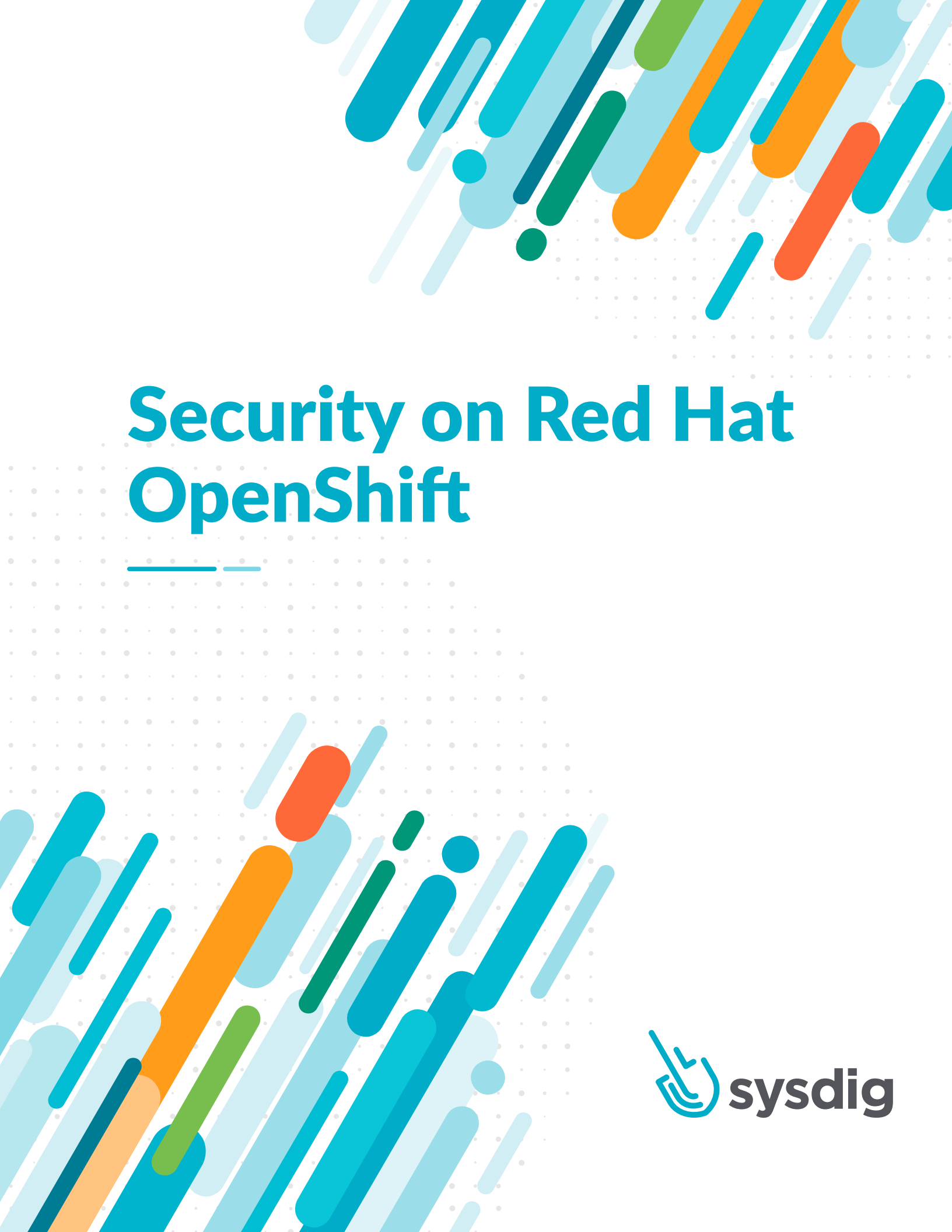
Security on Red Hat OpenShift



Contents

About This Guide

As enterprises begin to move from initial sandbox to production deployments, they face operational challenges in maintaining container security and reliability.

New paradigms like containers, microservices and hybrid cloud workloads disrupt the way enterprises implement security processes. Containers provide a great level of portability and isolation, which make them ideal for moving applications from development into production. They are like black boxes, however, which means it's harder to see what's inside in order to monitor and secure them.

By creating a Secure Devops workflow that integrates security, compliance and monitoring, organizations can accelerate deployment and confidently run container workloads in production on OpenShift with Sysdig, whether SaaS or on-premises. This allows you to:

- Speed up deployment by validating security policies and configurations during the build process.
- Stop runtime threats without impacting performance.
- Prevent issues by monitoring performance and capacity and organizations using Kubernetes-native controls.
- Have a single source of truth to accelerate incident response and streamline compliance.

This definitive guide for security and compliance on Red Hat OpenShift discusses how you can ship cloud applications faster by embedding security, compliance and monitoring into your DevOps workflow. The Sysdig Platform on OpenShift is open by design, with the scale, performance and usability that enterprises demand.

Why security is top of mind for OpenShift users

The primary goal of OpenShift is to provide a great experience for development, operations and security teams to build, deploy and securely run containerized workloads and accelerate container application deployment. But different teams and roles have different concerns and points of view on what security means, what's required to move into production and how to implement new security processes.

Developers

OpenShift helps developers take advantage of both containerized applications and orchestration without having to know the underlying infrastructure details. OpenShift pipelines streamline the process of building, distributing and deploying containerized applications. Using Source-to-Image (S2I), an open-source framework for combining source code and base images, developers can push changes to a repository (such as Github). OpenShift will create a container image from the source code and push it to a built-in private registry. Ensuring these images are free of known vulnerabilities and following security best practices is a major challenge that often compromises application integrity.

Cloud/DevOps

Operations teams are responsible for maintaining high availability, quality of service and health of the application and infrastructure. Teams often use the built-in web console to manage the infrastructure and platform capabilities, and also to leverage playbooks to automate application deployments. Operations teams are required to ensure they build security into the platform with features like pod security policies, network policies, and more.

Security and compliance

Security operations, SecOps, DevSecOps and CSIRT teams need to continuously monitor OpenShift environments at runtime to protect against anomalous behavior and zero-day attacks, as well as perform incident response if a violation occurs. Teams need to monitor new container infrastructure and applications that are deployed to ensure they conform with regulatory and internal compliance requirements.

Managing security risk on OpenShift with Sysdig

Why customers benefit from using OpenShift with Sysdig

With unified security, compliance and monitoring, enterprises can confidently run cloud-native workloads on OpenShift in private, hybrid and multi-cloud environments. By automating security, compliance and monitoring for a secure DevOps workflow, teams can maximize performance, manage security risk and ship cloud applications faster.

OpenShift provides security capabilities, including:

- Host infrastructure with RHEL/RHCOS.
- Vulnerability scanning with Clair.
- Extensive compliance audit workflows with OpenSCAP.
- OpenShift platform built-in security controls like RBAC and OAuth, Pod Security Context, Security Context Constraints (SCC) and Pod Security Policy to enforce them, Network Policy and Image Policy capabilities.

