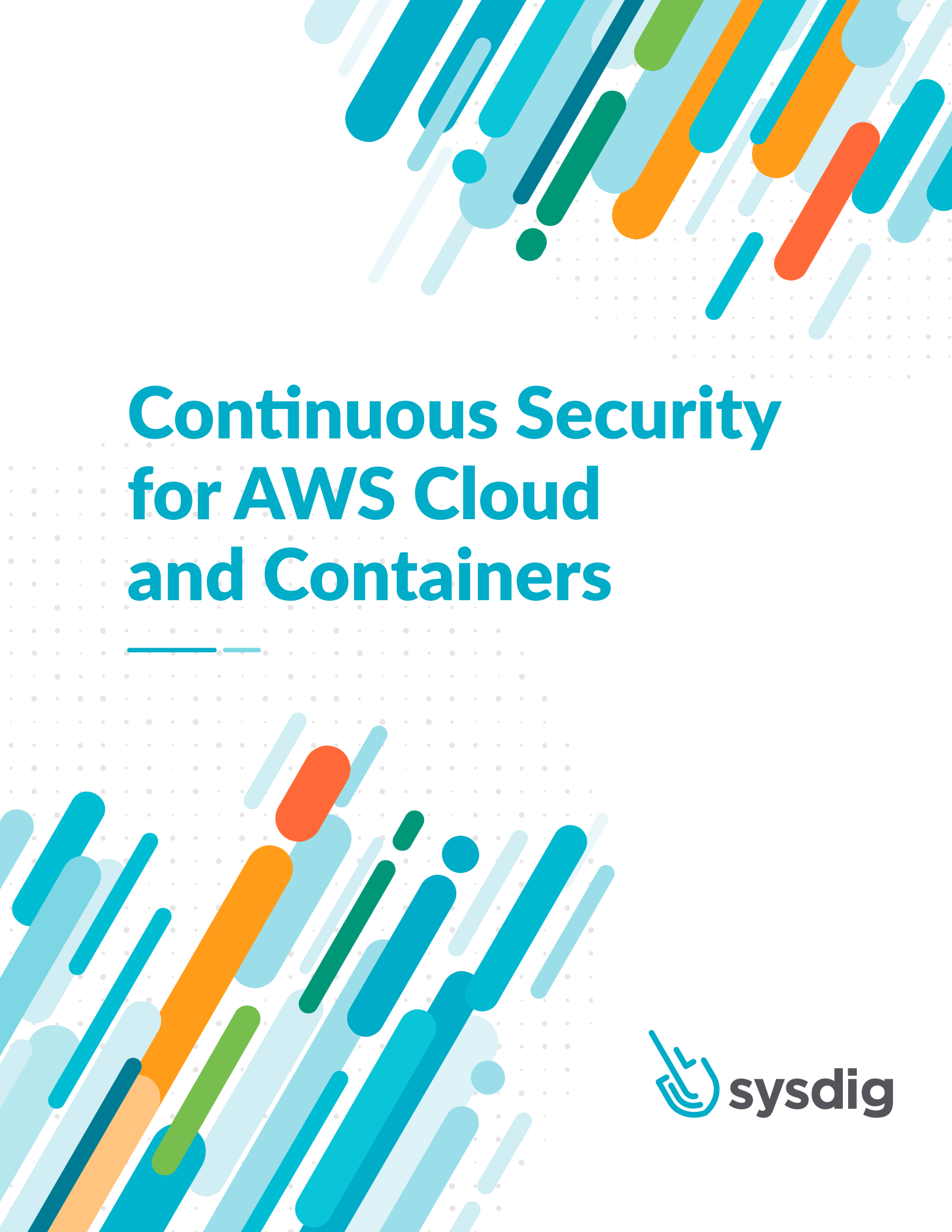
Continuous Security for AWS Cloud and Containers



Contents

Continuous Security for AWS Cloud and Containers

Speed, agility, and scalability are no longer “nice to haves” for IT leaders. These are now core to the way modern organizations operate, and it is critical for CIOs to ensure they have a modern foundation that enables them to quickly move and innovate.

Delivering on these demands is happening on the back of public clouds, which provide the dynamic environment that supports these needs. It’s also facilitated with container application development and DevOps approaches that allow development teams to rapidly spin up software, make adjustments, and continuously deliver solutions that meet customer and market needs.

These changes are not just about business practices in a digital format. The fundamental aspects of the cloud and containers are enabling an entirely new way of doing business.

For all of this to happen, companies need complementary security that can keep pace with the speed and agility of the cloud and containers, but don’t slow down the very processes that deliver faster results. This duality in goals – accelerating delivery while ensuring security – demands an approach that both protects data and workloads, and facilitates agile application development. In other words, make it safe but don’t slow it down.

New paradigms like containers, microservices, and hybrid cloud workloads disrupt the way enterprises implement security. Containers provide great portability and isolation, making them ideal for moving applications from development to production. As enterprises move from initial sandbox to production deployments, they face challenges establishing cloud security and compliance processes, as well as operating containers securely and reliably. Deploying workloads in the cloud involves complex interactions among microservices. Serverless instances function as fluid architectures, changing every few minutes or seconds to create a constantly changing security environment. Use of these new solutions enable business to move fast, but present a new set of potential threats.

Cloud teams are increasingly adopting Amazon Web Services (AWS) cloud and container services, including Amazon ECS, Amazon EKS, and AWS Fargate, to deliver applications faster at scale. Along with the roll-out of architectures with containers and orchestration, what’s needed to stay on top of the security, performance, and health of applications and infrastructure has shifted.

The Sysdig Secure DevOps Platform provides security to confidently run containers, Kubernetes, and cloud. With Sysdig, you can secure the build, detect and respond to threats, and continuously validate cloud posture and compliance. In addition, our solutions will help you maximize performance and availability by monitoring and troubleshooting cloud infrastructure and services. At Sysdig, we provide a SaaS platform, built on an open-source stack that includes Falco and sysdig OSS, the open standards for runtime threat detection and response.

By creating a secure Devops workflow that integrates security, compliance, and monitoring, organizations can accelerate deployment and confidently run container and cloud workloads in production on AWS with Sysdig. This allows you to:

- Speed up deployment by validating security policies and configurations during the build process.
- Continuously assess cloud security posture and compliance.
- Stop runtime threats without impacting performance.
- Prevent issues by monitoring performance and health across infrastructure, services, and applications.
- Conduct incident response using detailed records.

This guide offers a framework for establishing comprehensive cloud and container security for AWS environments with specific recommendations for how Sysdig can complement and enhance native AWS tools.

Why security and visibility are top of mind for AWS customers

There are three key elements to AWS security that are critical to the protection of data, applications, and cloud infrastructure.

Sharing responsibility for security

In a public cloud like AWS, security is a shared responsibility. AWS handles the security OF the environment while the customer is responsible for everything that happens WITHIN the environment. AWS delivers out-of-the-box security features like user authentication, Amazon Simple Storage Service (S3) bucket monitoring, and logging and monitoring with AWS CloudTrail. However, users must also consider how they will identify and remediate misconfigurations, known vulnerabilities, and behavioral anomalies across their workloads.

Continuous cloud change requires continuous monitoring. That monitoring must function across all cloud and orchestration activities to provide visibility into in-use cloud assets and audit settings. It also has to perform continuous scanning and analysis of cloud and container activity to manage health and security risk.

Automating to move fast and scale securely

Security and DevOps teams have to validate that security controls are actually working as intended, but also aren't slowing down development efforts. Many enterprises perform manual checks for this, but that's simply not scalable. Automation is the only way to do this effectively, so companies require tools that can analyze cloud activity without manual processes to help you understand if things are operating as expected, even in the largest deployments.

With an automated approach, cloud activity can be analyzed and interpreted, and DevOps and security teams can be alerted about abnormal behavior within their AWS environment. This helps you address vulnerabilities and issues before they are exploited, slow down your development process, and impact your business applications.

Optimizing for development and container orchestration

AWS offers two important container services, Amazon Elastic Kubernetes Service (EKS) and Elastic Container Service (ECS). Each functions as a comprehensive container orchestration system. They are designed to optimize development, operations, and security processes that support the secure creation and deployment of containerized workloads, and help accelerate container application deployment. Along with ECS and EKS, you can also use the AWS Fargate serverless compute engine for containers.

In these orchestrated application environments, legacy security tools no longer work as they can't see inside containers, handle the dynamic nature of Kubernetes, or scale across clusters, availability zones, and regions. What's needed is a container and cloud security stack built for containers, Kubernetes, and cloud that integrates into your DevOps workflow.

Addressing the unique needs of different AWS users

Your organization's teams and roles will have different concerns and points of view on visibility and security, as well as which processes are required to move workloads into production.

Developers

AWS helps developers take advantage of cloud services, containerized applications, and orchestration without having to know the underlying infrastructure details. AWS continuous integration and continuous delivery (CI/CD) pipelines streamline the process of building, distributing, and deploying containerized applications. Using AWS frameworks like AWS CodeBuild and AWS CodePipeline for combining source code and base images, developers can push changes to a repository such as GitHub. AWS container services will create a container image from the source code and push it to a registry like Amazon Elastic Container Registry (ECR). Ensuring container images are free of known vulnerabilities and follow security best practices is a major challenge that often compromises application integrity and can slow down release schedules.

Cloud/DevOps

Cloud and DevOps teams are responsible for maintaining high availability, quality of service, health, and performance of applications and infrastructure. Users leverage the built-in AWS web console to manage the infrastructure and platform capabilities, and also rely on playbooks to automate application deployments. DevOps teams are required to ensure that they build security into the platform with features like Falco (the open-source cloud native runtime security project), Pod Security Policies, network policies, and more.

Security and compliance

Security operations, SecOps, DevSecOps, and CSIRT teams adhere to the cloud's shared responsibility model. However, to be effective at preventing threats, identifying risk, and isolating vulnerabilities, security teams need to continuously monitor AWS cloud and container environments to protect against anomalous behavior and zero-day attacks, as well as perform incident response if a violation occurs. Security teams also set policies based on compliance frameworks and internal requirements, and apply those to the various resources operating in the AWS environment. In addition, security teams must identify and monitor new cloud infrastructure and applications that are deployed to ensure they conform with regulatory and internal compliance requirements.

Managing security and visibility on AWS container services with Sysdig

With unified security, compliance, and monitoring, you can confidently build and run cloud-native workloads on AWS container services in private, hybrid, and multi-cloud environments. By automating these critical capabilities for a secure DevOps workflow, teams can maximize performance, increase agility, optimize data integration across apps and other data repositories, manage security risk, and ship cloud applications faster.

AWS container services provide a baseline coverage for security and monitoring across the entire container platform -- workloads, accounts, users, and all the interactions happening within the AWS environment. As you scale out the number of applications, clusters, locations, and cloud providers, Sysdig extends AWS container services, providing additional security and monitoring capabilities to:

- Secure the build pipeline
  - Automate scanning within CI/CD pipelines and registries.
  - Consolidate container and host scanning.
  - Efficiently flag vulnerabilities and identify owners.
  - Block vulnerable images from being deployed.
- Detect and respond to runtime threats
  - See all threats with Falco, the open standard for detection, and implement zero-day threat detection.
  - Prevent lateral movement with Kubernetes network policies.
  - Conduct incident response using detailed records.
  - Get deep runtime visibility into cloud and container services including Fargate, ECS, and EKS.
- Continuously manage cloud posture and compliance
  - Identify misconfigurations and compliance violations at build and runtime.
  - Monitor account and access security at the individual and group levels.
  - Measure progress with detailed reports.
  - Save time with out-of-the-box policies for PCI, NIST ,and SOC2.
- Monitor containers, Kubernetes, and cloud services
  - Prevent issues by monitoring performance and capacity.
  - Accelerate troubleshooting using granular data.
  - Scale Prometheus monitoring across clusters and clouds.
  - Audit container activity and accelerate incident response.

At Sysdig, we provide the only comprehensive, unified platform that features cloud and container security and monitoring. Incorporating the capabilities of a Cloud Workload Protection Platform (CWPP) with Cloud Security Posture Management (CSPM), as well as

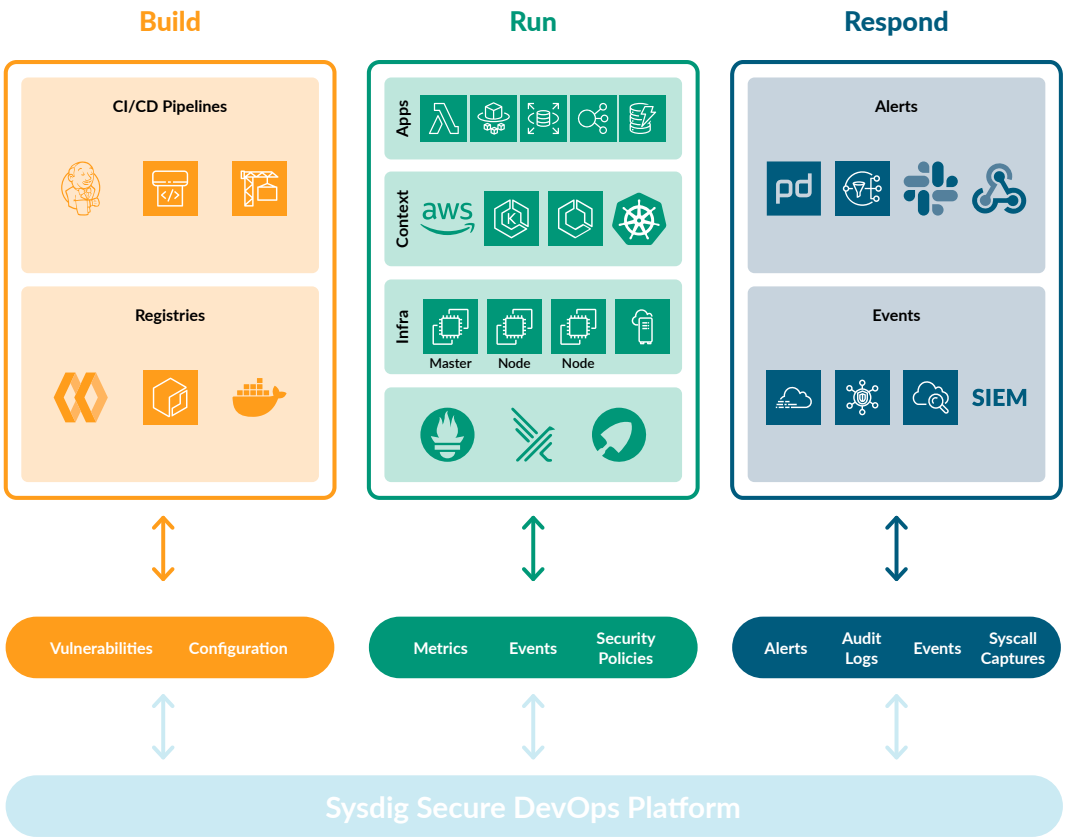
health and performance observability, we equip DevOps and Security teams with a single source of truth across cloud workloads, accounts, containers, and Kubernetes.

