sonraí SECURITY | Google Cloud

Google Cloud Checklist for 2022

Expert Advice on GCP Security and Risk Priorities

sonraísecurity.com | info@sonraísecurity.com | 646.389.2262

Contents

Introduction

Google Cloud Platform holds steady ground in the world of cloud providers ranking consistently at third in Gartner's Magic Quadrant Leader category. While it may not have the highest share of the market, it poses a wonderful selection for unique and particular use cases. GCP is praised for its flexibility and control in four major categories: Compute, Storage, Big Data, and Services.

Being many organization's only cloud provider, and one of even more organization's multiple cloud providers, GCP faces sophisticated security threats and concerns. In fact, Google Cloud's November 2021 report revealed just how targeted cloud workloads have become. Nearly 75% of intruder attacks came from misconfigurations, third-party access or poor customer security hygiene. This information came from Google's own review of over 50 recently compromised instances – straight from the horse's mouth.

This same review and related blogs by Google Cloud Execs noted that many successful attacks are tied to poor customer security practices and a general lack of control management. This emphasizes how critical the shared responsibility of the customer is. It is a strong misnomer and quite frankly, blind faith, that once you migrate to the cloud, that the security of your organization solely lies in the hands of the provider. This could not be farther from the truth; Google Cloud Platform (GCP) is responsible for the security of their cloud platform, while you are responsible for everything that you build on that platform.

This document aims to guide GCP customers by recommending best practices for the highest protection level for their GCP infrastructure and the sensitive data stored in GCP. We want customers to feel empowered with the knowledge and guidance needed to protect your organization.

Shared Responsibility Model

Google Cloud, like other providers, operates ideally under a shared responsibility model. Simply put, GCP is responsible for security of the cloud, while GCP customers are responsible for security within the cloud. This entails the provider making sure the cloud platform is inherently built and maintained to be secure and reliable, but past that, the customer steps in. Overall, the distribution of your responsibility vs. theirs depends on what services you're using (Paas, Iaas, Saas, etc.)

Google Cloud Responsibility

As previously mentioned, in large, the resources that build the cloud platform falls under the GCP's purview. Starting at the bottom of the stack, within IaaS, GCP secures hardware, storage, encryption and the network that provides this service. Moving into PaaS, this expands to include all the previously mentioned, plus Guest OS, data & content, access and authentication, identity, and operations. It can get blurry in the PaaS realm because the responsibility share falls somewhere in between. Finally, for SaaS, this is largely under the provider's control with GCP ownership over everything outside of content, access policies and usage.

Customer Responsibility

Customers, on the other hand, are responsible for maintaining the security of what is in the cloud, at a bare minimum, the customer is always responsible for securing their services, content, access policies and usage. A CSP offers many security services and configuration options, but it is the customer's responsibility to ensure that they are enabled, configured and/or monitored effectively. Using the platform services can expand responsibility to deployment and web app security. Furthermore, IaaS expands responsibility to the identity, operations, access, and network security jurisdiction for the customer.

It is important to note, oftentimes the default settings of a cloud platform are not the most secure. It should be a priority for an organization to evaluate the settings that make the most sense for their business needs, if you're trying to optimize your cloud security. Start with the low-hanging fruit, those controls that ensure that you achieve a basic level of security, and then work outwards from there based on what is important to you and your business.

Cloud Responsibility Reminder Table

Below you'll find a responsibility table to visually offer reminders as to what action falls under whose jurisdiction:

	Customer	GCP
Preventing or detecting when a GCP account has been compromised	✓	
Preventing or detecting a privileged or regular GCP user behaving in an insecure manner	✓	
Business continuity management (availability, incident response)	✓	✓
Protecting against GCP zero-day exploits and other vulnerabilities		✓
Providing environmental security assurance against things like mass power outages, earthquakes, floods, and other natural disasters		✓
Providing physical access control to hardware/software		✓
Configuring GCP Managed Services in a secure manner		✓
Ensuring network security (DoS, man-in-the-middle (MITM), port scanning)	✓	✓
Ensuring custom applications are being used in a manner compliant with internal and external policies	✓	
Updating guest operating systems and applying security patches	✓	
Restricting access to GCP services or custom applications to only those users who require it	✓	
Configuring GCP services (except gcp Managed Services) in a secure manner	✓	
Preventing sensitive data from being uploaded to or shared from applications in an inappropriate manner	✓	✓
Database service patching		✓

Top Security Challenges in Google Cloud Platform (GCP)

The threats to GCP can take on many forms, so we've listed some of the most common ones below:

GCP Compromise

The possibility always remains that an attacker could compromise an element in the GCP platform and either gain access to data, take an application running on the platform offline, or permanently destroy data. While you can't necessarily do much about this, you should identify it as a risk and have strategies in place to manage the risk.

Insider Threats

Whether it is malicious behavior or just employee negligence, insider threats are a growing source of vulnerability. This often results in unintentional data exposure to the public or straight up data theft. Either way, it is a major risk to your business and needs to be managed as such.

Unsecured Storage Containers

Google is known for its strength in containers. But human error is often behind misconfigured cloud servers and data leakage. Setting a cloud server with no credentials during development and forgetting to tighten up security one in production is a recipe for problems.