Sysdig extends Red Hat OpenShift capabilities, providing additional security capabilities, including:

- Extensive image scanning, including third-party libraries, configuration validation and vulnerability management.
- Runtime security to detect and block attacks, and implement zero-day threat protection, powered by Falco, the open-source cloud native runtime security project.
- Incident response, container forensics and audit with deep visibility into container activity.

Maximize Performance & Availability

- Security monitoring for OpenShift, and other container and cloud workloads across multiple providers.

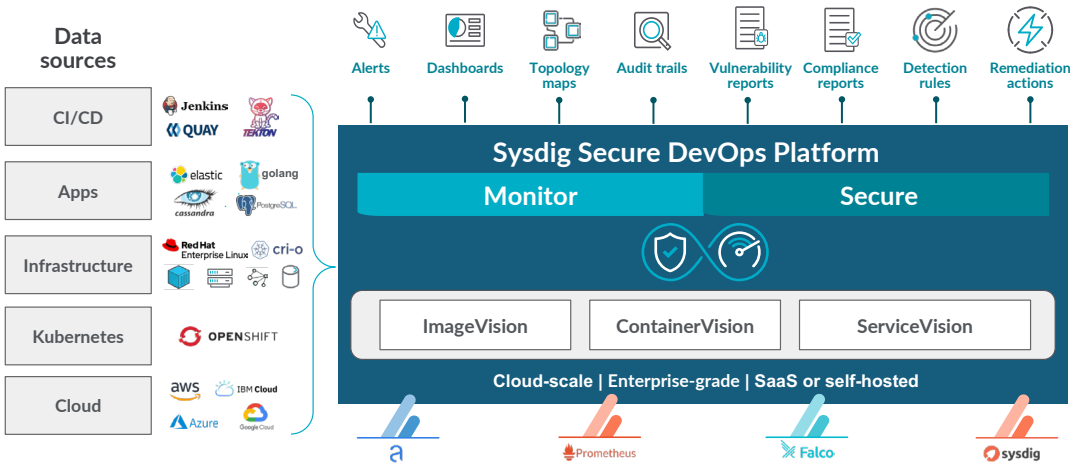
Validate Compliance:

- Compliance validation across the application lifecycle to help implement regulatory compliance standards like, NIST, PCI, etc.
- Check configuration against CIS benchmarks and internal security standards.

Sysdig provides centralized visibility and security for operating OpenShift at scale. With a single agent deployed per host, Sysdig can scale to 10,000+ nodes to secure and monitor containers and applications running on OpenShift clusters.

Sysdig enhances the Red Hat security portfolio provided with the OpenShift platform across the entire application lifecycle. This gives customers more confidence in their Red Hat OpenShift platform and allows the business to accelerate and expand their digital transformation initiatives.

Sysdig Secure DevOps Platform



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

Host Security

Red Hat Enterprise Linux (RHEL) and CoreOS (RHCOS) come with extended Linux security features, such as:

1. Linux namespaces and control groups used by CRI-O, to create the isolated container limiting visibility and resources of the processes running inside.
2. seccomp profiles, that restrict the system calls that a container can execute.
3. SELinux profiles to enforce access control policies.
4. Fine-grained control over superuser permissions, allowing certain behaviors without running as the root user.
5. Controlled immutability (with RHCOS) to lock down management via remote management from the OpenShift cluster and limit OS modifications to only a few system settings.

These critical capabilities ensure a baseline level of trust and security in the host operating systems (RHEL/RHCOS). These are typically applied to containers through the container engine like CRI-O and orchestrated by OpenShift through Pod Security Context and Pod Security Policy definitions.

Authentication and Authorization

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

OpenShift provides…

The OpenShift Container Platform master includes a built-in OAuth server. Users and service accounts can obtain OAuth access tokens to authenticate themselves to the API as a form of role-based access control (RBAC). Often, OAuth leverages an existing external directory like LDAP or Active Directory.

OpenShift leverages Kubernetes RBAC system to define what users and services can do (create, read, update, delete) and communicate across any resource within the cluster (nodes, projects, deployments, pods, etc.).

Sysdig adds…

Sysdig can leverage OpenShift resources to define who can access any of the visibility, metrics, notifications and security policies provided by Sysdig. This is known as Teams, introducing the concept of service and metadata-based access control to complement the existing RBAC mechanisms of OpenShift.

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

Sysdig supports 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

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.

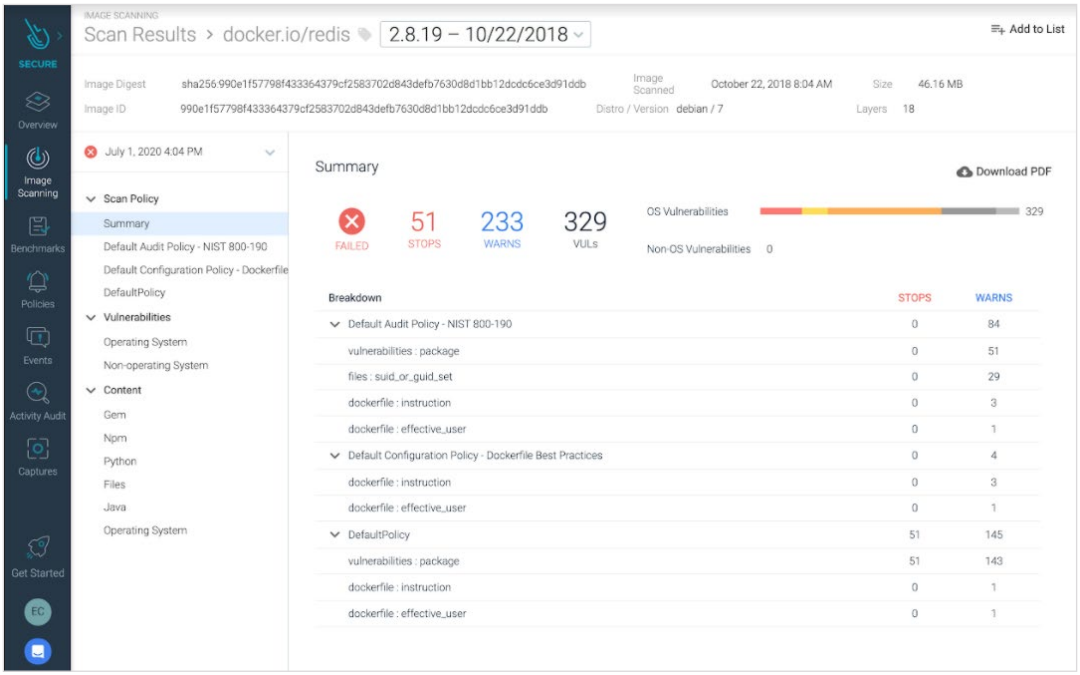
OpenShift provides…

Clair is the open-source engine that powers the Red Hat Quay container registry security scanner to detect vulnerabilities in OS packages across images within Red Hat Quay, and then notify developers as those issues are discovered. Red Hat Quay and Clair have boosted confidence in using containers in production, and organizations now want to get deeper into vulnerability scanning policies, security best practices, and regulatory compliance.

