Understanding Threat Detection and Response Capabilities in a CNAPP

How FortiCNP leverages the Fortinet Security Fabric and AWS security services to enable threat protection in AWS environments

Table of Contents

Introduction 3

Cloud-native Threat Detection and Response Through the Lens of the Fortinet Security Fabric 4

Gaining Actionable Insights with FortiCNP 5

The Benefits of Using FortiCNP to Detect and Respond to Threats 8

Conclusion 9

Introduction

Protecting the services and networks that support cloud-driven organizations differs from that offered by legacy security architectures. A Cloud-native Application Protection Platform (CNAPP) can help. As a centralized, integrated risk management platform, it is designed to remove the complexity of meeting the security demands of cloud environments and applications. Security tools and cloud services provide the visibility needed to:

- Detect and respond to threats across the entire cyber landscape.
- Identify potential security risks in an application's source code.
- Deliver insights on an organization's security posture.
- Implement and automate security earlier in the application lifecycle across public and private cloud infrastructures.

To mitigate potential attack vectors effectively, a CNAPP requires an integrated, elastic security architecture that addresses an expanded threat landscape and adapts to changes across cloud environments. The Fortinet Security Fabric can deliver that infrastructure, along with the capabilities needed for a CNAPP.

The Security Fabric can detect, monitor, block, and remediate attacks across the entire attack surface. Using security findings or real-time threat events from FortiGate firewalls and other Fortinet solutions, the Fabric delivers broad protection and visibility into every network segment and device. With its visibility and observability capabilities, it is possible to detect and respond to threats all across a cloud-first network landscape.

This ebook explores how cloud security solutions within the Fortinet Security Fabric, such as FortiCNP and FortiGate, and AWS can enable threat detection and response in a CNAPP.

Cloud-native Threat Detection and Response Through the Lens of the Fortinet Security Fabric

The Fortinet Security Fabric integrates FortiGuard AI-powered security, secure networking, Zero Trust access, cloud security, and Fortinet Fabric Management so it can mitigate security risk, improve protection, and reduce complexity. Its threat intelligence, data correlation, automation, AI, machine learning, and container protection capabilities interoperate and respond to threats as a single, coordinated system.

Three key attributes enable the Fortinet Security Fabric to provide comprehensive real-time cybersecurity protection from users to applications:

Broad

Converged networking and security offerings across endpoints, networks, and clouds enable organizations to detect threats and enforce security everywhere.

Integrated

The integration of industry-leading security technology, AI-powered analysis, and automated prevention enable organizations to close security gaps and reduce complexity.

Automated

A context-aware, self-healing network and security posture enable faster time-to-prevention and efficient operations.

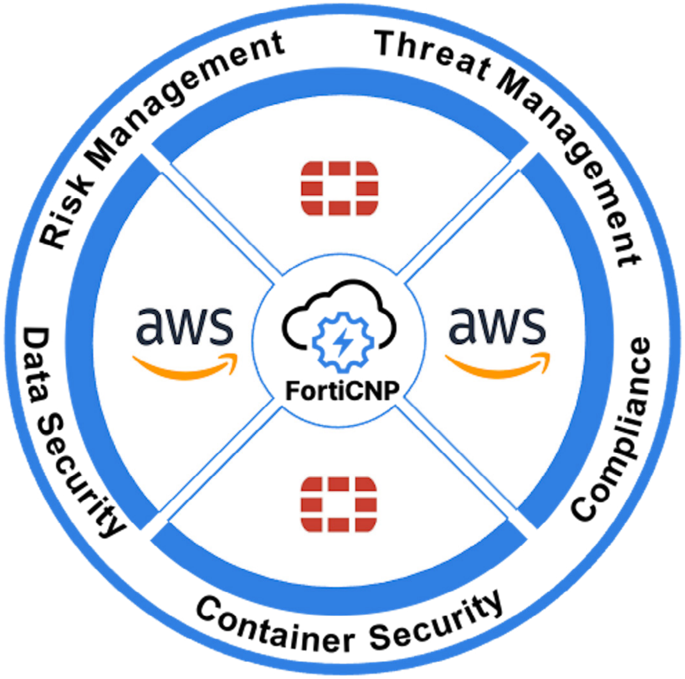
One operating system drives the Fortinet Security Fabric, enabling it to deliver solutions and products more easily than other platforms for a range of key pillars. These include network operations, security operations, Zero Trust access, threat intelligence, cloud security, network security, and open ecosystems.

One of the solutions in the Fortinet Security Fabric, FortiCNP, provides broad visibility across your cloud environments, enabling the threat detection and response that CNAPPs need.

Gaining Actionable Threat Insights with FortiCNP

A CNAPP integrates multiple security solutions so your teams can experience a bird's eye view of their cloud security posture. Then, they can detect and respond to threats based on correlated security events that present the highest risk to your organization. That's where FortiCNP shines.

FortiCNP integrates with AWS cloud-native security services, Fortinet Security Fabric products, and FortiGuard Labs to provide risk management, threat management, compliance, container security, and data security. As a result, it can correlate and contextualize security alerts and findings into actionable insights. These insights are used to detect and respond to threats.

