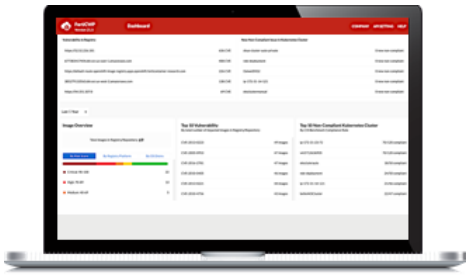
DATA SHEET

FortiCWP Container Guardian

Container Protection for Cloud-Native Applications



Available in:

Cloud

The adoption of cloud native technologies to deliver new products and services has enabled Organizations to rapidly transform key areas of their business. These technologies include the use of containers in microservices architectures, which have streamlined the way applications are built, tested, deployed and redeployed. Conversely, this has led to a new attack surface, leading to new risks that can expose organizations if not properly addressed.

Traditional security tools lack the in-depth capabilities to secure container workloads. Container security requires visibility and protection during all stages of a container lifecycle.

FortiCWP's Container Guardian embeds security throughout the software development cycle for container workloads and monitors for the following security risks:

Propagation of vulnerabilities into CI/CD pipeline

Vulnerabilities and Misconfigurations in Container and Kubernetes environments

Non-compliant configurations based on industry-wide security best practices

Key Features

FortiCWP Container Guardian provides deeper visibility into the security posture for container-based workloads, across multi-cloud environments.

- Centralized visibility into the risk profiles for containers and workloads
- Shift Left security: embeds security into SW development lifecycle
- Integrations with developer toolchains to automate and build CI/CD pipeline with policy enforcement tools to control build process
- Continuously monitors and scans for known vulnerabilities, threats, and misconfigurations
- Secures containers, hosts, and Kubernetes environments
- Enhances compliance to CIS security benchmarks with tools to monitor and drive security governance

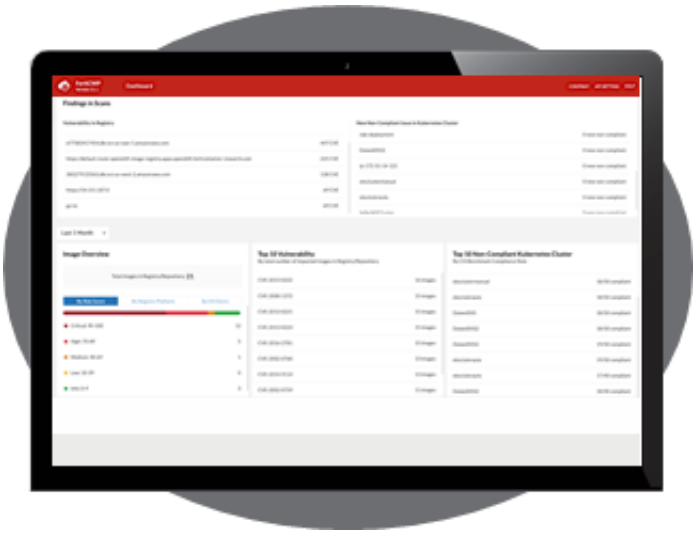
FEATURE HIGHLIGHTS

FortiCWP Container Guardian provides deeper visibility into the security posture for container-based workloads, across-multi-cloud environments. FortiCWP Container Guardian automates security and builds CI/CD pipeline from trusted images. Container registries are scanned for known vulnerabilities to prevent propagation across images, containers, and Kubernetes environments. FortiCWP Container Guardian minimizes risk for Kubernetes workloads by detecting container misconfigurations and non-conformance against security best practices.

FortiCWP Container Guardian simplifies DevSecOps adoption by integrating security in the early stages of the software development process to provide ongoing protection for containers and Kubernetes workloads.

Centralized Visibility

FortiCWP Container Guardian provides a centralized dashboard with key insights into container registries and workload clusters in multi-cloud environments. Risk profiles for container images enable security teams to focus on the highest priority images to remediate, while the investigation and analysis tools ensures workload clusters conforms to CIS Security best practices to prevent unsecure workloads from being deployed.



FortiCWP Container Guardian Dashboard

Automates Security and Builds CI/CD Pipeline

FortiCWP Container Guardian scans images during the build cycle to detect for known vulnerabilities. Automated policies can fail the build to prevent vulnerabilities from being propagated into container registries through the application lifecycle.

Container Guardian has integrations with developer toolchains, such as Jenkins, to integrate image vulnerability scanning into the CI/CD workflow when images are created, with customizable policies for allowing images below a specified severity threshold to be deployed to container registries. This ensures only trusted images are allowed to run on hosts or Kubernetes clusters.

Automating security allows DevOps team to focus on more critical aspects of the application build cycle.

Vulnerability Management

Vulnerabilities discovered on deployed images in container registries can make it easier for hackers to exploit these weaknesses to their advantage. While patching can alleviate the issue, the vulnerability may have already been exploited, causing damage to an organization. The most effective way to mitigate the risk is to identify the vulnerabilities before the images are deployed to container registries.