Sysdig adds…

Sysdig extends existing Red Hat image scanning capabilities with a customizable policy enforcement engine that has a wide variety of security checks and best practices. This allows users to create a customized security policy to 'shift left' security responsibility. Application developers and DevOps engineers gain deeper visibility earlier in the life cycle as they build their applications, going further than just a list of OS packages CVEs by looking at:

- Third-party libraries vulnerability detection (Java, Python, Ruby and NodeJS).
- Secrets credentials like passwords, tokens or keys inside container images.
- Container best practices (i.e., immutable builds, health checks, avoiding 'latest' base images, etc.).
- Security best practices (i.e., restricted port exposure, running as a privileged user, blacklisted distros, packages or licenses, etc.).



Combining all of these capabilities, users can build policies like “Detect if any running image that has a vulnerability classified as medium or high and there has been a fix available for more than seven days.”

DevOps and security teams can easily query across a catalog of images, packages, and CVEs, as well as check for advanced conditions like CVE age, fix available, software version, and more. Finally, these reports can be downloaded and shared (PDF/CSV) with vulnerability management teams, CISO’s, etc.

CI/CD pipeline security

OpenShift provides…

OpenShift tightly integrates with Jenkins and Tekton (used in OpenShift 4.1+ Pipelines) to implement Continuous Integration/Continuous Delivery (CI/CD) pipelines. This allows developers to automate builds, code inspection, scanning and test validation.

Sysdig adds…

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

Leveraging Sysdig’s scanning integration with CI/CD pipelines, developers can directly understand why a failure occurred and what needs to be fixed without leaving the CI/CD UI. 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.

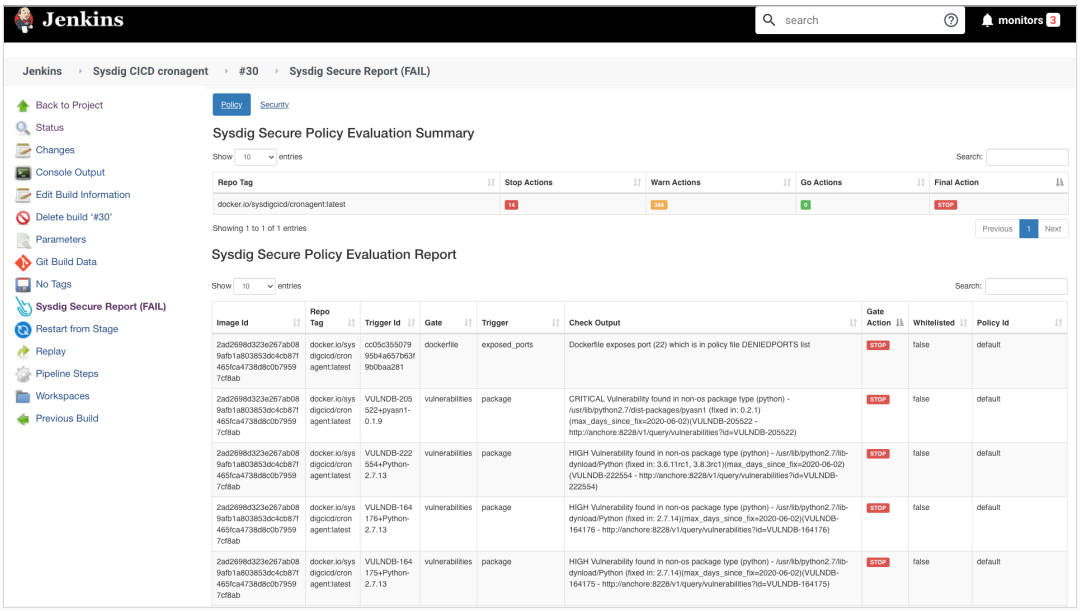


Image assurance

OpenShift image policies or Kubernetes admission controllers can be used to prevent unapproved images from being deployed on the cluster. OpenShift will check against Sysdig Secure whether an image is compliant with the configured security policies and new deployments will be blocked or go through. 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 passed the checks.

Registry Security

OpenShift provides...

Red Hat provides certified containers for Red Hat products and partner offerings via the Red Hat Ecosystem Catalog, which is a public container registry hosted by Red Hat. Container content is monitored for vulnerabilities by Red Hat and updated regularly. At the same time, quay.io offers hosted public and private repositories for application container images in the Cloud.

If you are hosting images locally, OpenShift comes with its own registry. For more advanced requirements, Red Hat also provides Quay, a secure private container registry tailored for the enterprise.

Sysdig adds...

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

Compliance

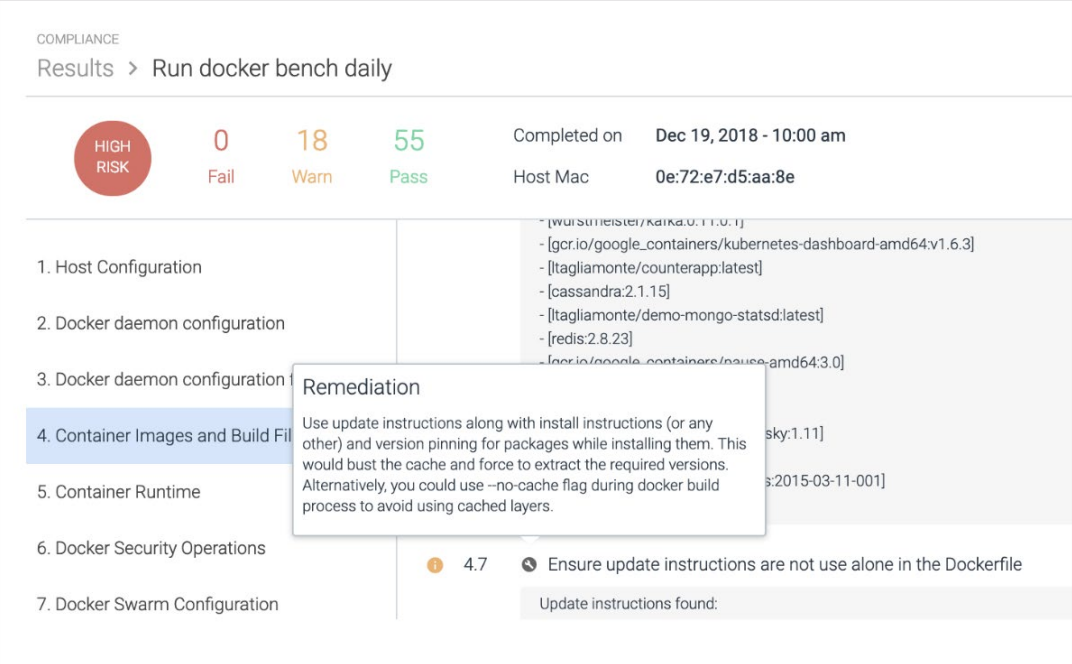
Enterprise computing environments, running microservices and OpenShift, consist of hundreds or thousands of interconnected applications and services, and a large and diverse set of users. To maintain control over the security of this vast environment, a standard way to scan systems for compliance with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

OpenShift provides...

