



University
Pro



Veeam Data Platform: Enterprise Data Security

Cyber Secure

On Demand



**Course duration:**

On-Demand — 16 hours

Course Components:

120 Video Lessons / 57 Clickable Labs

Average Lesson Duration:

10 min (Self-Paced Lessons)

Overview

The Veeam Data Platform: Enterprise Data Security course is designed to equip IT professionals with the expertise needed to implement robust data protection strategies, defend against ransomware, and align backup security with enterprise-wide cybersecurity frameworks.

Participants will gain experience in configuring Veeam's advanced security features, integrating with SIEM/SOAR platforms, enforcing zero trust principles, and doing what's needed for compliance with industry regulations.

By the end of the course, attendees will be prepared to enhance their organization's data resilience, mitigate risks, and respond effectively to cyber incidents.

Audience

This course is intended for cybersecurity teams, backup administrators, IT security architects, and compliance officers who are responsible for ensuring the security and resilience of enterprise backup environments. It is also designed for professionals who work in large-scale infrastructures where data protection is critical.

Prerequisites

Attendees should be familiar with Veeam Backup & Replication. A foundational understanding of cybersecurity principles, enterprise authentication methods, and regulatory compliance requirements will help participants get the most from this course.

Certification

The Veeam Data Platform: Enterprise Data Security course is the third in a three-part series that makes up the Veeam Certified Security Expert (VMCSE).

Completion of:

- VDP: Enterprise data security
- VDP: Scale, Automate, Secure
- VDP: Monitor, Manage, Analyze

satisfies the prerequisite for taking the VMCSE exam.

VMCE certificate holders will only be eligible for taking the VMCSE exam and certification.

Students who complete the Veeam Data Platform: Enterprise Data Security course on its own will receive a shareable badge after completion.

✓ Objectives

After completing this course, students will be able to:

- Implement robust data protection strategies that are aligned with leading cybersecurity frameworks.
- Configure and harden Veeam environments with advanced security features and zero trust principles.
- Integrate Veeam with SIEM, SOAR, and threat detection platforms for enhanced monitoring and automated response.
- Strengthen ransomware resilience and improve incident response for enterprise backup environments
- Ensure compliance with industry regulations and automate security governance for on-premises and cloud backups.
- Design secure enterprise backup architectures to maximize data resilience and minimize risk.
- Collaborate with Security Operations Centers (SOCs) by sharing telemetry and alerts from backup infrastructure for enhanced threat visibility.
- Apply forensic principles and conduct post-incident analysis to validate backup integrity and support regulatory investigations.

📄 Course Contents

Module 1: Cybersecurity Frameworks and Enterprise Backup Security

Learning Objectives:

- Identify cybersecurity frameworks (NIST, CIS, ISO 27001) and their relevance to enterprise backup security.
- Explain how Veeam's security features align with cybersecurity frameworks.
- Analyze the role of data protection in enterprise risk management.

Module 2: Zero Trust Data Resilience in Enterprise Backup Security

Learning Objectives:

- Explain Zero Trust Data Resilience (ZTDR) and its role in enterprise backup security.
- Apply zero trust principles (e.g., least privilege, continuous verification, micro-segmentation) to Veeam deployments.
- Configure Veeam components (e.g., RBAC, MFA, SIEM integration) for zero trust security.

Module 3: Advanced Hardening for Veeam Deployments

Learning Objectives:

- Implement hardened Veeam deployments with advanced security configurations.
- Apply encryption, access control, and network segmentation for backup security.
- Use deception techniques (i.e., honeypots) to detect attacks early.

Module 4: Cloud Backup Security and Compliance

Learning Objectives:

- Secure Veeam backups for AWS, Azure, and Google Cloud.
- Implement IAM roles and least privilege access for cloud backups.
- Ensure compliance for cloud backup security (e.g., GDPR, CCPA, FIPS).



Module 5: Enterprise Backup Security Architecture

Learning Objectives:

- Design secure enterprise backup architectures for disaster recovery (DR).
- Apply security best practices for on-premises, cloud, and hybrid backup infrastructures.
- Ensure backup storage security (e.g., hardened repositories, cloud object storage).

Module 6: Advanced Ransomware Resilience and Incident Response

Learning Objectives:

- Explain the ransomware kill chain and attack progression.
- Implement forensic analysis and incident response for backup environments.
- Integrate threat intelligence into enterprise backup security monitoring.

Module 7: Security Logging, SIEM/XDR, and Threat Detection for Backups

Learning Objectives:

- Implement security monitoring and log analysis for enterprise backup security.
- Integrate Veeam with SIEM/XDR solutions for anomaly detection.
- Automate security threat responses with SOAR workflows.

Module 8: Compliance-Driven Backup Security and Governance

Learning Objectives:

- Identify enterprise compliance requirements and their impact on backup security.
- Explain how Veeam supports security audits and regulatory reporting.
- Automate compliance enforcement using Veeam ONE, SIEM, and SOAR workflows.

➔ To discover more about our training programs, please visit [Veeam University PRO page](#)

Certification Journey

