Mindtree
A Larsen & Toubro Group Company

Mindtree Cloud Security Posture Assessment

A Mindtree POV / April 2021

Welcome to possible

Table of Contents

CLOUD SECURITY POSTURE MANAGEMENT

Cloud Security Posture Management

Cloud Security Posture Management (CSPM) has become more popular in today's market as it predominantly helps in identifying and remediating risks across organizations' cloud infrastructures. It also helps in automating the manual effort by remediating the misconfigurations.

CSPM focuses on visualizing cloud security risks and performing risks assessment, compliance monitoring, incident response and DevOps integration. It also helps organizations in applying the best practices for cloud security to multi-cloud, hybrid as well as container environments.

WHY IS CSPM REQUIRED?

CSPM allows organizations to monitor security risk and fix some of them automatically. It focuses on addressing the below security policy violations:

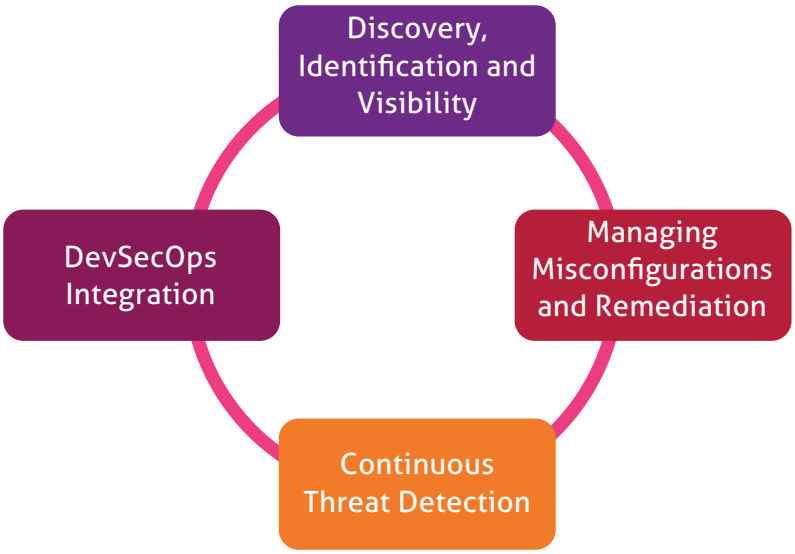
Lack of visibility across multiple cloud environment and mitigating violations

Identification of excessive or unused account permissions

Cloud misconfigurations, Open IP ports, unauthorized modifications etc.

CSPM - THE PROCESS

CSPM discovers the misconfigurations issues, identifies security risks and ensures visibility across the cloud infrastructure, and thus provides a unified view of the associated cloud accounts. In addition, CSPM proactively helps in continuous threat detection and DevSecOps integration to capture the insights of policy violations.



Discovery, Identification and Visibility

- CSPM helps in identifying risks across various cloud platforms before they pose a security risk to the organization.
- To discover, identify and provide visibility across the cloud infrastructure including sensitive resources, assets and security configurations.
- To access the cloud resources in multi-cloud environments and accounts.
- Cloud resources, details, risks associated are discovered automatically upon successful deployment. For example: Misconfigurations, security and change activity.
- Targeted threat detection to reduce alert fatigue

Managing Misconfigurations and Remediation

- CSPM eliminates security risks across the cloud platform and helps in accelerating the delivery process.
- To identify and remediate policy violations, it compares the cloud application configurations to organizational benchmarks.
- Misconfigurations and open IP ports etc. are the common issues that expose the risk to the cloud resources, and to deal with these issues, recommendations and automated remediation are performed so as to prevent vulnerabilities.
- Continuous monitoring the storage and database instances, so as to avoid the accessibility to the public environment and ensure high availability, encryption etc.

Continuous Threat Detection

- Threats can be easily detected in the early stage of development cycle when performing the cloud security posture for the organization.
- It focuses on prioritizing the vulnerability based on the environment and thus reduces the alerts.
- CSPM enables continuous monitoring of the environment for any malicious activity, and unauthorized access to cloud resources and user activities across the cloud environment using real-time threat detection.

DevSecOps Integration

- Its cloud-native, agentless posture management provides centralized visibility and control over all cloud resources.
- It eliminates complexity and friction across multiple cloud accounts and multi cloud providers.
- To enable faster remediation and response to the threat it can also be integrated with the existing DevOps tools set.
- Integration with Security Information and Event Management (SIEM) helps in capturing insights related to cloud misconfigurations, notify if there is any policy violation and streamline the visibility across the cloud environment.

CLOUD SECURITY POSTURE MANAGEMENT - BENEFITS

CSPM continuously monitors and tracks the enterprise cloud environments to identify gaps between the actual and the stated security policies to avoid risks that may occur later.

