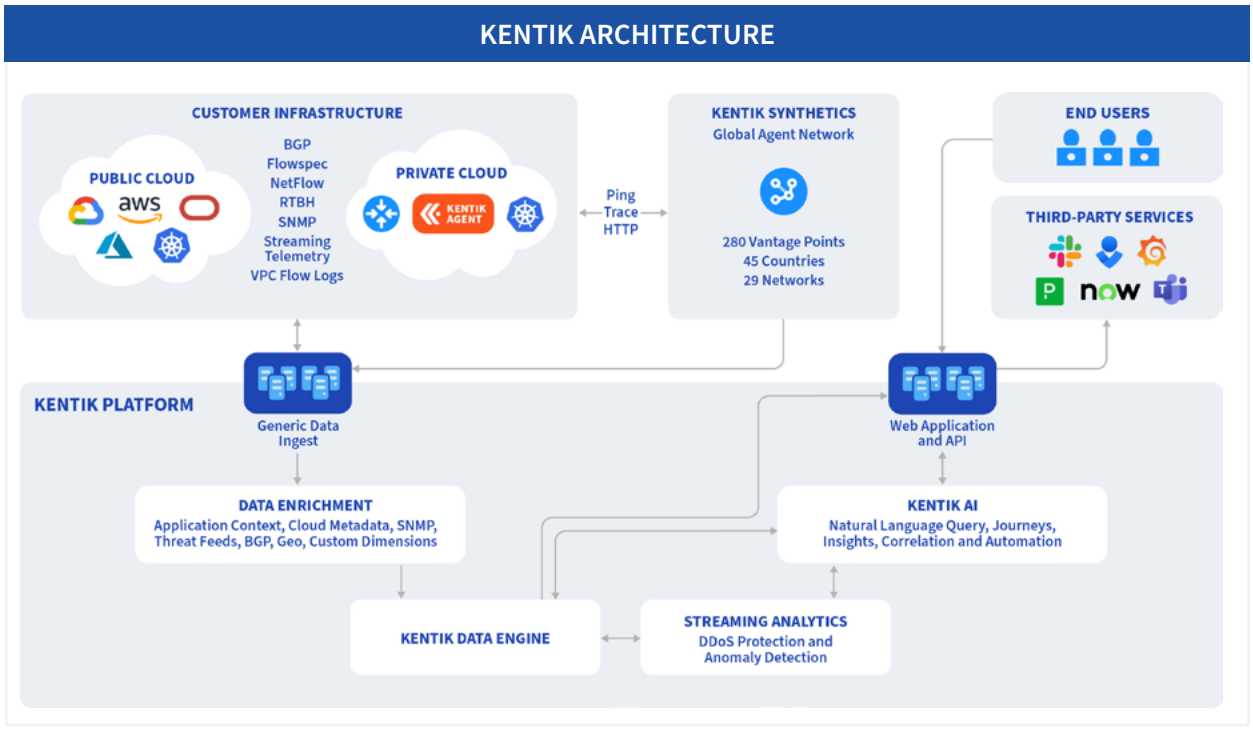
When you partner with Kentik, you're trusting us to provide you with insight into complex network environments, which means processing metadata and telemetry about how your devices are functioning. Before you get started, we want to make sure you have insight into how we're securing our systems and infrastructure.

The basics

Kentik is a SaaS-hosted web solution that helps our customers gain visibility and control over complex network environments, including network management, monitoring, testing, and security detection features. The platform has been architected to provide multi-factored scalability, reliability, and security. Due to the volume of information we process, the system is run from Kentik-maintained servers operated out of world-class co-location facilities in the US and Germany. Managing our own hardware lets us maximize the amount of data we can process for you and allows us to meet the needs of Fortune 50 customers, global ISPs, CDN providers, and major players in video streaming services. In addition to our managed infrastructure, we also maintain a small amount of infrastructure with major cloud hosting providers to help ingest customer data more smoothly.



Kentik's primary data sources include NetFlow data, VPC flow logs, SNMP, streaming telemetry, results from synthetic tests (such as traceroutes, pings, and tests for accessibility of web pages and APIs), public cloud metrics and BGP routing information. This data can be sent directly to us (over

the internet or via private network interconnect), but many customers use Kentik-provided agents to collect, encrypt, and transmit data in route to our system.

