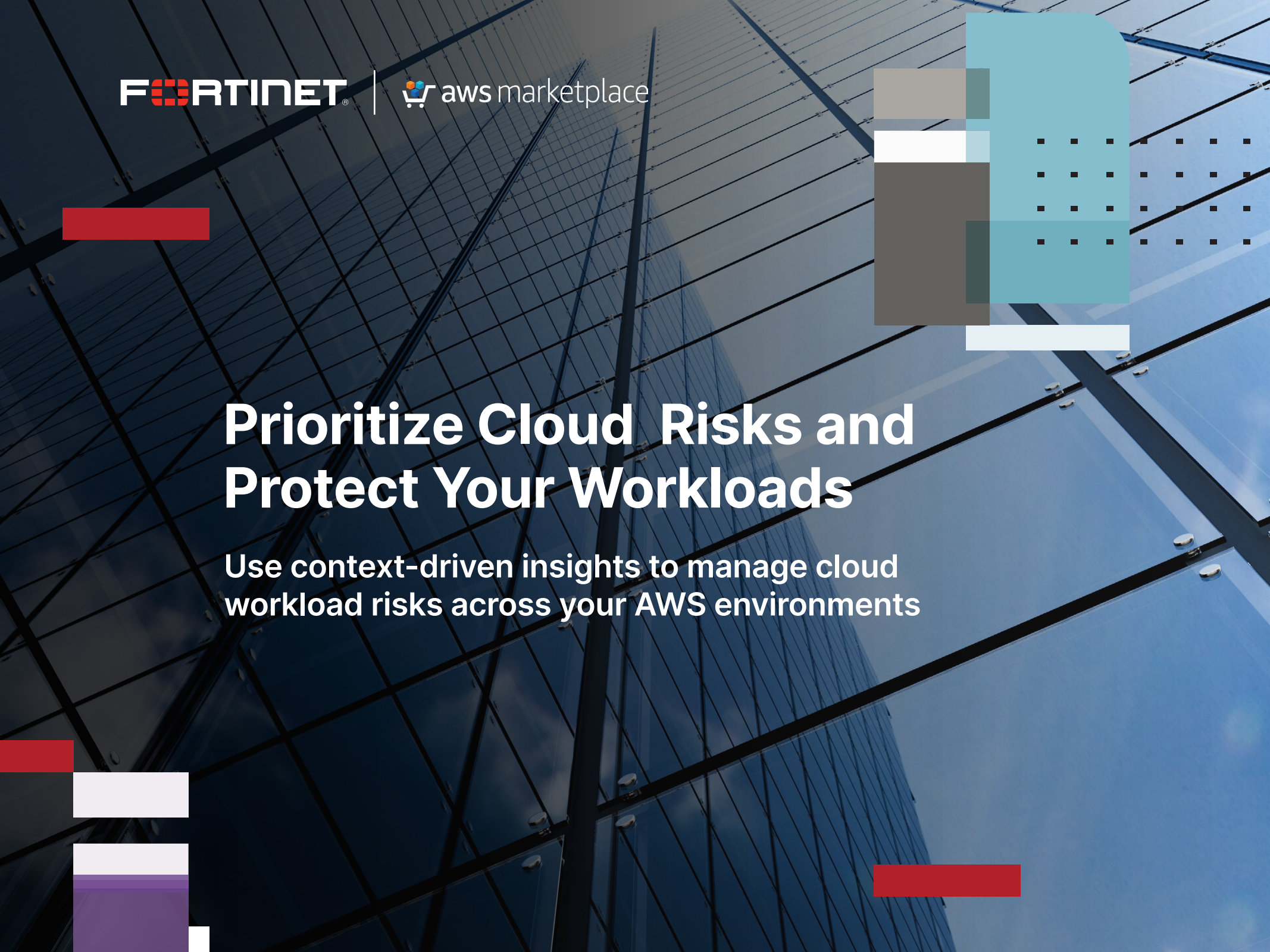
FORTINET
aws marketplace
Prioritize Cloud Risks and Protect Your Workloads
Use context-driven insights to manage cloud workload risks across your AWS environments

Table of Contents

Keeping Pace with Accelerated Cloud Adoption

As companies worldwide grow their cloud footprints, they've benefitted from increased resiliency, more agile business models, and faster innovation. Many of these companies embarked on, or accelerated, their digital transformations with Amazon Web Services (AWS), the world's most broadly adopted cloud platform.

