ManageEngine
Log360

CASE STUDY

Sundt Construction Automates Log Management with Log360

About the Organization

Sundt Construction was founded in the year 1890 by Mauritz Martinsen Sundt, a Norwegian ship carpenter who immigrated to the US as a teenager. In the last 130 years, the company has had a storied history and has been involved in some major projects, including the construction of the University of Arizona in 1936 and the revamp of the Austin–Bergstrom International Airport in 1999.

Sundt has completed work in nearly all 50 states of the US. Today, it maintains a core presence in the southwest and western United States, with 11 offices across four states, an extensive network of craft professionals, and active projects throughout the country.

> *You can either hire a lot of staff numbers or you can just buy this product. Without this tool we'd have had at least 4 or 5 of us sitting here doing the job.*

Lance Malone,
Senior information security analyst.

The IT Challenge

Lance Malone is a senior information security analyst at Sundt Construction, based out of the office in Phoenix, Arizona. The cybersecurity team at this office is comprised of three people including Malone.

There were two main challenges for Malone's team:

Manual sifting of logs: Malone had to sift through all the network logs manually, and import them into Excel before zeroing-in on the root cause of any cybersecurity incident.

Lack of manpower: Since there are only three people on this particular team, it was extremely difficult to dedicate a third of the workforce to looking at logs all day.

The Solution

After deploying Log360, the cybersecurity team at Sundt's Phoenix office was able to:

- **Tackle unique reporting requirements:** Apart from out-of-the-box reports, Log360 provided Sundt the ability to create its own reports. This way, the company always knows about any incident that happens. When incidents take place, Malone immediately receives an automated email.

- **Analyze the root cause:** With the use of the ElasticSearch feature, Malone's team can easily zero-in and drill down on any issue. This feature gives them the ability to drill down based on event ID, machine name, IP address, and so on. This way, the team can find out where the trouble originated and take the necessary steps for remediation.

- **Take immediate action:** Log360 enables the IT security team to set threshold rules and conditions on all events that occur in their network, including critical security events. Malone can customize Log360 to receive instant alerts or even execute batch files in the occurrence of a breach.

The other thing Malone touches on is ManageEngine's support and customer service. He said, "[ManageEngine's] support and customer service is just absolutely phenomenal to use. [They're] great to talk with. I honestly have no complaints there at all."

Business Impact

Sundt values the return on investment from Log360. It has also improved the company's productivity substantially. If not for the solution, a third of Sundt's IT workforce would be assigned to analyzing security incidents.

Another major business impact is the extent of monitoring of the heterogeneous network. Malone said, "I can see all the devices, their activities, [and] their IPs."