Get the SaaS Advantage

To meet the demands of dynamic cloud-native environments and digital business, visibility and security solutions are increasingly moving to the cloud. From endpoint detection and response (EDR) to network security and monitoring, cloud-based software-as-a-service (SaaS) solutions enable enterprises to break free from hardware dependency and instantiate services wherever required from the data center, to the public cloud, and out to the edge.

The Sysdig Platform is a SaaS-first solution, purpose-built to drive the standard for cloud and container security. Our solution is more than just a hosted single-tenant instance in the cloud. It is designed to address the unique needs of cloud teams who need to get started quickly providing a single view of risk from source to run, with no blind spots, no guesswork, no black boxes. With Sysdig, you can find and prioritize software vulnerabilities, detect and respond to threats and anomalies, manage cloud configurations, permissions and compliance while increasing your efficiency and reducing costs, so you can focus on delivering great software.

This document digs deeper into the advantages of SaaS, providing insight into the operational controls and practices of the Sysdig SaaS solution designed to help you securely and efficiently implement cloud-native security and monitoring, and comparing this with the equivalent on-premises deployment.

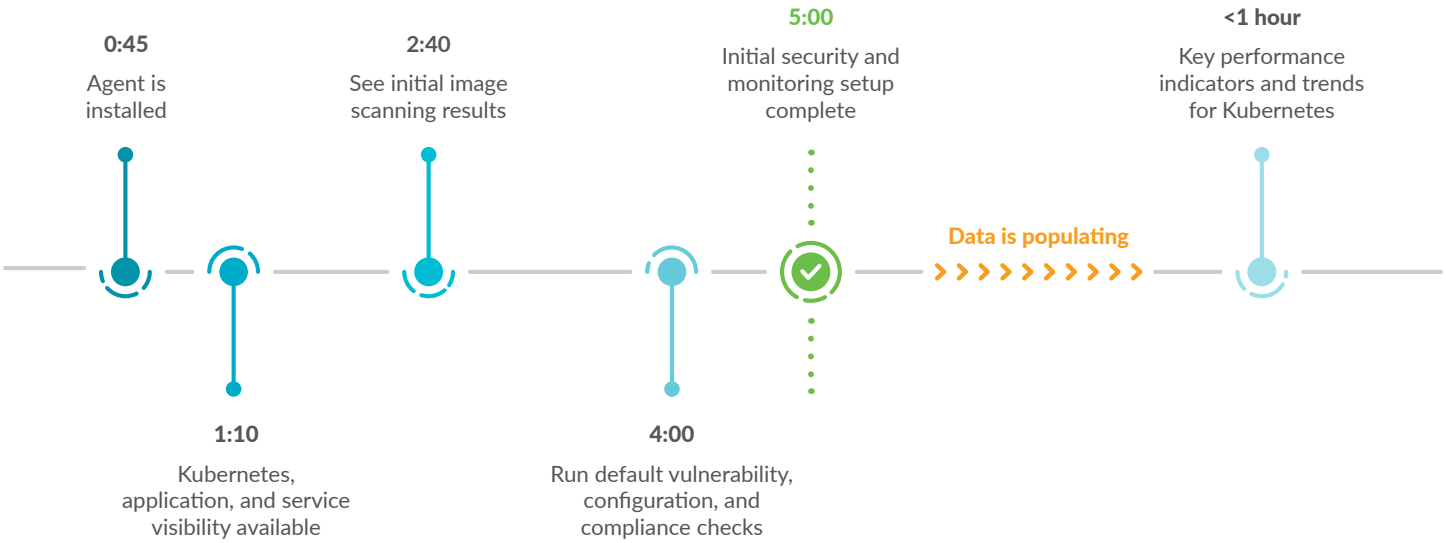
Using SaaS to your advantage

By taking advantage of the Sysdig SaaS platform for security and monitoring of your cloud-native environments, you will get up and running faster and reduce complexity. Additional benefits include faster access to features, easy scaling, reduced costs, and greater operational efficiency. Later in the document we'll cover these in more detail.

Get results faster

Sysdig's SaaS approach ensures you get started quickly with cloud-native monitoring and security. You can get started and see any activity within any app/service by any user across cloud, containers and hosts in less than five minutes. This includes instant access to a full range of capabilities for visibility into your cloud-based infrastructure, container and Kubernetes environment. From the initial trial and evaluation to full-production use, SaaS simplifies your experience and accelerates your time to value.