Red Hat Enterprise Linux and Red Hat CloudForms provide tools that allow for fully automated compliance audits. These tools, under the OpenSCAP project umbrella, are based on the Security Content Automation Protocol (SCAP) standard. Within these tools, you will find specific container-oriented checks, like oscap-docker, that perform CVE scans of containers and check them against predefined policies. This is done to validate security compliance content as well as generate reports and guides based on these scans and evaluations.

Sysdig adds...

Sysdig extends compliance across the OpenShift container lifecycle for standards like NIST and PCI, and tracks progress using compliance dashboards. Starting with the infrastructure layer, Sysdig performs specific host and platform compliance checks, like Kubernetes benchmarks and Docker CIS benchmarks, and also provides remediation guidance for policy violations occurring in OpenShift master or worker nodes. This makes it faster to resolve configuration issues when they come up.

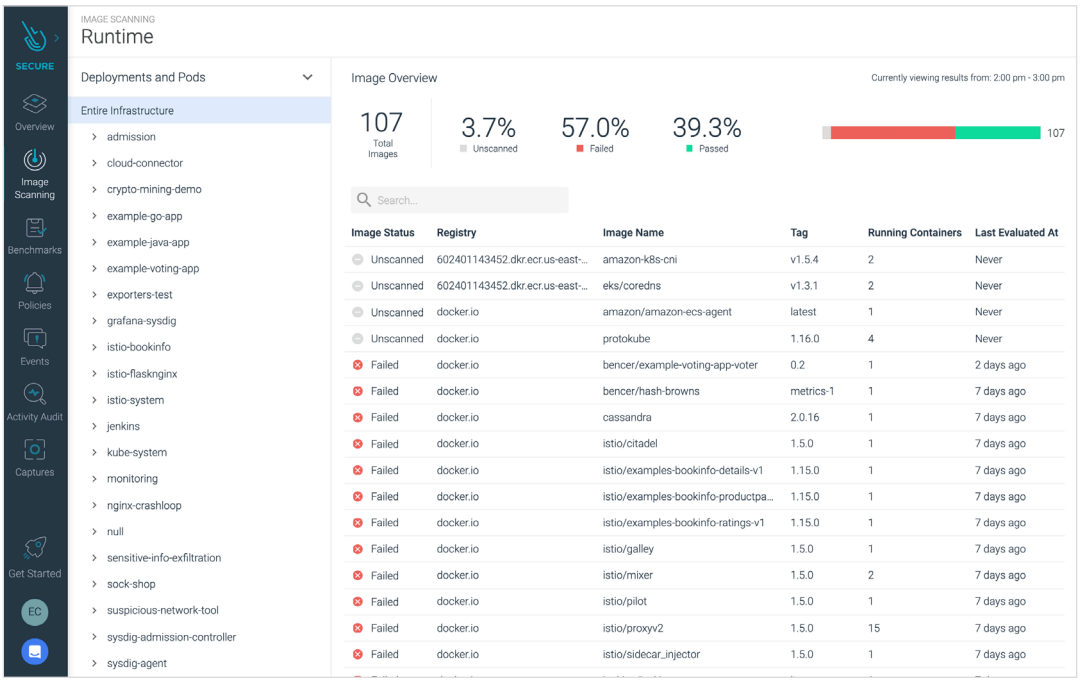


Sysdig Secure gives you the tools to implement container image security and compliance best practices, such as NIST SP 800-190, PCI DSS, Dockerfile and more. Using Sysdig Secure container image scanning policies, you can validate cloud compliance and enforce best practices, including:

- 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. This enables analysis of 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 OpenShift API for auditing purposes (audit secret resources access, requests by unauthorized users, etc.).

When a new high/critical CVE is published, Sysdig Secure lets you assess your exposure immediately. You can quickly identify all the affected services and accountable teams. Developers or application owners are identified using Kubernetes or via cloud metadata, like service, deployment or application, and alerted to view their images and vulnerabilities.

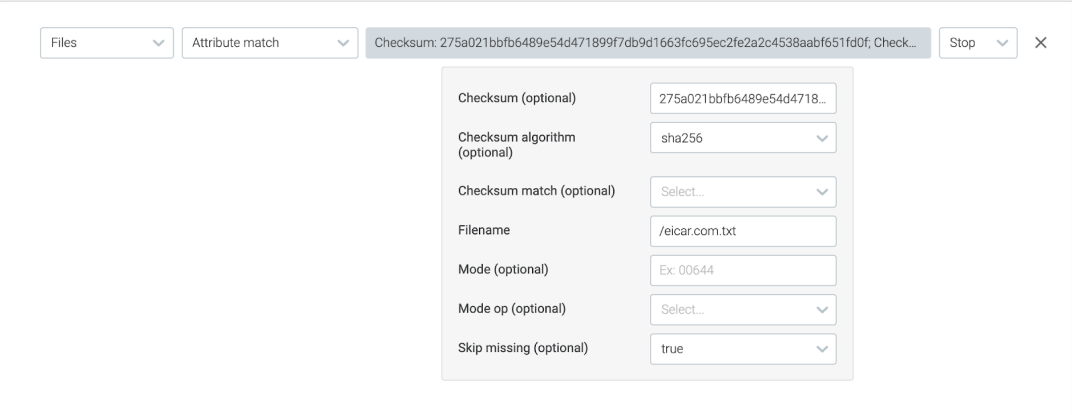


File Integrity Monitoring

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 address security risks as soon as possible and fail builds early if FIM policies are not met. The file integrity monitoring policy allows you to:

