Fortinet offers customers a comprehensive set of products and solutions to address their public cloud infrastructure security needs. Customers need to continuously manage cloud risk, manage and respond to active threats, and implement security earlier in the application lifecycle across multiple public and private cloud infrastructures. Fortinet Cloud Native Protection (FortiCNP) simplifies cloud security operations and empowers security teams to take impactful, timely actions by utilizing deep integrations with a broad range of cloud security products, services, and technologies.

FortiCNP provides security visibility and insights for Cloud workloads such as virtual machines, databases, gateways & containers. FortiCNP analyzes the configuration and activity of cloud workloads over time to identify risk and threats. It integrates with AWS, Azure and GCP APIs to monitor and track security aspects of resources including configurations, data, and traffic. It also scans containers for vulnerabilities & misconfigurations, it scans cloud data stores for sensitive or malicious content, and generates reports on the environment’s compliance posture against common regulatory standards.

FortiCNP, Fortinet’s cloud-native protection product helps security teams prioritize risk management activities based on a broad set of security signals from their cloud environments. Beyond the built-in CSPM and data scanning capabilities, FortiCNP collects information from multiple cloud native security services that provide vulnerability scanning, permissions analysis, and threat detection as well as Fortinet cloud security products. Based on the information it collects, FortiCNP calculates an aggregate risk score for cloud resources, so customers can then manage risk management work based on resource risk insights (RRI) FortiCNP produces. Unlike traditional CSPM and CWPP products that require agents, excessive permissions and produce unmanageable volumes of data, by integrating with cloud native security services and other Fortinet Security Fabric products, FortiCNP provides deep security visibility across cloud infrastructures and helps prioritize security workflows for effective risk management.
Resource Risk Insights

Resource Risk Insights (RRI) turn overwhelming volumes of data into actionable insights. By correlating information from a breadth of cloud native and Fortinet security products into a comprehensive cloud risk graph database, FortiCNP creates a current and accurate map of risk interdependencies for your cloud environment. You can customize RRI's based on environmental and workload specific attributes to best suit your environment. RRI's are based on analysis of configurations, vulnerabilities, permissions, accessible data, threats and the relationship between these findings.

Malware Scanning

FortiCNP Malware Scanning utilizes Fortiguard Labs malware scanning technology across all data stores in your cloud environment to protect from the potential impact of dormant malware. Instead of scanning workloads in runtime, which requires deploying agents that detect malware after the fact, FortiCNP provides the ability to detect malware throughout the data supply chain by scanning cloud data stores, disk volumes and workload images\(^1\).

Cloud Native Integration

FortiCNP’s RRI technology allows you to enjoy the ease of deployment offered by cloud provider security services, without the associated alert fatigue. This model eliminates the painful process of agent deployment and takes advantage of single click deployment of cloud native security services. Once activated, FortiCNP ingests findings from these services, correlates them, and presents you with actionable insights. Some of the integrated services include:

- Vulnerability Assessment Services
- Entitlement Management Services
- Threat Detection Services
- Data Scanning and Classification Services
- Fortinet Security Fabric (FortiGate, FortiWeb)

The following table provides a summary of the capabilities:

<table>
<thead>
<tr>
<th>FEATURE</th>
<th>DESCRIPTION</th>
<th>INTEGRATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerability Management</td>
<td>FortiCNP analyzes the impact of vulnerabilities against your cloud resources to assess risk.</td>
<td>Microsoft Defender for Cloud, Amazon Inspector, Amazon GuardDuty, VPC Flow Logs, CloudTrail</td>
</tr>
<tr>
<td>Threat Detection</td>
<td>FortiCNP ingests information from Cloud Native security services and Fortinet products for Workload and Network threat detection findings.</td>
<td>Microsoft Defender for Cloud, NSG Flow Logs</td>
</tr>
<tr>
<td>Entitlement Management</td>
<td>FortiCNP incorporates permission information to correlate the impact of risk across different resources.</td>
<td></td>
</tr>
<tr>
<td>Data Security</td>
<td>FortiCNP scans for malware in data and utilizes data classification information from cloud native tools to evaluate the impact of security risk on or from your data.</td>
<td>Amazon S3, Azure Blob, GCP Cloud Storage</td>
</tr>
<tr>
<td>Kubernetes Security</td>
<td>FortiCNP integrates with Kubernetes Environments to scan configuration and monitor traffic flows.</td>
<td>Amazon EKS, Azure AKS, Google Kubernetes Engine, Self-Managed Kubernetes</td>
</tr>
</tbody>
</table>

\(^1\) Disk volume and workload image scanning to be available in next release
### FEATURE DESCRIPTION

**Container Registries**
FortiCNP Scans container registries for vulnerabilities allowing DevOps teams to pass or fail build pipelines based on scan results.

**Ticketing & CI/CD Integration**
FortiCNP allows security analysts to interact with other teams in the ways that are most natural to the organization.

