



Elastic + DOD: Protecting Missions with Advanced Search and Analytics




The US Department of Defense (DOD) relies on secure IT infrastructures and communications for successful global mission accomplishment. Its systems must be defended against foreign adversaries, insider threats, and inadvertent disclosure of sensitive information. With the power of real-time data analytics and advanced search, military and intelligence organizations can respond to all potential threats.

The Elastic Stack (Elasticsearch, Kibana, Beats, and Logstash) enables users to handle security data with unprecedented speed and accuracy. Elastic products support incremental, scalable, and secure approaches to introducing advanced search and analytic capabilities into existing workflows. By indexing data upon ingest, Elastic immediately leverages all information for analysis — from structured (logs) and semi-structured (packet capture or PCAP) to unstructured (files) and geospatial data. Additionally, Elastic Endpoint Security combines prevention, detection, and response into a single autonomous agent to stop threats at the earliest stages of attack. Elastic accelerates the search process by making data available in near real time and enables multiple DOD operations, including the following:

- **Threat hunting:** Run *ad hoc* queries against any form of system data to uncover potential incursions or latent threats as they evolve.
- **Endpoint security:** Prevent, detect, and respond through a single agent, with always-on protection for off-network or offline devices.
- **Interoperability:** Integrate seamlessly with legacy systems across data silos with products that can be used independently or as an integrated suite.
- **Rapid data analysis:** Manage petabytes of data efficiently, providing results in seconds and allowing for proactive analysis and reporting.
- **Monitoring:** Evaluate data at scale and speed for mission analytics, performance metrics, application performance monitoring, and log management for tactical sensors and traditional IT sources.
- **Geospatial monitoring:** Monitor both geographically dispersed tactical systems and administrative infrastructures with robust cyber analytics, geospatial analysis, and centralized reporting for real-time situational awareness.

Elastic Users in the DOD



Elastic is approved for use on DOD networks and is already trusted and used by every branch of the US military. The DISA recently selected Elastic as the primary tool for collecting, transforming, aggregating, and delivering network data to JRSS users. The following branches of the US military are also using Elastic to protect their missions.

US Air Force

Elastic is an integral part of the United States Air Force Defensive Cyber Operations. The USAF uses Elastic Endpoint Security to prevent, detect, and hunt for advanced threats to protect critical infrastructure. With speed and automation capabilities that can be deployed rapidly and at scale, Elastic enables USAF cyber teams to better protect the nation's networks and data and maintain the information advantage.

The Hill Air Force Base Enterprise Data Center uses Elastic as a hosted logging service to meet compliance standards for real-time monitoring of more than 100 information systems operated by the Ogden Air Logistics Complex and located at bases nationwide.

US Navy

The Navy Fleet Cyber Command relies on Elastic to support their threat hunting activities, including the use of Elasticsearch for its Cyber Protection Teams. Elastic protects more than 500,000 computers, ships hulls, mechanical and electrical systems, weapons and navigation systems, aviation systems, and the technology controlling physical devices on bases and facilities. Additionally, the Naval Warfare Information Center Pacific uses Elastic for network logging and leverages security analytics in support of computer network defense.

US Army

Elastic technology is actively employed in advanced research environments to enable Army information security initiatives, including insider threat detection and defensive cyber operations. The Army Futures Command (formerly CERDEC) performs network and system monitoring as one of 23 cyber defense entities within the DOD. By leveraging real-time operational data through the application of new technologies and advanced analytics, CERDEC/ARL conducts defensive cyber operations and research against the most sophisticated cyber threats.

Army Human Resource Command is using the Elastic Stack to audit events and monitor items on open systems and network data. Elastic is providing log collection for 25,000 events per second to maintain 98.5% uptime on HRC servers, supporting rapid event audit, detection, and response.

National Guard

The National Guard Bureau provides cybersecurity expertise to state and local government authorities. Task Force Echo provides training, readiness, and oversight of Army National Guard Cyber Protection Battalions to ensure units are ready, resourced, and capable of conducting cyberspace operations in support of state and federal requirements. The certification training includes instruction on network-focused threat hunting, protocol and packet analysis, network sensor engineering, and security operations — all built on top of the Elastic Stack.

The Missouri National Guard Cybersecurity Team led the RockNSM and CAPES Stack projects to identify and respond to threats identified on network traffic. Built using the Elastic Stack, these projects allow users to securely search, analyze, and visualize data from any source and in any format in real time. RockNSM transforms cyber operations from a defensive, reactive posture to a proactive posture. The program has been so successful that it has been adopted by military and government agencies and commercial entities around the world. In 2018, RockNSM won the Public Sector Innovation Award as part of 1105 Media's Annual Government Innovation Awards recognizing outstanding innovation across government.

Elastic Can Support Your Defense Cybersecurity Mission

The Elastic Federal team stands ready to lend its valuable experience and resources to support its DOD partners. Contact us to learn how to advance your cybersecurity capabilities and visit www.elastic.co/federal.