Shadow IT

Shadow IT uses information technology systems, devices, software, applications, and services without explicit IT department approval … and more worrisome, without visibility and proper security controls. It has grown exponentially in recent years with the adoption of cloud-based applications and services. Organizational departments often work around the shortcomings of the central information systems to help them achieve their goals, but at the same time create a hidden risk that affects the entire business.

Third-Party Access Compromise

Many enterprises outsource their business needs to experts, and while that is a wonderful solution for growth, it increases the entry ways into your cloud environment.. The security posture of your third-party vendors quickly becomes your responsibility. A misconfiguration in your third-party's cloud environment can lead to disaster for you.

Cloud Data Sprawl

Cloud growth has led to an overwhelm of data store management. Development means an explosion of data store options with teams utilizing Cloud Storage, Local SSD, Google Kubernetes Engine, and many, many more. Adding these to Google Storage dilutes the traditional sense of a 'data center', making things abstract to practitioners. Cloud sprawl typically occurs when an organization lacks visibility into or control over its cloud computing resources.

Lack of Application Protection

Network firewalls don't always help you when it comes to the public cloud. Attacks on applications more than doubled, according to the 2020 Verizon Data Breach report. GCP offers solutions like Cloud Armor and Apigee to address these concerns.

Managing Access Rights Manually

Managing access rights manually leads to increased risk. This makes it nearly impossible to detect privilege escalation across your infrastructure, plus manual intervention makes it easy to offer excessive permissions to machines. You need to continuously inventory your Identities, determine their effective permissions and receive alerts should deviations occur.

Enabling Root Account Access

Often, organizations still use an active root account and allow access via service account keys. The root is the account that has access to all files and commands across the operating environment. Giving so much power to one entity means disaster if it's compromised.

Assigning Service Account Keys to a Root Account

Again, the root account shouldn't be used for any purpose. Assigning an access key to the root account is a recipe for disaster. If your company currently assigns service account keys to any root account, put a stop to this immediately.

Improperly Storing Service Account Keys

Possible threats include credential leakage, privilege escalation, information disclosure and more. Using a service like Google Cloud Secret Manager addresses this concern. You can also use other methods entirely to authenticate service accounts.

Accounts Without MFA

Compromised passwords are a major concern, allowing hackers to access corporate resources. It is a best practice to enforce MFA across your organization.

Cloud Responsibility Reminder Table

Below you'll find a responsibility table to visually offer reminders as to what action falls under whose jurisdiction:

- □ Enable Security Command Center Dashboard
- □ Set up Organization Policy Service
- □ Define your resource hierarchy
- □ Create an organization node
- □ Manage your Google identities
- □ Federate your identity provider with GC
- □ Migrate unmanaged accounts
- □ Control access to resources
- □ Apply Principle of Least Privilege
- □ Use Cloud IAM recommender
- □ Delegate responsibility into groups and service accounts
- □ Define an organizational policy to restrict access
- □ Use Virtual Private Cloud (VPC) to define your network
- □ Manage traffic with firewall rules
- □ Limit external access or direct internet exposure
- □ Adopt service account firewall rules instead of tag-based rules
- □ Do not use default network for new projects
- □ Centralized Network control
- □ Put a load balancer in front of all web services
- □ Connect your enterprise network
- □ Secure your apps and data
- □ Use VPC service controls
- □ Consider deleting default firewall rules and make your own
- □ Breakdown network into subnets
- □ Use GC global HTTPs load balancer
- □ Integrate Google Cloud Armor
- □ Control app access using IAP
- □ Set up Cloud logging
- □ Set up Cloud monitoring
- □ Set up an audit trail
- □ Export logs
- □ Enable DevOps culture & Site Reliability Engineering
- □ Enable Google Cloud Key Management Service
- □ Enable Google Cloud Identity
- □ Enable Stackdriver Logging
- □ Enable Google Access Transparency
- □ Enable Google Cloud Security Scanner
- □ Enable Google Cloud Resource Manager
- □ Enable Google Cloud Compliance
- □ Plan Disaster Recovery Strategy
- □ Understand how your resources are charged
- □ Set up billing controls
- □ Build a Center of Excellence

sonraí SECURITY

Google Cloud

About Sonrai Security

Sonrai Security delivers an enterprise identity and data governance platform for AWS, Azure, Google Cloud, and Kubernetes. The Sonrai Dig platform is built on a sophisticated graph that identifies and monitors every possible relationship between identities and data that exists inside an organization's public cloud. Dig's Governance Automation Engine automates workflow, remediation, and prevention capabilities across cloud and security teams to ensure end-to-end security. The company has offices in New York and New Brunswick, Canada, backed by ISTARI, Menlo Ventures, Polaris Partners, and Ten Eleven Ventures.

Further Reading

- Guidance on How to Configure, Deploy and Use the Public Cloud Securely
- How to Build a Cloud Center of Excellence
- 7 Common Data Misconfigurations for GCP

Resources

- Google Cloud Architecture Center
- Google Cloud Security Foundations Guide
- Best Practices for Enterprise Organizations

Ready to secure your GCP Environment? We're here for you. Our cloud security experts are ready to help. Reach out to Sonrai Security today.

646.389.2262 | sonraísecurity.com | info@sonraísecurity.com