What is Digital Experience Monitoring?

A GUIDE FOR ISPS, TELCOS AND SERVICE PROVIDERS

kentik®

kentik

Table of Contents

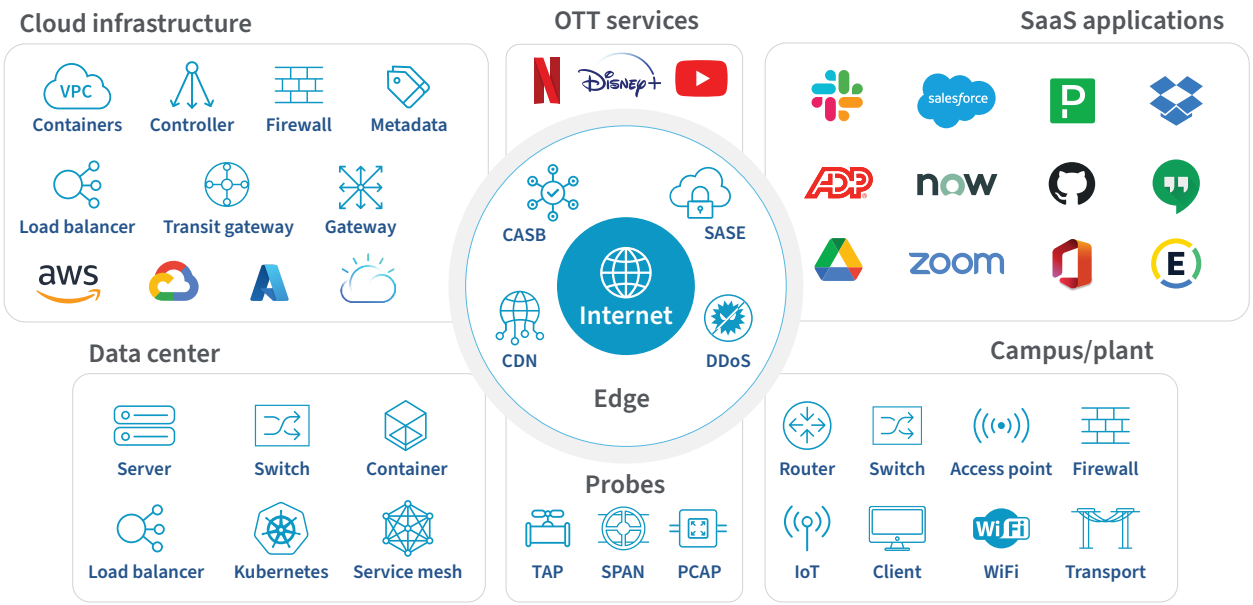
Preface

Digital experience monitoring (DEM) helps businesses identify digital pain points and optimize the digital experience they deliver across channels, including mobile applications, websites, social media sites, WAN, LAN, cloud and other digital assets.

Evolving from application performance management (APM) and end-user experience monitoring (EUEM), DEM technologies can detect and solve a variety of application and network infrastructure problems and improve visibility into network and application performance.

Depending on the role you have and the type of organization you work with, your area of interest in DEM likely varies. For example, a website designer is likely to place more emphasis on user-experience measurements and tools, whereas a media publisher is going to focus on delivery metrics such as jitter and buffering.

No matter what business you're in, as long as you're digitally reliant, DEM technologies are going to increase in importance as you seek to improve the reliability and responsiveness of your digital experiences — whether it's experiences for your employees, customers, suppliers and/or partners.



The increasing complexity of digital experience monitoring

This guide focuses on DEM for service providers, an area where Kentik has a lot of expertise. Many of the concepts applicable to service providers are also likely to be of interest to SaaS, PaaS, enterprise IT, and media/OTT network and IT professionals. Service providers sit in the middle between end users/eyeballs and publishers.

Why should service providers care about DEM when it's not their applications or content that's being consumed? It's because service providers have learned the hard way that they need to be able to identify and isolate the root causes of any issues their customers' experience — preferably before their customers do.

There are many headline-grabbing outages (see the Kentik blog on "The 10 top network outages of 2021"). But for service providers, the constant headaches and awkwardness often stem from devices being overloaded in their network and having customers call to complain about the impact on their traffic. Being able to observe the condition of the networks entering and leaving your network is critical for maintaining customer trust — a vital factor in business success.

Definitions

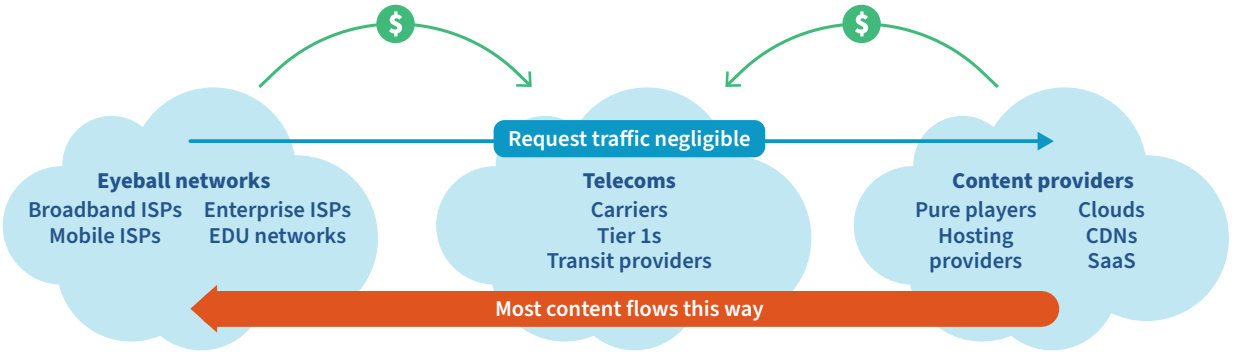
Service providers

Generally, we refer to service providers as the companies responsible for providing and maintaining the internet's infrastructure:

- **Eyeball networks/ISPs** - broadband, mobile, enterprise and education
- **Telecom** - carriers, Tier 1, transit providers
- **Content providers** - content delivery networks (CDN), hosting providers, storage service providers and cloud service providers

These services aren't mutually exclusive as many service providers offer a broad range of services. For example, Amazon/AWS offers CDN, storage and cloud services. Lumen offers CDN, transit and DIA (Dedicated Internet Access).

