# Goldman Sachs: Accelerating Business With Microservices

## Company Details

**The Goldman Sachs Group** is a leading global financial institution that delivers a broad range of financial services to a large and diversified client base that includes corporations, financial institutions, governments and individuals. Founded in 1869, the firm is headquartered in New York and maintains offices in all major financial centers around the world.

## Industry

Financial Services

## Sysdig Solutions

Sysdig Secure, Sysdig Monitor

## Infrastructure

Amazon Web Services (AWS), Google Cloud Platform (GCP), On-Prem, Private

Goldman Sachs

For Goldman Sachs, speed of software innovation is critical. The ability to be competitive relies on a talented team with software applications that help deliver insights to clients. The engineering division at Goldman Sachs is on the front lines of ensuring the professionals at the firm have the tools necessary to advise customers as the global economy changes.

With this in mind, Goldman Sachs has adopted DevOps principles and microservices to deliver containerized applications at scale across on-premises and cloud environments. As a result of this transformation, Goldman Sachs has accelerated software delivery velocity from one build every two weeks to over a thousand per day.

In the firm's adoption of microservices, Goldman Sachs invested in Sysdig to fuel the company's growth in offering host and container monitoring and security solutions.

## Challenges

While speed is a key objective, Goldman Sachs cannot compromise compliance and security. As part of a highly regulated industry, the firm needs a way to ensure it monitors its containerized applications and data. Furthermore, as the business runs on software, performance and availability are fundamental.

## Solutions

Sysdig plays a key role in helping cloud teams at Goldman Sachs successfully monitor microservices at scale. With Sysdig, Goldman Sachs is able to:

- Optimize performance and availability of business-critical services
- Accelerate incident response and troubleshooting

Cloud-native technology has enabled Goldman Sachs to significantly increase the efficiency of its DevOps teams. Using containers, the firm has accelerated software development, automated business continuity, and simplified infrastructure management. At the same time, security and compliance processes have had to change to be effective. Goldman Sachs cannot run its business without the right tools to ensure visibility.

> **"At our scale, it is important to have a complete record, even if the containers last only a few seconds. We need to be able to capture this data at scale to conduct not only forensics investigations, but also security audits."**
>
> **Wes Williams,**
> Global Head of Security Incident Response at Goldman Sachs

"With a highly dynamic environment that spans cloud providers and on-premises data centers, security, monitoring, and troubleshooting took on a whole new dimension," relates Chetan Mehendiratta, Vice President of Engineering at Goldman Sachs.

"Our charter is to optimize and secure the services running in our environment. We need, for instance, to understand communication patterns and cluster usage, to identify bad behavior and security events, and to know if an application is under- or over-utilized. To achieve these goals, we not only need detailed telemetry, but we need application context. This is a hard problem to solve."

Goldman Sachs engaged Sysdig in late 2016, embarking on a rigorous technology evaluation to determine a fit for the firm's unique set of requirements. Goldman Sachs found that Sysdig enabled the necessary visibility needed while integrating security and compliance into the company's DevOps workflows. With Sysdig, the firm is able to address dozens of use cases spanning monitoring, troubleshooting, scanning, compliance, threat detection, and auditing, all at massive scale. In addition, Goldman Sachs deploys Sysdig to monitor and secure its environment at scale and supports a population of more than 9,000 developers.

## Monitoring Applications at Massive Scale

With a highly dynamic and massively scalable multi-cloud environment, the central monitoring team at Goldman Sachs uses **Sysdig Monitor** to auto-detect and monitor hosts, containers, and orchestrators. The team can easily identify applications and containers across on-premises and public clouds. The telemetry gathered spans application, infrastructure, and process-level activity at an unprecedented scale, polling millions of containers per second.

Armed with a rich set of data, Goldman Sachs is able to build custom service connection maps that identify containers and processes that belong to a particular application and detail which services communicate with other services. In addition, these maps are enriched with granular activity data that helps identify and troubleshoot issues across the stack.

## Identifying Rogue Connections and Top Talkers Across Clouds

With Sysdig, the monitoring team tracks millions of network connections between entities, data centers, regions, and clouds, and then attributes network usage to containers. Knowing which processes and containers are top talkers helps Goldman Sachs more effectively:

- Isolate applications using the most network data
- Identify rogue connections that could indicate a security violation
- Attribute container processes to network usage for better capacity planning
- Perform troubleshooting to maximize availability

## MITRE ATT&CK Detections for Cloud-Native Environments

With **Sysdig Secure**, Goldman Sachs has access to security detection policies and complete visibility into process, file, network I/O, and user activity. Both out-of-the-box and customizable rules help Goldman Sachs detect common misbehaviors and potential indicators of compromise. In addition, the security team is able to take advantage of community-driven rules as well as the latest detections made available by the Sysdig threat research team.

Part of any good security strategy involves aligning the security team to a standard. The Goldman Security Incident Response Team (SIRT) used the MITRE ATT&CK framework to align detection strategies and compare tools during its selection process.

"Security is driven around best practices and we needed a way for our teams to efficiently apply MITRE ATT&CK practices that are integrated into our day-to-day security processes," explains Wes Williams, Global Head of Security Incident Response at Goldman Sachs.

Goldman Sachs evaluated existing logging tools as well as open source solutions, including Falco, the open source cloud-native runtime security project originally created by Sysdig. After its evaluation, the SIRT concluded that logging could not sufficiently support the set of detections required.

Goldman found that Sysdig Secure, based on Falco, expanded the company's ability to detect incidents and use granular data with context to quickly respond. Robust detection that minimizes the noise of false positives improved the team's efficiency and confidence.

> **"With a highly dynamic environment that spans cloud providers and on-premises data centers, security, monitoring, and troubleshooting took on a whole new dimension. Our charter is to optimize and secure the services running in our environment. We need, for instance, to understand communication patterns and cluster usage, to identify bad behavior and security events, and to know if an application is under- or over-utilized. To achieve these goals, we not only need detailed telemetry, but we need application context. This is a hard problem to solve."**
>
> **Chetan Mehendiratta,**
> Vice President of Engineering
> at Goldman Sachs

## Auditing and Forensics Records for Ephemeral Workloads

Data collected by Sysdig for audit and forensics is a critical enabler of Goldman's strategy. These data sources allow analysts to see user and system activity from the moment an event occurred. This includes executed user commands, every network connection established or attempted, and the ability to drill down into any I/O activity, even if the host is no longer running. In the future, the SIRT plans on utilizing Sysdig Secure to monitor containers in addition to current host monitoring for compliance and security events.

> **"Security is driven around best practices and we needed a way for our teams to efficiently apply MITRE ATT&CK practices that are integrated into our day-to-day security processes."**
>
> **Wes Williams,**
> Global Head of Security Incident Response at Goldman Sachs

"At our scale, it is important to have a complete record, even if the containers last only a few seconds," explains Williams. "And we need to be able to capture this data at scale to conduct not only forensics investigations, but also security audits."

The incident response team extracts immediate value through 30+ built-in detections provided by Sysdig Secure. The Sysdig data ensures that Goldman Sachs has a complete record of activity and is able to reconstruct events at a granular level for audit purposes.

Visit www.goldmansachs.com to learn more about Goldman Sachs.

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

START FREE TRIAL

sysdig


CS-GOLDMANSACHS Rev. C 5/23