

Sysdig Secure DevOps Platform



Unified visibility and security to confidently run containers, Kubernetes, and cloud.

Why Sysdig?

- **Cloud Security** – Assess security posture, flag misconfigurations, and detect suspicious activity.
- **Kubernetes Security** - Secure containers and Kubernetes in public and hybrid clouds.
- **Image Scanning** – Automate scanning locally in CI/CD pipelines, registries, and hosts.
- **Runtime Security** – Detect and respond to threats with out-of-the-box and custom policies.
- **Continuous Compliance** – Validate compliance against standards like PCI, NIST, ISO, HIPAA, and SOC2.
- **Monitoring & Troubleshooting** – Scale monitoring with full Prometheus compatibility.
- **Incident Response & Forensics** – Capture activity to identify the cause and impact of issues.



Overview

Sysdig Secure DevOps Platform helps teams secure the build, while detecting and responding to threats. It also continuously manages configurations and compliance, and monitors containers, Kubernetes, and cloud services. Sysdig is a Software-as-a-Service (SaaS) platform that provides deep visibility across workloads and cloud infrastructure.

Product features

Security Built on Open-Source

Container and cloud security built on open-source innovation:

- Unify threat detection and response using Falco and Sysdig.
- Continuously assess security configurations and detect threats using Cloud Custodian and Falco.
- Enforce compliance and governance via policy-as-code based on Open Policy Agent (OPA).
- Scale Kubernetes monitoring with full Prometheus compatibility.

Deep Visibility Across Containers and Cloud

Alert on threats, operational issues, and compliance risks:

- Gain deep visibility across hybrid and multi cloud environments.
- Scan for vulnerabilities pre-deployment and at runtime.
- Assess runtime drift, threats and performance issues with rich context and auto-remediate .

