Cloud Security: Focus on Six Main Control Areas

By Dave Shackleford, IANS Faculty

The Takeaway

Trying to tackle all possible security controls in the cloud is a daunting endeavor. This report explains how focusing on six key control areas (workload security, logging/monitoring, network security, data protection, cloud-native guardrails and identity management) helps ensure security teams get a solid head start in the cloud.

The Challenge

The security team for a healthcare organization wants to ensure it follows the most important, foundational security practices for the cloud. Specifically, the team asks:

- What are 10-20 things that must absolutely be done to secure the cloud?

1. Secure the Workloads

Workload security in the cloud can cover traditional servers, containers, container orchestration services and serverless functions. General best practices for workload security include:

- **Centralize vulnerability scanning services and endpoint security products**. Tools that work in numerous cloud environments and report back to a central console are ideal for updating monitoring dashboards and processes. In addition, new cloud workload protection platforms (CWPPs) use a combination of network segmentation, system integrity protection, application control, behavioral monitoring, host-based intrusion prevention and optional anti-malware protection to protect cloud workloads from attack. These products offer zero trust and micro-segmentation capabilities, as well as endpoint detection and response (EDR) functionality. Whether you choose a CWPP or not, ensure you have endpoint protection for traditional server workloads.

- **Build images using industry standards**: Use well-known hardening guidance from organizations like the Center for Internet Security (CIS) to lock down containers and traditional workloads.

- **Minimize workload network exposure**: Ensure any applied security groups or network security groups (NSGs) are properly locked down and don't allow access from the internet unless intended.

- **Consider a third-party for container, Kubernetes and serverless security**: Evaluate providers that can cover container security (runtime and image scanning), orchestration controls and monitoring for services like Kubernetes, and serverless scanning and monitoring. Attempting to cover this with only cloud-native services and controls can be extraordinarily challenging.

2. Implement Cloud Logging and Monitoring

For cloud logging and monitoring, consider:

- **Cloud security posture management (CSPM).** For larger cloud deployments and any multi-cloud scenarios, CSPM tools and services can continually assess and report on the state of cloud environment configuration and security. Key features to look for include:
    - **Configurable and automated remediation capabilities:** Ideally, any discovered issues should be remediated automatically or with minimal manual intervention.
    - **Custom policy and rules engine enforceable across multiple clouds:** The granularity and flexibility of a policy engine is one of the most important features for any CSPM solution. Policies must properly and accurately assess cloud service provider settings and asset configuration.
    - **Integration with DevOps pipeline stages and tools:** A CSPM platform should ideally be able to integrate and monitor any code or image repositories, build tools, etc.
    - **Detailed and configurable reporting:** Because CSPM is really a monitoring tool at heart, reporting is critical.

- **Cloud-native logging**: Turn on services like CloudTrail in Amazon Web Services (AWS), Azure Activity log and Azure Monitor in Azure, and Stackdriver in Google Cloud Platform (GCP) to record all API calls made within the control plane.

- **Cloud-native monitoring services**: Any infrastructure-as-a-service (IaaS) cloud environment is likely to offer additional monitoring services and capabilities that may provide security control insights, offer alerting and tracking of events and integration with APIs and automation capabilities for event-driven response.

- **Network flow logs**: All major IaaS clouds offer network flow logging (VPC Flow Logs in AWS and GCP, NSG Flow Logs in Azure). These should be sent to a central storage and analysis engine.

3. Focus on Network Security

Network security options are plentiful in modern cloud environments today. To get started:

- **Logically segment subnets:** Use subnet design to control and corral network traffic as you normally would in your own environment.

- **Control routing behavior:** Cloud routing is a major factor in shaping network data pathways (although much more simplistic than most internal routing models) and needs to be carefully controlled.

- **Enable dedicated circuits:** Implement dedicated network circuits like AWS Direct Connect, Azure ExpressRoute and GCP Cloud Interconnect to your internal network as needed (forcing tunneling back to on-premises assets). This will provide some protection from network traffic exposure on the internet.

- **Consider virtual network appliances:** For most organizations, cloud-native firewall and intrusion prevention services (IPS) like Azure Firewall and AWS Network Firewall are less than adequate in terms of features and efficacy. IANS recommends looking at traditional next-gen firewall (NGFW) and IPS vendors for network security gateways as virtual appliances in large cloud deployments.

