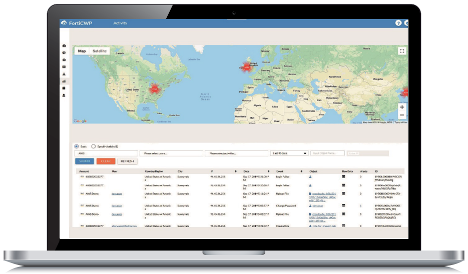
DATA SHEET

FortiCWP

Visibility and Insight for IaaS Workloads and Storage



FortiCWP is Fortinet's cloud-native Cloud Workload Protection (CWP) service. FortiCWP integrates with APIs provided by cloud vendors including AWS, Azure and Google Cloud Platform to monitor and track all security components, including configurations, user activity, and traffic flow logs. FortiCWP will also scan containers for vulnerabilities and misconfigurations, and cloud data stores for sensitive or malicious content. Reports can also be generated on your environment's compliance posture against common regulatory standards.

Equipped with predefined security policies out-of-the-box FortiCWP monitors the following security risks:

- Malicious Traffic
- Suspicious User Activity
- Sensitive Data & Malware
- Compliance Violations
- Vulnerabilities and Misconfigurations

Key Features

FortiCWP provides centralized dashboards, reports, and maps, to track security events and user activity.

- Centralized visibility
- On-demand data scanning
- User insights and policies
- Compliance and DLP
- Threat protection and response
- Risk assessment and account scores
- FortiGuard integration for advanced threat detection
- Configuration assessments and compliance reports
- Visibility and security for containers

FEATURE HIGHLIGHTS

Using an API-based approach, FortiCWP is tightly integrated with leading IaaS providers to access usage and data stored in various clouds. FortiCWP gives IT security professionals the ability to scan provisioned cloud resource configurations, data and usage for potential threats, misconfigurations and compliance violations. This approach also ensures that all users of the organization's IaaS resources are monitored and protected by FortiCWP no matter where they are or what device they are using.

Built from the "Fabric-up", FortiCWP is designed for deep integration into the Fortinet Security Fabric to provide consolidated cloud usage management and reporting.

Central Visibility

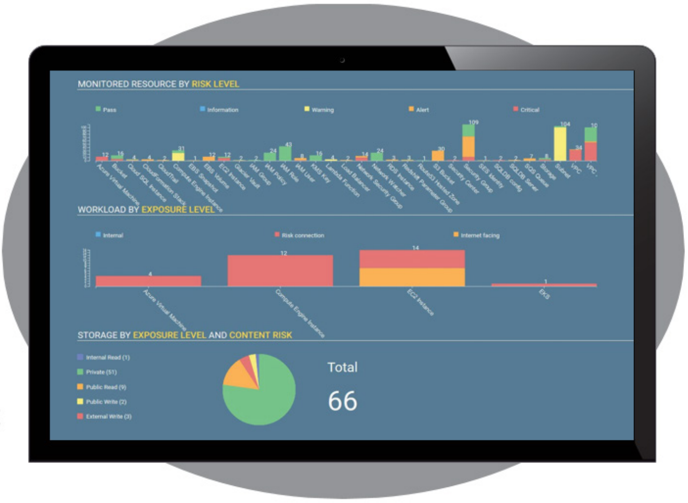
FortiCWP provides central visibility and reporting for multi-cloud environments. FortiCWP provides dashboards, logs, and reports that make it easy to understand your security status at a glance. User activity, cloud resources, files and data, policies and much more can be centrally viewed. User activities can be displayed as a list or on a map. Relationships between resources are graphically displayed so administrators can quickly understand infrastructures of all monitored cloud accounts and so that the relationship between cloud resource instances and services can easily be understood.

On-Demand Data Scanning

Unlike a proxy-based service or hardware device, FortiCWP directly connects to the cloud provider to access data and files stored in an organization's accounts. New information is validated against data leakage policies and scanned for threats. Existing information or "data at rest" is also scanned to ensure it meets business policies. If a business policy is updated, it can be easily applied to data stored in the cloud by the administrator.

Compliance and DLP

FortiCWP offers a highly customizable suite of data loss prevention tools that defend against data breaches and provides a set of predefined compliance reports. Using industry-standard regular expressions, FortiCWP can be configured for nearly any policy to meet data protection needs and provide tailored reports on DLP activities. For organizations that must meet compliance standard, FortiCWP offers predefined reports for standards including PCI, HIPPA, SOX, GDPR, ISO 27001, and NIST which allows organizations to generate compliance reports instantly for auditing teams, so policy violations can be identified and remediated.



FortiCWP Resource Monitoring

User Insights and Policies

FortiCWP offers many tools to provide insights into user behaviors and their activities on cloud-based applications. Administrators can monitor usage as needed and have the ability to view user entitlements, dormant users, and conduct detailed configuration assessments.

Threat Protection and Response

FortiCWP uses User Entity Behavior Analytics (UEBA) to look for suspicious or irregular user behavior. It also sends out alerts for malicious behavior. User and entity behavior analytics is a security process that monitors the normal actions of users. FortiCWP uses risk scoring techniques and advanced algorithms to detect anomalies over time.