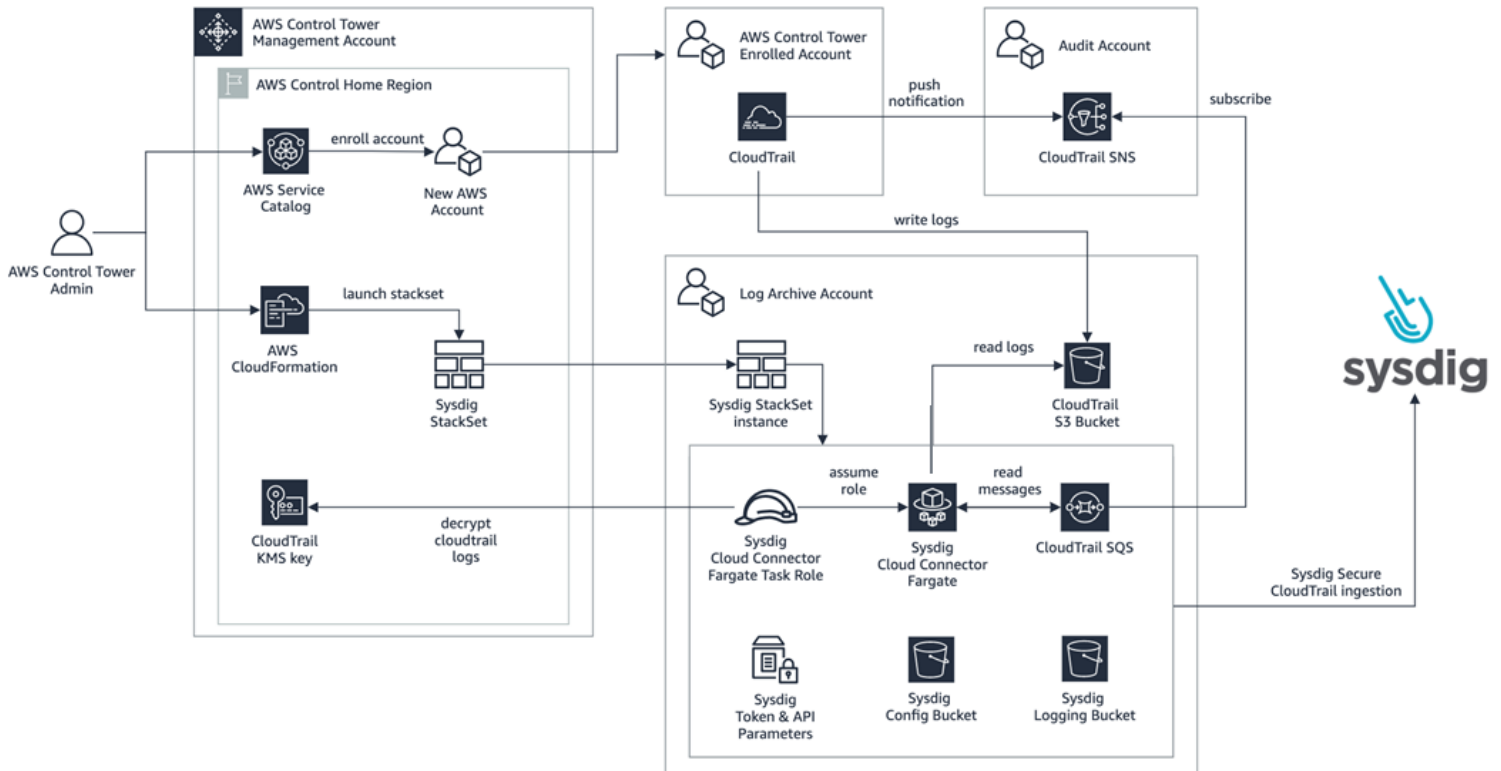
Radically Simple to Run and Scale

Simplify operations with SaaS delivery and curated workflows:

- Scale up as you grow without worrying about backend data management.
- Dig deep with lightweight, yet powerful, instrumentation for containers, Kubernetes and cloud.
- Easy integration with your DevOps tools and processes.

How it works

Sysdig Secure integrates with AWS Control Tower to enable visibility, security and compliance for containers, Kubernetes, and cloud services in multi-account AWS environments. The solution automatically provisions the Sysdig Secure Cloud Connector to ingest CloudTrail logs from existing and newly added AWS accounts. Sysdig Secure policies automate detection of unexpected and unwanted behavior. Together, AWS Control Tower and Sysdig help ensure that your accounts conform to security and compliance best practices.



Differentiators

- Radically simple SaaS-based approach simplifies deployment, management, and scaling.
- Out-of-the-box policies for threat detection and compliance save time and reduce risk.
- Unified visibility across cloud and containers helps teams respond to threats faster.

What our customers are saying

LogDNA Delivers Higher Uptime and Improved Customer Experience

Challenges

LogDNA realized they needed better visibility and security for their AWS environment. Their DevOps team realized managing Prometheus servers was time consuming, there was a lack of alerting before an event impacted the customer experience, and there were no audit trails for debugging and troubleshooting.

Solution

The implementation of Sysdig improved LogDNA's customer experience by reducing the time to resolve performance issues and provided improved efficiency for compliance and audit processes.

Benefits

- Ability to catch customer-impacting events 98% of the time
- Dashboards help to understand what is going on in the environment
- Audit trails for efficient troubleshooting and compliance reporting
- Fast ramp with dashboard and alert creation across all environments
- Minimal maintenance effort

“ *There is no better choice than Sysdig to meet our monitoring and security needs. Sysdig reports on our entire AWS infrastructure, including infrastructure and application events.* ”

Ryan Staatz, Systems Architect, LogDNA



About LogDNA

LogDNA is a centralized log management solution that empowers DevOps teams with the tools that they need to develop and debug their applications with ease. They help thousands of companies, from startups to large enterprises, take control of their data and gain valuable insights from their logs.



About Sysdig

Sysdig enables companies to confidently run cloud-native workloads in production. With the Sysdig Secure DevOps Platform, cloud teams embed security, maximize availability, and validate compliance. The Sysdig platform is open by design, with the scale, performance, and usability enterprises demand.

Additional Resources

- [Sysdig Secure Product Page](#)
- [Continuous Cloud Security with Sysdig](#)
- [Sysdig Cloud Connector](#)
- [Guide: Continuous Cloud Security on AWS](#)