These tools operate as a unified security and visibility layer over AWS environments to eliminate silos of information that exist across operations, development, DevOps, and security teams. At Sysdig, we enable security and DevOps teams to accurately identify and triage incidents, quickly determine cause, and perform forensics even for container workloads that are no longer running.

Using the Sysdig platform, security and DevOps teams can report on security issues across the entire AWS environment, including suspicious user behavior, threats to data, and vulnerabilities affecting running images in specific namespaces and clusters. For example, if a new vulnerability is reported, Sysdig can help your DevOps teams quickly identify the affected images in a particular public cloud (AWS) region, namespace, cluster, etc., as well as the team that owns the fix. With this approach, you can resolve issues quickly by analyzing vulnerabilities and granular system data automatically correlated to both cloud and Kubernetes contexts.

We help you deliver reliable and secure cloud applications and provides centralized visibility and security for operating AWS container services at scale. Sysdig is a SaaS-first platform, hosted in AWS. With a single agent deployed per EC2 instance, the Sysdig platform can scale to 10,000+ nodes to secure and monitor containers and applications running on AWS container services clusters.

You can get started quickly with guided onboarding, out-of-the-box dashboards, and curated workflows. Because Sysdig plugs into your cloud environment and existing DevOps workflow using automation and out-of-the-box integrations, visibility and security controls won't slow you down.



Sysdig provides container and orchestration insights for AWS container services by using the following:

- ImageVision™ identifies and prevents images with vulnerabilities or misconfigurations from being shipped.
- ContainerVision™ gives request-level visibility inside your containers and across microservices. It provides in-depth metrics and events without invasive instrumentation.
- ServiceVision™ integrates with ECS and EKS to automatically enrich all of your metrics and events with orchestration metadata.
- CloudVision™ enables a consolidated view of cloud activity using cloud logs.

Securing AWS container services

Let's look at the various security controls provided by AWS and how Sysdig extends security, compliance, and monitoring for AWS solutions across the cloud native stack and container lifecycle.

AWS provides security capabilities including:

- Secure hosting infrastructure with Amazon EC2, Amazon Linux 2, and Bottlerocket.
- Access Control with AWS Identity and Access Management (IAM).
- Image scanning with Clair on Amazon ECR.
- Compliance enforcement with AWS Config.

Host security

Cloud security is the highest priority for AWS. Customers benefit from a datacenter and network architecture built to meet the requirements of the most security-sensitive organizations. As a managed service, Amazon EC2 is protected by AWS global network security procedures.

AWS recommends using a layered approach that includes host-based controls for EC2 instances, which can restrict access to the environment. Typically, an enterprise will employ a host-based intrusion detection system (HIDS) that monitors and analyzes network traffic, host-level access, and corresponding log files. Amazon CloudWatch is a standard solution to collect and distribute alerts from a HIDS.

AWS provides...

To securely operate containers on AWS, Amazon offers secure, stable, and high-performance operating systems to run cloud-native applications. This includes Amazon Linux 2 and Bottlerocket.

- **Amazon Linux 2** is the next generation of Amazon Linux that is secure by default. It reduces the number of non-critical packages, limiting exposure to potential security vulnerabilities. With Amazon Linux 2, security updates rated "critical" or "important" are automatically applied on the initial boot.
- **Bottlerocket** is a Linux-based, open-source operating system that is purpose-built by AWS to run containers on virtual machines or bare metal hosts. Bottlerocket includes only the essential software to run containers, which improves resource usage, reduces security attack surface, and lowers management overhead. In Bottlerocket, security updates can be automatically applied as soon as they are available in a minimally disruptive manner, and can be rolled back if failures occur.

In addition to enabling secure operations in the cloud, these solutions can also be utilized in on-premises facilities using AWS Outposts. Sysdig has validated its security, monitoring, and compliance capabilities with both Amazon Linux 2 and Bottlerocket in public, private, and hybrid deployments. This ensures customers can securely and consistently run container workloads in production using these solutions with Amazon EKS and ECS.

Sysdig adds...

Sysdig provides host scanning to help you detect package vulnerabilities on virtual and physical server or cloud-native host instances. Detailed reports will help your operational teams understand what needs to be patched to avoid incidents like breaches or zero-day vulnerabilities.

Sysdig Secure provides detection for host OS and non-OS packages and reduces time-to-fix by assessing impact and ownership using rich cloud and Kubernetes context. A single vulnerability management solution for hosts and containers will help you reduce risk, keep pace with regulatory requirements and compliance, and save time by consolidating workflows.

Authentication and authorization

AWS Identity and Access Management (IAM) gives admins the ability to securely access, integrate with, and interact with AWS services. This allows enterprises to give permission to individuals and groups; from a centralized source, admins can allow and deny access based on role, organization, geography, or any other category that is relevant to maintaining security for workloads and other resources.

Users access various services through requests based on their AWS credentials. However, for some resources like S3 storage, granular-level permission can be granted to provide unique access to only that source. The request context is evaluated based on policies that AWS users apply to their environment. Policies are stored as JSON documents and operate as the de facto source for permissions.

Specific access to AWS services is provided through standard interfaces including the Web UI, CLI, and APIs. Additionally, services interact with AWS container services so they can be aware of their orchestration state and execute actions against these platforms. Imagine a CI/CD pipeline pushing a new deployment into production. How do you control and measure who can do what?

AWS provides...

AWS IAM enables you to manage access to AWS services and resources securely. Using IAM, you can create and manage AWS users and groups, and use permissions to allow or deny access to AWS resources. IAM administrators control who can be authenticated (signed in) and authorized (have permissions) to use EKS, ECS, and Fargate resources.

Sysdig adds...

With Sysdig, you can define who can access any of the visibility, metrics, notifications, and security policies for your AWS container services. This is known as Sysdig Teams, introducing the concept of service and metadata-based access control to complement the existing AWS IAM mechanisms.

With Sysdig Teams, administrators can define groups of users that have access to a specific service or limited set of services deployed on AWS. For example, an application owner might only see vulnerability scan results of images in a specific namespace. Limiting the exposure with access controls and providing a default configuration for each specific team helps streamline security information for users and teams.

Sysdig supports role-based access controls (RBAC) to define user privileges and provides federated access control across different teams in an organization. In addition to the admin role, a variety of access roles are available, including View Only, Standard User, Advanced User, and Team Manager.

Image scanning

Container applications and infrastructure components are built on top of readily available packages, many of which are open-source software that might contain old library versions. It's important to know where these packages originally came from, who built them, and whether there are any known vulnerabilities inside them.

AWS provides...

Amazon Elastic Container Registry (ECR) is a fully-managed Docker container registry that makes it easy for developers to store, manage, and deploy Docker container images. Amazon ECR is integrated with AWS container services like ECS and EKS, simplifying your development to production workflow.

As users begin adopting containers on AWS takes, ECR scanning is the first step towards delivering continuous security and compliance. ECR uses the Common Vulnerabilities and Exposures (CVE) database from the open source Clair project to provide you with a list of scan findings. You need to ensure you are scanning your images pulled from ECR for both vulnerabilities and misconfigurations so you don't push applications running on AWS that are exploitable.

Sysdig adds...

Sysdig Secure embeds security and compliance across all stages of the Kubernetes lifecycle. Leveraging 15+ CVE threat feeds, Sysdig Secure provides a single workflow to detect vulnerabilities and security or compliance-related misconfigurations. As your teams build applications, Sysdig prevents vulnerable images from being pushed through your CI/CD pipeline and identifies new vulnerabilities in production.

Sysdig Secure provides additional ECR scanning capabilities that extend beyond ECR default image scanning. When configured with ECR, Sysdig Secure pulls images stored within the registry into the engine for analysis. Teams can scan for vulnerabilities, compliance checks, and misconfigurations before deployment. Vulnerabilities can be detected in base images, OS packages, and third-party libraries like Python packages from PIP, or Java JAR files that developers might be pulling into their application images before they hit production.

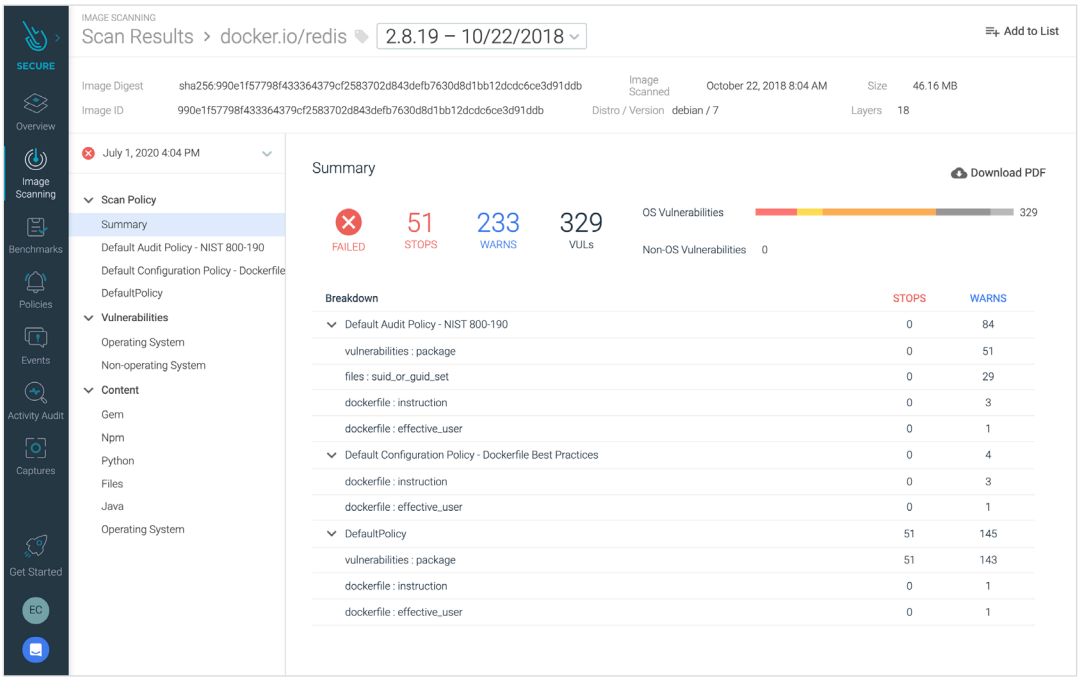
When it comes to pre-deployment scanning, Sysdig provides two container image scanning options.

- A standard approach that requires you to send your images to Sysdig for scanning. Post-scan, you can view the results within the Sysdig Secure UI.
- Local scanning, also known as inline scanning, scans images directly within your CI/CD pipeline or ECR registry. This option enables a more secure approach as you don't need to share registry credentials or image contents outside of your AWS environment. You also get scan results quickly by having the scan automated and reports generated directly within ECR.

Sysdig Secure provides visibility into:

- Official OS package vulnerabilities.
- Unofficial package vulnerabilities.
- Configuration checks (e.g., exposing SSH in a Dockerfile, users running as root).
- Vulnerabilities in third-party libraries such as Javascript NPM modules, Python PiP, Ruby GEM, and Java JAR archives.
- Secrets, credentials like tokens, certificates, and other sensitive data.
- Known vulnerabilities and available updates.
- Metadata (e.g., size of an image).
- Compliance checks for frameworks like NIST 800-190, PCI, etc.

These artifacts are stored and evaluated against custom scanning policies that can be specified to a particular registry, repository, or image tag. Sysdig Secure scanning policies help detect vulnerabilities, misconfiguration, or compliance issues within your images and generate pass/fail results directly in the UI.



Local scanning for Fargate images

For Fargate users, a feature unique to the Sysdig solution is the ability to trigger scans of images within ECR for Fargate tasks as they start. Taking advantage of Amazon EventBridge, Sysdig intercepts the Fargate request, identifies the image, and performs the scan. This automated local scanning capability helps you ensure the security of your containers intended to run on the serverless platform.

CI/CD pipeline security

CI/CD pipelines automate steps in your software delivery process, such as build and test, to help your teams deliver updates to your customers faster and more frequently. Embedding security into your delivery pipeline as you build applications helps you identify and address vulnerabilities faster, and keeps your developers productive.

AWS provides...

AWS allows you to set up a Continuous Integration/Continuous Delivery Pipeline to automate your software delivery process. Several tools help DevOps teams automate the software delivery process: CodeCommit for version control, CodeBuild for building and testing code, and CodeDeploy for automatic code deployment. On top of all of these tools, CodePipeline allows them to visualize and automate these different stages.

AWS CodeBuild is a fully managed, continuous integration service that compiles source code, runs tests, and produces software packages that are ready to deploy. CodeBuild scales continuously and processes multiple builds concurrently, so builds are not left waiting in a queue.

AWS CodePipeline is a fully managed, continuous delivery service that automates release pipelines for application and infrastructure updates. CodePipeline automates the build, test, and deploy phases of the release process every time there is a code change, based on the defined release model.

Sysdig adds...

Image Scanning for CI/CD pipelines that are used with AWS raises the confidence that DevOps teams have in the security of their deployments, detecting known vulnerabilities and validating container build configuration early in their pipelines. By detecting those issues before the images are published into a container registry or deployed in production, fixes can be applied faster, improving delivery to production time.

Sysdig Secure image scanning integrates directly into your CI/CD pipeline of choice, including AWS CodeBuild, AWS CodePipeline, Jenkins, Bamboo, GitLab, CircleCI, Tekton, and more. You can catch vulnerabilities and misconfigurations in third-party libraries, official/unofficial OS and packages, configuration checks, credential exposures, and metadata. Using Sysdig's local inline scanning you can detect issues before the images are even pushed to the registry.

Sysdig's scanning integration with CI/CD pipelines gives developers the information they need directly within their CI/CD tool to understand why a scan failed and what needs to be fixed. For non-critical policy violations, warnings will suggest what needs to be changed to improve the security of the container image without aborting the pipeline.

Using Sysdig, images built using AWS CodePipeline can be scanned without having the images leave the infrastructure and the need for a staging registry. Multiple scans can be run in parallel, improving throughput.

