# First Financial Bank Unifies Threat Data and Streamlines Response

First Financial Bank (NASDAQ:FFIN), headquartered in Abilene, TX, is one of the nation's most financially secure banking institutions, ranked number 1, 2, or 3 by Bank Director Magazine for the past seven years. With 69 locations throughout Texas and more than $7.5 billion in total assets, First Financial offers the best of "Big Bank" customer and technological benefits without sacrificing the local, personal touch of community banking.

Securing strong customer relationships is a top priority for First Financial Bank. Maintaining a culture of innovation and staying at the forefront of cutting-edge technology is critical to achieving that goal. As cybercriminals find new and more sophisticated ways to breach financial institutions, First Financial is committed to meeting today's risks head-on and adapting to the evolving threat landscape.

## The Challenge

### Fragmented and Manual Threat Detection

When Michael Cole took on his new role as Chief Information Security Officer at First Financial, he inherited more than 15 different security tools. These siloed systems provided a limited and fragmented view into First Financial's threat environment. The team didn't have the visibility they needed to understand what security incidents were occurring, what to prioritize, or how to respond appropriately. Cole knew that this lack of visibility was dangerous and could potentially lead to a breach, jeopardizing the customer relationships First Financial had worked so hard to build over the past 126 years.

Taking a step back, Cole and his team evaluated their current security suite and eliminated tools that were unsuitable for their IT environment. During this process, they also tried to optimize their current SIEM vendor, Splunk. It soon became clear, however, that while Splunk contained valuable threat intelligence, accessing and benefiting from that intelligence buried within the Splunk system proved difficult.

According to Security Analyst John Lovell, "Splunk has the answers, but in order to access those answers, we had to ask the right questions. We didn't have the time or people who were trained to do that." That's when First Financial turned to LogRhythm.

**Organization**
First Financial Bank

**Industry**
Banking and financial services

**Employees**
1,400 nationwide

**Key Impacts**

- $50,000 in yearly cost savings over Splunk
- Full 24x7 visibility from a single pane of glass
- Automated detection and analysis of advanced threats in real time
- Customizable dashboards enabling streamlined response workflows and processes

> "From the first day, LogRhythm gave us useful information. That was something Splunk could not do."
>
> –Michael Cole, Chief Information Security Officer, First Financial Bank

## The Solution

### Centralized Platform Provides Immediate Value

After implementing LogRhythm, First Financial had visibility into their entire ecosystem from a single pane of glass. "From the first day, LogRhythm gave us useful information. That was something Splunk could not do," said Cole. LogRhythm's ease of use benefited the team from both an operational and a security perspective.

For example, soon after implementation, LogRhythm surfaced and sent alerts about an operational issue where two branch router cooling fans were about to fail. The team quickly fixed the problem before an outage could occur and put necessary measures in place to avoid future outages.

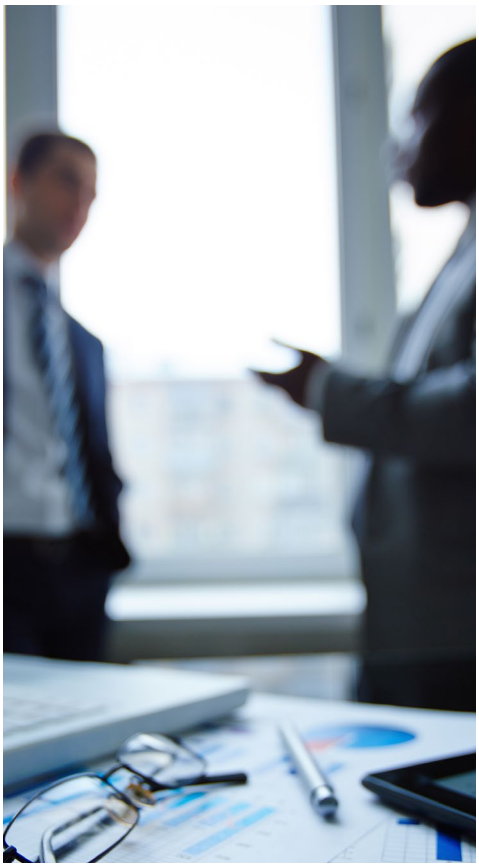
From a security point of view, LogRhythm also empowered First Financial to identify and neutralize a brute-force attack on a privileged user account. Through LogRhythm's alerts and powerful investigative capabilities, Lovell discovered that an executive was continuously getting locked out of his Microsoft Office 365 account and the cause was an attacker originating from China. Lovell said, "Once our investigation determined the root cause, we were able to take steps to fully respond to and remediate the incident."

### Pre-built and Customizable Features Streamline Processes

Not only does LogRhythm provide First Financial with much-needed visibility and investigative capabilities, but, according to Lovell, it also equips the team to organize and process that information faster and more effectively than ever before. "I can just glance at the LogRhythm console, see what's going on, and dive deeper if necessary. It frees up a lot of my time."

Pre-built and customizable features, including an AI Engine, rules, alarms, and dashboards, help First Financial analysts organize and funnel the relevant data to the appropriate teams. "With LogRhythm, people are only seeing what they need to see to complete their job," said Lovell. "They're not inundated with a slew of information irrelevant to them."

Comprehensive visibility, streamlined workflows, and faster response times are the key reasons why Cole highly recommends LogRhythm to security teams like his. The incredible cost savings was icing on the cake. "Switching from Splunk to LogRhythm saved us $50,000 in costs per year—and that number is coming directly from our CFO."



> "Switching from Splunk to LogRhythm saved us $50,000 in costs per year—and that number is coming directly from our CFO."
>
> –Michael Cole, Chief Information Security Officer, First Financial Bank