Advanced Cloud Security

Continuous Security Strategies for Cloud Infrastructure

CONTENTS

SAMIR BEHARA
SENIOR CLOUD INFRASTRUCTURE ARCHITECT, AWS

Enterprises are rapidly migrating to cloud-based environments to transform their business and stay competitive. Due to the Covid-19 pandemic, the speed of cloud migrations and digital transformation have drastically increased across all sectors, and significant measures were taken over a short period to support the increase in remote work and collaboration. This caused a rise in the demand for online services, which required more advanced technologies. Unfortunately, this rapid growth in cloud computing has also fueled a steep proliferation in cloud security incidents.

Cyber threats have become more sophisticated. Hence, it's a good idea to utilize the expertise of public cloud providers like AWS, Azure, Google Cloud Platform, Oracle Cloud, IBM Cloud, etc., to better manage assets against security threats. Cloud security is a collection of proactive measures to protect your cloud assets from internal and external threats. This Refcard will walk through common cloud security challenges, continuous security for cloud infrastructure, and advanced strategies for securing cloud workloads.

COMMON CLOUD SECURITY CHALLENGES

As enterprises increasingly adopt cloud technologies, it's crucial to design a secure cloud architecture. If you don't adhere to cloud security guidelines, organizations can expose themselves to cybersecurity threats, resulting in an unwanted impact on cloud infrastructures and workloads. First, let us look at the most common cloud security challenges facing nearly every organization.

ATTACK SURFACE MANAGEMENT

The attack surface is dynamic and continuously changing. As organizations grow, the number of deployed cloud resources increases. Modern infrastructure spins up resources based on demand. As a result, it's challenging to have complete visibility into your cloud resources and other digital assets. The distributed workforce also creates challenges with securing devices across the globe.

Inventory of all the internet-facing resources is required; otherwise, organizations will miss scanning resources for vulnerabilities. Gaps in your monitoring strategy can result in the external exploitation of resources. You can't secure resources that you're not aware of. There are high chances that *attacks happen on unmanaged or untracked resources*. During cyberattacks, hackers primarily target the cloud assets that are exposed to the internet.

RANSOMWARE ATTACKS

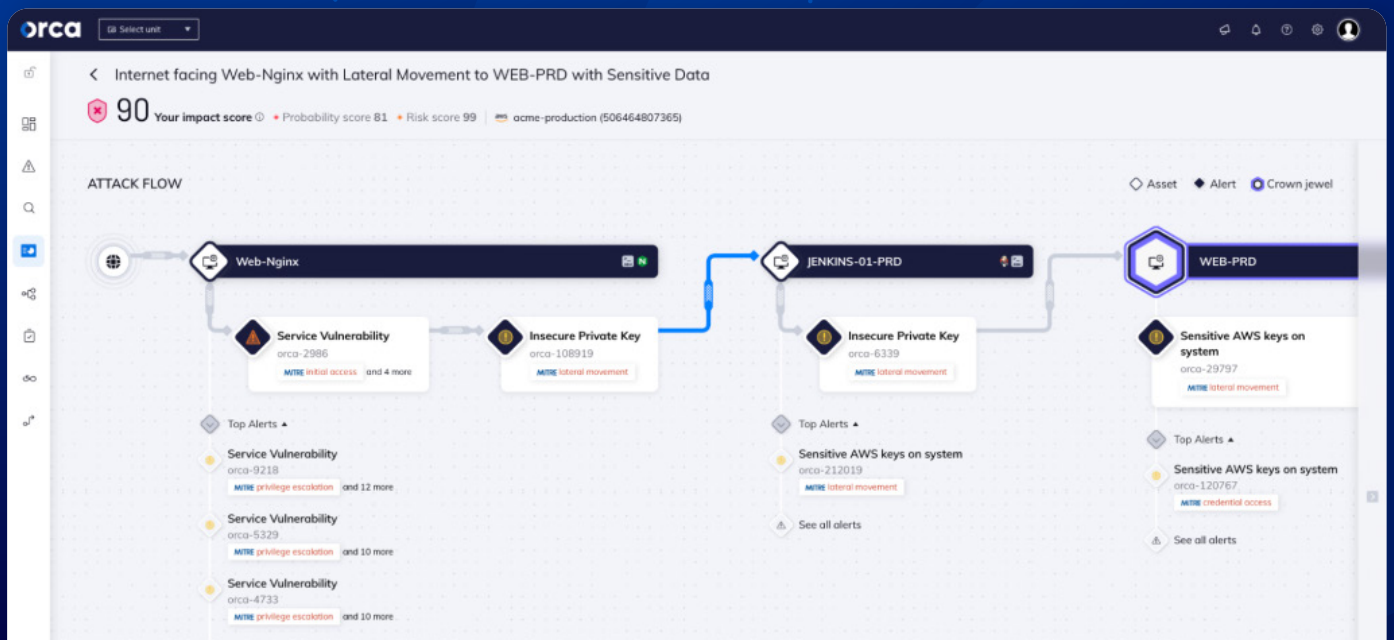
Ransomware is a malware attack that can prevent or limit users from using their systems until a ransom fee gets paid. In other cases, files in your system are locked or encrypted, making them unusable. Ransomware attacks have increased in recent years: The malware target can either be an individual or an enterprise.

