elastic | opala

SUCCESS STORY

Opala protects critical medical data and optimizes cloud infrastructure with Elastic

Region
United States

Industry
Software and Technology

Solution
Elastic Security, Elastic Observability

Reduces P1 incidents by 88%

- With Elastic Observability, Opala has seen a massive reduction in high-severity IT incidents.

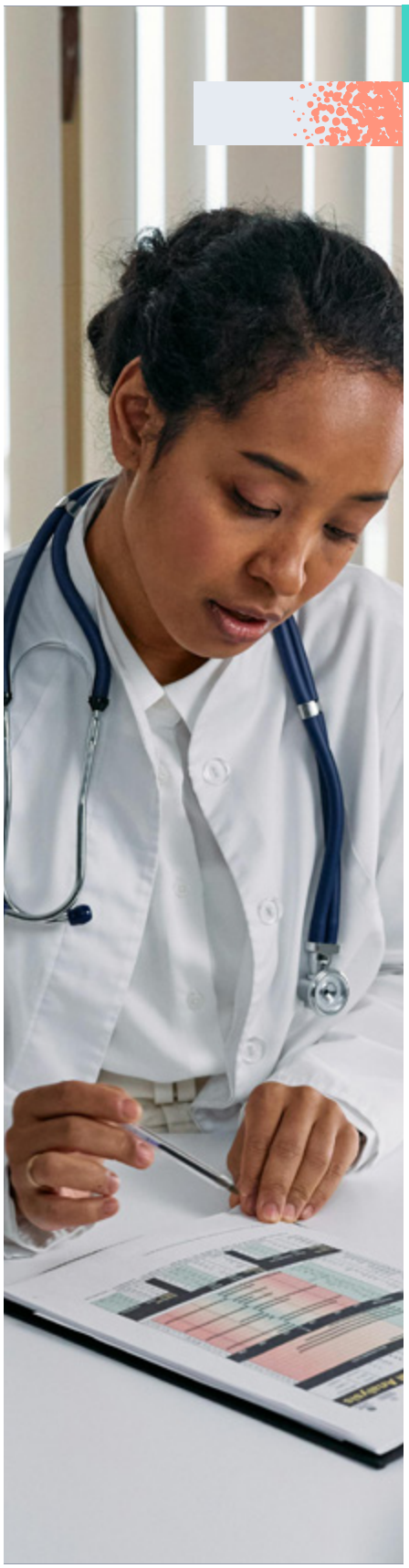
Delivers 99.99% uptime

- With Elastic Observability, Opala has improved from 99.3% to “four-nines” service availability.

Provides rich context for threat hunts in just 15 minutes

- Opala can input an indicator of compromise and search through petabytes of historical data in a matter of minutes with Elastic Security.

Opala replaces Datadog, CrowdStrike, SumoLogic and AWS CloudTrail with the Elastic stack, increasing availability, shortening the software deployment cycle, and boosting security.



Opala leads the way in helping healthcare payers, patients, and providers exchange medical data that improves health outcomes and ensures accurate, timely payments. The business stores around 690 million healthcare records for 6.5 million patients using Elastic to protect this sensitive, highly valuable data.

Joe Ben Slivka, Director, Cloud Infrastructure and Cybersecurity, Opala, is responsible for the security and efficiency of Opala's networks, systems, and applications. "My number one goal is to ensure that our environment is secure, hasn't been breached, and is always available so our customers don't even have to think about it," he says.

When Slivka first joined the business, it was still grappling with a 'lift and shift' cloud migration that kept much of the on-premises infrastructure and design intact. This included an array of disparate observability and security solutions that resulted in week-long deployment cycles and time-consuming outages. Fixing an incident required many hours of engineering time and manual investigations to resolve issues.

Slivka had a clear vision of what was needed. "Infrastructure and security go hand in hand, especially in cloud-native systems." This especially matters to a business that collects around 5.6 billion events every 15 minutes. "Given that scale, there's no reason to aggregate it to a separate security information and event management (SIEM) system while also managing an observability solution."

elastic

A game changer for observability and security

Having worked with Elastic in previous roles, Slivka took the initiative to investigate Elastic's latest capabilities in pursuit of a unified security and observability platform.

"The real selling point of Elastic became clear once I explored the changes that have occurred over the last four or five years," says Slivka. "As well as cutting edge storage and search, the availability of built-in integrations and visualizations is a game changer. Elastic was the clear leader when it comes to delivering both security and observability in a single platform."

