



HPE Solution Architecture for securing and monitoring Red Hat OpenShift Container Platform on HPE Synergy using Sysdig Monitor and Sysdig Secure as SaaS

Contents

Executive summary 3

Solution overview 3

 Container security challenges 3

Solution hardware 6

 Software licenses 8

Security controls and risks 8

 HPE Composable Infrastructure security controls 8

 Container security risks 11

Sysdig for securing containers 12

 Sysdig Monitor 14

 Sysdig Secure 14

Sysdig Secure and Sysdig Monitor as SaaS for the Red Hat OpenShift Container Platform 14

 Automated deployment of the Sysdig agent on the Red Hat OpenShift Container Platform 15

Summary 19

Appendix A. Image scanning using Sysdig Secure 20

Change Tracker 24

Resources and additional links 25



Executive summary

Security is a required component of any production IT infrastructure solution. In the era of digital transformation, emerging technologies such as Hybrid IT, Cloud, Software Defined Intelligence, and the Internet of Things (IoT), are generating new business opportunities. These complex technologies help to accelerate business innovations, promote agility, build better customer relations, and extend IT beyond the data center. IT organizations are employing new approaches such as microservices architectures, a variety of cloud services, containers, container orchestration tools, and continuous delivery methodologies to respond to business needs by quickly developing and pushing out new capabilities.

While IT organizations are becoming cloud-native to satisfy market needs, they additionally face new security challenges while adhering to the essential security principles. For example, authentication, authorization, privacy and availability all present unique challenges in cloud versus traditional on-premises environments. On the innovation front, cloud-native solutions such as microservices, Docker, and Kubernetes help to build sustainable ecosystems. These solutions provide a suitable platform for the developers to build products faster. The applications are built as microservices and run on a containerized and dynamically orchestrated platform that fully exploits the advantages of the cloud computing model. As opposed to conventional virtualized applications, containers may live for just a few minutes, or even seconds, and may not even have significant official IP addresses and namespaces. This means that customary practices, for example security scanning of applications periodically, may lead to missing a bigger vulnerability for short lived workloads. As a result, there is a need to integrate continuous container security assessment and vulnerability management with continuous integration and continuous deployment (CI/CD) pipelines.

To help accelerate container application delivery and to enjoy the benefits of more reliable, secure software, Hewlett Packard Enterprise and Sysdig have collaborated to secure Red Hat OpenShift Container Platform on HPE Synergy using the Sysdig cloud deployment model for Sysdig Secure and Sysdig Monitor. The Cloud-native visibility and security platform from Sysdig unifies container security, monitoring, and forensics for OpenShift Container Platform environments.

Red Hat OpenShift Container Platform provides organizations with a reliable platform for deploying and scaling container-based applications. HPE Synergy provides the flexible infrastructure and you need to run that container platform to dynamically provision and scale applications. The Cloud-native visibility and security platform from Sysdig allows DevOps, security professionals, and service owners to get context-rich information to dig deeper into their containerized environments and reliably build, run, and respond to issues in millions of containers.

This document provides guidance for deploying the Sysdig agents that communicate with the Sysdig Secure and Sysdig Monitor for securing and monitoring Red Hat OpenShift Container Platform on HPE Synergy Composable Infrastructure using HPE Nimble Storage or HPE 3PAR StoreServ Storage. This document also describes the following benefits of using Sysdig Secure and Sysdig Monitor to secure Red Hat OpenShift Container Platform on HPE Synergy.

- Automated installation and deployment of Sysdig agents on Red Hat OpenShift Container Platform, thus reducing the manual effort of installing and configuring Sysdig agents from an hour to a few minutes.
- Using the Sysdig Monitor, OpenShift Container Platform administrator can manage the risk, health, and performance of the containers.

Using the Sysdig Secure, the OpenShift Container Platform administrator can perform container image scanning, run-time protection, and forensics to identify vulnerabilities, block threats, enforce compliance, and perform audit activity across enterprise cloud-native environments at scale.

Target audience: This work is intended for Chief Technology Officers (CTOs), Chief Information Security Officers (CISOs), data center managers, enterprise architects, security architects, and implementation personnel wishing to learn more about securing Red Hat OpenShift Container Platform on HPE Synergy Composable Infrastructure. Familiarity with HPE Synergy, Red Hat OpenShift Container Platform, container-based solutions, Ansible, core networking, and enterprise security knowledge is assumed.

Solution overview

Container security challenges

Containers are packages that deploy and run applications that access a shared operating system kernel. Although able to be used for stateful applications, containers are inherently stateless and do not retain session information. Multiple instances of a container image can run simultaneously and new instances can replace failed ones without disruption to the application's operation. In the first phase of the container lifecycle, developers build the application components and package them into multiple images. These images are developed on a base layer containing minimal distribution of common operating systems, and they contain all the executables and libraries required to run an application. After image creation, organizations typically perform testing and then decide to approve/disapprove the images. For example, test automation tools and personnel use the images to validate the functionality of the final application, and security teams perform penetration testing on these



images. The consistency of building, testing, and accrediting exactly the same artifacts for an application is one of the key operational and security benefits of containers.

These images are typically stored in central locations called registries. Registries make it easy to control, share, find, and reuse images across hosts. Registries allow developers to easily store images as they create, tag, and catalog them for identification and version control. They also aid in discovery and re-use as well as assisting in finding and downloading images that others have created. Registries may be self-hosted or consumed as a service.

Once stored in a registry, images can be easily pulled and then used by developers across any environment in which they run containers. The container orchestration tools such as Kubernetes enable the developers or the automation working on their behalf to pull images from registries, deploy those images into containers, and manage the running containers. Orchestration tools are also responsible for monitoring the container resource consumption, job execution, and machine health across hosts. Finally, hosts run and stop the containers as directed by the orchestrator.

Figure 1 shows the container technology lifecycle phases starting from image creation to container deployment in a production environment.

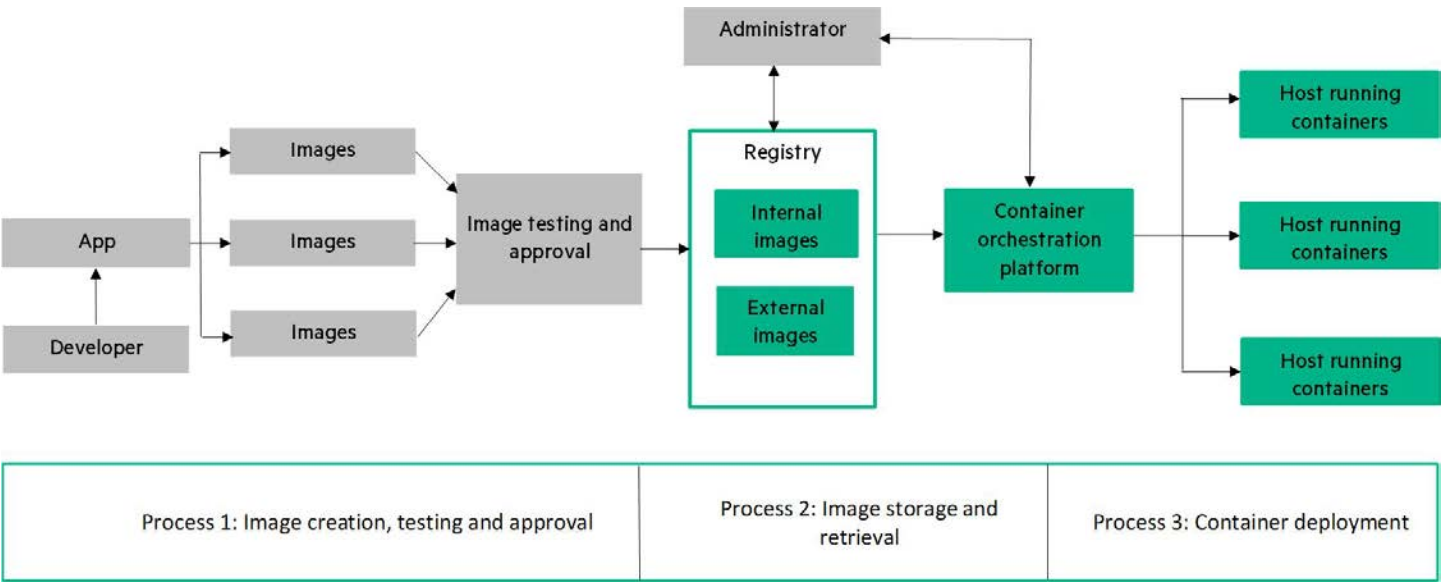


Figure 1. Container technology architecture and lifecycle

Understanding the container technology architecture and lifecycle highlights the following security challenges:

- It is challenging to assess the compliance posture of containers and Kubernetes environments.
- There is a frequent lack of visibility into container infrastructure and security incidents at runtime.
- There is a lack of ability to inspect a container activity after it is gone.
- As the number of images in the registry increases it becomes more critical that critical vulnerabilities within images are identified quickly.
- Keeping track of secrets and credentials exposed by an image, among thousands of images, is complex and time consuming.
- Identifying if an image is exposing any blacklisted ports is important to stop a hacker from gaining entry through a back door.
- Tracking the licenses and their types that are used by an image.
- Performing a compliance check on each container to identify any violations is critical.
- Regular health checks must be performed on the containers.