The traffic flows predominantly from the content providers, over telecom, to the eyeball networks and the money for this traffic flows to telecom providers.



Digital experience monitoring (DEM)

Digital experience monitoring is a category of performance analysis technologies that provide visibility into the availability, performance and quality of the experience an end user receives as they interact with an application. Users can be customers or users of a service and/or employees.

DEM observes how the users and supporting infrastructure behave as they interact with on-premises and cloud applications to do their job. Gartner describes DEM as "a performance analysis category of technologies that provide visibility into the end-user experience as they interact with applications and all related resources." In this book, we'll focus on the DEM needs of service providers.

Why is DEM important?

Now more than ever, businesses are required to deliver exceptional user experiences to their internal and external audiences. With the shift to cloud and mobile, as well as remote work, this requirement is more challenging. DEM tools give IT and network operations personnel visibility into the experience that end users are having as they interact with on-premises and cloud applications. They enable operations staff to ensure user and customer issues are resolved and the network is performant.

DEM links performance data to the experience that devices provide to either human or machine users.

DEM builds on and complements other performance monitoring tools and technologies, such as APM and network performance monitoring (NPM). Like these solutions, DEM uses data to identify and remediate performance issues. However, whereas APM and NPM are designed to provide baseline overviews of performance for certain types of resources (namely, applications and network infrastructure), DEM links performance data to the experience that devices provide to either human or machine users.

DEM is a means of contextualizing and applying the insights delivered by APM and NPM tools.

Thus, DEM doesn't replace APM and NPM as much as it is a means of contextualizing and applying the insights delivered by APM and NPM tools. DEM helps close the gap between data and experience, providing an end-to-end picture of how users across your environment are experiencing your service.

To put this another way, NPM tools are engineered to ingest data from nearly everything from any device and give accurate general information about all devices on the network. In contrast, DEM shares very detailed performance information from endpoint systems, taking measurements only on selected applications and devices.

Measurements

DEM is powered by measurements that provide snapshots of the status of your environment. And we're not just talking about generic measurements here, like whether a resource is up or down.

Instead, you need to be able to answer questions like whether a service is performing well enough for customers to do what they need to do. Knowing that requires monitoring your applications, clouds and network resources on a continuous basis.

When evaluating your performance, three primary metrics matter:

- **Latency**: Usually measured in milliseconds, latency is the time required for a network packet to traverse from the source to the destination. When a service experiences high latency, it feels like it's delayed or sluggish.
- **Packet loss**: Expressed as a percent of total data packets sent, packet loss happens when a packet doesn't arrive, arrives out of order, or arrives too late to its destination. Packet loss causes a choppy, "in-and-out" digital experience.
- **Jitter**: A derivation of latency, measured in milliseconds, jitter is the variance in latencies across a set of network packets. Jitter results in an uneven, or jumbled, digital experience.

The most significant contributors to latency, loss and jitter include cabling and connectors, distance, routers and switches, congestion, non-optimized applications and endpoints. Even if you're running your service in the public cloud, you're not out of the woods on performance. Your configurations, routing choices, and ingress and egress policies can all affect how snappy your service is. Even factors like the cloud service's faulty software or equipment can play a role, and you need to stay a step ahead by measuring all the different stages that contribute to the overall application experience.

The components of DEM

It's well understood that an optimized network is critically important to service providers. The push to maintain a finely-tuned infrastructure is fed by a constant urge to stay competitive and grow the business. The challenge to optimize the network has been complicated by the migration to the cloud and the adoption of container architectures. This has introduced blind spots into the traditional hop-by-hop visibility that network professionals rely on.

For service providers, DEM should focus on answering two key questions:

What is the state of the traffic to and from my network?

What might happen if...?

The first question is answered primarily by **traffic monitoring (NPM)** and the second by **synthetic testing**. In addition, endpoint monitoring and real-user monitoring (RUM) may be helpful for providing additional context, although they are not primary data sources for service providers performing DEM.

NPM explained

Whether it's a router, switch or network device, it will be capable of being monitored the first time it transmits a packet onto the network. It doesn't matter if the environment is a LAN/WAN, software-defined networking (SDN), or network function virtualization (NFV) component.

NPM answers the *what is* question.

One of the goals of NPM is to monitor, measure, diagnose and generate alerts for any IP address in the environment. In other words, it answers the *what is* question. This includes internet of things (IoT), cloud-hosted services (e.g., containers), wireless endpoints, and servers/VMs. To gain insight into these devices, they must send messages on their health to a collection point.

NPM tools are designed to ingest numerous data formats and transmission methods. Devices connected to the network send data in multiple formats. Most of these transmissions are standards-based or in a syntax common enough to be considered a standard such as NetFlow, IPFIX, sFlow, SNMP, syslog, event logs and packet capture. More recently, the JSON format is used when sending network performance and security telemetry.

DNS data exfiltration is another transmission technique that can be used for both the malicious and legitimate transmission of information. There are many others, and more methods are sure to become available. Data sources ingested by NPM solutions may include many different types of events, device metrics, streaming telemetry and contextual information.