But migrating to the cloud has also given way to complex and layered environments, which can be more difficult for security teams to protect against threats. It's imperative that companies develop a strong security posture that can keep pace with cloud-powered innovations. Not only should they align with the Shared Responsibility Model—where AWS protects the cloud infrastructure and customers secure their data—but also enable security teams to maximize their efforts and address the most pressing threats.

Central to a strong security posture is proactive risk management that focuses on the highest impact risks.

Cybersecurity risk management is the practice of proactively evaluating the context behind the risk, that includes factors such as security posture, vulnerability, permissions, and threat signals. With this broader context, security teams can make more informed decisions around risk prioritization, mitigation, and remediation. Solutions that can also consolidate and contextualize alerts from AWS security services, as well as other integrated security solutions, helps provide broad visibility across the cloud footprint. This will help produce better insights into cloud risk and remediation workflows, saving time and effort, while still keeping your AWS workloads protected.

Cybersecurity risk management is the practice of evaluating the broader context associated with risks so security teams can prioritize and make more informed decisions around mitigation and remediation.

Continue reading this ebook to learn about the challenges that can impede a robust risk management strategy, as well as solutions to help your security team develop a solid risk management foundation.

Risk Management Blind Spots

In today's rapidly evolving cloud landscape, new risks constantly emerge. Traditional security teams lack the capabilities to address these new threats, making it challenging to move from a reactive approach to a proactive strategy. The following roadblocks can stand in the way of adequately responding to risks.

Too many security tools can be counter productive

In an ever-evolving threat landscape, as new risks emerge, organizations tend to add new security tools to their overall infrastructure to bolster their security posture. Over time, this leads to security sprawl and creates more silos and potential blind spots that make it difficult to act proactively against threats. In fact, a disparate set of tools—with different features, management, and interfaces—can lead to fractured visibility across AWS environments, increasing the likelihood that risks are not properly assessed and mitigated. With too many security tools, organizations will have a hard time identifying high-priority risks to address, due to vulnerabilities, sensitive information, or misconfigurations, ultimately leading to insufficient security coverage.

If this sounds familiar, you're not alone. According to IBM, nearly one-third of today's enterprise organizations have more than 50 separate security tools deployed. Not only is the growing volume an issue, but also the lack of native integration between them. In addition, too many disparate security tools can result in increased costs to manage and update them.

Alert fatigue leads to missed action

Security teams also struggle with alert fatigue due to the volume of alerts each of the security tools generate. These alerts often lack context and require security teams to manually research and investigate each one. And as the volume of alerts increase, the alerts begin to exceed the security teams' ability to process and effectively manage them, leading to missed actions.

Security teams can see more than 1,000 cybersecurity alerts per day

But just how many alerts is too many? According to Dimensional Research, security stakeholders reported dealing with at least 1,000 alerts every day. As cloud adoption accelerates, companies also see an increase in the amount of security data they need to analyze, which can create an ever-increasing security backlog.

While many security solutions produce alerts about potential threats, few provide enough contextual information that security teams need to properly investigate and take action to mitigate. As a result, security teams have difficulty prioritizing critical risks because they waste time triaging large volumes of low risk findings, weeding out false positives, and even go so far as ignoring the alerts as they continue to be inundated by the flood of notifications.

Build a Solid Foundation for Managing Risks

Risk management is not a one-and-done process. For it to be effective, security teams should consider it an ongoing practice that evolves with innovation and operations. Building a solid foundation for risk management will help bolster your security posture to withstand any past, present, and emerging threats.

Automate and reduce risk with AWS security services

From data protection, to threat detection, to identity and access management, AWS offers a range of security services to secure your AWS environments. Natively integrated and easy to deploy, AWS services can provide visibility into cloud service configurations, workload vulnerabilities, cloud permissions, data profiles, network traffic, and threats across your AWS environment.

Gain visibility across your entire technology stack

To accurately assess risk, security teams need comprehensive visibility into their infrastructure, cloud services, workloads, applications, devices, and other resources. By nature, cloud environments shift and new threats can emerge. To keep pace in such a dynamic landscape, visibility into all your active workloads is critical.