To address these container security challenges within the context of Red Hat OpenShift Container Platform, this document proposes a solution that uses the Sysdig Secure and Sysdig Monitor cloud deployment model to secure and monitor Red Hat OpenShift, an enterprise-ready Kubernetes container platform installed and configured on HPE Synergy Composable Infrastructure. Figure 2 shows the solution diagram for securing and monitoring Red Hat OpenShift Container Platform on HPE Synergy using Sysdig Secure and Sysdig Monitor. It begins with the user configuring the Red Hat OpenShift Container Platform on HPE Composable Infrastructure to enable access for the Sysdig Secure and Sysdig Monitor.

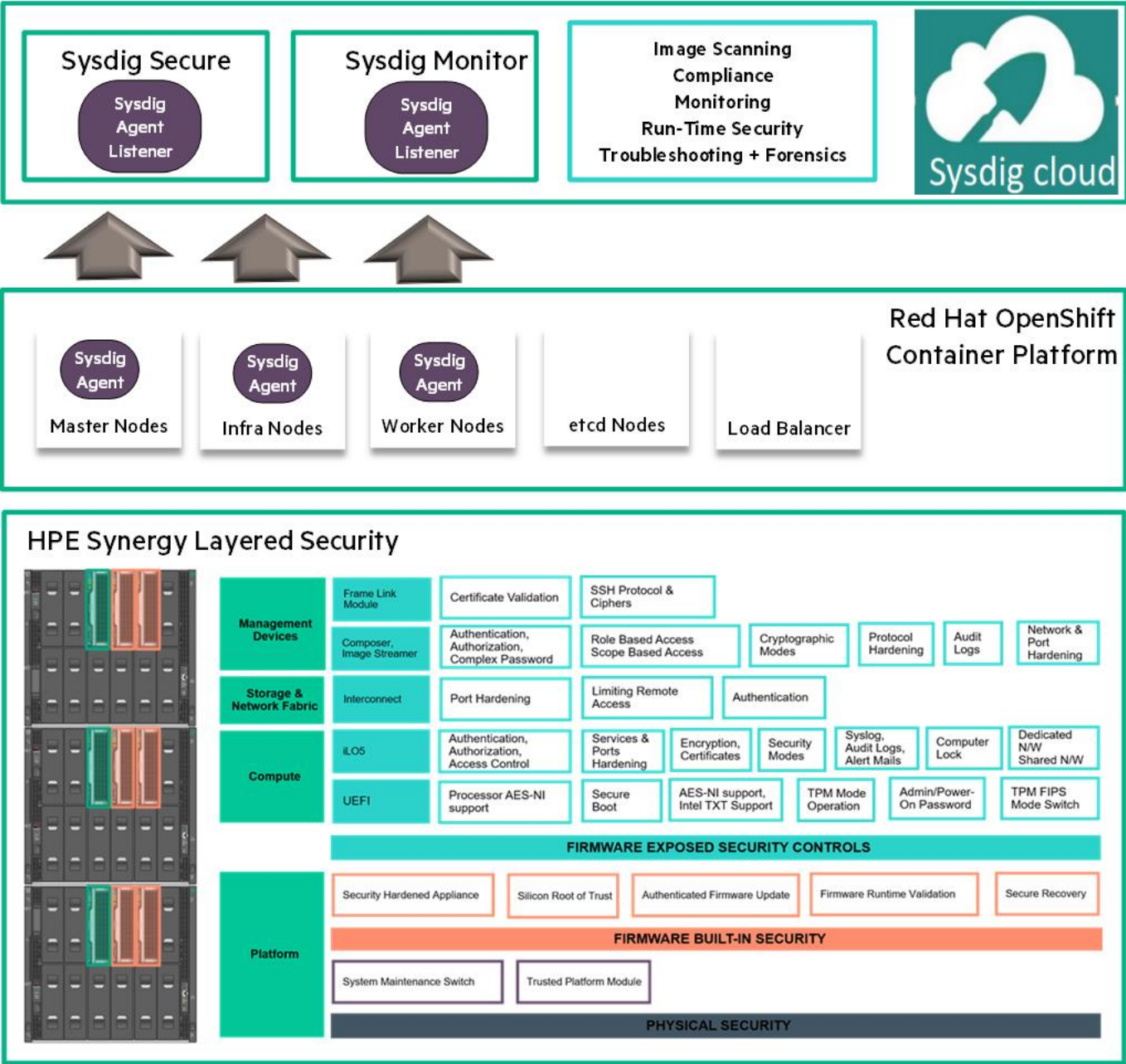


Figure 2. Security overview for Red Hat OpenShift cluster platform on HPE Synergy

The Sysdig Secure and Sysdig Monitor cloud deployment model is a SaaS offering, where Sysdig runs a multi-tenant backend as a service for user based on the subscription model they have chosen. For security and monitoring of OpenShift containers the Sysdig agent must be installed



on each node in the OpenShift cluster. These agents run as a daemon to enable Sysdig Monitor and Sysdig Secure functionality. Sysdig Monitor provides deep, process-level visibility into dynamic, distributed production environments. Sysdig Secure provides image scanning, run-time protection, and forensics to identify vulnerabilities, block threats, enforce compliance, and perform audit activity across OpenShift clusters. The key benefits that this solution provides are:

- Automated build and deployments, continuous integration/continuous delivery (CI/CD), and build and container metrics in Red Hat OpenShift provide a rapid flow of information and continuous feedback from the build and deployment process back to the development teams. This lets developers detect and rectify anomalies immediately, which is far more effective than fixing them later in production where fixes impact cost and service delivery more critically.
- Increased operational efficiency with HPE Synergy Composable Infrastructure
- Faster incident resolution for OpenShift cluster using Sysdig Monitor
- Simplified compliance for the entire solution
- Service-based access control for container security and monitoring
- Less time spent on managing platforms, containers, and vulnerabilities

Solution hardware

This solution is built on HPE Synergy, the first platform built from the ground up for composable infrastructure. HPE Synergy empowers IT administrators and developers to create and deliver new value instantly and continuously. This single infrastructure reduces operational complexity for traditional workloads and increases operational velocity for the new breed of applications and services. Through a single interface, HPE Synergy composes compute, storage, and fabric pools into any configuration for any application. It also enables a broad range of applications from a bare metal to virtual machines to containers, and operational models such as hybrid cloud and DevOps. HPE Synergy enables IT to rapidly react to new business demands. Figure 3 shows the front view of HPE Synergy over which this solution is built. For the installation and configuration of Red Hat OpenShift on HPE Synergy, refer to the deployment guides available at <https://github.com/hewlettpackard/hpe-solutions-openshift>.



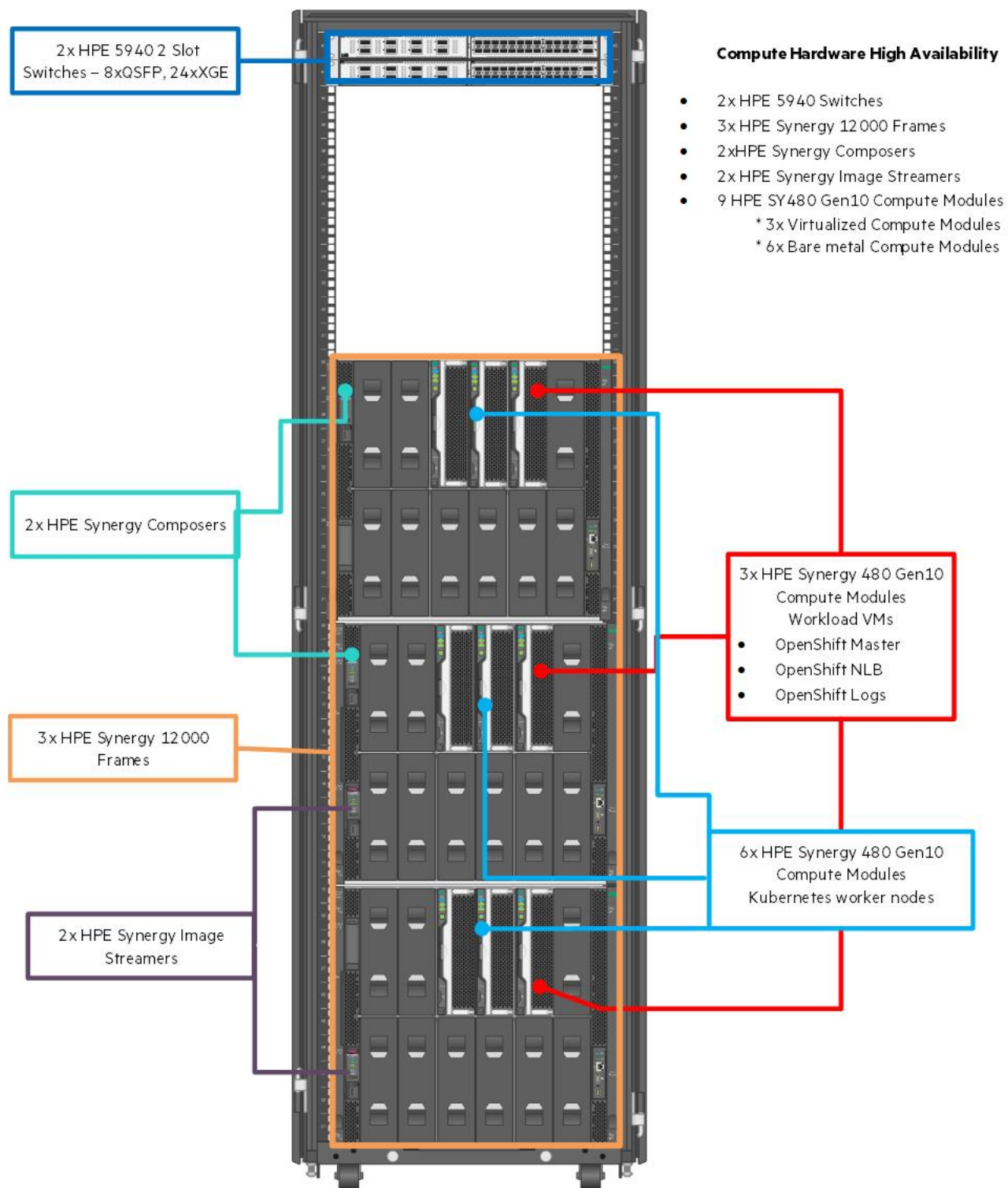


Figure 3. Front view of the solution built on HPE Synergy



Software licenses

The installer should utilize valid Red Hat subscriptions in order to access all of the required repositories. The installer also requires valid subscription and administrator privileges to access Sysdig Secure and Sysdig Monitor as well as a valid access key for Sysdig agent installation.

