

No. 110

CYBERSECURITY

Google Cloud Security

Securing projects, identities, data and workloads on Google Cloud

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 110

Google Cloud Security

Securing projects, identities, data and workloads on Google Cloud

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

Google Cloud Security
Securing projects, identities, data and workloads on Google Cloud

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. Google, Google Cloud, Google Workspace and related product names are trademarks of Google LLC. Wiz is a trademark of its owner. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by any vendor named in this book.

The information in this book is provided for general education. AI products, features, plans, prices and policies change frequently; always confirm details in the vendor's current documentation. Screens marked “Illustration” are simplified drawings, not captures of real software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this book 1

PART I · FOUNDATIONS

1 Shared responsibility 5
2 What attackers do 6
3 The resource hierarchy 7
4 Inheritance 8
5 IAM basics 9
6 Roles 11
7 Service accounts 13
8 Securing Cloud Identity and Workspace 14

PART II · GUARDRAILS AND VISIBILITY

9 Identity federation 16
10 Organization policies 17
11 Cloud Audit Logs 18
12 Security Command Center 19
13 Recommendations and insights 21
14 Google's security portfolio 22
15 Access Transparency and Access Approval 23

PART III · PROTECTING RESOURCES

16 Network security 25
17 Cloud Armor 27
18 VPC Service Controls 28
19 Identity-Aware Proxy 29
20 Protecting data 30
21 Encryption and secrets 31
22 Compute Engine 32
23 GKE and Cloud Run 33

FREE SAMPLE · ojayo.com

24 AI workloads 34
25 Detecting abuse through cost and quotas 35

PART IV · OPERATIONS

26 Infrastructure as code 37
27 Security operations 38
28 Incident response 39
29 Backup and resilience 40
30 Compliance and sovereignty 41
31 Common mistakes 42
32 A worked example 43
33 A 90-day plan 44
Checklists 45
Glossary 46
Further reading 47

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

What this book covers, who it is for, and how to use it.

Google Cloud hosts applications, data platforms and AI workloads for organizations around the world. Like every cloud, it uses a shared responsibility model: Google secures the infrastructure, and customers secure their identities, configurations and data. Google's own threat research shows attackers targeting exactly those customer-controlled areas: unpatched software, weak credentials and misconfigurations.

This book explains Google Cloud security for beginners. It starts with how Google Cloud is organized and who can access what, then covers guardrails, visibility, networks, data, workloads, AI and operations.

What this book covers

- The resource hierarchy, IAM, groups, service accounts and federation.
- Organization policies and secure-by-default settings.
- Cloud Audit Logs and Security Command Center.
- VPC design, firewall rules, Cloud Armor, VPC Service Controls and Identity-Aware Proxy.
- Cloud Storage, encryption, secrets, Compute Engine, GKE, Cloud Run and AI workloads.
- Google Security Operations, Wiz, incident response and a 90-day plan.

Who this book is for

- **Administrators and engineers** new to Google Cloud.

FREE SAMPLE · ojayo.com

- **Developers and data teams** deploying to Google Cloud.
- **Security beginners** working in Google environments.

How the book is organized

- **Part I — Foundations** (Chapters 1–8): shared responsibility, threats, the resource hierarchy, inheritance, IAM, roles, service accounts, and Cloud Identity and Workspace.
- **Part II — Guardrails and visibility** (Chapters 9–15): federation, organization policies, audit logs, Security Command Center, recommendations, Google's security portfolio, and access transparency.
- **Part III — Protecting resources** (Chapters 16–25): networks, Cloud Armor, VPC Service Controls, Identity-Aware Proxy, storage, encryption and secrets, Compute Engine, GKE and Cloud Run, AI workloads, and cost signals.
- **Part IV — Operations** (Chapters 26–33): infrastructure as code, Google Security Operations, incident response, backups, compliance, common mistakes, a worked example, and a 90-day plan.
- **Reference**: checklists, glossary and further reading.

Callouts

TIP
Practical advice you can use straight away.

IN PRACTICE
How an idea looks in a real Google Cloud environment.

WATCH OUT
Common mistakes and risks.

KEY IDEA
The one thing to remember from a section.

FREE SAMPLE · ojayo.com

A note on screens

Consoles and product names change; check Google Cloud documentation for current details. Screens are **simplified illustrations**, not actual Google Cloud screens.

FREE SAMPLE · ojayo.com

PART I

Foundations

These chapters explain shared responsibility, the threats Google observes, and how resources and permissions are organized.

FREE SAMPLE · ojayo.com

CHAPTER 1

Shared responsibility

Google secures the platform; you secure how you use it.

Google's side

Google secures its data centres, custom hardware, global network and the platform beneath managed services, and encrypts data at rest by default.

Your side

You control identities and IAM, configuration of services, network exposure, data classification and the code you deploy.

Shared fate

Google describes its approach as **shared fate**: providing secure defaults, blueprints and guidance to help customers configure securely, not just a dividing line.

FREE SAMPLE · ojayo.com

CHAPTER 2

What attackers do

Google publishes what it sees attackers doing.

Initial access in Google Cloud, H2 2025	Share
Exploited third-party software	44.5%
Weak or missing credentials	27.2%
Misconfiguration	21%

Figure 2.1 What Google observed

Threat Horizons

Google Cloud's **Threat Horizons** reports describe real incidents. Its report published in early 2026 found that, in the second half of 2025, exploited third-party software had overtaken weak or missing credentials as the main way into Google Cloud environments, and that identity compromise underpinned most incidents across cloud and SaaS.

Lessons

Patch internet-facing software quickly, use strong authentication, avoid long-lived keys and fix misconfigurations.

FREE SAMPLE · ojayo.com

CHAPTER 3

The resource hierarchy

Resources sit in a hierarchy.

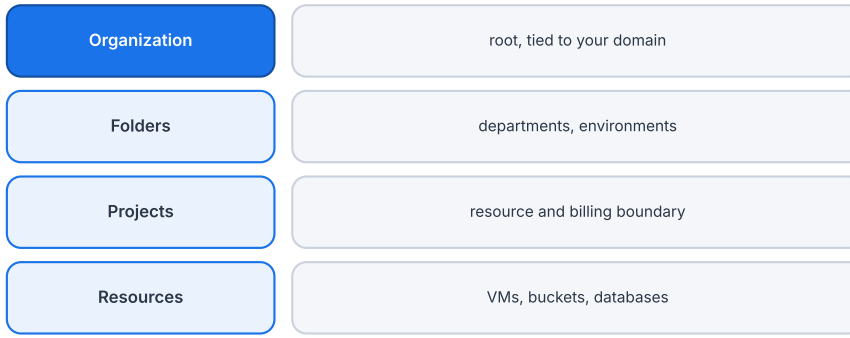


Figure 3.1 The Google Cloud resource hierarchy

Organization

The **organization** node is linked to your company domain through Cloud Identity or Google Workspace. Create one; projects outside an organization are hard to govern.

Folders and projects

Folders group projects by department or environment. **Projects** are the main boundary for resources, APIs, IAM and billing. Separate production and development projects.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security (you are reading this)
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

Google Cloud Security

Enjoyed it? The full book has 52 pages and 33 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.