Apply a defense-in-depth strategy

As the threat landscape evolve and grow rapidly in scale and sophistication, applying a multi-tiered approach to security creates a defense-in-depth solution, strengthening an enterprise's defense against threats. Augmenting AWS services with integrated cloud-native solutions provides a broader and more strategic method to managing cloud risk.

See Risk Management in Action

With your foundation for risk management in place, you can take the next step of managing risk with greater insights from a cloud-native security solution. Here's what insight-driven risk management looks like in practice.

1. Alerts are generated: Security services such as Amazon GuardDuty and Amazon Inspector generate alerts and findings from different events, some of which include cloud service configurations, workload vulnerabilities, cloud permissions, data profiles, network traffic, and threats. These alerts lack context, making it challenging to make informed decisions for mitigating and remediating. The integrated solution is equipped to ingest and correlate the volume of alerts from cloud resources such as compute instances, containers, database services, and data storage services.

2. Context is provided: Native integrations with security services and solutions across the technology stack enable broader context across more cloud workloads. Because of this, the security solution is able to provide teams with prioritized, context rich, and actionable insights about resources that present the highest risk and need immediate attention. For example, instead of simply alerting about a suspicious file, the solution will incorporate other factors such as, the contents of the file, as well as the permissions associated with it, among others, to accurately assess the risk. The risk evaluation will differ depending on the combination of factors evaluated in association with that file.

3. Reduced alert fatigue: With each of the security solutions comes a litany of alerts that often require manual analysis, which can quickly compound across an organization's cloud deployment. Inundated with alerts, security teams can face decreased productivity, inefficient workflows, and security risks accumulating faster than they can be addressed. When the security solution correlates and contextualizes all these alerts, you can reduce the burden of investigation, analysis, and action.

4. Informed action is taken: With more context, consistent workflows that scale security across the cloud help security teams apply their skills to the high-priority tasks that require their expertise instead of burning cycles on manual investigation and triage of alerts. In addition, integrated workflow solutions allow them to better manage their mitigation and remediation tactics.

FortiCNP Makes Insight-Driven Risk Management Possible

So where can you find a security solution that enables insight-driven risk management? Meet FortiCNP. FortiCNP is a SaaS-based, cloud security solution, natively integrated with AWS security services and Fortinet's Security Fabric, that delivers friction-free cloud security with context-rich actionable insights to help organizations manage their cloud risks. Security teams will gain context-rich insights for their high-risk resources, so they can focus on the most impactful threats to their organization.

FortiCNP improves your risk management with:

Context-rich, actionable insights:
FortiCNP's patented Resource Risk Insights™ technology correlates and contextualizes security findings from AWS security services and Fortinet security products to calculate risk and stack rank highest risk resources based on analysis of the security posture, vulnerabilities, permissions, and threat signals. By presenting actionable information on the highest priority issues, security teams can take quick remedial actions to effectively manage and mitigate risk. Actionable insights allow organizations to prioritize risk based on the severity of issues and protect the usage of various AWS resources, such as compute instances, containers, database services, and data storage services.

Automated workflows and remediation:
For high-priority risk insights, FortiCNP helps streamline the mitigation and remediation process by integrating with digital workflow solutions, such as JIRA and ServiceNow. This integration allows security teams to automate and manage their response. For fixes that should ultimately be implemented in the CI/CD pipeline, stop-gap remediation can be implemented for AWS environments using Fortinet's cloud security products to protect from threats before permanent fixes are implemented.

Maximize the value of cloud-native security services:
With FortiCNP you can maximize the value and benefit from easy deployment capabilities for your AWS security services, which are natively designed for your AWS environments. This helps eliminate integration friction that many companies have in a fragmented security architecture. Additionally, these services have access to security events that external security solutions cannot access, helping to manage and protect AWS workloads more effectively.

Be Proactive with Your Risk Management

With FortiCNP you'll have a simple and effective cloud-native solution that turns findings and alerts into actionable insights to help you secure your AWS workloads. Advance to proactive risk management to stay on top of cloud risks while keeping up with the speed of innovation.

Start your free trial of FortiCNP on AWS Marketplace.

www.fortinet.com

July 13, 2022 9:05 AM

FortiCNP eBook_07132022_RA

123456-0-0-EN