Security controls and risks

This section discusses a high-level outlook of the security controls that are available to customers who adopt HPE Synergy and then delves into the details of container security risks.

HPE Composable Infrastructure security controls

It is important for customers to get a holistic view of the security controls available to them. Hewlett Packard Enterprise has security features and functionalities built into servers from the hardware level to the firmware. HPE Synergy Composable Infrastructure enables IT organizations to accelerate application and service delivery through the use of fluid resource pools, made up of compute, storage, and fabric with software-defined intelligence. Each resource of the composable infrastructure components is made up of multiple products. For example, Synergy compute nodes include Integrated Lights-out (iLO), Unified Extensible Firmware Interface (UEFI), and so on. Another example is the management device, HPE Synergy Composer, which exposes its functions using HPE OneView and the HPE Synergy Frame Link Modules. With so many products available within the HPE Composable Infrastructure, it is important to understand the security controls available within each of them to be able to prevent potential security breaches.

This solution provides a layered view of security controls that are available to HPE customers. Figure 4 shows the layered security view across various HPE Composable Infrastructure components.

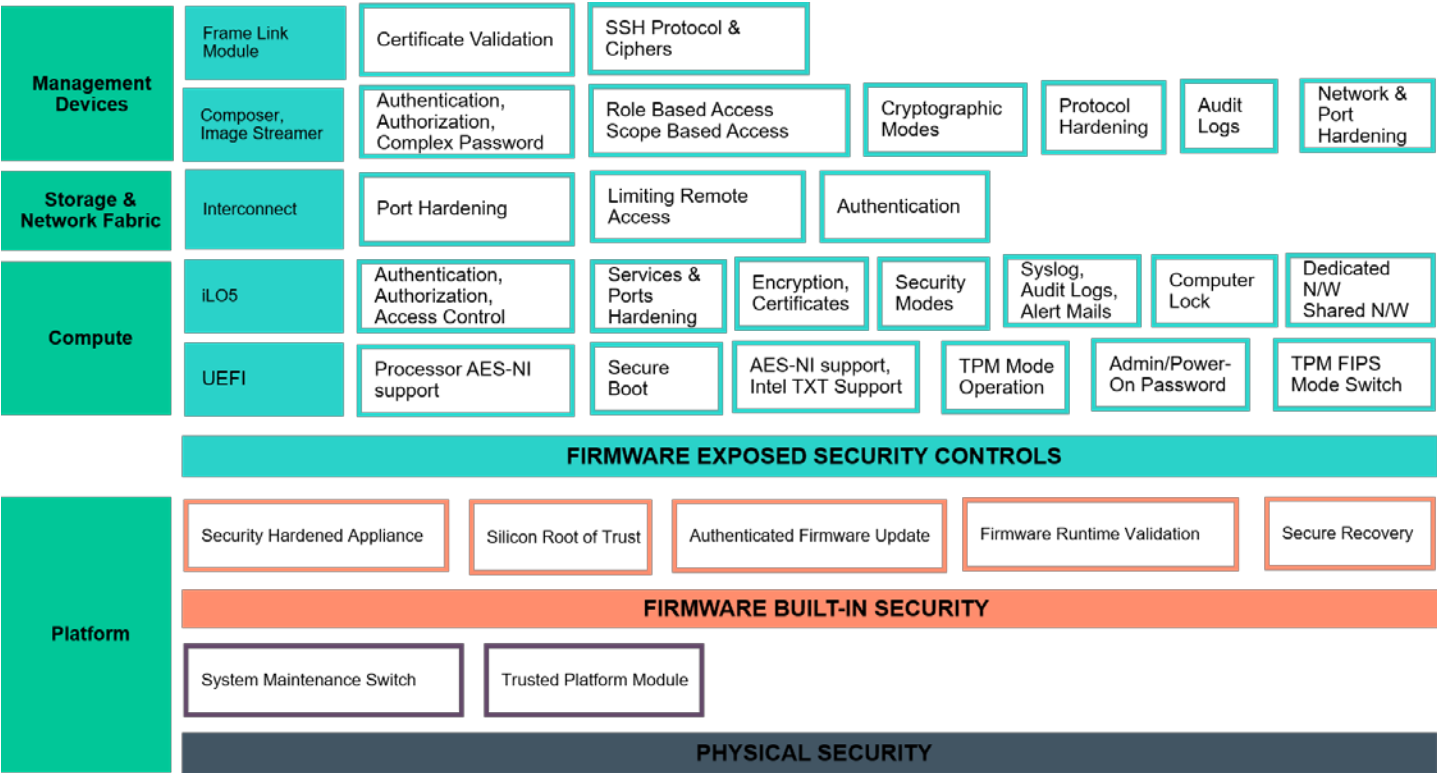


Figure 4. The layered security view of HPE Composable Infrastructure

Table 1 describes the three security control layers shown in Figure 4, physical security, firmware built-in security, and firmware exposed security controls. The objective of choosing this layered security view is to ensure visibility to the depth of security risk that an infrastructure can have and also to expose the depth of defense that is built-in to the HPE Composable Infrastructure design. Security controls at each layer are designed to comply with the requirements of one or more security tenets. The security tenets are a set of security principles that ensure the security within the information systems. For example, authentication, authorization, access control, password policies, cryptographic ciphers, secure protocols, forensic analytics – logs, alerts, threat modeling, security certifications, and standards.

Table 1. Physical and firmware based security controls within HPE Composable Infrastructure

Security control layers	Description
Physical security controls	Physical security describes measures designed to ensure the physical protection and detection of a threat event in the infrastructure.
Firmware/hardware built-in security controls	<p>This covers:</p> <ul style="list-style-type: none"> • The security technologies built into the firmware to make it more secure for any communication with the underlying hardware, and safe for user data at rest/transit. • The threat modeling followed within Hewlett Packard Enterprise to secure the infrastructure components.
Firmware exposed security functionality	<p>This is the exhaustive list of security controls that lets the customers:</p> <ul style="list-style-type: none"> • Define the boundaries for accessing various infrastructure components. • Set quantum safe ciphers for encryption. • Generate alert and log changes to the infrastructure.

Firmware built-in security controls

It is important to understand how Hewlett Packard Enterprise has used various technologies to ensure the firmware built-in security controls provide highest level of infrastructure security. This section provides a brief overview on the security controls that Hewlett Packard Enterprise has built in the firmware that is used by HPE Synergy. These security controls offer an added advantage to HPE Synergy customers.

Silicon Root of Trust

The iLO5 chipset contains a first of its kind Silicon Root of Trust for the HPE Synergy Gen10 Compute Module which is included with the iLO standard license. Silicon Root of Trust provides an inextricably tied link between the silicon and firmware, thus making it impossible to insert any malware, virus, or compromised code that would corrupt the boot process. The Silicon Root of Trust enables the boot process to provide a secure start. When the system boots, the iLO5 chip validates and boots its own firmware first, then validates the system BIOS. Because the Silicon Root of Trust is inextricably tied into the iLO5 hardware, every validated signature throughout the boot process can be trusted. However, in the unlikely event where iLO5 finds tampering or corruption at any point in the process, trusted firmware is immediately available for secure recovery. Hewlett Packard Enterprise can address platform security all the way back to the supply chain because Hewlett Packard Enterprise designs the iLO5 entirely—hardware and firmware—and controls the iLO5 production process. Unlike other companies, Hewlett Packard Enterprise does not outsource the server management controller. Hewlett Packard Enterprise also has strict internal processes that dictate the firmware approval process. This gives customers an unprecedented level of assurance that no hackers have compromised the firmware before the customers receive their server.

Automatic Secure Recovery

Validates the iLO firmware when power is applied. If the firmware is invalid, the iLO firmware is flashed automatically (iLO Standard license). Also validates the system ROM during server startup. If valid system ROM is not detected, the server is prevented from booting. Recovery options include swapping the active and redundant ROM, and initiating a firmware verification scan and recovery action (iLO Advanced Premium Security Edition license).