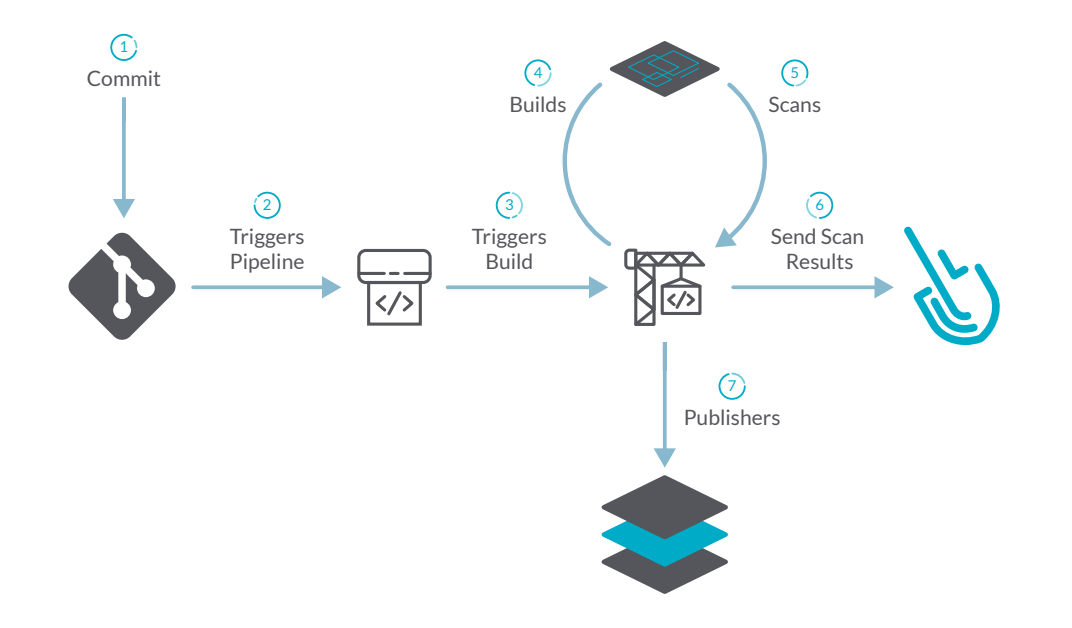


Image assurance

Image assurance focuses on preventing unapproved images from being deployed in your container environment. This helps you reduce issues and errors by evaluating and verifying images based on your defined policies prior to running in production.

AWS provides...

Kubernetes admission controllers can be used with EKS to prevent unapproved images from being deployed in your orchestrated container cluster. Using this Kubernetes capability, EKS supports the evaluation of requests to the Kubernetes API to deny requests that fail to meet defined security requirements.

Sysdig adds...

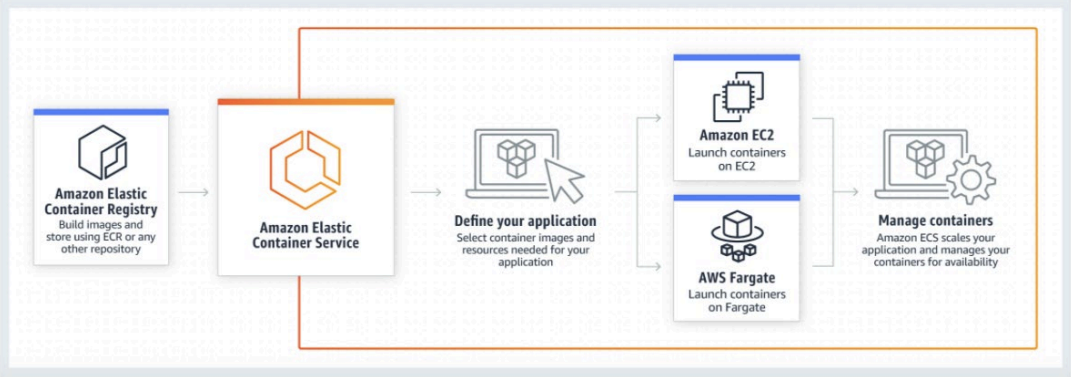
EKS can check against Sysdig Secure to evaluate whether an image is compliant with the configured security policies. When using the admission controller, this security validation decision will be propagated back to the API, which will reply to the original requester and only persist the object in the etcd database if the image passes the checks.

Registry security

In addition to securing your container images, the security of your registry itself is another key step to reduce risk for your organization. Using RBAC to manage who can pull and push container images, as well as using a private registry, are some of the steps you can take to protect your organization.

AWS provides...

Amazon ECR is a managed AWS Docker registry service that is secure, scalable, and reliable. Amazon ECR supports private Docker repositories with resource-based permissions using AWS IAM so that specific users, or Amazon EC2 instances, can access repositories and images. Developers can use the Docker CLI to push, pull, and manage images.



Sysdig adds...

Sysdig Secure container image scanning supports all Docker v2 compatible registries, including CoreOS Quay, Amazon ECR, DockerHub Private Registries, Google Container Registry, Google Cloud Artifact Registry, JFrog Artifactory, Microsoft ACR, SuSE Portus, and VMware Harbor.

Compliance

Enterprise computing environments running microservices on AWS consist of hundreds or thousands of interconnected applications and services, as well as a large and diverse set of users. To maintain control over the security of this vast environment, a standard way to scan systems for compliance with security policies is needed.

AWS provides...

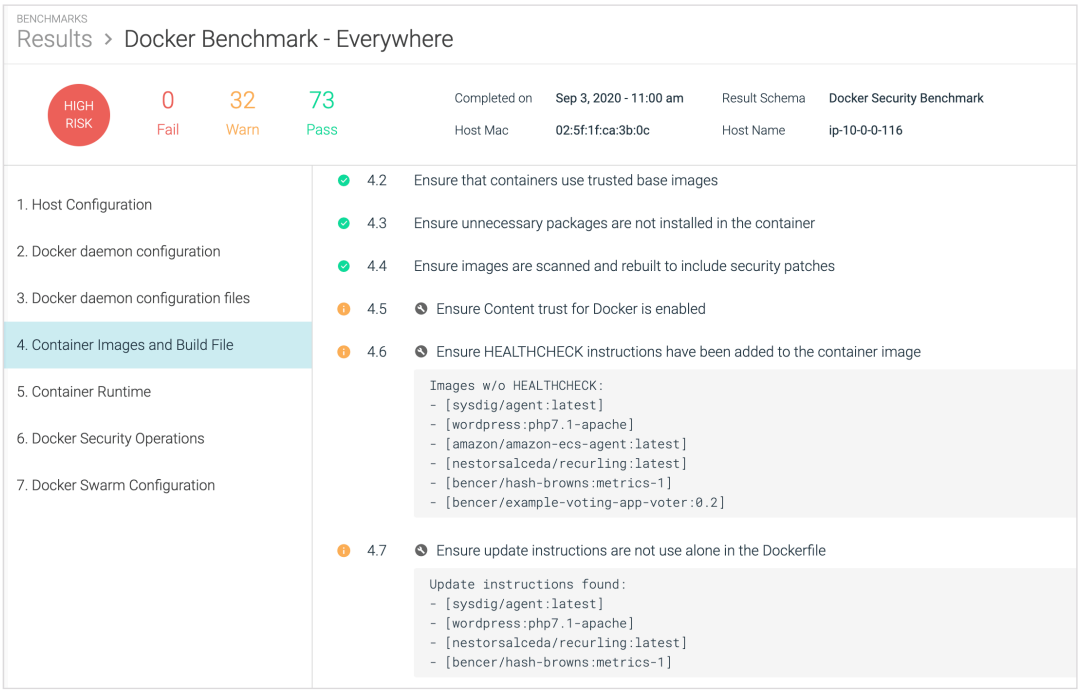
AWS Config is a service that enables you to assess, audit, and evaluate the configurations of your AWS resources. It continuously monitors and records your AWS resource services configurations and allows you to automate the evaluation of recorded configurations against desired ones. This enables you to simplify compliance auditing, security analysis, change management, and operational troubleshooting.

Sysdig adds...

Sysdig extends compliance across the container lifecycle for standards like NIST and PCI. Being able to validate that a deployment is compliant with desired configurations is one of the first compliance steps. But compliance requirements don't end there. Compliance for containers introduces unique requirements and should be implemented at various points:

- Checking against cloud, container, and infrastructure security best practices using Center for Internet Security (CIS) benchmarks for AWS, Docker, and Kubernetes.
- During build, mapping container image scanning policies to standards like NIST 800-190, PCI, and HIPAA.
- During runtime, using policies to continuously detect attack frameworks like MITRE ATT&CK or check compliance after deployment.
- Auditing any changes in your container environments, which is part of SOC2, PCI, ISO, and HIPAA requirements.

Sysdig helps you track progress using compliance dashboards. Starting with the infrastructure layer, Sysdig performs specific host, platform, and container compliance checks, like AWS Foundation benchmarks, Kubernetes benchmarks, and Docker CIS benchmarks. Sysdig also provides remediation guidance for correcting policy violations. This makes it faster to resolve configuration issues when they come up.

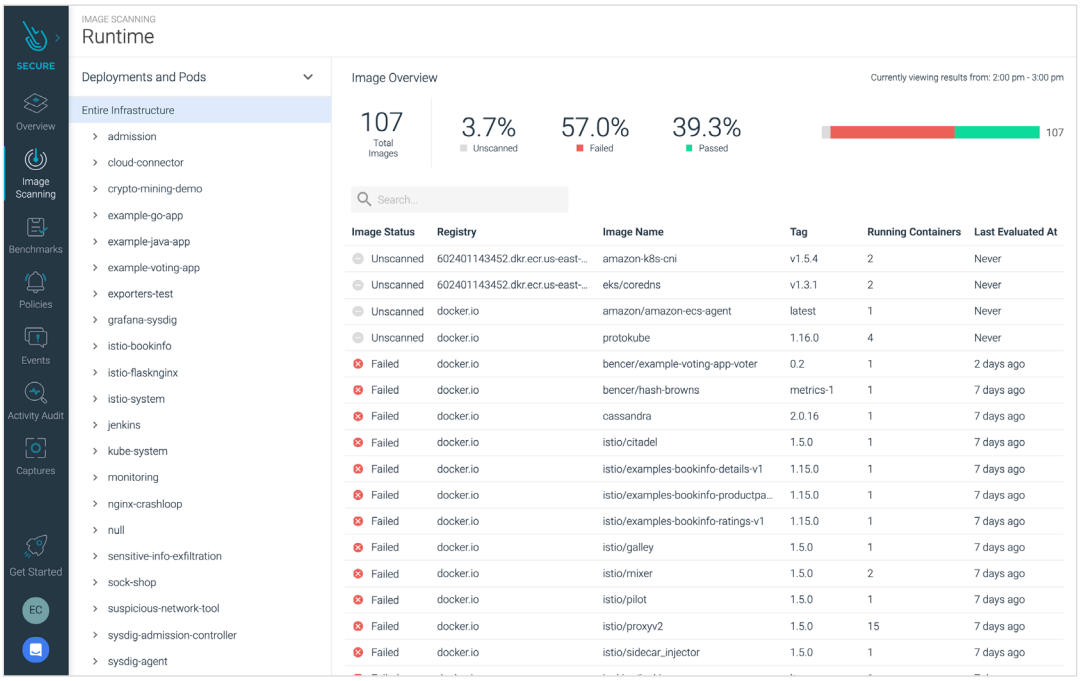


Sysdig Secure gives you the tools to implement container image security and compliance best practices, such as NIST SP 800-190, PCI DSS, Dockerfile, and more. Using Sysdig Secure container image scanning policies, you can validate cloud compliance and enforce best practices at the image level, including:

- Limiting image size.
- Blacklisting GPlv2 licenses.
- Ensuring containers use trusted base images and only necessary packages.

Sysdig provides runtime compliance assurance by translating leading security standards like NIST SP 800-190, PCI DSS, CIS benchmarks, HIPAA, GDPR, or the MITRE ATT&CK framework into a set of up-to-date security policies. It will analyze container behavior after deployment, auditing any runtime drift. Sysdig taps into any executed command on the system (both at the host and inside any container, like docker exec or oc attach) or the Kubernetes API for auditing purposes (audit secret resources access, requests by unauthorized users, etc.).

When a new high/critical CVE is published, you can assess your exposure immediately. Affected services and accountable teams can be quickly identified. Developers or application owners are identified using Kubernetes or cloud metadata, like service, deployment, or application, and alerted to view their images and vulnerabilities.



Network security

The shift of applications to containers and the cloud is a catalyst for rethinking your security model. Many cloud teams are taking a Zero Trust approach, requiring authentication and authorization even for networks internal to their organization.

The ability to segment, isolate, and control networks is a critical point of control for Zero Trust and is increasingly essential to achieving more effective security in container and Kubernetes environments.

Without the right tools, DevOps teams will struggle to see how their containerized apps are communicating and may miss malicious attempts that take advantage of open network policies. Applying a Zero Trust network security model in Kubernetes is challenging without knowing how applications are being used.

AWS provides...

Containerized applications on AWS typically require access to other services running within the cluster, as well as external AWS cloud services. AWS addresses network security for Kubernetes by assigning specific EC2 security groups directly to pods running in EKS clusters.

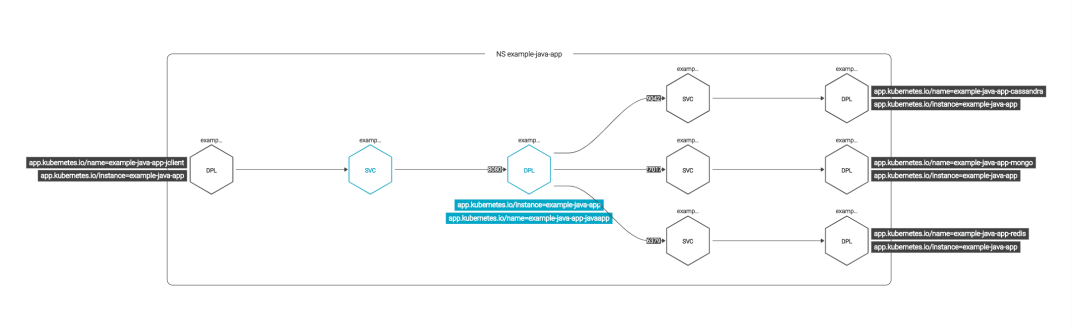
Security groups for pods enable network security compliance by running applications with varying network security requirements on shared compute resources.

Network security rules can be defined within EC2 security groups and applied to pod-to-pod and pod-to-external AWS service traffic for applications with Kubernetes native APIs. With this approach, you can reuse operational knowledge and tooling with AWS security group policies to implement security at the networking and authentication layers.