orca security

Get a Cloud Security Risk Assessment.

See how easy cloud security can be.

START TODAY



There are two types of ransomware attacks that exploit weaknesses in the security posture:

- **Crypto ransomware** encrypts files on a computer so that the user cannot access the files.
- **Locker ransomware** locks victims out of the computer so that they cannot use it.

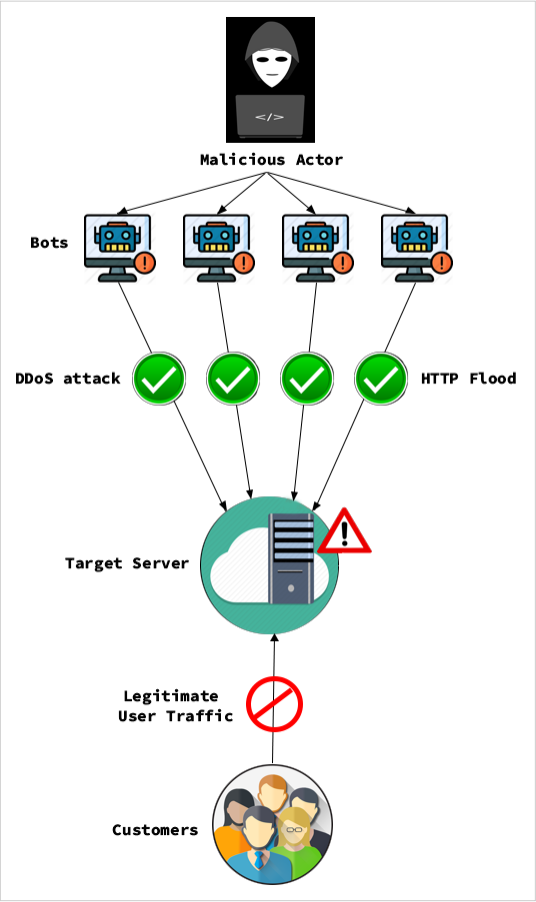
Malicious software gets injected into the system via a phishing attack — e.g., when you get tricked into clicking a link in an email, opening an email attachment, or visiting a malicious site. Infected files are then installed in the target machine, consequently taking control of the resources.

DISTRIBUTED DENIAL OF SERVICE ATTACKS

A DDoS attack is one of the most widespread cyber threats where a large amount of traffic from multiple sources is sent to a service, thus overwhelming the target and negatively impacting behavior. This malicious traffic originates from a single IP address or IP range that consumes all the resources; the legitimate users cannot access the service or see degraded service performance.

