-language question typed into Journeys is parsed by a large language model that automatically assembles the correct queries, path traces, and anomaly checks across Kentik's data engine. Instead of pivoting through dozens of dashboards, an engineer can simply ask, "Why can't users in New York reach our SaaS front-end?" and get an answer that correlates flow records, packet-loss spikes, and cloud gateway latency in seconds.

By retaining the entire conversational history, the AI can refine each follow-up and filter by ASN, zooming into a five-minute window or overlaying synthetic HTTP tests, all without losing context. The result is a guided root-cause analysis that not only isolates the failing path but also explains *why* it failed, complete with suggested remediations and links back to the raw telemetry for verification. By elevating complex SQL-like exploration to a chat-level interface, network intelligence enables any engineer, regardless of their tooling expertise, to quickly obtain answers and maintain smooth traffic flow.



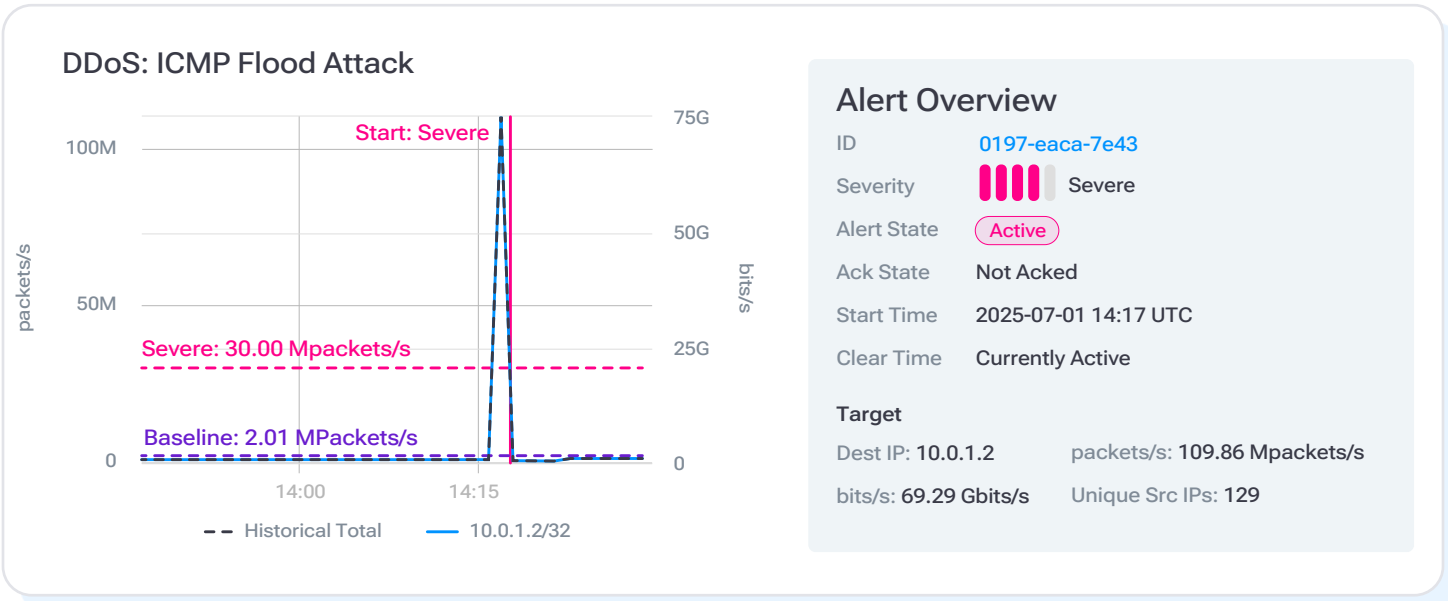
The image above shows an unexpected drop in network traffic, an event that typically wouldn't trigger an alert like a spike might. Kentik correlates and analyzes various types of telemetry, enriching the data with relevant metadata to provide context. This allows engineers to quickly understand the contributing factors – in this case, UDP traffic between two IPs tied to a specific application.

07

Intelligence incident triage

Network intelligence treats every flow record, routing table entry, device metric, and cloud flow log as part of a single time-aligned dataset. When an incident occurs, network intelligence can automatically cluster events that share key dimensions, such as common AS paths, identical loss signatures, and application tags, and present them as a single narrative thread instead of a hundred noisy alerts.

This is more than simple de-duplication. A network intelligence platform runs anomaly detection policies and alert templates in the background, tags each hit with application context, and then feeds that enriched stream back to the conversational AI. The engineer can keep drilling down into the problem while the model refines the query on the fly, revealing a previously invisible problem as the root cause. The result is faster triage, fewer all-hands Zoom calls, and a clear, evidence-backed path from symptom to underlying fault.

