CLOUD NATIVE SECURITY: A BEGINNER'S GUIDE

Cloud native systems empower organizations to build, deploy, and run scalable workloads in dynamic environments.

While such environments support an agile development framework, these also bring a fresh set of security challenges that can't be solved with traditional IT security practices. Though portability, autoscaling, and automation are key features of an efficient cloud native ecosystem, the same features also lead to potential gaps that are susceptible to be exploited by attack vectors.

In this article, we delve into the security landscape of a cloud native system, while exploring the elements and strategies to enforce security in such frameworks.

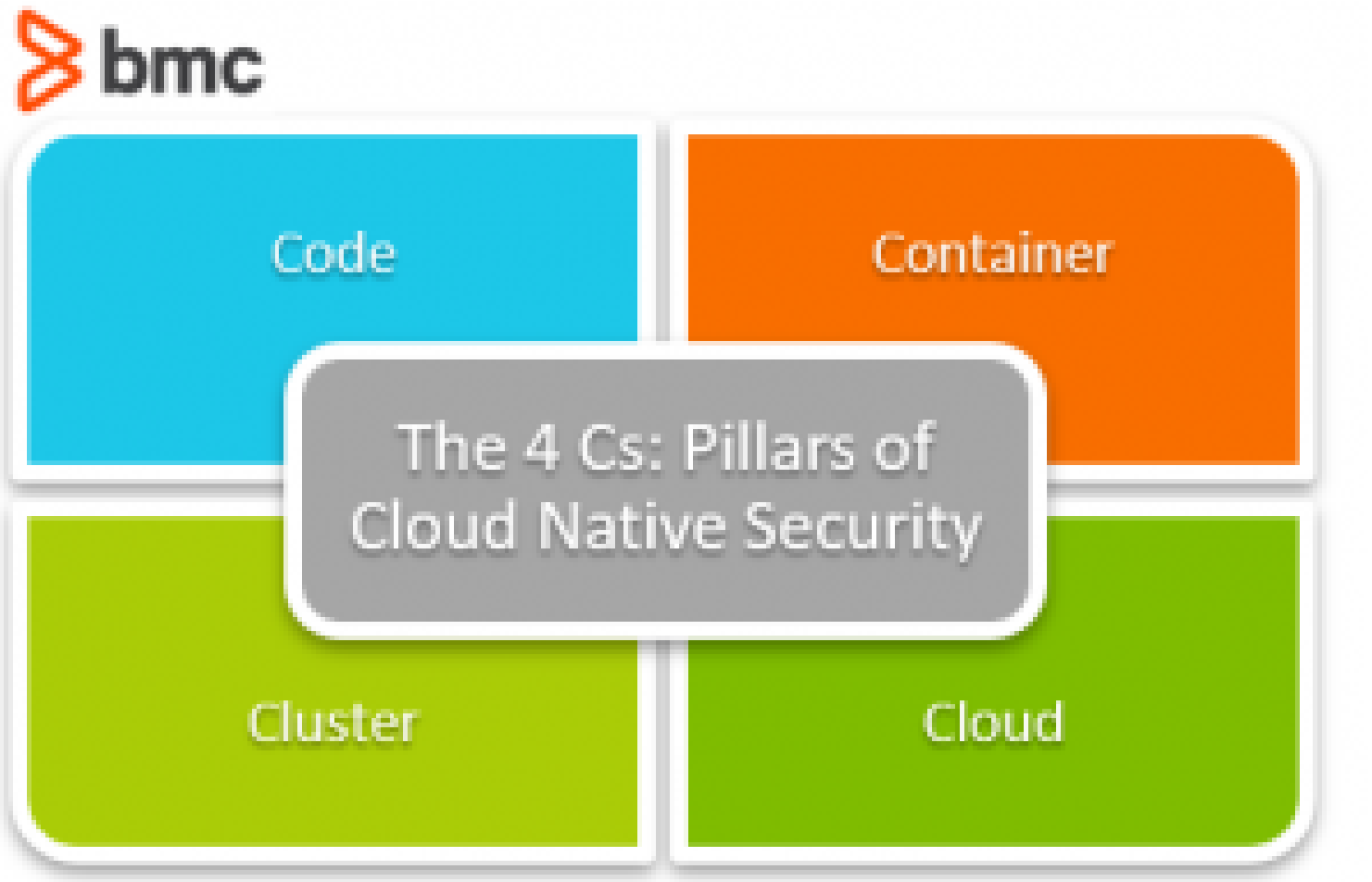
Cloud native security overview

Cloud native applications lack fixed perimeters present in traditional IT. As a result, static firewalls rarely solve their purpose to secure applications that run on multi-cloud, on-premises, or off-premises cloud instances.

The flexible, scalable, and elastic nature of cloud environments additionally reduces the speed and accuracy with which security teams can diagnose security incidents. Combined with these are the rapid delivery and release cycles that make it complex to manage and provision security policies manually.

These factors collectively present challenges that require a non-traditional, focused approach to

mitigate security events of cloud native systems.



Pillars of cloud native security

An effective cloud native security model addresses threats across every level of a workflow—simply remember the 4 Cs:

Code

Analyzing, debugging, and cleaning up source code is the first step to identify and fix vulnerabilities such as Cross-Site Scripting (XSS) and SQL Injection during the build phase of a software development lifecycle (SDLC).