DDoS attacks can have various impacts: unhappy customers, revenue loss for the business, damage to an organization's reputation, and loss of productivity. DDoS attacks can be classified into infrastructure layer attacks (SYN floods and UDP reflection attacks) and application layer attacks (HTTP floods and DNS query floods).

Figure 1: DDoS attack in action



DATA BREACHES

Data breaches are one of the top cybersecurity threats as enterprises are rapidly moving to the cloud. Data breaches have impacted organizations of all sizes for many reasons — lack of visibility, gaps in resource monitoring, sensitive information not stored securely, etc.

Data leaks are primarily due to:

- Compromised passwords
- Stolen devices
- Non-compliant resources
- Misconfigurations
- Lack of proper security measures and training

In addition, bad actors can get unauthorized access to critical data via weak or stolen user credentials, unpatched components, and human error. In such scenarios, there is a risk of data being modified and incurring data loss that might be irreversible.

SUPPLY CHAIN ATTACKS

A supply chain attack is a cyberattack targeting a trusted third-party vendor who offers services or software vital to the supply chain. In some cases, cloud-native applications are more susceptible to supply chain threats. For example, anyone can contribute to the development of open-source software solutions. Using this access, hackers can program vulnerabilities into open-source solutions, making it easy to introduce a threat to companies that use the software.

In addition, cloud environments are interconnected, so bad actors try to take advantage of the weakest component in the chain. During such attacks, a ripple effect is created that impacts a broader audience and eventually reaches the victim, who is not the initial target.

CRYPTO-MINING ATTACKS

Cybercriminals are stealing system resources and using this to illegally profit from digital currency mining. They do this by installing a crypto-mining tool on victims' machines and using resources on those systems. As a result, attackers can use the computing power of others without their knowledge or permission, causing a slowdown in device performance.

There are two types of crypto-mining attacks:

1. **Browser-based crypto-mining** injects JavaScript into a website and performs mining activities while a user views the page.
2. **Malware-based crypto-mining** takes over your entire computer and uses the computer CPU to mine coins on your system at a much higher level.

PHISHING ATTACKS

Phishing is a type of social engineering attack where the attacker sends fraudulent email communications that appear to be from a trustworthy source, luring the target to respond to the email. It often results in

stealing sensitive data (credit card information, passwords, access to sensitive files, etc.) or installing malware on the victim's machine. Attackers use this information to steal money, gain confidential data, or access the company's network.

The rise of phishing attacks is a risk to enterprises and has continuously evolved to adopt new techniques. Subtypes of a phishing attack are *vishing* (voice-call phishing) and *smishing* (SMS phishing).

MALWARE ATTACKS

A malware attack is a typical cyberattack where malicious software gets installed on someone's machine without their knowledge. Malware uses various attack vectors that disrupt the standard functionality of the services for cybercriminals to gain unauthorized access to systems and networks. A large number of breaches occur in enterprises with the help of malware. Cloud assets get exposed to the internet and, hence, can assist in spreading malware. Malware takes different forms and attacks in varied ways:

- Viruses
- Trojans
- Adware
- Spyware
- Ransomware

CONTINUOUS SECURITY FOR CLOUD INFRASTRUCTURE WITH DEVSECOPS

Continuous security extends DevOps practices and helps embed security into the application development lifecycle. Let us now understand how to integrate security into the code pipeline, automate the implementation of secure processes into each phase of the DevOps pipeline, and help teams move faster.

