voices

**CrowdStrike** Customer Case Study

# Search for Next-Gen Log Management Solution Ends with CrowdStrike Falcon LogScale

For 150 years, Great American Insurance Group — a specialty property and casualty insurer with $8 billion in 2021 gross premiums written — has focused on technical innovation to adapt to changing times. So when the company sought a replacement for its legacy log management solution, decision makers focused on modern alternatives.

According to Sumit Bhargava, Divisional Assistant VP at Great American Insurance Group, maintaining the on-premises solution was distracting from the core business.

"The solution required constant caring and feeding to keep it running from a scalability standpoint. The basic features of a log management solution are to ingest and search data. And that's where our previous solution didn't scale to a level that a future-facing organization like ours depends on," said Bhargava.

The tech veteran knew he wanted a cloud-based log management platform. Rather than constantly fiddling with the number of nodes and servers, he wanted to focus on mission-critical objectives such as compliance, threat hunting and producing secure code.

"Quite simply, we needed a cloud-based solution to ingest all logs and quickly perform searches that matter to us," said Bhargava. "Our previous solution wasn't meeting our needs, so we went looking for what's next in the log management space."

That's when Great American Insurance Group turned to CrowdStrike Falcon® LogScale.

**Head-to-Head Comparison**

During its search for a new solution, the company quickly zeroed in on two options: Falcon LogScale and a popular open-source solution. Key requirements included ease of ingestion, fast searches and role-based access control.

Falcon LogScale immediately stood out in the head-to-head comparison, according to Bhargava.

"The ease of ingestion and search speed of Falcon LogScale definitely stood out during the POC."

**Sumit Bhargava**
Divisional Assistant VP, Great American Insurance Group

"With the other solution, it took too long to parse and prep the data for searches. With Falcon LogScale, we can very quickly pipe in the logs and start benefiting from fast searches," said Bhargava. "The ease of ingestion and search speed of Falcon LogScale definitely stood out during the POC."

After speaking with several references, Bhargava selected Falcon LogScale. Next came implementation. Having already ingested billions of events during the POC, onboarding became a simple proposition, aided by CrowdStrike training sessions and third-party integration support.

"We ended up going into production very quickly. The CrowdStrike Falcon® platform is one of the few platforms I've implemented where the onboarding was fast, thanks in part to the CrowdStrike engineers who helped us get up and running quickly," said Bhargava.

GREAT AMERICAN INSURANCE GROUP

## INDUSTRY
Insurance

## LOCATION/HQ
Cincinnati, OH

## CHALLENGES
- The legacy on-premises log management solution required too much maintenance
- It was also too expensive to collect and retain all the necessary logs
- The company wanted a next-gen, cloud-based log management solution to increase speed-to-insight and broaden data access

## SOLUTION
With Falcon LogScale, Great American Insurance Group gets a modern log management solution to log everything and search log data with sub-second latency.

"Our previous solution wasn't meeting our needs, so we went looking for what's next in the log management space. Falcon LogScale enables us to ingest significantly more data than the previous solution ... we've scaled up immensely."

**Sumit Bhargava,**
Divisional Assistant VP, Great American Insurance Group

voices

**CrowdStrike** Customer Case Study

### Scaling Up

Today, Great American Insurance Group uses Falcon LogScale as its cloud-based enterprise log management platform for four main use cases: compliance, operations, security and DevOps. According to Bhargava, everything starts with data ingestion.

"Falcon LogScale enables us to ingest significantly more data than the previous solution," said Bhargava. "We've scaled up immensely with Falcon LogScale."

He points out that Falcon LogScale isn't just a closet the company throws data into then forgets about it. All across Great American Insurance Group, logs are actively being used on a daily basis.

"From an operations standpoint, I've been pleasantly surprised at how much we've been able to do with Falcon LogScale," said Bhargava. "Being able to track sensitivity around our environment and look at all our routers, switches, security devices and servers has enabled us to react to events much faster. Our operations posture has been further enhanced since implementing Falcon LogScale."

Great American Insurance Group can now log everything and easily access archived data. In addition to helping with compliance, longer data retention helps with security use cases. The company uses Falcon LogScale to augment its security information and event management (SIEM) tool by sending a subset of data to the SIEM for more advanced searches.