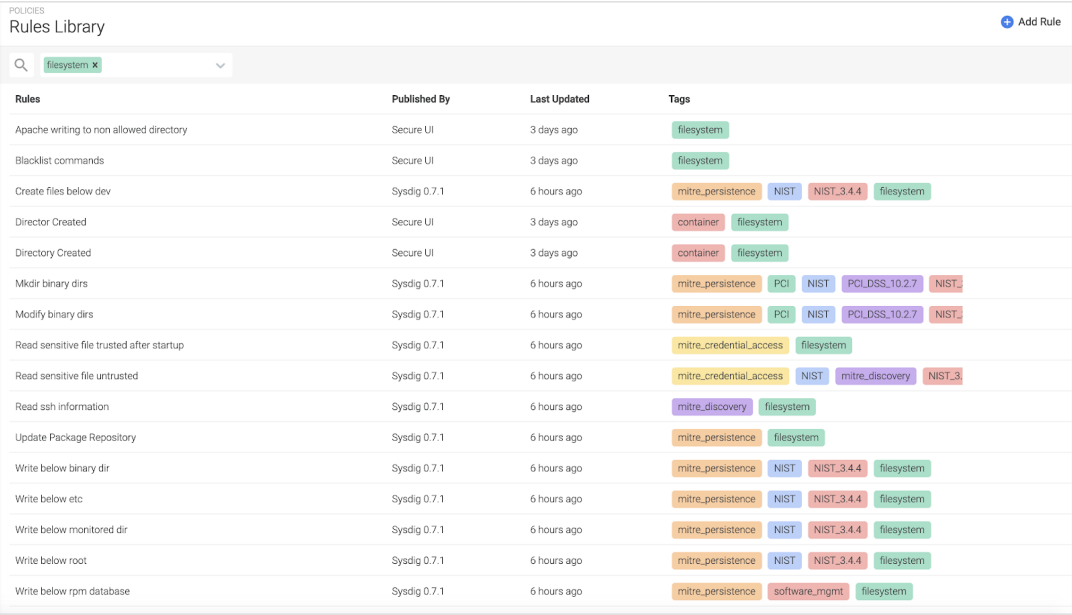
- Check if a **file exists** or is missing, and trigger alerts based on the condition.
- Validate a specific file against its **SHA256 hash**. You already know the SHA256 for the binary or binaries in your containers. Any modification to the executable files is suspicious and potentially dangerous.
- Validate **file permissions**. For example, if a file has an executable bit where it's not expected, you should flag that as an alert.
- Check for **file names** based on regex.
- **Inspect contents**, looking for exposed passwords, credential leaks, etc.



Sysdig Secure provides default container image scanning policies and user defined policies.

You can also implement FIM policies at runtime that would 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:

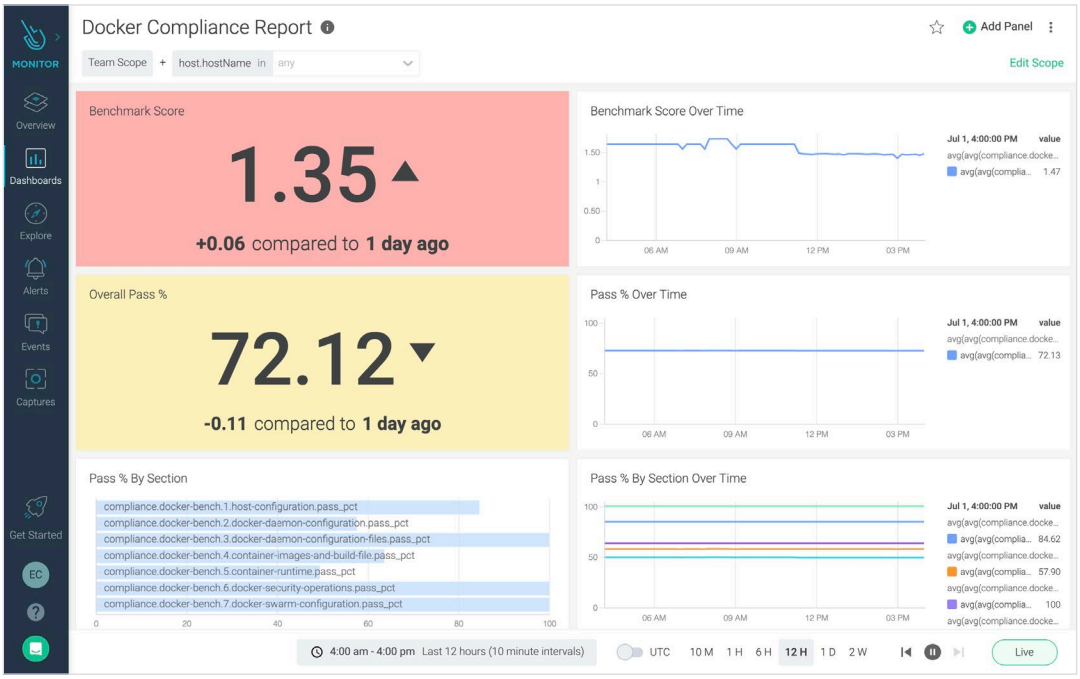
- Creation or removal of files or directories.
- Renaming of files or directories.
- Changes to file or directory security settings such as permissions, ownership and inheritance.
- Changes to the files of a container.
- Modification of files below the container's path.
- Deletion of bash history.



Filesystem policies in the Rules Library in Sysdig Secure makes it easy for you to quickly implement FIM policies.

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 OpenShift clusters.



