# Google Cloud BeyondCorp (Zero Trust) Implementation Training Course

Professional Development Training Course Outline

| | | | |
|---|---|---|---|
| **Category** | Data Security | **Duration** | 5 Days |
| **Base Fee** | $1,500 USD | **Delivery Mode** | Online / On-site Hybrid |

## Course Introduction

The modern enterprise landscape is defined by hybrid workforces, multi-cloud environments, and sophisticated cyber threats. Traditional network-centric security models, which rely on a porous perimeter, are no longer adequate. This training course is your deep dive into Google Cloud BeyondCorp Enterprise (BCE), Google?ÇÖs definitive implementation of the Zero Trust security model. BeyondCorp fundamentally shifts the security paradigm from "trust the network" to "never trust, always verify," securing access based on user identity, device health, and contextual factors. This intensive, hands-on training empowers security architects and cloud engineers to design, implement, and manage a robust, VPN-less access solution. You will master key components like Identity-Aware Proxy (IAP) and Access Context Manager, transforming your organization's security posture to enable truly secure access for employees, partners, and applications from any location and any device.

Google Cloud BeyondCorp (Zero Trust) Implementation Training Course provides the strategic roadmap and technical expertise necessary to execute a successful Zero Trust migration using Google Cloud's proven architecture. Participants will move beyond theoretical knowledge to practical, real-world implementation, learning to enforce least-privilege access and establish a dynamic, policy-driven security framework. A core focus will be on integrating BCE with existing cloud and on-premises applications, ensuring a seamless yet highly secure user experience. By the end of this program, you will be equipped to mitigate risks like lateral movement and credential compromise, delivering a more secure, scalable, and compliant access model. The skills acquired are critical for any organization committed to cybersecurity modernization and protecting its most valuable assets in today's cloud-native world

## Programme Curriculum

**Google Cloud BeyondCorp (Zero Trust) Implementation Training Course**

**Introduction**

The modern enterprise landscape is defined by hybrid workforces, multi-cloud environments, and sophisticated cyber threats. Traditional network-centric security models, which rely on a porous perimeter, are no longer adequate. This training course is your deep dive into Google Cloud BeyondCorp Enterprise (BCE), Google? ÇÖs definitive implementation of the Zero Trust security model. BeyondCorp fundamentally shifts the security paradigm from "trust the network" to "never trust, always verify," securing access based on user identity, device health, and contextual factors. This intensive, hands-on training empowers security architects and cloud engineers to design, implement, and manage a robust, VPN-less access solution. You will master key components like Identity-Aware Proxy (IAP) and Access Context Manager, transforming your organization's security posture to enable truly secure access for employees, partners, and applications from any location and any device.

Google Cloud BeyondCorp (Zero Trust) Implementation Training Course provides the strategic roadmap and technical expertise necessary to execute a successful Zero Trust migration using Google Cloud's proven architecture. Participants will move beyond theoretical knowledge to practical, real-world implementation, learning to enforce least-privilege access and establish a dynamic, policy-driven security framework. A core focus will be on integrating BCE with existing cloud and on-premises applications, ensuring a seamless yet highly secure user experience. By the end of this program, you will be equipped to mitigate risks like lateral movement and credential compromise, delivering a more secure, scalable, and compliant access model. The skills acquired are critical for any organization committed to cybersecurity modernization and protecting its most valuable assets in today's cloud-native world

**Course Duration**

5 days

**Course Objectives**

1. Master the principles and pillars of the Zero Trust Architecture (ZTA) model as defined by NIST and implemented by Google's BeyondCorp.
2. Design a secure, scalable VPN-less remote access solution using BeyondCorp Enterprise (BCE) for a hybrid workforce.
3. Implement Identity-Aware Proxy (IAP) to enforce granular, context-aware access control for Google Cloud and on-premises applications.
4. Configure and manage Access Context Manager (ACM) policies based on device health, geo-location, and user attributes.
5. Secure GCP resources with fine-grained access policies using IAP and ACM.
6. Integrate Endpoint Verification to continuously assess and ensure the security posture and device compliance of all accessing endpoints.
7. Apply the principle of Least-Privilege Access to all user and service accounts within the BeyondCorp framework.
8. Migrate traditional, perimeter-based security models to a modern, identity-driven Zero Trust model with minimal disruption.
9. Leverage Google Cloud's Security Command Center and Cloud Audit Logs for continuous monitoring and real-time security analytics.
10. Automate the deployment and configuration of BeyondCorp components using Infrastructure-As-Code (IaC) tools like Terraform.
11. Differentiate between BeyondCorp's core components and deploy the appropriate solution for various web and SSH access use cases.

12. Troubleshoot common access policy and authentication issues encountered during a BeyondCorp implementation.
13. Develop a comprehensive governance and data loss prevention (DLP) strategy integrated with the BeyondCorp access controls.

