LTIMindtree | sysdig

Whitepaper

Enhancing Enterprise Cloud Security by Leveraging CNAPP and CTDR

Revolutionizing cloud security for businesses with CNAPP and CTDR! Discover how you can take your enterprise security to the next level.

Contents

Executive summary

With the rapid transition to cloud computing and the ongoing process of application modernization, organizations are faced with a multitude of challenges when it comes to ensuring robust enterprise cloud security. In this new paradigm, the traditional approach of siloed protection control is no longer sufficient. Instead, enterprises must strive to achieve cloud security that goes above and beyond what was previously considered acceptable. This shift in focus requires a comprehensive understanding of the unique challenges posed by cloud environments and the implementation of proactive measures to mitigate risks and safeguard sensitive data. By adopting a holistic approach to cloud security, organizations can confidently embrace the benefits of the cloud while maintaining the highest protection standards for their valuable assets.

Cloud-native applications have gained immense popularity in recent years, revolutionizing how businesses operate. However, with this increased reliance on cloud-native applications, the need for robust security measures has become paramount. Enterprises must ensure that their applications are adequately protected from potential attacks and vulnerabilities that may arise in a cloud environment. This is where cloud-native application protection platforms (CNAPPs) come into play.

These platforms are specifically designed to safeguard cloud-native applications, providing comprehensive security solutions that address the unique challenges of cloud environments. By implementing CNAPPs, businesses can ensure the smooth operation of their applications while mitigating the risks associated with cloud-based threats.

According to Gartner, there is a growing trend towards consolidating security tooling for the life cycle protection of cloud-native applications. "By 2026, 80% of enterprises will have consolidated security tooling for the life cycle protection of cloud-native applications to three or fewer vendors, down from an average of 10 in 2022.". This consolidation is expected to streamline security operations and enhance overall effectiveness in safeguarding cloud-native applications.[1]

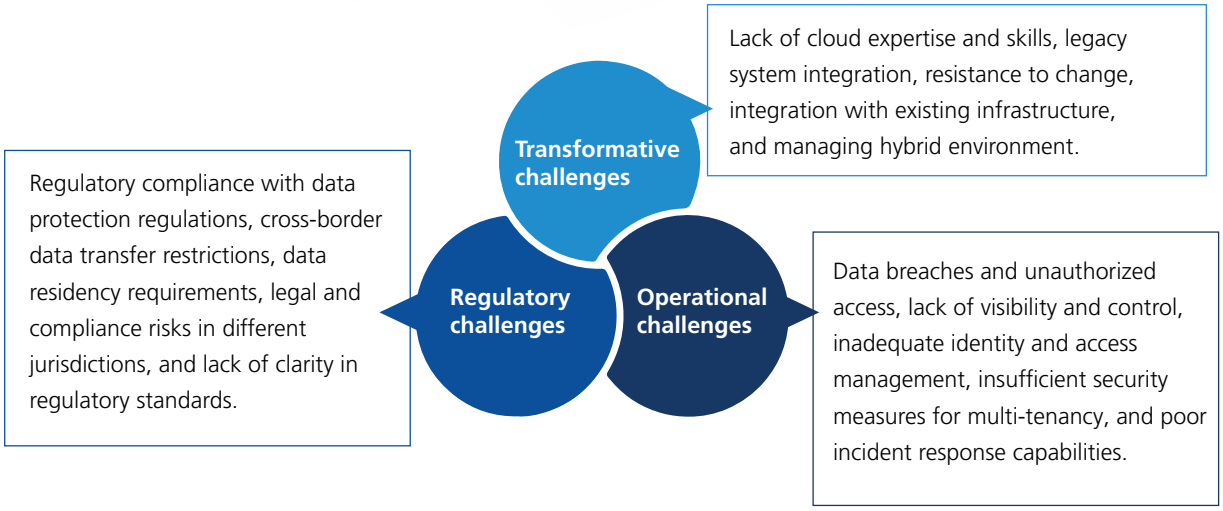
In this whitepaper, we will explore the enterprise security threat landscape, various cloud security risks and challenges, the attack journey, and how to improve enterprise cloud security using CNAPP and CTDR solutions.

Enterprise security threat landscape and emerging challenges

Understanding the cloud and container security threat landscape is crucial in comprehending the significance of CNAPP. Cloud environments bring forth a new set of security challenges due to their distributed nature and reliance on virtualization technologies. These challenges include data breaches, unauthorized access, malicious insider attacks, and vulnerabilities in containers.

Also, businesses today face a range of typical cloud challenges. These include managing complex infrastructures, ensuring compliance with regulatory standards, maintaining visibility across multi-cloud environments, and securing data transmission between cloud services.

The enterprise cloud security challenges can be categorized into three buckets based on their impact on business.



