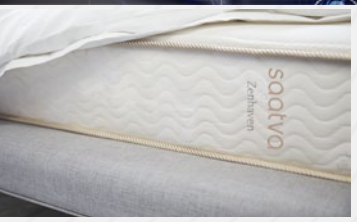

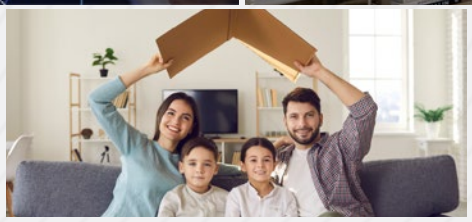

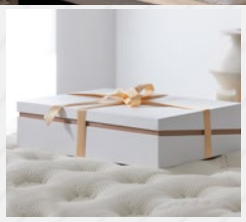

saatva

SMARTER LUXURY SLEEP

Luxury Mattress Retailer Puts Log Management Issues to Bed with CrowdStrike

Saatva is a luxury mattress company headquartered in New York and Austin. Since 2010, Saatva's mission has been to offer an unparalleled mattress shopping experience via high-quality products, fair pricing and superior customer service.

As a primarily online retailer, web application performance is fundamental to the company's success; poor online experiences can drive away shoppers and impact the bottom line. Saatva was using an open-source log management solution to gather insights into application throughput and latency issues, but its homegrown ELK (Elasticsearch, Logstash and Kibana) stack was proving too difficult to use and maintain.

After evaluating a number of options, including Datadog and Papertrail, Saatva selected CrowdStrike for its next-generation log management solution. Doing so has given the company widespread benefits and the confidence to explore security use cases with CrowdStrike.

Visibility Meets Speed

CrowdStrike Falcon® LogScale is a modern log management and observability solution. It enhances IT observability by allowing organizations to view and explore threats, identify system vulnerabilities and gain valuable insights from all log and event data in real time.

For Saatva, Falcon LogScale improves DevOps visibility and provides actionable insights into application performance, response time and scalability issues. Developers, QA engineers, support teams and technical analysts all use Falcon LogScale to quickly pinpoint and resolve application and system design issues.

One such user is Chris Miller, Software Engineering Support Manager at Saatva. Addressing any bug or other issue with Saatva's website starts with him — and he uses Falcon LogScale to quickly troubleshoot anything that comes up.

"Before LogScale, we'd have to manually attempt to reproduce problems, which can be tedious and time consuming," explained Miller. "Being able to quickly pinpoint and resolve application bugs using Falcon LogScale makes our jobs faster and easier."

He lamented an ELK stack that was "too old and slow" for Saatva, and required constant upkeep, which distracted the team from its core functions. Switching to Falcon LogScale has driven efficiencies across the organization.

"Falcon LogScale is probably 100x faster than ELK, simply because it works," said Miller. "It's made us 5x faster at resolving issues, leading to a better website and customer experience."

INDUSTRY

Retail

LOCATION/HQ

New York and Austin

CHALLENGES

- Saatva's previous open-source log management platform (ELK) was too old, slow and prone to issues.
- As attack surfaces grew, the company's managed endpoint solution no longer provided adequate visibility and protection.
- The company's small IT team didn't have the capacity to monitor for security issues 24/7.

SOLUTION

Saatva uses CrowdStrike Falcon LogScale for DevOps visibility and CrowdStrike Falcon Insight XDR for endpoint detection and response.

RESULTS

- Zero breaches with CrowdStrike
- 100x faster searches, compared to previous log management solution
- 5x faster troubleshooting

Data-Driven Decisions

Falcon LogScale features customizable, sharable dashboards that make it easy for Saatva teams to visualize data and investigate issues across systems.

"I've never worked with an easier tool to integrate into our system," said Daniel DeRossette, Senior Engineer at Saatva. "With LogScale, we can quickly create dashboards to identify errors across microservices, monitor throughput, visualize system latency ... you name it."

For Saatva, Falcon LogScale not only provides modern log management at petabyte scale, it displays information in a straightforward way, keeping management in the know while steering practitioners into action.

"We use Falcon LogScale to make data-driven decisions," said DeRossette. "For example, we have an event-driven microservice that runs on AWS and translates order data from our sales channel to our logistics tool. We created a dashboard to visualize system timing sequences so we could fine-tune our design and eliminate latency and processing issues."

Next Logical Step: CrowdStrike for Security

For Saatva, success with Falcon LogScale opened the door to CrowdStrike security use cases as well. In 2021, the company licensed CrowdStrike Falcon® Insight XDR for endpoint detection and response to protect its expanding attack surface.

According to Saatva Security Analyst Reed Britton, the shift to remote work meant there were more employee devices outside the network perimeter. At the same time, the company was opening viewing rooms across the U.S. — all of which contained endpoints that needed protection as well.

"We've got lots of employees working remotely with personal devices. There's potential for them to introduce security risks and cause havoc on the network," acknowledged Britton.

Saatva was using Sophos managed through a third party for endpoint detection and response (EDR), but it wasn't providing adequate visibility, according to Britton.

"After reading great reviews about CrowdStrike on analyst websites, and given our success with Falcon LogScale, switching to CrowdStrike for EDR was an easy decision," said Britton. "Now, we have visibility into all our devices and can take action to eliminate threats."

Saatva also added CrowdStrike® Falcon OverWatch™, a 24/7 managed threat hunting service. Given the company operates around-the-clock, but doesn't always have security staff available during those hours, Falcon OverWatch provides a stopgap measure to keep the company safe.

"We have a tiny IT team, so OverWatch acts as an extension of our security team and watches our backs 24/7," said Reed.

Plans to Expand

Saatva's ambitions continue to grow, with four new viewing rooms slated to open in 2023. As the company expands, so do its attack surfaces and security risks. As such, Saatva aspires to expand its partnership with CrowdStrike.

"We're very happy with CrowdStrike," concluded Reed. "I'm always trying to get more modules."

"Being able to quickly pinpoint and resolve web application bugs using Falcon LogScale makes our jobs faster and easier."

–Chris Miller, Software Engineering Support Manager, Saatva

ENDPOINTS

400

CROWDSTRIKE PRODUCTS

- CrowdStrike Falcon® LogScale
- CrowdStrike Falcon® Insight XDR endpoint detection and response
- CrowdStrike® Falcon OverWatch™ managed threat hunting

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.**

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

Start Free Trial

Learn more **www.crowdstrike.com**

CROWDSTRIKE

we stop breaches