Firmware runtime verification

With the iLO Advanced Premium Security License, the iLO5 chipset enables runtime verification of firmware. The firmware verification feature allows to run an on-demand scan or implement scheduled scans. To respond to detected issues, iLO administrator user choose between logging the results or logging the results and initiating a repair action that uses a recovery install set.



Authenticated firmware updates

The iLO5 chipset expands the number of firmware items that customers can update directly and securely on HPE Gen10 servers. This is a standard feature on the iLO5. Firmware items that can be securely validated and updated from the iLO now includes SPLDs, HPE ProLiant Power Interface Control Utility (PowerPIC) firmware, the Intel Innovation Engine and Intel Management Engine, and other low-level system components. The iLO contains a firmware repository stored on non-volatile flash memory (NAND) which allows components such as the Service Pack for ProLiant (SPP) and other firmware updates to be applied and installed offline through iLO5.

Best practices followed by Hewlett Packard Enterprise to deliver a security hardened HPE Synergy Composer

Hewlett Packard Enterprise follows Secure Development Lifecycle and uses a security assessment tool called Comprehensive Applications Threat Analysis (CATA) to identify and remediate security defects in the appliance operating system.

Note

The design of the appliance is based on CATA fundamentals and underwent CATA review.

Following is a list of factors that contribute to appliance security hardening:

- HPE Synergy Composer is hardened to enforce mandatory access control. This means users of HPE Synergy are provided the role based access control that enables an administrator to establish access control and authorization for users based on their responsibilities.
- The HPE Synergy Composer is governed by scope-based access control that enables an administrator to establish access control for users by allowing a role to be restricted to a subset of resources managed by the appliance.
- The appliance is configured and maintains a firewall that blocks unused ports. Restricting all non-essential port usage reduces the attack surface of the operating system in HPE Synergy Composer.
- The appliance operating system bootloader is password protected. This means HPE Synergy Composer cannot be compromised by someone attempting to boot in single-user mode.
- The appliance is designed to operate in an isolated management Local Area Network (LAN). Hewlett Packard Enterprise recommends creating a private management LAN and keeping that separate, or air-gapped, from production LANs using VLAN or firewall technology (or both).
- Hewlett Packard Enterprise supports digital signing of all software/firmware updates to ensure integrity and authenticity. This implies that when the customer is re-imaging HPE Synergy Composer in order to quickly bring it to a specific firmware revision level, the digital signature is verified by the re-imaging process.
- Operating-system-level users are not allowed to access the appliance, with the following exceptions:
 - A special **pwreset** command is used only if the infrastructure administrator's password is lost or forgotten. This command requires that you contact your authorized support representative to obtain a one-time password.
 - A setting that enables an authorized support representative to obtain a one-time password so that they can log in to the appliance console (and only the console) to perform advanced diagnostics. Customers can either enable or disable access with this setting.
- Hewlett Packard Enterprise closely monitors security bulletins for threats to appliance software components and, if necessary, issues software updates.



Container security risks

Broadly, container security risks can be divided into five risk areas such as image risk, registry risk, host OS risk, container risk, and orchestrator risk as shown in Figure 5. The NIST SP 800-190 Application Container Security Guide at <https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2017-10.pdf> lists the container security risks in more detail.

Image Risk	Registry Risk	Host OS Risk	Container Risk	Orchestrator Risk
Image vulnerabilities Configuration defects Embedded malware Embedded clear text secrets Untrusted images	Insecure connections to registries Stale images in registries Insufficient authentication and authorization restrictions	Large attack surface Shared kernel Host OS component vulnerabilities Improper user access rights Host OS file system tampering	Vulnerabilities within the runtime software Unbounded network access from containers Insecure container runtime configurations App vulnerabilities Rogue containers	Unbounded administrative access Unauthorized access Poorly separated inter-container network traffic Mixing of workload sensitivity levels Orchestrator node trust

Figure 5. Container security risk categories

Image risk

Container images are effectively static archive files that include all the components used to run a given application. Components within an image may be missing critical security updates or be otherwise outdated. As such, a common risk in containerized environments is the deployed containers having vulnerabilities because the version of the image used to generate the containers has vulnerabilities. Images can also have configuration defects. For example, an image may not be configured with a specific user account to “run as” and thus runs with greater privileges than needed. Because images are just collections of files packaged together, malicious files could be included intentionally or inadvertently within them. Such malware would have the same capabilities as any other component within the image and thus could be used to attack other containers or hosts within the environment. Many applications require secrets to enable secure communication between components. When an application is packaged into an image, these secrets can be embedded directly into the image file system. However, this practice creates a security risk, because anyone with access to the image can easily parse it to learn these secrets. The portability and ease of reuse of containers increase the temptation for teams to run images from external sources that may not be well-validated or trustworthy. Using this externally provided image results in the same type of risks that external software traditionally has, such as introducing malware, leaking data, or including components with vulnerabilities.

Registry risk

Images often contain sensitive components such as an organization’s proprietary software and embedded secrets. If connections to registries are performed over insecure channels, the contents of images are subject to the same confidentiality risks as any other data transmitted over the network in clear text. Because registries are typically the source location for all the images that an organization deploys over time, the set of images they store can include many vulnerable, out-of-date versions. Registries are typically trusted as a source of valid, approved software. Compromising a registry can potentially lead to the compromise of downstream containers and hosts.

Host OS risk

Every host OS has an attack surface which represents the collection of all the methods attackers can use to attempt to access and exploit the vulnerabilities of that host OS. The larger the attack surface, the better the odds are that an attacker can find and access a vulnerability, leading to a compromise of the host OS and the containers running on top of it. Although containers provide strong software-level isolation of resources, the use of a shared kernel invariably results in a larger inter-object attack surface than is seen with hypervisors, even for container-specific OSs. In



other words, the level of isolation provided by a container runtime is not as high as the one provided by hypervisors. Container-specific OSs are typically not optimized to support multiuser scenarios since interactive user logon should be rare. Organizations are exposed to risk when users log on directly to hosts to manage containers, rather than going through an orchestration layer. Insecure container configurations can expose host volumes to greater risk of file tampering. For example, if a container is allowed to mount sensitive directories on the host OS, that container can then change files in those directories. These changes could impact the stability and security of the host and all other containers running on it.

Container risk

By default, in most container runtimes, individual containers are able to access each other and the host OS over the network. If a container is compromised and acting maliciously, allowing this network traffic may expose other resources in the environment to risk. An attacker may also be able to exploit vulnerabilities to compromise the runtime software itself and then alter that software so that it allows the attacker to access other containers, monitor container-to-container communications, and so on. Container runtimes typically expose many configurable options to administrators. Setting them improperly can lower the relative security of the system. For example, on Linux® container hosts, the set of allowed system calls is often limited by default to only those required for safe operation of containers. If this list is widened, it may expose containers and the host OS to increased risk from a compromised container. Rogue containers are unplanned or unsanctioned containers in an environment. If these containers are not put through the rigors of vulnerability scanning and proper configuration they may be more susceptible to exploits.

Orchestrator risk

In many cases, a single orchestrator may run many different applications, each managed by different teams, and with different sensitivity levels. If the access provided to users and groups is not scoped to their specific needs, a malicious or careless user could affect or subvert the operation of other containers managed by the orchestrator. Orchestrators often include their own authentication directory service, which may be separate from the typical directories already in use within an organization. This can lead to weaker account management practices and ‘orphaned’ accounts in the orchestrator, because these systems are less rigorously managed. Because many of these accounts are highly privileged within the orchestrator, so any unauthorized access to them can lead to system wide compromise. Maintenance of trust between the nodes in the environment requires special care. The orchestrator is the most foundational node. Weak orchestrator configurations can expose the orchestrator and all other container technology components to increased risk. Examples of possible consequences include unauthorized hosts joining the cluster and running container or, the compromise of a single cluster host implying compromise of the entire cluster.

Sysdig for securing containers

Sysdig has adopted a platform approach to container security where it uses common telemetry and back-end process to address various use cases. Sysdig leverages its Cloud-Native Intelligence Platform, and the applications that run on top of it are Sysdig Secure and Sysdig Monitor. Sysdig indicates that the products are updated with approximately one major and one minor release per year, with monthly updates as needed. Sysdig supports both SaaS and on-premises deployment. Customers choose to purchase either Sysdig Monitor or Sysdig Secure, or to bundle both products.

The typical use cases that Sysdig is targeting include:

- Application health and performance monitoring
- Vulnerability management
- Container run-time security
- Container forensics, monitoring, and troubleshooting
- Compliance and auditing

For monitoring, the goal is to provide enterprise-class observability of modern Linux environments with native support for container-based workloads. From a security perspective, the objective is to provide security across the lifecycle of the workloads, from build time through runtime and forensics. Sysdig has built an architecture with endpoint collectors, back-end processing, and a customized front end. The endpoint collectors—currently using a kernel module. That back-end ties to various orchestration services using an API-based component named ServiceVision. The ServiceVision provides support for many current container orchestration services. The metadata from these systems is used to enrich the data from the collectors and allow querying and policy enforcement for service-level (as opposed to container-level) aspects, including service performance, load, compliance, and more. Then it uses the additional information to perform analytics and alerting on incoming data. The data is made available using customized workflows and interfaces for both security and monitoring.