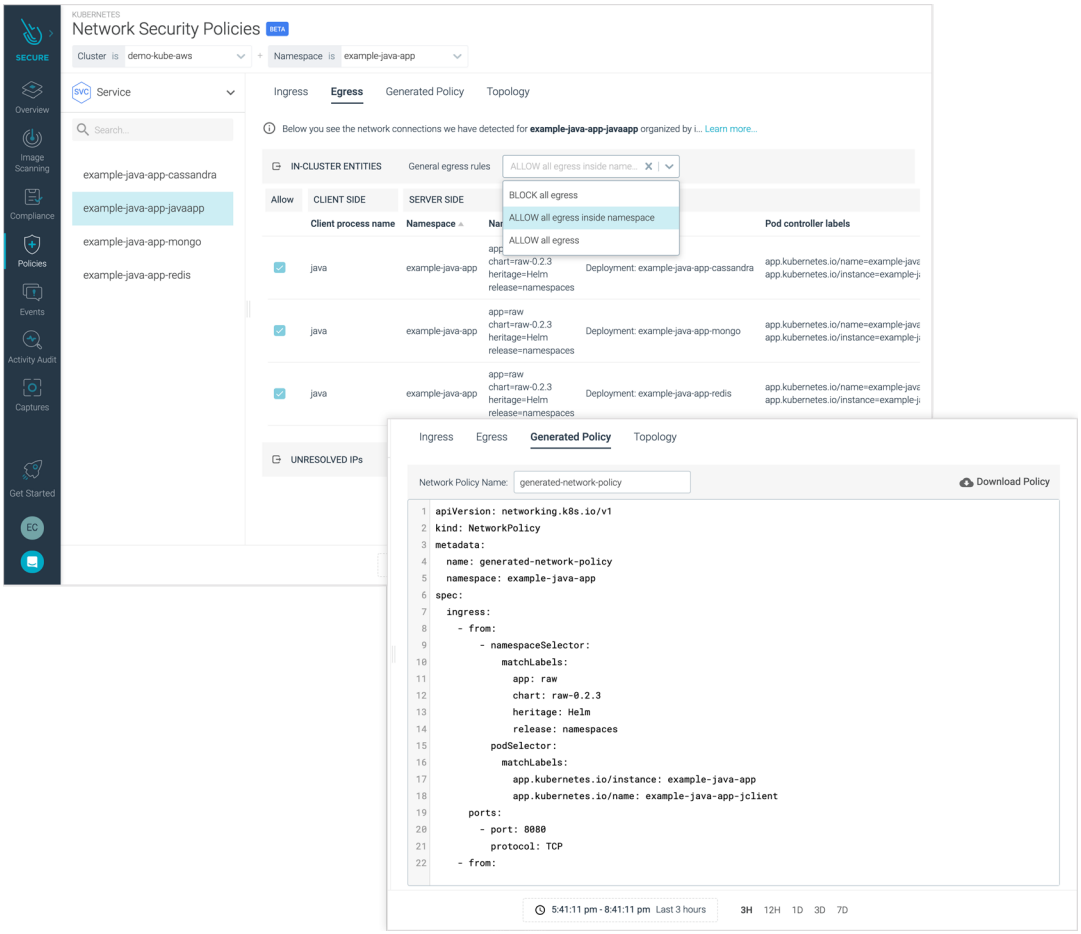
Sysdig adds...

Kubernetes network policies provide a native option for controlling network traffic within your clusters to achieve network security. With native controls, you get better performance, reliability, and security because Kubernetes enforces network microsegmentation. The challenge, however, is that Kubernetes network policies can be hard to implement without the right application knowledge and Kubernetes expertise. Sysdig helps remove these barriers to simplify implementing Zero Trust network security with Kubernetes controls.

Sysdig Secure automatically discovers all network traffic for EKS pods, services, and applications through visibility into system calls. The data is auto-tagged with Kubernetes context and labels, and used to simplify your experience when implementing Kubernetes network policies.



Dynamic topology maps let you visualize all network communication between apps and services, and drill down into the traffic flow over a particular time frame. Using this information in a simple UI, you can apply segmentation and refine network policies to allow or block connections. Sysdig will automatically generate a YAML file that you can use to apply the policy to your Kubernetes cluster.



In addition, Sysdig Secure can fingerprint every connection – and the processes that are establishing connections. This Audit Tap capability helps cloud teams investigate network activity at a fine-grained level with full visibility into context, including labels. Enterprises subject to regulations, such as NIST and PCI, can leverage this capability along with network segmentation to meet compliance requirements.

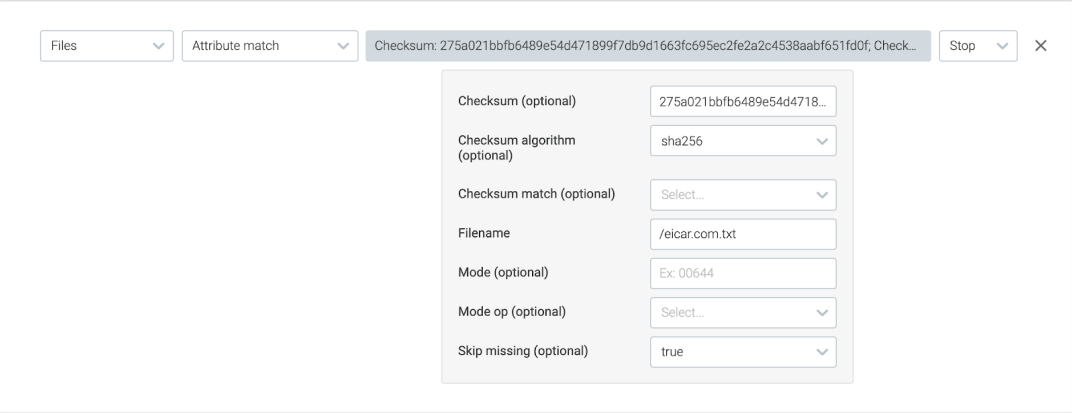
Using Sysdig to enable Zero Trust network security based on an open, standards-based approach vetted by the community delivers better performance, reliability, and security because Kubernetes provides enforcement. This eliminates the need for man-in-the- middle enforcement mechanisms. By providing an easy-to-use interface and automating guardrails for teams who may lack Kubernetes expertise, Sysdig helps AWS users save time and reduce network security risk.

File Integrity Monitoring (FIM)

File integrity monitoring gives you visibility into all of your sensitive file-related activity. It's used to detect tampering of critical system files, directories, and unauthorized changes, regardless of whether the activity is a malicious attack or an unplanned operational activity.

With Sysdig Secure, you can scan for specific file attributes and embed them as part of the image scanning policy within your CI/CD pipelines. This allows you to fail builds early if FIM policies aren't met. The file integrity monitoring policy allows you to:

- Check if a file exists or is missing, and trigger alerts based on the condition.
- Validate a specific file against its SHA256 hash. Any modification to binaries in your containers is flagged as suspicious and potentially dangerous.
- Validate file permissions. For example, you can be alerted if a file has an executable bit where it's unexpected.
- Check for file names based on regex.
- Inspect contents, looking for exposed passwords and credential leaks.



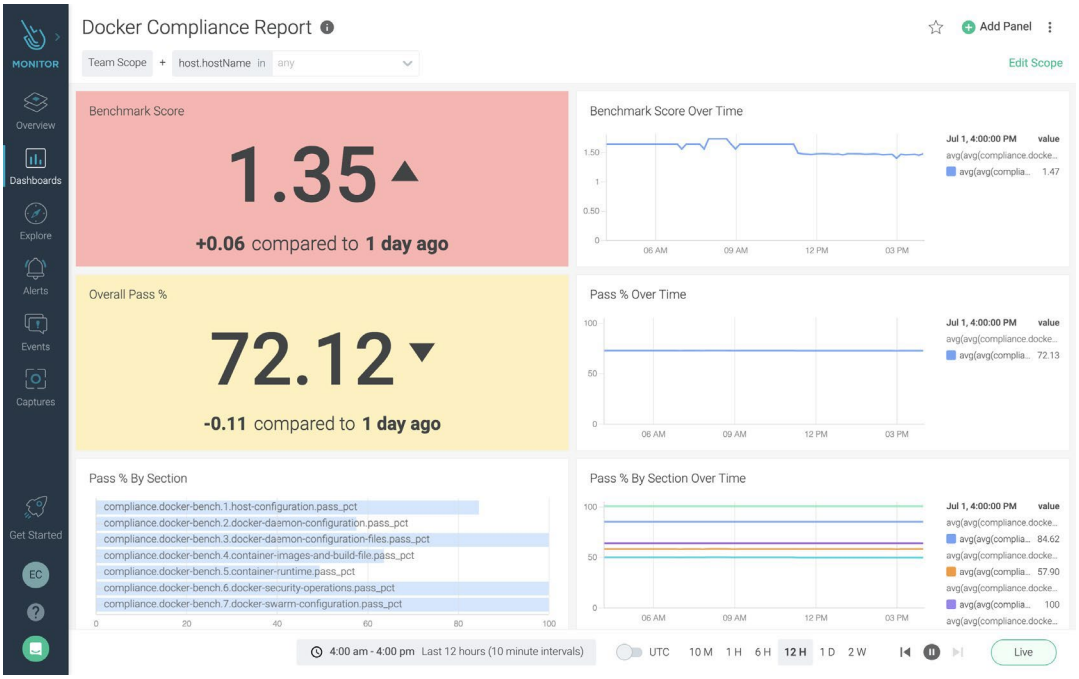
You can also implement FIM policies at runtime that alert on any suspicious changes to a filesystem. These are common file integrity monitoring checks that you should include as rules to enforce a strong security posture:

- Creation or removal of files or directories.
- Renaming of files or directories.
- Changes to file or directory security settings such as permissions, ownership, and inheritance.
- Changes to the files of a container.
- Modification of files below the container's path.
- Deletion of bash history.

Beyond generating robust reports, the Sysdig platform translates security benchmarks into a set of security metrics and dashboards. Internal and external compliance and audit teams can analyze their security posture, quickly visualize patterns and trends, and gain valuable insights into their compliance posture to:

- Compare your security posture to any previous point in time.
- Understand the risk and compliance posture across applications and environments.

- Alert when a compliance check falls below the accepted policy.
- Detect any configuration drift across AWS container clusters.



Runtime security

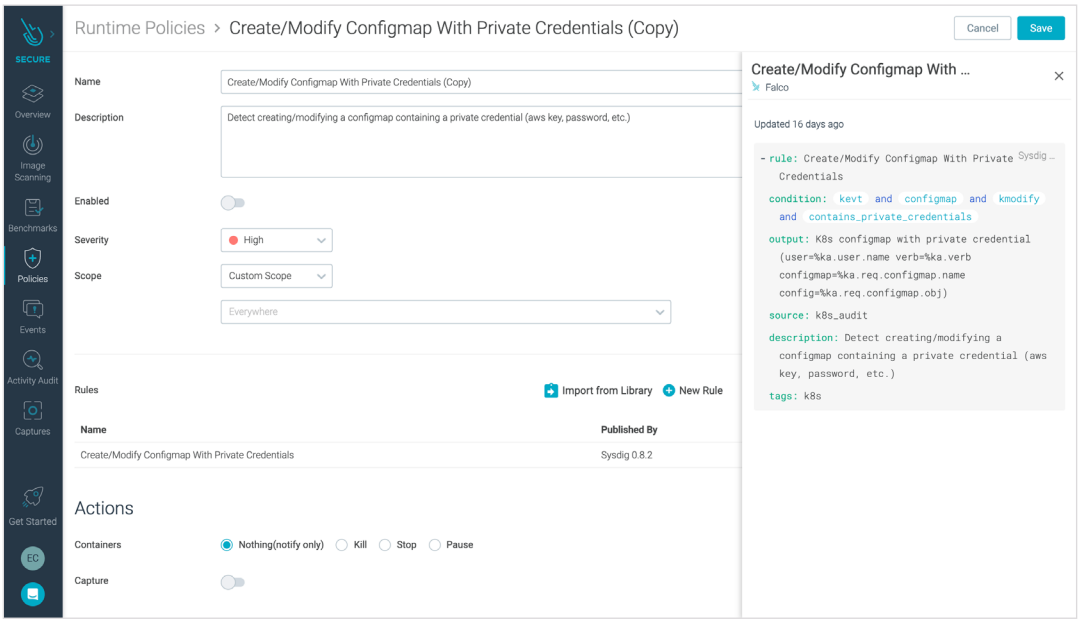
Security monitoring

Gaining visibility across both monitoring and security for AWS cloud and container services is necessary for a successful transformation journey. For example, the security team needs to know if a crypto-mining or denial of service (DoS) attack can be further explained by an abnormal deviation in a particular performance metric.

Additionally, once in production, it's important to reduce risk by configuring applications with the minimum privilege and access permissions. At the same time, you need to be able to create and maintain a runtime policy that observes workload behavior and looks for anomalous activity, blocking any threats and attacks not caught in your CI/CD or registry scanning.

Threat detection

Sysdig leverages the CNCF Falco project open-source detection engine to monitor anomalous activity on hosts and containers at runtime. It also ingests and monitors activity from AWS CloudTrail logs as well as your orchestration layer when using Kubernetes and the EKS-managed service.



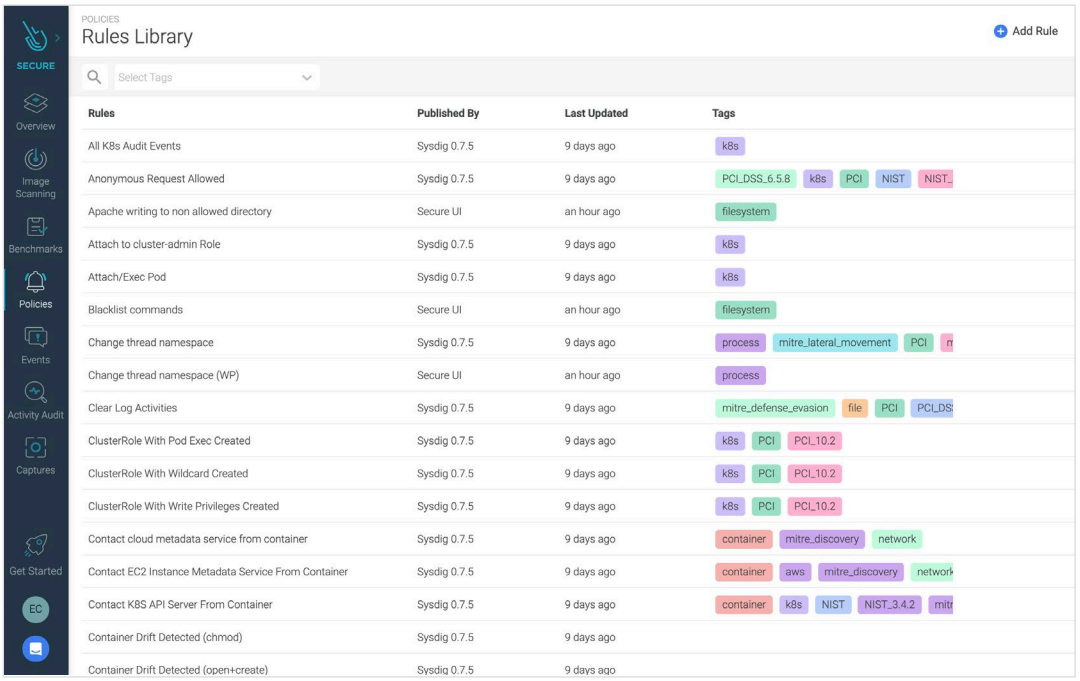
Read more about ingesting Kubernetes server API events from EKS here.

