

# VERTEX AI AND GENERATIVE AI SECURITY

Course Code: 899024

This course is designed to empower your organization to fully harness the transformative potential of Google's Vertex AI and generative AI (gen AI) technologies, with a strong emphasis on security.

Tailored for AI practitioners and security engineers, it provides targeted knowledge and hands-on skills to navigate and adopt AI safely and effectively. Participants will gain practical insights and develop a security-conscious approach, ensuring a secure and responsible integration of gen AI within their organization.

## What You'll Learn

### Skills Gained

- Establish foundational knowledge of Vertex AI and its security challenges.
- Implement identity and access control measures to restrict access to Vertex AI resources.
- Configure encryption strategies and protect sensitive information.
- Enable logging, monitoring, and alerting for real-time security oversight of Vertex AI operations.
- Identify and mitigate unique security threats associated with generative AI.
- Apply testing techniques to validate and secure generative AI model responses.
- Implement best practices for securing data sources and responses within Retrieval-Augmented Generation (RAG) systems.
- Establish foundational knowledge of AI Safety

## Who Needs to Attend

AI practitioners, security professionals, and cloud architects.

## Prerequisites

Fundamental knowledge of machine learning, in particular generative AI, and basic understanding of security on Google Cloud.

# VERTEX AI AND GENERATIVE AI SECURITY

Course Code: 899024

VIRTUAL CLASSROOM LIVE

\$2,399 CAD

2 Day

## Virtual Classroom Live Outline

### **Module 1: Introduction to Vertex AI Security Principles**

- Google Cloud Security
- Vertex AI components
- Vertex AI Security concerns
- Review Google Cloud Security fundamentals.
- Establish a foundational understanding of Vertex AI.
- Enumerate the security concerns related to Vertex AI features and components.
- Lab: Vertex AI: Training and Serving a Custom Model

### **Module 2: Identity and Access Management (IAM) in Vertex AI**

- Overview of IAM in Google Cloud
- Control access with Identity Access Management.
- Simplify permission using organization hierarchies and policies.
- Use service accounts for least privileged access.
- Lab: Service Accounts and Roles: Fundamentals

### **Module 3: Data Security and Privacy**

- Data encryption
- Protecting Sensitive Data
- VPC Service Controls
- Disaster recovery planning
- Configure encryption at rest and in-transit.
- Encrypt data using customer-managed encryption keys.
- Protect sensitive data using the Data Loss Prevention service.
- Prevent exfiltration of data using VPC Service Controls.
- Architect systems with disaster recovery in mind.
- Lab: Getting Started with Cloud KMS
- Lab: Creating a De-identified Copy of Data in Cloud Storage

### **Module 4: Securing Vertex AI Endpoints and model deployment**

- Network security
- Securing model endpoints
- Deploy ML models using model endpoints.
- Secure model endpoints.
- Lab: Configuring Private Google Access and Cloud NAT

### **Module 5: Monitoring and logging in Vertex AI**

- Logging
- Monitoring
- Write to and analyze logs.
- Set up monitoring and alerting.

### **Module 6: Security risks in generative AI applications**

- Overview of gen AI security risks
- Overview of AI Safety
- Prompt security
- LLM safeguards
- Identify security risks specific to LLMs and gen AI applications.
- Understand methods for mitigating prompt hacking and injection attacks.
- Explore the fundamentals of securing generative AI models and applications.
- Introduce fundamentals of AI Safety.
- Lab: Safeguarding with Vertex AI Gemini API
- Lab: Gen AI & LLM Security for Developers

### **Module 7: Testing and evaluating generative AI model responses**

- Testing generative AI model responses.
- Evaluating model responses.
- Fine-Tuning LLMs.
- Implement best practices for testing model responses.
- Apply techniques for improving response security in gen AI applications.
- Lab: Measure Gen AI Performance with the Generative AI Evaluation Service
- Lab: Unit Testing Generative AI Applications

### **Module 8: Securing Retrieval-Augmented Generation (RAG) systems**

- Fundamentals of Retrieval-Augmented Generation
- Security in RAG systems
- Understand RAG architecture and security implications.
- Implement best practices for grounding and securing data sources in RAG systems.
- Lab: Multimodal Retrieval Augmented Generation (RAG) Using the Vertex AI Gemini API
- Lab: Introduction to Function Calling with Gemini

Jul 20 - 21, 2026 | 9:00 AM - 5:00 PM EDT

Visit us at [www.globalknowledge.com](http://www.globalknowledge.com) or call us at 1-866-716-6688.

Date created: 4/23/2026 6:28:52 AM

Copyright © 2026 Global Knowledge Training LLC. All Rights Reserved.