Sysdig cuts onboarding to 5 minutes



Reduce complexity

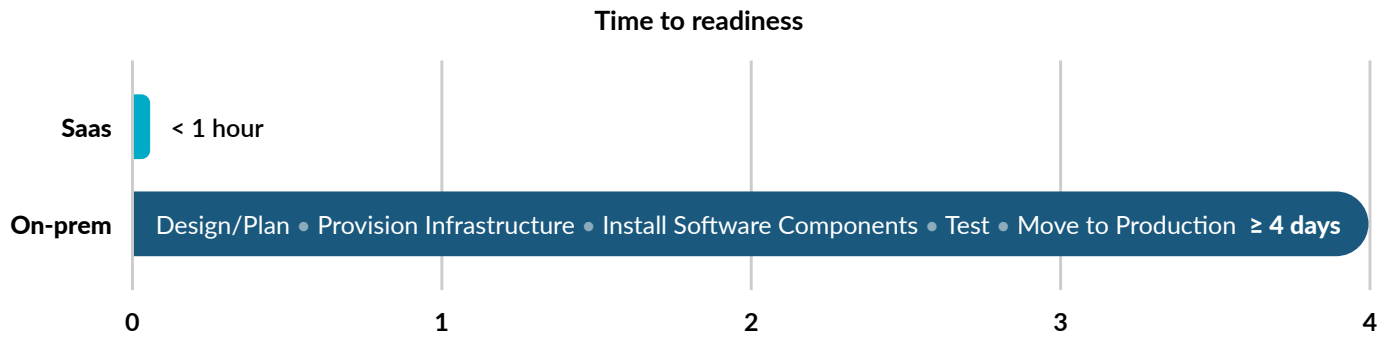
Building, maintaining, and operating on-prem infrastructure for monitoring and security is complex and costly. From project planning and execution to purchasing, integrating, and maintaining hardware and software, there are a lot of pieces for you to manage. With SaaS, rather than focusing resources on operations, you can spend more effort on your core objective of delivering new software capabilities.

No hardware costs

By taking a SaaS-approach, there's no need for in-house hardware to support security and monitoring. In addition, you avoid paying for accompanying software licenses and professional services – and your staff won't need to spend time on maintenance and support tasks.

As shown in the following diagram, a typical deployment for a 100-node Kubernetes cluster requires four servers equipped with sufficient resources to support your workloads. Provisioning and installation of the required backend software components require a four-day professional services engagement and involves staff from server, network, and storage teams.

Hardware and services requirements: 100 node cluster	
Server	**Storage**
4 servers 16 cores of CPU per node 64GB RAM per node	Cassandra – 450GB Elasticsearch – 150GB MySQL – 60GB PostgreSQL – 60GB
Professional services requirement: 4-days	



Lower operational costs

With a self-hosted solution, you'll require ongoing monitoring and support of the backend infrastructure and components. Additionally, as your environment expands, you will also need to continue to provision new hardware to accommodate growth.

With the Sysdig SaaS platform, as your container applications grow, you can scale up without worrying about backend hardware provisioning and ongoing data management. In addition, Sysdig manages required tasks like backup, restore, and disaster recovery for you in the cloud. The Sysdig SaaS platform also provides built-in high-availability across cloud availability zones, delivering reliable platform access without requiring you to build or manage your own HA solution.

Get faster access to new features

The cloud-native market is constantly changing. Sysdig's SaaS-first approach means you get instant access to new security and monitoring innovations that help you keep pace. New SaaS features are released weekly vs. quarterly for self-hosted software. Furthermore, Sysdig handles the rollout of platform software and feature updates for you, so you're always up-to-date.

Frequently, upgrading an IT-managed solution needs to be closely scheduled, depending on night shifts and on-call rotation engineers, placing a burden for the team responsible for this task. Choosing the Sysdig's SaaS platform, you can start using that feature you were waiting for, as soon as it's announced in the release notes. Forget about the change management workflow and accelerate feature delivery. Don't wait for months for a feature to get released into your self-hosted solution.

Quickly adapt to business changes

The Sysdig SaaS platform enables flexibility for you to adapt to changing business dynamics and easily right size for the environment you need to support. You can effortlessly scale up and down and avoid the wasted expense of underutilized hardware and the challenges of under-provisioning.

In addition, you can painlessly operate across clouds and deliver security and monitoring from a single point. A consistent, single-pane view of your entire infrastructure facilitates quicker issue resolution. This includes support for Amazon, Google, Microsoft, and IBM clouds.

