CUSTOMER STORY

Securing 80+ Million Users: How NTT DOCOMO Relies on Sysdig

NTT DOCOMO is a leading player in Japan's telecommunications sector, supporting approximately 87 million customers. In addition to cell phone access, the company provides optical communication services, satellite phones, content streaming, and shopping services. They also provide payment processing and business services through a subsidiary, NTT Communications Corporation.

RAFTEL, developed in 2019, is planned to be migrated to the GKE environment in 2024 to enhance interoperability between their services.

NTT docomo

INDUSTRY

Business Services

CHALLENGES

- Establish DevSecOps processes within Kubernetes
- Gain visibility into all clusters and pods to protect against vulnerabilities; troubleshoot and monitor performance
- Manage increased operational complexity created by Kubernetes migration while adhering to strict compliance requirements

OUTCOMES

- More efficient and effective management and operations
- Full compliance coverage with Sysdig
- Refined incident response process with improved early detection

CHALLENGES

Developing Next-Gen API Infrastructure

NTT DOCOMO started out exclusively as a telecommunications provider. However, over the past several years, the company has begun introducing new products and services to its portfolio, ranging from video and music streaming to enterprise software. Because each service calls a wide variety of APIs, this leads to increased processing complexity.

“Not only was the number of services and systems using APIs increasing, but the number of underlying systems on the receiving end had also increased,” explained Mr. Masatoshi Kato, Senior Manager, Service Design Department at NTT DOCOMO. “We concluded that the best way to address these challenges was by consolidating all APIs in one place and making them into a common infrastructure. This would allow any developers working with our services to access whatever APIs they needed.”

NTT DOCOMO began working on the next-generation infrastructure that would make this approach possible, known as RAFTEL. To support development, they adopted Google Cloud’s API infrastructure service, Apigee. From there, they migrated to Google Kubernetes Engine (GKE).

Shifting API access to the public cloud meant that NTT DOCOMO would need to manage a significant increase in traffic to web and smartphone applications. They’d need a way to flexibly control capacity and provide on-demand resources for their services. This ultimately drove their decision to migrate to Kubernetes.

Securing Google Cloud

NTT DOCOMO was subject to strict regulatory requirements, none of which were necessarily compatible with public cloud infrastructure.

The company’s first step was to begin transitioning toward DevSecOps. Starting with RAFTEL, they planned to integrate security into every phase of their development lifecycle.

To facilitate a DevSecOps workflow, they had strict requirements for their cloud security tool. First, they’d need full visibility of all containers in their environment. They would also require a means of detecting cloud misconfigurations, protecting against container vulnerabilities, and preventing unauthorized access. Finally, they needed a way to detect, identify, and send alerts about threats and vulnerabilities in real-time.

Compliance was also important. “Compliance was extremely time-consuming for engineers to do manually. We were looking for a tool that would help us with that,” said Mr. Norikazu Yamaguchi, Manager, Service Design Department at NTT DOCOMO.

Security and compliance weren’t NTT DOCOMO’s only considerations. They were also looking for a way to reduce operational complexity and improve application performance on RAFTEL. They recognized that doing so would not only help them improve their overall quality of service, but also reduce operating costs.

“We wanted to be able to carry out performance monitoring and troubleshooting while managing multiple clusters and pods,” said Mr. Kato.

SOLUTIONS

One Tool, Three Teams Aligned

NTT DOCOMO compared security solutions from several different vendors, as well as Google.

"One of the engineers involved in evaluating vendors was a fan of Wireshark," recalled Mr. Kuniyuki Fukuda, Assistant Manager, Service Design Department at NTT DOCOMO. "He recognized Sysdig right away and enthusiastically told us that the creator of Sysdig developed Wireshark. When I visited Sysdig's U.S. headquarters, I had the opportunity to speak directly with the creator, now the company's CTO and founder, who provided us with a demonstration and thorough explanation of Sysdig's approach to cloud security. While some companies have approached cloud security from the posture perspective, Sysdig doesn't stop there, it spans the entire lifecycle and really excels at detection, investigation, and response."

A short time later, NTT DOCOMO deployed **Sysdig**.

Sysdig is a versatile tool that different teams are using to speak the same language.

- The company's infrastructure team uses Sysdig to manage cloud infrastructure security and ensure compliance.
- The operations team uses Sysdig to optimize application performance.
- The development team relies on Sysdig to debug and troubleshoot containerized applications.

