INTEZER

Security Features of the Big 3 Cloud Providers

This is the final installment in our five-part series on cloud security. In Part 1 we focused on how to develop a security strategy and identify the right controls for your workloads in the cloud. We looked at how a well-balanced security strategy reduces the attack surface while efficiently detecting and responding to breaches in runtime. Successful application of this strategy depends on the security controls and solutions that help implement them, whether cloud-native or third party.

To better understand these tools, in earlier parts of this series we looked at the different security solutions offered by the three largest cloud service providers—AWS, Azure, and GCP.

In our final part of this series, we'll compare the controls provided by the Big 3. This will provide you with a single point of reference as you define your cloud security strategy for workloads across different clouds.

Cloud Security Controls and Categories

There are several controls available to help you implement a security strategy suited for your cloud workloads. They include:

- Network security
- Vulnerability management
- Cloud Workload Protection Platforms (CWPP) with runtime and Linux threat management capabilities
- Cloud Security Posture Management (CSPM)
- SIEM capability
- Additional threat detection and monitoring capabilities

Refer to Part 1 for a detailed discussion on these security controls.

The majority of these controls can be implemented using native services in AWS, Azure, and GCP. There are a few capabilities, like runtime protection and Linux threat detection, that can be augmented through third party solutions. We will compare the capabilities of the different cloud platforms below for each control.

For more detailed information about their services, you can always refer back to our blogs on:

AWS

Network

Control	AWS		
Network segmentation	- Virtual Private Cloud (VPC) - Security groups and network access control lists (Network ACLs)	- Virtual Network (VNet) - Network Security Groups (NSG) - Application Security Groups (ASG) - Azure Firewall	- Virtual Private Cloud (VPC) - Firewall rules - Network policies for containers
Web Application Firewall	- AWS WAF	- Azure WAF	- Google Cloud Armor
DDoS protection	- AWS Shield	- Azure DDoS protection	- Google Cloud Armor

Table 1: Network security controls offered by AWS, Azure and GCP

Cloud Security Posture Management (CSPM)

Control	AWS		
CSPM (Enforces security configuration on cloud workloads like VMs and databases and monitors posture of workloads against security baselines)	- AWS Config - Amazon Inspector - AWS Security Hub	- Azure Security Center	- Security Command Center

Table 2: CSPM controls offered by AWS, Azure and GCP

Vulnerability Management

Control	AWS		
Patch management	- AWS Systems Manager Patch Manager	- Azure Update Management	- OS patch management
Runtime vulnerability scanning and management	- Amazon Inspector	- Azure Security Center vulnerability assessment	- Cloud Security Scanner

Table 3: Vulnerability management controls offered by AWS, Azure and GCP

Cloud Workload Protection Platform (CWPP)

Control	AWS		
Runtime protection	• Native CWPP not available, leverage third party tools like Intezer Protect	• Microsoft Defender • Add security for Linux workloads and protect from in-memory malicious code through third party solutions like Intezer Protect	• Leverage third party tools like Intezer Protect for workload-centric security and runtime protection
Hardened VMs	• Native hardened VMs aren't available, use CIS Hardened Images	• Native hardened VMs aren't available, use CIS Hardened Images	• Shielded VMs

Table 4: CWPP controls offered by AWS, Azure and GCP

Container Security

Control	AWS		
Image scanning	• ECR image scanning	• ACR container registry image scanning	• Container Analysis Service
Container environment protection	• Standard K8s security features: IAM, security groups, RBAC, network policies • Requires third party tools for runtime scanning and vulnerability management	• ASC container environment protection	• Trusted Image deployment through Binary Authorization

Table 5: Container security controls offered by AWS, Azure and GCP

Security Information and Event Management (SIEM)

Control	AWS		
SIEM (Aggregates data from multiple sources and delivers security insights)	• Some SIEM-like features provided by Security Hub but no native SIEM tool • Recommended to integrate with third party tools for SIEM capability	• Azure Sentinel	• Integration with Chronicle Detect to analyze telemetry data

Table 6: SIEM controls offered by AWS, Azure and GCP

Additional Threat Detection Capabilities

Control	AWS		
Cloud account-level threat detection (Monitor administrative activities and accurate detection of threats at cloud account level)	• Amazon GuardDuty	• Azure Security Center threat protection	• Event Threat Detection

Table 7: Additional threat protection offered by AWS, Azure, and GCP

Security Logs and Monitoring

Control	AWS		
Security logs and monitoring	• CloudWatch Logs • CloudTrail • VPC Flow Logs	• Azure Activity logs • Azure AD logs • NSG flow logs	• Cloud Audit Logs

Table 8: Security logs and monitoring offered by AWS, Azure and GCP

Conclusion

AWS, Azure, and GCP all offer tools and services to help you apply important security controls. These tools are recommended for ease of integration, support, and manageability.

Evolving threats in the cloud, however, demand more sophisticated tools to augment your security. This is especially important for Linux threat detection, unauthorized code execution, and in-memory exploits. Intezer Protect can be used along with native security tools and services to ensure you're running only trusted code round-the-clock.