**Reports**
FortiCNP provides point in time risk snapshot and compliance reports to non-FortiCNP users.

<table>
<thead>
<tr>
<th>Resource Risk Insights (VM, Container, Storage, Database)</th>
<th>Integration w/ Public Cloud Security Services</th>
<th>Threat Insights</th>
<th>Ticketing</th>
<th>Kubernetes Configuration Assessment &amp; Visibility</th>
<th>CI/CD Pipeline Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>FCX-XX-FCWPW-XXX-XX</td>
<td>FCX-XX-FCWPS-XXX-XX</td>
<td>FCX-XX-FCWPC-XXX-XX</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### PRICING - BYOL

<table>
<thead>
<tr>
<th>Cloud Native Protection</th>
<th>Data Protection</th>
<th>Container Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC1-10-FCWPW-315-02-DD*</td>
<td>FC2-10-FCWPW-315-02-DD*</td>
<td>FC1-10-FCWPC-327-02-DD*</td>
</tr>
<tr>
<td>FortiCNP Cloud Native protection – Risk, Threat and Data insights for 20 resources in all supported public cloud environments.</td>
<td>FortiCNP Cloud Native protection – Risk, Threat and Data insights for 100 resources in all supported public cloud environments.</td>
<td>FortiCNP Container Protection. Subscription per 4 container hosts/worker nodes.</td>
</tr>
<tr>
<td>FC2-10-FCWPW-316-02-DD*</td>
<td>FC2-10-FCWPS-317-02-DD*</td>
<td></td>
</tr>
<tr>
<td>FC5-10-FCWPS-316-02-DD</td>
<td>FC5-10-FCWPS-317-02-DD*</td>
<td></td>
</tr>
</tbody>
</table>

### PRICING – AWS MARKETPLACE

<table>
<thead>
<tr>
<th>Base monthly subscription</th>
<th>Minimal subscription protecting 20 workloads and scans up-to 100GB of data for malware.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monthly Protected Cloud Resources</td>
<td>Additional protected resources that were protected during the month using highest watermark metering. Increments of 1</td>
</tr>
<tr>
<td>Base Annual Subscription</td>
<td>Minimal subscription protecting 100 workloads and scans up-to 1TB of data for malware.</td>
</tr>
<tr>
<td>Annual Protected Cloud Resources</td>
<td>Allocation of additional protected resources for the year. Increments of 100</td>
</tr>
<tr>
<td>Scanned Data</td>
<td>Volume of data scanning capacity beyond the first 1TB. Increments of 10TB</td>
</tr>
<tr>
<td>Overage</td>
<td>Any exceeded capacity for protected workloads or data scanning charged per monthly prices</td>
</tr>
</tbody>
</table>

---

**Container Registries**
- Amazon ECR
- Azure Container Registry
- Google Container Registry
- Harbor Container Registry
- OpenShift Container Registry

**Ticketing & CI/CD Integration**
- JIRA
- ServiceNow
- Jenkins

---

**Reports**
- FCX-XX-FCWPW-XXX-XX
- FCX-XX-FCWPS-XXX-XX
- FCX-XX-FCWPC-XXX-XX

**Resource Risk Insights (VM, Container, Storage, Database)**

**Integration w/ Public Cloud Security Services**

**Threat Insights**

**Ticketing**

**Kubernetes Configuration Assessment & Visibility**

**CI/CD Pipeline Integration**

---

**Pricing - BYOL**

**Cloud Native Protection**
- FC1-10-FCWPW-315-02-DD*
  - FortiCNP Cloud Native protection – Risk, Threat and Data insights for 20 resources in all supported public cloud environments.
- FC2-10-FCWPW-315-02-DD*
  - FortiCNP Cloud Native protection – Risk, Threat and Data insights for 100 resources in all supported public cloud environments.
- FC1-10-FCWPC-327-02-DD*
  - FortiCNP Container Protection. Subscription per 4 container hosts/worker nodes.

**Data Protection**
- FC2-10-FCWPS-316-02-DD*
- FC2-10-FCWPS-317-02-DD*
  - FortiCNP Data Protection Advanced (Standard plus DLP scanning) – License for pattern-matching (DLP), malware and anti-virus scanning of 100GB of data. Requires FortiCNP protected resource license. Cannot be combined with FortiCNP Data Protection, Standard.
- FC5-10-FCWPS-316-02-DD*
- FC5-10-FCWPS-317-02-DD*
  - FortiCNP Data Protection Advanced (Standard plus DLP scanning) – License for pattern-matching (DLP), malware and anti-virus scanning of 1TB of data. Requires FortiCNP protected resource license. Cannot be combined with FortiCNP Data Protection, Standard.

---

**Pricing – AWS Marketplace**

**Base monthly subscription**
- Minimal subscription protecting 20 workloads and scans up-to 100GB of data for malware.

**Monthly Protected Cloud Resources**
- Additional protected resources that were protected during the month using highest watermark metering. Increments of 1

**Base Annual Subscription**
- Minimal subscription protecting 100 workloads and scans up-to 1TB of data for malware.

**Annual Protected Cloud Resources**
- Allocation of additional protected resources for the year. Increments of 100

**Scanned Data**
- Volume of data scanning capacity beyond the first 1TB. Increments of 10TB

**Overage**
- Any exceeded capacity for protected workloads or data scanning charged per monthly prices

---

**Ordering Guide**

**Cloud-Native Application Protection Platform**

---

**Footnotes**

- © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare®, and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet’s General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet’s internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant thereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.