Encryption

We help you monitor a variety of network data, including several types of data that were historically sent without encryption. Fortunately, we offer several ways to make sure *everything* you send to us can be encrypted with minimal work. To make this work, we offer dedicated proxy agents that collect data and encrypt it en route to us, options to transfer data to our data center using private tunnels (private network interconnects), and ways to collect data directly between accounts of major cloud providers.

We make sure everything you send to us can be encrypted with strong, modern encryption techniques, and we enforce use of TLS 1.2 or greater. When we store data, we make sure to secure it at rest with AES-256 grade encryption and we regularly test our infrastructure to make sure our use of encryption reflects modern best practices. When designing these systems, we make sure to use algorithms and approaches that meet FIPS 140-2 requirements.

Secure development lifecycle (SDLC)

We're constantly working to make our systems better, which means we release updates many times each week. When we release updates, we make sure of the following:

- All code changes are tested using both human and automated testing, with at least one independent individual other than the author signing off on the change.
- All changes are documented and tracked using standard project management and CI/CD systems to make sure they're thorough, controlled, and well understood.
- Changes are tested in non-production environments before migration to production, and we *never* do this testing using raw Production data.
- We maintain the ability to quickly revert system changes if they introduce unexpected bugs, issues, or behavior.
- Maintenance windows and performance issues are documented on a dedicated status page (US: https://status.kentik.com/, EU: https://status.kentik.eu/) for Kentik services.
- We use independent tools to help monitor and patch vulnerabilities in our system, including major libraries and dependencies.
- Developers are trained on secure software development practices and corporate security requirements.

Vulnerability patching, penetration testing, and bug bounty

We perform frequent and regular vulnerability scanning of our infrastructure to make sure we're aware of exploitable security risks. Kentik service runs entirely on netbooted ("root") diskless Linux. Gold (boot) images are kept updated by rebuild and running images via config management and/or by rebooting into new gold images. Patches are deployed to remediate vulnerabilities and run only supported versions of software. Operating system images are hardened to provide only the necessary ports, protocols, and services to meet business needs using repeatable technical controls.

We also run a bug bounty program to ensure that risks that might evade traditional vulnerability scanners are found, evaluated, and fixed. At least once a year, we also engage a reputable third-party firm to perform penetration testing of the application and supporting infrastructure, with these reports available for customer inspection under NDA. Any issues identified by these processes are tracked and resolved according to internal policy requirements, with the functioning of the program reviewed by SOC 2 auditors.

Kentik is open to coordinating any customer-initiated assessment activity, provided that it is scheduled in advance, poses no potential to disrupt normal operations, is conducted on a running up-to-date copy of Kentik's SaaS platform, and is conducted at the customer's expense.

SOC 2

In addition to maintaining our own security standards, we engage third party auditors to test and report on our security practices. Once a year, we complete SOC 2 audits and are happy to share our reports with customers and prospects. SOC 2 reports include detailed descriptions of our security systems and core security commitments, as well as auditor reports on the efficacy and maintenance of those systems over a sustained period of time.

SOC 2 report include independent review of core company security protocols, including:

- Personnel management procedures, including background checks, fraud controls, and evaluations of competency
- Practices surrounding security incidents, business continuity, and disaster response
- Corporate risk assessment, compensating controls, and treatment plans
- Corporate and product specific security controls
- General robustness of policies and procedures
- Deployment and management of technical security controls

For more information, please request a copy of our most recent SOC 2 report.

Data minimization and privacy

Kentik deliberately keeps our privacy footprint small and provides customers with tools to minimize sensitive data processing. We deal with network metadata that's typically focused on our customers' network devices, and we avoid collecting most types of personal information. While our system *does* handle IP addresses, we offer tools that let you to redact portions of the IP address to keep personal info out of our systems.

If you decide to stop using Kentik, we provide ways to transition your network data into new systems; we also delete system data stored with us promptly after you discontinue services. If you need help handling privacy-specific requests to view, edit/correct, or delete information, we're happy to support that through our normal support channels and commit to meeting the legally mandated turnaround times for request handling. That being said, these types of requests are rare for the information we process.

We do not process payment card information (PCI) or electronic private health information (ePHI) within our system. If you'd like to use our services in environments that do process this type of information, we're happy to explore your needs as part of procurement conversations.