- Automated security assessment; continuous monitoring; reporting and management
- Prevent configuration vulnerability, visibility into cloud usage and security events
- Continuous visibility into cloud infrastructure and monitoring of multiple cloud environments to detect any policy violations.
- Assessing the data risk and detection of excessive account permissions
- Ability to automatically remediate the misconfigurations as and when required
- Enforcement of security best practices, regulatory compliance with common security standards for best practices such as CIS Foundations Benchmarks, SOC 2, PCI, NIST 800-53 or HIPAA.
- Prioritizing the risks, getting recommendations and remediation

Thus, CSPM helps organizations detect cloud misconfigurations, vulnerabilities and security threats that might result in compliance violations and data breaches, and takes remediation steps to prevent the security risks

CLOUD SECURITY POSTURE MANAGEMENT - BEST PRACTICES

- **Setting Security Configuration Baselines, Cloud-specific benchmarks**
- **Identify and analyze the associated risk and prioritize security violations**
- **Continuous Security Check**

Setting Security Configuration Baselines and Cloud-specific Benchmarks

- With the help of cloud-specific benchmarks and security standards, monitor your cloud's security posture.
- The ultimate aim is to ensure that while designing security procedures, cloud's dynamic nature should be considered.

Identify and Analyze the Associated Risk and Prioritize Security Violations

- When it comes to violation of alerts, the security team must ensure that they analyze the risks associated, and prioritize the most critical violation as soon as it occurs. Those violations should be given the high priority.

Continuous Security Check

- It becomes difficult to enforce security and find gaps on dynamic applications where new resources are constantly being used, which results in more risks for the organization. Thus, continuous security monitoring is required to minimize the security risks as well as gaps.
- Defining misconfiguration checks to avoid any violations during the execution of the deployment pipeline and adding the remediation's to correct the misconfigured settings.

MINDTREE CLOUD SECURITY POSTURE ASSESSMENT - BENEFITS

Mindtree Cloud Security Posture Assessment - Key Benefits

Fortify the Cloud Security Posture

1 Click Compliance Reporting

Advance detection of anomalous user activities

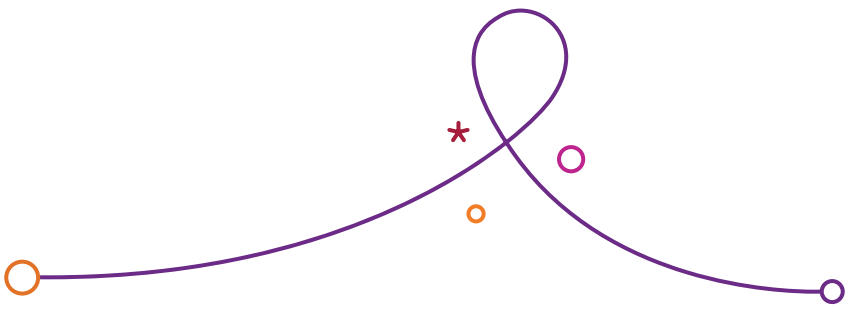
Automated threat detection

Prioritizing the risks, getting recommendations and remediation

Effort saving, Increased productivity due to automated security assessment etc.

- Leverage AI/ML tools to get visibility in minutes
- Minimize spending efforts in performing remediation actions rather than identifying the logs
- Detection of publicly exposed assets and identification of excessive and unused permissions
- Closure of open ports in the exposed machines to prevent threats, data breaches, potential attacks and blocking them before the data loss takes place to meet the compliance standards like CIS and GDPR
- Out-of-the-box compliance reporting leading to saving manual effort
- Improved compliance as per CIS Foundations, NIST and GDPR

CSPM helps organizations that are dealing with the multiple cloud accounts, with a large or critical workload. It ensures continuous visibility across the organization's cloud infrastructure and protects the workload environment. It also focuses on remediating misconfigurations and improves the overall security posture of the organization.



About Mindtree

Mindtree [NSE: MINDTREE] is a global technology consulting and services company, helping enterprises marry scale with agility to achieve competitive advantage. “Born digital,” in 1999 and now a Larsen & Toubro Group Company, Mindtree applies its deep domain knowledge to 275+ enterprise client engagements to break down silos, make sense of digital complexity and bring new initiatives to market faster. We enable IT to move at the speed of business, leveraging emerging technologies and the efficiencies of Continuous Delivery to spur business innovation. Operating in more than 15 countries across the world, we’re consistently regarded as one of the best places to work, embodied every day by our winning culture made up of over 22,000 entrepreneurial, collaborative and dedicated “Mindtree Minds.”