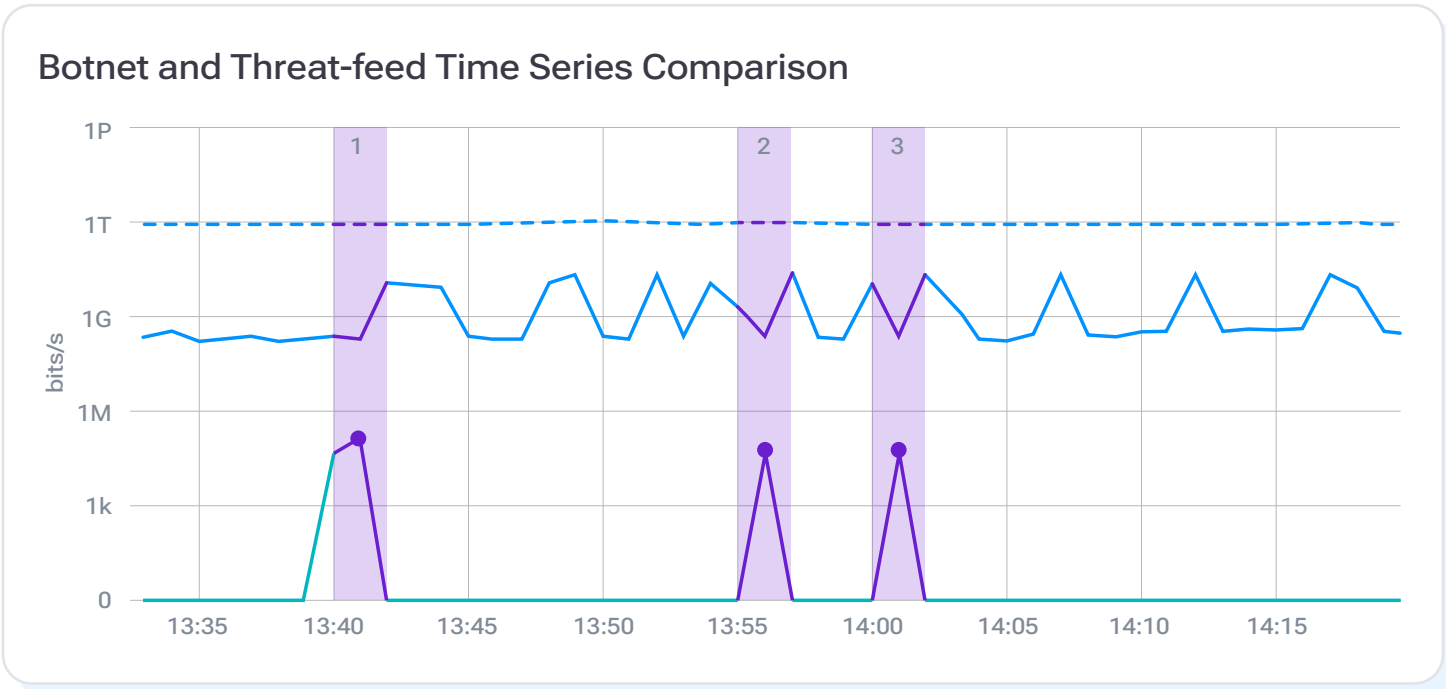


Here we see how the system has predetermined what "normal traffic" should look like, so that when a spike occurs, an automation kicks off to identify if the anomalous traffic matches any known malicious patterns. If it does, a programmatic mitigation will engage to remediate the attack and resolve the issue.

08 DDoS detection

A network intelligence engine ingests flow, metrics, and threat-feed enrichments at line rate, then applies workflows that learn normal traffic volumes, protocols, and source-destination pairs for every interface, location, application, and customer. When inbound packets suddenly surge past those baselines, whether due to a volumetric flood, SYN storm, or slow-rate application attack, the engine flags the deviation, enriches it with path and geo context, and pushes a "possible DDoS" event to an alerting system.

From there, the platform can auto-trigger mitigation via RTBH, third-party services such as Cloudflare or Radware, thereby decreasing the time-to-defense without generating false positives. The result is a closed-loop workflow where AI detects, explains, and helps neutralize DDoS attacks more quickly than manual dashboards can.