Scanning your containers once during the CI/CD process or from your AWS Elastic Container Registry is not enough. While known software vulnerabilities are detected, several security threats, by their very nature, only manifest during runtime, including:

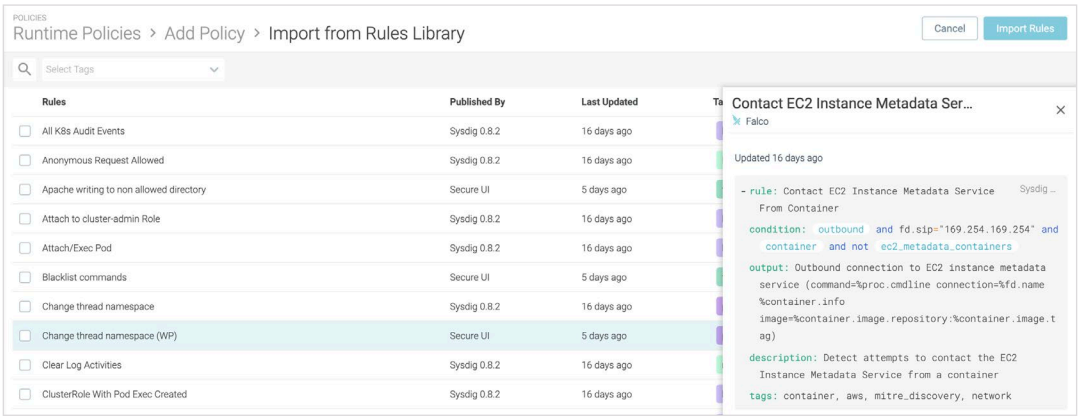
- Zero-day vulnerabilities and non-public vulnerabilities specific to your own software.
- Software bugs causing erratic behavior or resource leaking.
- Internal privilege escalation attempts or hidden/embedded malware.

Default policies are available out-of-the-box along with more than 200 rules that simplify the job of customizing security to meet your requirements. Using Sysdig Secure policies, you can easily implement runtime security to detect threats to your AWS cloud and container services, including Fargate, ECS, and EKS. This includes:

- Container runtime security policies for regulatory container compliance standards: NIST SP 800-190, PCI, CIS, or MITRE ATT&CK framework.
- Runtime detection of the most pervasive container attacks: cryptomining, secrets exfiltration, container isolation breaches, and lateral movements.
- Security monitoring for unexpected process activity, outbound connections, and terminal shell sessions.
- CloudTrail detection rules to identify suspicious activity across your AWS cloud services.

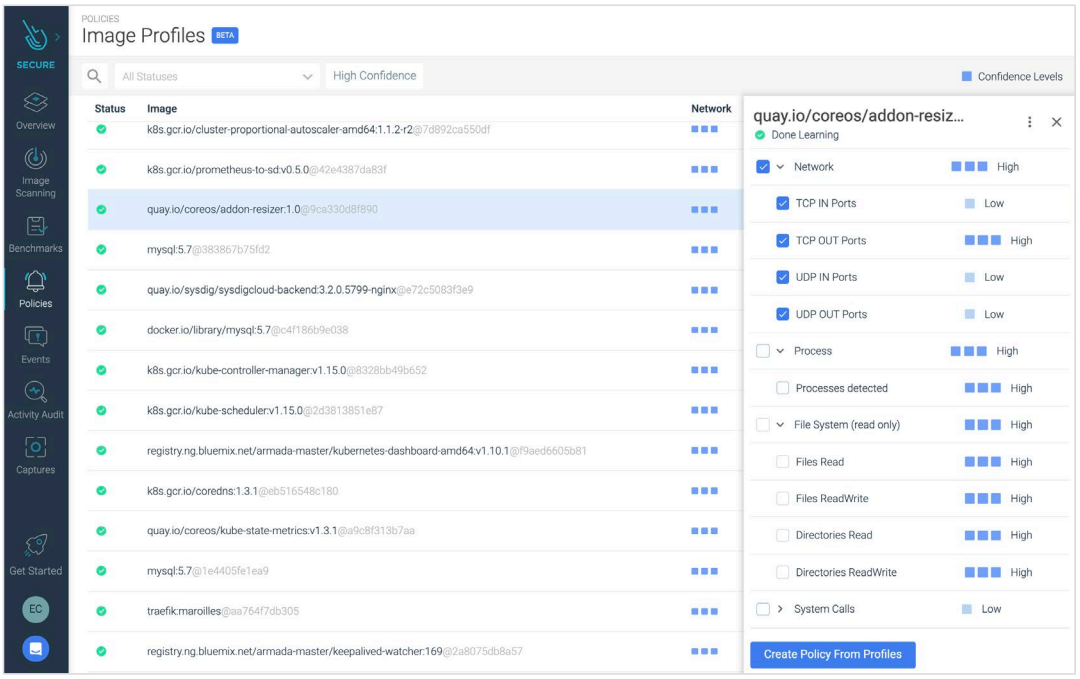


With an extensible policy engine powered by open-source Falco, operations, and security teams can customize or write their own rules through a visual interface to build fine-tuned policies that match their requirements. Falco rules that are community-sourced and curated are available on the Cloud Native Security Hub.



Runtime image profiling

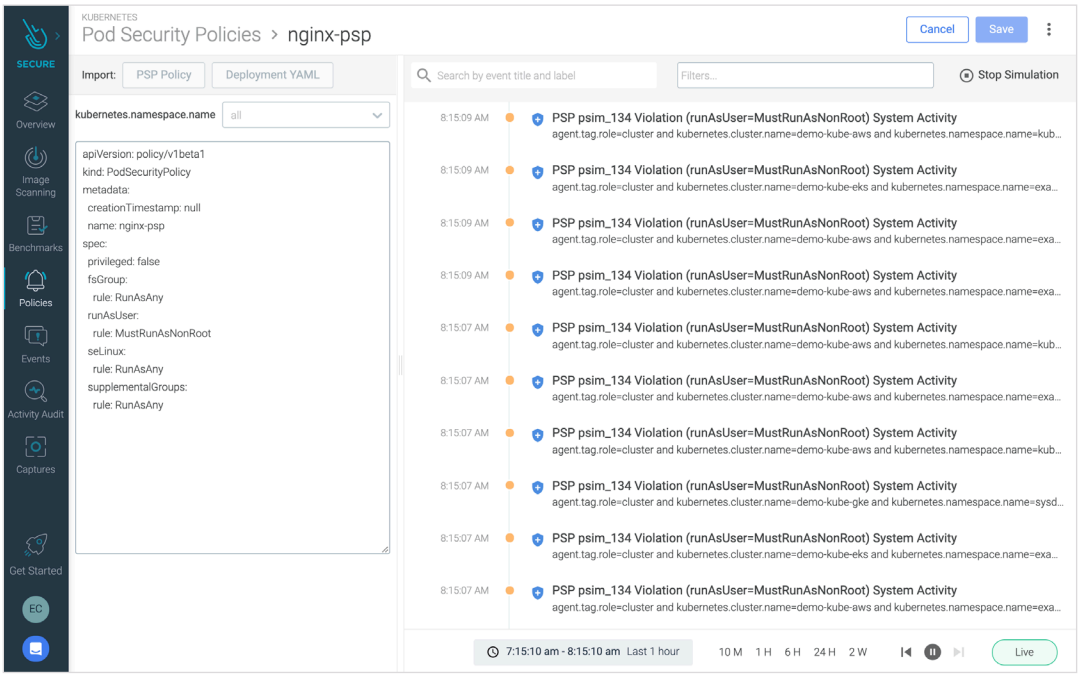
To ease the burden of creating and maintaining runtime security in large-scale environments, Sysdig Secure features runtime image profiling. Image profiling automatically models, analyzes, and learns container runtime behavior to create a comprehensive container runtime profile and automatically builds policies for you. This includes analyzing kube-apiserver activity and syscalls while enriching them with various metadata, including ECS, EKS, and cloud labels. This approach enhances anomaly detection through machine learning and helps you block threats before they propagate.



Threat prevention with Kubernetes native controls

Sysdig prevents threats using Kubernetes native controls, such as Pod Security Policies (PSPs). The Kubernetes Policy Advisor automates the generation of PSPs and validates them pre-deployment so they don't break applications when applied. This allows users to adopt PSPs in production environments quickly and easily. PSPs also provide a Kubernetes native control mechanism to prevent threats without impacting performance, unlike agents that have to intercept every action on the host.

Sysdig Secure leverages Kubernetes-native controls like PSP for enforcement. You can read more about it on the blog Pod Security Policies in production with Sysdig's Kubernetes Policy Advisor and learn about Sysdig runtime security capabilities here.



With Sysdig Secure, operations and security teams can ease the burden of creating container security policies and gain more transparency and assurance as they have greater control of what's happening under the hood.

AWS Cloud Security Posture Management

Threat research conducted by Sysdig shows that having a single view across cloud, workloads, and containers speeds the time to both detect and respond to lateral movement attacks, a common technique used in the majority of security breaches.

Using different cloud and container security tools complicates security operations as it requires manual correlation of different data sources to fully understand a breach and uncover the systems impacted. Sysdig pairs Cloud Security Posture Management (CSPM) and cloud threat detection with cloud workload protection, including container and Kubernetes security features in a single platform.

By unifying the incident timeline and adding risk-based insights, Sysdig reduces the time to detect threats in your AWS cloud services and containers from weeks to hours. Cloud development teams can see exactly where the attacker started and each step they took as they moved through the environment.

Cloud Asset Discovery

Cloud assets operate without the limitations of a perimeter, and because resources are continuously brought into AWS environments through APIs and other connectors, it's necessary to know which assets are actually interacting with your environment. Organizations need an inventory of assets, including intelligence about how all these data sources are connecting and interacting, in order to apply security across their entire AWS environment.

Applications in AWS are usually composed of multiple services that perform specific functions and are accessible through an API. For each service, there is a connection to other resources within the cloud environment — these include object stores, microservices, databases, S3 buckets, and other repositories and resources.

Most organizations apply a manual approach to identify these resources, their relationships, and their configurations. Manual management in an environment that is continuously expanding and contracting isn't scalable, so automated services are necessary to create and track an inventory of these assets and their behaviors.

What AWS provides...

AWS Application Discovery Services collect usage and configuration data about on-premises servers and other cloud assets. It's integrated with AWS Migration Hub, which enables immediate identification of new assets as they enter an environment either through integration or another form of connection. With Application Discovery Services APIs, users get access to system performance and utilization data for all discovered servers

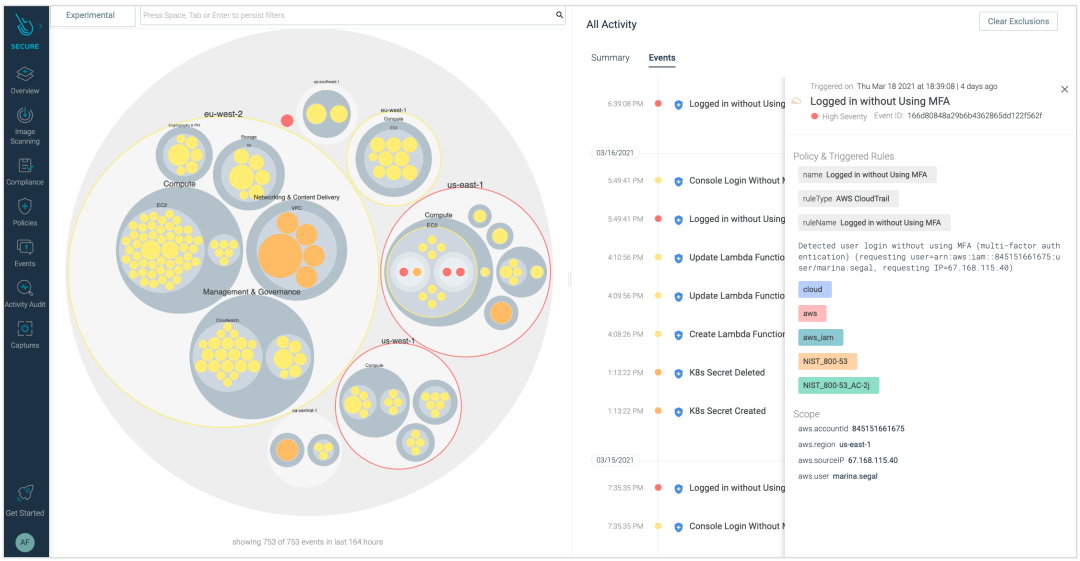
Using Application Discovery Service APIs, you can export the system performance and utilization data for your discovered servers. Input this data into your cost model to compute

the cost of running those servers in AWS. Additionally, you can export data about the network connections that exist between servers. This information helps you determine the network dependencies between servers and group them into applications for migration planning.

Sysdig adds...

Cloud security teams can use Sysdig to manage their security posture by automatically discovering the systems, applications, services, and scripts running across an AWS cloud environment. This lets you map cloud assets, including accounts, VPCs, regions, S3 buckets, RDS, etc. to gain a better understanding of where your sensitive data(e.g., customer data, data governed by compliance regulations) is stored and processed.

This capability – based on Cloud Custodian, an open source tool for securing cloud infrastructure – offers a real-time dashboard of the resources and assets operating in your AWS account as well as all assets that roll up into each resource and project. With a baseline for your current operating state, you can better prioritize the services with the most critical threats and accelerate remediation.



With Sysdig, you can drill into each AWS resource and project to see the corresponding configurations. Sysdig identifies and classifies the assets in each of your AWS accounts, along with data from other systems, to create one source of truth for all of the services in your cloud.

Asset management is a critical element of configuration compliance. Cloud environments are dynamic and complex. Manual tracking and detection of configurations and changes are impossible. Sysdig maps guidelines for PCI-DSS and NIST 800-53 to the assets in your AWS environment, continuously checking and providing alerts when configurations don't meet the requirements for these particular compliance frameworks.

