ElastiFlow

See what matters.

Unify Your Observability!

Bridging the NetOps, DevOps, and SecOps Divide

As networks become more complex, NetOps teams are conscious of deploying more flexible, programmable, and scalable network infrastructure. Most legacy monitoring tools were designed for NetOps teams to monitor and plan the network or for DevOps teams to monitor the latency of their apps. SecOps haven't had the tools to investigate network traffic or be notified of unusual traffic.

This results in siloed teams, tools, and processes, and it fosters inefficiencies. But there is another way.

Introducing:

ElastiFlow NetObserv

ElastiFlow NetIntel

elastiflow.com

The ElastiFlow Approach to Unified Network Observability

NetIntel

NetIntel enhances your network detection and response posture by enriching your network flow data with indicators of compromise, IP reputation, application context, and MITRE ATT&CK information. The NetIntel threat feed is sourced from thousands of our global collectors, validated by all the network traffic we collect, so threats that matter are brought to your immediate attention.

NetIntel brings intelligence about your network traffic into your list of threat alerts. Other threat feeds provide Indicators of Compromise based on external bad actors, but many attacks originate from the inside (Phishing, disgruntled employees, etc.). NetIntel leverages your network data and business context to arm you with the information you need to prioritize threats.

Benefits of NetIntel:

- Know if your users are talking to bad actors
- Know if legitimate users are accessing apps they shouldn't
- Know what cloud services employees are using - shed light on Shadow IT!

NetObserv

NetObserv collects SNMP and flow data from routers, switches, firewalls, and hosts, and enriches the data with geo, ASN, threat intelligence, DNS, and user-defined business context. NetObserv collects unsampled flow data and normalizes this data with over 4,700 device profiles.

NetObserv collectors are easily integrated with your chosen open data platform so that data can be aggregated across platforms, such as app monitoring or security feeds. By feeding this data lake, AI and ML models have a rich environment to generate the insights needed by your network, security, and development teams.

Some of the most popular backend pipelines include Elasticsearch with Kibana, OpenSearch, and Kafka with an analytics database like Druid. ElastiFlow also has integrations with Slack and Tines. Each piece of the pipeline can be scaled out and enhanced with features like ML, ETL (extract, transform, load), and enrichment. We offer deployment options for cloud, on-prem, and virtual environments.

The ElastiFlow Advantage

1. Enhanced Network Security

Network data is the most important tool we have to identify relevant IoCs. ElastiFlow enriches your network data, combines this data with intelligence generated by our global threat sensors, to generate alerts based on your networkdata, revealing not only external threats but internal as well.

2. Powerful analytics

ElastiFlow provides powerful analytics tools that allow you to troubleshoot problems, plan capacity, and investigate security incidents. The collection of unsampled flow data means that you can see and investigate everything.

3. Easy to use

ElastiFlow is easy to use and requires no special training. Our easy setup guide will get you started in minutes - not hours or weeks.

4. Complete network visibility

ElastiFlow collects unsampled flow data and standardizes data from network devices, including industry-leading vendor-specific field support, to actually achieve complete network visibility. ElastiFlow adds context to this data including geo location, app and service information.

5. Open data

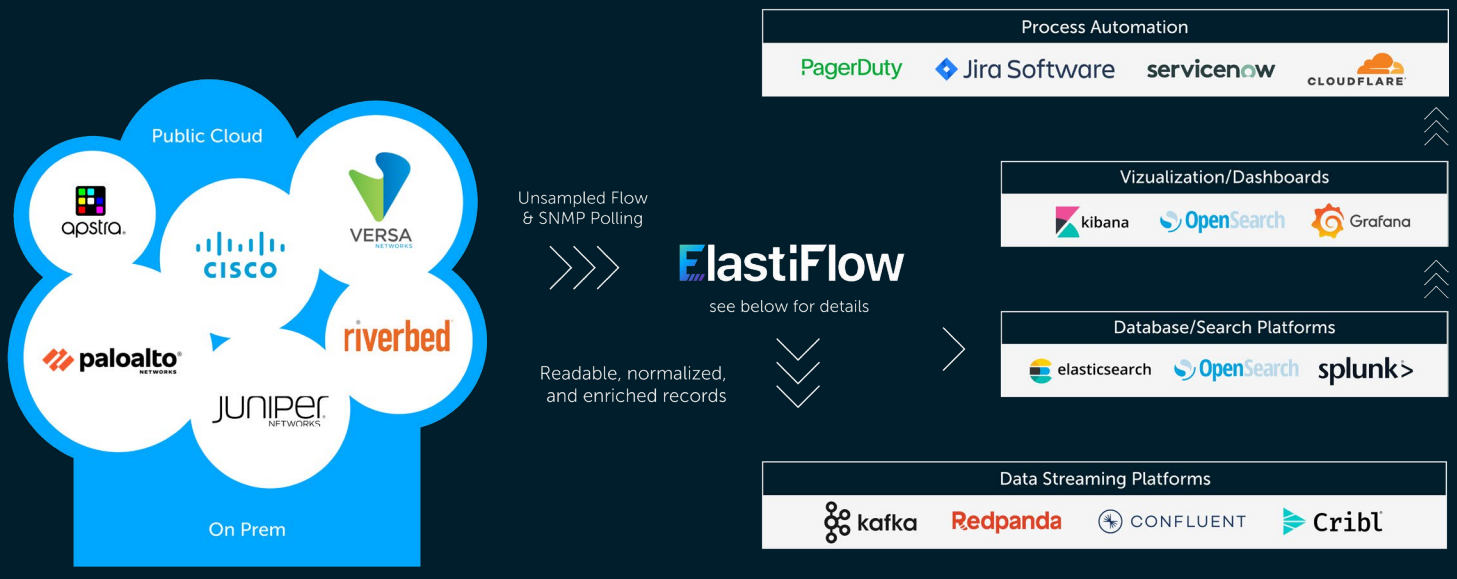
ElastiFlow takes an open data approach to network observability, meaning you remain in control of your data and can economically leverage this data. Use other open data platforms to leverage additional AI and ML models.

