SFBLI Boosts Efficiency and Strengthens Security Posture with Splunk Attack Analyzer

Key Challenges

Southern Farm Bureau Life Insurance Company's (SFBLI) solution for analyzing incoming submissions from its external facing web application slowed down sales and created alert fatigue that could jeopardize the company.

Key Results

With Splunk Attack Analyzer, SFBLI speeds up business operations and strengthens its overall security posture — lowering the risk of compromise and better protecting its customers' sensitive data.

FARM BUREAU INSURANCE SOUTHERN FARM BUREAU LIFE INSURANCE COMPANY

Industry: Financial Services

Solutions: Security

Products: Splunk SOAR, Splunk Attack Analyzer

From supporting families through life's biggest challenges to protecting against stolen data.

Southern Farm Bureau Life Insurance Company (SFBLI) provides peace of mind to everyday people like farmers, police officers, teachers and their families across 11 U.S. states. When the unexpected happens, SFBLI steps in with a commitment to service, respect, integrity and accountability. With these core values in mind, the company must protect its customers' sensitive data, as well as the company's intellectual property. What's at stake? SFBLI could fall victim to a malware attack that shuts down its operations indefinitely. Customers could have their medical records, banking information and social security numbers in the hands of cybercriminals.

A particular vulnerability is its external-facing web application, where agents and customers upload sensitive documentation and insurance policies for the policy and e-service departments to fulfill. This portal poses a significant risk: Because SFBLI agents are third parties, bad actors could use it to target the company if one gets compromised.

Outcomes

70%
decrease in file scan time

Reduced
false positives from 26% to near zero in 6 months

~5 mins
for analysis, orchestration and response combined, down from ~20 mins for just analysis

To protect against devastating malware attacks and stolen data, the small cybersecurity team at its Jackson, Mississippi branch relied on sandbox solutions to analyze uploaded files for malicious content. However, they experienced an overwhelming amount of false positives, creating alert fatigue that could ultimately compromise the company. On top of that, each scan took roughly 20 minutes to complete, slowing down sales and impacting daily business operations. SFBLI needed a faster, more accurate solution that provided the same peace of mind the company gives its customers.

SOARing to efficiency with automated scans and detailed alerts

SFBLI's journey with Splunk began a few years prior when Cyber Security Architect Kyle Notvest needed a way to automate his team's day-to-day processes and boost efficiency. His research ultimately led him to Splunk SOAR, and he couldn't have been more pleased with the results. One of the first things he did with Splunk SOAR was automate the server scan process, bringing it down from 30-40 minutes — to mere seconds, giving back valuable time to his small, yet mighty team. SFBLI now also uses Splunk SOAR for multiple use cases, such as taking in and enriching alerts from various tools: "It's doing the initial investigation and putting those results into tickets, enriching them with the data we need to investigate the alerts," says Notvest. Dedicated to protecting the company and its customers' sensitive data, the security team now works with fewer distractions, improving the company's overall security posture.

> Faster isn't always better, but when it comes to finding malicious things and getting the files needed to underwrite and service insureds to the company quicker, faster is better. Splunk Attack Analyzer has increased our speed and efficiency."
>
> **Chris Powell,** Director, Cyber Defense and Security Operations, Southern Farm Bureau Life Insurance Company

Solving a critical business dilemma with security, reliability and efficiency

Notvest was in the audience at .conf for the unveiling of Splunk Attack Analyzer. He knew instantly that it was the solution he needed to protect SFBLI's vulnerable external-facing web application. "It was a night and day difference between what our current sandboxes were doing and what Splunk Attack Analyzer was doing for us," says Notvest.

With Splunk Attack Analyzer, Notvest saw a 70% decrease in scan time. "A big problem we faced with our sandbox solution was that it took so long, it caused our playbook to time out," he says. When that happened, someone on the security team would have to review, approve and re-upload the file manually. And if they missed an alert that the follow-up scan failed, that would further delay the delivery of critical documents to the business departments, slowing business operations significantly.

Splunk Attack Analyzer also lowered the false positive rate to near zero. "There was a time when 27% of file uploads were marked as malicious or suspicious," says Notvest. "All of them ended up being legitimate and clean. With Attack Analyzer, we had near zero false positives in 6 months. This was a huge win for my team. The overload from all the noise risked us missing what could be a legitimate threat because we were too busy investigating something that was not," he adds. Eliminating unnecessary distractions and alert fatigue enables Notvest's team of seven to operate like a true SOC for the first time: More productive and efficient overall with added confidence in protecting its customers' sensitive data.

Onboarding new security team members has never been easier: "The consistency of analysis up-levels new members of our team and assures me that what they're doing is accurate," says Notvest. "I have confidence in them and the company's security because we have Splunk Attack Analyzer."

Fine-tuning a well-oiled machine

Instead of manually investigating dozens of suspicious emails, files and URLs daily, the SFBLI cybersecurity team now uses Splunk Attack Analyzer as a faster and more accurate means to perform these critical investigations. And the results are a welcomed change: Prior to Attack Analyzer, the team spent up to 20 minutes on analysis alone. Now, analysis, orchestration and response happen in less than five. "Before Attack Analyzer, it was hard for us to investigate every single one of these alerts," says Notvest. "Now, I'm confident that we're not missing alerts, not getting alert fatigue or just plain overloaded." Currently, Notvest is actively working on automating the process for uploading flagged content into the Attack Analyzer UI. "The end goal is to have SOAR flag artifacts as potentially malicious and automatically feed them into Attack Analyzer for further investigation."

splunk>

Learn more: www.splunk.com/asksales

www.splunk.com