Security risks associated with enterprise cloud security

Stolen credentials

Unauthorized access to cloud services using compromised login credentials can happen when an attacker gains access to usernames and passwords through various methods such as phishing, social engineering, or brute-force attacks. An example of a stolen credential attack is the Revil attack (also known as Sodinokibi ransomware). In this attack, cybercriminals targeted managed service providers (MSPs) and used stolen credentials to gain access to their clients' systems. Once inside, they encrypted the data and demanded a ransom for its release.

Critical vulnerability

A critical vulnerability is a flaw in the cloud infrastructure that can be exploited by attackers to gain unauthorized access or perform malicious activities. LABRAT vulnerability affected Microsoft Exchange servers. This vulnerability allowed attackers to remotely execute code on the server and gain control over the entire infrastructure. It was exploited by various threat actors to steal sensitive data or deploy ransomware.

Lateral movement

The technique used by attackers to move laterally within a compromised network or cloud environment after gaining initial access. They exploit vulnerabilities or use stolen credentials to access and control other systems or accounts. An example of lateral movement is the SCARLETTEEEL attack, which targeted various organizations. The attackers gained initial access through phishing emails and then moved laterally within the network, compromising multiple systems and exfiltrating sensitive data.

Data exposure risk

When sensitive or confidential information stored in the cloud is unintentionally exposed due to misconfigurations, weak access controls, or vulnerabilities. An example of data exposure is object-level broken authentication. This occurs when an attacker gains unauthorized access to specific objects or files within a cloud storage system. For instance, if an object in a cloud-based storage service has weak authentication controls, an attacker could bypass those controls and gain access to the object, potentially exposing sensitive data.

Configuration drift

When a modification occurs within a container, it is classified as drift, which could potentially indicate a security breach. Unfortunately, container drift can also arise from outdated practices, where system administrators perform maintenance on active containers, inadvertently blending their actions with those of malicious actors. As a result, threat actors and malware can camouflage themselves within the noise generated by legitimate activity, allowing them to execute their harmful codes without detection. With Sysdig's Drift Control, teams can effortlessly identify, mitigate, and swiftly respond to incidents involving container modifications in a production environment, commonly referred to as container drift.

Understanding attack journey: visualize security risks

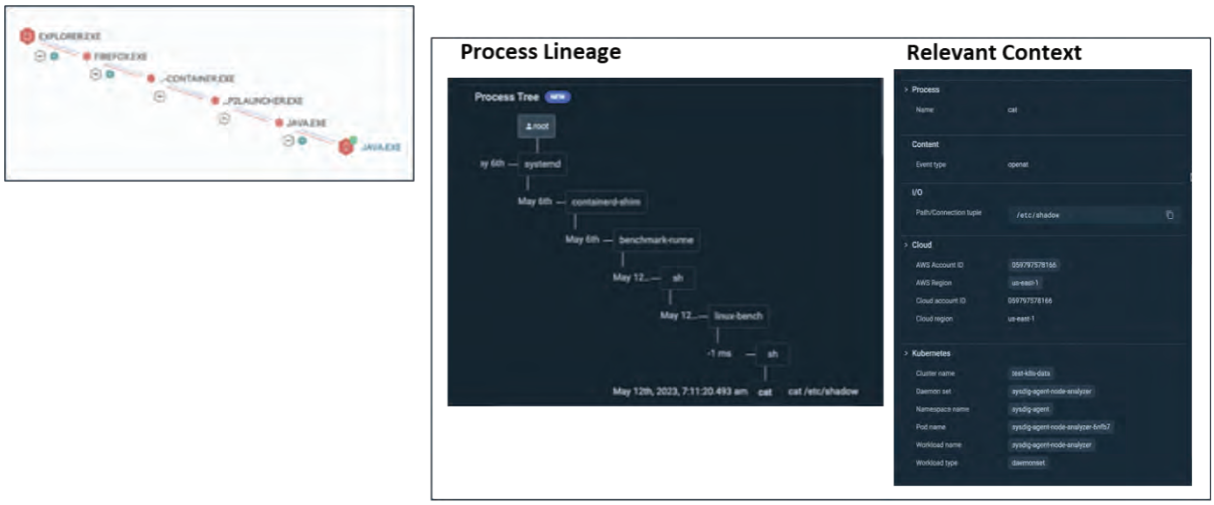


Figure 1 Attack Path Analysis

Attack path analysis is a complex activity and needs expertise and in-depth analysis. At LTIMindtree, we perform thorough research on the attack path by leveraging our expertise in identifying critical risks and finding correlations between risks and runtime events.

