splunk>

CASE STUDY

University of Texas at Austin Ensures Network Security For Distributed Campus

THE UNIVERSITY OF TEXAS

Executive summary

The University of Texas at Austin is a top-ranked state research university and the flagship of the University of Texas System. Like many colleges and universities, UT Austin depends heavily on its wired and wireless networks to enhance the educational experience and quality of life for students, faculty and staff. The university needed to grow its security posture with a flexible solution that could address the needs of its distributed environment. Since deploying Splunk Enterprise, the university has seen benefits including:

- Faster insight into events and anomalies
- Reduced organizational risk and incident investigation time
- Improved security posture

Why Splunk

UT Austin's 350-acre campus includes nearly 200 buildings linked by a 10-gigabit fiber optic backbone. Up to 120,000 individual devices may be connected to the network at any time, including servers, wireless access points, desktops, mobile devices and other systems. UT Austin's Information Security Office (ISO) and Information Technology Services (ITS) are responsible for ensuring network security.

Before deploying the Splunk solution, the ISO analysts relied primarily on intrusion detection/prevention system (IDS/IPS) appliances and custom developed software to monitor network activity. "We wanted to plug into the many different servers and devices downstream that were coming under attack to correlate our network information with actual system log data," says Cam Beasley, UT Austin's chief information security officer. "We didn't want a big heavy SIEM product because we hadn't had much luck with them in the past. We needed a more flexible system that we could adapt to our unique needs."

The ISO team saw that Splunk represented an important analytical tool that met most of the needs of network and information security analysts by helping them investigate security threats and incidents faster and more accurately across the distributed UT Austin network. More important, Splunk Enterprise enabled ISO to move to a more

Industry

- Higher education

Splunk Use Cases

- Security

Challenges

- Highly distributed environment
- Need for unified solution to monitor network activity
- Unique needs required solution more flexible than traditional SIEM
- Need for rapid security threat investigation and mitigation
- Security team reactive instead of proactive

Business Impact

- Saves hundreds of hours per year in security analyst time by automating workflows and providing faster insight into events and anomalies
- Reduces organizational risk by preventing costly network breaches and negative publicity
- Reduces incident investigation time by providing fast access and analysis of log data from any source
- Improves security posture by filtering out false positives and providing data visualization
- Avoids loss of intellectual property
- Ensures uptime and service continuity by catching unknown threats and new zero-day attacks

Data Sources

- Network flow
- Departmental servers
- System logs: Linux/UNIX, Windows, OS X, Solaris
- Security data: IDS/IPS, firewalls, access controls

Splunk Products

- Splunk Enterprise

proactive posture by helping identify unknown threats and network anomalies and allowing it to alert departments and schools faster.

Effective security for a distributed campus

The solution allowed UT Austin to distribute Splunk forwarders to many units to access log data where it was not able to before. In the main datacenter, where all departments are represented, UT Austin has an extensive distributed search infrastructure based on Splunk, including numerous forwarders, indexes and search engines. This has helped the ISO team provide effective network security for a highly distributed campus.

ISO also uses apps from the Splunk ecosystem to enhance its Splunk deployment. For instance, one app helps identify anomalies based on geographical location. A user can login at one location at a certain time and then login again moments later at a different location. In the case of geographically impossible logins, ISO is alerted and can shut down a suspicious logon that may indicate a compromised user account.

Faster, more accurate threat identification and containment

Splunk Enterprise has helped automate the identification and response to malware threats, helping to control outbreaks and reduce or eliminate escalations. Searches that used to take 10 minutes can now be done in seconds. Splunk software also helps ISO identify and create signatures for new threats and deploy those signatures much faster. The team can identify and control suspicious events before they escalate into outages or breaches.

For example, when the so-called Flashback Trojan began infecting Apple's OS X operating system, the ISO team used its own custom Splunk application for event correlation and anomaly detection in combating Flashback. "Splunk helped us do a lot of the initial detection and identification of anomalies," Beasley says. "We used our Splunk solution to trigger on certain types of events and alert us. By reducing our response time, we were able to contain the event."

"We use Splunk software daily and it's critical to our operations. It makes us better equipped to detect new anomalies and respond to them quickly. Without it, we would be far less effective—I'm sure of that."

Cam Beasley, CISO, Information Security Office
University of Texas, Austin

"Searches that used to take ten minutes can now be done in seconds with Splunk. When an analyst has to do that several times per day, the savings add up. More importantly, Splunk software helps us identify and create signatures for new threats and deploy those signatures much faster."

Cam Beasley, CISO, Information Security Office
University of Texas, Austin

Campus-wide growth for full visibility

The ISO team has helped evangelize the use of Splunk software and provides assistance to other departments or groups. Dozens of instances of Splunk Enterprise are currently in use across the university.

"Splunk provides a simple visual view into our data that enables us to see emerging patterns, compare results, isolate commonalities and take action that prevents escalations and outages," Beasley says. "We use Splunk software daily and it's critical to our operations. It makes us better equipped to detect new anomalies and respond to them quickly. Without it, we would be far less effective—I'm sure of that."