NPM and service providers

Today, service providers face significant challenges from every direction. Network teams are being pressed to operate more efficiently while the infrastructure complexity continues to accelerate. The volume of alerts and potential network problems continue to grow, false alarms mask real problems, and network teams struggle to keep pace — especially with today's complex networks that span both traditional and cloud infrastructure.

Service providers face challenges from every direction. Network teams are pressed to operate more efficiently while the infrastructure complexity continues to accelerate.

Traffic monitoring for service providers is critical and is primarily used to:

- Strategize and support interconnection efforts
- Ensure their customers are getting expected performance
- Evaluate embedded cache requests
- Ensure capacity is well planned
- Route around congestion
- Understand and mitigate internet events
- Understand how applications are driving traffic

The following types of network data are important for monitoring performance:

- **Network flow data**: This data captures information about the IP traffic going to and from network interfaces that your traffic traverses in your on-premises network.
- **SNMP data**: Simple Network Management Protocol (SNMP) is a protocol for exchanging management information between network devices. It measures the time it takes for data to be received from a router as an example.

Synthetic monitoring explained

Synthetic transaction monitoring (STM) proactively tests services such as SaaS applications like Salesforce, API endpoints and the network that connects us to them. Unlike real-user monitoring, STM isn't generally run against active users. Its mission is usually intended to test hosted applications and network conditions. Synthetic testing helps you answer *what if?*

> **Synthetic testing helps you answer *what if?***

Synthetic monitoring techniques typically involve simulating user behavior and network conditions by running tests that emulate traffic patterns across various layers of the network stack. These may range from simple IP pings and traceroutes that measure packet loss, latency and jitter to higher layer HTTP GETs/PUTs. They can also include complex transaction scripts that execute a series of browser page loads, simulating user actions like logging into a website, browsing a catalog, making a purchase, etc.

Synthetic monitoring techniques typically involve running a mix of HTTP commands (POST, GET, PUT or DELETE) on a regular and periodic basis. Testing can also be done on connection times and database query speeds. Depending on the synthetic monitoring solution in use, the frequency of such testing can vary from daily, hourly or even down to one-second intervals.

For network STM, metrics on response times, packet loss, jitter and transaction times are gathered and sent off to the DEM-collection platform where correlations are performed. The performance of the network can be measured for paths towards applications, servers and infrastructure such as DNS or public or private clouds. AIOps techniques (e.g., predictive analysis, pattern matching and causal analysis) can be applied to get deeper insights as to why there is an application performance problem.

Synthetic monitoring use cases

- Finding and fixing application or network issues before they impact users
- Benchmarking and baselining the performance of applications, application support infrastructure (such as DNS servers), APIs, websites and networks across a variety of variables, such as performance across different time frames and geographies, or performance against peers or industry standards
- Preparing for significant network transitions, such as adding a new geographic market to a service offering or moving an existing data center to the cloud

- Ensuring the performance of one's own service offerings is adhering to customer SLAs, and providing regular reporting on performance versus such SLAs
- API monitoring
- General monitoring and testing of network and internet user traffic

End-user monitoring explained

End-user monitoring, also known as end-user experience monitoring, is a practice of monitoring a user's behavior or actions while using an application. There are two common approaches to end-user monitoring: **endpoint monitoring** and **real-user monitoring**.

> **End-user monitoring is a practice of monitoring a user's behavior or actions while using an application.**

Endpoint monitoring

Endpoint monitoring provides visibility into the user devices and performance testing from the endpoint via an agent. This includes things like the version of the operating system, CPU and memory usage, storage space and network metrics. While it can seem similar to desktop inventory software, the focus is on continued performance and availability. Consumers can use an endpoint monitoring service, such as Speedtest.net, to test their broadband connection speed.

Endpoint monitoring use cases:

- Monitoring the performance of applications running on thick clients, such as operating systems and storage space
- Monitoring the performance of end-user hardware and the performance of the configuration of that hardware/device, including mobile devices
- Employee user-experience monitoring
- Running network performance tests from end-user agents
- Monitoring of endpoint issues impacting the performance of employees
- Adoption and usage of new/old applications by employees

Real-user monitoring

Real-user monitoring (RUM) is used to monitor and measure the end-user experience when using the applications the business depends on. These applications include services like customer relationship management (e.g., Salesforce), collaboration tools (e.g., Slack, Microsoft Teams) and social media platforms (e.g., Twitter, Facebook).

RUM uses application monitoring to look at actual performance that users are experiencing (e.g., application response times, latency, location, browser). Usually this is available on a per-transaction basis and includes telemetry on bottlenecks that may be due to browser CPU or RAM overload.

Real-user monitoring use cases:

- User journeys and customer experience analysis
- Root-cause analysis of front-end application problems
- Monitor quality of experience for external applications, such as different browsers and native mobile app

Again, RUM isn't of primary importance when it comes to service providers with respect to the services they offer their customers.

DEM and service provider dynamics

Service providers — MSOs, telcos, mobile carriers, CDNs, cloud providers and ISPs — feel increasingly squeezed today. On one side, providers face continuous costly infrastructure investment, driven by relentless content traffic growth. On the other side are revenue threats from third-party over-the-top (OTT) services that compete with in-house offerings and profit from the very same traffic that's driving up costs. Understanding and managing these dynamics are huge challenges that providers must meet to ensure the next phase of their success.

Whether you provide hosting, CDN, transit, mobile, B2B or FTTB (fiber to the building), your customer experience will depend not only on the performance of your network, but also on upstream providers. If you don't have visibility into upstream networks then you will be caught off-guard when your customers are experiencing latency or other performance degradations.

