SOLUTION BRIEF

FortiCNP Manages Cloud-Native Risk Through Actionable Insights

Executive Summary

Nearly all organizations have adopted the cloud to modernize their operations, enable rapid innovation, and accelerate growth, and there are no signs of this slowing down. Gartner estimates that by 2025, over 95% of new digital workloads will be deployed on cloud-native platforms.[1]

But as more organizations move their critical workloads into the cloud, this has also introduced new risks. Traditional security solutions lack the capabilities to adequately respond to the risks. And adding new point-product security solutions to their overall infrastructure often results in a fragmented security architecture, making any kind of management challenging and increasing risk.

FortiCNP Risk Management Capabilities

- Maximizes the value of cloud-native security tools
- Prioritizes remediation actions based on high-risk resources
- Streamlines risk management and remediation processes

Cloud Workloads Require a Cloud-Native Security Solution

Modern digital business applications and services are composed of multiple workloads. These workloads can be highly complex and may be deployed across hybrid and multi-cloud environments. To protect these workloads against an evolving and expanded threat landscape, cloud security must be able to scale across all environments and multiple threat vectors in the technology stack while keeping pace with the changes within the cloud.

FortiCNP is Fortinet's cloud-native application protection platform (CNAPP) that integrates security capabilities for cloud security posture management (CSPM), cloud workload protection platform (CWPP), and other security solutions aimed to protect cloud-native applications to provide a friction-free approach to managing cloud risk across cloud resources and environments.

FortiCNP simplifies cloud security so organizations can quickly operationalize their defenses to manage risk. Fortinet's innovative approach helps address some of the challenges often associated with security solutions, as well as some of the barriers to cloud adoption.

Fragmented Security Solutions Can Weaken Security Posture

In today's rapidly evolving IT environment, organizations will continue to invest in new and innovative security solutions to counter new risks. The challenge is that many of these point solutions are not integrated, so with each new solution added, an organization's security infrastructure becomes increasingly complex and fragmented. A recent study showed that 59% of enterprise organizations have more than 50 separate security tools deployed, with security teams using most of them to investigate and respond to a typical security incident.[2]

Having too many disparate security tools is counter-effective and can expose organizations to increased risks. And not only does this result in increased costs to manage and update, but solutions with different features, management tools, and interfaces can lead to fragmented visibility. This makes it even harder for organizations to identify higher priority risks from vulnerabilities, sensitive information, misconfigurations, sophisticated attacks, and resource risk in distributed environments, which ultimately leads to insufficient security coverage.

Alert Fatigue Inhibits Proactive Risk Management

As organizations proactively enhance their solutions to achieve better security coverage and strengthen their defenses, they often underestimate the volume of security notifications that are generated by each security solution. And in some cases, security solutions can trigger thousands of notifications daily, which many organizations are not equipped to prioritize and manage.

What's more, many of the notifications lack the context needed to prioritize the mitigation efforts, so this places the responsibility on security teams to manually research and investigate each alert. This manual process makes it increasingly difficult to manage risk and address security needs quickly. Because of this, over 80% of security analysts suffer from alert fatigue.[3] Furthermore, a recent survey found that more than one-third of security analysts end up ignoring security alerts when their queue gets too full.[4]

Proactive risk management is one of the primary responsibilities of CISOs. And this can be achieved by implementing effective cloud-native security solutions to manage and mitigate risk. But if the security teams are overburdened with the volume of data to investigate or are ignoring them altogether, this can jeopardize an organization's security. Missing just one alert can distinguish between securing an organization from a critical risk or causing a widespread security breach that impacts customers and damages an organization's brand and can bring large regulatory fines.

Managing Cloud Risks with Resource Risk Insights (RRI)

FortiCNP helps security teams proactively manage cloud risks by consolidating the volume of security alerts and findings across multiple sources to provide a resource-centric view, with actionable insights for prioritizing critical resources.

FortiCNP Resource Risk Insights (RRI) technology correlates and contextualizes security alerts and findings from the integrated security services and Fortinet Cloud Security solutions across cloud environments to produce an aggregated risk score. This score factors in various aspects that include compliance, vulnerabilities, data attributes, user access and behaviors, in addition to local attributes such as an organization's custom policies. RRI prioritizes resources, making it easy to focus on the critical risks with actionable insights to help security teams take immediate action.