The core technology at the collector level is named ContainerVision. It consists of the kernel module for analyzing system calls and capturing custom metrics formats—such as Prometheus, statsD, and JMX—and a container for managing the module and interfacing with the rest of the



Sysdig offering. Sysdig claims that the collector is tunable and features low resource consumption. For security use cases, it supports enforcement actions such as stopping or pausing a container and doing deeper forensics capture. Sysdig supports multiple container runtime engines and networking options including Istio. The Sysdig back-end connects to container orchestration systems using an API-based component. The various container orchestration systems supported by Sysdig include Kubernetes, Docker, DC/OS, OpenShift, GKE, Microsoft Azure and IBM Cloud. The metadata from these systems is used to enrich the data from the collectors and allow querying and policy enforcement for service-level (as opposed to container-level) aspects, including service performance, load, compliance, and more.

The Sysdig back-end implements the workflows, querying capability (based on the Prometheus query language), user interface, alerting of security violations, and enforcement. These features are used to support monitoring and security use cases which have been packaged into Sysdig Monitor and Sysdig Secure commercial offerings.

Sysdig Monitor focuses primarily on monitoring and troubleshooting container security risks and has been used to implement what the company calls 'enterprise-grade Prometheus' capabilities. It supports numerous service and application related performance metrics. These capabilities come together to deliver rich system, container, and application data to dramatically simplify monitoring the application health and performance. The ContainerVision used by Sysdig simplifies visibility and makes it possible to inspect applications running inside containers without requiring any instrumentation of the container or application. On the other hand, ServiceVision extracts service labels from your orchestrator to add service context to all of the metrics and events for greater clarity and precision when viewing data. Sysdig Secure provides functionality across build, run, and response phases of the container security lifecycle. For build security, Sysdig Secure tries to CI/CD pipelines and systems such as Jenkins or GitLab for testing builds for security violations. Sysdig Secure also performs checks against Common Vulnerabilities and Exposures (CVE) databases and for improper storage of credentials. For runtime protection, Sysdig Secure enforces protection policies that can restrict execution based on metadata information. Sysdig Secure also checks for rogue containers, potentially vulnerable images, and host compliance against benchmarks such as The Center for Information Security (CIS). Sysdig Secure response capabilities can be particularly useful for capturing additional forensic data from ephemeral workloads or integrated with external systems such as SIEM platforms. Figure 6 shows the Sysdig product offerings.

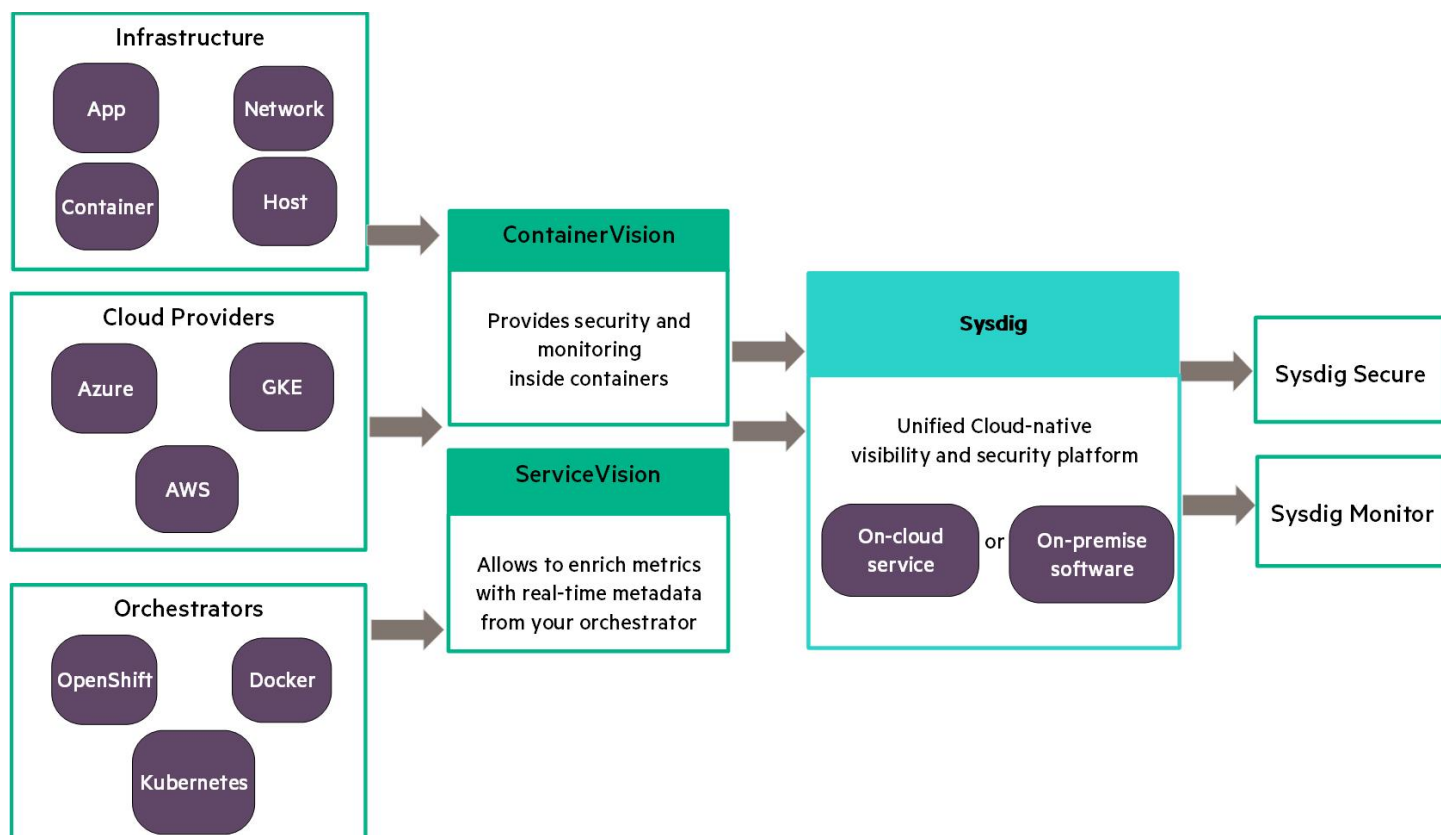


Figure 6. Sysdig products



Sysdig Monitor

Sysdig Monitor is a monitoring, troubleshooting, and alerting suite offering deep, process-level visibility into dynamic, distributed production environments. Sysdig Monitor captures, correlates, and visualizes full-stack data and provides dashboards for monitoring. With Sysdig Monitor users can do the following:

- Simplify discovery and metric collection: Transparent instrumentation dynamically discovers applications, containers, hosts, networks, and custom metrics, such as Prometheus, JMX, and statsD for deep insight into complex environments.
- Visualize service reliability: A consolidated overview of your service performance, capacity, and risk profile helps developers and DevOps quickly identify application issues and take action.
- Monitor infrastructure and applications: Deep integrations with Kubernetes, OpenShift, Docker, Mesos, DC/OS, and more lets you see beyond infrastructure into how your applications and services are performing.
- Build robust dashboards: Out-of-the-box and customizable dashboards enable at-a-glance views of your infrastructure, applications, compliance, and metrics and lets you visualize your environment the way you want.
- Simplify and scale Prometheus monitoring: Turnkey, horizontal scalability, enterprise access control and security, Prometheus metrics correlation, and PromQL queries with any event or metric, help you keep pace with large, complex environments.
- Explore the entire infrastructure: Automatic correlation of data across your infrastructure, including custom metrics from statsD, JMX, and Prometheus provides deep insight into complex environments.
- Proactively alert for faster response: Configurable alerts enable proactive notification of any condition including events, downtime, and anomalies to help you get a handle on issues before they impact operations.
- Accelerate troubleshooting: Deep container visibility, service-oriented views, and comprehensive metrics help you hunt threats and eliminate issues faster.

Sysdig Secure

Sysdig Secure is part of the Cloud-native visibility and security platform that enables enterprises to effectively secure, monitor, and troubleshoot containers and microservices in production. Sysdig Secure brings together image scanning, run-time protection, and forensics to identify vulnerabilities, block threats, enforce compliance, and perform audit activity across enterprise cloud-native environments at scale. Sysdig Secure is available as both a hosted SaaS and an on-premise software offering. Sysdig Secure helps users do the following:

- Secure the CI/CD pipeline: Identify, remediate, and mitigate vulnerabilities from deployment to production. Scan images in a registry or as part of the CI/CD process to uncover vulnerable libraries, packages, and configurations. Create vulnerability policies to fail builds, prevent images from running, and get alerted of new vulnerabilities in production.
- Block attacks: Run-time defense allows enterprises to see anomalous behavior in their application, container, host, or network, and stop or quarantine containers automatically.
- Enforce compliance. Automate and enforce regulatory compliance controls for Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), CIS, for all containers and Kubernetes environments across the lifecycle. Report on vulnerabilities, compliance posture, and incidents with robust customizable dashboards.
- Capture deep forensics: Automatically record 100% of pre- and post-attack activity, correlated with policy violations. Drill down from policy violation, to user activity, system call, and even down to the actual data written to file. Sysdig Secure forensics allow you inspect data outside of production, even if the containers are long gone.
- See full performance data: Using Sysdig Monitor, enterprises also see all performance data of their system. This gives enterprises additional early indicators of potential security problems.

