This document focuses on security considerations related to Kentik's data protection and privacy architecture, implementation, contractual and regulatory responsibilities, and operational methodologies. It is intended as a supplement to the overall Kentik Security article in the Kentik Knowledge Base.

Kentik's Platform is Multi-Tenant but Segregated

The Kentik Data Engine (KDE) is designed as a multi-tenant system with tightly enforced customer data segmentation. All customer network data — whether coming from flow records, BGP routing data, SNMP, Geo IP mapping, or business policy mappings (tags or custom columns) — are stored in separate file trees on our backend storage nodes.

Data access is allowed only through our REST APIs, our portal, or our alerting system, and involves credentialed access through our control and access layers. Individual user accounts have no path to access information from outside their own company.

The Kentik Information Security and Privacy Program

Kentik has adopted the NIST 800-53 framework as the basis for its information security and privacy program.

The Kentik information security program includes elements from the following control areas: Access Control, Security Awareness & Training, Audit & Accountability, Security Assessment & Authorization, Configuration Management, Contingency Planning, Identification & Authentication, Incident Response, Maintenance, Media Protection, Physical & Environmental Protection, Planning, Personnel Security, Risk Assessment, System & Services Acquisitions, System & Communication Protection, System & Information Integrity, Personally Identifiable Information, Supply Chain Risk Management and Program Management.

The Kentik information privacy program includes elements from the following areas: Authority to Collect, Privacy Impact Assessments, Privacy Requirements for Contractors and Service Providers, Privacy Monitoring and Auditing, Privacy Awareness and Training, Accounting of Disclosures, Validation of PII, Minimization/Removal of PII, Data Retention and Disposal, Internal Use, and Sharing with Third Parties.

Kentik and Common Regulatory Requirements

- PCI-DSS: Kentik does not store or process credit card information.
- HIPAA: Kentik does not store or process any electronic protected health information (ePHI).

General Data Protection Regulation (GDPR) and Kentik

The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union. It addresses the export of personal data outside the EU.

Kentik does not store or process information commonly classified as personally identifiable information (PII) such as:

- Social Security number
- Drivers license number
- Home address
- Medical information
- Credit card or payment card information

Data Ownership and Obfuscation

Kentik has no rights to customer data without permission. All information ingested as part of the service is controlled by the customer. The customer may at any time purge all customer supplied data ingested by Kentik as part of our network monitoring and analysis offerings.

Kentik's standard contract includes a non-disclosure agreement that requires Kentik to protect customer confidential data. While customers can elect to allow aggregated and anonymized access to their data for internet-wide measurement, Kentik places no pressure on customers to opt in, and unless included in contractual agreements, non-disclosure prevents Kentik from using data in this way. Kentik does not share customer data with any third party.

For customers who wish to use Kentik but require the obfuscation of IP addresses for privacy or regulatory needs (e.g. GDPR), the Kentik "chfagent" flow proxy software supports flexible masking options that enable bits to be masked before being sent to Kentik.

It should be noted that obfuscation may limit the ability to detect and mitigate attacks down to the /32 or /128, and may force black-holing and mitigation to capture (and often impair) more traffic than is necessary. With that said, alerting does support grouping and mitigating on any CIDR boundary, so it is possible to use Kentik to learn, detect, and alert only on /24s or shorter prefixes.

Kentik has disaster recovery (DR) sites running in an active/active configuration. We do not store offline backups of any customer data. Because of that, there are no offline systems on which we must delete or purge data when required. Kentik does not store data for longer than 120 days, unless extended retention is requested by the customer.

Access Control and Authorization – Methods and Tunable Access Restrictions

Kentik supports the following approaches to govern customer access:

- User access: single sign on (SSO) and two-factor authentication (2FA).
- API and UI access: ACL's tunable on a per-user basis.

Access into Kentik production systems is only permitted to authorized Kentik personnel. Access is controlled through a combination of encryption certificate authentication and two-factor authentication via a hardware token (e.g. YubiKey). Once access to a system has been obtained, further access is controlled within the system based on the role of the individual.

Kentik staff who have access to the backend systems are limited to senior administrators via logged 2FA authentication. We rigorously monitor performance and data transfer across our clusters, including per-machine IOPS and CPU, each software component, and the overall health of the system. Software components and system health are monitored by both synthetic and passive (actual traffic) performance and data flow monitoring.

While Kentik does use individual Independent Contractors to perform work for the company, we never send flow data to any third party, or contract work to outside organizations that provide Kentik access to persons that are not contracted to us directly.

