FortiCWP™
Visibility and Insight for IaaS Workloads and Storage

FortiCWP is Fortinet’s cloud-native Cloud Workload Protect (CWP) service. FortiCWP hooks into the 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 cloud scan data stores for sensitive or malicious content and it will produce reports on your environment’s compliance with common regulatory standards.

FortiCWP provides centralized dashboards, reports and maps to track security events and user activity. Its features include:

- 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

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

- Malicious Traffic
- Suspicious User Activity
- Vulnerable Configuration
- Sensitive Data & Malware
- Compliance Violations
HIGHLIGHTS

Using an API-based approach, FortiCWP is tightly integrated into 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.

FEATURES

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 to 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.

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.

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 standards, 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 remediated.

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.
FEATURES

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 issues. To help assess risks, FortiCWP generates a security risk score.

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

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.

Order Information

<table>
<thead>
<tr>
<th>Product</th>
<th>SKU</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FortiCWP Workload Guardian</td>
<td>FC1-10-FCWPW-315-02-DD</td>
<td>FortiCWP Workload Guardian - Cloud workload protection. Subscription per 20 hosts/instances for all supported public clouds</td>
</tr>
<tr>
<td>FortiCWP Storage Guardian</td>
<td>FC1-10-FCWPS-316-02-DD</td>
<td>FortiCWP Cloud Storage Protection, Basic – Subscription per 1TB data</td>
</tr>
<tr>
<td></td>
<td>FC1-10-FCWPS-317-02-DD</td>
<td>FortiCWP Cloud Storage Protection, Advanced (with additional DLP scan) – Subscription per 1TB data</td>
</tr>
</tbody>
</table>

Note: The SKUs are newly available for purchase in 2019 Q4.