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
FEATURE HIGHLIGHTS


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 ensure workload clusters conform to CIS Security best practices to prevent unsecure workloads from being deployed.

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.

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

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