LTIMindtree

Point of View

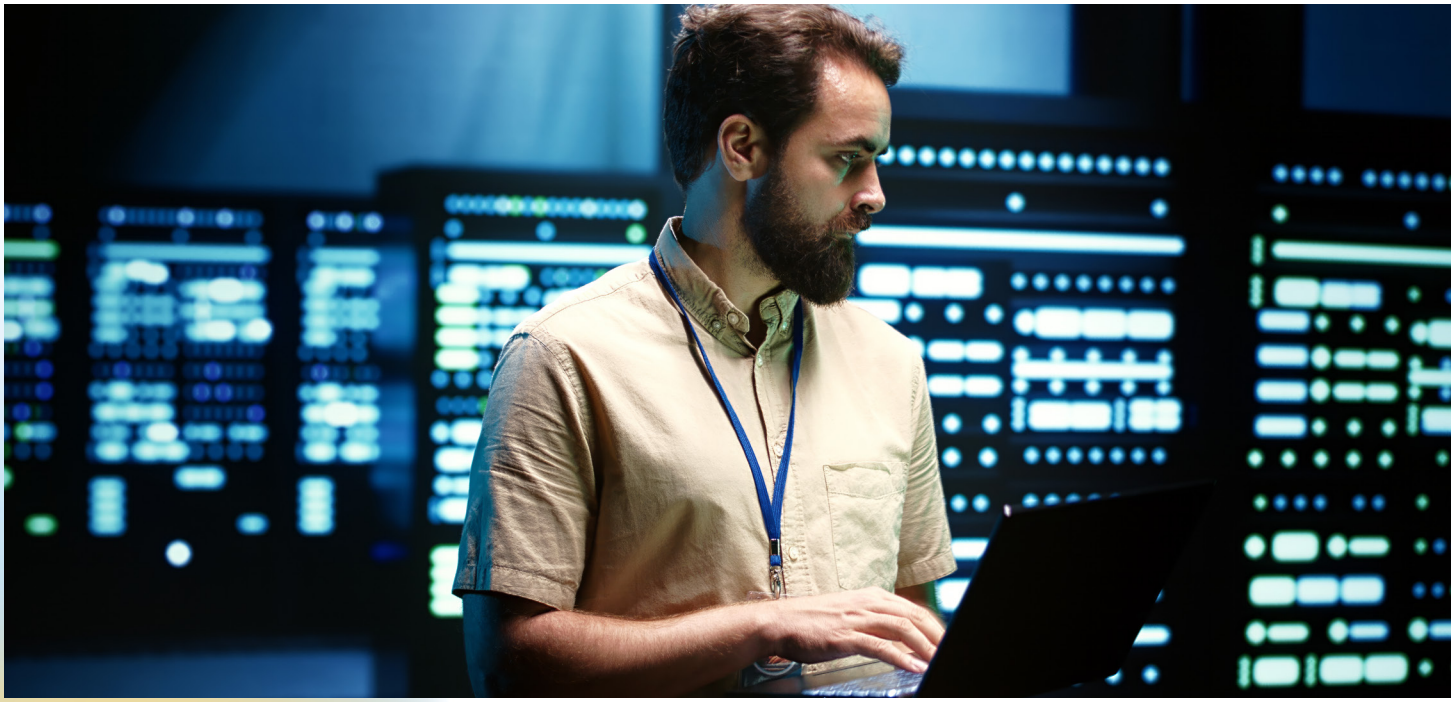
A CISO's Guide to Building an Effective Cloud and Container Security Program

Authors:

Dilip Panjwani | Ravi Kollipara

Today, enterprises of all sizes are leveraging the power of cloud technologies to enable their digital agendas. However, it has become crucial for the Chief Information Security Officers (CISOs) to prioritize the security of these environments. 39% of businesses experienced a data breach in their cloud environment in 2022[1]. Any breach in the cloud environment can have catastrophic consequences, including data loss, reputation damage, and financial losses. As the threat landscape for cloud-related attacks rises, CISO's role becomes more critical.

In today's constantly evolving digital landscape, securing, and proactively safeguarding the cloud against potential threats is essential. **In this POV, we will dive deep to understand how the cloud is shifting security requirements. We will also discuss creating a strong cloud security program to protect the environment.**



Evolving security challenges in the cloud

The concept of cloud computing has advanced significantly and integrating it into business operations has resulted in numerous advantages for companies. As organizations embrace the cloud, they must also consider the new security implications that come with it.

