

CASE STUDY

LendingTree Cuts Alert Noise by 90%, Transforms Visibility

LendingTree is a financial services marketplace. Founded in 1996, they began in the mortgage space before branching out into student loans, small business loans, and the insurance business. Their goal is to provide an easy-to-navigate platform that allows consumers to make the best decisions possible for their financial health.

According to John Turner, Senior Security Architect for LendingTree, the organization places a high value on developing secure products and services for consumers—not to mention innovating as quickly as possible to stay ahead of the competition.

Currently, Turner focuses on all areas of information security, specifically on the application security side. “I oversee developer training, solutions architecture, new product development, and anywhere else where we need to have security embedded as far left as possible in the development process,” he notes.

The shift-left mentality is essential at LendingTree. As Turner says, “Security isn’t an afterthought or something we bolt on. It’s something we build in from the very beginning, whether it’s infrastructure, code, people processes, or data security.”

Turner considers security the most creative area of technology, inspiring out-of-the-box thinking. “Security has always excited me,” Turner shares. “It’s almost an art form. It’s open to interpretation and creativity, and every solution is unique.”

Turner applies this creativity to securing LendingTree’s diverse cloud infrastructure. “We’re essentially a cloud-native company, spanning all three major cloud providers,” he explains. However, as LendingTree has grown through acquisitions, they’ve brought up a number of legacy systems from the more traditional client-server data center environment, which they’ve migrated to the cloud.

Given this complexity, the security team at LendingTree has grown accustomed to working with numerous tools across their multi-cloud environment. “We are always pushing the envelope,” states Turner. “Innovation is key at LendingTree.”

This data problem also limited LendingTree’s ability to expand within the cloud. “Without the necessary visibility, there was no way that we could demonstrate that this was going to be a safe transition,” Turner says.

The team also struggled with gaining visibility into their server lists and containerized workloads. “Moving into a containerized environment, there weren’t a lot of tools out there that would let us assess the security posture of a container or host, or to see the communication between containers on hosts,” Turner notes. “If I can’t see into the inner workings, then there’s a huge blind spot that makes it hard to quantify what’s happening across our environments.”

Then, there was the issue of compliance. Staying on top of regulations is pivotal in finance, especially with a constant stream of new requirements from state and federal regulators, in addition to those of LendingTree’s partner institutions. “Compliance for us is not negotiable,” Turner notes. “It will keep us in business or put us out of business.”



“Everyone, even non-security teams, saw how Lacework FortiCNAPP could enable us to reach the next level of visibility, compliance, vulnerability management, and threat detection.”

John Turner
Senior Security Architect,
LendingTree

Details

Customer: LendingTree

Industry: Financial Services

Location: Charlotte, North Carolina

Business Impact

- Saved \$200k a year by decommissioning existing tools
- Cut alert volume by 90% with context-rich alerts
- Reduced alert investigation time from 10 hours a day to 5 minutes per alert
- Easily generated SOC 2 compliance reports to pass audits and lower insurance premiums

In an effort to tackle their data, visibility, and compliance goals all at once, LendingTree began its search for a cloud-native application protection platform (CNAPP) that could do it all.

Challenges

“Cloud security is critical for LendingTree,” says Turner. “It enables our business to scale in any direction very quickly.”

But for all the benefits, it comes with its share of challenges. “Planning for cloud security is a very big task,” Turner notes. “The security threat landscape is constantly evolving, and we have no idea what’s going to come down the road. We have to constantly reevaluate, reassess, and ensure that we’re positioned properly.”

Turner says that prior to implementing Lacework FortiCNAPP, “Our challenge from a security and infrastructure perspective was making sure that we leveraged all of the possibilities that the cloud offers while maintaining operational stability and security.”

Staying secure can be a daunting task. “We implemented many products as we expanded our cloud environments, but nothing could give us the assurance that we were growing securely,” recalls Turner. “It was like drinking from a firehose. We had so many alerts and so much data coming in from so many different places that it was impossible to manage.”

The volume of data was so high, in fact, that filtering through it quickly became unsustainable. “We were dealing with 200 alerts a day, and our frontline security operations center (SOC) staff was spending 10 hours a day to triage these alerts,”

Turner remembers. “Out of that, we might have three or four actionable alerts that were escalated to our engineering teams for remediation. That overhead alone was a significant driver for us to find a new solution.”

Solutions

As it turns out, Lacework FortiCNAPP was just the solution LendingTree needed.

From a deployment standpoint, the Lacework FortiCNAPP data platform demonstrated the wide range of security capabilities that LendingTree was looking to add. Turner’s team saw firsthand how it could solve the alert noise challenge. “Lacework FortiCNAPP helped us deal with the massive amount of information that we were getting out of all the different systems, from the native security tools and logging and alerting tools that came from cloud providers to third-party tools that we had purchased to help solve these problems,” Turner states.

Moreover, the LendingTree team learned how the patented anomaly detection component of Lacework FortiCNAPP could increase their visibility. By ingesting massive amounts of data, it builds a baseline of each user’s cloud environment and alerts on unusual behavior, including unknown threats. “The technology was mind-blowing for me,” Turner recalls. “That’s the type of visibility we needed. I knew as soon as I saw it that it was going to be transformative for us.”

The platform was so simple to use that it gained widespread popularity across the organization. “After one demo, different teams were coming to us, saying, ‘We need this,’” remembers Turner. “Everyone, even non-security teams, saw how Lacework FortiCNAPP could enable us to reach the next level of visibility, compliance, vulnerability management, and threat detection.”

Choosing a security product can be especially difficult since it involves so many areas of the business. But with a powerful CNAPP like Lacework FortiCNAPP, the choice was easy for LendingTree. “I’ve been in the industry for many years,” says Turner. “When we sat down with our infrastructure and DevOps teams to review Lacework FortiCNAPP, that was the only time I’ve ever seen all the teams agree on a solution.”

Solutions

- FortiCNAPP

“The technology was mind-blowing for me, that’s the type of visibility we needed. I knew as soon as I saw it that it was going to be transformative for us.”

John Turner
Senior Security Architect,
LendingTree