Attack path analysis is of utmost importance to businesses operating in a cloud environment. In the cloud, where data and applications are hosted on remote servers, the attack surface and potential vulnerabilities are increased. By conducting attack path analysis, businesses can gain valuable insights into the specific pathways that attackers may exploit to compromise their cloud infrastructure.

It helps identify risks, prioritize security efforts, proactively mitigate attacks, and fortify cloud systems against potential threats. By leveraging attack path analysis, businesses can enhance their overall security and protect their valuable data and applications in the cloud environment.

Here are some of the benefits of attack path analysis:

- Identify individual risks and discover critical paths that an attacker might use to get access to assets. This helps in prioritizing security efforts effectively.
- It bridges the gap between possible risk and real-time events to mitigate attacks before they can move laterally.
- With the attack journey, organizations can assess the resources at risk, their findings, and the critical path an attacker may take when exploiting any weaknesses.

Protecting enterprise clouds with CNAPP and CTDR

As organizations increasingly migrate their applications and infrastructure to the cloud, they must also adopt robust security measures such as CNAPP and CTDR solutions to safeguard their sensitive data and protect against potential cyber threats.

Cloud security reference model leveraging CNAPP and CTDR

CNAPP and CTDR are two security solutions that work together to provide comprehensive protection for cloud-native applications. CNAPP employs cutting-edge technologies such as container security, API security, and vulnerability management to ensure that applications running in the cloud are fully protected against potential vulnerabilities and attacks. With its holistic approach to cloud security, CNAPP is designed to safeguard cloud-native applications from a wide range of threats, providing users with peace of mind and confidence in their cloud-based operations.