Sysdig users are able to customize all the data provided in inventory management, reducing the need to manually correlate event information. Because Sysdig Secure also delivers related context about Kubernetes activity, users can get a better understanding of what is happening with workloads in parallel with AWS managed cloud services security events.

Cloud Infrastructure Entitlements Management

Identity and access management (IAM) misconfigurations are one of the most common concerns in cloud security. Access controls and permissions that are too permissive can be exploited by attackers to gain unauthorized access. This can result in lateral movement within your environment and expose sensitive data.

To prevent cloud permission risk, cloud teams can leverage a Cloud Infrastructure Entitlements Management (CIEM) solution. CIEM tools specialize in looking for accounts and roles with excessive or unused permissions, as well as unused accounts. Due to the fine granularity of permissions available in the Cloud environments, CIEM tools are key to achieving proper access configurations. Carefully giving exactly what a user or system needs to perform its actions is fundamental to cloud security. Using this "least privilege" concept is a crucial best practice to avoid risks of data breaches, contain privilege escalation, and block lateral movement.

AWS provides...

AWS Identity and Access Management (IAM) Access Analyzer provides monitoring and analysis of new or updated resource policies to help you understand potential security implications. You can preview Access Analyzer findings before deploying resource permissions so you can validate that your policy changes grant only intended access. This helps you preview how your policy will affect public and cross-account access before deploying resource permissions.

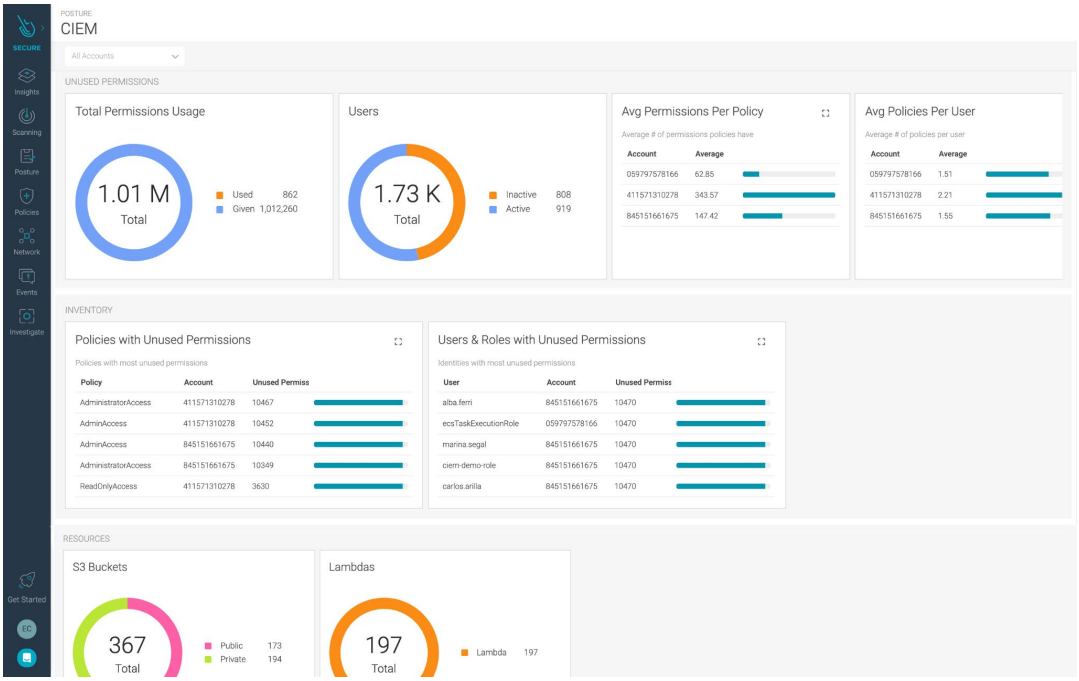
Sysdig adds...

Sysdig includes Cloud Infrastructure Entitlements Management that provides you with a comprehensive view into access permissions across your AWS accounts, users, and services including serverless functions. Because Sysdig Secure analyzes audit logs of executed cloud commands and correlates this activity with policies, roles, and users in your accounts, it can use this same information to create a profile of permission usage. This helps you simplify the auditing of access configurations and meet compliance requirements.

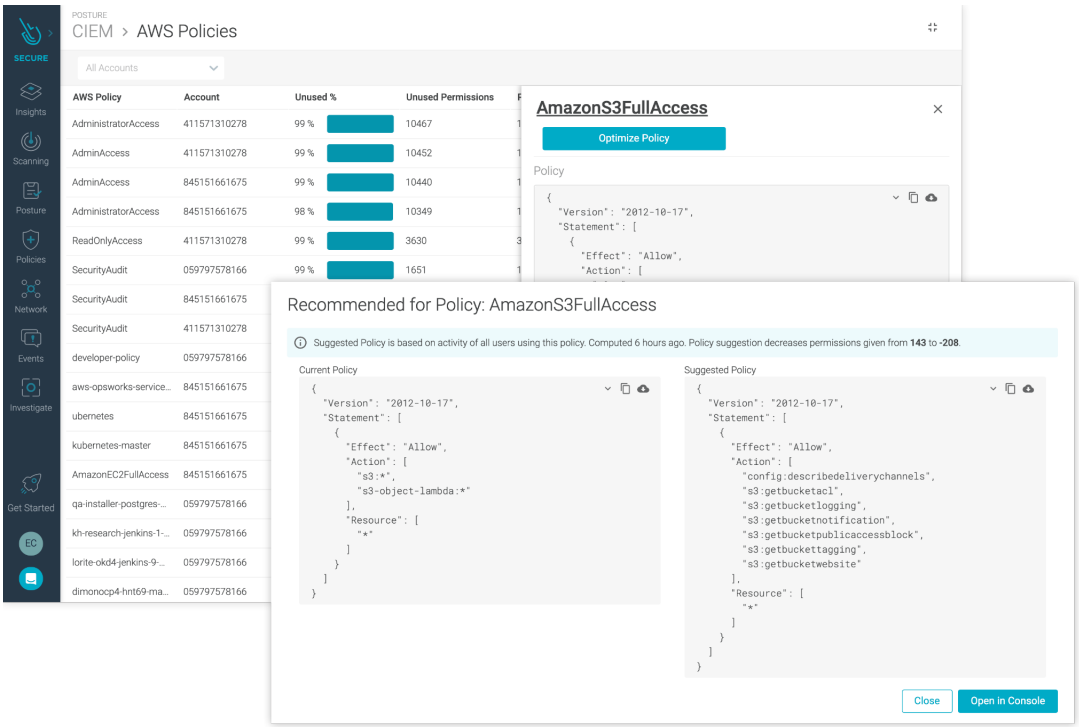
Sysdig CIEM visualizations help you understand real permission usage and determine where there is overly permissive or outdated access that puts you at risk of exposure to credential misuse. An out-of-the-box dashboard informs you of:

- The total permissions given and used.
- How many users are inactive and which you should consider deleting.
- Averages of permissions per policy and policies per user.
- The policies, users, and roles with the worst case of unused permissions.

You can use these metrics to track your progress towards a stronger IAM security posture.



Sysdig Secure helps you improve IAM configurations by analyzing the cloud entitlements that are granted versus what is actually needed. The solution helps you identify the “just-enough” privileges and auto-suggests policies that you can use to manage and enforce least privilege access in a matter of minutes.



Static Configuration Management

Even when applications and other cloud-based systems are designed with an emphasis on security, changes in the cloud environment mean that settings and configurations that were initially established may not be relevant as the cloud environment adapts to change. Vulnerabilities become exposed as a result of these changes, and configurations that oversee apps running in production may pose security risks. The key, then, is to apply configuration management to AWS resources in order to ensure compliance with specific regulatory frameworks, but also to maintain a security posture that maps to the organization's AWS accounts.

With cloud workload and application development changing rapidly, app features evolve continuously. This results in corresponding configuration changes that cannot be manually tracked. Between AWS and Sysdig, cloud users benefit from continuous cloud configuration monitoring and audit reports across their AWS accounts, which detect compliance violations across the networking, storage, user access, and logging aspects of an AWS infrastructure.

AWS provides...

AWS Config performs continuous assessment, auditing, and reporting on configurations in AWS resources. It monitors and logs an environment's AWS resource configurations, and enables the application of predefined configurations when changes are needed. It allows admins to review configuration changes and how they impact the relationships between and among other AWS resources, and provides analysis of historical evolution of changes. Users can see what configurations their workloads have been operating within over a period of time to determine when (and where within the environment) a change in an AWS resource impacted a configuration.

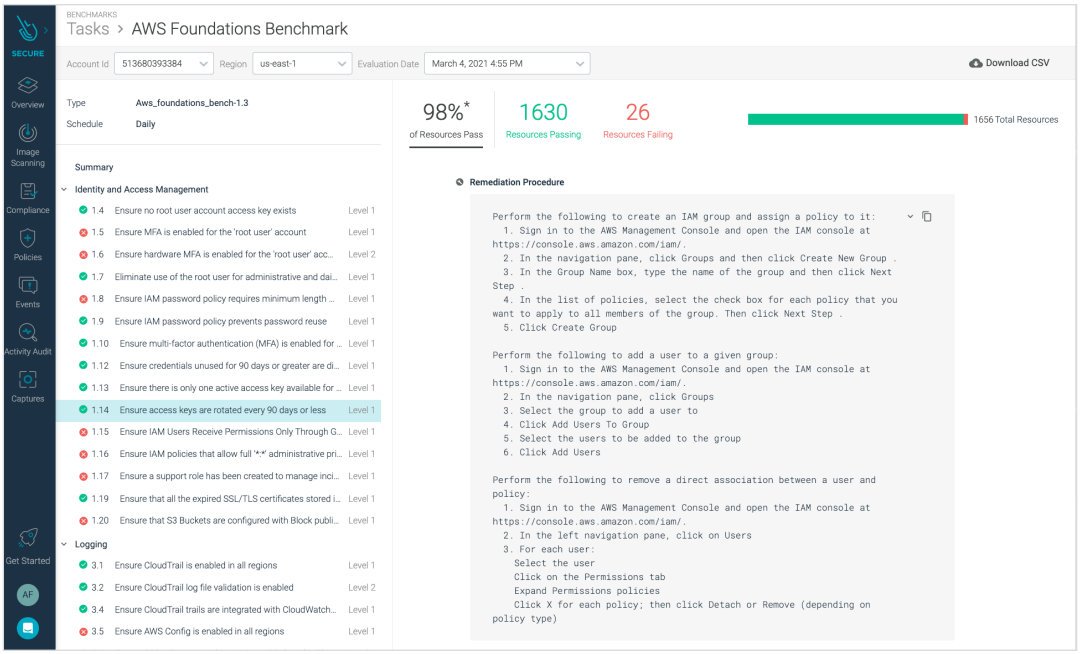
When enabled, AWS Config discovers the supported AWS resources that exist in a given account and generates an accepted configuration report for each resource. It creates configuration items for every supported resource in a user's environment.

Sysdig adds...

As AWS accounts involve more workloads and integrations across a growing number of applications, the volume of events and operational trails can become overwhelming. Analysis is impossible without a scalable, automated approach. Sysdig Secure helps you identify risky configuration settings and gain visibility into the current security posture of your cloud and container environment. This simplifies detection of misconfigurations, such as public storage buckets, exposed security groups, leaked secrets/credentials, etc., to quickly determine if you have configuration drift.

Sysdig periodically analyzes your cloud configuration against the AWS Foundations CIS benchmark, a curated collection of checks on your AWS account that will inform you which services and configurations present a security challenge. The readout also provides guidance that will help you take the right steps to remediate configuration issues across your cloud assets.

From the perspective of security and DevOps teams, by providing configuration insights in an easy-to-read, contextual format which aids auditing, Sysdig provides tangible business benefits by simplifying compliance and adherence to policies. This is increasingly an essential task for security teams because it allows them to reach their goals in an automated fashion.



Threat Detection with AWS CloudTrail logs

AWS CloudTrail is a native service that enables governance and compliance auditing of your AWS environment. User, role, or AWS service actions are logged as events in CloudTrail. This includes any changes to the AWS Management Console, AWS Command Line Interface, and AWS SDKs and APIs.

AWS provides...

The event history available from CloudTrail simplifies security analysis, resource change tracking, and troubleshooting. You can use the information CloudTrail provides to detect unusual activity in your AWS accounts and to simplify operational analysis and troubleshooting. CloudTrail allows you to track and respond to account activity threatening the security of your AWS resources.

You can also leverage AWS GuardDuty, a threat detection service that monitors for malicious activity and abnormal behavior in AWS workloads, accounts, API calls, and the data stored in S3 buckets. It relies on audit logs from CloudTrail to identify anomalous activity that could suggest a security issue.

Sysdig adds...

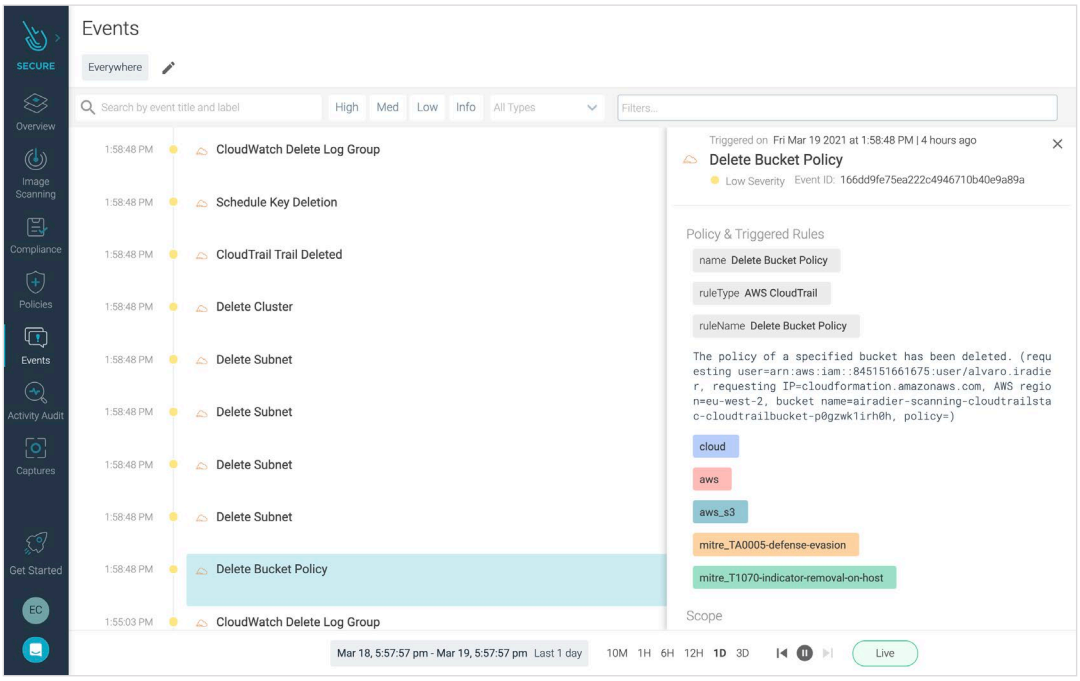
As your infrastructure grows, the amount of events and operational logs available from CloudTrail can increase to a size that prohibits manual analysis and response. Delays in reacting to a threat can potentially have major consequences.