Sysdig Secure and Sysdig Monitor as SaaS for the Red Hat OpenShift Container Platform

The Sysdig Secure and Sysdig Monitor works with Red Hat OpenShift Container Platform during each phase of the container lifecycle and provides a single platform to accelerate the development of reliable, secure cloud-native software on OpenShift. Sysdig Secure takes a services-aware approach to runtime security and forensics and brings together deep container visibility with OpenShift integration to block threats more effectively. Red Hat OpenShift Container Platform leverages Kubernetes as a container orchestration tool and possesses the details of how the



containers are deployed in order to map the physical deployment of containers to the logical services that are running. Sysdig leverages a deep integration with Kubernetes to map the monitoring metrics from individual containers up to the applications and services that users actually want to monitor. Sysdig uses metadata about the pods, replication controllers, and even any custom metadata to give users a way to monitor the actual applications that are deployed across many containers. Sysdig Cloud provides a rapid and cost-efficient way to gain deep insight into the performance of an OpenShift cluster. With access to this data, OpenShift operators can easily understand the health of the cluster, enable customized alerting, and have instant access to troubleshooting tools to help diagnose underlying problems. Day 2 operations of an OpenShift cluster will be difficult without this level of visibility, and are made much easier when combined with Sysdig Cloud.

Automated deployment of the Sysdig agent on the Red Hat OpenShift Container Platform

This section describes how to install Sysdig agents in an automated way on Red Hat OpenShift Container Platform running on HPE Synergy Composable Infrastructure. Sysdig agents can be installed on a wide array of Linux hosts. The assumption here is that a user will run the Sysdig agent as a pod which then enables the Sysdig agent to automatically detect and monitor Red Hat OpenShift Container Platform. HPE used Sysdig DaemonSet to deploy the Sysdig agents on every node of the OpenShift Container Platform cluster. A DaemonSet ensures that all OpenShift nodes run a copy of a pod. As nodes are added to the cluster, pods are added to the newly introduced nodes. As nodes are removed from the cluster, those pods are in turn garbage collected. Deleting a DaemonSet will clean up the pods it created. This DaemonSet internally runs three kinds of daemons on every node:

- Cluster storage daemon
- Logs collection daemon
- Monitoring daemon

Once these daemons are deployed on OpenShift nodes, the Sysdig Monitor automatically begins monitoring all of the hosts, applications, pods, and services and automatically connects to the OpenShift API server to pull relevant metadata about the environment. If licensed, Sysdig Secure launches with default policies that a user can view and configure to suit their needs.

To install Sysdig agents on the Red Hat OpenShift Container Platform nodes, use the repository located at the HPE OpenShift Solutions GitHub at <https://github.com/hewlettpackard/hpe-solutions-openshift>. This repository contains Ansible plays and scripts to automate installation.

About the repository

- **Playbooks:** This folder contains the playbooks required for Sysdig agent installation on the Red Hat OpenShift Container Platform.
- **Roles:** This folder contains a role called "sysdig-agent-deploy-ocp" which is responsible for performing the actions required for Sysdig agent integration.
- **Hosts:** This is the host file which will be used by Ansible Engine to reference hosts during Sysdig agent deployment. Provide the OpenShift Container Platform master node complete host name in this file.
- **site.yaml:** In this file, the playbook "sysdig-agent-deployment.yaml" is imported. This file defines the entire workflow for Sysdig integration.

Prerequisites

In order to successfully deploy Sysdig agents on the OpenShift Container Platform nodes, refer to following pre-requisites:

- Red Hat OpenShift Container Platform 3.11 is up and running.
- Worker nodes in the Red Hat OpenShift Container Platform deployment can be virtual or physical running RHEL 7.6.
- The installation user has SaaS based access to Sysdig Secure and Sysdig Monitor for the purpose of container security.
- The installation user has admin rights and privileges for Sysdig Secure and Sysdig Monitor.
- Sysdig agents with version 0.90.3 are deployed on OpenShift Container Platform.
- The installation user has a valid access token that is given by Sysdig and is specific to their credentials on Sysdig Monitor and Sysdig Secure.
- The installation user has updated the kernel to make sure all RHEL nodes are running the same kernel version. Run the following command to install kernel headers on master, infra and worker nodes of OCP: `yum -y install kernel-devel-$(uname -r)`



Custom attributes\variable files and plays

Each playbook has a role associated with it. Each role has a set of tasks under the "task" folder and variables under the "var" folder. These variable values need to be defined by the user according to the installer's environment before running the plays:

- `sysdig-agent-deploy-ocp/vars/main.yml`: This file will be used during Sysdig agent deployment to OpenShift and contains Sysdig related variables.
- `sysdig-agent-deploy-ocp/tasks/main.yml`: This file contains the actual Sysdig agent installation steps.
- `sysdig-agent-deploy-ocp/files/sysdig-agent-configmap.yml`: This file is provided by Sysdig and handles the Sysdig software related configurations.
- `sysdig-agent-deploy-ocp/files/sysdig-agent-daemonset-redhat-openshift.yml`: This file is provided by Sysdig and handles the Sysdig daemon related configurations.

How to use playbooks

This section describes the steps that need to be performed to use the playbooks:

1. Clone the repository to the Ansible Engine host using the following command:

```
# git clone https://github.com/hewlettpackard/hpe-solutions-openshift
```

2. From the Ansible Engine command prompt, browse the cloned directory and navigate to following sub-directory:

```
# cd OpenShift-Synergy-RA-master/synergy/scalable/security-sysdig
```

3. Update the variables in the following files:

– hosts

- Provide the master node (only 1 master node is required) fully qualified domain name or ip address under [master]. All the Sysdig specific files will be copied to this master node.

– vi roles/sysdig-agent-deploy-ocp/vars/main.yml

- Provide a value for the project name for Sysdig integration with OCP under the "**projectname**" variable.
- Provide the Sysdig access key/token value. This value is retrieved from the user setting by logging into either Sysdig Secure or Sysdig Monitor GUI in "**accesskeyval**" variable.

– vi roles/sysdig-agent-deploy-ocp/files/sysdig-agent-configmap.yml

- Enter "OpenShift" as the cluster type.
- Enter the Sysdig Collector address and port. Check with Sysdig team to know which collector is accessible in your environment and over which port.
- It is recommended to access Sysdig collector over Secure Socket Layer (SSL) port. For both the keys "ssl" and "ssl certificate validate" set the value as "true".
- Set the variable related to the underlying Kubernetes deployment that is OpenShift in this solution, to true.
- Enter the cluster name of the OpenShift cluster.

4. Run the play using following command:

```
# ansible-playbook -i hosts site.yml
```

5. To verify the deployment, log in to the master node that is mentioned in the hosts file and type the following command:

```
# oc get pods
```



This command will output all the Sysdig agent names running on each of the nodes within your OpenShift cluster as shown in Figure 7. If you see a pod with a pending status, then there might be a possibility that the underlying OCP node is not functional.

NAME	READY	STATUS	RESTARTS	AGE
sysdig-agent-2p68f	1/1	Running	0	4d
sysdig-agent-2rqb6	1/1	Running	0	4d
sysdig-agent-4z7bp	1/1	Running	0	4d
sysdig-agent-8j6xt	1/1	Running	0	4d
sysdig-agent-8ld76	1/1	Running	0	4d
sysdig-agent-jf725	1/1	Running	0	4d
sysdig-agent-qlfx6	1/1	Running	0	4d
sysdig-agent-tlzs5	1/1	Running	0	4d
sysdig-agent-vvxck	1/1	Running	0	4d

Figure 7. Sysdig agents running on OpenShift nodes

6. Check the number of nodes that are currently up and running in the OpenShift Container Platform deployment using the command “oc get nodes” as shown in Figure 8.

```
[root@buramaster03 ~]# oc get nodes
```

NAME	STATUS	ROLES	AGE	VERSION
burainfra01.tennet.local	Ready	infra	19d	v1.11.0+d4cacc0
burainfra02.tennet.local	Ready	infra	19d	v1.11.0+d4cacc0
burainfra03.tennet.local	Ready	infra	19d	v1.11.0+d4cacc0
buramaster01.tennet.local	Ready	master	19d	v1.11.0+d4cacc0
buramaster02.tennet.local	Ready	master	19d	v1.11.0+d4cacc0
buramaster03.tennet.local	Ready	master	19d	v1.11.0+d4cacc0
buraworker01.tennet.local	Ready	compute	19d	v1.11.0+d4cacc0
buraworker02.tennet.local	Ready	compute	19d	v1.11.0+d4cacc0
buraworker03.tennet.local	Ready	compute	19d	v1.11.0+d4cacc0

Figure 8. OpenShift nodes information



7. From the Sysdig Secure web interface, click on the icon named **POLICY EVENTS** and you will see the web interface for **Policy Events** tab. On the **Policy Events** tab, click the **Groupings** drop-down list and select **Entire Infrastructure**. The user with administrative privileges should be able to see all of the OCP nodes as in Figure 9.

