GCP Security Checklist for 2023 and Beyond

GCP is regarded as one of the leading cloud providers, accounting for around 8% of the market. Google operates dedicated data centers in over 200 countries worldwide. When customers use a console or an API to spin up computing, storage, network, and security capabilities, they benefit from this worldwide network of cloud regions. Furthermore, these infrastructure technologies apply in various scenarios, including Google's public, hybrid, multi-cloud, and edge-cloud environments.

GCP security or Google Cloud Platform security is a set of tools and services designed to protect customers' data and applications. It includes a variety of security measures, including access control, authentication, encryption, and data loss prevention. It aims to offer a detailed insight into the security of cloud-based applications and visibility and control over network traffic.

Google Cloud security provides shared resources and data to multiple users and organizations. Without proper security measures, the data and resources can be vulnerable to malicious activity, including hacking, theft, and unauthorized access. Moreover, public cloud providers may not have the same security practices as an organization's internal IT team, making it even more critical to ensure that proper security protocols are in place.

Below is a GCP security checklist that businesses must adhere to when using Google Cloud Services.

#1 Define Workload Identities and Manage Account Impersonation

Managing user accounts is vital in GCP to ensure that only authorized users can access sensitive data or services. This helps to mitigate the risk of data breaches or unauthorized access.

Here's a checklist that will ensure access for only authorized users:

Leverage the Best Practices in Google Cloud Identity and Access Management (IAM)

Google Cloud IAM is a security process that allows organizations to define user roles, assign and manage user permissions, and define authentication and authorization protocols for users to access their resources.
Here are some of the best practices in GCP IAM:

- Make sure no project-level IAM member is assigned Service Account User or Service Account Token Creator roles.
- Use GCP IAM Recommender, a machine learning-driven policy tool. It analyses the IAM logs over 90 days and recommends what policies you should remove.
- Have corporate login credentials, not personal accounts.
- Don’t associate any API keys to your GCP projects.
- Enable Multi-Factor Authentication (MFA) for GCP user accounts.
- Limit GCP IAM primitive roles to within Google Cloud projects.

Use strong passwords and two-factor authentication

Strong passwords and two-factor authentication (2FA) are important tools for protecting user credentials. By enabling 2FA, you can require users to enter a code sent to their mobile phone or email address each time they log in.

Store and encrypt credentials with Key Management Service

Cloud Key Management Service (KMS) is a service that allows you to encrypt and store user credentials securely. By encrypting user credentials before they're stored in the cloud, you can ensure that they are only accessible to authorized users.

It protects data in transit, as it is sent between GCP services and the user. It ensures that data stored in GCP is secure and can only be accessed by authorized personnel.

Monitor activity with Cloud Audit Logs and Access Transparency

A knowledge of **Google Cloud Logging and Monitoring Essentials** is fundamental to a safe and secure cloud experience.

Cloud Audit Logs allow you to monitor user activity on GCP resources and take action if suspicious activity is detected. You can also use Access Transparency, a GCP security tool that provides detailed logs of all access attempts to GCP resources. It includes detailed information about each access request, including the time, the requesting user, and the action taken.

Use Cloud Identity-Aware Proxy (IAP)

Cloud IAP is a service that provides an additional layer of security for user credentials. IAP allows you to control access to applications and services based on user identity.

By having a comprehensive user access management system in place, organizations can ensure that only authorized users have access, and they can minimize the entry of threat actors that can jeopardize data security.

#2 Use Private Networks

Using private networks for GCP security can help organizations protect their data and resources from malicious activity and unauthorized access. Private networks create a secure boundary around the resources and services hosted in the cloud, allowing organizations to control who can access and manipulate the data and how.

It can benefit organizations subject to compliance regulations, as private networks help ensure that all data is kept within the organization's control and meets the necessary security requirements.

#3 Configure Firewall Rules

Firewalls are the first line of defense against malicious activity and unauthorized access. They help protect GCP resources by allowing only authorized traffic from known IP addresses to access GCP resources.
They also help block malicious traffic from entering GCP services.
In GCP Security, you can create two types of firewall rules: ingress rules and egress rules.