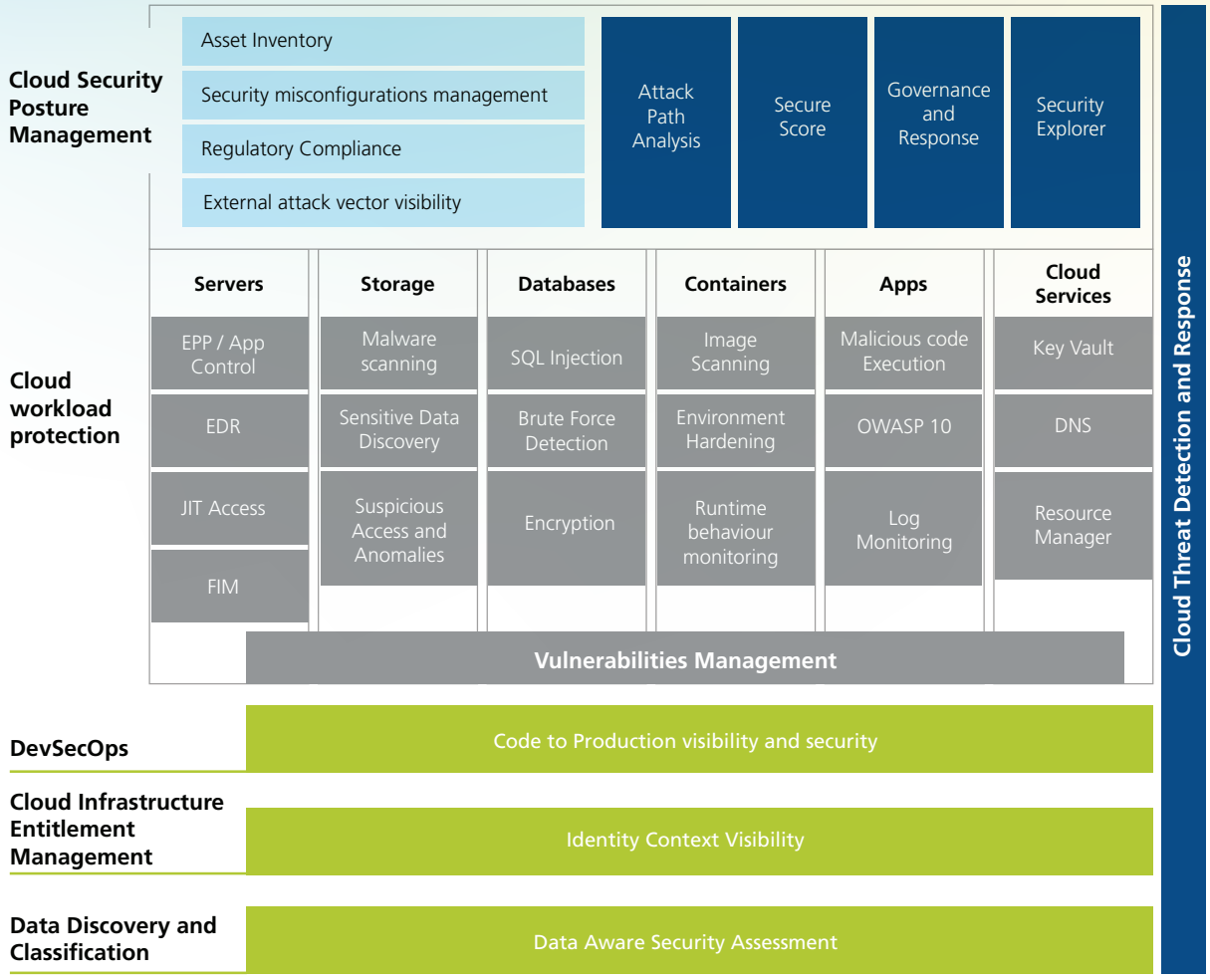


Figure 2 Cloud security reference model leveraging CNAPP and CTDR

Let us dive deep and explore how these technologies can help you protect your cloud ecosystem.

CNAPP with runtime insights

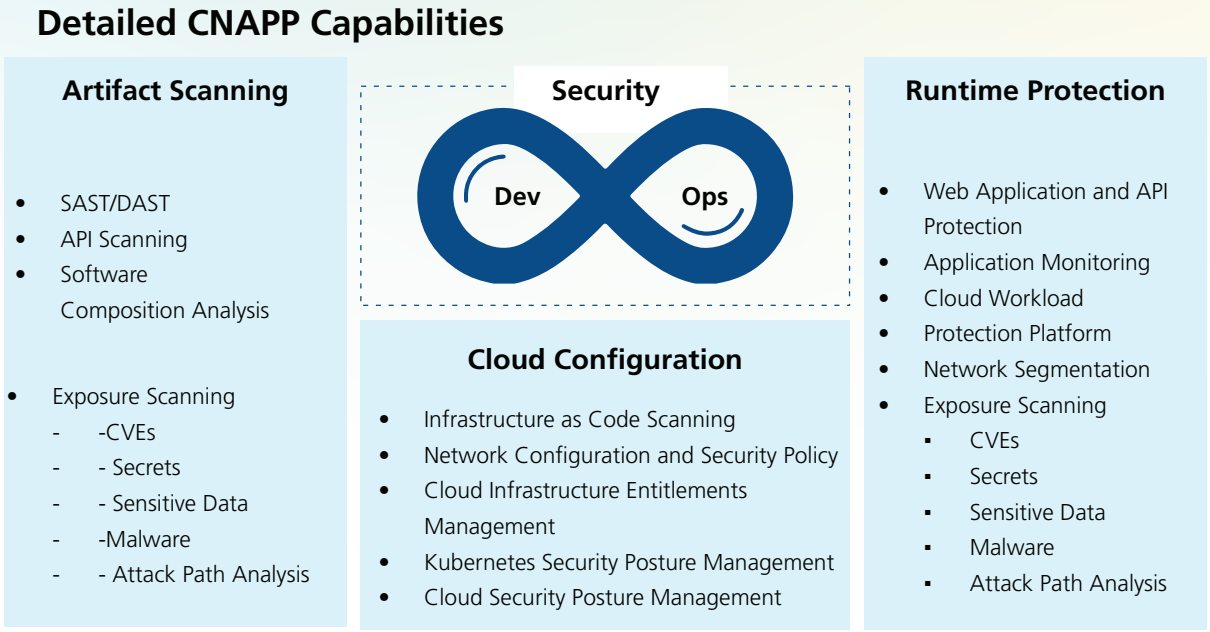


Figure 3 CNAPP detailed view by Gartner, https://www.gartner.com/reviews/market/cloud-native-application-protection-platforms

CNAPP is designed to intake and examine diverse data sources. With the surge in data volume, especially with the widespread use of microservices on containers/Kubernetes, the accumulation of both high and low-fidelity signals becomes massive. This leads to the essential question: How can I determine the highest-priority risks in my cloud-native infrastructure?

Having a profound understanding of what's running allows you to narrow down the focus on tasks requiring immediate attention. In essence, awareness of what's running, often referred to as runtime insights, provides the crucial context for security and DevOps teams to prioritize and address the most critical risks initially.

To secure innovation in the cloud, we need runtime insights to prioritize the most critical risks and stay ahead of evolving threats.