DEVSECOPS BENEFITS AND BEST PRACTICES

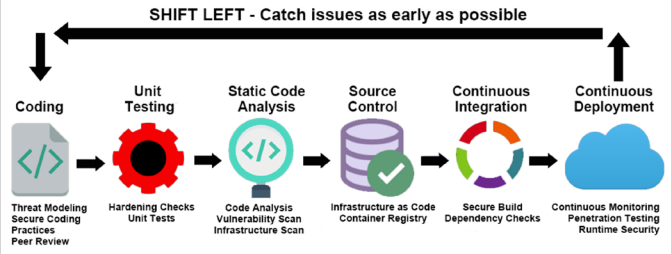
DevSecOps introduces security into the automated CI/CD processes and ensures that security is treated as a first-class citizen. Integrating security into the software development lifecycle empowers developers to build a security mindset and catch vulnerabilities in the code early in the lifecycle. In addition, it ensures that security best practices are followed throughout the CI/CD pipeline and are not an afterthought.

When you're operating in a cloud environment, DevSecOps helps to eliminate silos between development, operations, and security teams. You can leverage DevSecOps tools in your organization to improve the security posture of your application during the development phase. Some key elements for implementing DevSecOps in an organization:

- Static code analysis
- Vulnerability scanning
- Secrets management
- Infrastructure automation
- Container security
- Data protection
- Identity and access management

Figure 2 below demonstrates how you can inject security into the DevOps pipeline and enforce security best practices to be followed from the beginning of the SDLC.

Figure 2: Building security into DevOps pipeline



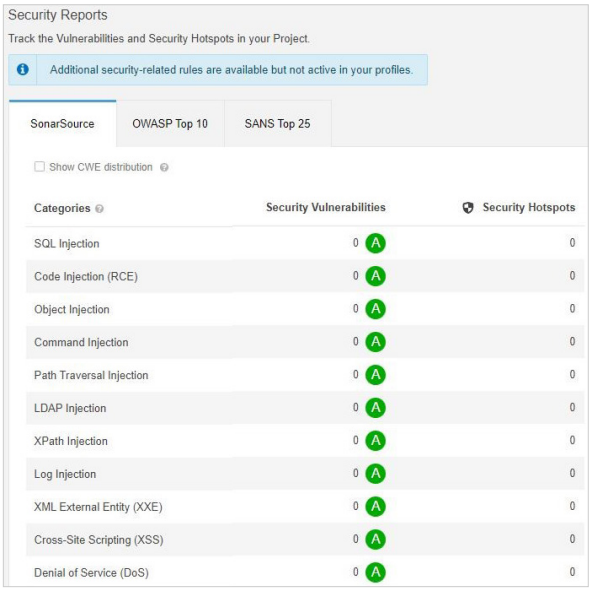
APPLICATION SECURITY TESTING WITH SAST AND DAST

Static application security testing (SAST) and dynamic application security testing (DAST) are testing strategies used to identify security vulnerabilities in the application. These complimentary testing methodologies are part of the software release lifecycle and help the development teams to test and release secure software.

SAST is a white-box testing methodology that requires access to the application source code and gets scanned for vulnerabilities as part of every code commit. You can set up security rules (OWASP Top 10, SANS Top 25, and CWE Top 25), quality gates for your application, and fail your CI/CD pipeline if the code doesn't meet the quality threshold. Developers get early feedback about vulnerabilities and security hotspots, allowing them to take ownership of the issue and fix them before production deployment.

DAST is a black-box testing methodology that requires a running application to test vulnerabilities by sending various types of malicious inputs to the application. These tests mimic a hacker's action and test runtime vulnerabilities like SQL injection and cross-site scripting. Compared to SAST, DAST identifies vulnerabilities towards the end of the SDLC and hence is more expensive to fix security issues.

Figure 3: Scanning codebase for security hotspots



AUTOMATE CONFIGURATION MANAGEMENT USING IAC

Infrastructure as Code (IaC) helps automate cloud resource provisioning through declarative code stored in source control. IaC minimizes configuration drifts across environments since there is no need to apply configuration changes manually. Development teams can be more productive by automating infrastructure deployments and confidently performing reputable deployments. When dealing with complex cloud environments, you can leverage IaC to deploy code that follows the best practices like static code analysis, peer review, and automated testing. You can use various IaC tools to automate the provisioning of resources in your environments.