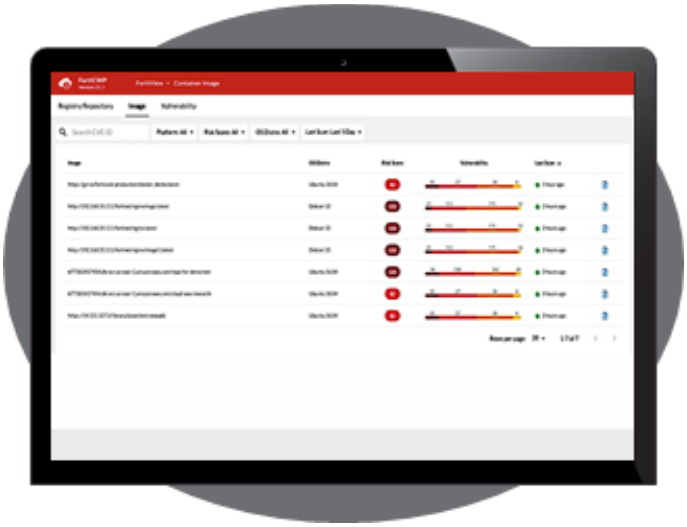
FortiCWP Container Guardian gives Administrators deeper insights into vulnerabilities for images, containers, hosts and work nodes with automated policy enforcement. Container images are analyzed against known vulnerabilities with results shown as risk scores based on the severity of the vulnerability discovered. And as new vulnerabilities emerge, Container Guardian will continue to monitor and scan containers and Kubernetes environments to provide ongoing protection.

FEATURE HIGHLIGHTS

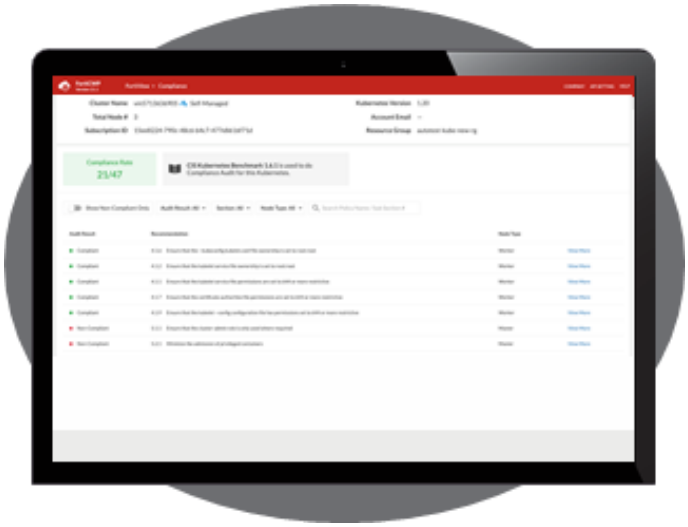
Validates against Industry-wide Security Best Practices

FortiCWP Container Guardian provides visibility into the compliance posture across containers and Kubernetes workloads. Integrations with leading Security benchmark policies allows DevOps teams to build container and workloads using CIS security best practices. FortiCWP's Container Guardian performs compliance assessments on Kubernetes workloads, with policies that can be set to auto-remediate or alert Administrators with recommendations to remediate.

Container Guardian's continuous monitoring will scan for new non-compliant issues. Policy enforcement tools monitor and drive security governance to prevent deployment of unsafe workloads.



FortiCWP Container Guardian Vulnerability Management



FortiCWP Container Guardian Compliance

Broad Platform Integration

FortiCWP Container Guardian supports containers running on Linux. It supports self-managed and hosted orchestration platforms such as Amazon Elastic Kubernetes Service (EKS), Google Kubernetes Engine (GKE), Azure Kubernetes Service (AKS), and integrates with Amazon Elastic Container Service (ECS), Google Cloud Registry (GCR), Azure Container Registry (ACR), Harbor and Red Hat Openshift.

ORDER INFORMATION

The FortiCWP Workload Guardian license is required to enable visibility and protection for public cloud resources and workloads.

- FortiCWP Storage Guardian license add-on license is required for monitoring and protection of public cloud storage
- FortiCWP Container Guardian add-on license is required to enable security for container workloads

PRODUCT	SKU	DESCRIPTION
FortiCWP Workload Guardian	FC-10-FCWPW-315-02-DD	FortiCWP Workload Guardian – Subscription per 20 hosts
FortiCWP Workload Guardian	FC2-10FCWPW-315-02-DD	FortiCWP Workload Guardian – Subscription per 100 hosts/instances for all supported public cloud
FortiCWP Storage Guardian	FC-10-FCWPS-316-02-DD	FortiCWP Cloud Storage Protection, Basic, per 100GB data
FortiCWP Storage Guardian	FC1-10-FCWPS-316-02-DD	FortiCWP Cloud Storage Protection, Basic, per 1TB data
FortiCWP Storage Guardian	FC-10-FCWPS-317-02-DD	FortiCWP Cloud Storage Protection, Advanced (w/ DLP scan), per 100GB data
FortiCWP Storage Guardian	FC1-10-FCWPS-317-02-DD	FortiCWP Cloud Storage Protection Advanced (w/ DLP scan) per 1TB data
FortiCWP Container Guardian	FC-10-FCWPC-327-02-DD	FortiCWP Container Guardian. Subscription per 4 container hosts/work nodes

FCWP-CG-DAT-R1-20210623