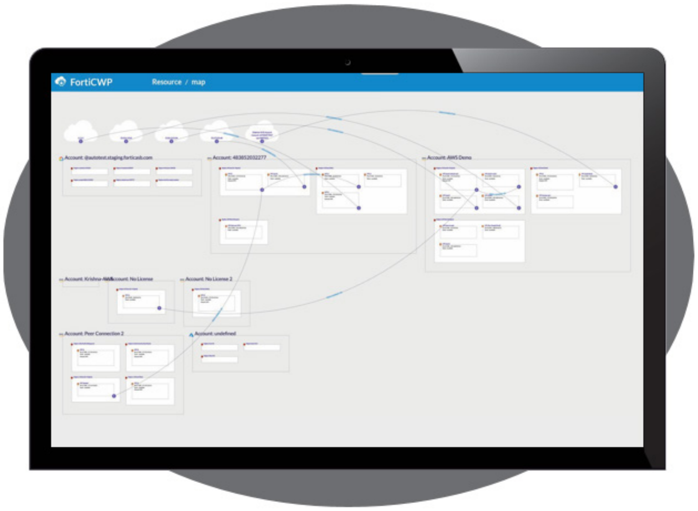
FortiGuard Integration for Advanced Threat Detection

FortiCWP automatically includes the award-winning FortiGuard antivirus services to scan files stored in the cloud. This service is provided at no extra cost to FortiCWP subscribers.

FEATURE HIGHLIGHTS

Risk Assessment and Account Scores

FortiCWP's deep risk assessment and continuous analysis solution enables security teams to focus on the highest priority issues, take quick remediation as well as utilizing auto fixing option to effectively manage and address risk. Actionable alerts enable organizations to prioritize response based on the severity of the issues. To help assess risk, FortiCWP generates a security risk score.



FortiCWP Resource Mapping

Configuration Assessments and Compliance Reports

FortiCWP performs hundreds of IaaS configuration assessments across the organization's global IaaS deployment on AWS, Azure, and GCP. FortiCWP identifies risks associated with the unsecure provisioning and configuration of cloud resources. Using the information that is gathered by continuously evaluating existing cloud configurations, FortiCWP generates compliance reports that list gaps from regulation requirements of supported reports. FortiCWP provides out-of-the-box policies for standards such as PCI, HIPPA, SOX, GDPR, ISO 27001, and NIST.

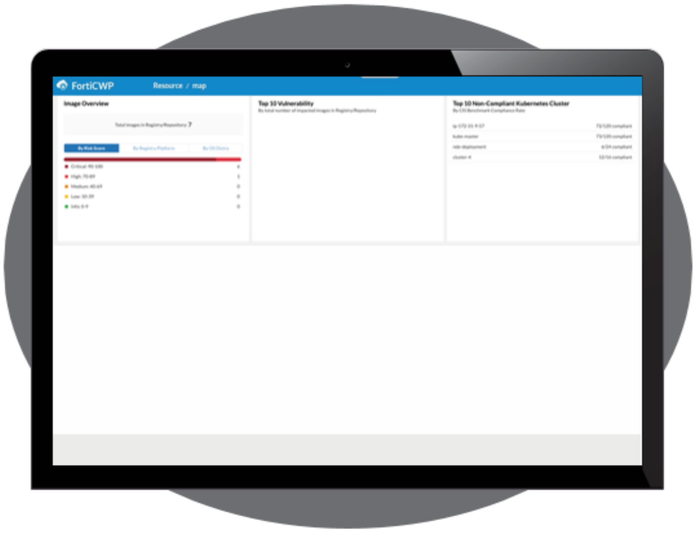
Integration into DevOps toolchain

Container Guardian integrates with common CI/CD tools to embed security testing into the software development cycle and enforces policies to control the build process.

Integrated Security for Containers

FortiCWP's Container Guarding provides deeper visibility into the security posture for container registries and repositories. Container images are scanned for vulnerabilities during the build process with policy enforcement tools to prevent vulnerability propagation before images are deployed into container registries. Registries are continuously monitored and scanned for new vulnerabilities to provide continuous protection.

Container Guardian performs continuous audits in containers and clusters to detect misconfigurations and other non-compliant security practices with policies to alert IT teams or auto-remediate.


FortiCWP
Resource / map
Image Overview
Total images in Registry/Repository 7
By Risk Score
By Registry Platform
By OS Distro
Critical 90-100 4
High 70-89 1
Medium 40-69 0
Low 10-39 0
Info 0-9 0
Top 10 Vulnerability
By total number of impacted images in Registry/Repository
Top 10 Non-Compliant Kubernetes Cluster
By CIS Benchmark Compliance Rate
ip-172-31-9-57 73/120 compliant
kube-master 73/120 compliant
nde-deployment 6/24 compliant
cluster-X 13/16 compliant

FortiCWP Container Guardian

ORDER INFORMATION

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

www.fortinet.com