SUCCESS STORY

Informatica brings data to life for internal customers with Elastic Observability and Elastic Security

Informatica, an enterprise cloud data management leader, replaces complex observability and SIEM solutions with Elastic's single pane of glass platform, boosting application performance while protecting systems from external threats.

Region
United States

Industry
Software & Technology

Solution
Elastic Security,
Elastic Observability

Cuts costs by 50%

With Elastic, Informatica has reduced observability and security costs by 50% compared with solutions from other vendors.

Accelerated MTTR

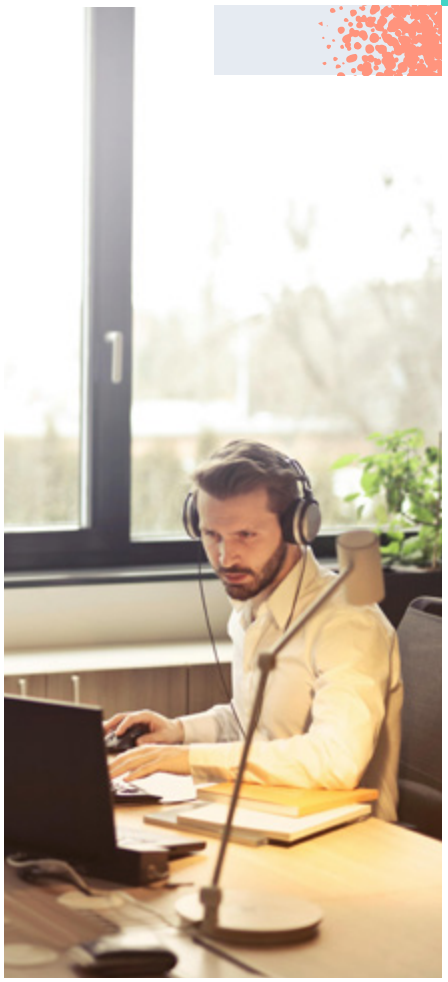
Informatica has reduced the time it takes to identify and fix issues using machine learning and other advanced monitoring tools from Elastic.

Reduces storage cost and complexity

With Elastic Searchable Snapshots, Informatica has reduced dependency on expensive 'hot' storage and decreased hardware costs significantly.

If data is the fuel that powers large businesses, Informatica is the engine that converts it into the energy that drives efficiency and innovation in every conceivable industry from education and government to financial services and retail.

Its flagship platform, Intelligent Data Management Cloud (IDMC), enables customers to turn chaotic data into a trusted resource that informs smarter decisions. Taking advantage of machine learning and generative AI, IDMC is used by 85 of the Fortune 100 and manages more than 54 trillion cloud transactions per month.



"We bring data to life for our customers," says Amreth Chandrasehar, Director of ML Engineering, Observability, and Site Reliability Engineering at Informatica. "Wherever an organization stores its data, we make it accessible to their stakeholders including developers, data analysts, and business users."

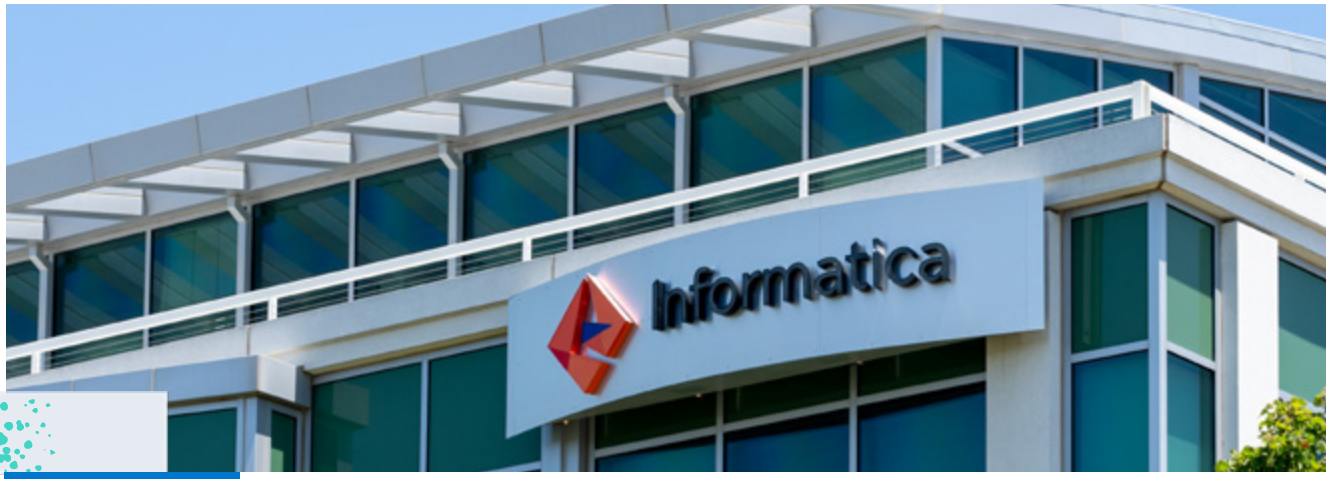
Chandrasehar and his team are responsible for keeping Informatica's own systems secure and constantly available to internal customers. "Any disruption or security breach can have consequences for the business and our customers," he says. "Our job is to stay one step ahead of any events that threaten system performance and fix them before they become serious."