Steps involved

1. **Identify security requirements:** Understand the security requirements of the cloud-native application and define the threat detection and response capabilities needed.
2. **Architecture design:** Design the cloud-native application architecture using CNAPP principles, incorporating security measures such as secure network design, access controls, encryption, authentication, and authorization mechanisms.
3. **Monitoring and logging:** Implement robust monitoring and logging mechanisms within the cloud-native application to capture relevant security events and logs. These can include application logs, system logs, network traffic logs, and user activity logs.
4. **Event collection:** Set up mechanisms to collect security events and logs from various sources within the cloud environment, such as cloud provider logs, application logs, and infrastructure logs. Use log aggregation or centralized logging solutions for efficient management of these logs.
5. **Threat detection:** Deploy Real-time threat detection tools that can analyze the collected security events and logs in real-time. These tools use various techniques like rule-based detection, anomaly detection, machine learning, or AI-based algorithms to identify potential threats or suspicious activities.
6. **Alerting and incident response:** Configure alerting mechanisms to notify relevant stakeholders or a Security Operations Center (SOC) when a security threat or incident is detected. Establish incident response procedures and workflows to handle identified threats effectively.
7. **Automated remediation:** Implement automated response actions wherever possible. For example, it automatically blocks suspicious IP addresses, isolates compromised resources or triggers automated incident response playbooks.
8. **Continuous improvement:** Continuously monitor and review the effectiveness of the integrated CNAPP and Threat Detection and Response solution. Regularly update security policies, conduct penetration testing, and keep up with emerging threats to ensure an optimized security posture.

CNAPP consists of the following key components:

- CSPM (Cloud Security Posture Management)
- CWPM (Cloud Workload Protection management)
- CASB (Cloud Access Security Broker)

CSPM (Cloud Security Posture Management)

CSPM plays a vital role in managing and maintaining the security posture of an organization's cloud environment. It helps identify misconfigurations, compliance violations, and other security gaps, allowing organizations to proactively address these issues and strengthen their overall cloud security posture.

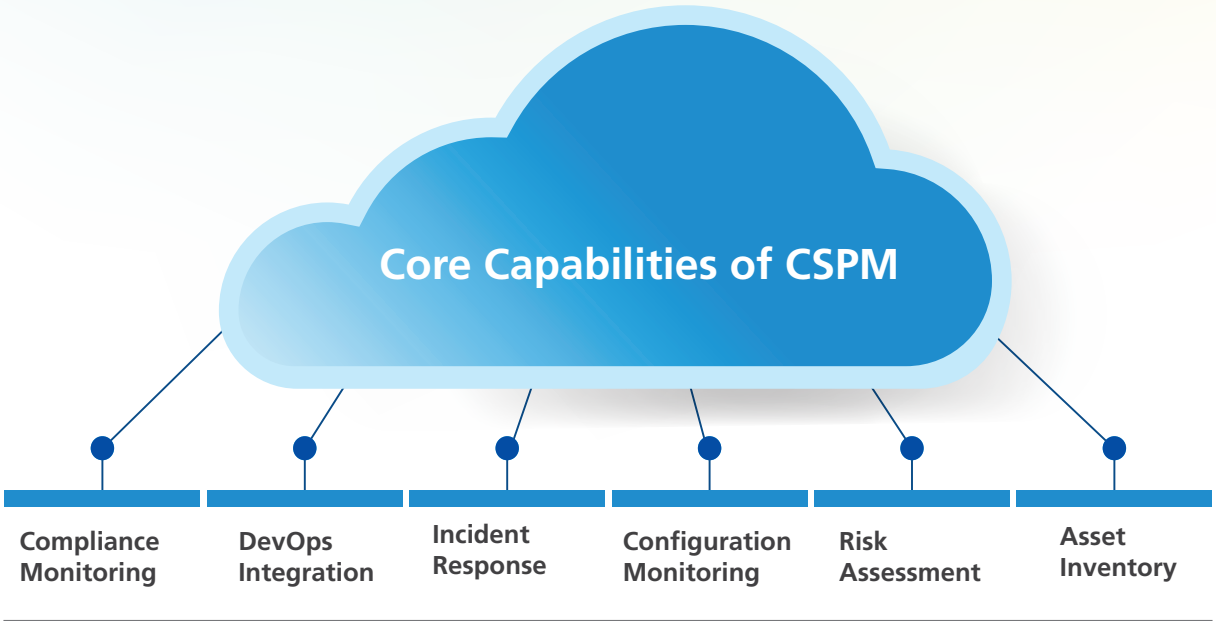


Figure 4 CSPM (Cloud Security Posture Management)

CWPM (Clould workload protection management)

CWPM focuses on securing the workloads and applications running within the cloud environment. It employs various techniques such as virtual machine (VM) security, intrusion detection, and anti-malware capabilities to protect against unauthorized access, malware infections, and other potential threats targeting cloud workloads.

