Elastic and ElastiFlow: Optimizing DoD network performance and IT operations

For network teams, dealing with secured networks is consistently getting more difficult as customer expectations grow and networks become more complex. U.S. Classified networks need to be secured; each one has special information that should only go to specific groups of people. Each network needs to own its control. Data owners on each classified network are commanded to ensure their data reaches only certain people, and these data owners need to be empowered to control the security of their data.

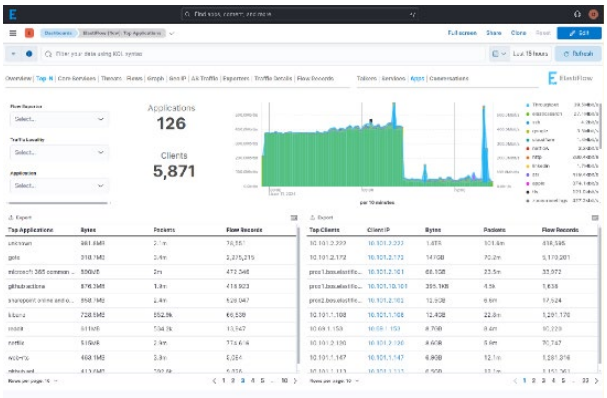
There was a time when data was rarely transferred between classified networks, but this continues to evolve. The expectation now is that most data must be available at many different military bases or agencies. This involves a large collection of firewalls, data scanners and routing protocols to assure the necessary control and protection of each network. Many different methods are used to assure protection of data and systems.

This list of protections only grows when we go up the stack. The new cyber buzzwords of today are focused on the application layer: Zero Trust, application service level agreements (SLAs), data mesh.

All of these terms assume a robust network layer. While it's exciting that these frameworks will help secure our cyber future, they are much easier to implement within unsecured networks. When we add all of the necessary security controls of a classified network, assuring a robust network layer is that much more difficult. This is why dealing with secured networks is getting more difficult in classified environments.

As network layer expectations grow, so does the technology needed to improve the network layer. The scale, speed, and ease of use continues to improve. More people get to see more relevant and potentially more informative data.

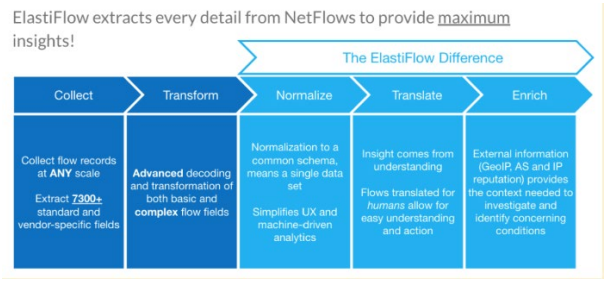
Using Elastic and ElastiFlow together can help you keep up with the new network requirements. This combination brings the new modern datastore capabilities with the latest in flow (netflow/sflow/ipfix, etc.) collection, enrichment, analysis and detection. Together, the solutions reveal the learning and insights you need to ensure optimal network performance and security insights.



What is ElastiFlow with Elastic?

Elastic has teamed with ElastiFlow to provide the best in modern flow monitoring connected to a limitless datastore and SIEM. Elastic is used throughout the US Army, Navy, Air Force and supporting agencies. Several training schools teach Elastic, and there are 100+ ATOs with Elastic throughout the military services. Many Security Operations Centers (SOCs), Risk Management Framework (RMF) offices, and the deployable Cyber Protection Teams (CPTs) are currently relying on Elastic for their cyber needs.

ElastiFlow is a new and modern way to get the most out of flow data. New datastores and extraction methods make it easy to not just monitor your network but also investigate performance and security issues. These new methods also make it easy to analyze years of flow data at the same time. No more black box networks in the path. No more aging out data. Months and even years of history can be queried and visualized. Connect all the flows from any time together in one view. ElastiFlow is built to collect and enrich sampled or unsampled network flow data at any scale, so that you get a comprehensive understanding of all network activity.



ElastiFlow feeds Elastic with flow data enriched with DNS, GeoIP, online application identification and threat information, so cyber and network teams get more actionable network data

See every flow — even that one

ElastiFlow with Elastic offers a solution to capture and analyze 1:1, unsampled flow data. This approach ensures that every packet and byte is accounted for, providing a comprehensive view of network activity. Old data does not have to be forgotten, either; it can be stored in low-cost S3 or equivalent storage.
Such granularity facilitates precise decision-making, enhances performance tuning, and strengthens security protocols. Every network conversation can be searched at any time. By integrating with advanced data compression technologies, such as adapting Elastic TSDS for

flow-data collection, ElastiFlow also addresses storage concerns, making this level of detailed observation both feasible and scalable. This shift not only eliminates the need for trade-offs between data depth and resource usage but also sets new standards in network data analysis, ensuring that network and cybersecurity professionals are equipped with the most detailed and actionable insights.