It's important to treat infrastructure resources like cattle and not pets by following the immutability principle — do not modify the configuration of the existing server; instead, create a new server with the updated configuration.

Figure 4: Infrastructure as Code in action

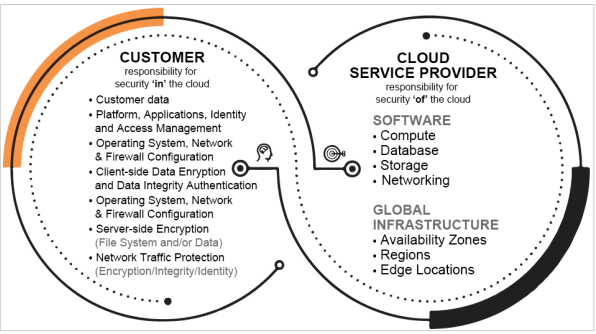
CLOUD COMPLIANCE AND GOVERNANCE

Maintaining security and compliance in the cloud is critical. Your environment is continuously audited and assessed for compliance when building services and deploying them to a public cloud provider. Security is built into the core cloud infrastructure, and safeguards are put in place to protect data privacy. For example, AWS provides a secure infrastructure that supports security standards and complies with many assurance programs across the globe like PCI, HIPAA, GDPR, SOC 1, FedRAMP, ISO 9001, etc. In addition, customers can take advantage of the controls the cloud provider has already implemented, resulting in minimized cost and scope during audits.

SHARED RESPONSIBILITY MODEL

The shared responsibility model can help run workloads securely in the cloud. You can consider it a compliance and security framework where the responsibilities of running workloads in a secured public cloud environment are well understood by the cloud service provider (CSP) and the customer. CSPs are responsible for the security of the cloud, whereas the organizations running workloads are responsible for security in the cloud.

Figure 5: Shared responsibility model



This model encourages close collaboration between the CSP and customer and makes the best use of the expertise of both parties.

The CSP manages the hardware and infrastructure layer, providing enhanced network controls and cloud security. Customers are then responsible for securing the workloads and data run in the cloud, along with configuration and access management.

ADVANCED STRATEGIES FOR SECURING APPLICATION WORKLOADS IN THE CLOUD

Attackers are continuously searching for any weak links to exploit. In this section, let us investigate some of the top strategies for implementing a secure cloud environment.

DATA PROTECTION

Data security and privacy are the top requirements of customers. Any confidential customer data needs to be carefully handled. It takes a long time to build customer trust; hence, protecting critical and sensitive assets is essential.

Customers have complete control of their data in the cloud. They can decide the storage type and geographic regions of the data stores. Excessive permissions are an anti-pattern, and the principle of least privilege should be adhered to. Access to confidential information should be given to people who need it. In general, admin privileges should be closely monitored; if a user account with excessive permissions gets compromised, the risk factor increases.

Cloud providers strive toward being compliant and ensuring customer data protection in ways such as making it easy for users to implement encryption (at rest and in transit) and monitor data processing. Cloud providers have compliance certifications and attestations to satisfy the data privacy requirements of customers around the world.

For example, the General Data Protection Regulation (GDPR) privacy law protects the personal data of European Union residents. Cloud providers make it easy for you to run workloads in the cloud under the GDPR guidelines.

VULNERABILITY MANAGEMENT

It is crucial to discover vulnerabilities quickly and remediate them with high priority. As a good practice, ensure that your resources are continuously evaluated for compliance. Cloud providers offer many tools to gain in-depth visibility into your resources. It allows you to monitor the workloads, accounts, resources, and data for malicious behavior. Vulnerability management needs to be automated and performed at scale.

In the cloud, you have access to managed services that can automatically discover your workloads, continuously scan them for vulnerabilities, and provide real-time findings for remediation. In addition, you can scan the container images and handle vulnerabilities easily in a multi-account environment.

