ICG Consulting Leverages Sysdig and AWS To Compete With Major Shops

Company Details

ICG Consulting is a cloud-hosted vendor management and back office solution for leading companies, including Duke Energy, US Foods, and Love's Travel Stops. The company provides vendor portals, web invoicing, workflow management software, and dynamic discounting along with other solutions to help businesses communicate, collaborate, and transact.

Sysdig Solutions

Sysdig Secure, Sysdig Monitor

Infrastructure

Amazon Web Services (AWS)

Orchestration

Amazon Elastic Kubernetes Service (EKS)

ICG CONSULTING
BUSINESS PROCESS SOLUTIONS

Since 1990, ICG Consulting 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 Consulting 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.

Challenges

- Reduce noise and alert fatigue
- Accelerate time to identify and fix critical vulnerabilities
- Reduce risk without slowing down development
- Support journey to maturity from on-prem environments to the cloud
- Empower a small team with more robust security and monitoring capabilities without adding overhead

Business Impact of Sysdig

- 15% cost savings in cloud resources
- 30% reduction in alerts without sacrificing security
- 10% weekly increase in release pace
- Consolidated 5 tools down to 1
- Through automation, eliminated need to hire up to two additional analysts

"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 Consulting.

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

> **"Between AWS and Falco, we had a strong multi-level security strategy to help ensure we had security shored up across a compliant network. 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."**
>
> **Marcus Boelter,**
> Technical Consultant at ICG Consulting

"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."

Scaling Open Source To Address Customer Demand

Early in its cloud journey, ICG Consulting partnered with Amazon Web Services (AWS) because, "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, Technical Consultant at ICG Consulting. "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."

Prioritizing Vulnerabilities

Being a boutique firm, ICG Consulting 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 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's clients. Sysdig's SaaS deployment and pre-built policies within Sysdig Secure helped 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 enabled 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."

Since onboarding Sysdig, the ICG 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, pod, and user level to better understand the nature of the alert.

Better Capacity Planning Saves up to 15% On Cloud Bill

When setting ingress rules for inbound traffic, ICG Consulting uses a combination of AWS and Sysdig Monitor to view how efficient pods are within a cluster and make sure that 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."

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.

> **"You are able to autotune Sysdig, which enables us 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."**
>
> **Marcus Boelter,**
> Technical Consultant at ICG Consulting

Tool Consolidation

Image scanning within Sysdig Secure in tandem with AWS ECR also helps to streamline ICG Consulting's 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,**
> Technical Consultant at ICG Consulting

"With Sysdig, we went from five different tools to scan images, down to one," said Boelter. "This saves us four hours per week while increasing our releases by 10% per week, without increasing our team size."

Continuously Validating Compliance

Compliance is an important factor for ICG Consulting. "We were able to easily implement the out-of-the-box rules to ensure we meet NIST compliance," said Boelter.

Substantiating the company is compliant is another challenge when working with highly regulated companies. As ICG Consulting 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 SOC compliance. This provides transparency into ICG Consulting's security and gives clients peace of mind.

Visit www.icgconsulting.com to learn more about ICG Consulting.

To learn more about Sysdig, visit www.sysdig.com or to try a free trial:

START FREE TRIAL

sysdig