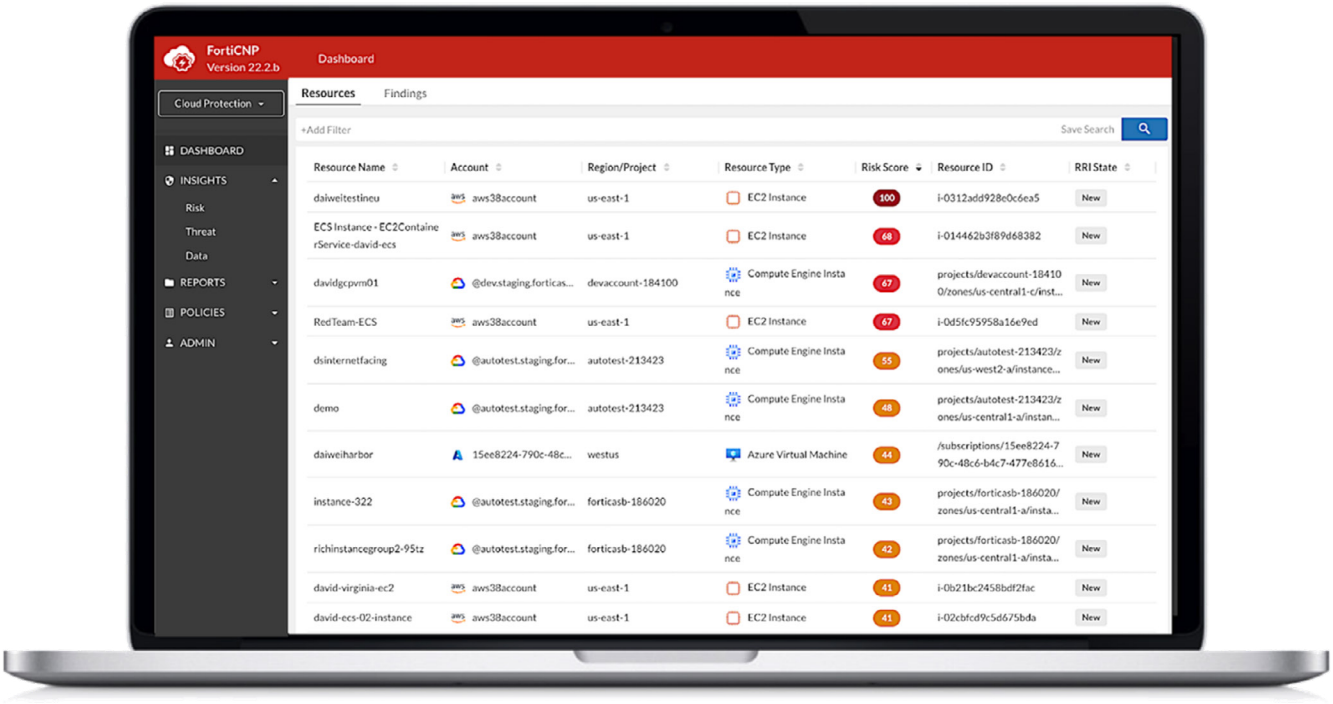

Figure 1: FortiCNP generates context-rich security insights from volumes of security alerts.

Complement the Value of Cloud-Native Security Services

Cloud service providers (CSPs) continue to invest in technologies to secure cloud resources. And many of the CSP security services have become proficient in providing risk, vulnerability, and threat information for compute, storage, and database resources. This is good news considering that 57% of organizations have struggled to find cloud security specialists to manage the increasingly complex threat landscape.[5]

Leveraging a CSP's cloud-native security services can provide many benefits for their customers. They are easy to deploy and have deep integrations across the services and infrastructure for that specific cloud environment. This alleviates the integration challenges that many companies experience in a fragmented security architecture. Additionally, these services provide deep coverage, helping to manage and protect the cloud workloads more effectively.

FortiCNP complements CSP-native security services, as well as Fortinet Security Fabric products, to provide a multilayered approach to managing cloud risks. RRI provides context-rich actionable insights for cloud resources. And actionable alerts allow organizations to prioritize actions based on the severity of the findings and protect the usage of various public cloud resources such as compute instances, containers, database services, and data storage services.

FortiCNP uses each cloud platform's API to gain visibility for the cloud workloads to analyze and prioritize resource risks across cloud environments. To help security teams prioritize the most critical risks, RRI calculates risk and prioritizes the resources with the highest risks, based on their risk score. This enables customers to maximize the value of the security tools without overwhelming security teams with a high volume of security data that is often generated.

Integrations with FortiGuard Labs further enrich FortiCNP insights with real-time traffic and device security information on malicious IP addresses, domains, URLs, and botnets.

CISOs also benefit because FortiCNP helps to accelerate the value of the cloud-native security controls, which are easy for developers to implement, and to recognize the benefits of the Fortinet security solutions implemented. And through the FortiCNP dashboard, CISOs will have visibility into how the organization's security posture improves over time.

Beyond the predefined policies used to manage standards-based and best-practice misconfiguration risk, FortiCNP allows organizations to create custom policies that can evaluate cloud configurations using advanced scripting capabilities.