Sysdig solves the challenge of automating the evaluation of CloudTrail events in real time by using a flexible set of security rules based on open-source Falco threat detection – the same engine that detects threats across your containers and Kubernetes deployments.

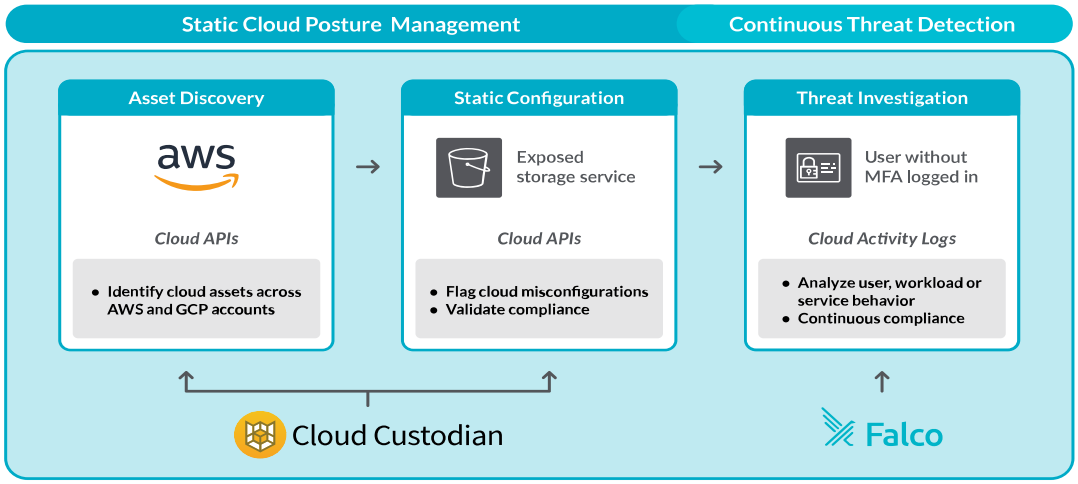
Using Sysdig's integration with CloudTrail, you can use pre-configured policies, or craft your own detections to alert on unexpected activity. You can save time by leveraging a comprehensive set of over 100 community-driven, out-of-the-box Falco rules. In addition, DevOps and security teams get findings quickly by seeing events directly in AWS Security Hub, without ever leaving their AWS environment.

Once configured, Sysdig Secure will continuously detect and report suspicious cloud activity and events for services such as IAM, RDS, EC2, RedShift, and VPC across all of your cloud accounts. Here are just a few use case examples:

- Look for suspicious IAM activity and abnormal permission changes.
- Detect process execution patterns for unexpected behavior or remote code executions.
- Look for credential theft, especially for longer-lived or high-privilege credentials.
- Identify changes in configuration of cloud resources (e.g., S3), infrastructure ports for virtual servers, containers, and container orchestration platforms.
- Identify sensitive data leaks through unintentional exposure of information.
- Examine data from past incidents to detect patterns.



You can view the growing list of [CloudTrail supported services on the AWS website](#).



Monitoring AWS container services

Monitoring the dynamic nature of container-based applications is critical for high availability and performance of cloud services. Microservice architectures running on containers and cloud have made applications easier to scale and faster to develop, allowing faster innovation and accelerated time-to-market for new features. As the number of microservices grows within an application, it can become difficult to ensure visibility inside these environments. Microservices-based applications can be distributed across multiple instances, and containers can move across multi-cloud infrastructure as needed. Monitoring the Kubernetes orchestration state is key to understanding if Kubernetes is keeping all of the service instances up and running.

AWS provides...

AWS offers Amazon CloudWatch, a service that monitors and observes the operational health of AWS resources and applications through logs, metrics, and events.

CloudWatch provides data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and get a unified view of operational health. It collects monitoring and operational data in the form of logs, metrics, and events, providing a unified view of AWS resources, applications, and services that run on AWS and on-premises servers. CloudWatch can detect anomalous behavior in an environment, set alarms, visualize logs and metrics side by side, take automated actions, troubleshoot issues, and discover insights to keep your applications running smoothly.

Prometheus metrics can also be collected in CloudWatch to monitor, troubleshoot, and alert on application performance degradation and failures faster.

Sysdig Adds....

Sysdig Monitor allows you to maximize the performance and availability of your cloud infrastructure, services, and applications. Built on open source, it provides immediate, deep visibility into rapidly changing container environments. You can resolve issues faster by using granular data derived from actual system calls enriched with cloud and Kubernetes context along with Prometheus metrics. Sysdig Monitor helps you remove silos by unifying data across teams for hybrid and multi-cloud monitoring.

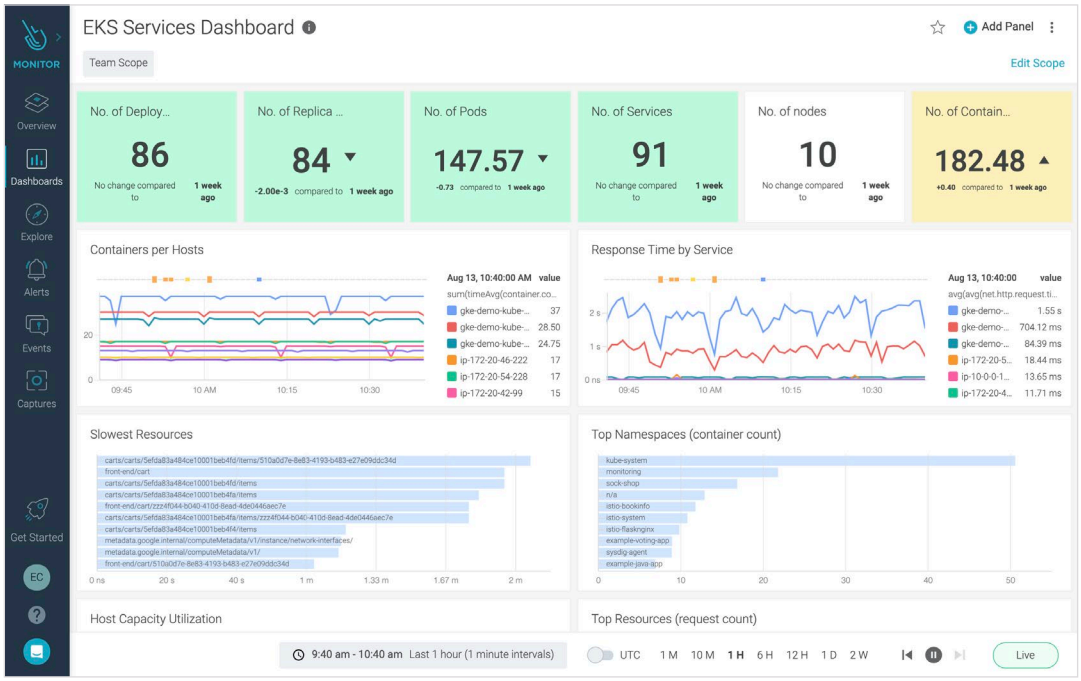
With Sysdig Monitor, we offer a scalable managed Prometheus service that frees cloud teams from the burden of setting up and managing their own monitoring system without sacrificing the benefits of the Prometheus open standard. Sysdig Monitor provides automatic discovery and assisted deployment of Prometheus monitoring integrations along with preconfigured dashboards and alerts.

Support for the Prometheus Query Language (PromQL) and a PromQL Explorer Sysdig simplifies your interaction with metrics to speed mean time to discover (MTTD) using queries. In addition, a PromQL Library helps you discover popular queries from the monitoring community to learn new ways to get to the information that really matters.

Kubernetes and container monitoring

With Sysdig, cloud teams receive automatic alerts and detailed health and performance information, including golden signals for clusters, deployments, namespaces, and workloads. Deep visibility into container activity enriched with cloud and Kubernetes context allows teams to manage the complexity of container deployments. This allows you to:

- Monitor health and performance with deep visibility into infrastructure, services, and applications.
- Visualize the operational status of your clusters with Kubernetes orchestration context.
- Immediately identify owners for issue resolution using container and cloud context.
- Identify pods consuming excessive resources and monitor capacity limits.
- Monitor application auto-scaling behavior to control unexpected billing.
- Reduce cost by optimizing capacity across clusters and clouds.

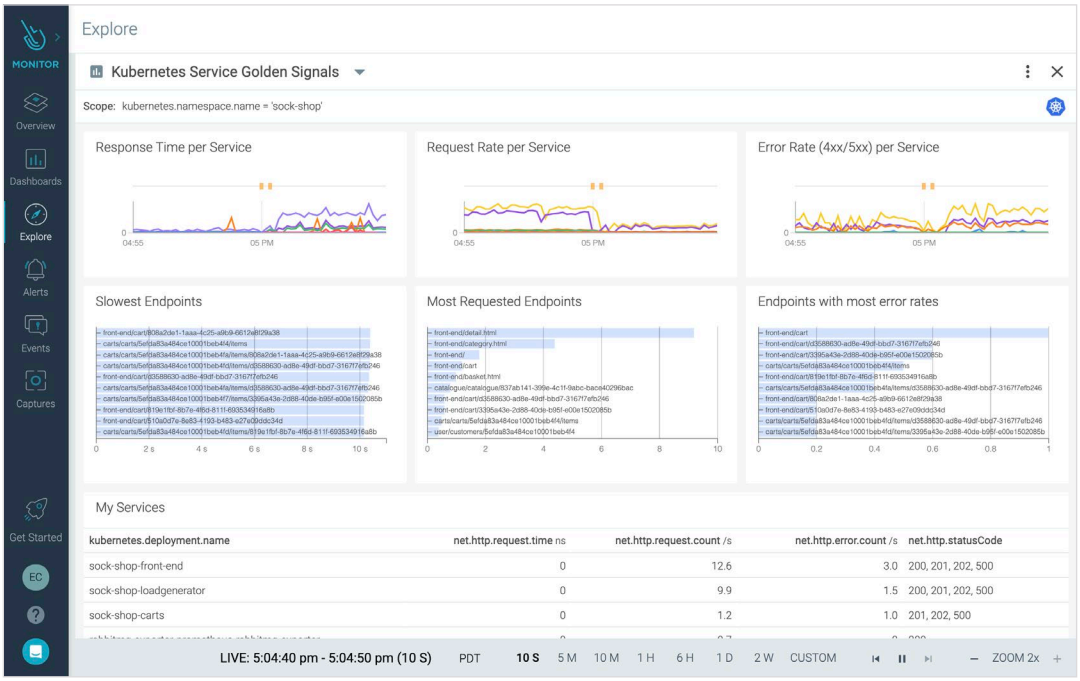


Application and services monitoring

Latency, error, traffic, and saturation metrics are known as the golden signals for monitoring service health. These metrics indicate the real health and performance of your application as seen by users interacting with that service. You can save time by looking at what really matters and avoiding traps that could mask the real problems with applications.

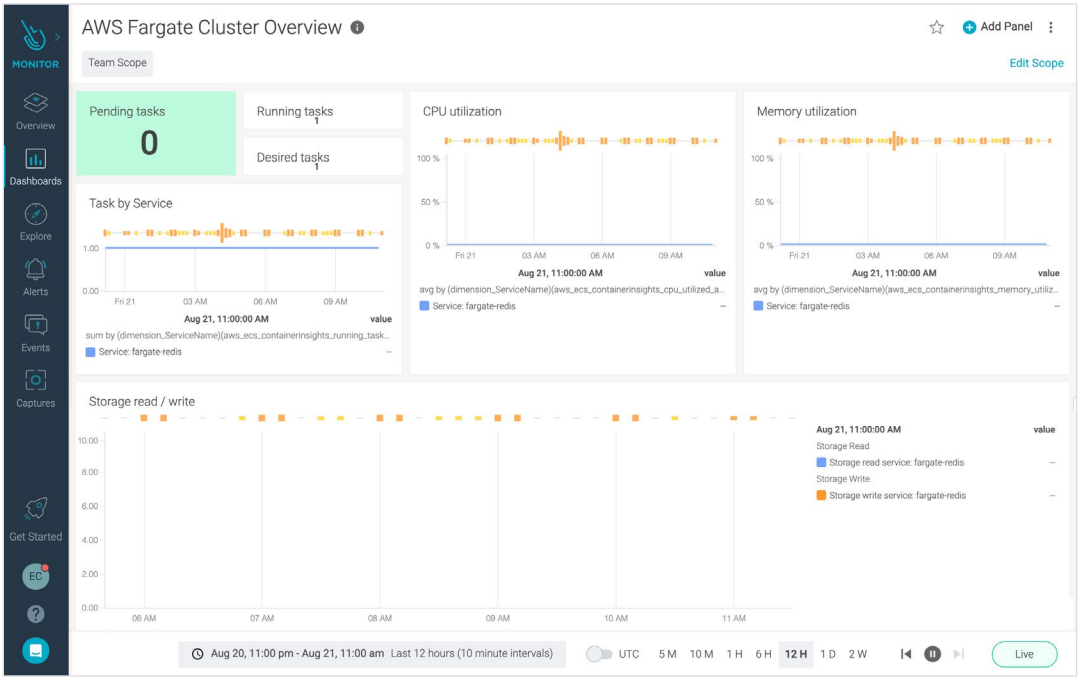
Sysdig Monitor allows you to:

- Accelerate time to insight, with a single source of truth for application availability and security, so teams can resolve issues faster.
- Improve application performance and rapidly solve issues with deep container visibility and granular metrics enriched with Kubernetes and cloud context.
- Observe metrics from cloud services, databases, and other key components in your AWS environment using out-of-the-box dashboards.
- Monitor the impact of a given security incident on the availability of a service to your users.
- Reduce risk by utilizing enterprise-grade access controls for your monitoring system including teams, SSO, and RBAC.
- Leverage your existing developer investment with full Prometheus and PromQL compatibility at cloud-scale.
- Extend monitoring to hundreds of applications and services using Prometheus compatible exporters, dashboards, and alerts.
- Get productive faster by using curated, documented, and supported monitoring integrations for Kubernetes platforms and cloud-native services available from PromCat.io.