Some commonly used testing mechanisms to securing source code include:

- Static Code Analysis (SCA)
- Dynamic Application Security Testing (DAST)
- Static Application Security Testing (SAST)

Container

Containers host application workloads and are considered one of the most critical elements of a cloud native setup.

It is extremely critical to not only secure application workloads of a cloud native ecosystem, but also to secure the containers that host these workloads. Some common approaches to securing

containers include:

- Minimizing the use of privileged containers
- Strengthening container isolation
- Continuous vulnerability scanning for container images
- Certificate signing for images

(Explore security in Docker & Kubernetes.)

Cluster

Containers running at scale are deployed on physical/virtual machine clusters. A cluster typically includes various components, such as worker/master nodes, control plane, policies, and services.

Securing cluster components commonly require the following practices:

- Administering robust Pod and Network security policies
- RBAC authorization
- Optimum cluster resource management
- Securing Ingress using TLS secure keys

Cloud

The cloud layer acts as the interface that communicates with the external world, including users, third-party plugins, and APIs. Vulnerabilities on a cloud layer are bound to cause a major impact on all services, processes and applications that are hosted within it.

It is extremely critical for security teams to adopt security best practices and develop a threat model that focuses particularly on the cloud infrastructure layer and its components. Some commons practices to secure the cloud layer includes:

- Encrypting ETCD data at REST (Kubernetes)
- Frequently rotating and renewing CA certificates
- Limiting the use of privileged access
- Disabling public access

Key elements of a cloud native security platform

Cloud native security tools have gradually evolved from rudimentary collections of multiple tools and dashboards to well-defined platforms that consider all layers of the ecosystem.

A cloud native security platform (CNSP) focuses on the following elements of a tech stack to administer a comprehensive secure framework:

- **Resource inventory.** The CNSP maintains asset logs in the SDLC and keeps track of all the changes for automatic resource management.
- **Network security** ingests logs of traffic flow directly from the deployment platforms and develops a deep understanding of cloud native firewall rules to scan and monitor network threats.
- **Compliance management** supports different major compliance frameworks to monitor security posture and compliance throughout the cloud framework.

- **Data security** utilizes out-of-the-box classification rules to scan for malware, monitor regulatory compliance, and ensure data compliance across deployment environments.
- **Workload security** secures application workloads by proactively mitigating runtime threats of production instances.
- **Identity & access management (IAM)** administers robust access and authentication framework to secure user accounts as the first line of defense by leveraging multiple third-party tools.
- **Automatic detection, identification & remediation** supports robust threat modelling by utilizing historical data and the existing security landscape of the industry.
- **Vulnerability management** identifies and secures vulnerable points of the entire stack from a holistic standpoint.

Administering cloud native security

The fundamental benefit of leveraging a CNSP to administer security is that it gives organizations the freedom to choose a security stack to suit the organization's specific use case.

Before choosing a CNSP, however, it's important that the organization performs appropriate due diligence to opt for the right strategy and factors in the best practices for a comprehensive robust security framework.

Cloud native security strategies

Cloud native security is typically administered by opting for the strategy that supports the business-to-vendor working model while ensuring comprehensive security across various layers and processes of the tech stack. Some commonly used cloud native security strategies include:

- **The Shared Responsibility Model** leverages the involvement of both the cloud service provider(s) and an organization's in-house security team to ensure application security. This is done by assigning and sharing ownership of maintaining security for individual components of a cloud native framework. Though this model typically gives the advantage of planning the security framework inside-out, it may often get complicated in multi-cloud environments due to variations in component ownership.
- **Multi-Layered Security**, also referred to as the 'defensive depth' approach, involves monitoring all layers of the network to identify and mitigate potential threats individually. The strategy essentially relies on a number of different tools and approaches to counter attacks alongside planning contingency in the event of a compromise.
- **Cloud-Agnostic Security** is commonly used for multi-cloud models by leveraging a common CNSP for multiple cloud service providers. The strategy essentially provisions a single pane of glass of security best practices to be followed by multiple parties and distributed teams to streamline monitoring, compliance, and disaster recovery.

Benefits of cloud native security platforms

Modern CNSPs combine automation, intelligence, data analytics, and threat detection to mitigate security gaps in highly distributed cloud instances. Besides enabling a robust security framework, some additional benefits of adopting a cloud native security platform include:

- **Improved visibility & monitoring.** Cloud native security platforms enable continuous testing across all CI/CD layers, allowing teams to monitor and mitigate security incidents at the component level.
- **Platform flexibility.** By supporting TLS across a multi-cloud and hybrid deployment environment, CNSP allows a platform-agnostic development model.
- **Enhanced backup & data recovery.** Automation enforced by CNSPs enable rapid patch deployments and mitigations of security threats

Cloud native is already here

A Fortinet survey indicates that 33% of surveyed businesses already run more than half of their workloads on the cloud. Out of all the benefits these organizations gain, security continues to be a major challenge they face. In this context, organizations must also realize that most security failures occur due to security misconfiguration—not inherent architectural vulnerabilities.

A Gartner's report validates this by claiming that through 2025, 99% of cloud security failures will be the customer's fault. This exposes the outright failure of organizations to adopt the right practices and tools to mitigate avoidable attacks.

To measure an application's success, security should no longer be an afterthought. It's as critical as scalability and agility.

Related reading

- BMC Multi-Cloud Blog
- BMC Security & Compliance Blog
- IT Security Policy: Key Components & Best Practices for Every Business
- What Is the CIA Security Triad? Confidentiality, Integrity, Availability Explained
- The State of Cloud Security Today