What are the critical DEM questions service providers need to answer?

Traffic (or NPM) monitoring tells you what is the state of your network:

- How is traffic flowing to/from/within my data center?
- How is traffic flowing to/from/between my cloud instances?
- What apps are consuming the most amount of bandwidth?
- How much are we spending on egress?
- Are we nearing network capacity?

Synthetic monitoring tells you what might happen if:

- You had users accessing your application from somewhere new
- You added a DNS server instance and you want to make sure the right users get to it
- A payment API server is slowing down: Does that mean your users can't checkout anymore?
- Your cloud provider has a network outage in US-East: Can your users in New York still access your application?
- Is an outage in a provider's network impacting your customers from getting to your data center?

Attributes of a DEM solution

Implementing DEM effectively can cut the time it takes you to configure, research, analyze, plan and investigate in the context of your network. To help your productivity, evaluate solutions with these variables in mind:

Single view: Done right, DEM involves bringing all your data and context together in a single view. This process allows you to identify issues and find the answers you need, and it reduces the chance you'll miss something big.

Searchability: If you're on the hook for keeping your network healthy, secure and highly performant, you probably spend a fair bit of time troubleshooting to keep it that way. You need to be able to ask any question, any which way, and get an immediate answer.

Done right, DEM involves bringing all your data and context together in a single view.

Rich context: When your DEM program involves enriching your data, you have the context you need to have the full picture. For example, enrichment gives you the name and geographic location of a router instead of the IP address alone. Only then can you answer questions with confidence, sequence your research, report metrics accurately per audience and prioritize your activities.

Automated workflows: You should have your network DEM platform instrumented to initiate workflows in the platform or third-party systems, such as systematically sharing network telemetry with other observability tools, automatically adding or adjusting network capacity and activating threat mitigations.

What to look for when evaluating DEM tools

There are many different sorts of DEM tools on the market, so it's vital to think about the following while developing a strategy and evaluating experience monitoring tools.

Ability to integrate into existing tools and systems: DEM tools need to integrate seamlessly within an organization's infrastructure so there isn't any additional work required from IT teams for them to deploy or set up new software solutions. Can your app monitoring data integrate with your DEM solution?

Scalability: Your DEM solution must cost-effectively scale. Very significant data volumes are captured by these tools. On-premises options can be costly to scale. Where DEM is required to monitor many assets, you must consider scalability up front as it may affect the overall cost and ROI of your DEM solution.

Performance and availability: These include real-time performance indicators, such as interface response times and capacity flags. DEM tools should be able to provide real-time event tracking for anomalies such as outages.

Data types needed: Network data doesn't reveal all the information you will need. Service names, provider names and traffic types (video, audio, application, etc.) may be needed to identify maps of providers and services to label traffic with context.

Testing parameters: How often do you need to run tests and how will you configure them? Does the DEM solution provider have tests configured in the markets that interest you now and ones that are likely to be of interest in the future?

***What if* and *what is* integration**: You'll want your actual traffic flows to guide your testing and the results of your testing to be easily translatable to your actual traffic flows. Integrated traffic monitoring with synthetic testing makes answering *what is* and *what if* a whole lot easier.

> **"Deep packet inspection comes at a huge cost, so most organizations do not do it. So, the granular information and analysis from Kentik provide insights they have never had before, such as details about which sources, destinations, and applications generate the most traffic. We just include that as part of our service, which customers see as hugely valuable."**
>
> ***—Grant Kirkwood, co-founder and CTO of Unitas Global***

Conclusion

Being able to monitor the digital experiences you and your customers are delivering is critical for any service provider looking to compete effectively. Helping your customer troubleshoot and identify possible issues that could impact end-user experience is critical in building and maintaining customer trust and building advocacy.

In this new environment, you often don't control much of what your customers depend on, but that won't stop them turning to you for answers. Uptime metrics and outage notifications are not enough. You need to understand where the bottlenecks are, where they're likely to be, and the root cause of any performance issues across devices, applications and networks.

The added complexity that cloud migration and remote work have brought to monitoring the digital experiences necessitates DEM solutions that provide total observability to actual and planned traffic. Network teams practicing observability in architecture and action will drive better performance, reliability, security, remediation and growth.

DEM from Kentik

Kentik is on a mission to bring down the boundaries between customers, teams, tools and methodologies. We want to make it trivial to answer virtually any question as it pertains to the network. We bring clear observability to DEM.

Observability is crucial to service providers. The Kentik DEM solution delivers unprecedented visibility into the digital experience that service providers deliver for their customers. Having a view that enables the answering of any question immediately is key to being a trusted supplier. If service providers can notify customers proactively about potential performance issues with their infrastructure or possibly about an outage elsewhere, they'll go a long way to building customer trust and confidence.

The Kentik Network Observability Cloud offers a modern, SaaS-based approach to deliver network performance monitoring and diagnostics. The platform combines flow-based network monitoring, cloud network observability and synthetic monitoring features to enable proactive monitoring of all types of networks.

By tracking performance data (such as response time and capacity utilization) and quickly getting to root cause of downtime and performance issues across internet, cloud and web applications, IT teams can implement more effective planning and optimization, resulting in improved customer experiences and greater network efficiencies.

