nuaware
An Exclusive Networks Company

Solution Brief

Better together: Securing Docker Containers with Sysdig

www.nuaware.com

nuaware
An Exclusive Networks Company

Securing Docker Containers with Sysdig

Cloud-native services like containers, Kubernetes, and serverless have transformed application development, but traditional security tools struggle to provide visibility into containerized workloads. This results in an overwhelming number of alerts, making it difficult to focus on real threats. Sysdig is purpose-built for the cloud, enabling enterprises to secure their workloads at cloud speed by leveraging Runtime Insights.

Sysdig enhances container security by providing a complete cloud-wide context, allowing teams to prioritize the most significant risks and detect active lateral movement. Rather than viewing container vulnerabilities in isolation, Sysdig correlates security findings across the entire cloud infrastructure to expose real threats.

Real-Time Detection and Response

- Full visibility across containers, servers, kubernetes, and serverless to detect threats in less than 5 seconds.
- Capture all interactive commands and system calls to investigate and respond in minutes.

KSPM

- Tie Kubernetes security violations with the infrastructure-as-Code (IaC) manifest the defines your Kubernetes resource.
- Auto-generate pull requests for remediation directly at the source.

Vulnerability Management

- Identify in-use packages to prioritize the most critical vulnerabilities to fix first.
- Simplify setup and scanning using an agentless approach to find vulnerabilities across your cloud environment.

Agentless Cloud Context

- Multidomain correlation between containers and cloud to automatically identify the riskiest combinations without any manual matching.
- Alert on log activity via Falco in real time to highlight active cloud risk.

nuaware
An Exclusive Networks Company

Why Docker and Sysdig Are Better Together

Falco

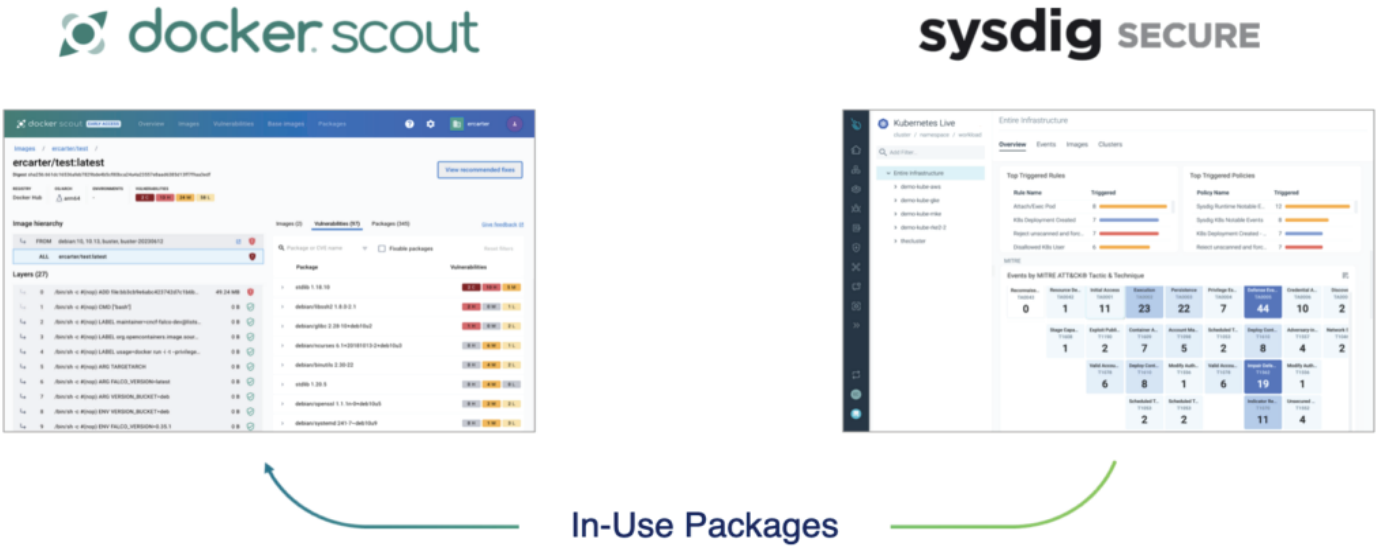
Sysdig provides unmatched visibility into containers and Kubernetes, helping teams quickly identify critical vulnerabilities and detect threats. By correlating container security data with other cloud insights, Sysdig ensures the most pressing risks are addressed before attackers can exploit them.