See “their” cyber data (the data mesh version)

With legacy flow tools, we all have seen that NetFlow diagram with a big black box. This is because the network may be a single network, but it is owned by many independent agencies and services. The box exists because the flow goes into a different part of the network that is managed by a different team. And the more connected we are between services and agencies, the more of these black boxes are seen in legacy flow tools. This makes it difficult to truly troubleshoot a problem because an analyst can only troubleshoot the part of the network that they have access to see.

Elastic Cross Cluster Search (CCS) can remove those black boxes. CCS enables you to see those flows owned by other teams. All you need is that organization’s permissions and their data is added to your data. It looks exactly like your data. The other organization decides what data you see and nothing more, giving everyone full ownership of their data. Many teams in the DoD are using this approach today to connect datasets from around the world, from different clouds, and from behind different firewalls.
This lets you see the whole network path — no more black boxes.

Ease of use — the AI version

ElastiFlow and Elastic are built fully around AI and ML. As we all know, AI is changing everything. New technology is built from the ground up with AI/ML. The chatbot (LLM) is just a click away at any time. What does this mean? This means that every flow record, every log, every metric in Elastic can be used to interact with your favorite LLM. Elastic automatically brings additional context to every conversation. For instance, if the user asks the LLM for more information about an alert, Elastic adds key context to the query, resulting in the LLM answering with details pertinent to your environment. Advances in AI let any user open up a tool and look like a seasoned pro. The AI will even provide exact instructions on how to resolve any issue.

Open Schema with Cross Cluster Search — connect the data

In a schema, every data field is brought into ElastiFlow and Elastic in the same way. We can search for user IDs or IP addresses between Cisco devices and Juniper, from VMware to OpenShift, from ServiceNow to a GOTS product. Every system will bring in their data and it will all look the same. This allows an analyst to truly see every single log with a specific website URL or error code. In other words, you're able to correlate data between systems.

Together, Elastic and ElasticFlow have correlated over 10,000 industry standard fields into a combined schema. The Elastic Common Schema (ECS) has been adopted by several organizations within the DoD and commercial world. It is an industry standard, and it continues to be improved as it grows.

Connecting this schema with the SIEM data of other clusters allows you to see across the full attack spectrum. View the audit logs, firewall logs, flow data and any other security data together in a single view. Every network move, every act in the app, every login attempt that the attack makes will be seen in one single view. The full attack spectrum on one screen.

Real-world outcomes

What does this all mean? With all of these new capabilities, modern flow technologies change the game with flow data.

1. Accurate and detailed forensics:
In the event of a security incident, the ability to bring in all of the data, and not just some of it (unsampled data) allows for a detailed forensic analysis. You can trace the exact path of an attack through the network, understand the scope of the compromise, and identify the entry point and subsequent movements of the attacker within the network.
This precision is crucial for mitigating damage, repairing vulnerabilities, and preventing future breaches.

2. Improved cyber policy enforcement:
Comprehensive data helps in fine-tuning network policies and controls. For instance, unsampled NetFlow data can help validate the effectiveness of firewall rules, intrusion detection systems settings, and other security mechanisms by providing evidence of their performance in real-world traffic conditions.

3. Enhanced anomaly detection:
By monitoring all the data, machine learning and anomaly detection systems can be trained with complete datasets, leading to more accurate models of normal behavior and more precise identification of outliers.

This reduces false positives and false negatives, helping security teams focus their efforts where they are most needed. ElastiFlow can bring application context into flow data so you can see anomalies in app usage — “Why is my user in this department accessing this application in this location?”

4. Regulatory compliance and reporting: DoD has strict regulatory requirements for data handling and security. Unsampled NetFlow and Elastic SIEM data ensures that compliance audits are thorough and verifiable, with clear trails of data movement and user activity across the network.

5. Optimization of cyber performance and security: Beyond security, unsampled data can be used to optimize network performance. Identifying over-utilized or under-utilized links, diagnosing latency issues, and understanding traffic patterns can help in making informed decisions about infrastructure investments and upgrades.

To learn more, please reach out to dod@elastiflow.com and dod@elastic.co