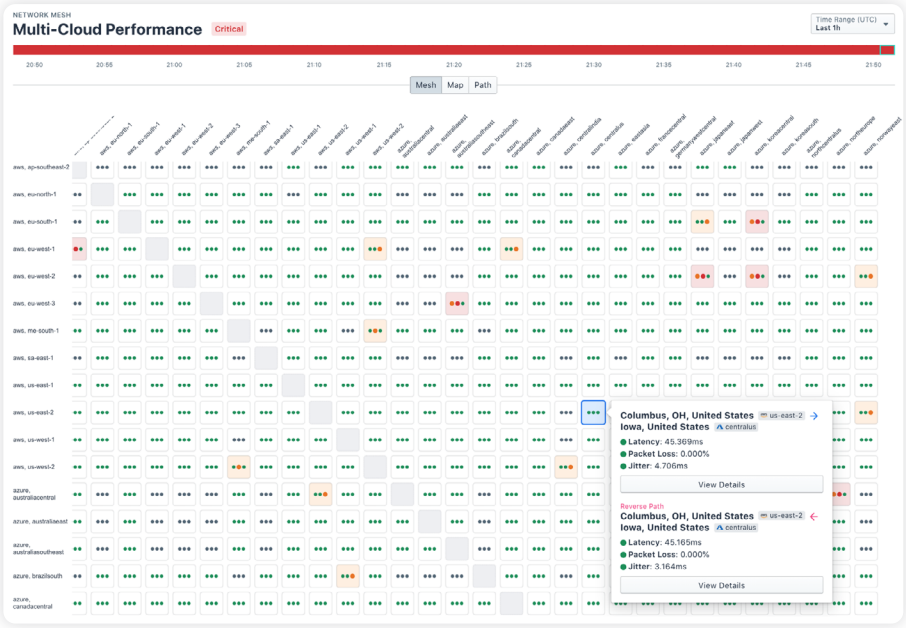
> **"With a distributed infrastructure on every continent, it is absolutely critical for us to have end-to-end, global network monitoring. We not only need to know what is happening across our own network, but we also need to be aware of incidents that occur outside of our network, for example, with our upstream operators."**
>
> ***— Oleg Yudin, head of network and cyber security at G-Core Labs***

Our solution integrates traffic monitoring and synthetic testing which enables us to quickly recommend synthetic-testing scenarios based on your actual traffic. This connection transcends past outdated approaches like DPI, monitoring appliances and data lakes to deliver a deep, detailed picture of traffic associated with CDNs, OTT services and subscribers.

The following pages give a glimpse into how the Kentik Network Observability Cloud can help you answer any question about your network.

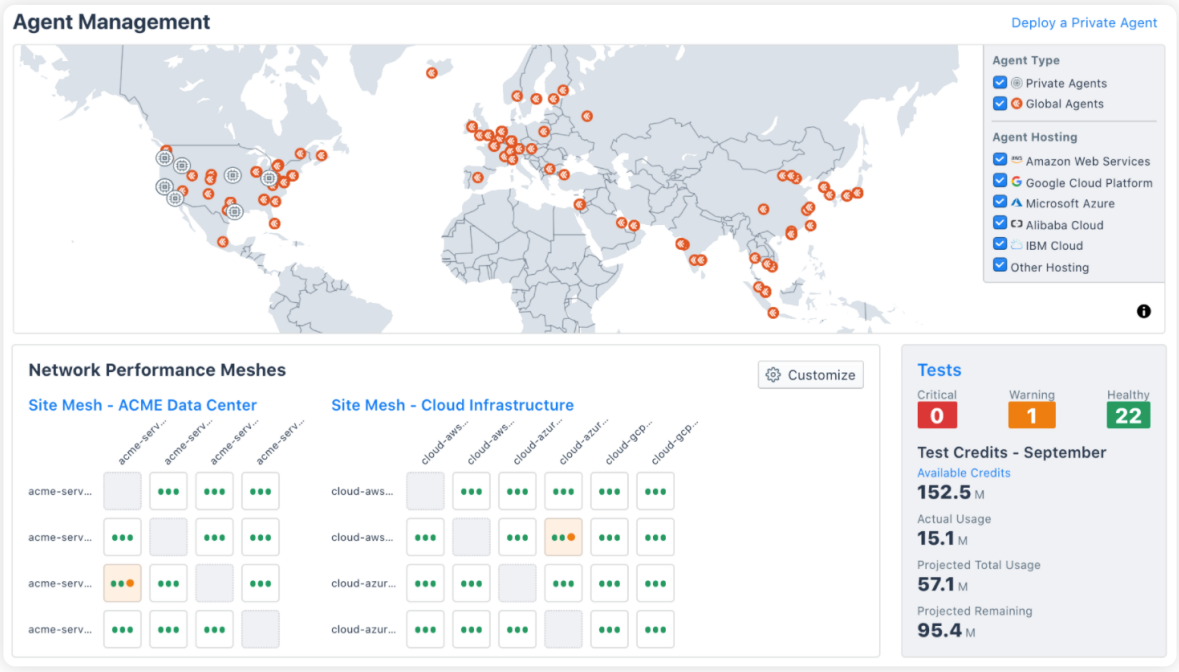
See the big picture

Set up complex, multi-site performance mesh tests with just a few clicks. Our matrix view and visual cues show you problems at a glance. See how you are running applications between data centers and public clouds.