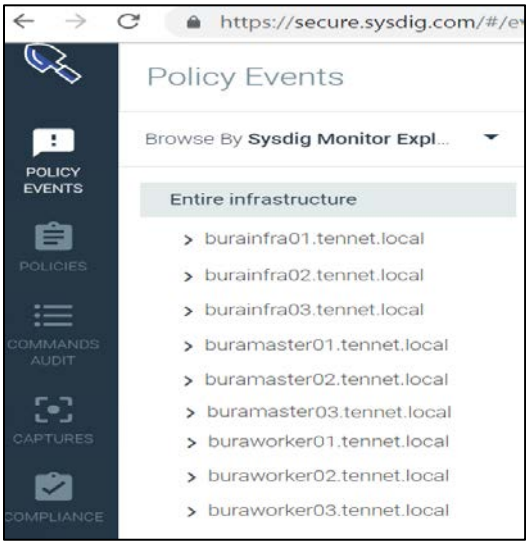


Figure 9. OpenShift cluster in Sysdig Secure

8. From the Sysdig Monitor web interface, click on the icon named **EXPLORE** and you will see the web interface for the **Explore** tab. On the Explore tab, click the **Data Source** (two rectangles) drop-down menu and select the data source named **Sysdig Agents** from the drop-down list. Then open the **Groupings** drop-down list and select **Clusters and Nodes**. The user with administrative privileges should be able to see all of the OCP nodes as in Figure 10.

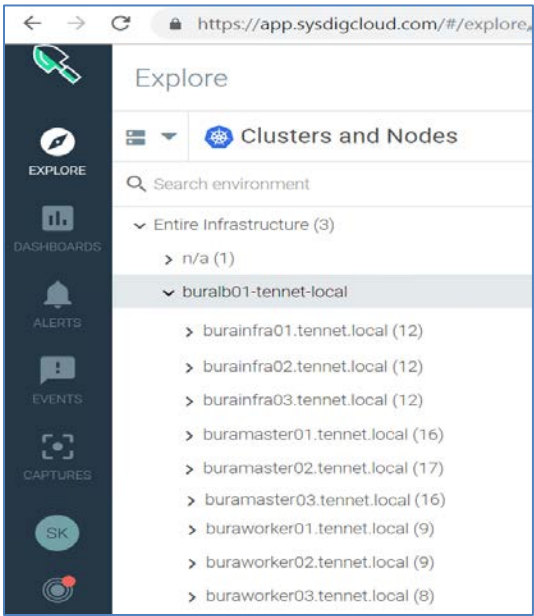


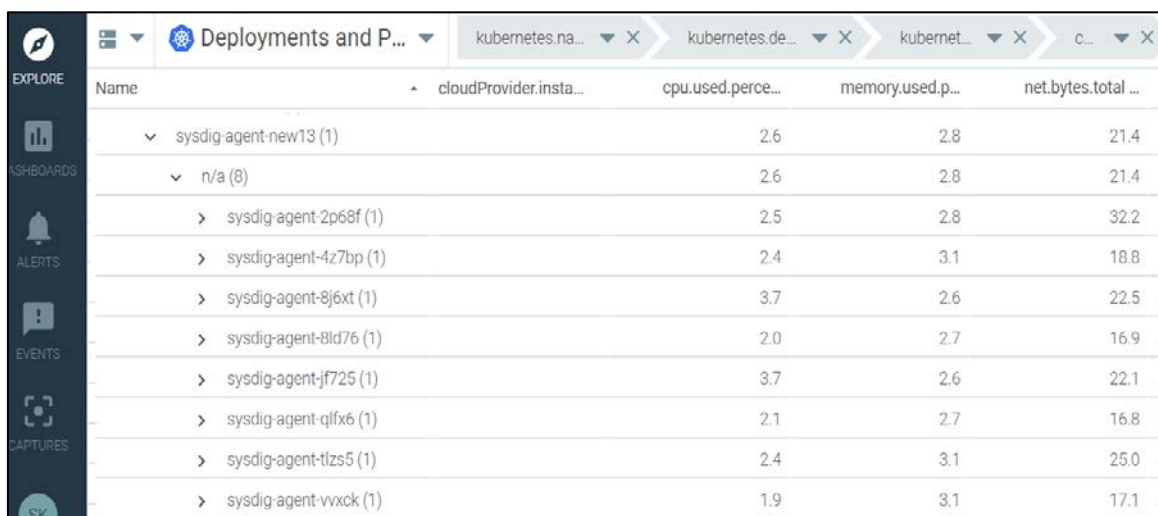
Figure 10. OpenShift cluster in Sysdig Monitor



Note

- For an explanation of host requirements for Agent Installation, refer to: <https://sysdigdocs.atlassian.net/wiki/spaces/Platform/pages/192151570/Host+Requirements+for+Agent+Installation>.
- It is recommended to use port 6443 that transfers and receives data over Secure Sockets Layer/ Transport Layer Security (SSL/TLS) protocol. Sysdig agents transfer data to Sysdig Cloud over HTTPS that encrypts and decrypts the requests as well as the responses that are returned by the Sysdig Cloud.
- The OpenShift cluster name can be found by using the command “`oc config view`” from any master node.

9. From the Sysdig Monitor web interface, click on the icon named **EXPLORE**. On the Explore tab, click the **Data Source** (two rectangles) drop-down menu and select the data source named **Sysdig Agents** from the drop-down list. Open the **Groupings** drop-down list and select **Deployment and Pods**. A user with administrative privileges should be able to see all the agents and their details as shown in Figure 11.



Name	cloudProvider.insta...	cpu.used.perce...	memory.used.p...	net.bytes.total ...
▼ sysdig-agent-new13 (1)		2.6	2.8	21.4
▼ n/a (8)		2.6	2.8	21.4
➤ sysdig-agent-2p68f (1)		2.5	2.8	32.2
➤ sysdig-agent-4z7bp (1)		2.4	3.1	18.8
➤ sysdig-agent-8j6xt (1)		3.7	2.6	22.5
➤ sysdig-agent-8ld76 (1)		2.0	2.7	16.9
➤ sysdig-agent-jf725 (1)		3.7	2.6	22.1
➤ sysdig-agent-qlfx6 (1)		2.1	2.7	16.8
➤ sysdig-agent-tlzs5 (1)		2.4	3.1	25.0
➤ sysdig-agent-vvxck (1)		1.9	3.1	17.1

Figure 11. Sysdig agents running on the OpenShift cluster

Summary

With the ever-increasing vulnerabilities present from the hardware to the firmware to the OS, containers, applications, and workloads, the threat landscape is increasing. Though multiple security controls are available across various infrastructure components, customers don't really get the holistic view of controls that is needed to ensure every surface is properly hardened. More importantly, due to the extensive number of security controls and multiple documents available to customers, it is a challenge to identify the best practices to be followed in order to achieve the highest level of security or to comply with industry or business specific compliance requirements such as PCI DSS and HIPAA. The current Hewlett Packard Enterprise solution addresses three major security concerns:

- A view of container security risks and concerns.
- The layered view of the security controls across hardware and firmware that are available to the customers in the HPE Composable Infrastructure.
- A consolidated view of the OpenShift Container Security and Monitoring using Sysdig Secure and Sysdig Monitor.

With Red Hat OpenShift Container Platform and HPE Synergy, you can compose and reconfigure your container environment. The solution is optimized for continuous integration and continuous delivery (CI/CD) by Red Hat OpenShift Container Platform, and for running cloud-native microservices applications alongside existing traditional and stateful applications. With Sysdig cloud deployment model for Sysdig Secure and Sysdig Monitor, you can take a services-aware approach to run-time security and forensics. You can visualize the health of your Red Hat OpenShift Container Platform running on HPE Synergy Composable Infrastructure to get comprehensive metrics to help you identify and

eliminate issues faster. You can also build fine-grained alerts for proactive notification of events, anomalies, and downtime, and solve problems faster by seeing what happened, even after containers and hosts are gone.

Appendix A. Image scanning using Sysdig Secure

Sysdig Secure provides the following benefits for Red Hat OpenShift Container Platform:

- **Vulnerability management:** Scan images and block vulnerabilities across your CI/CD pipeline, registry, or in production.
- **Compliance and audit:** Detect violations of external compliance requirements such as The Center for Information Security (CIS), Payment Card Industry Data Security Standard (PCI DSS), General Data Protection Regulation (GDPR), or enforce custom compliance controls.
- **Adaptive run-time defense:** Identify and block threats based on application, container, or network activity.
- **Forensics:** Trigger automatic system captures to see activity before and after security events.

OpenShift Container images can be scanned using the following steps:

1. Log in to Sysdig Secure using valid administrator credentials.
2. Select the desired node from the OpenShift cluster and look for statistics about scanned and unscanned images as shown in Figure A1.