IDENTITY AND ACCESS MANAGEMENT

Amidst today's remote work culture, the need for remote access to cloud environments has increased too. From a security perspective, it's critical to authenticate the user's identity and define the user's privileges in cloud environments.

Managing identities and permissions for humans/services in the cloud is challenging. It is critical to have the proper guardrails that prevent unauthorized access to sensitive information. You should also continuously review the permissions in your environment to ensure adherence to the principle of least privilege.

Creating fine-grained permissions to resources and enabling multi-factor authentication is a step in the right direction. In a multi-account environment, having the ability to establish centralized policies to enforce preventive guardrails is beneficial.

KUBERNETES SECURITY

Organizations are rapidly embracing microservices and containers to drive their cloud-native architectures. Kubernetes is the most popular open-source container orchestration solution. Securing the container deployment pipeline and deployment environment is important. Use trusted images from reliable registries and scan the container images for vulnerabilities.

It is good practice to start with a minimal base image to help with portability and better performance. You should also have continuous monitoring of your containerized applications. Administrator access to the Kubernetes cluster should be limited, and role-based access control (RBAC) for regulating users' access to the cluster is strongly recommended.

Figure 6: Kubernetes cluster monitoring

THREAT DETECTION

The public cloud is exposed to new threats, causing challenges from a security standpoint. Managed services in the cloud provide in-depth visibility, continuous monitoring, and intelligent threat detection.

For organizations to handle threats optimally, the ability to parse logs in real-time, identify suspicious activity, and alert teams about malicious behavior is critical. CSPs allow you to monitor cloud environments for anomalies and unusual activities using machine learning algorithms. This allows teams to detect suspicious network-based activities like ransomware, DDoS, Trojan horses, etc., and remediate threats early with automated responses.

IMPLEMENTING SECURITY BEST PRACTICES IN THE CLOUD

Cloud-native security ensures that security principles are embedded into the workflows of modern organizations using the right tools. This section explains core cloud security concepts and implementation details.

CLOUD MISCONFIGURATIONS

Misconfigurations in the cloud are the most common cause of security breaches. These simple misconfiguration issues can be avoided by:

- Proactively monitoring solutions that scan environments for vulnerabilities
- Granting scoped access to resources
- Deploying code via pull request automation
- Abiding to baseline security policies
- Educating team members about cloud threats

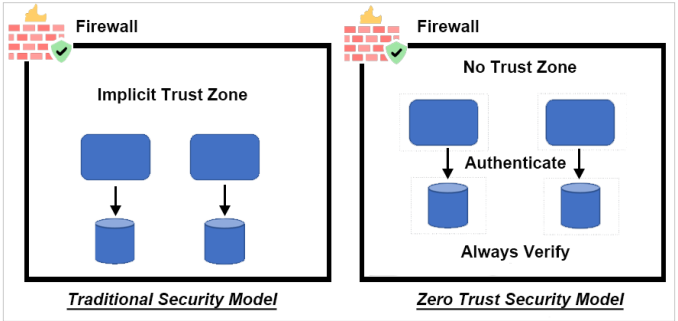
SUPPLY CHAIN SECURITY

Third-party libraries can introduce vulnerabilities into your application stack. Ensure that you're using the latest version of the third-party libraries or frameworks. You should have a strategy to periodically scan and monitor the codebase for vulnerabilities. A consolidated list of all third-party libraries in use — and complete visibility into your supply chain — is critical.

ZERO-TRUST ARCHITECTURE

Zero trust is a security model that minimizes the risk of digital transformation and moves away from traditional perimeter-based security. Under this model, you should not implicitly trust anything inside an organization's network or cloud environment. If any malicious users can get into the network, they can access every resource. Instead, enforce principles to authenticate and authorize requests, follow the least access privilege model, and segment the network to minimize the potential blast radius.