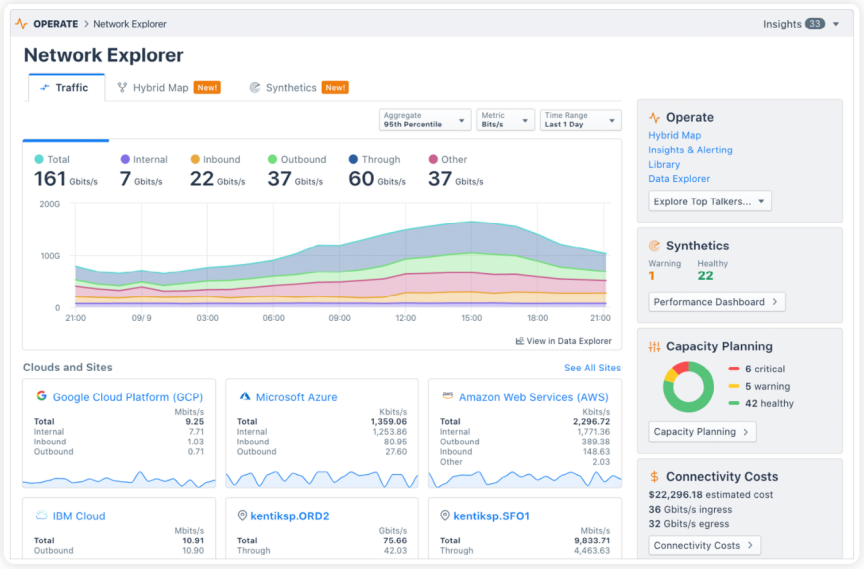
Manage network performance

Manage subscriber experience and ensure availability and performance across your network, edge and backbone. Auto-configure performance tests based on actual traffic and test continuously so you don't miss a thing. Investigate only what matters.



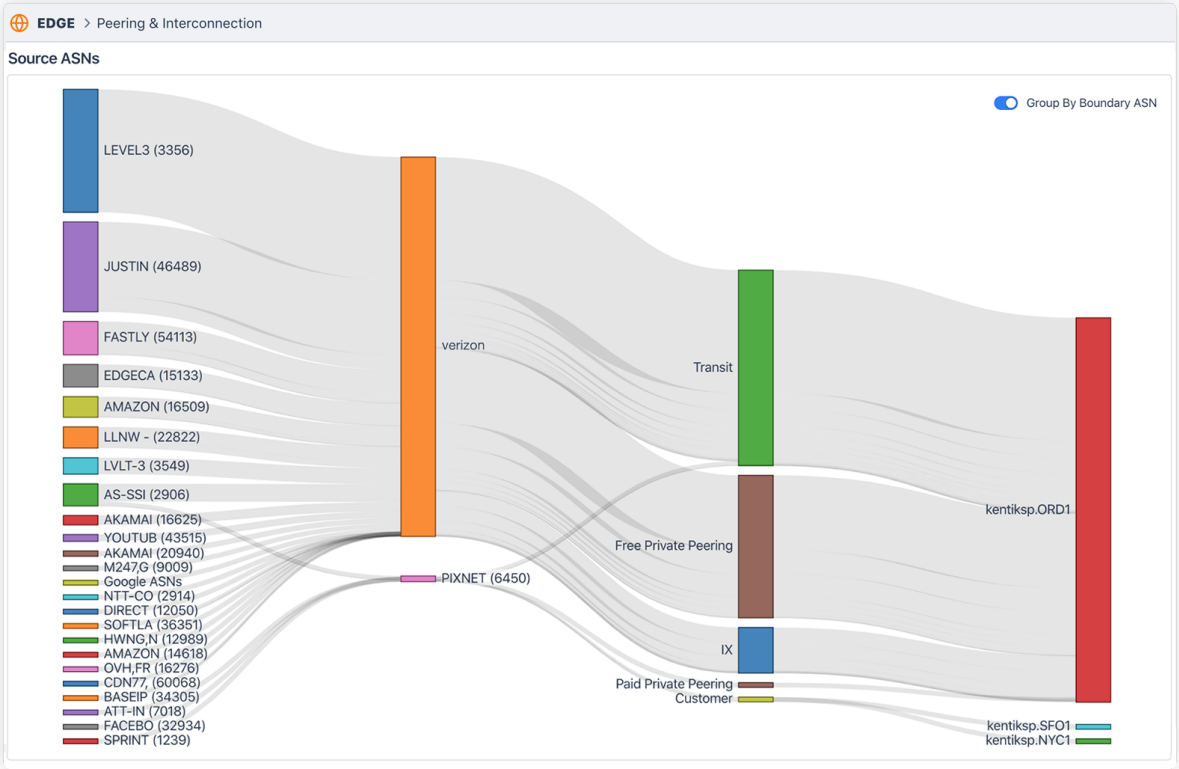
Troubleshoot issues

When the world relies on your network, every glitch matters and seconds count. Start with unprompted, AI-driven insights or simply by asking questions. Drill into network issues interactively to understand their root cause. When you're in the heat of the moment, like during an outage, finding answers quickly is everything.



