SUCCESS STORY

BRAZIL | TELECOMMUNICATION | ELASTIC SECURITY

Brazilian online media giant slashes incident resolution time by 80% with Elastic AI

By uniting security and observability on Elastic, UOL can harness generative AI to enhance threat detection and reduce the cost of running multiple platforms.

The UOL Group is the largest Brazilian content, technology, services, and payment company. Eight out of ten Brazilian internet users access UOL every month to read news, stream sports and TV series, and take advantage of online services including email and technical support.

80% faster incident resolution time

With Elastic, AI-assisted root cause analysis cuts incident fix times from days to minutes.

50% fewer false positives

Elastic Attack Discovery helps UOL triage alerts so teams can focus on real threats.

100% unified visibility

Cross-team collaboration improves with a single “pane of glass” for multiple groups across the business in Elastic.

This vast media organization operates on a sophisticated digital infrastructure, managed by a large IT team that oversees more than 200 applications and thousands of cloud resources, containers, and on-premises servers. Ensuring the smooth operation of such a diverse ecosystem is a complex task, further challenged by the coexistence of modern platforms with legacy systems, some of which have been in place for over two decades.

For this reason, UOL has been an enthusiastic user of Elastic for more than 10 years. Today, the company uses the latest Elastic Security and Elastic Observability solutions, which include cutting-edge generative AI for root cause analysis and incident detection.

Alcides Zanarotti Junior, CTO, UOL, says, “Elastic has always been a trustworthy platform thanks to its scalability and regular feature updates, especially machine learning and AI in recent releases.”

The company adopted the enterprise version of Elastic Observability in 2020, extending the use of the platform across the wider business and removing the need to run multiple observability systems. This initiative, called logcenter, runs on a single on-premises Elastic cluster and provides a ‘single pane of glass’ in the form of Kibana dashboards used by different teams to monitor their systems.

Most recently, the UOL Security Team migrated from Splunk to Elastic Security to protect the organization’s systems and data. Fabiano Marques, Director of Operations, Processes, and Solutions, UOL, says, “It is far more efficient to run observability and security on a single platform. Before, we had to look at two to three systems. Now everything is in the same place.”

> With Elastic, the time needed to fix actual security events has been reduced by 80%, and false positives are down 50%.
>
> **Alcides Zanarotti Junior**
> CTO at UOL

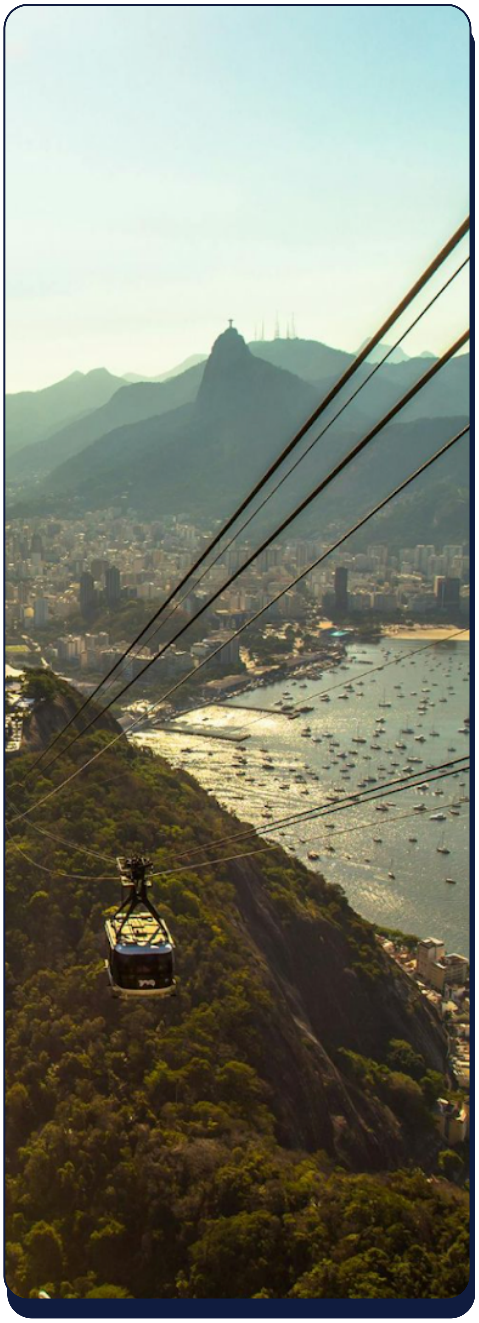
Taking advantage of generative AI

Consolidating observability and security on a single platform also opens the door to a wealth of cutting-edge Elastic AI features. These include advanced endpoint detection and response (EDR) and the Elastic AI Assistant that enables users to interact with Elastic Security using natural language for tasks such as alert investigation, incident response, and query generation or conversion.

UOL has also deployed Elastic Attack Discovery for threat detection and resolution. Attack Discovery enhances visibility by triaging alerts, reducing false positives, and presenting results in an intuitive interface so UOL's security team can quickly understand issues and take action. The company has also integrated Attack Discovery with AWS Bedrock, enabling users to leverage Elastic's capabilities within the Bedrock environment and use Bedrock's large language models (LLMs) to power Elastic's AI Assistant and other applications.

Combined, these features have enabled UOL to massively accelerate root cause analysis and resolution. "Before Elastic with AWS Bedrock, it would take days or hours to grab a log, search for the issue, put it on a dashboard and start analyzing. It now takes just minutes," says Zanarotti Junior.

Often, Elastic's predictive observability simply prevents issues from occurring in the first place. "With Elastic, the time needed to fix actual security events has been reduced by 80%, and false positives are down 50%," he says.



> Elastic has completely changed how we think about security and observability for the better. Technology keeps evolving and so will we, together.
>
> **Alcides Zanarotti Junior**
> CTO at UOL

A positive shift in security and DevOps culture

The way that Elastic has helped steer the company's security culture is just as important as the technology itself. As any large business knows, teams are often attached to their applications, and it takes an exceptional alternative to change their minds. This is where Elastic excels.

"Our employees are motivated to understand and resolve security issues as effectively as possible," says Marques. "Elastic answers this question so well that one of our biggest challenges is managing the queue of teams that now want to use it for their environment."

It has also led to a more pragmatic approach to security. Instead of delivering set features, the security team now asks internal customers about the issues that they face and builds team-specific rules and alerts in response. For example, high memory usage might indicate a virus or a misbehaving script. Or if a team spots repeated connection attempts from a suspicious IP address, the team can block it and put new rules in place.

High-quality technology also equates to a higher quality of life. In simple terms, Elastic reduces the number of incidents that require employees to work late into the night or at inconvenient hours fixing an issue. "Now I can see all the teams including operations, DevOps, and development teams speaking the same language. It's fantastic," says Marques.

For UOL, the journey with Elastic is far from over. As Brazil's largest digital media and services platform, the stakes are high, and the pace of change is relentless. With every new release and beta program, the company sees fresh opportunities to outpace threats and embed AI into the heart of its operations. "Elastic has completely changed how we think about security and observability for the better," says Zanarotti Junior. "Technology keeps evolving and so will we, together."