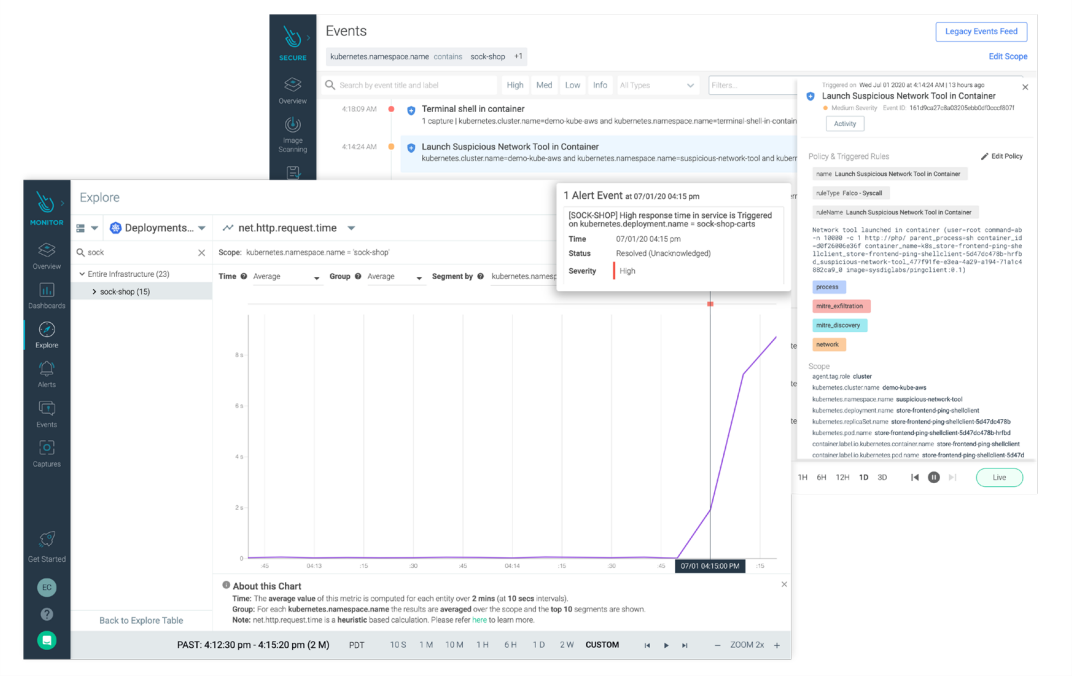
Runtime Security

Security monitoring - Continuous monitoring of container runtime environment

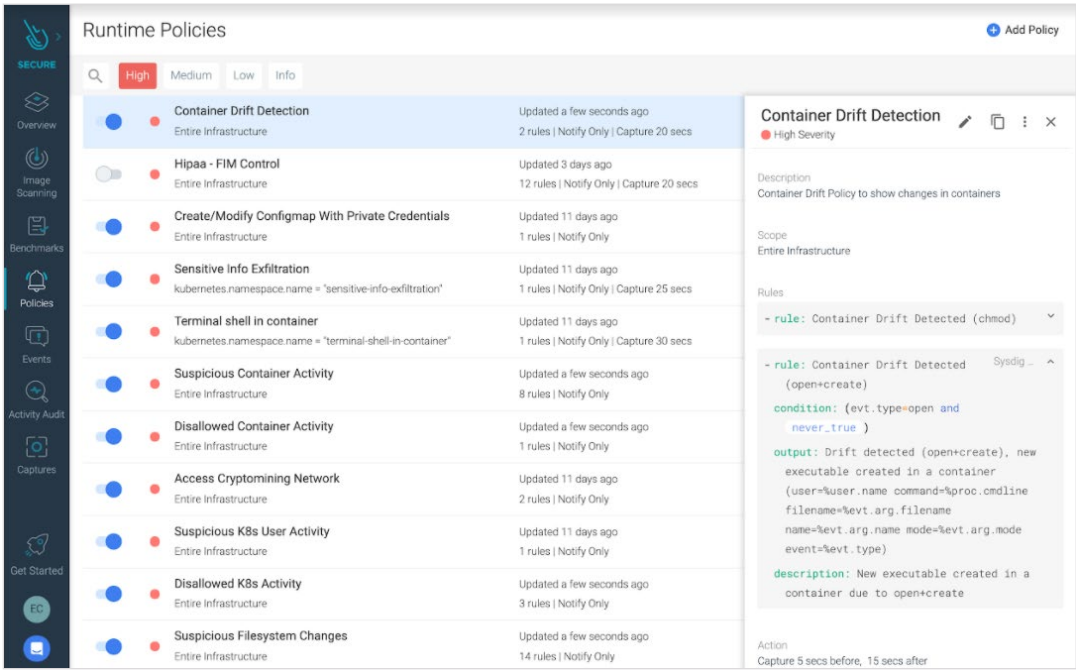
Gaining visibility across both monitoring and security data turns out to be the biggest challenge for a successful transformation journey. For example, the security team needs to know if a crypto-mining or denial of service (DoS) attack can be further explained by an abnormal deviation in a particular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

Sysdig adds…

Sysdig provides deep visibility into containers, network, filesystem, application and system activity, without invasive instrumentation, to provide comprehensive visibility across OpenShift environments. Leveraging the latest eBPF kernel technology, the Sysdig agent instruments through the host OS (with full support for RHEL and RHCOS) without tampering with container images or the code.

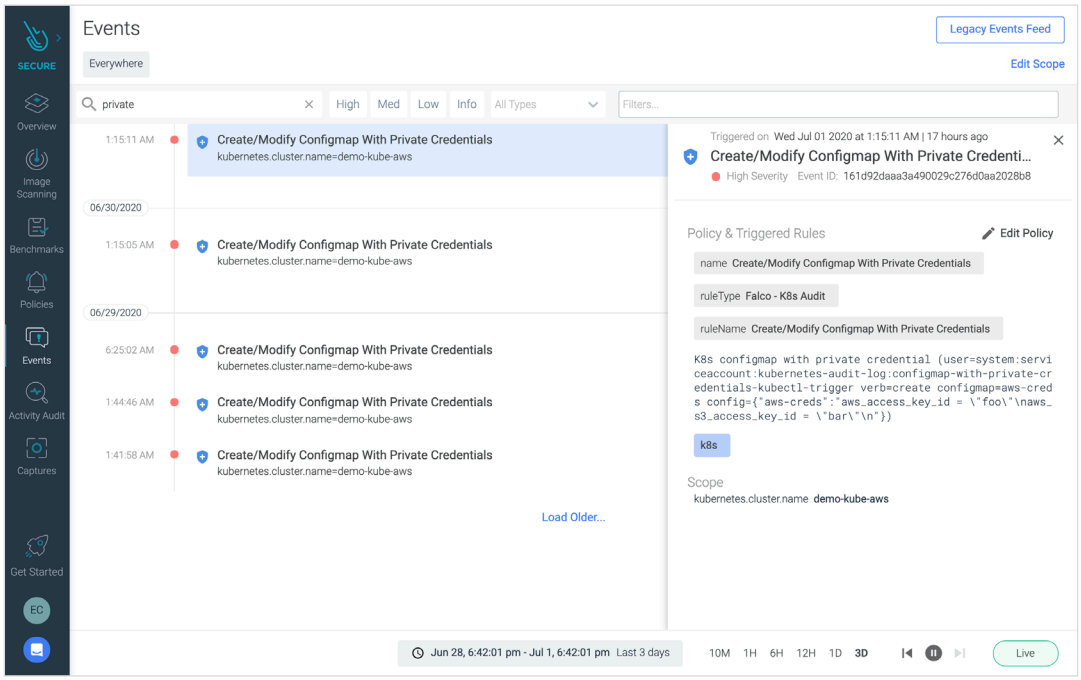


Controlling changes from the original image that security approved can be a significant challenge. Configuration drift increases the chance of lateral movement (e.g., altered RBAC settings) and other runtime security threats. Sysdig Secure provides real-time visibility to quickly fix configuration drift.



Sysdig also taps into the OpenShift audit log API to detect suspicious activity coming from users (via kubectl or oc command line) and serviceAccounts (via the API), for example:

1. Storing clear text credentials or access keys in deployment configMaps.
2. Attempts to create Pods with elevated privileges, unapproved images or sensitive mounts.
3. Unauthorized attempts to create privileged serviceAccounts, roles or clusterRules.
4. Tampering within the Kubernetes control plane namespace.