Sysdig supports a number of AWS services natively and also makes it easier to use Prometheus with Amazon CloudWatch. Sysdig Monitor extracts AWS CloudWatch metrics via Prometheus that can be visualized using pre-built Sysdig and/or Grafana dashboards. A curated repository of vetted Prometheus exporters, dashboards, alerts, and recording rules for AWS services are available from Promcat.io, an open-source resource catalog for enterprise-class Prometheus monitoring.

Having validated support with documentation saves weeks of effort by reducing developer time spent researching and maintaining Prometheus integrations. Example AWS integrations include support for AWS Fargate, AWS Lambda, AWS Application Load Balancer (AWS ALB), AWS Elastic Load Balancer (AWS ELB), and Amazon Simple Storage Service (Amazon S3).



Service mesh visibility

To make management of microservices more efficient and easier to operate, service mesh solutions like Istio, Linkerd, and AWS App Mesh have become the next core building blocks of microservices infrastructure built on containers. A service mesh helps to run, manage, and monitor containerized microservices more efficiently at scale with capabilities such as service discovery, authentication, load balancing, encryption, and tracing.

AWS provides...

AWS App Mesh is a managed service mesh platform for ECS, EKS, and Fargate. It makes it easy to monitor and control microservices running on AWS. App Mesh standardizes how microservices communicate, giving users end-to-end visibility and ensuring high-availability for their applications. It provides a single view and point of control for all of the communication between microservices in applications without changing the code.

AWS App Mesh uses the open-source Envoy proxy, making it compatible with a wide range of AWS Partner Network (APN) and open-source tools for monitoring microservices.

Sysdig adds...

Sysdig supports AWS App Mesh, providing additional visibility into how microservices running on AWS container services are performing, with further insight into the security profile and overall health of their service mesh. With Sysdig, AWS App Mesh users can monitor the performance of their service mesh as well as view performance and security metrics across their infrastructure, giving added control to containerized environments.

Sysdig enhances AWS App Mesh monitoring with the ability to automatically scrape metrics from the Envoy proxy's Prometheus endpoint. It allows enterprises to securely collect, alert on, and visualize the metrics from Envoy. Once collected, Sysdig correlates the data with the vast amount of metrics and events data that it collects and enriches from across the entire container infrastructure, including Kubernetes.

Container forensics and incident response

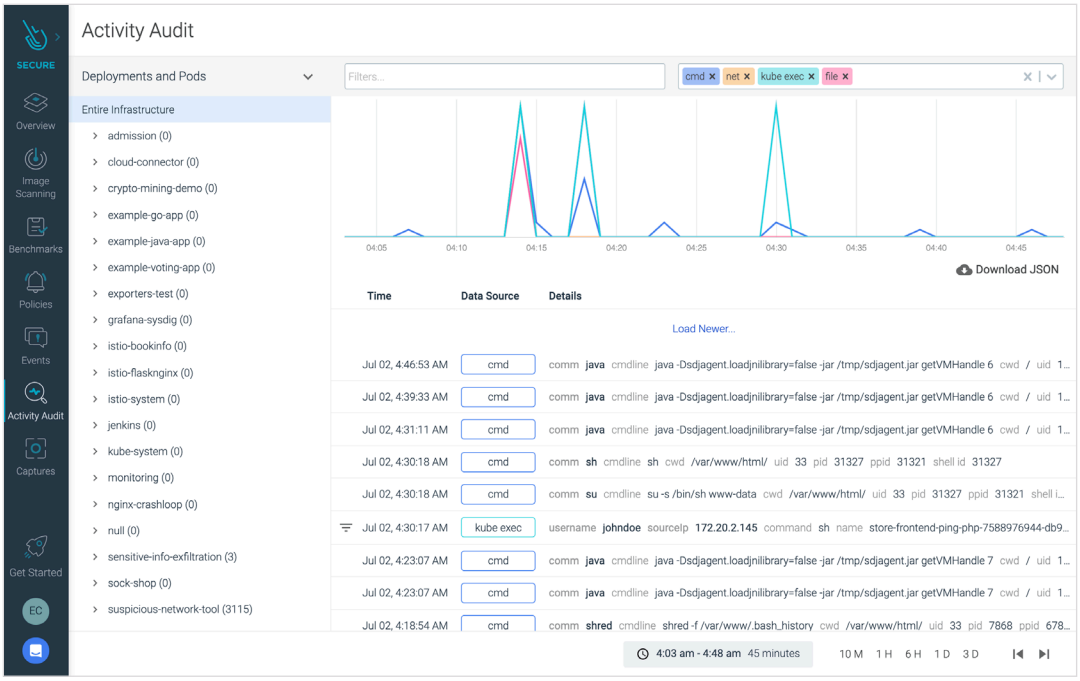
When troubleshooting an issue or performing a post-mortem analysis of a security incident, one of the typical challenges is that when a container is destroyed, all of the relevant information is gone.

With container solutions like EKS, ECS, and Fargate, this happens all the time. Containers can be moved between nodes and services are scaled up and down, deleting container instances. You need to be able to identify the root cause of problems and recognize whether the issue comes from malicious activity or a misconfiguration of the app.

While CloudWatch provides insight using logs, metrics, and events, it was not built for troubleshooting dynamic containers. The ephemeral nature of containers makes it difficult to analyze what happened with a security incident after the container is gone. How can you reproduce the steps taken by the intruder? How did they gain access? What was the impact? Did they install any malware? Was any data leaked? How far did the attack extend?

Sysdig adds...

Sysdig's Activity Audit speeds incident response and enables audit for EKS, ECS, and Fargate. Sysdig captures and correlates executed commands, network, and orchestrator activity so SOC teams can spot what happened. With Sysdig captures, you can also record all container activity at a detailed level, including spawned processes, network connections, file system activity, etc., so you can understand events in detail and conduct Kubernetes forensics even after the container is gone.



Read more about this in Incident response in Kubernetes with Sysdig's Activity Audit.

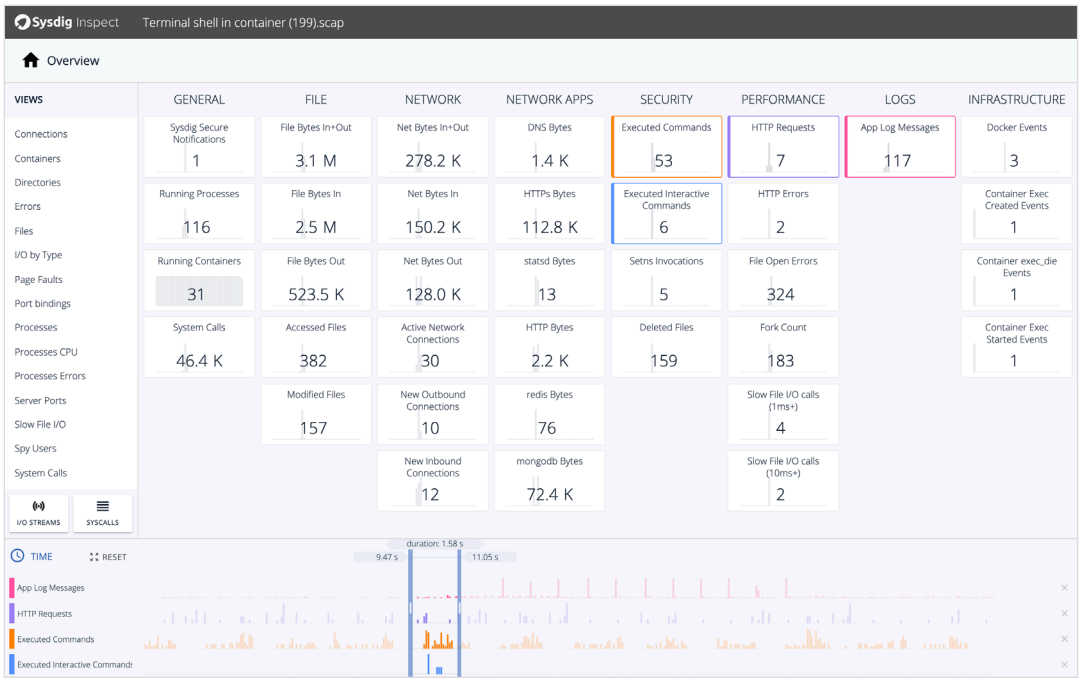
Sysdig will deliver notifications to your alerting channels, AWS SNS, or SIEM. This allows you to consolidate security findings across your container environments so you can view and manage security alerts, and automate compliance checks across your AWS account. Both Sysdig Secure and Falco send events to Cloudwatch through FireLens, as seen on Multi-cluster security with Falco and AWS Firelens on EKS & ECS.

With Sysdig, security teams can resolve issues inside pods and conduct forensics by reconstructing system activities correlated with AWS context.

Sysdig provides:

- **Detailed forensics reports** to quickly understand and contain the impact of any security breach.

- **Streamlined incident response** to quickly determine what happened with a detailed activity record. Audit trails help you easily recreate the steps taken on intrusion, including file activity, network traffic, application protocols, commands, logs, or events. This enables you to investigate incidents such as data exfiltration, lateral movement, etc, allowing you to recover quickly and strengthen defenses going forward.
- **Post-mortem analysis** on a container outside production. This lets you analyze forensic captures and recreate all system activity, even if the EKS, ECS, or Fargate containers are no longer running.



Better together with AWS and Sysdig Secure DevOps Platform

Sysdig and AWS have a long partnership designed to help customers easily migrate workflows and transition to applications built on top of AWS container and cloud services. With Sysdig, enterprises gain the ability to take advantage of those things the cloud is optimized to do: develop and deliver rapidly, innovate continuously, scale business and technology operations, trade capital expenses for variable ones, and do it all with the necessary security and visibility needed to protect users, data, and resources.

Sysdig Secure gives organizations immediate and comprehensive cloud security that enables them to uphold their part of the AWS shared responsibility model. The Sysdig Secure DevOps Platform allows DevOps and Cloud teams, running container workloads on AWS container services, to embed security into their workflows, get visibility into performance and availability, monitor their containers, and implement compliance requirements.

All of these integrations are supported by Sysdig as an AWS Advanced Partner in the AWS Partner Network (APN) with competencies in container security, monitoring, and DevOps. Our goal is to help customers securely run any workload on AWS.

There are several different security and monitoring layers that developers, platform operations, and security teams have to keep in mind as they build cloud applications. The following table summarizes these layers and highlights the capabilities of AWS container services, as well as the joint benefits of leveraging the Sysdig Secure DevOps Platform to further enhance security, compliance, and monitoring for containers and Kubernetes.

Container platforms

Platform	AWS Solution	Benefits of Sysdig + AWS
Kubernetes	Amazon Elastic Kubernetes Service (EKS)	Automate security compliance and monitoring to confidently run containers, Kubernetes, and cloud.
Cloud containers	AWS Elastic Container Service (ECS)	Automate security compliance and monitoring to confidently run containers, Kubernetes, and cloud.
Serverless compute for containers	AWS Fargate	Get comprehensive visibility and a unified view across AWS Fargate security posture, vulnerabilities, threats, and performance.

Security

Security Layers	AWS Solution	Benefits of Sysdig + AWS
Host OS	Amazon Linux 2, Bottlerocket	Implement host scanning to identify OS and non-OS vulnerabilities. Analyze EC2 configurations to ensure hosts meet CIS benchmark best practices.
Access Control and Cloud Infrastructure Entitlements Management (CIEM)	AWS Identity and Access Management (IAM) IAM Access Analyzer	Monitor IAM changes for unexpected changes and security threats. Gain visibility into excessive permissions and entitlements, manage and enforce least privilege access, and simplify audit of access controls to meet compliance. Implement service-based access control to streamline security and monitoring information to an individual user/team.
Image Scanning & Vulnerability Management	Amazon ECR scanning with Clair (Package Image scanning)	Scan images pre-deployment within CI/CD pipeline or registries (e.g.,ECR, CloudBuild, CloudPipeline, Quay, DockerHub, etc.). Get runtime vulnerability reporting to assess the impact of new CVEs.
Compliance	AWS Config	Enforce continuous compliance with out-of-the box configuration checks for CIS, PCI, NIST, SOC 2, etc., and report with custom assessments and dashboards.
Network Security	Amazon EC2 security groups	Automate and simplify use of native Kubernetes network policies. Visualize all network communication between pods, services, and applications. Audit connections to or from any process and implement a Zero Trust approach to container security.

Security Layers	AWS Solution	Benefits of Sysdig + AWS
File Integrity Monitoring		Sysdig Secure filesystem policies make it easy for you to quickly implement file integrity monitoring (FIM) and alert on any suspicious changes to files and directories.
Cloud Workload Protection Runtime Detection & Threat Prevention		Scope runtime security policies based on any AWS, ECS, and EKS label/metadata to detect and prevent anomalous behavior. Detect and block attacks, combining deep visibility through system calls, CloudTrail logs, and audit events with AWS metadata. Powered by open-source CNCF runtime security project Falco.
Cloud Security Posture Management	AWS CloudTrail CIS AWS Foundation Benchmarks AWS GuardDuty	Discover cloud assets, gain visibility into configuration issues, and detect cloud service threats. Sysdig unifies CSPM and cloud threat detection with cloud workload protection to reduce the time to detect threats in your AWS cloud services.
Container Forensics		Conduct forensics and post-mortem analysis even after ECS or EKS terminates containers/pods.

Conclusion

AWS cloud and container services are helping organizations move fast and innovate to deliver solutions that meet customer and market needs. AWS provides coverage for security and monitoring of cloud accounts, workloads, and containers. As you scale out your applications, clusters, locations, and integrations, Sysdig helps you confidently run containers, Kubernetes, and cloud with a container and cloud security stack built on open-source innovation. Sysdig complements AWS services with deep and unified security and visibility. They are radically simple to run and scale, protecting your workloads wherever you choose to operate with AWS public and hybrid cloud infrastructure.

Additional resources

Partnership Overview

Sysdig & AWS partner page

Sysdig & AWS partner brief

Guides

5 Keys to a Secure DevOps Workflow on AWS

Continuous Cloud Security Checklist for AWS

Case Studies

Worldpay gains competitive edge with faster delivery of PCI-compliant payment solutions

Webinars

Accelerate Threat Detection Across AWS Cloud and Containers

Ship Apps Faster on AWS with Unified Visibility and Security

Find out how the Sysdig Secure DevOps Platform can help you and your teams confidently run cloud-native apps in production. Contact us for additional details about the platform, or to arrange a personalized demo.

www.sysdig.com