GDPR

We offer DPAs to all customers that include the EU Standard Contractual Clauses (SCCs). Our DPA includes our authoritative commitments for GDPR compliance and can be found here: https://www.kentik.com/pdfs/KentikDataProtectionAddendum.pdf, including coverage for the data processing in the UK and Switzerland. We act as a Processor under the law and are happy to support you in the fulfillment of your GDPR-specific obligations. If you prefer, we can host your data in Frankfurt, Germany – please discuss this with your account executive or solutions engineer during the procurement stage. We don't expect to process any information classified as sensitive under the GDPR.

Data centers

We use co-location facilities located in Ashburn, Virginia, USA and Frankfurt, Germany. Co-location facilities ensure the availability of redundant power, HVAC, environmental protection, and security systems and including video monitoring, biometric identification, and customer-specific physical locks or cages around sensitive equipment. Any physical disks or storage media being decommissioned are securely destroyed prior to disposal, typically via mechanical shredding through a dedicated firm. Co-location facilities maintain high levels of compliance certifications that we review on an annual basis, and we additionally procure our own redundant network connections due to the volume of information we process.

Data segregation

Kentik is offered as a multi-tenant system with logical segregation of data between customers. We've carefully structured the system to ensure that customer data is maintained in separate file trees on our backend storage nodes; this makes it easier for us to always maintain strict data segregation and minimizes the chance for errors or inconsistencies to lead to data mix-ups. Our REST API, portal, and alerting system require credentialed access, which is verified and enforced through our control and access plane; this ensures individuals have *no* access to information beyond their own company. There is no "universal" endpoint via our database or API that allows access to data from multiple or all customers. Efficacy of data segregation is tested as a component of our annual penetration testing and our continuous bug bounty program.

Authentication, access, and monitoring

We support authentication via username and password, with support for multi-factor authentication (MFA). Our MFA options include TOTP systems (like Google Authenticator, Authy, etc.), and hardware tokens, including Yubikey. We also support SSO integrations via SAML 2.0. We test integrations with various identity providers, including Okta, OneLogin, Google, Salesforce, Duo, Shibboleth (LDAP and AD), and others. You can find more info on our options at: https://kb.kentik.com/v4/Cb11.htm#Cb11-Authentication_SSO.

Internally, only technical operations users have access to the Kentik production infrastructure. When such employees manage production systems, they are required to use VPNs to protect their access and additionally use hardware tokens (Yubikeys) to authenticate with infrastructure. To protect access to our corporate systems, we use a combination of SSO and systems configured to enforce MFA.

Security program and team

Kentik maintains dedicated security staff, with a CISO in charge of the security team, including compliance, privacy, and technically focused individuals. The CISO is part of the executive leadership team reporting to the CEO and maintaining lines of communication with our Board of Directors. Security staff work in close coordination with engineering, infrastructure, HR, legal, sales, customer success, and product teams to make sure customer, auditor, and internal needs are continuously met.

Kentik's security program includes a robust set of internal policies, which minimally include coverage for the following areas. Please request a copy of our SOC 2 report for a full listing of internal policies.

- Access control
- Security and privacy awareness
- Change and configuration management
- Contingency planning, including incident response, business continuity, and disaster recovery

- Data classification, retention, and handling practices
- Authentication requirements
- Encryption requirements and management standards
- Personnel security, including roles and responsibilities of those supporting security
- Physical security
- Risk assessment and treatment
- Secure development
- Vendor management

Personnel management

Kentik is a remote first company with a global workforce. All employees and contractors receive security and privacy trainings and are required to sign NDA or Confidentiality Agreements as a condition of employment to protect customer/tenant information. Pursuant to local laws, regulations, ethics and contractual constraints, Kentik performs a standard reference checks and background review as part of employment. Employee terminations are managed via a defined process, including removal of access rights to the Kentik infrastructure as part of the termination process.

Backups, retention, and disaster recovery

Kentik maintains disaster recovery infrastructure running in an active/active configuration; this means we can switch over to backup servers quickly and are able to continuously ensure that backup infrastructure is online and responsive. Our contracts typically specify a 99.99% uptime minimum, and we post information about any service disruptions to our public status page.

Data retention windows are specified in customer contracts, with our default retention for granular network monitoring data set to 45 days and higher-level derived statistics available for 120 days. Customer-defined data retention can be specified per license, for instance, a customer could specify that their edge flows are retained for one year but internal data center flows for 30 days.