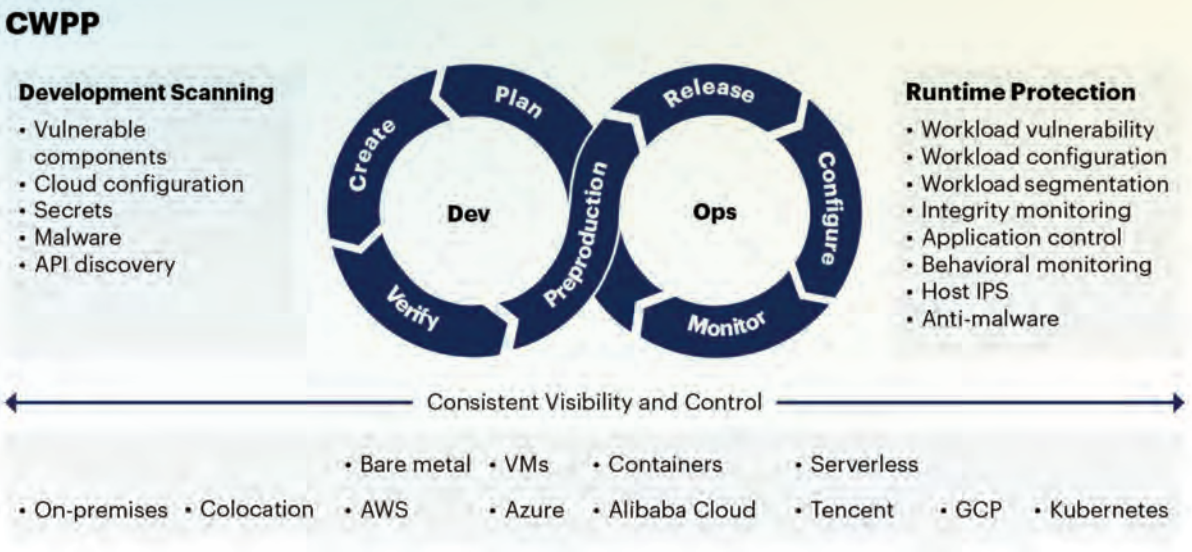


Figure 5 CWPP (Cloud Workload Protection Platform by Gartner), 12, July 2021, https://www.gartner.com/en/documents/4003465

CASB (Cloud Access Security Broker)

CASB acts as a critical intermediary between an organization's on-premises infrastructure and its cloud services. It ensures secure access to cloud applications by enforcing policies and providing visibility into users' activities. CASB also helps organizations meet regulatory compliance requirements by offering data loss prevention (DLP) capabilities and encryption for data at rest and in transit.

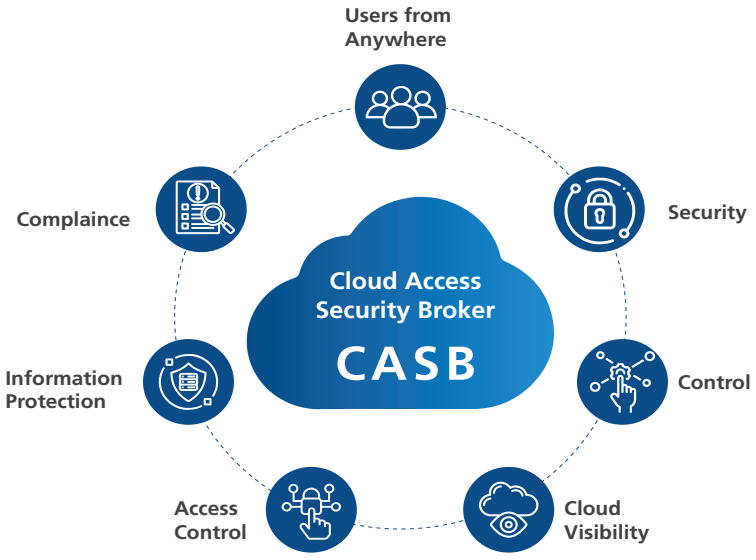


Figure 6 CASB (Cloud Access Security Broker)

CTDR (Cloud Threat Detection and Response)

Additionally, implementing cloud threat detection and response mechanisms is essential to effectively identify, analyze, and respond to potential cloud-based threats. By continuously monitoring the cloud environment, organizations can quickly detect suspicious activities, anomalous behavior, or potential data breaches. This enables them to take immediate action and mitigate any potential damage caused by cyber threats.

By adopting these comprehensive security measures, organizations can ensure the confidentiality, integrity, and availability of their data while effectively mitigating the risks associated with cloud-based operations.