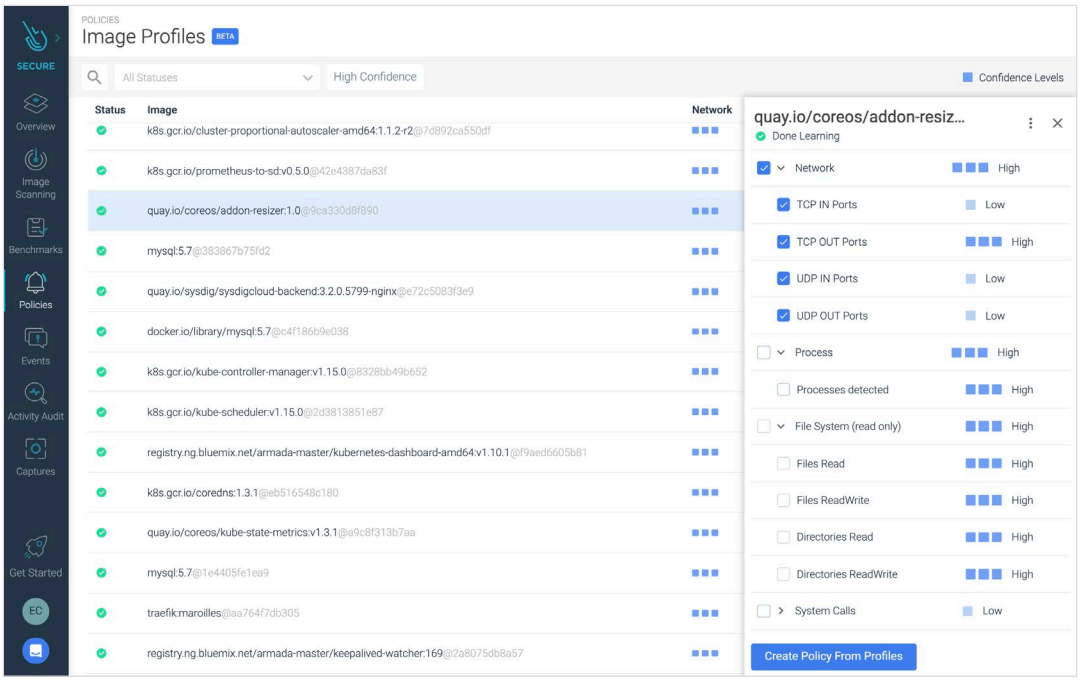
Threat detection

Scanning your containers once during the CI/CD process or from your OpenShift 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.

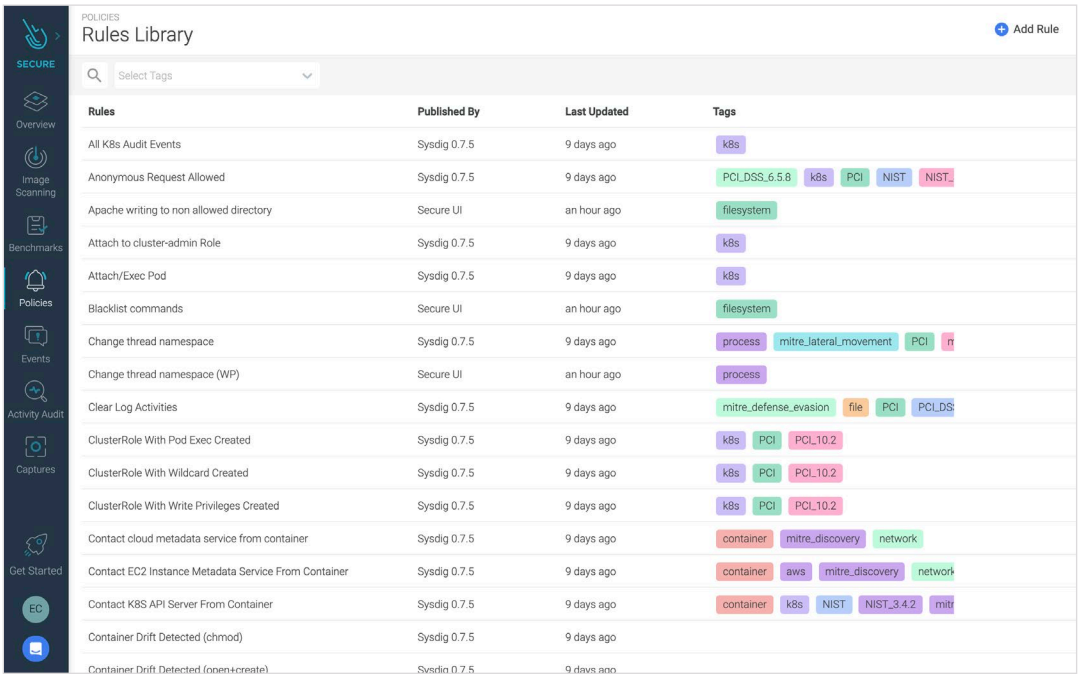
Sysdig adds…

Sysdig's approach to runtime defense in large-scale environments is to automatically model runtime behavior through a machine learning process. Analyzing kube-apiserver activity and syscalls while enriching them with various metadata, including OpenShift and cloud provider labels, allows Sysdig to create a robust container runtime profile.



More than 60 default runtime security policies are available out-of-the-box, including:

1. Container runtime security policies for regulatory container compliance standards: NIST SP 800-190, PCI, CIS or MITRE ATT&CK framework.
2. Runtime detection of the most pervasive container attacks: cryptomining, secrets exfiltration, container isolation breaches and lateral movements.
3. Security monitoring for unexpected process activity, outbound connections and terminal shell sessions.



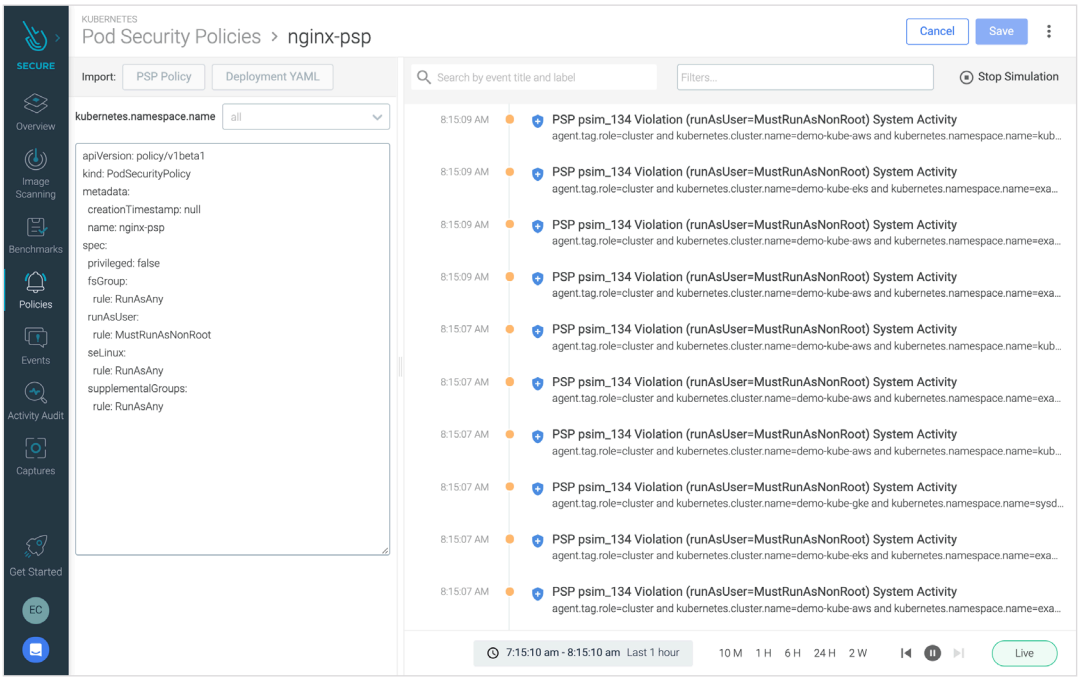
With an extensible policy engine powered by the CNCF Falco project, operations and security teams can customize or write their own rules through a visual interface to build fine-tuned policies that match their requirements. Falco rules that are community sourced and curated are available on the Cloud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

Runtime rules can be applied to any scope such as a particular OpenShift cluster, namespace, deployment, pod, etc., and managed at scale across multiple clusters, cloud providers and data centers.

