

Splunk For Law Enforcement

At Splunk we turn your criminal investigation data into law enforcement action. The sheer amount and breadth of data common to a modern investigation can be overwhelming, especially if the analysis of that data is across different tools or is a manual exercise. Splunk provides a centralized platform to correlate data, perform advanced analytics to various data sources and apply built-in AI to quickly identify unusual behaviors or anomalies. Investigations are collaborative in their efforts and everyone on the team plays an important role. Having a comprehensive view into the investigative data for all participants can reduce the time to come to conclusions from days or weeks to minutes. Splunk can support your intelligence-led policing strategy by helping you remove the barriers between data and action. We are here to support your agency in any of your efforts.

What is Splunk?

A data platform that powers security, observability and custom applications. Splunk is a data platform

that helps monitor, search, analyze and visualize large amounts of law enforcement data. Splunk has many law enforcement applications and it doesn't require complicated databases, connectors or controls. Splunk can also be used as a highly scalable and reliable cloud solution.

"I never thought that Splunk could be such a useful law enforcement tool. Splunk lets us query our data like a Google search. We connect the dots and see patterns and insights that were once hidden in all the statistics. We're improving our services and operating smarter and more cost-effectively. The bottom line is we're making our city safer and giving the public greater returns on its tax dollars."

— Chandler Police Department



Investigate



Analyze



Volume

Cyber Crimes

- Online Harassment
- Industrial Espionage
- Drug
- Malware
- D/DOS
- Botnets
- Phishing

Network Traffic, Audit, Authentication, Application, Logs, etc.

Dozens of Sources
10s GB to TB+

Personal

- Homicide
- Kidnapping
- Assault and Battery
- Arson
- Rape
- Domestic Abuse

Cel Tower Records, Call Records, Device Dumps, Network Traffic Logs, etc.

Hundreds of Sources
10s GB to TB+

Property

- Theft
- Burglary
- Larceny
- Robbery
- Auto Theft
- Shoplifting

Cel Tower Records, Call Records, Device Dumps, Network Traffic Logs, etc.

Hundreds of Sources
10s GB to TB+

Financial

- Money Laundering
- Embezzlement
- Tax Evasion
- Fraud
- Blackmail
- Crypto-currency

Network Traffic, Audit, Authentication, Application Logs, Cel Tower Records, Call Records, Device Dumps, Network Traffic Logs, etc.

Hundreds of Sources
10s GB to TB+

How Law Enforcement Agencies Use Splunk

Criminal investigations (WCC, OC, PC, fraud)

Investigators use Splunk to speed up investigations with disparate data sources from different companies and agencies.

Crime analysis (historical data)

Allocate resources with complete and timely analyses of data from all relevant sources — criminal records, incident reports, 911 calls, cell phones, and more to make sense of data to more effectively deploy assets and officers.

Ingesting search warrant returns (crim, cell towers, insider threat and social media)

Consolidate all served legal process documents, including .csv, .pdfs, emails, excel and word docs. Splunk provides a single pane of glass for viewing and analysis.

Mission analytics (drones, surveillance, Telephones, vehicle telematics)

Use data to drive mission decisions, resource allocation and post-operation analysis.

Fly away team

Take Splunk with you to gather evidence and location information from photos, videos and data. Monitor real-time communications data and do analytics on-site in real time.

Fusion center

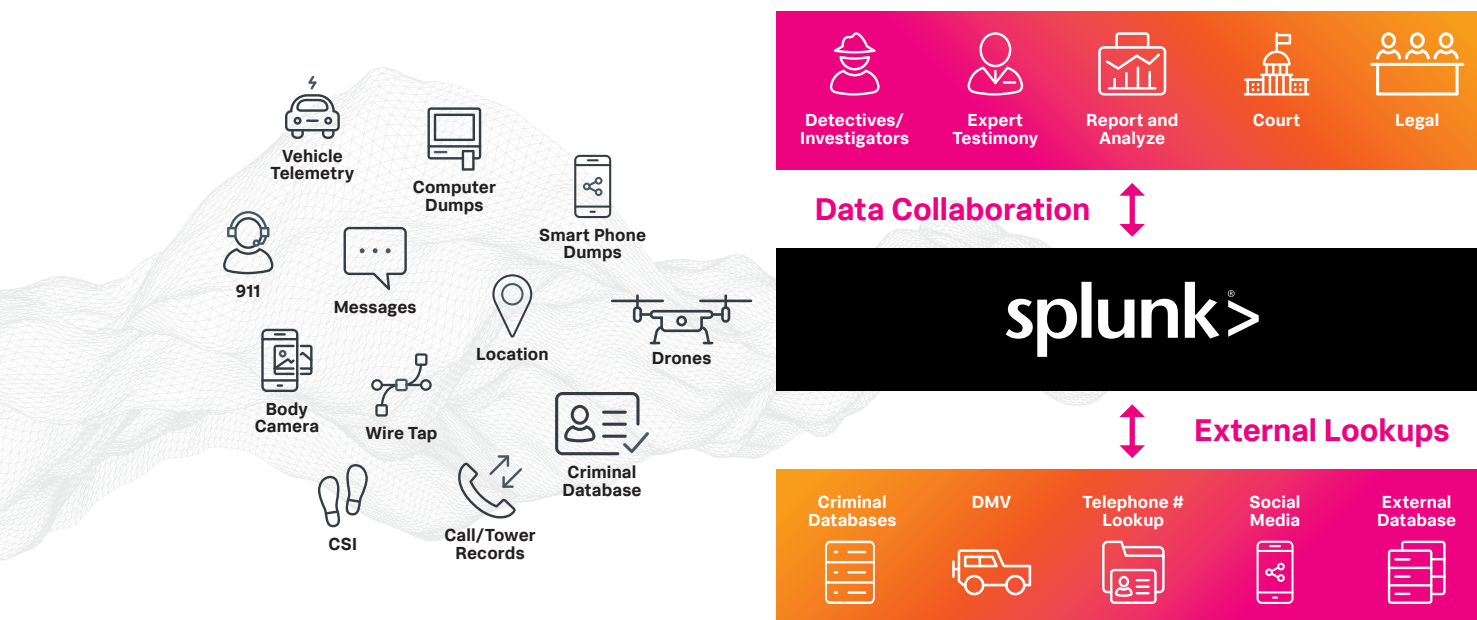
Fusion centers receive information from a variety of sources, including SAR from stakeholders within their jurisdictions, as well as the federal information and intelligence community.

Human Trafficking — Crimes Against Children

Splunk and The Global Emancipation Network (GEN) have developed a human trafficking investigation platform called Minerva that uses advanced data analytics to enable information-sharing, and collaboration across local and federal law enforcement, government agencies, non-profit and commercial organizations, and academic institutions.

Money laundering and Fraud

Splunk solutions can combat different types of fraud across banking, financial, healthcare and other industries.



Contact Splunk Group 1020 | Email Group1020@splunk.com | Chat Group1020 | Website www.splunk.com



Splunk Group 1020 is a group of law enforcement subject matter experts. Group 1020 takes its name from Police 10 codes, 10-20 which signifies location and data locations. Our motto is: Semper Invictus – Always for the better and greater.