"Having logs for a longer period gives us the ability to identify root causes of any issue and look at certain cases reactively," said Bhargava. "But Falcon LogScale allows us to be more proactive as well, as we now have security dashboards that enable us to do near real-time analysis. The augmentation strategy is working really well for us."

### From Minutes to Seconds

Speed is another common theme across Falcon LogScale use cases at Great American Insurance Group. With the previous solution, ingesting data took minutes. That's no longer the case.

"With Falcon LogScale, our logs appear instantly. It's not a visible delay where we're waiting minutes, like with before. Now we can search three billion events in under a second," said Bhargava.

This speed directly translates into business benefits, according to Bhargava.

"In a typical IT environment, you'd be looking for a resolution in multiple places. With Falcon LogScale, we have one view where we can have our searches and continually narrow the focus until we find the possible fix. We've had many instances where we've been able to detect and resolve issues much faster, which I'd say gives us a competitive advantage," said Bhargava.

He notes how the speed of Falcon LogScale translates into a better customer experience as well. "Getting the logs quicker enables us to look for issues faster and avoid service interruptions that could linger," said Bhargava. "Falcon LogScale plays a big role in helping us catch abnormalities faster and respond to those events."

## RESULTS

Search 3 billion events in under a second

Log users jumped from 10 to 1,000+

Logs are now used for security, DevOps, ITOps and compliance

## CROWDSTRIKE PRODUCTS

- CrowdStrike Falcon® LogScale
- CrowdStrike Falcon® Discover
- CrowdStrike Falcon® Insight XDR
- CrowdStrike Falcon® Prevent
- CrowdStrike Falcon® Intelligence
- CrowdStrike Falcon® Firewall Management
- CrowdStrike Falcon® Identity Threat Protection
- CrowdStrike Falcon® Spotlight

"With Falcon LogScale, our logs appear instantly. It's not a visible delay where we're waiting minutes, like with before. Now we can search three billion events in under a second."

**Sumit Bhargava,**

Divisional Assistant VP, Great American Insurance Group

voices

**CrowdStrike** Customer Case Study

### Doing More with Less

For many organizations, tech budgets are about doing more with less. Great American Insurance Group wanted to expand its usage of logs across the business, yet the previous solution didn't allow role-based access control, restricting usage to a handful of users.

Falcon LogScale enables role-based access control. As a result, log usage at Great American Insurance Group has skyrocketed. In fact, the company now has more than 1,000 users on Falcon LogScale, as compared to fewer than 10 with the incumbent solution.

"More than the number of users, I would say the type of users is critical," explained Bhargava. "We now have users of all technical abilities running queries. And we can control which logs they can access based on which roles they carry. That's been a game-changer for us."

More users. More data. More speed — but at what cost? Before the POC, Bhargava asked for a rough price estimate. He was impressed by Falcon LogScale's simple cost structure.

"I appreciate the simple view of how CrowdStrike prices the solution and helps customers grow in it. That was definitely a differentiator," said Bhargava. "As we compared enterprise-grade log management solutions, Falcon LogScale came in at around one-third the cost of similar platforms we considered."

### Exceeding Expectations

Bhargava is proud of what the company has accomplished with Falcon LogScale in just 18 months. Still, there's much work to be done, he said.

DevOps is one area where the company plans to expand its usage of logs. The insurer uses a private cloud to churn out code. Before Falcon LogScale, developers were missing a logging solution to support code production. Today, Falcon LogScale enables developers to create specific dashboards for their application needs, thus enabling faster and cleaner code.

"It's a big step forward, but the possibilities are endless," said Bhargava. "Given our success with Falcon LogScale to date and growing use of cloud-based solutions, we plan to add more and more log sources as we roll out Falcon LogScale to other areas of the business."

He sees Falcon LogScale as a key enabler in helping the company remain forward-facing.

"Falcon LogScale has exceeded our expectations. Its ingest speeds are faster. Its searches are faster and more flexible. We're achieving so much more than we expected as we embarked on this journey," concluded Bhargava. "We're a happy customer."



## ABOUT CROWDSTRIKE

**CrowdStrike** (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data. Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

CrowdStrike: **We stop breaches.**

Learn more: **https://www.crowdstrike.com/**

Follow us: **Blog** | **Twitter** | **LinkedIn** | **Facebook** | **Instagram**

Start a free trial today: **https://www.crowdstrike.com/free-trial-guide/**



CROWDSTRIKE

we stop breaches