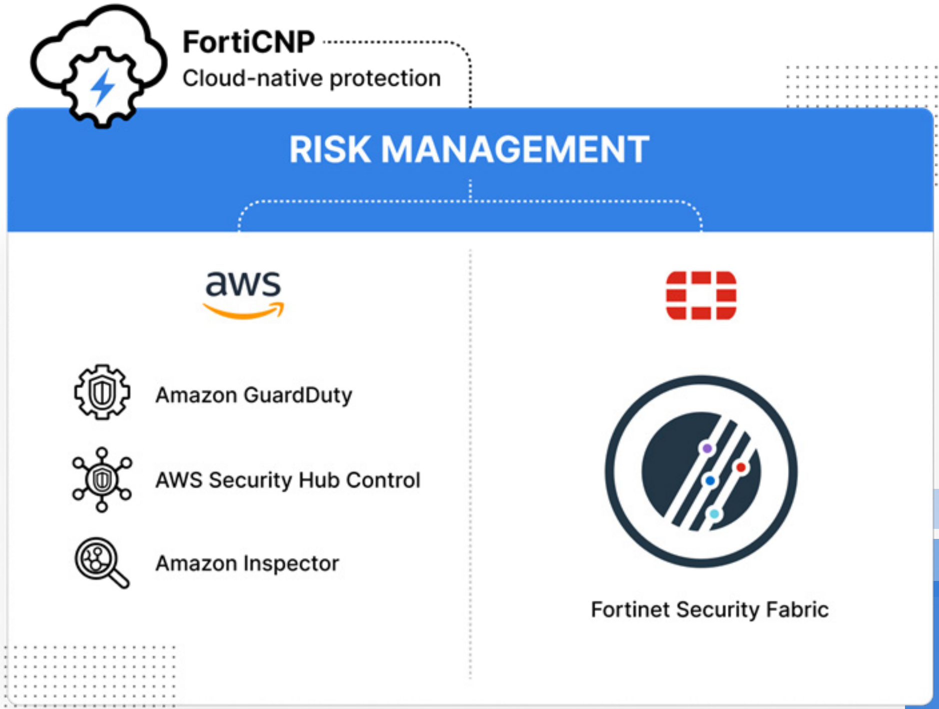


Collecting Cloud-first Security Data for Actionable Insights

FortiCNP provides comprehensive visibility based on security signals from the Fortinet Security Fabric or FortiGuard and their cloud environments. It integrates with multiple AWS security services and Fortinet Security Fabric solutions to collect, normalize, and analyze their data:

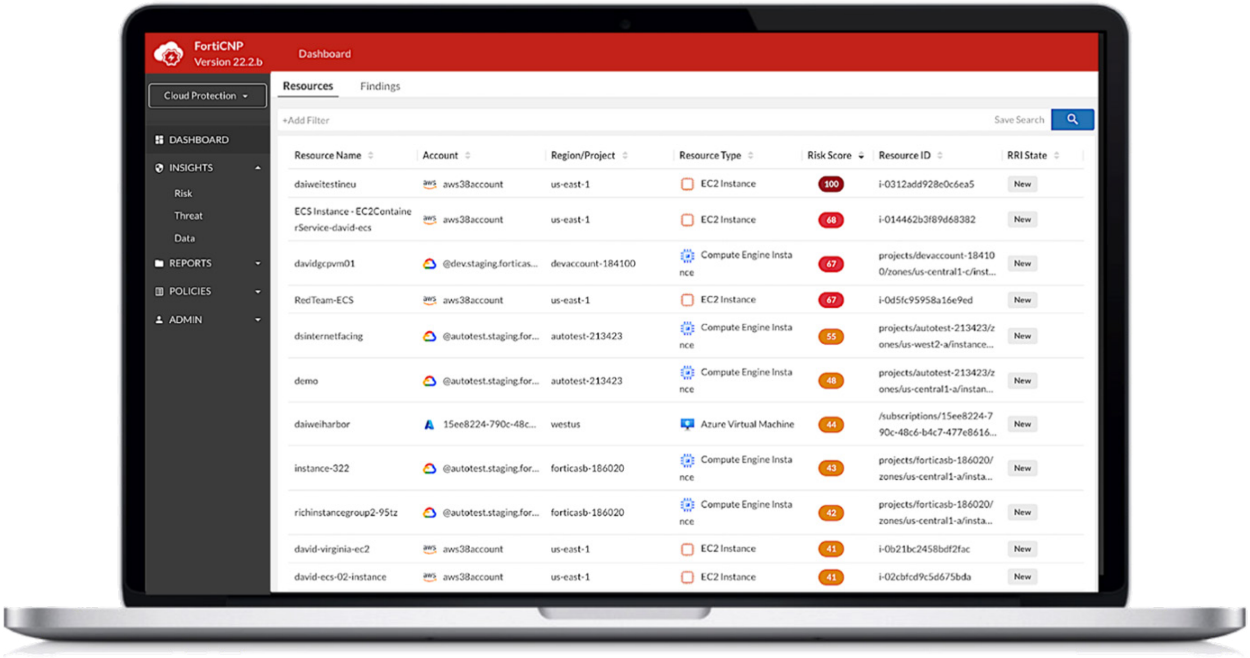
- **Amazon Inspector:** scans workloads for vulnerabilities and open network exposure to help operationalize security throughout the resource lifecycle.
- **AWS Security Hub:** collects security data from across AWS accounts, services, and supported third-party partner products to identify security issues.
- **Amazon GuardDuty:** identifies suspicious traffic and API activity in AWS environments.
- **IaC template scanning:** looks for misconfigurations and exposed secrets across the development lifecycle.
- **FortiGate events and logs and FortiGuard IPS rules:** provides a wealth of information about traffic across cloud environments and networks.