Standardizing and centralizing with Elastic

Until about four years ago, Informatica used several observability and SIEM solutions to achieve this goal. Maintaining multiple vendor relationships compromised Informatica's efficiency and cost too much time and money. These issues ultimately inspired Chandrasehar to find a more streamlined solution.

"The Elastic release of Elastic Cloud on Kubernetes (ECK) worked well for Informatica," says Chandrasehar. "ECK provides us with a comprehensive observability and SIEM solution that we can split into multiple clusters and use to comply with the latest data privacy and security requirements in different regions and territories."

Within a few months, Informatica was able to migrate its entire logging workload to an in-house ECK cluster which now ingests 37 terabytes of logs per day and 2.8 trillion documents per month. It sounds like a massive amount of workload, but Chandrasehar says that one of Elastic's key strengths is its manageability. If I want to scale my data nodes or make configuration changes, I can do it seamlessly through ECK. Everything is automated so that all the new data is available in our Elastic cluster in a matter of seconds."



Viewing the data world through a single pane of glass

Rather than source separate solutions for observability and SIEM, Informatica now benefits from a single pane of glass for insights into Informatica applications hosted in multiple regions and across its four cloud partners: AWS, Azure, Google Cloud, and Oracle. This has delivered efficiencies and cost savings that result from a single vendor relationship and streamlined software costs.

For example, it takes just three people to manage the Elastic platform day-to-day. In addition, Informatica has reduced costs by taking advantage of Elastic Searchable Snapshots. This enables it to retain data in a searchable form for 90 days while reducing dependency on expensive 'hot' storage.

37 TB
Log ingestion per day

200 million
Bytes per second ingestion in Kafka

2.8 trillion
Documents ingested per month

10 PB
S3 storage (standard and glacier)

1.5 million
API calls per day

1.5 PB
Provisioned in cluster storage

> With Elastic, we have a single vendor for observability and SIEM. This represents a cost saving of 50 percent compared to other solutions for an organization of our size.

Amreth Chandrasehar
Director of ML Engineering, Observability and Site Reliability Engineering, Informatica

elastic

Boosting observability with machine learning

Informatica uses Elastic Observability to monitor more than 100 applications and 300 Kubernetes clusters. Logs are ingested into the Elasticsearch database, and the team uses Kibana dashboards to visualize KPIs including availability, latency, and service saturation. The outputs from this process include problem statements and resolutions that significantly shorten the mean time to repair (MTTR).

Chandrasehar also highlights the role of Elastic APM, which includes powerful machine learning features that can be deployed out of the box. This enables Informatica to accurately forecast anomalies while providing engineers with alerts and insights that reduce the time to identify and fix the root cause of the issue.

Machine learning can also be applied to networking traffic/load balancer logs, threat hunting, and database logs. "Database failures mostly happen when there are unexpected spikes in database connections that are left open. This machine learning model can identify the pattern from previous trends and warn the appropriate team in advance of any issues," says Chandrasehar.

> Elastic's search functionality is incredibly fast. We store trillions of documents, but a search query returns accurate results in little more than 10 seconds.
>
> **Amreth Chandrasehar**
> Director of ML Engineering, Observability and Site Reliability Engineering, Informatica

Fixing security issues before they become problems

Elastic Security provides Informatica with a comprehensive SIEM solution that enables the organization to detect and respond to threats at speed and scale. It tracks about 8.5 billion events per day using Elastic's comprehensive collection, analysis, correlation, and transformation tools. These events are scrutinized using over 400 detection rules, some of which are available out of the box and others configured by a dedicated security team that manages the SIEM cluster.

"Elastic Security is another example of where we can use machine learning to generate real-time alerting, reporting, and auditing. We can tell if something is going wrong in a matter of seconds instead of waiting for one of our internal customers to tell us that they have an issue."

Comprehensive support from a dedicated team

From the very first proof of concept, Chandrasehar was impressed by the commitment of the Elastic team. “They provided substantial support from day one even before we fully committed. That level of engagement sets Elastic apart from other vendors and gave us the confidence to move forward with full deployment.”

Since then, Informatica has been a leading contributor to the Elastic roadmap, submitting more than 50 feature requests with the support of Elastic project managers and developers.

Elastic Professional Services also plays a key role in the success of Informatica’s ECK deployment. “Like any customer I’m always very demanding of my software vendors,” says Chandrasehar. “The Elastic Professional Services team has always been there to answer our questions and resolve issues quickly. It’s like having an extra pair of hands on the team.”

Seeking added value from generative AI

Informatica is now keen to explore new artificial intelligence features available in the latest Elastic releases which includes Elastic AI Assistant for observability. Elastic AI Assistant enhances observability workflows with generative AI to improve troubleshooting processes and provide automated explanations for complex information. “We’ll be looking at this closely,” says Chandrasehar.

He can also see the potential of other Elastic tools and features that he hopes to deploy in the coming year. These include Root Cause Analysis (RCA) management, and OpenTelemetry. “With the support of Elastic and the Elastic Professional Services team, we’re looking forward to doing even more with new features when they become available. Elastic is a major technology partner for Informatica today and will be for many years to come.”