CTDR use cases

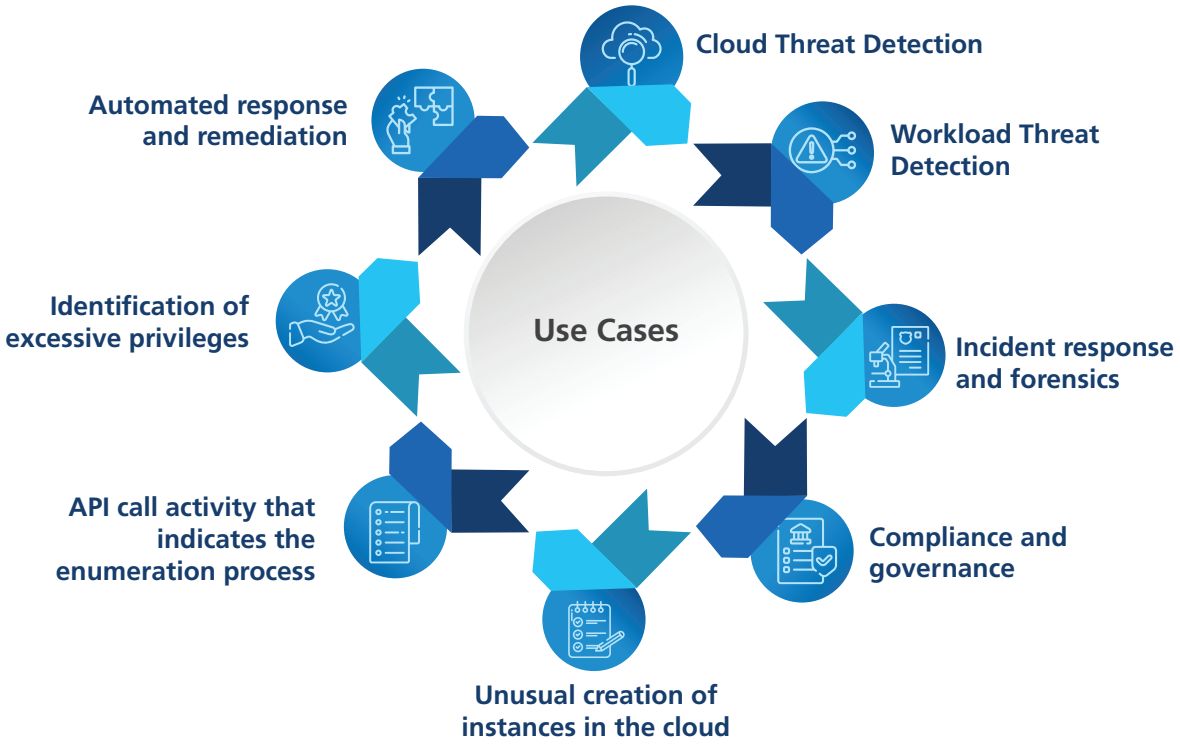


Figure 7 CTDR use cases

Cloud threat detection

This use case involves the detection of suspicious activities in real-time within a cloud environment. It helps to identify and respond to potential security threats promptly. When a suspicious activity is detected, appropriate alerts can be generated for further investigation, or automated actions can be taken to mitigate the threat.

Workload threat detection

Workload threat detection focuses on identifying threats at runtime within a cloud environment using managed policies in a multilayered approach. It aims to protect the workloads and applications running in the cloud infrastructure.

Incident response and forensics

Investigating and responding to security incidents that occur on ephemeral (short-lived) workloads within a cloud environment. Incident response teams can analyze the artifacts left behind by an incident and gather evidence for further analysis or legal purposes.

Compliance and governance

It focuses on enforcing policies across different environments within a cloud infrastructure and ensuring adherence to regulatory requirements and internal policies. A shared policy model is used to define and manage these policies consistently across the organization.

Unusual creation of instances in the cloud

CTDR can identify and react to incidents involving an abnormal creation of Amazon Elastic Compute Cloud (EC2) instances. A cloud identity role is responsible for creating a significantly higher number of resources/instances than usual, indicating a potential attack on the cloud workload. Further investigation of the EC2 workload revealed the presence of a crypto-mining bot, which is considered a sign of a security breach.

API call activity that indicates the enumeration process

An increasingly prevalent CTDR use case involves the utilization of API calls and interactions with APIs, as these comprise most of the cloud service and object interactions. CTDR can detect anomalous agents

interacting with a cloud API. The kinds of requests that were being made were consistent with known reconnaissance and cloud enumeration attacks, and it was discovered that the IAM role that had been assigned to the API calls was overly permissive.

Identification of excessive privileges

The identification of over-privileged accounts is possible with the assistance of CTDR. Managing cloud identities and permission policies is one of the major hurdles in creating and sustaining a secure cloud environment. Several cloud IAM roles are provided with excess privileges, which could result in abuse and malicious actions.

Automated response and remediation

CTDR can streamline and simplify the implementation of common detection and response playbooks by leveraging the cloud infrastructure for automation. A few of the great starting CTDR use cases for many teams could be automated alerting, quarantining, configuration changes, and rollback, as well as investigations and evidence collection.