Using that data, FortiCNP calculates an aggregate risk score for threats to cloud resources that helps teams determine which to respond to and when.



What’s the RRI? Threat Analytics Visualized

FortiCNP also produces Resource Risk Insights™ (RRI), that enable you to see where issues or incidents might need addressing. An RRI is a current and accurate map of risk interdependencies for your cloud environment. You can also customize an RRI based on environmental and workload specific attributes to best suit your environment.



Resource Name	Account	Region/Project	Resource Type	Risk Score	Resource ID	RRI State
daiweitestineu	aws aws38account	us-east-1	EC2 Instance	100	i-0312add928e0c6ea5	New
ECS Instance - EC2ContainerService-david-ecs	aws aws38account	us-east-1	EC2 Instance	68	i-014462b3f89d68382	New
davidgcpvm01	@dev.staging.forticas...	devaccount-184100	Compute Engine Instance	67	projects/devaccount-184100/zones/us-central1-c/inst...	New
RedTeam-ECS	aws aws38account	us-east-1	EC2 Instance	67	i-0d5fc95958a16e9ed	New
dsinternetfacing	@autotest.staging.for...	autotest-213423	Compute Engine Instance	55	projects/autotest-213423/zones/us-west2-a/instance...	New
demo	@autotest.staging.for...	autotest-213423	Compute Engine Instance	48	projects/autotest-213423/zones/us-central1-a/instan...	New
daiweiharbor	15ee8224-790c-48c...	westus	Azure Virtual Machine	44	/subscriptions/15ee8224-790c-48c6-b4c7-477e8616...	New
instance-322	@autotest.staging.for...	forticasb-186020	Compute Engine Instance	43	projects/forticasb-186020/zones/us-central1-a/insta...	New
richinstancegroup2-95tz	@autotest.staging.for...	forticasb-186020	Compute Engine Instance	42	projects/forticasb-186020/zones/us-central1-a/insta...	New
david-virginia-ec2	aws aws38account	us-east-1	EC2 Instance	41	i-0b21bc2458bdf2fac	New
david-ecs-02-instance	aws aws38account	us-east-1	EC2 Instance	41	i-02cbfcd9c5d675bda	New

> “FortiCNP gives us comprehensive cloud visibility. An intuitive dashboard allows us to easily track risk management over time. “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 allow broader visibility and easier, more proactive cloud security management.”
>
> —Caio Hyppolito, CTO, BK Bank.

The Benefits of Using FortiCNP to Detect and Respond to Threats

FortCNP is not like traditional cloud security posture management and cloud workload protection platform products. Those products require agents, excessive permissions, and other tools to harness insights from massive volumes of data. FortiCNP eliminates the painful process of agent deployment. In a single click, you can deploy cloud-native security services to respond to threats to your data, networks, and workloads.

Data Security

It's no secret that you need to protect the data in your applications, Amazon Simple Storage Services (Amazon S3) buckets, files sent across the cloud, and development environments. FortiCNP analyzes configurations, files, and documents in cloud storage services to help you detect misconfigurations, sensitive data, and potential malware. It also enforces policies to analyze sensitive data activity and investigate data leakage across your cloud environments.

Network Protection

The data that FortiCNP collects and transforms into insights from FortiGate events and logs, FortiGuard IPS rules, and Amazon Inspector can help you discover network threats. As a result, you can protect east-west traffic and eliminate network disruptions. Because anomalous activity can occur once beyond the firewall, integrated threat intelligence can help you understand what that looks like and protect the network.

Workload Protection

Access control is the key to protecting workloads. FortiCNP can provide visibility into data loss, behavioral anomalies, and misconfigurations from IAC template scans, container security and permissions logs, and more. As a result, you can detect threats, vulnerabilities, and open ports even for a configuration you have just set up. But FortiCNP doesn't stop there. It can continuously monitor risk posture and activity for new and evolving threats.

Conclusion

Comprehensive visibility into potential threats that supports response is critical to the effectiveness of a CNAPP. The Fortinet Security Fabric provides integrated cloud security capabilities that collect information from multiple security services, such as vulnerability scanning, permissions analysis, and threat detection.

An integral part of the Fortinet Security Fabric, FortiCNP correlates and contextualizes security alerts and findings from Fortinet and AWS solutions to analyze cloud risk. Cloud resources are then prioritized based on the highest risk. Finally, RRI provides actionable insights with consistent workflows to help security teams to detect and respond to threats.

For more information, visit: aws.forticnp.com/free-trial

FORTINET®

January 2023