The Power of Runtime Insights

Sysdig Sage™

Docker Scout offers developers actionable insights into the software supply chain, helping them enhance application security and reliability. By partnering with Docker, Sysdig adds an extra layer of runtime security, delivering better visibility and empowering development and security teams to focus on real, imminent risks.

Sysdig Secure™



nuaware
An Exclusive Networks Company

Key Benefits of Sysdig Runtime Insights with Docker Scout

Ship More Secure Images

Developers can compare images from the build phase to those running in production, quickly identifying risks, eliminating unnecessary packages, and building leaner, more secure container images. Integration with the Docker Build and Push GitHub Action provides insights directly within GitHub, preventing the deployment of risky images.

Eliminate Shift-Left Security Gaps

Shift-left security enables teams to make informed decisions earlier in development. By correlating image analysis with runtime context, Docker and Sysdig generate actionable insights to secure the software supply chain effectively.

Accelerate Cloud-Native Application Delivery

Sysdig Runtime Insights streamline software validation, allowing developers to identify and remediate imminent risks quickly. This speeds up innovation and ensures secure cloud-native application delivery.

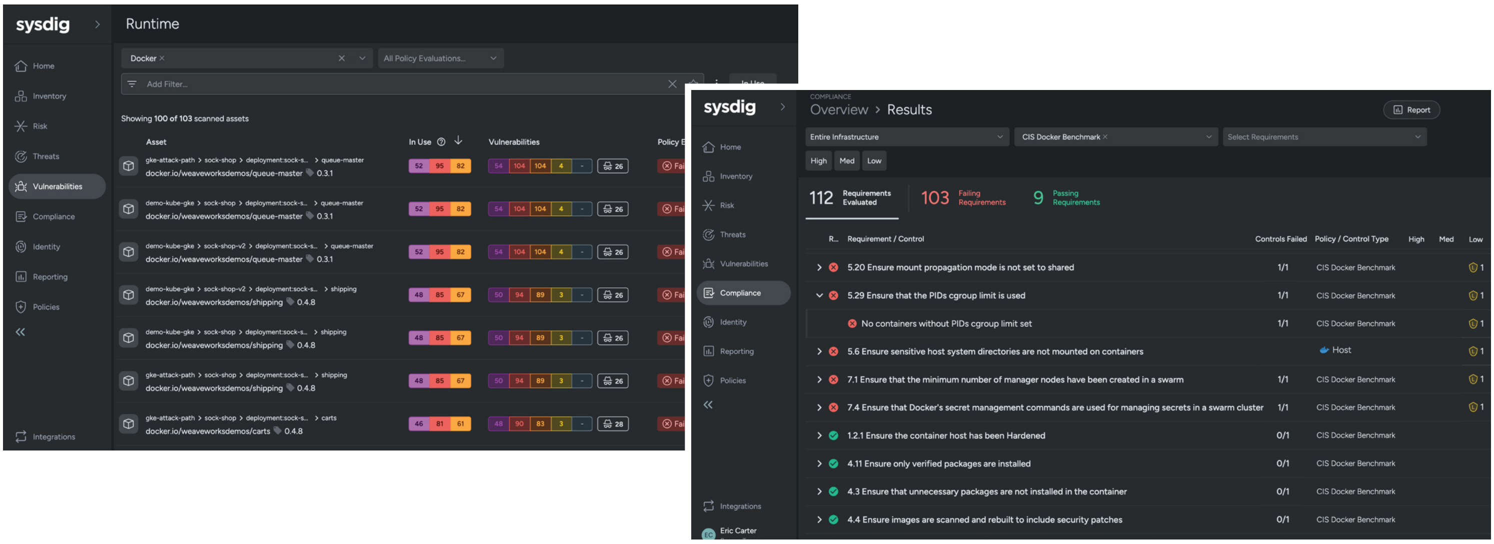
Reduce Monitoring Noise

Sysdig and Docker users can cut security alert noise by up to 95% by distinguishing between active vulnerabilities and inactive ones. This enables security teams to focus on the most critical issues, saving time and improving efficiency.

Get Started Today

Secure your Docker containers with Sysdig and gain the visibility you need to protect your cloud-native applications.

Contact us today to learn more.



Runtime

Docker ×

All Policy Evaluations...