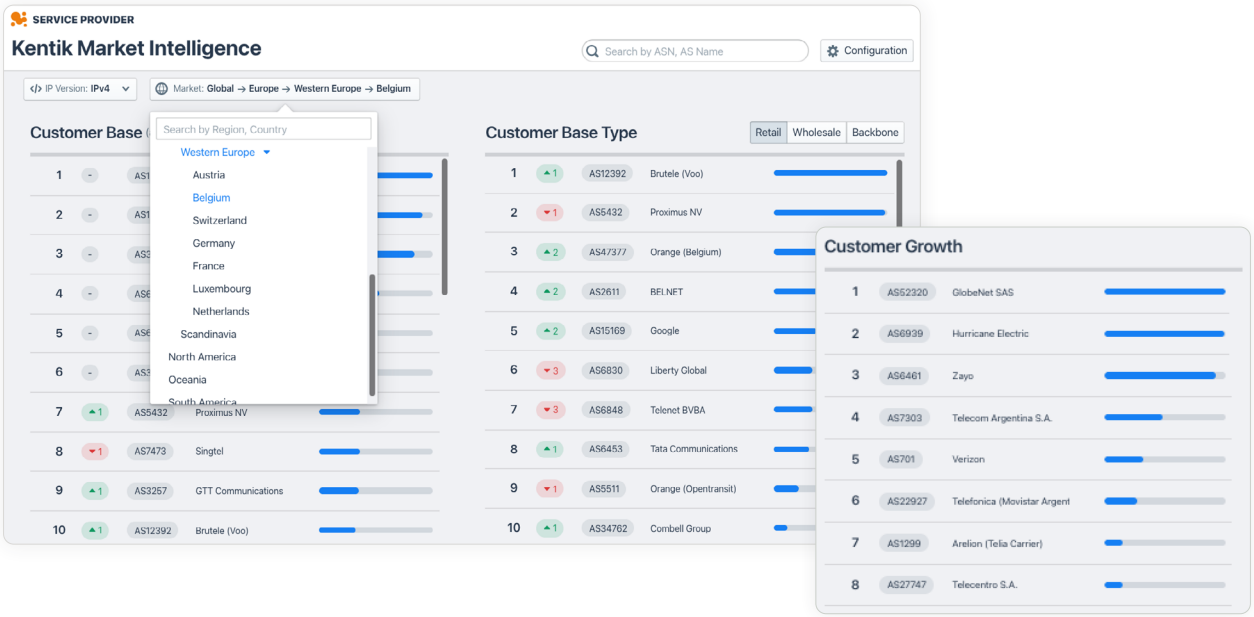
Improve peering and interconnection

Optimize performance and cost by managing interconnections. Discover the most appropriate origin or destination networks to interconnect with based on your traffic flows, connectivity mix, paths and dynamics. Get information about peers on any internet exchange or colocation.



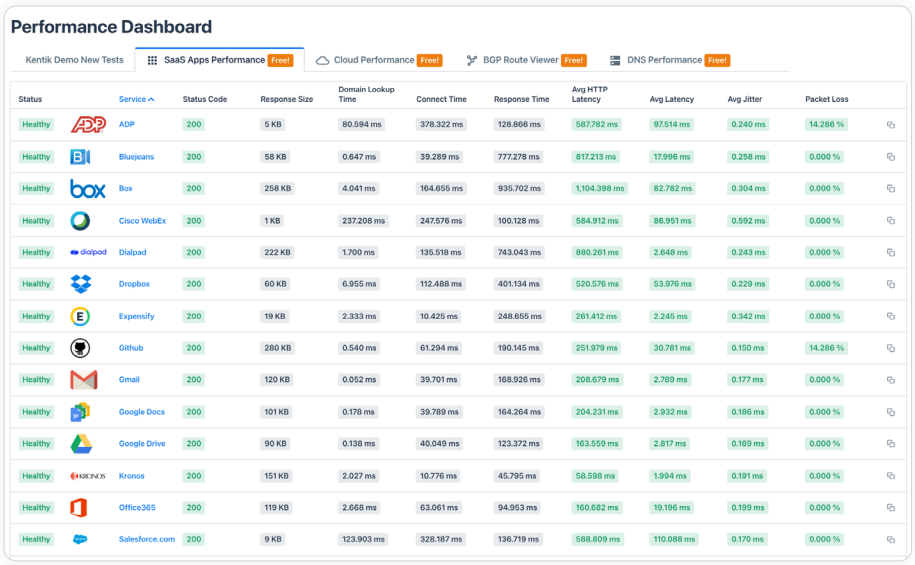
Gain competitive market insights

Kentik Market Intelligence (KMI) enables you to observe and evaluate the size, market share and the relationship of Autonomous Systems (ASes) globally and regionally. See how ASes rank in your markets of interest, who is adding customers, and which potential customers are reliant on a single upstream provider.



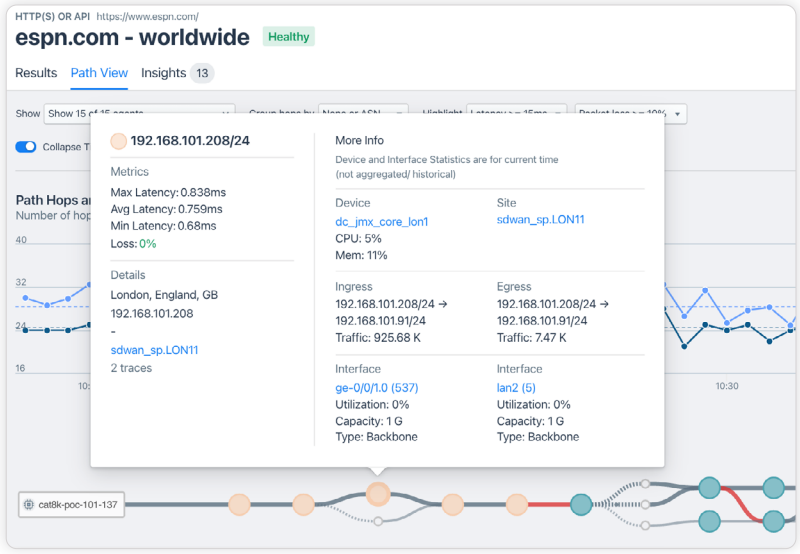
Evaluate applications directly

Set up HTTP server, page load and API tests for applications and services. Monitor critical application infrastructure, such as web or DNS servers. Monitor SaaS performance anywhere with our fleet of globally distributed agents. Keep tabs on the elements that make up the user experience.



