

BETTER TOGETHER:



Unparalleled Network Observability

Harness the full potential of your network by combining the power of Elastiflow's network traffic analysis and performance monitoring with the Elastic Stack. This integrated solution empowers teams to transform raw flow data into actionable, real-time intelligence, fostering cross-team collaboration and accelerating incident response.



Gain Complete Network Visibility with Instant Insights

Make data-driven decisions with a comprehensive understanding of your entire network infrastructure. The solution ingests a wide array of flow data, including NetFlow, IPFIX, sFlow, and cloud flow logs, with the ability to decode over 7,300 vendor-specific fields. Raw data is transformed into actionable intelligence through a multi-stage enrichment process that adds critical context, including GeoIP and ASN information, cloud and application identification, integrated threat intelligence, and user-defined metadata.

This enriched data provides a complete picture, allowing you to move beyond simple traffic monitoring to deep, contextual analysis and network optimization.



Drive XOps Collaboration

Break down the silos that hinder operational efficiency. Elastiflow creates a single, unified source of truth for all network activity, accessible within Elastic. When NetOps, SecOps, and DevOps teams work from the same enriched data, dashboards, and reports, collaboration becomes seamless.

This shared visibility enables your organization to move from reactive to proactive operations, accelerate incident response and root cause analysis, improve end-user digital experience, and increase operational efficiency.



Accelerate Time-to-Value

Elastiflow delivers immediate insights by equipping your Elastic deployment with a suite of out-of-the-box tools designed to provide instant value. Instead of starting with a blank slate, you get a fully functional analytics



platform in minutes. This turnkey solution includes 120+ machine learning jobs that automatically detect anomalies, identify patterns, and surface potential threats without manual configuration and 40+ pre-configured, customizable dashboards for at-a-glance monitoring of traffic, performance, security, and more.



Enterprise-Grade Performance and Scalability

Built to handle the demands of modern networks, ElastiFlow's architecture is centered around a high-performance unified collector. It is designed to scale effortlessly as your data volume grows. We provide native support for Elastic's Time Series Data Streams (TSDS), a feature that can reduce storage costs for high-volume flow data by up to 70%. Our Advanced Index Sorting offers additional storage savings while simultaneously accelerating query times, ensuring you get the answers you need, faster.

Key Use Cases Unlocked

- **Network Traffic Analysis:** Understand exactly who is talking to whom, what paths they are taking, and which applications consume the most bandwidth.
- **Capacity Planning:** Analyze historical trends to accurately forecast bandwidth requirements, plan infrastructure upgrades, and avoid service degradation.
- **Performance Troubleshooting:** Quickly pinpoint the source of issues to resolve network, application, and service slowdowns faster.
- **Security Monitoring:** Detect DDoS attacks, data exfiltration, network scanning, and other malicious activities by leveraging enriched data and machine learning.

ElastiFlow +  elastic



ElastiFlow
Aggregate - Standardize - Enrich - Prioritize

 **Security**

 **elasticsearch**

 **Observability**



elastiflow.com



See it in action

Ready to take a closer look at the ElastiFlow platform?
Contact us today to learn more.
Schedule a demo and get a free trial