Add Filter...

Showing 100 of 103 scanned assets

Asset	In Use			Vulnerabilities						Policy E
gke-attack-path > sock-shop > deployment:sock-s... > queue-master docker.io/weaveworksdemos/queue-master 0.3.1	52	95	82	54	104	104	4	-	26	Fai
demo-kube-gke > sock-shop > deployment:sock-s... > queue-master docker.io/weaveworksdemos/queue-master 0.3.1	52	95	82	54	104	104	4	-	26	Fai
demo-kube-gke > sock-shop-v2 > deployment:sock-s... > queue-master docker.io/weaveworksdemos/queue-master 0.3.1	52	95	82	54	104	104	4	-	26	Fai
demo-kube-gke > sock-shop-v2 > deployment:sock-s... > shipping docker.io/weaveworksdemos/shipping 0.4.8	48	85	67	50	94	89	3	-	26	Fai
demo-kube-gke > sock-shop > deployment:sock-s... > shipping docker.io/weaveworksdemos/shipping 0.4.8	48	85	67	50	94	89	3	-	26	Fai
gke-attack-path > sock-shop > deployment:sock-s... > shipping docker.io/weaveworksdemos/shipping 0.4.8	48	85	67	50	94	89	3	-	26	Fai
gke-attack-path > sock-shop > deployment:sock-s... > carts docker.io/weaveworksdemos/carts 0.4.8	46	81	61	48	90	83	3	-	28	Fai

COMPLIANCE
Overview > Results

Report

Entire Infrastructure | CIS Docker Benchmark × | Select Requirements

High | Med | Low

112 Requirements Evaluated | 103 Failing Requirements | 9 Passing Requirements

R...	Requirement / Control	Controls Failed	Policy / Control Type	High	Med	Low
✗	5.20 Ensure mount propagation mode is not set to shared	1/1	CIS Docker Benchmark			1
✗	5.29 Ensure that the PIDs cgroup limit is used	1/1	CIS Docker Benchmark			1
✗	No containers without PIDs cgroup limit set	1/1	CIS Docker Benchmark			1
✗	5.6 Ensure sensitive host system directories are not mounted on containers		Host			1
✗	7.1 Ensure that the minimum number of manager nodes have been created in a swarm	1/1	CIS Docker Benchmark			1
✗	7.4 Ensure that Docker's secret management commands are used for managing secrets in a swarm cluster	1/1	CIS Docker Benchmark			1
✓	1.2.1 Ensure the container host has been Hardened	0/1	CIS Docker Benchmark			
✓	4.11 Ensure only verified packages are installed	0/1	CIS Docker Benchmark			
✓	4.3 Ensure that unnecessary packages are not installed in the container	0/1	CIS Docker Benchmark			
✓	4.4 Ensure images are scanned and rebuilt to include security patches	0/1	CIS Docker Benchmark			

About us

About Nuaware

Nuaware, an Exclusive Networks company, specializes in DevSecOps, providing seamless access to best-in-class technologies. As a value-added distributor, Nuaware enables organizations to adopt modern security architectures with a shift-left security approach and managed cloud security, supported by the appropriate technologies, training, and a robust partner ecosystem

About Exclusive Networks

Exclusive Networks (EXN) is a global cybersecurity specialist that provides partners and end-customers with a wide range of services and product portfolios via proven routes to market. With offices in over 45 countries and the ability to serve customers in over 170 countries, we combine a local perspective with the scale and delivery of a single global organisation.

About Docker

Developers can create and deploy secure applications to any cloud or on-premises infrastructure using Docker Desktop, resulting in faster delivery times. The Pro, Team, and Business subscriptions provide companies with additional features that enhance the value of Docker Desktop. These features include the ability to manage secure software supply chains, centralise policy visibility and control, and manage users and access.

Docker Desktop requires a paid subscription (Pro, Team, or Business), available for as little as $5 per month for larger enterprises (over 250 employees or over $10 million in annual revenue).

About Sysdig

Sysdig are on a mission to make every cloud deployment secure and reliable. Innovators everywhere rely on their products and the open source projects they support.

Sysdig pioneered cloud-native threat detection and response by creating Falco and Sysdig open source as open standards and key building blocks of our platform.

nuaware
An Exclusive Networks Company

nuaware.com

info@nuaware.com

+44 (0) 203 488 0530