Operational Methods – Optimized for Data Protection

All database queries are logged for no less than 14 days. For on-premises Kentik clusters, the systems can be integrated into customer security monitoring systems.

Physical Security

Kentik hosts its production system at Equinix facilities, all of which have mandatory 24x7 biometric authentication for access, logging of any removed equipment, and video surveillance in entrances, hallways, and cages. Equinix facilities are ISO27001 certified and SOC 2 Type 2 data centers.

Vulnerability Assessments & Penetration Testing

Kentik performs weekly vulnerability assessments against its public facing infrastructure. Kentik also performs quarterly internal vulnerability assessments weekly. The vulnerability assessment targets all web servers, firewalls, network equipment, database servers, management systems, and Kentik application servers.

Kentik also performs annual semi-annual penetration tests against its public-facing systems. The penetration tests are performed by an independent third party. Kentik has also engaged a commercial bug-finder service that constantly tests our public-facing infrastructure and provides monetary

rewards to individuals who find flaws. We do not allow unsupervised audits of any of our systems containing, or having access to, customer data.

Executive report statements from technical testing are available upon request.

Secure Software Development

The Kentik software development process follows the OWASP guidelines for secure web development, including use of the OWASP dependency checker. We use static analysis and our architecture reviews include gaming and threat modeling. For additional information on the Kentik operational and development practices, please review the Security Methodology topic in our Knowledge Base.

Encryption

Kentik supports the encryption in transit of all flow, routing, and customer metadata and API usage. By default, data in flow protocols such as sFlow, NetFlow, and IPFIX are sent over unencrypted UDP, however Kentik offers a free software agent ("chfagent") that delivers flow and SNMP data over encrypted multiplexed TLS-transported streams.

All customer data is encrypted at rest on all Kentik production systems that store or process customer information.

Additionally, single or redundant private network interconnects (PNIs) are possible for customers whose networks connect at Equinix Ashburn VA USA data centers. This connection type may be a physical connection from cage to cage or between buildings. No data transferred between a customer and Kentik via PNI ever crosses over a public network connection.

Both in-transit and at-rest encryption meet the FIPS 140-2 standard.

All production systems are additionally protected by our access processes, data flow monitoring, and auditing. Production systems are physically protected inside of Equinix data centers with physical access controls and real-time video surveillance monitoring.

We have no near-line storage. Any asset removed from our production SaaS infrastructure triggers immediate 24x7 response as part of our effort to ensure constant availability of the Kentik services. If a storage device must be removed from the Equinix facilities, the data on the encrypted drive is erased before being removed from the facility.

Incident Response

Kentik has a dedicated team for security incident monitoring and response. Kentik has developed an incident response program to help prepare our dedicated Incident Response Team.

Kentik works with an independent firm not less than annually to recreate real-life scenarios and test the effectiveness of our IR program, which is based on the NIST 800-61 Computer Security Incident Handling Guide. This program identifies six distinct phases of the IR process:

- Preparation
- Detection & Analysis
- Containment
- Eradication
- Recovery
- Follow-up

Third Party Security

Third-party vendors used by Kentik undergo a thorough security risk assessment and are analyzed by our security team. Once the vendor meets Kentik's security requirements, Kentik will periodically reassess their security controls and agreements in place. Kentik ensures that all data is returned and/or deleted at the end of a vendor relationship. Customer data is not shared with any third parties without the explicit authorization of the customer.

Commonly Asked Questions

1. **What data does Kentik store?**
   Kentik stores network traffic data related to "flows" (sets of related packets), including IP address information. Kentik does not store or process information commonly classified as personally identifiable information.

2. **Does Kentik encrypt data at rest?**
   All customer data is encrypted at rest on all Kentik production systems that store or process customer information. At-rest data encryption meets FIPS 140-2 standards.

3. **Does Kentik encrypt data in transit?**
   In-transit encryption meeting FIPS 140-2 standards is available when using our local proxy agent (chfagent).

4. **Can Kentik remove data regarding an individual IP from our system?**
   Customers have complete control over their data and can purge all stored information at will.

5. **What information do you share with third parties?**
   We do not share any information with third parties unless requested to do so by the customer.

6. **Does Kentik have a data protection officer?**
   Kentik has a designated individual filling the role of data protection officer.

7. **Does Kentik have a breach notification policy?**
   Breach notification is integrated into the formalized Kentik Incident Response plan.

8. **How long does Kentik store data?**
   We store customer data for as long as you are an active customer. Once you cancel service, we purge your data from our system. You also can purge your data at any time. Our standard retention period for flow data is 45 days for “full” resolution and 120 days for “trending” resolution.

Version: June 2, 2021