

DATA SHEET

# FortiCNP for AWS

Available in:



Cloud

## Prioritize Risk Management Activities

The rapid adoption of cloud computing is causing security teams to operate in a reactive state to provide adequate security coverage for the increasing volume of cloud workloads. This situation means teams are unable to handle the volume of alerts created by the large amount of acquired security tools.

FortiCNP, Fortinet's cloud-native protection product, helps security teams prioritize risk management activities based on a broad set of security signals from their AWS environments. Beyond the built-in CSPM and data scanning capabilities, FortiCNP collects information from AWS 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 the insights that FortiCNP produces.

Unlike traditional CSPM and CWPP products that require agents, excessive permissions, and produce unmanageable volumes of data, FortiCNP provides deep security visibility across cloud infrastructures and helps prioritize security workflows for effective risk management.

### Key Features

- Cloud Risk Prioritization
- Vulnerability Management
- Cloud Security Posture Management
- Malware Scanning
- Deep AWS Integrations
- Workflow Integration

### Key Benefits

- Reduce time to identify, triage, and prioritize cloud risk remediation work
- Maximize the value of AWS security services and Fortinet cloud security products

## FEATURE HIGHLIGHTS

### Resource Risk Insights

Fortinet's patent-pending Resource Risk Insights (RRI) technology turns overwhelming volumes of data into actionable insights. By correlating information from a breadth of AWS and Fortinet security solutions into a comprehensive cloud risk graph database, FortiCNP creates a current and accurate map of risk interdependencies for your AWS 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.

*"FortiCNP gives us comprehensive cloud visibility with an intuitive dashboard that allows us to easily track risk management over time," said Caio Hyppolito, CTO at BK Bank. "Most importantly, it enables our team to focus on securing high priority resources instead of spending time working through long lists of security findings. Integrations with the products we already have allow us to get even more value out of our deployment and enables broader visibility and easier, more proactive cloud security management."*

### Malware Scanning

FortiCNP's malware scanning feature utilizes Fortiguard Labs technology across all data stores in your AWS 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<sup>1</sup>.

### Cloud Native Integration

FortiCNP's RRI technology allows you to enjoy the ease of single-click deployment offered by AWS security services, without the associated alert fatigue. 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
- Threat Detection Services
- Data Scanning and Classification Services
- Fortinet Security Fabric (FortiGate, FortiWeb)

*"Deploying multiple third party tools in the cloud can be an endless task – utilizing the cloud native tools while rationalizing their output, and correlating it with security information we get from other Fortinet products saves us time and delivers results..."*

Roger Rustad, Security Engineer, Fortinet CISO Office.

### Related Products

The following AWS services provide FortiCNP security findings to make insights more accurate.

- Amazon GuardDuty
- AWS Security Hub
- Amazon Inspector
- FortiGate-VM
- FortiWeb Cloud

### Additional Information

To learn more and activate your free trial, please visit [AWS Marketplace](#)

<sup>1</sup>. Disk volume and workload image scanning to be available in next release.



## TECHNICAL SPECIFICATIONS

FEATURES		
	DESCRIPTION	INTEGRATIONS
<b>Cloud Security Posture Management</b>	FortiCNP scans and monitors customer cloud configurations to evaluate best practices and detect misconfiguration risk.	AWS Security Hub
<b>Vulnerability Management</b>	FortiCNP analyzes the impact of vulnerabilities against your cloud resources to assess risk.	Amazon Inspector
<b>Threat Detection</b>	FortiCNP ingests information from AWS security services and Fortinet products for workload and network threat detection findings.	Amazon GuardDuty AWS VPC Flow Logs AWS CloudTrail
<b>Entitlement Management</b>	FortiCNP incorporates permission information to correlate the impact of risk across different resources.	
<b>Data Security</b>	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.	Amazon S3
<b>Kubernetes Security</b>	FortiCNP integrates with Kubernetes environments to scan configuration and monitor traffic flows.	Amazon EKS Self-Managed Kubernetes
<b>Container Registries</b>	FortiCNP Scans container registries for vulnerabilities allowing DevOps teams to pass or fail build pipelines based on scan results.	Amazon ECR
<b>Ticketing and Ci/CD Integration</b>	FortiCNP allows security analysts to interact with other teams in the ways that are most natural to the organization.	JIRA ServiceNow Jenkins
<b>Reports</b>	FortiCNP provides point in time risk snapshot and compliance reports to non FortiCNP users.	
AWS SERVICE INTEGRATION DESCRIPTION		
<b>AWS Resource API</b>	The AWS Resource API is used to collect information regarding your cloud resources in a read-only manner.	
<b>AWS Organizations</b>	AWS organizations are used to import environments that include more than a single AWS account and are organized using the AWS organizations feature.	
<b>AWS CloudTrail</b>	FortiCNP ingests AWS CloudTrail events to identify changes to your environment.	
<b>AWS VPC Flow Logs</b>	AWS VPC Flow logs are used to establish traffic patterns in your environment as well as detect deviations from normal patterns.	
<b>AWS Security Hub</b>	AWS Security Hub is used to collect all security information from AWS services such as Amazon GuardDuty, Amazon Inspector and others. FortiCNP utilizes the finding normalization and aggregation capabilities of AWS Security Hub. AWS Security Hub controls are not used by FortiCNP.	
<b>Amazon GuardDuty</b>	GuardDuty Threat Detection Service is used by FortiCNP to cross correlate risk with imminent threats and prioritize.	
<b>Amazon Inspector</b>	Inspector Vulnerabilities are used to establish package, library and network configuration vulnerability risk.	



## ORDER INFORMATION

PRODUCT	SKU	DESCRIPTION
<b>BRING YOUR OWN LICENSE (BYOL)</b>		
<b>Cloud Native Protection</b>	FC1-10-FCWPW-315-02-DD*	FortiCNP Cloud-native Protection – Risk, Threat and Data insights for 20 resources.
	FC2-10-FCWPW-315-02-DD*	FortiCNP Cloud-native Protection – Risk, Threat and Data insights for 100 resources.
<b>Data Protection</b>	FC2-10-FCWPS-316-02-DD*	FortiCNP Data Protection Standard. License for malware and anti-virus scanning of 100GB of data. Requires FortiCNP protected resource license. Cannot be combined with FortiCNP Data Protection Advanced.
	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	FortiCNP Data Protection Standard. License for malware and anti-virus scanning of 1TB of data. Requires FortiCNP protected resource license. Cannot be combined with FortiCNP Data Protection Advanced.
	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.
<b>Container Protection</b>	FC1-10-FCWPC-327-02-DD*	FortiCNP Container Protection. Subscription per 4 container hosts/worker nodes.
<b>AWS MARKETPLACE</b>		
<b>Monthly</b>	Base monthly subscription	Minimal subscription protecting 20 workloads and scans up-to 100GB of data for malware.
	Protected Cloud Resources	Additional protected resources that were protected during the month using highest watermark metering. Increments of 1
	Scanned Data	Volume of data that has been scanned for the month beyond the first 100GB. Increments of 1
<b>Annual</b>	Base Annual Subscription	Minimal subscription protecting 100 workloads and scans up-to 1TB of data for malware.
	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

\* Denotes TBA



www.fortinet.com

Copyright © 2022 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 hereto, 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.

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA (<https://www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf>) and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy ([https://secure.ethicspoint.com/domain/media/en/gui/19775/Whistleblower\\_Policy.pdf](https://secure.ethicspoint.com/domain/media/en/gui/19775/Whistleblower_Policy.pdf)).