sysdig | CUSTOMER STORY

ICG INNOVATIONS
DRIVING EFFICIENCY

ICG Innovations Leverages Sysdig and AWS to Compete With Major Shops



Summary

As a consulting firm competing against much larger organizations, ICG Innovations needed a way to scale its cloud-native services without adding cost or complexity. As client environments moved rapidly to Kubernetes and Amazon Web Services (AWS), the team faced growing pressure to improve security visibility, reduce operational noise, and deliver measurable value back to customers. By standardizing on the Sysdig platform, the organization gained unified visibility across cloud, containers, and hosts, allowing teams to focus on real risk instead of chasing alerts. The result was a more efficient security operation that improved release velocity, optimized cloud spend, and strengthened ICG Innovations' ability to compete on both quality and cost. Today, Sysdig helps the company operate as a true security and business enabler for its clients.

Key Results

- Automation eliminated the need to hire two additional analysts.
- Consolidated five tools down to one.
- Increased visibility across cloud, container, and hosts to quickly identify issues at the node, pod, and user level.

ICG Innovations

Cloud-native consulting and SaaS provider for enterprise applications.

HEADQUARTERS

Arizona, USA

INDUSTRY

Software Technology

Customer Overview

Since 1990, ICG Innovations has been a trusted expert in back-office applications, such as business process automation, advanced technology, and systems integration. As a result, the company has established a diverse book of clients, which includes major financial services organizations, energy companies, well-known hospitality brands, and diversified shipping and logistics conglomerates.

As a software as a service (SaaS) provider, ICG Innovations is acutely aware that cloud-native challenges need cloud-native solutions, that existing tools cannot be applied to secure cloud workloads, and that any cloud-native tools a company adopts should be easy to deploy and scale.

“When we launched more than 30 years ago, everything was on-prem, but now it is all cloud hosted,” said Jim O’Rourke, Director of Business Development at ICG Innovations.

With the shift to cloud-based services, ICG Innovations’ clients can better scale and are offered greater business flexibility, faster application delivery times, and enhanced security. Overall, the increased visibility and agility offered through the cloud and ICG Innovations’ services has helped cut down on invoice process cycle times, reduced costs by millions of dollars, and significantly lowered support costs for its customers.

“We’re proud to be a real business enabler for our clients, but the topic we all continue to come back to is how to enhance security in a world where new threats are always popping up and we are dealing with back-office information – financial and other personal information,” said O’Rourke. “Equally as important, we want to scale our own services in a way where we can stay competitive with larger consulting firms through a higher quality of service with comparable cost.”

> “We’re proud to be a real business enabler for our clients, but security is always top of mind as new threats continue to emerge and we manage highly sensitive financial and personal information.
>
> **Jim O’Rourke,**
> **Director of Business Development, ICG Innovations**

Business Challenges

- Increase visibility into cloud infrastructure and enhance reporting.
- Gain cost and staffing efficiencies to compete with larger consulting firms.
- Add value to business relationships by improving intelligence and focusing resources on clients’ biggest security challenges.

CHALLENGES

Scaling Open Source To Address Customer Demand

Early in its cloud journey, ICG Innovations partnered with AWS. “For our size, it’s important to have strategic partners who help us, like AWS,” explained O’Rourke. Additionally, during the initial move to the cloud, the company leveraged Falco security rules for visibility into its user logs, services, and activity within its Kubernetes environment.

“Between AWS and Falco, we had a strong multi-level security strategy to help ensure we had security shored up across a compliant network,” said Marcus Boelter, Senior Technical Consultant at ICG Innovations. “As we scaled, Sysdig was the natural next step for us — between the strength of the Sysdig technology based on Falco and its partnership with AWS, we knew we could deliver even more quickly by adopting Sysdig.”

Boelter added that, “By the nature of Kubernetes with its constant updates, it was difficult to understand how we were dealing with logs. As services were created, pods would ramp up and drop off, and having a steady stream of alerts made security unwieldy as we grew. Adding Sysdig Secure enabled us to cut through a significant portion of complexity, and with its highly tuned detection engine, helped us focus on what’s important.”

SOLUTIONS

Prioritizing Vulnerabilities

Being a boutique firm, ICG Innovations needs to focus its resources on its customers and developing applications that make money. It can’t be wading through a massive number of alerts and fine-tuning them. Additionally, in the event of an issue, ICG Innovations needs information on containers that are no longer around. Sysdig Secure and Sysdig Monitor proved to have the right capabilities out-of-the box, while enabling rapid customizations according to the needs of each of ICG Innovations’ clients. Sysdig’s SaaS deployment and pre-built policies helps speed up the deployment, accelerating time to value.

