

Chandler Police Department Proactively Manages Systems Vital to Public Safety



Executive summary

The police department for the city of Chandler, just outside Phoenix, has its own technology staff to improve delivery of police-related services and increase security for confidential records, data and processes. To ensure system availability and performance, the department required a solution to monitor its IT operations, including critical public safety application. Since deploying Splunk Enterprise, the police department has seen benefits including:

- Detailed visibility and intelligence into all law enforcement activities
- More effective resource allocation and faster officer response
- Stronger security for networked resources

Why Splunk

The Chandler Police Department (PD) maintains a network that links the main police station and two satellite facilities. It sought to track the performance of mission-critical applications such as a computer-aided dispatching system (CAD) that stores calls from citizens and a records management system (RMS) that is the repository for all activities, incidents and investigations of its 320 police officers. By indexing logs from these applications and visualizing the data in dashboards, Splunk Enterprise has enabled the department to track the health of its infrastructure, ensure the availability of its systems and proactively address potential problems.

In addition, Chandler PD learned that the Splunk platform could correlate its machine-generated logs with data from its RMS, providing such operational analytics as the frequency and nature of reported incidents and the performance of its officers. Chandler PD also uses the Splunk App for VMware to monitor virtual machines and its servers in the department's virtualized environment, allowing staff to maximize utilization and anticipate when a system will be overtaxed. Using the Splunk DB Connect application, which allows the indexing of structured data, Chandler PD has eliminated the costs of programming and is able to enrich data gleaned from machine-generated logs with statistics from the RMS database, allowing for deeper analytics and greater insights.

Industry

- Public sector (law enforcement)

Splunk Use Cases

- IT operations
- Security
- Business analytics

Challenges

- Need to monitor data from multiple web servers and systems
- Wanted to improve delivery of police-related services
- Critical need to increase security for data and processes
- Lacking full operational visibility into virtualized environment

Business Impact

- Monitoring critical applications without substantial IT resources
- More effective resource allocation and faster officer response
- Improved operational efficiencies and greater productivity
- Detailed visibility and intelligence into all law enforcement activities
- Better data protection and quality control
- Enhanced management of a virtualized environment
- Improved compliance with internal policies and officer oversight

Data Sources

- Log events from web, LDAP & application servers
- Log events & structured data from a records management system
- Log events from a computer-aided dispatching system

Splunk Products

- Splunk Enterprise
- Splunk DB Connect
- Splunk App for VMware

Fighting crime with operational analytics

According to the systems administrator (sysadmin) for Chandler PD—who is also a police officer—“Suddenly, we could perform operational analytics on our entire data trove and gain powerful, new insights and intelligence. The Splunk platform makes querying the RMS far more informative and user friendly.”

Chandler PD is using Splunk software for a variety of law enforcement and operational analytics. A Splunk dashboard tracks when incidents are reported and when officers arrive at the scene, enabling in-depth analysis of response rates and the frequency, timing and locations of crimes. Such insights allow the department to allocate officers and resources more efficiently. Dashboards monitor communications among officers to audit compliance with internal policies for appropriate behavior.

Splunk DB Connect uses lookup tables to access employees’ names and employee ID numbers, permitting staff to better identify one another as they access reports on the department’s intranet. This functionality is particularly useful as employees are offered personalized Splunk dashboards. Officers can easily review the number and kinds of arrest or crime reports they submitted over the past month, while sergeants can also monitor the overall performance of their teams.

Harnessing available resources to enforce the law

Chandler PD administrators are also using Splunk software to enhance the department’s security. They use audit trails to determine who accesses sensitive files or if unauthorized users try to enter the network. With such visibility, they verify that employees retrieve only the data for which they have approval. They even use Splunk software to monitor the department’s video surveillance systems

“Splunk Enterprise lets us query our data like a Google search. We connect the dots and see patterns once hidden in all the statistics. We’re improving services, operating smarter and giving the public greater returns on its tax dollars.”

Sysadmin / Police Officer

Chandler Police Department, Chandler, Ariz.

to ensure that cameras are always functioning and there is adequate disk space for the footage. “Thanks to Splunk software, we maximize system uptime by troubleshooting before trouble begins,” notes the sysadmin. “Proactive management is important for any IT department, but it’s essential for maintaining systems vital to public well-being.”

Going beyond operational visibility

For Chandler PD, the Splunk platform goes beyond simply offering visibility into its IT operations— it is a source of operational analytics, business intelligence, quality control, internal compliance and security. The department has gained in-depth intelligence into the timing, nature and location of all reported incidents and crimes, enabling officers to satisfy the needs of citizens faster and more effectively.

“I never thought that Splunk could be such a useful law enforcement tool,” concludes the sysadmin. “Splunk Enterprise lets us query our data like a Google search. We connect the dots and see patterns once hidden in all the statistics. We’re improving services, operating smarter and giving the public greater returns on its tax dollars.”

[Download Splunk for free](#) or get started with the [free cloud trial](#). Whether cloud, on-premises, or for large or small teams, Splunk has a deployment model that will fit your needs.



Learn more: www.splunk.com/asksales

www.splunk.com