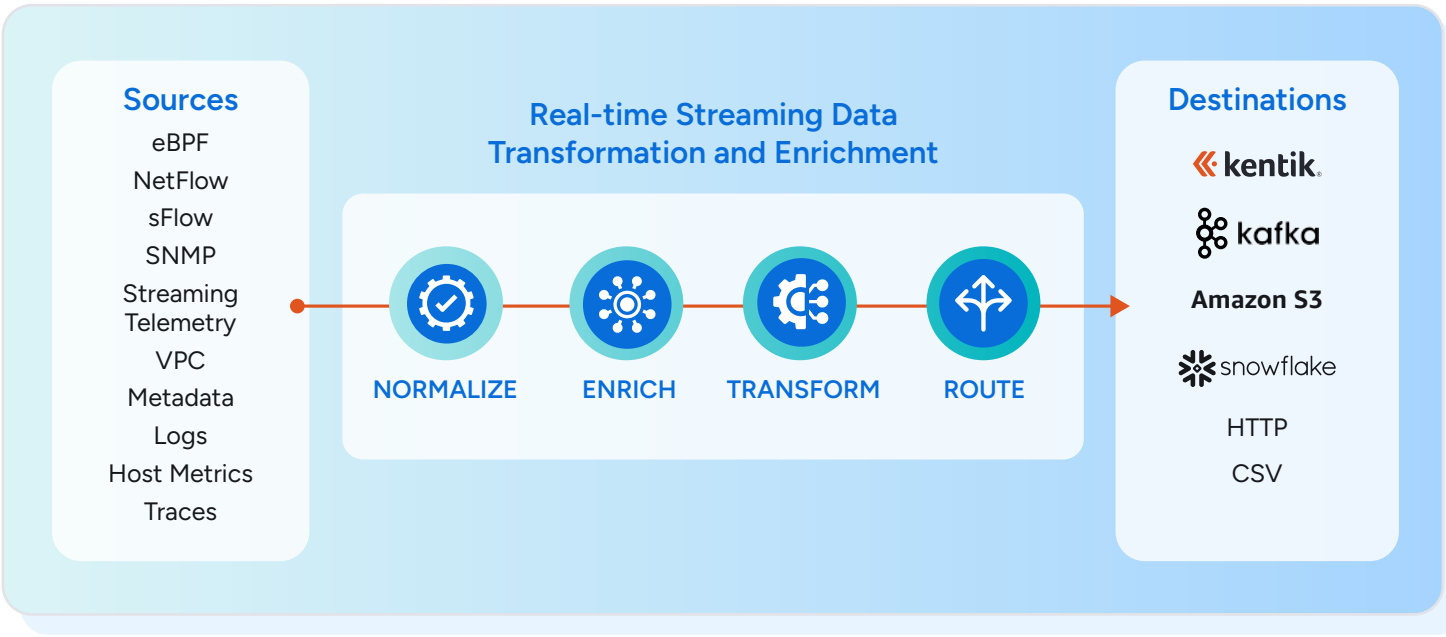
Here we see multiple data points represented in a time series where they are compared to a dynamically-learned baseline as well as known malicious traffic definitions such as from threat feeds.

09

Identify potential security threats

Network intelligence baselines regular network traffic so that when an infected device starts sending high-volume uploads to an unfamiliar IP range, or when an authenticated service dribbles small amounts of data out at odd hours, Kentik flags the pattern and sends an alert. Because historical telemetry data is retained, security analysts can pivot instantly to weeks of historical context and verify whether the spike is a harmless backup or actual malicious activity.

Network intelligence enables an engineer to ask in plain language to view all flows that match an exfiltration policy within the last fifteen minutes, and the platform automatically generates and runs the queries that slice across the platform's data engine.



10 Reliable data for closed-loop automation and orchestration

Network intelligence turns the sprawl of flow logs, BGP tables, SNMP, cloud, and device metrics into a single, time-aligned source of truth. Its ingestion layer accepts raw feeds at line rate, then runs a built-in ETL pipeline for stream processing, enrichment, outlier filtering, and machine learning-ready feature extraction, all before writing the cleansed data into the Kentik Data Engine for sub-second query and model access.

Because Kentik owns the entire pipeline, NetOps teams don't have to architect, build, and maintain an entire data pipeline; instead, they get ready-to-use, normalized telemetry through one API or SQL-like interface.

That reliability is what closed-loop automation and orchestration stacks need to act with confidence. Orchestration platforms can then subscribe to Kentik's enriched event stream, correlate it with intent policies, and launch remediation workflows, such as rerouting around a flapping transit, throttling a tenant, or spinning up extra cloud capacity, without first rebuilding a data lake. Kentik's consistent schema and AI-ready features ensure that network intelligence provides the same authoritative view of the network that engineers see when they manually crawl the network, one device at a time.

Bringing it all together

You've just taken a journey through ten powerful ways network intelligence is truly changing the game for network operations. We've seen how it stitches together your entire network's story, giving you a level of clarity you might never have thought possible. From predicting those frustrating outages before they hit, to smartly managing your capacity, bolstering security, and even making troubleshooting feel intuitive – it's all about making your life, and your network's life, easier and far more effective.

The days of frantically digging through data and constantly putting out fires are fading fast. Network intelligence isn't just another tool; it's about giving your network experts genuine superpowers, letting machines handle the repetitive grind so your brilliant team can focus on strategy and innovation. Imagine the peace of mind that comes from knowing your network is running smoothly, costs are truly optimized, and everything's secure, all while your business moves faster than ever.

Ready to transform your network into a truly smart, resilient, and powerful asset that propels your business forward? Discover how Kentik brings these vital network intelligence use cases to life – visit Kentik.com.

Kentik is the network intelligence platform for modern infrastructure teams. Unlike traditional monitoring and observability tools, we demystify complex network operations, enabling organizations to deliver applications and innovation at scale. Built by network experts to make critical insight accessible to every engineer, Kentik is the real-time source of truth that understands every network in context, from data center to cloud to the internet. This single platform unifies and correlates cloud, device, flow, and synthetic data to turn telemetry into action. Market leaders like Akamai, Booking.com, Dropbox, and Zoom rely on Kentik to run, manage, and optimize their networks.

kentik®

The world's best infrastructure teams trust Kentik.

zoom box Canva servicenow Dropbox

Revised 20250716