> "Sysdig makes it easy to see our compliance status at a glance — and we believe that the platform's compliance score can be a motivating factor for better practices."
>
> **Mr. Kuniyuki Fukuda**
> Assistant Manager, Service Design Department

SOLUTIONS

Real-Time Incident Response

Sysdig has been invaluable from an incident response perspective. The platform's ability to correlate Kubernetes events, pod logs, and various metrics helps operators gain an immediate understanding of the situation when an incident occurs. NTT DOCOMO expects this will considerably reduce their response times compared to conventional operations.

"When a security incident occurs, the ability to have the right information correlated so we can quickly trace the timeline to identify the cause is invaluable," explained Mr. Taihei Ito, Service Design Department at NTT DOCOMO.

"Whether you're in the middle of incident response or managing vulnerabilities, the ability to drill down to the finer details of our network diagnostic tool from within Sysdig is highly valued by engineers. Sysdig develops its solutions on Kubernetes and prioritizes user-friendly design. They are the Kubernetes security experts and it shows because when we need information in the event of an issue, we can quickly and easily get it."

> "With Sysdig in place, we have a clearer picture of our risk and our response to vulnerabilities."
>
> **Mr. Norikazu Yamaguchi**
> Manager, Service Design Department

Prioritizing the Vulnerabilities that Matters

Prior to Sysdig's introduction, nearly all containers had either critical- or high-severity vulnerabilities.

"I was especially impressed by Sysdig's 'in-use' feature, which prioritizes components actively in use when scanning for vulnerabilities," Mr. Fukuda said. "This is a capability not typically found in most public cloud tools, and it's outstanding. I immediately recognized its potential to significantly reduce our security workload."

NTT DOCOMO sees Sysdig's automated vulnerability scanning and deep visibility at runtime providing advance warning of events that need to be addressed and how this can "result in a significant reduction in the cost of identifying and remediating vulnerabilities," according to Mr. Ito.

SOLUTIONS

Bringing Compliance to the Highest Standard

Sysdig also allows NTT DOCOMO to manage compliance with daily updates to requirements and status. After integrating Sysdig, they also made some unexpected discoveries about their compliance — namely, that they were missing a number of key items.

“Despite having established IT infrastructure compliance within the company, implementing a service with GKE and using Sysdig for compliance checks uncovered discrepancies and missing elements,” Mr. Kato said. “It was a pleasant surprise to find that the insights provided by Sysdig for business improvement were even more valuable than the tool’s core functions.”

“The compliance checks are quite detailed too,” observed Mr. Ito.

“Sysdig has been a great help where our business clients are concerned,” added Mr. Yamaguchi. “As IT infrastructure evolves, the number of compliance checks required grows. We face inquiries such as, ‘Given recent global attacks, is DOCOMO secure?’ The increased workload in our department has been significantly alleviated by Sysdig’s compliance capabilities.”

> “We’re excited about working with Sysdig. It’s going to play a major role in helping us develop a DevSecOps-based organizational culture.”
>
> **Mr. Masatoshi Kato**
> Senior Manager, Service Design Department

A Partner in More Than Security

NTT DOCOMO's migration to Kubernetes has enhanced resource efficiency and reduced costs. Typically, such migrations come with increased complexity, but this has not been the case here, thanks in large part to Sysdig. The company is already exploring additional applications for Sysdig's software, including using Sysdig not only for Kubernetes security and performance but also for overseeing their entire API ecosystem. The team is also eager to adopt **Sysdig Sage**, Sysdig's generative AI analyst.

"Our expectations for Sysdig are extremely high, given that we support services used by more than 80 million people," Mr. Yamaguchi concluded. "Currently, Sysdig is exceeding all of our expectations."

To learn more about NTT DOCOMO, visit **www.nttdocomo.co.jp**.

NTT docomo

INDUSTRY

Telecommunications

INFRASTRUCTURE

Google Cloud

ORCHESTRATION

Google GKE

SOLUTION

Sysdig Secure, Sysdig Monitor

About Sysdig

In the cloud, every second counts. Attacks move at warp speed, and security teams must protect the business without slowing it down. Sysdig stops cloud attacks in real time, instantly detecting changes in risk with runtime insights and open source Falco. We correlate signals across cloud workloads, identities, and services to uncover hidden attack paths and prioritize real risk. From prevention to defense, Sysdig helps enterprises focus on what matters: innovation.

Sysdig. Secure Every Second.

To learn more about Sysdig, visit **sysdig.com.**

REQUEST DEMO →