- An **ingress firewall** is a network security system that controls incoming network traffic by monitoring and blocking malicious traffic.
- An **egress firewall** is a network security system that controls outbound traffic by monitoring and blocking malicious traffic.

GCP security firewall rules should be configured to allow only the traffic necessary for services to function properly. All other traffic must be denied. When configuring GCP security firewall rules, consider the source, destination, port, and protocol. Regularly review and audit firewall rules to ensure they are up-to-date and secure.

#4 Enable VPC Flow Logs

VPC flow logs are an important security tool for GCP because they provide visibility into the network traffic flow within a VPC. Flow logs capture information about the source and destination IP addresses, ports, protocol, and the number of bytes and packets sent and received.
The data provided by VPC flow logs can be used to detect anomalies and malicious activity, monitor compliance with security policies, detect malicious IP addresses, and more. They can also be used to troubleshoot network issues and optimize performance.

#5 Deploy Security Scanning and Analysis Tools

Security scanning and analysis tools are essential in GCP to ensure the security and privacy of data stored in the cloud. These tools help to identify potential vulnerabilities that may expose sensitive data or cause security breaches. They ensure compliance with regulatory requirements and corporate policies, help detect malicious activity and intrusions, and investigate security incidents.

- **Utilize the Security Command Center:** This comprehensive security management platform allows monitoring, detecting, and responding to threats across the Google Cloud Platform. It can identify potential vulnerabilities, detect malicious activity, and take corrective action. It also provides access to security analytics and compliance reporting.

- **Leverage Container Analysis:** GCP Container Analysis offers 2 kinds of OS scanning possibilities to weed out vulnerabilities in containers. First one. On-Demand Scanning API manually scans container images for vulnerabilities, both locally on the computer and remotely in the Container or Artifact Registry. And the other one, Container Scanning API automates vulnerability detection by scanning every time an image is pushed to Container or Artifact Registry. Implementing this API enables language package scans for Java and Go vulnerabilities.

- **Use Cloud Security Scanner:** This is a GCP security tool that scans applications and GCP resources for common security vulnerabilities. The Security Command Center configures Cloud Security Scans. Managed scans run automatically once a week and detect/scan public web endpoints. They don't use authentication and send GET-only requests, minus any form submission on live websites. Use managed scans to centrally manage web application vulnerabilities for projects without involving individual project teams.

- **Leverage Cloud Data Loss Prevention (DLP):** Cloud DLP is a GCP security tool that helps you protect sensitive data. It can detect, classify, and protect sensitive data in GCP, including text, images, and other files.

- **Utilize Cloud Security Baseline:** Cloud Security Baseline is a GCP security tool that helps you ensure that your GCP resources are configured to meet security best practices. It provides a set of security best practices and a framework for evaluating and monitoring the protection of your GCP environment.

Thorough knowledge of **Google Cloud Storage Security Essentials** ensures fortified cloud protection and saves you time and resources in resolving security concerns.

#6 Use OS Patch Management

Use the GCP OS Patch Management to implement OS patches across Compute Engine VM instances (VMs) to ensure they remain periodically updated and safeguarded against vulnerabilities and defects. There are 2 distinct components to OS Patch Management:

- Patch compliance reporting offers insights on the status of VM patches across Linux and Windows distributions. You can view both recommendations and insights for your VM instances.
- Patch deployment automates the process of OS and software patch updates. This feature schedules patch jobs across VM instances and implements the patches accordingly.

Enabling automated security updates can help GCP security by ensuring that critical security patches and bug fixes are applied quickly and consistently across all GCP components. This can help protect against potential vulnerabilities, reduce the risk of data breaches and ensure that GCP services are running optimally.

Conclusion

Securing your data in the cloud is of utmost importance. Any breach can jeopardize the security of the company and its end-users. Data breaches can have a long-lasting impact on the business's bottom line and brand name.
Want to add more about Google Cloud security to your arsenal? AppSecEngineer's GCP Learning Path courses can help you hone your existing knowledge while bringing you up to speed with the latest developments in GCP security.
Look at AppSecEngineer's Training Library to identify your learning requirements, and sign up for some of the most comprehensive courses in the field of Google Cloud security today!

REF:

https://www.appsecengineer.com/blog/gcp-security-checklist-for-2023-and-beyond