

SPLUNK® FOR DEFENSE

Achieving security and efficiencies through data-driven intelligence

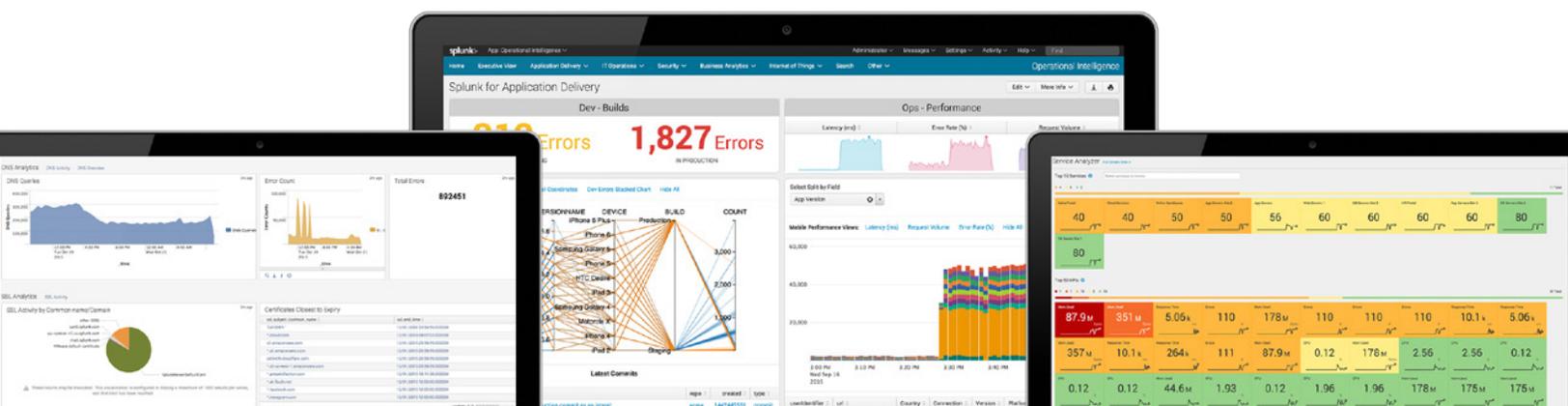
- **Generate Operational Intelligence** and value from machine-generated data
- **Defend against advanced exploits** and insider threats
- **Gain comprehensive visibility** into physical, virtual and cloud infrastructures
- **Deliver faster**, more cost-effective big data analytics
- **Monitor and analyze** Supervisory Control and Data Acquisition (SCADA) deployments in real time



Armed services agencies are faced with increasingly sophisticated digital threats that often go unseen by conventional security solutions. Agencies must harden and manage growing IT infrastructures to safeguard classified data and the systems that support operations, such as administrative processes and field missions. Agencies must also continuously monitor assets to ensure compliance while leveraging huge troves of data for intelligence.

Splunk software analyzes, visualizes and monitors data from any source—from remote surveillance and user logins to heating and cooling systems—enabling defense agencies to gain the awareness required to improve security, efficiencies and intelligence gathering. This data is a mission-critical resource and a military advantage, and hundreds of government agencies deploy Splunk software for data-driven analytics and holistic views of their operations.

Why Splunk for Defense? The Splunk platform can help consolidate tools, empowering agencies to streamline processes and retire legacy products. Defense agencies can also trim costs while gaining awareness of and intelligence into their infrastructures and assets.



Security

IT Operations

Big Data
AnalyticsControl SCADA
Infrastructure

Cloud

Splunk for Defense

Security

Prevent advanced exploits from compromising military installations and facilities. Gain the insights and agility to respond quickly to intrusions, breaches and other incidents. By correlating security data with other data sources—such as IT infrastructure data—agencies can protect mission-critical applications and uncover any exfiltration of classified information. Use real-time visibility into the activities of every employee and contractor, including the resources accessed, to identify potential insider threats. Support the Risk Management Framework and NIST standards, allowing for continuous monitoring, risk scoring and full reporting. Leverage machine data for forensic analyses and to track intrusions.

IT Operations

Gain end-to-end visibility across the entire IT infrastructure. Obtain operational awareness of applications and processes regardless of location, helping to preserve security, performance, availability and compliance. Dashboards enable users to monitor application performance, workflows and user experiences, regardless of their technical expertise. Capture multiple sources from physical and virtual layers and enable correlated searches to gain visibility into every layer, even in diverse and distributed cloud environments. Correlate data streams across IT and departmental silos to establish baselines and track SLAs.

Big Data Analytics

Simplify and accelerate big data analytics by quickly extracting intelligence from raw, unstructured data regardless of size or location, expediting decision-making and increasing agility. Explore, analyze and visualize data in Hadoop and NoSQL data stores without building fixed schemas, costly integrations or requiring migrations to separate in-memory stores. Role-based access controls ensure that only authorized personnel can access sensitive information.

Harden and Control SCADA Infrastructures

Strengthen the security of SCADA deployments, assess performance, improve efficiencies and support cost-saving green initiatives. Provide both high-level and granular views of the entire infrastructure, including oversight over and insight into environmental parameters, energy management, geospatial and surveillance data and any other distributed data streams. View data over time to discern trends and patterns in processes and operations, and quickly develop compliance reports.

Cloud

Splunk participates in the Federal Risk and Authorization Management Program (FedRAMP) to support government migrations to cloud solutions.

Thousands of public and private sector enterprises rely on Splunk products to improve security, increase efficiencies, make data-driven decisions and gain tactical and strategic advantages. [Learn more.](#)



Learn more: www.splunk.com/asksales

www.splunk.com