LTIMindtree and Sysdig advantage

LTIMindtree and Sysdig offer valuable benefits to enterprises looking to protect their cloud infrastructure. By leveraging CNAPP (Cloud Native Application Protection Platform) with runtime insights, we provide enhanced visibility into the security of your cloud environment, and runtime insights help prioritize the most critical security issues by focusing on what's in use. With our cloud security services, you can expect fine-grained attack lineage, allowing you to trace the origin and progression of any potential threats. Additionally, our solutions enable overall security posture enhancement and lightweight policy deployments.

We understand the importance of real-time protection, which is why we offer continual scanning to identify and address any security vulnerabilities in your cloud infrastructure. With LTIMindtree and Sysdig, you can rest assured knowing that your cloud is secure and protected from potential threats.

Here is how we can help our customers stay protected from cloud threats:

- Mitigating cloud risks by offering our expertise and experience in identifying and analyzing vulnerabilities. By leveraging the CSPM tool's inputs, LTIMindtree provides comprehensive risk assessments, identifies potential threats, and recommends suitable strategies to mitigate these risks effectively.

- With Sysdig, we expand our capabilities to provide end-to-end threat detection throughout the entire cloud fabric. By consolidating CSPM and CWPM, organizations can attain a full understanding of potential threats and proactively address them before they manifest into significant issues. We can also prevent advanced attacks and contain threats in real-time across the cloud fabric.
- Implementing and executing the right security controls for cloud infrastructure. Based on specific requirements and industry best practices, we can design and implement robust security controls to safeguard your cloud resources and data. This may include access management, encryption, intrusion detection systems, and continuous monitoring mechanisms to ensure the highest level of security within their cloud environment.
- Prioritize risk: Not all risks are created equal. Look for effective ways to prioritize risk across workloads, cloud configurations, and permissions. E.g., severity/exploitability.
- Need to see what's there and how it is used to do this properly.
- Leverage runtime insights to determine what is in use and therefore leaves you exposed to vulnerabilities, misconfigurations, and excessive permissions, so teams can focus on the right places to prevent breaches in the first place. (Describe runtime insights for prioritization)

Conclusion

In an era where cyber threats are constantly evolving, businesses must prioritize cloud security. By embracing CNAPP with runtime insights, organizations can stay one step ahead of attackers and maintain a secure cloud environment for their operations. LTIMindtree and Sysdig aim to collaborate with the customers and provide them with the necessary assistance and expertise to address their concerns related to cloud security. By offering our knowledge and resources, we help enterprises proactively manage and mitigate cloud risks and implement the right security controls to ensure the utmost security of their cloud infrastructure. To know more about our CNAPP and CTDR offerings, please feel free to reach out to us at LTIMindtree.CyberResilience@ltimindtree.com.

References:

1. 80% of enterprises will have consolidated security tooling, Gartner Market Guide for Cloud-Native Application Protection Platforms, April 24, 2023: https://www.gartner.com/en/documents/4295099
2. CNAPP (Cloud Native Application Protection Platform), Sysdig: https://sysdig.com/learn-cloud-native/cloud-security/cloud-native-application-protection-platform-cnapp-fundamentals/

About Authors

Peeyush Marwaha

Principal Director, Cybersec Tech Office and CoE, LTIMindtree

Peeyush is a passionate cybersecurity professional with nearly two decades of rich experience in cybersecurity, leading as DU/BU head for cloud security hyperscalers, incubating managed services operations, and building and growing cloud security hyperscalers in startup mode. Peeyush has worked extensively in Strategic Planning, Go To Market, Industry Analyst briefings/response, Presales and Bid Support, Process Management, Service Delivery, Operations, Quality Assurance, and Technical support functions in the cybersecurity domain. In his current role as a senior cloud leader, he spearheads cloud security practice and delivery enablement.

Phil Williams

Senior Vice President, Corporate Development, Sysdig

Phil is responsible for all corporate development, strategic alliances, and global systems integrator (GSI) initiatives at Sysdig, where he leads the team focused on building strategic partnerships across the security, cloud, and Kubernetes spaces. Phil has a passion for developing strategic alliances and ecosystems that deliver true value for both the partner and joint customers, and he has proven this in both startup and large public technology companies.

LTIMindtree is a global technology consulting and digital solutions company that enables enterprises across industries to reimagine business models, accelerate innovation, and maximize growth by harnessing digital technologies. As a digital transformation partner to more than 700 clients, LTIMindtree brings extensive domain and technology expertise to help drive superior competitive differentiation, customer experiences, and business outcomes in a converging world. Powered by 82,000+ talented and entrepreneurial professionals across more than 30 countries, LTIMindtree — a Larsen & Toubro Group company — combines the industry-acclaimed strengths of erstwhile Larsen and Toubro Infotech and Mindtree in solving the most complex business challenges and delivering transformation at scale. For more information, please visit **https://www.ltimindtree.com/**.