splunk>

CASE STUDY

Nevada Department of Transportation Bolsters Security and Operational Efficiencies

Executive summary

The Nevada Department of Transportation (NDOT), a division of Nevada's state government, aims to enhance public safety and commerce by planning, constructing, operating and maintaining the state's highways. NDOT oversees Nevada's 511 system, which enables citizens to determine road conditions and delays, as well as a statewide video camera network that allows motorists to view traffic levels prior to travelling. The department was looking for better reporting from its Internet content filtering solution to document web activity. Since deploying Splunk Enterprise, the department has seen benefits including:

- Optimized security posture
- Cost savings and improved operational efficiencies
- More efficient resource management

Why Splunk

NDOT's information security officer (ISO) was concerned about hacking attempts targeting NDOT as an agency responsible for transportation infrastructure. Unfortunately, NDOT's manual processes for system log reviews were tedious, unreliable and often too late to mitigate time-critical issues. To gain visibility into network traffic, the ISO needed to systematically collect the logs from various hosts as well as those from web servers.

Once NDOT began sending log event data from across its infrastructure into Splunk Enterprise, it immediately gained operational visibility into security and IT operations issues that had previously taken numerous man-hours to resolve. According to the ISO, "Splunk software automates the laborious process of sifting through logs and other machine-generated data, which saves time and trouble identifying the source of problems. Splunk gives us both holistic and granular views of our IT environment, enabling us to do root-cause analyses very quickly."

Industry

- Public sector
- Transportation

Splunk Use Cases

- Security
- IT operations
- Application delivery

Challenges

- Need to identify security vulnerabilities and document attempted hacks into network
- Cumbersome manual processes for system log reviews
- Required insight into network traffic across wide range of systems
- Lacked operational visibility into infrastructure

Business Impact

- Optimized security posture
- Cost savings and improved operational efficiencies due to identifying misconfigurations
- Rapid issue resolution and immediate operational visibility
- Improved public safety
- More efficient resource management
- Enhanced productivity

Data Sources

- Log events from traffic control systems
- Log events from servers, switches, routers and firewalls
- Log events from FTP servers
- Logs from network printers
- MS Active Directory logs

Splunk Products

- Splunk Enterprise

Providing better insights into challenges across the infrastructure

Upon deploying Splunk Enterprise, NDOT's security team determined that a variety of networked devices were misconfigured, which potentially compromised security and performance. For example, on the morning a firewall was installed at a remote location, NDOT discovered via the Splunk platform that someone overseas was attempting to use the device to access the network. Thanks to Splunk, the firewall was correctly reconfigured the same day, plugging what could have been a costly security hole. This helped to bolster the agency's defenses and enabled the ISO to verify the many attempts by hackers to penetrate NDOT's network.

The Splunk platform quickly proved to be a valuable solution for gaining insight into challenges across the agency's infrastructure—not just limited to security. For example, when some video feeds from NDOT's traffic video network weren't appearing, engineers initially attributed the problem to recently installed antivirus software. Data collected by Splunk Enterprise revealed that the video was indeed flowing, but the problem was with the browser used to display the footage.

When the ISO used Splunk Enterprise to find that some malicious files sent via FTP were being written to a set of non-public folders, she used the software to uncover a faulty script. Upon fixing the problem, she then used the Splunk platform to identify contractors and engineers who no longer use the FTP server and, for another safeguard, closed their accounts.

Improvements in operational efficiencies

For an additional benefit, NDOT has deployed Splunk Enterprise to improve operational efficiencies. In one case, a large color printer and copier had become costly to own because of its consumption of color inks. When discussions arose about replacing the device with an inkjet printer for each employee in the office, staff collected printing logs with Splunk software, and found that the printer's default setting was color rather than black and white, causing excess use of color cartridges. Resetting the printer was more cost-effective than replacing it with multiple inkjet printers, a discovery that saved the department thousands of dollars.

"Whenever there's a problem, we immediately go to Splunk for optics and intelligence. Splunk has empowered us to plug security gaps, improve efficiencies and save taxpayer money. We're limited only by our imaginations as to all the ways we can leverage the platform."

Information Security Officer
Nevada Department of Transportation

More intelligence for enhanced public safety

NDOT plans to enhance public safety by funneling logs from the state's 511 system into Splunk Enterprise to ensure information is always accurate and up-to-date. The staff will use the software to monitor the department's help desk system, Oracle databases and additional Active Directory logs. Moreover, NDOT will determine the impacts of change policies and view the operation of devices over time to learn if any are approaching thresholds that may compromise their performance.

"As we increasingly rely on Splunk, we're traveling from being reactive to proactive," concludes NDOT's ISO. "We're gaining the intelligence to know when a device or application will be overtaxed so we can take measures before problems arise, or when we can consolidate systems to stretch our budgets. Although Splunk has already demonstrated that it can help our agency improve public safety and operate more productively, efficiently and securely, we are just beginning to extract its full value."