Securing Windows Server Training

BILGINC IT Academy
info@bilginc.com
bilginc.com

Duration: **3 Day**

This three-day course equips IT professionals with the practical skills and knowledge required to secure Windows Server environments across on-premises, hybrid, and multi-cloud infrastructures.

Learners will explore the core security capabilities of Windows Server 2019, 2022, and 2025, including modern enhancements such as secured-core server, Azure Arc integration, and Hotpatching. The course focuses on strengthening identity protection, securing administrative access, protecting data, and implementing industry-aligned security baselines.

By combining hands-on exercises with real-world scenarios, this course enables learners to confidently design, implement, and manage a secure Windows Server platform that aligns with Microsoft best practices and modern security requirements.

Prerequisites

Before attending this course, learners should have:

- Experience configuring and managing Windows Server operating systems
- An understanding of Active Directory and Group Policy
- Knowledge of core networking concepts
- Awareness of fundamental security best practices

Target audience

This course is designed for:

- IT professionals with experience in day-to-day Windows Server administration
- Server administrators looking to deepen their security expertise
- Security architects who need to understand Windows Server security capabilities
- IT professionals working with non-Microsoft platforms who want to cross-train on Windows Server

Securing Windows Server Training

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Duration: **3 Day**

What You Will Learn

By the end of this course, learners will be able to:

- Configure and implement secured-core server features including virtualization-based security and secure boot
- Harden Hyper-V hosts and virtual machines
- Enable Azure Arc for centralised management across hybrid and multi-cloud environments
- Configure Azure Automanage and implement Hotpatch updates
- Apply Microsoft security baselines using Group Policy and OSConfig
- Protect identities using password policies, Credential Guard, and authentication silos
- Secure services using managed service accounts
- Apply least privilege principles to secure server administration
- Manage local administrator passwords using Windows LAPS
- Deploy and manage a public key infrastructure using Active Directory Certificate Services
- Secure data access using permissions and encrypted SMB connections
- Protect data at rest using BitLocker and Encrypting File System
- Configure advanced auditing policies
- Monitor server security posture using Microsoft Defender for Servers