Deployment of the Elastic Stack was seamless thanks to resale and service delivery partner Industrial Resolution. Tim Schreyer, Engineering Team Lead, Industrial Resolution, said, "One of the best things about Elastic is how quickly we can prove the operational and security benefits, as well as lower costs, by combining both solutions instead of running two systems."

He recalls the first time that he and Slivka added a new data source to Elastic. "We simply switched on the integration and the majority of what Opala needed was accessible on the front end of Elastic." This includes Kibana dashboards. "Instead of waiting for weeks to visualize a new data source, the dashboard was up and running in a day," says Schreyer.

Slivka adds, "Industrial Resolution acts as an extension of our team. They don't just complete tasks; they collaborate with us to achieve the results we need. They even worked with our developers to set up a mini CICD process, making everything faster and more efficient. That's huge."

> Using Elastic to consolidate observability and cybersecurity solutions goes beyond just financial savings. It also encompasses the consolidation of developer knowledge and skills. This centralization of infrastructure through Elastic enables our teams to work much more efficiently.

Shahryar Qadri
CTO, Opala

A boost for service availability

With the assistance of the team at Industrial Resolution, Opala has replaced cloud tools including Datadog, CrowdStrike and AWS CloudTrail with Elastic's unified observability and security platform. As a result, the business has seen a significant uptick in system, network and application performance.

For instance, service availability has increased from 99.3% to 99.99%. "In recent months, we have experienced multiple quarters with full four-nines availability," says Slivka.

Database performance has also improved thanks to insights gained from Elastic. "We were able to track latency on calls against the number of requests being made to Postgres," says Slivka. By integrating this observability information back into the development process, developers can quickly identify and correct bottlenecks, performance issues, and errors and push the changes through.

As a result, the average outage window has decreased to less than five minutes. Currently, Opala averages about one P1 incident per month, compared with two to three times per week before Elastic, realizing an 88% reduction in P1 incidents.

Mean time to resolution (MTTR) has also plummeted by 90%. Problems are now solved within minutes, as opposed to dozens of hours. "For our last outage, we had a working solution in 20 minutes," says Slivka. "The total time spent, including the post-incident review, was about six hours of engineering time—down from over 60 hours. That's a full week of development time saved, which we can now dedicate to delivering features and improving our customers' experience," he says.

> With Elastic, when someone gets an alert, they can simply click in and immediately see what actions need to be taken. The value of this — both for internal efficiency and customer trust in the reliability of the solution — can't be overstated.

Joe Ben Slivka
Director, Cloud Infrastructure and Cybersecurity, Opala

Another area that has seen a dramatic improvement is time to release. When Slivka joined Opala, it averaged around a month from the time the code was ready in development to production. With the deployment of Elastic, it has reduced that timeframe to about 48 hours including development testing, QA, and production.

A holistic approach to observability also improves customer communications. "When a customer calls to report an issue, we know that it is probably their system. In almost 10 months, we haven't had a single customer-reported outage," says Slivka.

A speedy response to cyber threats

The team also benefits from Elastic Security for cloud native security and endpoint protection capabilities in a single solution. Slivka says, “With Elastic Observability deployed, it was a natural extension to collect network logs for the security team to analyze for indications of compromise.” By gathering this data, they can conduct threat analysis, examine traffic patterns, and assess how the web application firewalls (WAFs) are functioning.

Time to identify security threats has fallen. “When a new threat emerges, we typically have an Indicator of Compromise (IOC) ready to go,” says Slivka. “We can input these into Elastic and initiate an internal threat hunt within just 15 minutes. That’s the power of Elastic—there’s simply no other way to achieve this level of responsiveness.” Now the team is evaluating Elastic Threat Intelligence. “The machine learning features are really appealing,” says Slivka. “We want to integrate it into our system so we can quickly and automatically pull in new indicators which enable us to see how our environment stacks up against the latest threats in real time.”

Clear roadmap for a secure and efficient future

Looking to the future, Opala hopes to take advantage of three additional Elastic features, including Elastic Observability Application Performance Monitoring (APM). “I’ve used many different tools over the years, and I don’t think there’s anything quite as robust as Elastic’s APM. It’s world-class,” says Slivka. With greater visibility into code performance, developers can work more efficiently, enabling Opala to scale down resources and reduce compute usage.

Lastly, Opala is looking at utilizing more of the AI components within Elastic, including Elastic AI Assistant which enables users to automate tasks such as alert investigation, incident response, and query generation or conversion using natural language. “Elastic’s AI features and roadmap are really impressive. Being able to connect business and operational data with a natural language interface could further enhance alert investigation and incident response.”