splunk>

CASE STUDY

Splunk® at Chandler Police Department

Police Department Makes Law Enforcement More Efficient with Splunk

"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."

Police Officer
Chandler Police Department, Chandler, Arizona

OVERVIEW

INDUSTRY
- Local government (law enforcement)

SPLUNK USE CASES
- Operational intelligence
- Network management
- Security monitoring and compliance
- Geographical analytics
- Troubleshooting

BUSINESS IMPACT
- Operational efficiencies
- Greater productivity
- Comprehensive law enforcement analytics
- Improved data sharing and quality control
- Enhanced management of a virtualized environment
- Improved compliance with internal policies
- Better officer oversight
- Data protection
- Ensured availability of physical surveillance

The Business

Founded in 1912, the City of Chandler is a prosperous suburb of Phoenix, Arizona, that spans 70 square miles. Chandler evolved from a sleepy agricultural town to a bustling municipality rich in technology and industrial enterprises. Tasked with ensuring the city's tranquility, the Chandler Police Department, with 320 officers and 150 civilian employees, serves the city's 250,000 residents with "respect, fairness and compassion."

Challenges

Previously, the City of Chandler provided IT services to all of its agencies, including the police. A few years ago, however, the police department launched its own technology staff to improve delivery of police-related services and increase security for confidential records, data and processes.

The police department (PD) staff maintains a network that links the main police station and two satellite facilities. To ensure system availability and performance, the department needed to monitor machine-generated logs from its LDAP (Lightweight Directory Access Protocol) and web servers, and especially its comprehensive records management system (RMS), Versadex. This RMS captures all police processes, investigations and records. It also stores calls from citizens and police dispatches from the department's computer-aided dispatching system (CAD).

"Chandler's public safety depends on our RMS and CAD solutions," says a Chandler police officer, who also handles some of the department's IT tasks. "Poor performance or failure are intolerable, and we needed a management tool to optimize their functionality."

Enter Splunk

With its ability to gather, index and graphically display machine-generated data in dashboards, Splunk proved an effective solution for the Chandler police department. The Splunk platform is now used to collect logs from the RMS, CAD and servers, allowing administrators to routinely track the health of their system infrastructure. Chandler PD also uses the Splunk App for VMware to monitor virtual machines and their servers in the department's virtualized environment, allowing staff to maximize utilization and anticipate when a system will be overtaxed.

"Splunk lets us know of a problem prior to someone alerting us to it," says the sysadmin for the Chandler Police Department. "Proactive management is important for any IT department, but it's essential for maintaining systems vital to public safety." As with many Splunk customers, the Chandler Police Department quickly realized that the solution's functionality extended beyond improved network management. The department's RMS system offers a wealth of information, but extracting and presenting data from the solution was complex and its functionalities were limited.

According to the police officer who also performs IT duties: "We found that Splunk can display statistical data from our RMS system. Our first use case was querying the software to identify the kinds of reports officers submitted in a given timeframe. Suddenly, we could perform operational analytics on our entire data trove. With that, Splunk became an indispensable tool for oversight and quality control."

Splunk also paid dividends in accelerating the department's access to structured data in the RMS database. Previously, administrators needed to write APIs, a laborious process. Then they discovered the Splunk DB Connect application, which allows Splunk to index structured data. This solution eliminated the costs of programming

OVERVIEW (CONT.)

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

PRODUCT

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

"We created audit trails for our servers to determine who accesses sensitive files or materials or if an unauthorized user tries to enter our network, Splunk gives us visibility into how our systems are used, enabling us to verify that employees retrieve only the data for which they have approval. We even use Splunk software to monitor the video surveillance systems in our three facilities to ensure that cameras are always functioning and there's adequate disk space for the digital footage."

Sysadmin
Chandler Police Department, Chandler, Arizona

Free Download

Download Splunk for free. You'll get a Splunk Enterprise 6 license for 60 days and you can index up to 500 megabytes of data per day. After 60 days, or anytime before then, you can convert to a perpetual Free license or purchase an Enterprise license by contacting sales@splunk.com.

and enriched data gleaned from machine-generated logs with statistics from the RMS's database, allowing for deeper analytics and greater insights.

Chandler PD now uses Splunk for a variety of operational analytics. Splunk presents the times when a citizen reports an incident and when officers arrive at the scene, and then calculates response rates across the city. A Splunk dashboard tracks the dates when an incident report was filed and when the incident actually occurred for analysis of the frequency and timing of crimes. Additionally, rather than manually parse email to determine if the National Crime Information Center (NCIC) responded correctly to a query such as a request for an arrest record, Chandler PD staff use Splunk to analyze these communications and graphically present the findings in a dashboard.

Splunk DB Connect makes querying the RMS more informative and user friendly. It 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 in the past month and sergeants can monitor the performance of their teams.

The department deploys Splunk dashboards to audit compliance with internal policies. The RMS captures messaging from the CAD system and feeds the data to Splunk, which reports inappropriate language between officers as they communicate in their patrol vehicles. "Before, if we wanted to look at a specific team, we'd have to print all the messages and then manually highlight improper words or phrases," explains the police officer source. "Splunk not only automates this process—saving a lot of time—a dashboard even alerts us when there's a problem."

To take its analytics to another level, figuratively and literally, the Chandler Police Department is implementing Google Maps for Splunk, an application that overlays data on maps in dashboards. Employees will be able to geo-locate incident reports on maps of the city to determine, for example, where burglaries are most likely to happen and to analyze response times to emergency calls in various neighborhoods.

Breakthroughs

Like many enterprises, the Chandler Police Department initially deployed Splunk to better manage its networked resources. "By troubleshooting before trouble begins, we maximize our system's uptime," notes the sysadmin. "With Splunk's comprehensive visibility, we're administering our infrastructure more productively and efficiently. Whenever a question arises, we turn to Splunk."

Thanks to views of both structured and unstructured data, the platform quickly became an invaluable source of operational analytics, business intelligence, quality control, internal compliance and security. The department relies on the solution for insights into crime patterns and how its officers respond to citizens' needs. It derives actionable intelligence by analyzing events by time and location, and has streamlined how employees report and share information. "Our officers greatly appreciate having data available to them so easily and cleanly," says the police officer. "Splunk vastly improves our processes, giving officers more time and information to do their jobs."

Moreover, Splunk enables the department to effectively audit employees' adherence to procedures and policies. Administrators are also mindful that Splunk can further enhance the department's security posture. For example, they are considering using Splunk to verify compliance with the Criminal Justice Information System (CJIS), a central repository of law enforcement records.

"I never thought that Splunk could be such a useful law enforcement tool," concludes the police officer. "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."

Item#CS-Splunk-ChandlerPolice-104