Unleash Network Insights Across Your Organization

NetObserv and NetIntel produce insights into network activity that will prove invaluable to not only NeOps but also their DevOps and SecOps colleagues. Tools such as Kafka, Elasticsearch, OpenSearch, Grafana, and Kibana are commonly used by these teams due to their scalability and extensibility. Historically, NetOps has turned to purpose-built, proprietary solutions to meet network observability needs.

Unfortunately, these solutions usually lock up your critical network data in silos making it unavailable to benefit from the growing power and insights that can come from exposing this data to observability solutions. This is especially the case as ML and AI tools become increasingly useful. Sure, many network observability solutions are advancing in ML and AI, but this data is often siloed. Your network data can add a new richness to application and security data.

ElastiFlow helps you bridge the NetOps, SecOps, DevOps divide.



ElastiFlow Use Cases

Network Security Analytics

1. Anomaly Detection

Detect anomalies in traffic patterns that may indicate malicious activities, such as unusual traffic volume, connections to malicious IP addresses, or unexpected traffic on specific ports.

2. Threat Identification

ElastiFlow can detect various network threats, including DDoS attacks, data exfiltration, botnet activities, and unauthorized access attempts. We bring to your attention real threats, not noise such as most port scans, identified using our global honey pots and your actual traffic.

3. Forensic Analysis & Incident Response

In the event of a security breach, ElastiFlow can help investigators understand the timeline of events, the scope of the attack, and the methods used by the attackers. This investigation can be done with context, such as which apps were accessed by which users in which locations - even communications by internal users.

4. Compliance and Reporting

Many regulatory standards require organizations to monitor network activity and maintain logs for security purposes. Unsampled flow collection means you'll have a comprehensive picture.

Performance and Availability

1. Capacity Planning & Cost Control

With the insights provided by ElastiFlow, network engineers can implement strategies to optimize network traffic flow, reducing latency, balancing load across network paths, and ensuring efficient use of available resources.

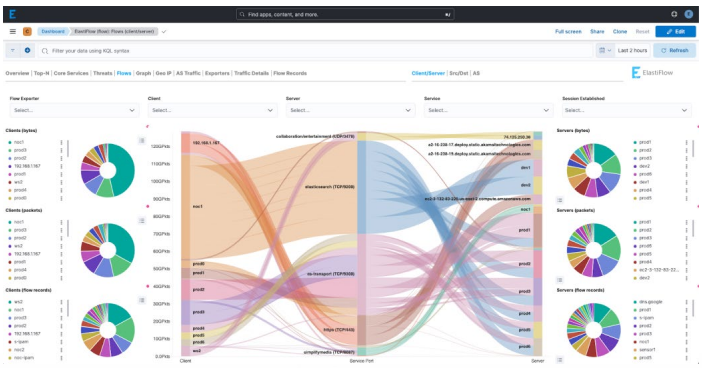
Analyze historical network usage, identify trends, optimize network resources, plan for capacity upgrades, and avoid bottlenecks.

2. Visibility and Insight

ElastiFlow provides granular information about network traffic flows, including source and destination IP addresses, ports, protocols, apps accessed, and the amount of data transmitted.

3. Identify Issues

Diagnose and troubleshoot network issues such as congestion, high latency, or packet Loss.



How can I get started with ElastiFlow?

Get started with Elastiflow by downloading it from our website. We offer a free trial so that you can try it out before you buy it. elastiflow.com