On a daily basis, system configuration backups are securely exported from our co-location facility into a cloud environment to make sure they are accessible during disasters affecting the co-location facility. Please note that our backups are restricted to system configurations necessary to rebuild your environment and *do not* include telemetry, NetFlow data, SNMP, etc. that are continuously streamed in high volumes. Such data is continuously regenerated by customer systems, extends to tens of petabytes in our system, and is stored using redundant media within the production environments, rendering additional backup unproductive.

Within a Kenitk cluster, all layers maintain high availability (HA) redundancy, including physical hardware, databases, general systems, and web portals. To ensure our system remains fast and

responsive, HA infrastructure is split between buildings within a single geographic region and metro area. Customers who want live HA between clusters can configure data sources to redundantly report data ingests to multiple Kentik public and/or dedicated private clusters.

Business continuity and incident response

We perform annual tests to make sure we're prepared to respond to security incidents and disruptions to services. Tests include tabletop drills where we practice walking through incidents in a structured setting, including technical elements, communications plans, internal coordination, and review of existing procedures. We also perform quarterly backup tests to make sure we can recover the system in the event of an adverse event.

Our program includes steps to prepare for incidents, detect and analyze them, contain the issue, eradicate the problem, recover systems, and perform post-incident follow ups. We commit to promptly notifying affected customers of incidents consistent with our contractual requirements and relevant data protection laws.

Logging, monitoring, and alerting

System activities are logged, with logs viewable by customers in application. Logs include coverage for access events, including successful and failed logins. Any time Kentik accesses customer accounts (e.g., in response to support requests), such access is logged and visible to customer personnel. Internally, we log database queries and retain them for forensic purposes.

Kentik maintains performance logging and alerting to make sure that systems remain responsive, healthy, and secure. Anomalous logs are escalated to the appropriate staff for review, with proactive alerts sent in internal communications channels, dedicated dashboards, and paging-based/incident response systems.

Third-party vendors and partners

Like most companies, we use a small set of high quality sub-processors and third-party vendors to provide our services, including the co-location facilities where our equipment is installed. These sub-processors are accessible from our legal page (https://www.kentik.com/legal/), and we make sure each is bound to a similar set of security and privacy commitments relative to what we offer to our customers. When engaging a new sub-processor, we review their security documentation, privacy posture, audit documents, and data handling practices to make sure they'll meet the needs of our most selective customers. We'll post any changes to our sub-processors publicly so you have a chance to review the change and escalate any potential concerns to our team.

To help you get the most out of Kentik, we support a number of customer-configurable integrations, including integrations with internal communications systems, notifications platforms, DDoS protection and response systems, and flexible integrations delivered via JSON webhooks. Integrations

are always controlled by the customer, and must use validated customer access credentials controlled by the user. Customers fully control access to generate and revoke those keys, accounts, and API permissions.

Kentik does not share any raw customer telemetry information with any third party systems; however, a few Kentik customers choose to sign contractual agreements allowing us to use aggregated or otherwise specified data for internal research purposes. This is never done without explicit contractual consent.

Next steps

If you have questions we didn't answer, please take a look at detailed documentation found in our Knowledge Base (KB) pages, starting with our security overview: https://kb.kentik.com/v0/Ab03.htm; we also encourage you to start up a conversation with our sales team who can connect you with the right people to answer specific questions or support your internal procurement processes. You can also get in touch with us at security@kentik.com or legal@kentik.com, depending on your concern.

If you want to learn how Kentik can be used to secure your *own* network, please take a look at https://www.kentik.com/solutions/detect-and-mitigate-ddos/, https://www.kentik.com/solutions/harden-zero-trust-cloud-network-policy/, and https://www.kentik.com/solutions/investigate-security-incidents/ which provide high level overviews of the system. Finally, if you like what you've seen, you can take a closer look for yourself right here: https://www.kentik.com/get-started/.

ABOUT KENTIK

Kentik is a leading observability company across the network, infrastructure, and cloud. Our platform is a must-have for the network front line, whether digital business, corporate IT, or service provider. Network professionals turn to Kentik to plan, run, and fix any network, relying on our infinite granularity, AI-driven insights, and fast search. Kentik makes sense of network, infrastructure, cloud, host and container flow, internet routing, performance tests, and network metrics. We show IT what they need to know about their network performance, health, and security to make their business-critical services shine. Market leaders like Akamai, Booking.com, Dropbox, and Zoom rely on Kentik for network observability. Visit us at kentik.com.