01 Broader target surface and enhanced attack sophistication

The complex and vast cloud infrastructures bring numerous entry points that provide more opportunities to exploit vulnerabilities. This vulnerability exploitation aims to gain unauthorized access to sensitive data or disrupt services. Cybercriminals use sophisticated methods such as cross-account or cross-cloud attacks, vulnerabilities specific to containers and serverless systems, and supply chain attacks.

02 Misconfigurations and human error

As per the latest cloud-native security report from Sysdig2, over 90% of cloud user permissions never get used. Improper configuration of cloud applications or human error could result in unauthorized access and the exposure of sensitive data. A common example of human error in the cloud is the failure to update software components regularly. This may create vulnerabilities that can be exploited by hackers. Similarly, weak passwords make it easier for attackers to access the system.

03 Vulnerability overload

Increased use of open-source technologies accelerates innovation. Statistics show an 80%3 increase in operational support system (OSS) utilization in 2022, which increases the importance of vulnerability testing. Keeping up with the latest updates and patches can be overwhelming for security teams due to the increasing number of discovered vulnerabilities. This problem is compounded by the fact that containers are highly dynamic. It makes it difficult to track which software or image versions are running.

04 Compliance and governance

Ensuring compliance and governance are vital components of maintaining secure cloud and container environments. Organizations must ensure their cloud and container environments adhere to applicable regulations, industry standards, and internal policies. Compliance requirements vary depending on the industry, the type of data being stored or processed, and the location of data.

CISOs, security teams, DevOps teams, and developers must invest time and resources to adapt security to the dynamic nature of the cloud explicitly. This adaptation is essential to address emerging risks without impacting cloud goals. Security done right can help instead of hindering cloud programs.

Tackling cloud and container security with shift left and shield right approach

Cloud security has become a critical concern for enterprises, and there is a growing need to implement robust security measures. **The industry has introduced a wide range of solutions focused on different areas of need:**

- **Cloud Workload Protection Platform (CWPP)**

  A solution designed to protect cloud-based workloads across multi-cloud environments, provide visibility and control over the workload, and detect threats.

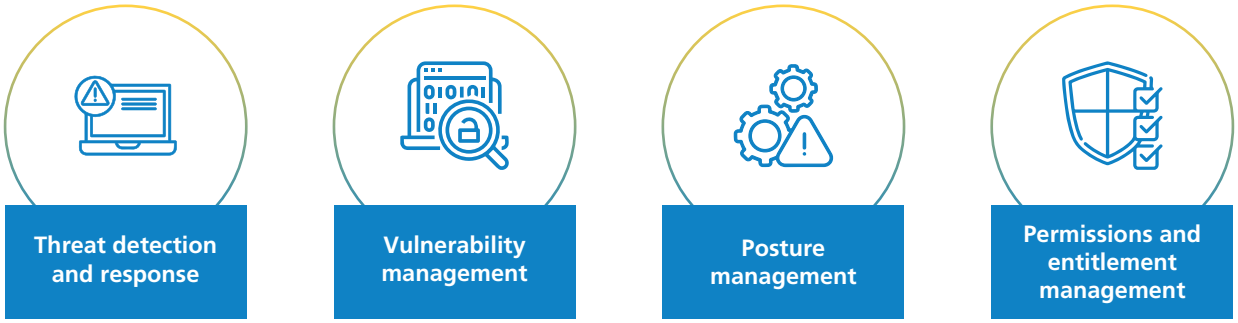
- **Cloud Security Posture Management (CSPM)**

  A solution that assists in identifying misconfigurations within cloud environments and helps maintain desired security posture.

- **Cloud Infrastructure Entitlement Management (CIEM)**

  A solution that manages access privileges within a multi-cloud environment, controlling user permissions and managing service accounts.

These solutions aim to secure different aspects of the cloud. **There is a growing need for a unified platform that fulfills four specific requirements:**



Cloud-Native Application Protection Platforms (CNAPP[4]) seek to unify these capabilities to bring a comprehensive and correlated view of risk to boost effectiveness.

Six goals for an effective cloud and container security program

A comprehensive security plan for cloud environments involves more than just implementing a few tools or solutions. It requires understanding different security threats that impact the cloud and container ecosystem. Additionally, it demands a keen awareness of how those threats can manifest in your organization's infrastructure.

01 Shift left

The shift left approach emphasizes integrating security measures as early as the development phase of the software. Identifying and addressing vulnerabilities in their early stages can prevent them from becoming more expensive and difficult to manage. This methodology enables developers to detect potential threats during the code-writing process in cloud and security programs. The approach saves time by eliminating fire drills to address security flaws after going live.

02 Shield right

Shift left is not enough; shield right is also required to ensure security measures remain effective after deployment. You must defend your production environment. Runtime security for threat detection and response is the safety net to ensure you are aware of malicious activity. It allows you to identify and block zero-day threats that occur unexpectedly in production. Runtime protection becomes more critical for securing containers as container workloads require real-time visibility of what is happening inside. This necessity demands strategic instrumentation to be done effectively.