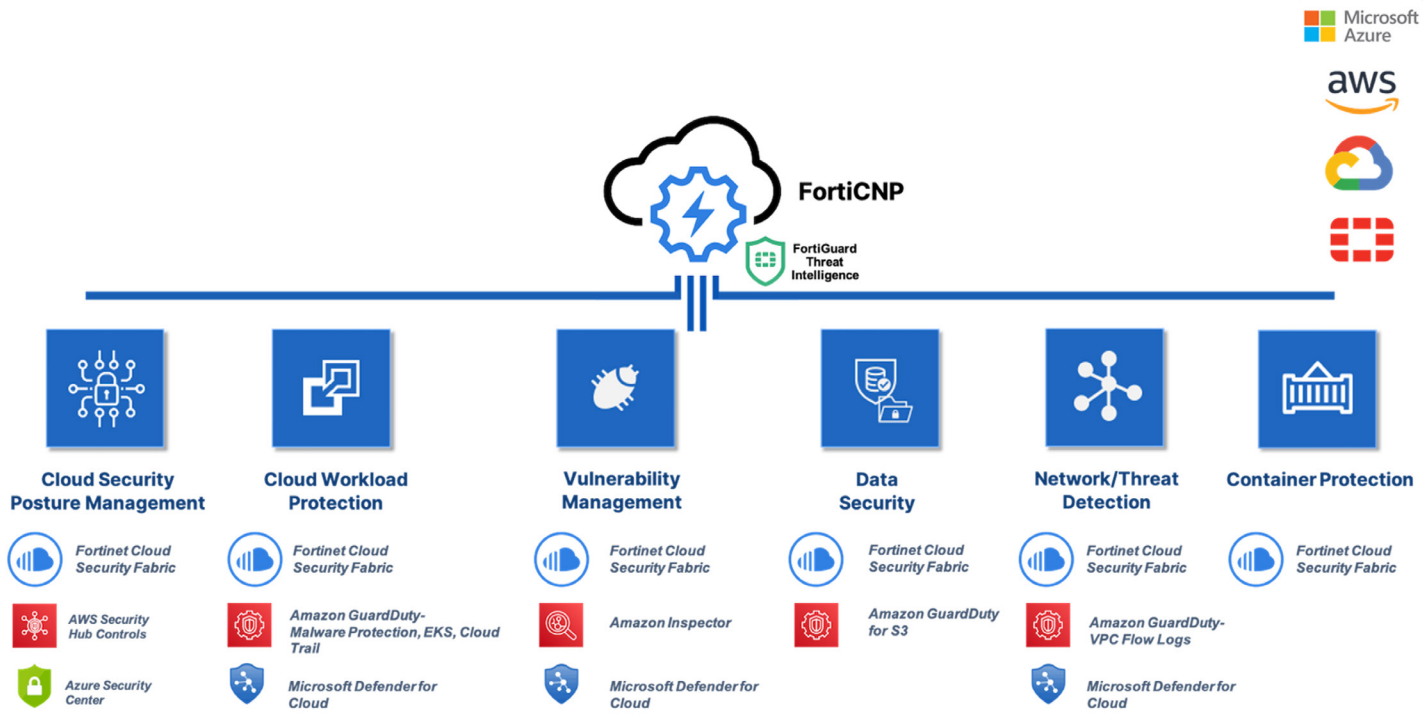

Figure 2: FortiCNP cloud-native security services integrations.

FortiCNP Streamlines Security Operations

For high-priority risk insights, FortiCNP helps streamline the mitigation and remediation process by integrating with digital workflow solutions, such as JIRA and ServiceNow, to automate and manage the process for resource owners to implement critical remediation steps.

Having consistent workflows enabled across multiple clouds helps security teams minimize gaps in security coverage and improve productivity.

Proactive Risk Management

Organizations must evolve their strategies to manage cloud risk proactively. This starts with utilizing cloud-native security services that offer broad and effective security coverage to address risk, vulnerabilities, and threats for compute, storage, and database resources. These services are easy to implement and alleviate the integration challenges many organizations often experience. And by combining the security alerts from these services and Fortinet cloud security products with FortiCNP comprehensive and context-rich RRI technology, organizations can get the most value from their investments while enabling them to focus on high-risk items to manage risk proactively.

[1] "Gartner Says Cloud Will be the Centerpiece of New Digital Experiences," Gartner, November 2021.

[2] "Cyber Resilient Organization 2021," IBM, 2021.

[3] "2020 State of SecOps and Automation Report," Sumo Logic, 2021.

[4] "The Voice of the Analysts," IDC, 2021.

[5] "2022 Cybersecurity Skills Gap," Fortinet, 2022.

www.fortinet.com

October 2022 2:08 PM
1627551-A-0-EN