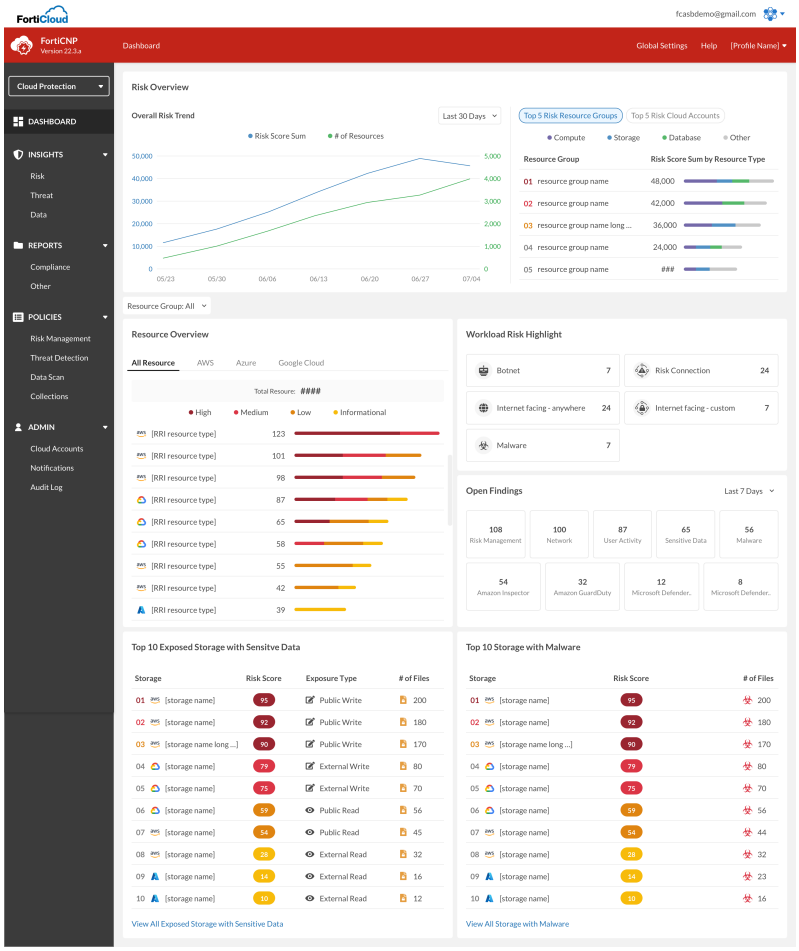
ORDERING GUIDE

Cloud-Native Application Protection Platform

Security Operations for Cloud Infrastructures

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:

FEATURE	DESCRIPTION	INTEGRATIONS
Cloud Security Posture Management	FortiCNP scans and monitors customer cloud configurations to evaluate best practices and detect misconfiguration risk.	AWS Security Hub Azure Security Center GCP Security Health Analytics
Vulnerability Management	FortiCNP analyzes the impact of vulnerabilities against your cloud resources to assess risk	Amazon Inspector Microsoft Defender for Cloud
Threat Detection	FortiCNP ingests information from Cloud Native security services and Fortinet products for Workload and Network threat detection findings.	Amazon GuardDuty, VPC Flow Logs, CloudTrail Microsoft Defender for Cloud, NSG Flow Logs
Entitlement Management	FortiCNP incorporates permission information to correlate the impact of risk across different resources	
Data Security	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 Azure Blob GCP Cloud Storage
Kubernetes Security	FortiCNP integrates with Kubernetes Environments to scan configuration and monitor traffic flows	Amazon EKS Azure AKS Google Kubernetes Engine Self-Managed Kubernetes

1 Disk volume and workload image scanning to be available in next release

FEATURE	DESCRIPTION	INTEGRATIONS
Container Registries	FortiCNP Scans container registries for vulnerabilities allowing DevOps teams to pass or fail build pipelines based on scan results.	Amazon ECR Azure Container Registry Google Container Registry Harbor Container Registry OpenShift Container Registry Docker Hub
Ticketing & Ci/CD Integration	FortiCNP allows security analysts to interact with other teams in the ways that are most natural to the organization	JIRA ServiceNow Jenkins
Reports	FortiCNP provides point in time risk snapshot and compliance reports to non FortiCNP users.	

	FCX-XX-FCWPW-XXX-XX-XX	FCX-XX-FCWPS-XXX-XX-XX	FCX-XX-FCWPC-XXX-XX-XX
Resource Risk Insights (VM, Container, Storage, Database)	✓		
Integration w/ Public Cloud Security Services	✓		
Threat Insights	✓		
Ticketing	✓		
Data Protection Insights (Malware)		✓	
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.
Data Protection	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.
Container Protection	FC1-10-FCWPC-327-02-DD*	FortiCNP Container Protection. Subscription per 4 container hosts/worker nodes.

PRICING – AWS MARKETPLACE		
Monthly	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
Annual	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

FORTINET

www.fortinet.com