03 Prioritize risk

To prioritize risk, one must first identify potential hazards, assess their likelihood and impact, and then list them based on severity. It allows the organization to focus on the most significant threats while balancing limited sources. It also involves conducting a comprehensive risk assessment, identifying all vulnerabilities and threats that could affect the organization's cloud or container infrastructure. The evaluation should also consider each threat's likelihood and potential impact. Utilize runtime insights to keep track of application execution and swiftly detect and address security threats as they occur.

04 Facilitate security automation

Instead of manually installing and configuring the software, developers can automatically monitor and manage resources using Infrastructure as Code (IaC). Ensuring the environment's security concerning IaC security involves scanning templates for security issues and using testing frameworks. It also includes using version control to track changes and implementing access controls to limit who can modify the code.

05 Consolidate tools to enable efficient security

Fragmented tools used across cloud environments can complicate coordination, leave visibility gaps, and increase cost. It is crucial to find ways to consolidate such tools without sacrificing security. CNAPP is the tool that allows organizations to consolidate cloud-native security tools, streamline security operations, and enhance the overall security posture. Moreover, it helps enterprises reduce the licensing costs, maintenance costs, and operational overhead associated with multiple security tools.

06 Addressing the skills gap

The need for more skilled cybersecurity professionals is a growing concern for many organizations, impacting risk and slowing productivity. As per the report from Cybersecurity Ventures5, there are currently 3.5 million vacant positions for cybersecurity professionals across the globe. The number of unfilled jobs leveled off in 2022 and remains at 3.5 million in 2023, with more than 750,000 positions in the U.S. To address this issue, leverage solutions that empower your developers while lifting the load. These solutions offer valuable insights that facilitate collaboration, automate repetitive tasks, and aid in prioritizing the overwhelming number of security alerts that require attention. Alternatively, consider evaluating a strong cloud security managed services partner. Such a partner should have the right skillsets and tools enablement to support customers with smooth onboarding and operations management.

Establishing a culture where security is a concern for everyone is important. All employees should be informed about potential security risks and their responsibilities in maintaining the organization's safety.

Conclusion

Adopting cloud technology is becoming necessary for organizations to accelerate innovation. However, this comes with security challenges that must be addressed immediately. As discussed earlier, cloud security has become a critical concern for enterprises. There is a growing need to implement robust security measures. These include cloud workload protection platforms, security posture management, and infrastructure entitlement management. An effective cybersecurity solution enhances the defense mechanism by adopting a strong platform "built for the cloud" like CNAPP. Furthermore, it involves promoting a culture of security among employees. One such solution is provided by our collaboration between Sysdig's container security expertise and LTIMindtree's DevSecOps. This collaboration has resulted in a joint resolution that enables organizations to effortlessly integrate security into their DevOps workflows.

References

01. Cloud assets the biggest targets for cyberattacks, as data breaches increase, Thales Group, July, 5, 2023:
https://www.thalesgroup.com/en/worldwide/security/press_release/cloud-assets-biggest-targets-cyberattacks-data-breaches-increase

02. Sysdig 2023 Cloud-Native Security and Usage Report, Sysdig, 2023:
https://sysdig.com/2023-cloud-native-security-and-usage-report/

03. The 2023 State of Open Source Report confirms security as a top issue, Javier Perez, Voices of open source, January 25, 2023:
https://blog.opensource.org/the-2023-state-of-open-source-report-confirms-security-as-top-issue/

04. What is a CNAPP? Sysdig:
https://sysdig.com/learn-cloud-native/cloud-security/cloud-native-application-protection-platform-cnapp-fundamentals/

05. Cybersecurity Job Report, Cybersecurity Ventures, 2023:
https://cybersecurityventures.com/jobs/

About the authors

Dilip Panjwani

Global Head of the Cybersecurity Technology Office and CoE, LTIMindtree

Dilip has over two decades of experience in leading some of the best cybersecurity practices for large Indian corporations and multinationals. As the Global Head of Cybersecurity Practice and CoE at LTIMindtree, his role involves building state-of-the-art and innovative cybersecurity solutions to transform customers' cybersecurity journey.

Ravi Kollipara

Sr. Director of Alliances, Global Systems Integrators, Sysdig

Ravi has a successful track record of building strategic alliances with the ecosystem of Global System Integrators for technology companies from inception to launching joint offerings. With more than 30 years of experience in various leadership positions, he has worked extensively in networking, storage, data management, security, and cloud-native technologies.