- **Deploy a perimeter network security zone:** Define a specific virtual private cloud (VPC) or VNet that all network traffic passes through to control network security functionality.

- **Optimize uptime/performance**: Service-level agreements (SLAs) and availability design are critical (as they are for any network). Use load balancing and different availability zones to control redundancy and uptime.

- **Disable Remote Desktop Protocol (RDP) and Secure Shell (SSH) to workloads**: Reducing the exposure surface of cloud workloads is a critical element of network security design, and remote management access is something that should always be reviewed carefully before enabling.

- **Implement IPsec**: IPsec tunnels can be implemented for point-to-point encryption between cloud environments and on-prem gateways.

4. Establish Data Security

One advantage of cloud storage is a new plethora of easy-to-implement encryption and other data security controls and services. Consider the following:

- **Import your own encryption keys to the cloud** versus using the automatically generated keys from the provider. This may afford you more flexibility and control over cryptographic algorithms in use and key lifecycle.

- **Enable key rotation practices** on a regular cadence.

- **Implement cloud-native backup, archival and recovery options for cloud storage** where available. Most major cloud providers offer a plethora of controls and services in these areas.

- **Consider cloud data loss prevention (DLP) and data discovery/classification services**: Services like Amazon Macie, Azure Information Protection and Google Cloud DLP can help to monitor and track data within cloud environments, but they may take time to enable and configure.

5. Get Guardrails in Place

The concept of “guardrails” in cloud security can mean many things, but usually indicates automated controls that perform monitoring, detection and response actions in the cloud. Many more advanced use cases and controls can be implemented, but sound starting points include:

- **Enable cloud-native monitoring and reporting**: The major IaaS providers all offer native services that can monitor the environment for security threats and unusual behaviors, alert and integrate with other security controls and processes, and provide some measure of reporting for analysts. These include Security Center in Azure, Security Command Center in GCP and GuardDuty or Security Hub in AWS.

- **Implement infrastructure-as-code (IaC) templates**: While not strictly a guardrail, IaC templates like Azure Resource Manager (ARM), AWS CloudFormation or HashiCorp Terraform can be used to implement controls and maintain them in a consistent fashion by reverting any detected changes to match the intended template definitions.

6. Configure IAM

While identity and access management (IAM) is a huge topic, some general best practices to consider include:

- **Centralize your identity management**: Having identity management spread out across too many tools and technologies can lead to weak privilege assignment and other configuration issues.

- **Enable single sign-on (SSO)**: SSO is a great way to accommodate user accounts that need access to multiple applications and assets.

- **Define password policies**: Passwords should be carefully defined and controlled for all cloud IAM and RBAC users.

- **Enforce multifactor authentication (MFA) for users:** MFA should be enforced for all cloud admins and engineers if possible (as well as end users, ideally).

- **Use defined policies for IAM and role-based access control (RBAC):** Leveraging defined roles and privileges within AWS, Azure or GCP can help improve security with a least privilege model. Assess all policies for excessive privileges regularly.

- **Control locations where resources are created using IaC templates with policy conditions:** Resources should only be allowed in approved regions and areas.

Cover Your Bases in the Cloud

Cloud security can get complex fast. Focusing initially on securing six key areas – workloads, logging/monitoring, network, data, guardrails and IAM – ensures your cloud initiatives get built on a strong, secure foundation.

Further Reading

IANS Cloud Security Update: Q1 2021, April 8, 2021

Set a Basic Foundation for Cloud Security, Sept. 15, 2020

Security-as-Code: Best Practices and Vendor Options, Jan. 12, 2021

Cloud Security: What to Expect in 2021, Dec. 29, 2020

Cloud Container Scanning Tools: A Market Overview, Oct. 10, 2020

Gauge the Viability of the CSPM Space, Aug. 14, 2019

Any views or opinions presented in this document are solely those of the Faculty and do not necessarily represent the views and opinions of IANS. Although reasonable efforts will be made to ensure the completeness and accuracy of the information contained in our written reports, no liability can be accepted by IANS or our Faculty members for the results of any actions taken by the client in connection with such information, opinions, or advice.