**Target Audience**

1. Security Architects
2. Cloud Engineers (GCP/Multi-cloud)
3. Cybersecurity Professionals
4. Identity and Access Management (IAM) Specialists
5. Network Security Engineers
6. DevSecOps Engineers
7. IT Directors/Managers overseeing security transformation.
8. System Administrators responsible for application and resource access.

**Course Modules**

**Module 1: Zero Trust & BeyondCorp Foundations**

- Understanding the shift from Perimeter Security to Zero Trust Architecture
- BeyondCorp as Google's decade-proven internal ZT implementation.
- Never Trust, Always Verify, and Least-Privilege Access.
- Overview of BeyondCorp Enterprise components
- Case Study: Google's internal migration to BeyondCorp.

**Module 2: Identity and Access Management (IAM) Core**

- Configuring Cloud Identity and Cloud Directory Sync for unified user management.
- Deep dive into Google Cloud IAM roles, policies, and conditions.
- Implementing strong authentication.
- Securing Service Accounts and machine-to-machine communication in a ZT context.
- Case Study: Implementing Conditional Access for privileged administrator accounts.

**Module 3: Identity-Aware Proxy (IAP) for Application Access**

- Detailed IAP setup for securing App Engine, Compute Engine, and GKE web applications.
- Defining and enforcing contextual access policies using the Access Context Manager.
- Enabling IAP TCP Forwarding for secure shell access to Virtual Machines.
- Integrating IAP with on-premises and multi-cloud applications via hybrid connectivity.
- Case Study: Securing a legacy on-premises application using IAP without a VPN.

**Module 4: Access Context Manager (ACM) & Policy Granularity**

- Creating and managing Access Levels based on source IP, device state, and location.
- Developing attribute-based access control logic for sophisticated policies.
- Applying ACM to Google Cloud APIs and sensitive administrative controls.
- Testing and validating complex ACM policies for various user roles and access scenarios.
- Case Study: Building a policy to allow access to sensitive data only from corporate-managed, encrypted devices within a specific country.

**Module 5: Endpoint Verification and Device Trust**

- Deploying and configuring the Endpoint Verification agent on corporate devices.
- Collecting and interpreting device attributes
- Defining Device Trust scores and integrating them into ACM access levels.
- Implementing automated remediation actions for non-compliant devices.
- Case Study: Forcing all remote users to meet specific device health criteria to access internal SaaS apps.

**Module 6: Network and Perimeter Modernization**

- Eliminating reliance on a traditional network perimeter and perimeter firewall rules.
- Using VPC Service Controls to create data perimeters and prevent data exfiltration.
- Securing east-west traffic with microsegmentation principles.
- BeyondCorp for access to SaaS applications
- Case Study: Implementing VPC-SC to protect a Cloud Storage bucket containing PII from unauthorized service access.

**Module 7: Monitoring, Auditing, and Operations**

- Configuring Cloud Audit Logs and Access Transparency for ZT visibility.
- Utilizing Security Command Center for continuous security posture assessment and policy violations.
- Setting up real-time alerts for unauthorized access attempts and policy breaches.
- Developing a Zero Trust incident response plan.
- Case Study: Investigating and responding to a thwarted attempt at lateral movement using BeyondCorp logs.

**Module 8: Deployment, Migration, and Future State**

- Developing a phased Zero Trust migration roadmap and communication strategy.
- Automating BeyondCorp deployment using Terraform and Google Cloud Deployment Manager.
- Best practices for a rollout to a large-scale workforce.
- Integration with AI/ML-driven threat intelligence and dynamic policies.
- Case Study: Planning and executing the decommissioning of an organization's legacy VPN after a successful BCE deployment.

## Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

**Register as a group from 3 participants for a Discount**

**Send us an email: info@fineskilltrainingcenter.org or call** *+254769199797*

***Certification***

*Upon successful completion of this training, participants will be issued with a globally- recognized certificate.*

***Tailor-Made Course***

*We also offer tailor-made courses based on your needs.*

**Key Notes**

**a.** The participant must be conversant with English.

**b.** Upon completion of training the participant will be issued with an Authorized Training Certificate

**c.** Course duration is flexible and the contents can be modified to fit any number of days.

**d.** The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

**e.** One-year post-training support Consultation and Coaching provided after the course.

**f.** Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

## Upcoming Scheduled Sessions

| Start Date | End Date | Location | Price |
|---|---|---|---|
| **21 Sep 2026** | 25 Sep 2026 | Online | $1,000 |
| **21 Sep 2026** | 25 Sep 2026 | Physical | $1,500 |
| **21 Sep 2026** | 25 Sep 2026 | Physical | $0 |
| **21 Sep 2026** | 25 Sep 2026 | Physical | $0 |
| **21 Sep 2026** | 25 Sep 2026 | Physical | $0 |
| **21 Sep 2026** | 25 Sep 2026 | Physical | $0 |
| **21 Sep 2026** | 25 Sep 2026 | Physical | $0 |
| **21 Sep 2026** | 25 Sep 2026 | Physical | $0 |

Ready to enroll or request a customized program? Book online or contact us:

**Register Online Now**