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.

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.



Container Forensics and Incident Response

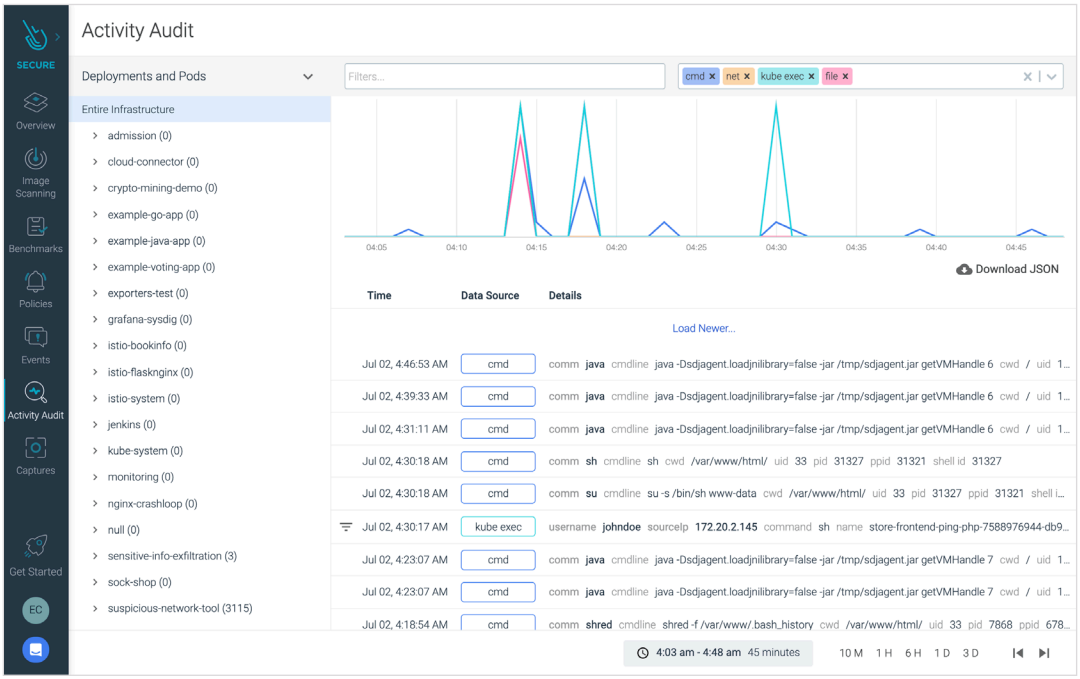
The ephemeral nature of containers makes it difficult to analyze what happened with a security incident after the container is gone. How can you reproduce the steps taken by the intruder? How did they gain access? What was the impact? Did they install any malware? Was any data leaked? How far did the attack extend?

Sysdig adds…

With Sysdig, security teams can resolve issues inside pods and conduct forensics by reconstructing system activities correlated with OpenShift application 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. Fine-grained policies leverage the Falco rules library to analyze and audit runtime policy violations. You can easily recreate the steps taken on intrusion, including file activity, network traffic, application protocols, commands, logs or events so you can investigate events such as data exfiltration, lateral movement, etc. This allows 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 OpenShift container pods are long gone.



Better together with Red Hat OpenShift + Sysdig Secure

There are several different security layers that developers, platform operations and security teams have to keep in mind as they are building their cloud applications on OpenShift. The table below summarizes these security layers and highlights the security capabilities of OpenShift, as well as the joint benefits of leveraging Sysdig Secure to further enhance the security and compliance posture of the OCP platform.

Security Layers	OpenShift	Benefit of Sysdig + OpenShift
Host OS Security	RHEL/RHCOS	Continuously scan the underlying Docker host configuration and ensure it meets CIS benchmarks.
Access Control	OAuth/RBAC	Implement service-based access control to streamline security and monitoring information to an individual user/team.
Image Scanning	Clair (Package Image scanning)	Scan image pre-deployment within the CI/CD pipeline or any OpenShift registries (RedHat Quay/DockerHub/etc.) Sysdig also provides runtime vulnerability reporting to assess the impact of new CVEs.
Compliance	OpenSCAP Red Hat Insights	Enforce continuous compliance for PCI, GDPR, HIPAA, etc. and report with custom assessments and dashboards.
Runtime Detection & Threat Prevention		Detect and block attacks, combining deep visibility through system calls with OpenShift metadata, labels and audit events. Powered by Falco, the open-source cloud native runtime security project originally developed by Sysdig.
Container Forensics		Conduct forensics and post-mortem analysis even after OpenShift terminates containers/pods.

Conclusion

OpenShift provides a baseline coverage for security across the entire container platform. As you scale out the number of applications, clusters, locations and cloud providers, Sysdig provides centralized visibility and security, complementing the existing Red Hat offerings.

Sysdig extends existing Red Hat security controls supplied on OpenShift platform, providing container security coverage across the build, run and respond lifecycle. This gives you more confidence in the Red Hat OpenShift platform and allows you to confidently run cloud native applications in production.

Sysdig Red Hat certifications

OpenShift users can download the Sysdig agent and the Sysdig agent operator from the Red Hat Container Catalog. This provides greater peace of mind knowing the agent container image and the operator are Red Hat certified and come with enterprise support.

Sysdig agent supports both OpenShift 3.X and 4.X, Red Hat Enterprise Linux version 7 and 8, and RHCOS.

Sysdig platform is available through a SaaS offering from Sysdig or can be deployed within your environment and in air-gapped environments on top of your existing OpenShift infrastructure.

Read more on Sysdig @ Red Hat Ecosystem Catalog.

Additional Resources

- OpenShift partnership brief
- Sysdig/OpenShift Partnership

Videos

- Chris Morgan on Sysdig and Red Hat partnership, Openshift insights: visibility and security
- Sysdig and Red Hat case story: ATPCO

Success Story

- Ford Motor Company optimizes delivery with cloud platform

Webinars

- DevOps Security, Monitoring and Compliance with OpenShift and Sysdig
- The 5 must-do's when implementing cloud native security in Red Hat OpenShift

Sysdig trial

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