Examine delivery paths

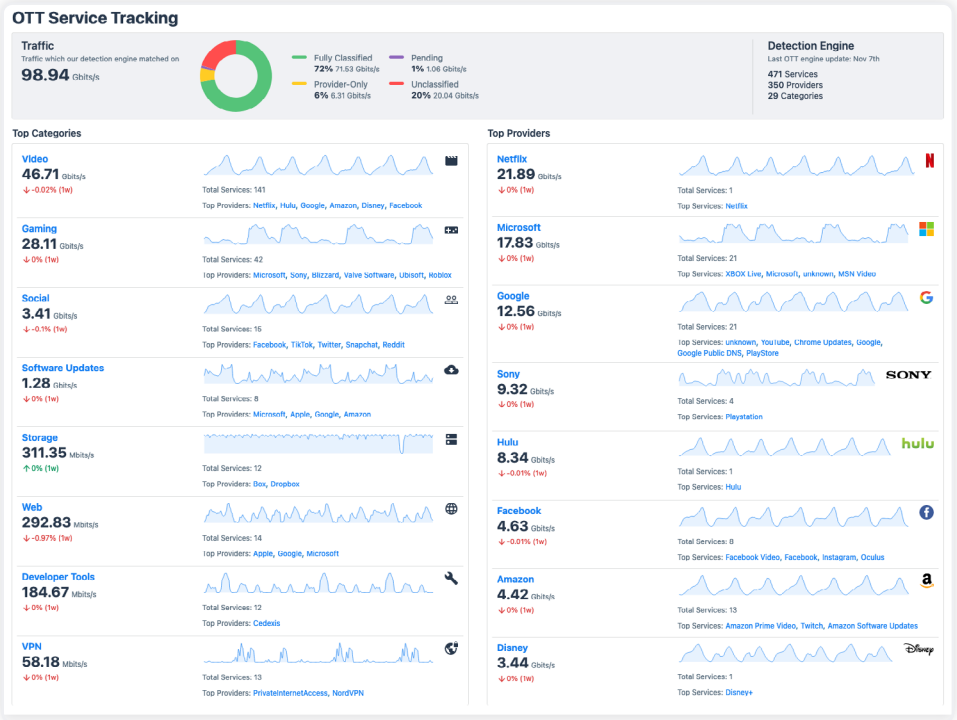
Visualize traffic paths and patterns as data flows from services to endpoints. Get a hop-by-hop view that makes it easy to drill into the root of performance problems. Get powerful visual cues on hover, such as color changes, thicker lines and additional information.



Trace/Path analysis infused with SNMP plus flow data

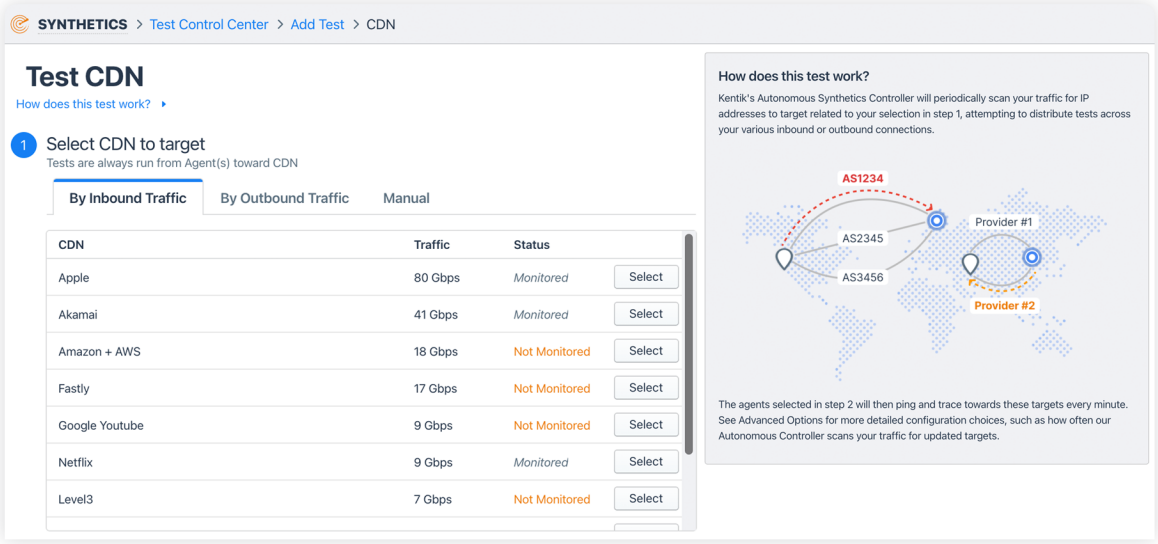
Analyze subscribers

Analyze subscribers, see traffic trends, and track your digital supply chain. Manage service quality across subscriber segments. Benchmark CDNs to optimize performance and cost. View granular consumption patterns by OTT service or market segment to uncover new revenue opportunities. By leveraging real-time telemetry from network equipment that's already in place, service providers can get key insights about cost, performance and customer behavior.



Gauge content delivery

Measure performance and track connectivity to CDNs or ASNs autonomously. See synthetic-test results in the context of real traffic from content providers. Evaluate CDN performance using Kentik's global CDN map and scenario-testing capabilities, which allows ISPs to test each CDN that delivers content via their network.



A comprehensive approach to DEM is essential for service providers who wish to defend and expand their leadership position in their chosen markets. Having the right DEM solution and strategy makes all the difference. Kentik offers custom demonstrations and a 30-day free trial.

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. Kentik makes sense of network, cloud, host, and container flow, internet routing, performance tests, and network metrics. We show network pros what they need to know about their network performance, health, and security to make their business-critical services shine. Networks power the world's most valuable companies, and those companies trust Kentik. Market leaders like IBM, Box, and Zoom rely on Kentik for network observability. Visit us at kentik.com and follow us at @kentikinc.

kentik®

Revised 20220317