Figure 7: Traditional security vs. zero-trust security



MALWARE AND PHISHING PROTECTION

Don't share sensitive personal information like usernames, passwords, bank information, or credit card details over email, phone, or text messages from unknown sources. Do not click on links in unsolicited emails or download attachments to your local machine.

Having an antivirus application scan downloaded documents is necessary. Be aware of the various phishing techniques and conduct security training programs for employees.

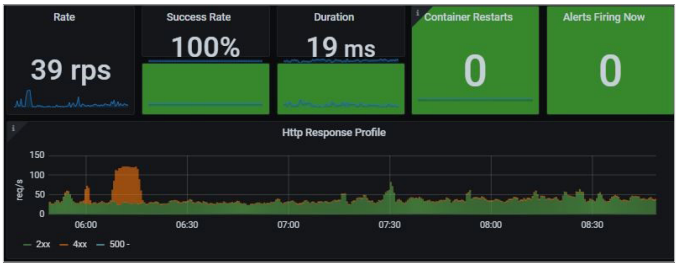
SECRETS MANAGEMENT

It's critical to manage secrets like passwords, API keys, SSH keys, certificates, database credentials, and encryption keys across your IT landscape. You must ensure that the sensitive information is accessible only to trusted entities and enforce strict password policies and rotate your passwords regularly. Don't hardcode secrets in application code stored in source control or use shared credentials.

CLOUD INFRASTRUCTURE VISIBILITY

Teams should have quick access to centralized logs for investigating performance and security issues — network logs, audit logs, performance logs, etc. Cloud services provide anomaly detection to detect common threat vectors and send real-time alerts. In a complex multi-cloud or hybrid environment, it's necessary to have the asset inventory and insight into the health of the resources. You should have observability tooling in place for monitoring cloud resources at scale.

Figure 8: RED metrics for monitoring microservices



DATA BREACHES

Many breaches occur due to human error, in which a bad actor gains access to the entire application landscape. It's therefore best to limit access to data, especially sensitive data.

You should encrypt confidential data using symmetric or asymmetric encryption. Keep monitoring in place and send notifications when you encounter anomaly behavior. It's also essential to have automated backups enabled for your database to recover critical data during adverse scenarios.

COMPLIANCE AS CODE

Organizations must comply with various regulatory frameworks, so compliance is a crucial functionality. You should have a strategy to detect and delete non-compliant infrastructure. Consider adding metadata to resources in the form of tags or labels to classify the resources. Use service control policies to enforce security guardrails.

CONCLUSION

Cloud-native architectures are growing quickly, and the dynamic environments amongst microservices, containers, and Infrastructure as Code make security challenging. The "shift-left" security approach requires collaboration between the development, security, and operations teams to improve the security posture of the workload.

Catching vulnerabilities at an earlier stage is less expensive and increases overall delivery speed. However, delaying the security review until the deployment time is a big risk. As you start embracing the shift-left strategy in your organization, ensure that security controls are automated and that teams adopt close collaboration and communication.

WRITTEN BY SAMIR BEHARA,
SENIOR CLOUD INFRASTRUCTURE ARCHITECT, AWS

Samir builds software solutions using cutting-edge cloud-native technologies. He has worked on large-scale enterprise applications involving complex business functions, web integrations, cloud migrations, and data management in various domains like manufacturing, insurance, and publishing. Samir is a frequent speaker at technical conferences and is the Organizer of the Steel City SQL Server user group, Birmingham. He is also the author of samirbehara.com.

DZone
600 Park Offices Drive, Suite 300
Research Triangle Park, NC 27709
888.678.0399 | 919.678.0300

At DZone, we foster a collaborative environment that empowers developers and tech professionals to share knowledge, build skills, and solve problems through content, code, and community. We thoughtfully — and with intention — challenge the status quo and value diverse perspectives so that, as one, we can inspire positive change through technology.