“With previous solutions, we had a lot of alerts that forced us to spend more time triaging what was important and what wasn’t,” said Boelter. “Sysdig enables us to autotune the solution to focus on the most pressing issues, filter our rules, and reduce the burden of alert fatigue. Within the first few weeks, we achieved a 30% reduction in alerts without sacrificing security.”

> “Within the first few weeks, we achieved a 30% reduction in alerts without sacrificing security.
>
> **Marcus Boelter,**
> **Senior Technical Consultant, ICG Innovations**

Since onboarding Sysdig, the ICG Innovations’ security team now receives less than 30 alerts per day. And with the increased visibility across its cloud, container, and hosts with Sysdig Secure and Sysdig Monitor, the team can quickly identify issues at a node,

Better Capacity Planning Saves up to 15% On Cloud Bill

When setting ingress rules for inbound traffic, ICG Innovations uses a combination of AWS and Sysdig Monitor to view how efficient pods are within a cluster and ensure its cloud resources are appropriately allocated. “By making sure that the pod is the right-size, we can drop up to four nodes per account,” said Boelter. “Sysdig and AWS help us save up to 15% on cloud resources – we can pass those savings directly through to our customers, as well as stay competitive with larger companies.”

> “Sysdig and AWS help us save up to 15% on cloud resources – we can pass those savings directly through to our customers, as well as stay competitive with larger companies.
>
> **Marcus Boelter,**
> **Senior Technical Consultant, ICG Innovations**

The added level of transparency and flexibility provided by its security team has also enabled the company to scale more rapidly without adding headcount. With the new security, monitoring, and reporting automations available through Sysdig, current analysts are able to secure and monitor client environments. In contrast, using other solutions may have required up to two additional staff members to perform the same function.

Tool Consolidation

Image scanning within Sysdig, in tandem with AWS Elastic Container Registry (ECR), also helps streamline ICG Innovations' continuous integration and continuous delivery (CI/CD) pipeline as its customers deploy new applications to the cloud. Previously, the company used up to five different resources to scan images. Not only is the process now working more efficiently, the company gets weekly reporting on potential issues so it can quickly address vulnerabilities.

> "With Sysdig, we went from five different tools to scan images, down to one. This saves us four hours per week while increasing our releases by 10% per week, without increasing our team size.
>
> **Marcus Boelter,**
> **Senior Technical Consultant, ICG Innovations**

Continuously Validating Compliance

Compliance is an important factor for ICG Innovations. "We were able to easily implement the out-of-the-box rules to ensure we meet National Institute of Standards and Technology compliance," said Boelter.

Substantiating the company is compliant is another challenge when working with highly regulated companies. As ICG Innovations reviews policies and alerts, as well as scanned images and detected threats, information is logged into a centralized reporting suite. The team then uses these reports to show proof of compliance across its environments, including System and Organization Controls (SOC) compliance. This provides transparency into ICG Innovations' security and gives clients peace of mind.

To learn more about ICG Innovations, visit icginnovations.com.

ICG INNOVATIONS
DRIVING EFFICIENCY

INDUSTRY

Software Technology

INFRASTRUCTURE

Amazon Web Services (AWS)

ORCHESTRATION

Amazon Elastic Kubernetes Service (EKS)

SOLUTION

Sysdig Secure, Sysdig Monitor

About Sysdig

Sysdig delivers cloud security the right way with open Sysdig delivers cloud security the right way with open innovation, agentic AI, and the uncompromising truth of runtime. In a world of black boxes and blind spots, Sysdig helps security and development teams prevent, detect, and respond to threats in the moment.

AI is only as powerful as the signals it receives, and Sysdig Sage™ – the first agentic AI analyst for cloud security – is fueled by the deepest runtime intelligence in the industry. It doesn't just observe. It reasons and acts with the context, speed, and precision that modern teams need to build and defend innovation in real time. Founded by the creators of Falco and Wireshark, Sysdig is trusted by more than 60% of the Fortune 500 and is built for those who refuse to compromise on security.

To learn more about Sysdig, visit sysdig.com.

GET A DEMO →

sysdig

CUSTOMER STORY

COPYRIGHT © 2022-2026 SYSDIG,INC.
ALL RIGHTS RESERVED.
CS-ICG REV. D 01/26