SaaS platform security, compliance, and availability

With Sysdig SaaS, you can reduce the scope of security and compliance for your business. You won't have to spend time and money addressing platform access, data security, auditing, and compliance for your monitoring and security platform. Sysdig takes care of it all for you in the cloud, so you can focus on securing your business applications.

Sysdig is committed to applying the best security and compliance standards for your data to reduce risk. The system collects data from customers via an SSL-based encrypted connection and stores saved data as encrypted (U.S. West Coast and Frankfurt data centers).

We have established over 60 operational controls and company policies designed to protect your data. This includes product controls designed to deliver security in-app, corporate controls to apply security best practices within Sysdig, data controls to protect information, and application controls to govern development and change management.

Sysdig SaaS security controls

Product Security

- Audit logging
- Role-based access controls
- Authentication and authorization

Corporate Security

- Background checks
- Security training
- SOC 2 policies
- Vendor management
- Facilities security

Data Security

- Agent security
- Data encryption at rest
- Data encryption in motion

Application Security

- Secure Software Development Life Cycle (SDLC)
- Quarterly penetration testing

In addition to the SaaS security controls noted above, we have integrated availability controls to ensure you have reliable platform access to help you meet your business objectives.

We have designed our availability practices to address the following availability risks:

- Insufficient processing capacity
- Insufficient internet response time
- Loss of processing capability due to a power outage
- Loss of communication with user entities due to a break in telecommunication services
- Loss of key processing equipment, facilities, or personnel due to a natural disaster

Our internal controls and procedures for security and availability meet the trust services criteria for Service Organization Control (SOC) compliance. Sysdig has successfully completed a SOC 2 Type 1 examination by an independent auditor and is in-progress with a SOC 2 Type 2 compliance audit. We continuously monitor security standards to integrate applicable requirements into our business and platform to ensure you can take advantage of the Sysdig SaaS solution while meeting your compliance and regulatory obligations.

- SOC 2 Type 1
- SOC 2 Type 2 (In-progress)

Visit our Trust Center to learn more about the protections and processes implemented by Sysdig.

Green data centers

All of our SaaS hosting regions are powered by renewable energy. Currently, Sysdig operates our SaaS solution across multiple hosting locations:

- East Coast of the United States, in Virginia
- West Coast of the United States, in Oregon
- Europe, in Frankfurt, Germany

Data Collection & Classification

Data is stored in Sysdig SaaS, with all data encrypted at rest. Data is isolated from individual customers through tagging all data with unique customer identifiers. This is a mandatory key used by the Sysdig application to limit all data queries to a specific individual customer. To provide our customers the best service, this is a shared platform with shared infrastructure components, however there is strict logical separation between customers.

There is the ability to offload forensic captures into a custom defined S3 compatible bucket. The capture travels from the Sysdig agent, to be temporarily stored in the Sysdig Platform backend, and then is offloaded to the S3 bucket. This bucket is unique to every customer and custom security and retention policies can be applied.

We don't collect or index any Personally Identifiable Information (PII) in the platform anywhere. PII may get stored in forensic captures if it is stored and handled in clear text by a customer's applications or hosts, but this is never indexed or processed in an PII identifiable way.

When is on-prem the right choice?

While SaaS offers significant advantages, some organizations still require an on-premises solution. You may be subject to compliance mandates that prohibit the use of public cloud solutions. Or, self-hosting an internal cloud may be your preferred approach and part of your organization's chosen strategy and expertise.

Sysdig offers a self-hosted deployment to deliver the benefits of the Sysdig Secure DevOps Platform entirely within your control. In addition, this approach enables advanced deployments in air-gapped environments to meet stringent security and compliance requirements.

If your primary requirement is to maintain business applications and data on-premises, another option is to secure and monitor your private infrastructure and containers using the Sysdig SaaS solution.

Ship cloud apps faster with Sysdig

With a SaaS-first offering, Sysdig gives cloud teams a fast path to delivering security and visibility for containers and Kubernetes. Cloud teams can embed security, compliance, and monitoring into their DevOps workflow to accelerate application delivery. The Sysdig platform is built on open source tools your team wants to use, with the scale, performance, and ease of use enterprises demand. With Sysdig, organizations of all sizes get results quickly and efficiently.

Find out how the Sysdig Platform can help your teams get a single view of risk from source to run, with no blind spots, no guesswork, no black boxes. Contact us for additional details about the platform, or to arrange a personalized demo.

www.sysdig.com