SOLUTION BRIEF

FortiCNP Manages 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 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. Organizations often react by adding new security solutions to their overall infrastructure, but this ends up resulting 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 containment process

Fragmented Security Solutions Can Weaken Security Posture

In today's rapidly evolving IT environment, organizations will keep investing in new 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 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.

Since many of the notifications lack the context needed to prioritize the mitigation efforts, this puts a burden on security teams to manually research and investigate alerts, making it increasingly difficult to manage risk and address security needs quickly. And 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 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.

Managing Cloud Risks Through Actionable Insights

FortiCNP, Fortinet's cloud-native protection solution, manages cloud risks by correlating alerts and findings from multiple sources to provide actionable insights.

FortiCNP Resource Risk Insights technology replaces the volume of security alerts and findings generated by each cloud security provider's (CSP) native security services and Fortinet Security Fabric products and services with context-rich actionable insights. FortiCNP risk-based prioritization intelligence helps security teams focus on higher-impact risks to address.

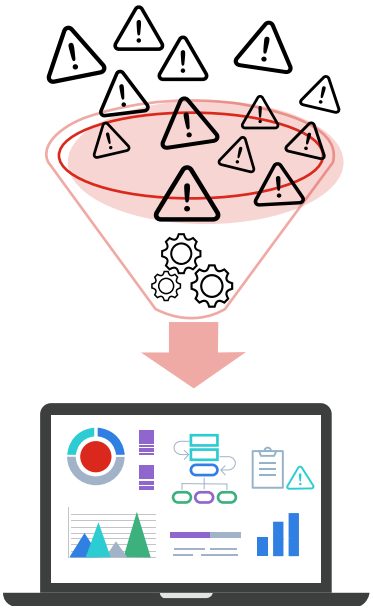

Figure 1: FortiCNP generates context-rich security insights from volumes of security alerts.

Complements the Value of Cloud-native Security Services

CSPs continue to invest in technologies to secure cloud resources. And many of the CSP security services have become efficient 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. These are the easiest 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 greater coverage as they have access to security events that external security solutions don't, 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 multi-layered approach to managing cloud risks. Security findings from the CSP's cloud-native security services, as well as Fortinet security products, are analyzed with FortiCNP Resource Risk Insights (RRI) technology to provide context-rich actionable insights for their cloud resources. Actionable alerts allow organizations to prioritize response based on the severity of issues 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 stack-ranks resources 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 Fortinet Security Fabric products and FortiGuard Labs further enrich FortiCNP insights with real-time traffic and device security information.

This helps increase productivity for security teams by reducing alert fatigue and enables teams to focus on the highest-impact risks. CISOs also benefit because FortiCNP helps to accelerate the value of the cloud-native security controls, which are easiest for developers to implement, and to recognize the benefits of the Fortinet security solutions implemented. CISOs can also generate reports from FortiCNP to show how an organization's security posture improves over time.

Beyond the predefined configuration assessment 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.

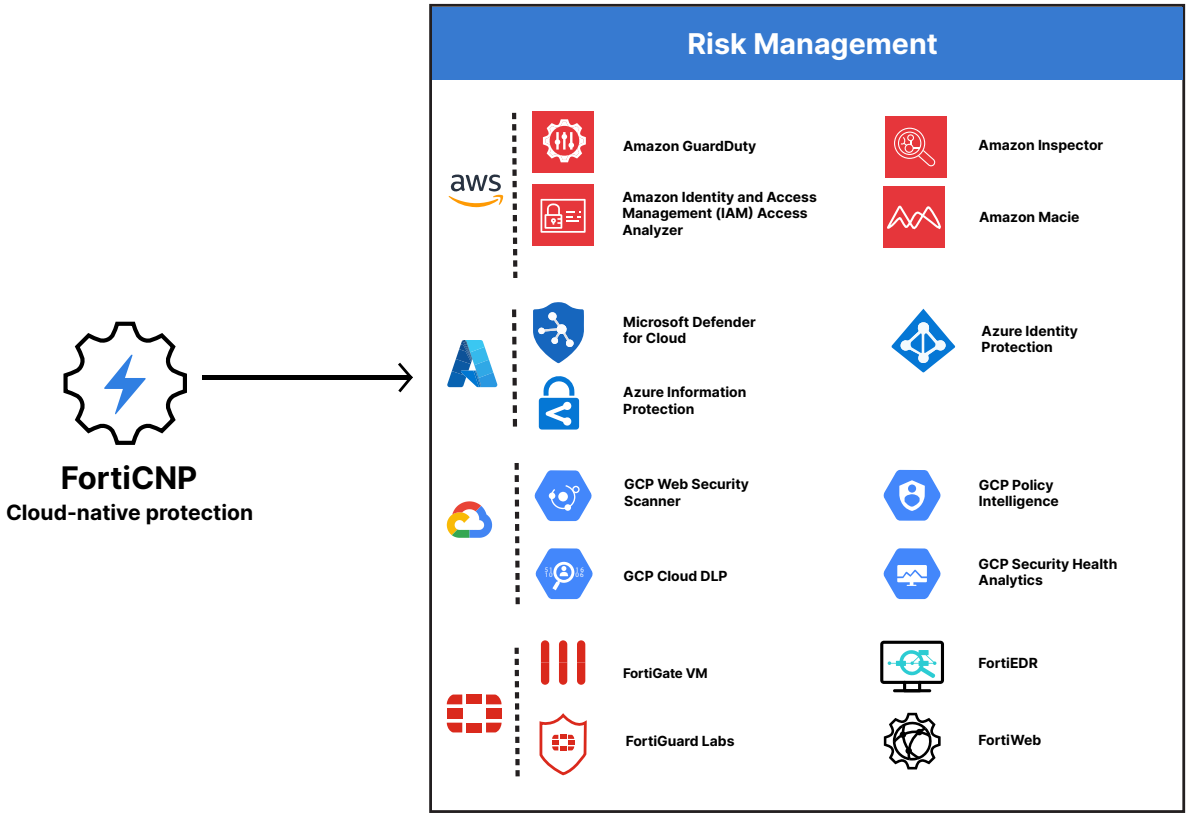

Figure 2: FortiCNP cloud-native security services integrations.

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 customers to address their specific needs.

For fixes that should ultimately be implemented in the CI/CD pipeline, stop-gap solutions can be implemented for cloud environments using Fortinet's cloud security products to protect from threats before the permanent fixes are implemented.

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 the easiest 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.

May 31, 2022 2:08 PM
1627551-0-0-EN