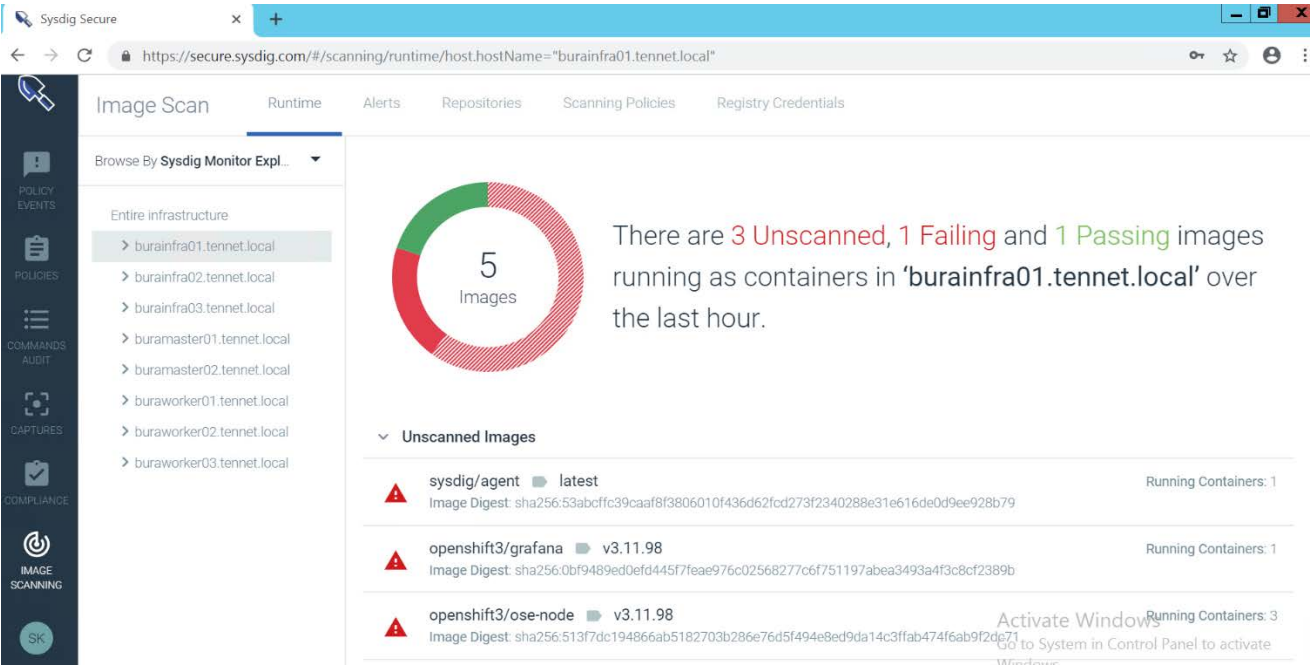


Figure A1. Select a node to be assessed for security from the OpenShift cluster



3. Select the image scan policy to learn the details of the security rules against which an image under scan will be assessed. Figure A2 shows the specifications from default policy named “NIST 800-190”.

Image Scan Runtime Alerts Repositories **Scanning Policies** Registry Credentials

Edit Policy

Name

Default Audit Policy - NIST 800-190

Description

This policy interprets NIST 800-190 controls and provides out of the box rules to detect image misconfiguration. We frequently update these policies and if you'd like to modify the policy you should use this as a base template to avoid modifications being overwritten.

Rules

Vulnerabilities	Stale feed data	Max days since sync: 7	Warn
Npms	Unknown in feeds	No parameters required	Warn
Vulnerabilities	Package	Package type: non-os; Severity comparison: >=; Severity: high	Warn
Vulnerabilities	Package	Package type: os; Severity comparison: >=; Severity: high	Warn
Dockerfile	Instruction	Instruction: USER; Check: not_exists	Warn
Dockerfile	Exposed ports	Ports: 22; Type: blacklist	Warn

Figure A2. Details of NIST 800-190 container security policy

4. From the OpenShift node repository being secured by Sysdig Secure, select the image that needs to be scanned as shown in Figure A3.

Image Scan Runtime Alerts **Repositories** Scanning Policies Registry Credentials

Repositories > openshift3/ose-node v3.11.98


Image ID: N/A

Image Created: N/A

OS / Version: N/A

Size: N/A

Layers: N/A



This image has not been scanned!

SCAN NOW

Note: This will attempt to scan the most recent digest associated with the image at 'registry.redhat.io/openshift3/ose-node:v3.11.98'.

Figure A3. Select the image to be scanned from the list of images available within the OpenShift cluster selected node



5. Provide the registry credentials as shown in Figure A4.

Image Scan

Runtime

Alerts

Repositories

Scanning Policies

Registry Credentials

Edit Registry

Path

registry.redhat.io,

Type

Docker V2

Username

Enter your username

Password

Enter your password

Internal Registry Address

Optional: e.g. docker.registry.svc:5000, docker-registry.default.svc.cluster.local:5000

Allow Self Signed

☐

Use Image to Test Credentials

☐

Figure A4. Registry credentials for the image

6. Start scanning the image and see the progress summary on the dashboard as listed in Figure A5.

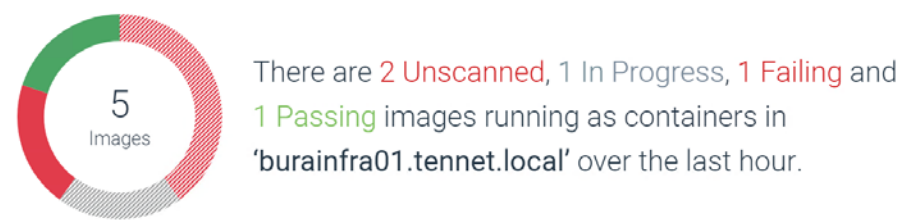


Figure A5. Image Scan summary



7. Once the scan completes, check the status of scan and look for vulnerabilities along with the recommendations to remediate the vulnerabilities as reported by Sysdig Secure as shown in Figure A6.

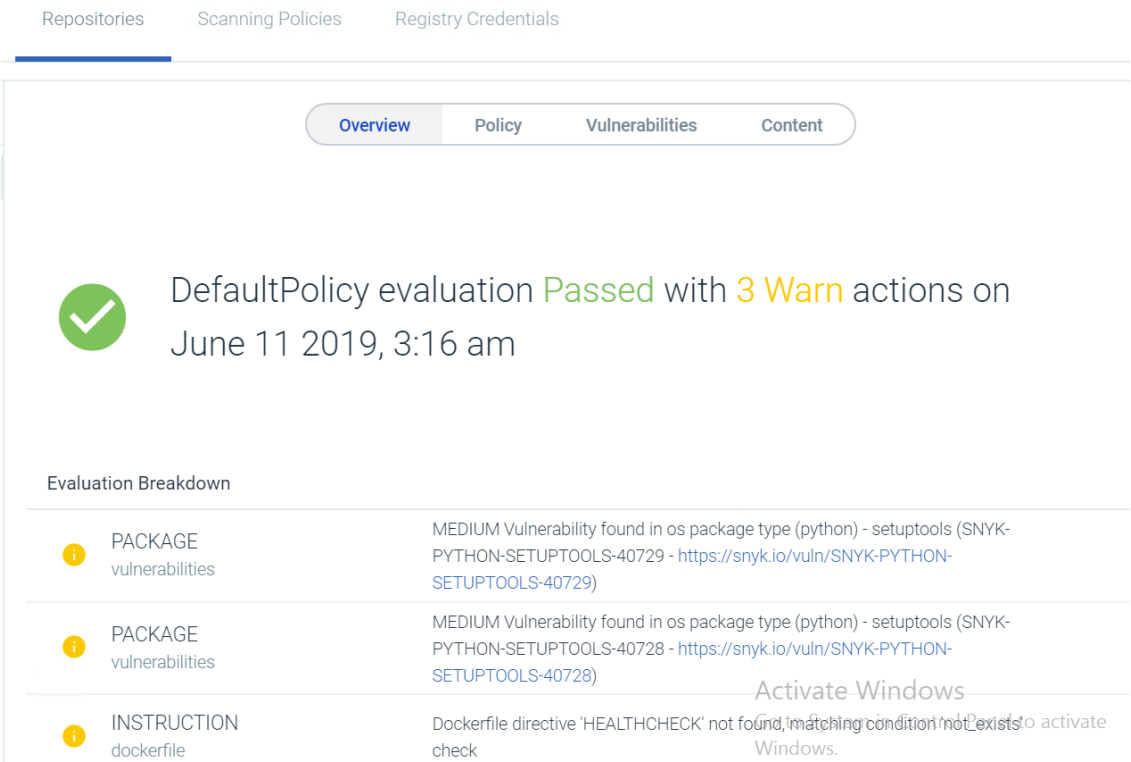


Figure A6. Summary of vulnerabilities reported by the Image Scanning process



Change Tracker

Version	Release Date	Changes
1.0	07/11/2019	Initial release



Resources and additional links

Red Hat, <https://www.redhat.com/>

Red Hat OpenShift Container Platform 3.11 documentation, <https://docs.openshift.com/container-platform/3.11/welcome/index.html>

HPE Synergy, <https://www.hpe.com/us/en/integrated-systems/synergy.html>

HPE OpenShift Solutions on GitHub, <https://github.com/HewlettPackard/hpe-solutions-openshift>

HPE Reference Configuration for Red Hat OpenShift on HPE Synergy and HPE Nimble Storage,
<https://h20195.www2.hpe.com/v2/getdocument.aspx?docname=a00056101enw>

HPE Reference Configuration for Red Hat OpenShift on HPE Synergy and HPE 3PAR StoreServ Storage,
<https://h20195.www2.hpe.com/v2/getdocument.aspx?docname=a00056102enw>

Sysdig, <https://sysdig.com/>

Agent Install on OpenShift,
<https://sysdigdocs.atlassian.net/wiki/spaces/Platform/pages/192348345/Agent+Install+Kubernetes+GKE+OpenShift+IBM>

To help us improve our documents, please provide feedback at www.hpe.com/contact/feedback.

Share 

© Copyright 2019 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Red Hat is a registered trademark of Red Hat, Inc. in the United States and other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Intel is a trademark of Intel Corporation in the U.S. and other countries. Microsoft is a registered trademark of Microsoft Corporation in the United States and/or other countries.

Version 1, July 2019

