elastic

Search. Observe. Protect.

Data as a force multiplier

Imagine a scenario where warfighters, autonomous systems, and strategic decision-makers all employ a Common Operating Environment. Now picture a command center where unsupervised machine learning and artificial intelligence-supported systems alert a junior operator to a potential, multi-pronged cyber attack — and initiate a response — before key systems are compromised. In both these cases, complete, trusted, up-to-the-minute data powers these mission-critical capabilities.

Empowering warfighters. Linking services.

Across the DoD, using data as a strategic asset has been an elusive goal. Ideally, data could be easily shared and applied as needed, within and across the armed forces, supporting everything from joint operations to frontline responses. But getting to that point is challenging, as current approaches to data are inflexible, limiting the military's ability to pivot based on mission requirements.

The DoD Data Strategy is designed to create a multi-domain environment where data can be accessed and used by warfighters, commanders, and strategic partners to make faster, fully-informed decisions and take decisive action. That data also drives innovation, enabling technologies like DevSecOps and Zero Trust and bringing breakthroughs to the field faster and more effectively.

Getting there will take a radical rethinking of processes and technology — and how delivering real-time answers from that data can give all stakeholders decision dominance.

Operational impacts and roadblocks

For technical teams and operators, long-standing, interrelated factors — some technical, some procedural — have a large effect on how data is stored, accessed, and used. These include:

- **Volume.** The sheer quantity of data collected across the armed forces is a major consideration, with terabytes of data being generated daily in geographically-dispersed locations.
- **Accessibility.** Restrictions put on resources by different organizations limits access to data needed to create comprehensive answers to time-sensitive questions
- **Compatibility.** The differing systems in use across the DoD, from cloud platforms to legacy solutions — with varying, often proprietary data formats — make access and sharing difficult, if not impossible.
- **Security.** The proliferation of threats and the evolving nature of cyberwarfare has put strict limits on data access.
- **Time.** The military must react at short notice — or no notice — based on changing conditions and command decisions.

Overcoming these challenges demands a common approach and the technology to make use of data at the precise point and time of need. The solution is enterprise-wide search.

Search drives actionable results. Instantly.

For many people, “search” brings up images of web searches, where queries are answered with links to data sources. That’s one aspect of search, but consider this: the ability to redraw a map as you drag it across a screen, update ETAs based on fluctuating weather and terrain information, or analyze the source of cyber attacks as they occur are all dependent on real-time search results — a continuous stream of queries and answers being displayed upon request.

The vast amount of data stored across the DoD presents a challenge when searching for those answers. Without a way to correlate and analyze all of the available inputs, answers will be incomplete, impacting the effectiveness of the information. But copying and moving terabytes — or even petabytes — of data to a central location is time- and bandwidth-consuming, and leads to issues of version control and timeliness.

Elastic takes a simpler approach: access and manage the data wherever it resides, whether that’s in the latest cloud databases or within proprietary legacy systems. In effect, this allows users to bring the question to the data, not the data to the questions. By itself, this saves time, manpower, and resources. But because Elastic indexes data as it is collected, that information is instantly ready to be accessed, analyzed, and used at the moment of need. Essentially, Elastic enables a “speed layer” that delivers answers almost as quickly as the question is asked.

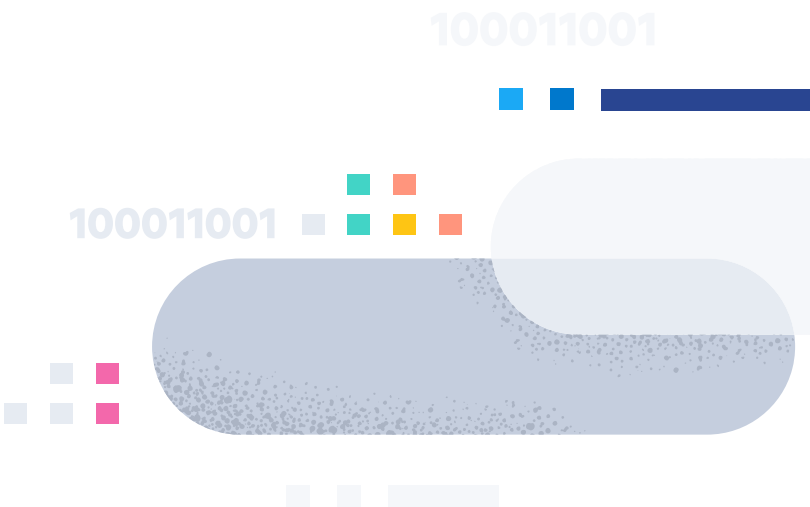
There’s another critical advantage to searching data where it resides: by eliminating duplicate resources, users are assured of a single source of truth — a reliable, comprehensive resource that ensures everyone is literally on the same page.

Interoperability is the key

Per the DoD Data Strategy, data must be readily available across the armed services, making interoperability critical. Standardization of data formats makes that possible, and enterprise-wide search makes it viable.

Interoperability is native to the Elastic Stack’s core design. Elastic’s free and open foundation means that data can be searched, analyzed, and presented without — or despite — the restrictions of distributed, proprietary solutions, which unlocks data to flow where and as needed. Using a common open source schema, the limitations presented by multiple systems, whether siloed or cloud-based, are removed.

As artificial intelligence and machine learning power more DoD systems, including autonomous systems that carry out mission objectives and adapt to unforeseen conditions, the ability to use data from across domains becomes even more urgent. An interoperable search and data management solution makes that not only possible, but practical.



elastic

Instant access to data still requires security

Creating a cross-domain environment of data access doesn't mean opening the gates to everyone. A Zero Trust approach is essential to prevent corruption or exfiltration of DoD data. Elastic's granular role-based access controls (RBAC) ensure that only those with the need and the authorization can reach information — but only the datasets they require to do their jobs. RBAC is a requirement of NIST compliance. DISA goes even further, recommending attribute-based access controls (ABAC). With Elastic's ABAC, organizations can apply policies that incorporate users, resources, and environments at a granular level.

Real-time results also support a proactive approach to cybersecurity, by identifying and alerting teams to anomalies and suspicious activity that could otherwise take much longer to notice. To amplify security operations, Elastic's SIEM and endpoint security module provide threat detection and threat hunting as well as anti-malware across the enterprise, including cloud implementations.

Meanwhile, Elastic Observability builds on the Elastic Stack, allowing IT and security teams to monitor traffic and application performance in a single pane of glass, enabling faster, more comprehensive analysis that can identify anomalies and bottlenecks faster, detecting potential issues before they impact productivity or secure operations.

Focus on mission enablement

With real-time information from all relevant sources, operators and decision-makers gain greater agility. At the same time, the cross-domain capabilities of Elastic's enterprise search can support efforts to enable the DoD Data Strategy, JADC2, and other data sharing initiatives. For IT and security teams, Elastic can save substantial time, reducing the need to transport, store, validate, and secure duplicate data.

The value of data is directly related to understanding and applying it at precisely the right place and time — whether that's in the hands of frontline operators, a command center overseeing a theater of operations, or the electronic mind of a UAV. Comprehensive, up-to-the-second data, powered by search, is absolutely essential to mission success.