SOLUTION BRIEF

FortiCSPM: Advanced Cloud Security Posture Management

Executive Summary

Cloud has become synonymous with digital acceleration as organizations continue to drive the evolution of their businesses through cloud adoption. With this, the velocity they build and deploy applications into the cloud has also increased.

Unfortunately, as organizations continue to expand their application and cloud footprints, their cloud risks increase significantly due to increasing complexity, loss of visibility, and exposure to configuration drift. To combat this, organizations need to shift security left in their CI/CD pipelines by implementing Policy-as-Code (PaC) security alongside proactively managing their risks using cloud security posture management (CSPM) capabilities.

FortiCSPM is an advanced CSPM solution that empowers organizations to get the deep visibility needed to manage risks in their cloud infrastructure environments. Using its PaC capibilities, organizations can readily formalize security and controls into a set of automated rules and logic that are easy to maintain and apply and with low false postives. FortiCSPM provides a unified experience for an organization to get centralized, consolidated, auditable, and unmatched visibility across their full cloud deployments, along with workflows that simplify remediation and automated validation of fixes.

“Misconfiguration of cloud security remains the biggest cloud security risk according to 59% of cybersecurity professionals... followed by exfiltration of sensitive data (51%), insecure interfaces/APIs (51%), and unauthorized access (49%).”[1]

Misconfigurations Remain the Biggest Cloud Security Risk

The desire for digital acceleration has led organizations to drive toward delivering faster and better application experiences and to bring applications and data closer to users and devices. This results in applications living wherever they deliver the most optimal desired business outcomes.

Unfortunately, this fluid environment creates challenges for CIOs and CISOs alike, which include increased operational complexity, visibility gaps, and an explosion of cloud platforms and tools. The lack of skilled cybersecurity staff resources and expertise further exacerbates these challenges.

According to the 2023 Cloud Security Report, a global survey of over 750 cybersecurity professionals conducted by Cybersecurity Insiders, the top challenges organizations face are:

- Lack of visibility (32%)
- Lack of consistent security policies (32%)
- Lack of staff resources or expertise (43%)[2]

Misconfigurations are often due to failure to change default settings or adhere to defined standards, including changes made to components and tools outside of change control processes, that result in configuration drifts. Misconfigured cloud infrastructure and assets create the vulnerabilities that attackers use to access systems and data. When this happens, organizations unknowingly leave themselves exposed to attacks and compromises that can lead to data breaches, reputational damages, and financial losses.

Easily Shift Security Left with Policy-as-Code

To help organizations combat misconfigurations and risks, and efficiently operationalize their cloud and DevOps cycles, FortiCSPM delivers a “no code approach” to providing security PaC that allows organizations to formalize both security and controls into a set of automated rules and logic that are easy to maintain and apply. FortiCSPM offers thousands of out-of-the-box policy checks based on industry standards and best practices. This makes it easy for organizations to define specific policies across a number of cloud platforms and tools based on reference definitions that ensure policy logics are consistent with the technology and version being monitored. Policies can also be validated before deployments. Organizations can now implement security standards without having a cloud expert or writing code.

With FortiCSPM, organizations gain increased visibility and automated assurance of policies that help them reduce complexity in managing their cloud risk exposure. Flexible, granular policies delivered by FortiCSPM help reduce false positives and noise, reducing the burden on security teams.

“90% of cybersecurity professionals want a single cloud security platform for consistent security policy across all cloud environments.”[3]

Single Console to Drive Governance Across All Cloud Deployments

Organizations pursuing digital acceleration often span their deployments across multi-cloud instances. As a result, it is critical for them to have consolidated visibility and control everywhere their cloud and application footprint exists. FortiCSPM empowers organizations with centralized policy management and automation across any environment. As a result, they can write policy once and apply it anywhere and everywhere.

FortiCSPM delivers a single console experience, consolidating visibility, reporting, compliance, and governance across all cloud deployments. Through the FortiCSPM console, organizations gain a centralized view of all cloud asset usage and states sourced directly from cloud service providers. Issues discovered can be assigned as tasks to stakeholders, including developers, for remediation. As a result, FortiCSPM can help organizations reduce complexity and alert fatigue, and managing risks more efficiently.

Making Secure DevOps a Reality

With FortiCSPM, organizations can seamlessly implement security controls earlier in the development life-cycle process to proactively address security issues before code gets deployed. As a result, organizations can proactively eliminate their risks and exposure before they become a problem.

FortiCSPM can be readily integrated into development and delivery pipelines and workflows to continuously monitor and evaluate those pipelines against security policy controls. The issues identified can be delegated and tracked for remediation. FortiCSPM can also automatically revalidate changes, delivering continuous, proactive security throughout the entire CI/CD pipeline.

Simplifying Compliance and Reporting

Along with its centralized visibility and automated evaluation and revalidation of security controls, FortiCSPM can help organizations readily address their compliance needs. Organizations can define policies that comply with the required business context and maintain granular control of policy deployment by geography, environment, business unit, application workload, or regulatory requirement. This helps reduce drifts that can lead to noncompliance events.

Additionally, organizations can leverage FortiCSPM to obtain clear and auditable reports of the state of security and regulatory compliance for every resource on every cloud at any time.

FortiCSPM Delivers PaC Security That Simplifies Managing Cloud Risks

As organizations expand their cloud and application footprint in pursuit of digital acceleration, they need to build in visibility and controls that empower them to readily identify exposures, proactively manage their risks, and meet compliance requirements. And given that most organizations lack adequate cybersecurity staff resources and skills, they need to deploy solutions like FortiCSPM that offer low false positives and flexible policies to reduce alert fatigue.

With its PaC capabilities and ease of integration into CI/CD pipelines for shift-left security, FortiCSPM empowers organizations to readily formalize security and controls into a set of automated rules and logic that are easy to maintain and apply. FortiCSPM also helps organizations achieve streamlined operations and compliance management with its centralized, consolidated, auditable, and unmatched visibility across their full cloud deployments, along with workflows that simplify remediation and automated validation of fixes.

[1] Cybersecurity Insiders, 2023 Cloud Security Report.

[2] Ibid.

[3] Ibid.

February 23, 2024 11:25 AM
2573923-0-0-EN