Microsoft

Windows Server 2022 comparison guide

Run business critical workloads in Azure, on-premises, and at the edge

Organizations are digitally transforming their operations and running business-critical workloads that span across cloud, on-premises, and the edge. As a result, the need to secure workloads and data has never been greater. Use this guide to determine if it's time to upgrade your servers.

Windows Server 2022 enables you to run business-critical workloads anywhere — in your datacenter, in the cloud, and at the edge — while staying ahead of emerging security threats and helping secure your data. This release builds on the advancements made in Windows Server 2019, the fastest-adopted Windows Server ever.

Windows Server 2022 delivers advanced multi-layer security, hybrid capabilities with Azure, and a flexible platform to modernize applications with containers.

How to use this guide

This comparison guide is intended for business decision makers, technical decision makers, solution architects, and IT pros to help communicate the differences between the Windows Server version they are running today and the latest version available from Microsoft. The guide compares selected features of Microsoft Windows Server 2016, Windows Server 2019, and Windows Server 2022.

Comparison matrix

The guide walks through three key capability areas to show the evolution of relevant features across Windows Server versions. The legend for this notation is given in the following table.

Feature	Not supported	Good	Better	Best
Feature name Feature definition	○	◔	◑	●

Advanced, multi-layer security

Public and private sectors continue to suffer major data breaches, at an average cost of $4.24 million in 2020.* As cybersecurity threats escalate and the cost of incidents grows, security continues to be a top priority for customers. Windows Server 2022 includes enhanced security features with Secured-core server and secure connectivity.

Feature and description	Windows Server 2016	Windows Server 2019	Windows Server 2022
Secured-core server			
Overview. Secured-core server brings together powerful threat protections for multi-layer security across hardware, firmware, and the operating system. It uses the Trusted Platform Module 2.0 and Windows Defender System Guard to launch Windows Server securely and minimize risk from firmware vulnerabilities. Secured-core server helps secure the foundation of virtualization-based security (VBS) features in the list that follows.	○	○	●
Hypervisor-protected code integrity (HVCI). Now enabled by default, HVCI is part of Secured-core server and applies hardware-rooted security to prevent advanced malware from tampering with the system.	◔	●	●
Credential Guard. Part of Secured-core server, this feature can be enabled as an option to provide preventative defense for sensitive assets like credentials.	◔	◔	●
Secured connectivity			
Overview. Secured connectivity adds an additional layer of security during transport for advanced protection and includes improvements to hypertext transfer protocol secure (HTTPS), transport layer security (TLS), and SMB Encryption.	◔	◔	●
Hypertext transfer protocol secure (HTTPS). HTTP over QUIC (HTTP/3) enables faster and more secure HTTPS connections.	◔	◔	●
Transport Layer Security (TLS). Part of secured connectivity, TLS 1.3 is the latest version of the internet's most deployed security protocol and encrypts data to provide a secure communication channel between two endpoints, when used with Windows Server 2022.	◔	◔	●

* Cost of a Data Breach Report 2021, Ponemon Institute

Feature and description	Windows Server 2016	Windows Server 2019	Windows Server 2022
Server Message Block (SMB) security enhancements. Previously, enabling SMB Encryption on SMB Direct RDMA networks disabled direct data placement and slowed performance; now data is encrypted before placement, reducing performance degradation when using RDMA while adding AES-128 and AES-256 protected packet privacy. Additional improvements include accelerated SMB signing performance with AES-128-GMAC, SMB encryption support for top secret class networks via AES-256-GCM and AES-256-CCM cryptographic suites, and configurable SMB Encryption and signing for internal cluster communications that works alongside existing client-server encryption.	○	○	●
SMB over QUIC allows on-premises, mobile, and telecommuter users access to file servers at the edge in Azure and on corporate networks—without a VPN. The server certificate creates a TLS 1.3-encrypted tunnel over the internet-friendly UDP port 443 instead of TCP/445 to avoid exposing SMB traffic to the network.	○	○	●
DNS over HTTPS (DoH) client. Enables the DNS client to protect its domain-name lookups from interference and observation.	○	○	●
Other key security features			
Windows Defender Application Control (WDAC) or code integrity. Helps ensure only authorized executables run on the server. Major improvements in WDAC include support for multiple base policies, supplemental policies, and path-based rules.	◔	◔	●
Advanced Threat Protection (ATP). Windows Defender ATP Exploit Guard is a new set of host intrusion prevention capabilities, such as preventative protection, attack detection, and zero-day exploits.	○	●	●
Cluster hardening. New clusters running Windows Server will not require NT LAN Manager (NTLM) authentication, which completely removes the requirement of Active Directory for clusters in Windows Server.	○	●	●
SDN encrypted subnet. Virtual network encryption provides the ability for the virtual network traffic to be encrypted between virtual machines that communicate with each other within subnets.	○	●	●
Just Enough Administration. Limits administrative privileges to the bare minimum required set of actions (limited in space).	●	●	●
Just-in-Time Administration. Provides privileged access through a workflow that is audited and limited in time.	●	●	●

Feature and description	Windows Server 2016	Windows Server 2019	Windows Server 2022
Control Flow Guard. Helps protect against classes of memory corruption attacks.	●	●	●
Remote Credential Guard. Works in conjunction with credential guard for Remote Desktop Protocol (RDP) sessions to deliver single sign-on (SSO), eliminating the need to pass credentials to the RDP host.	●	●	●
Dynamic Access Control. Enables administrators to apply access-control permissions and restrictions based on well-defined rules.	●	●	●
BitLocker. Uses a hardware or virtual Trusted Platform Module (TPM) chip to provide disk encryption for data and system volumes.	●	●	●

Hybrid

Extend your datacenter to Azure for greater IT efficiency and take advantage of cloud innovation with your on-premises investments — while you enjoy improved tools to help manage servers wherever they are.

Feature and description	Windows Server 2016	Windows Server 2019	Windows Server 2022
Azure Arc. Enables customers to manage, secure, and govern Windows Server on-premises, at the edge, or in multi-cloud environments from a single control plane in Azure. Brings in Azure management capabilities such as Azure Policy, Azure Monitor, and Azure Defender for those servers.	●	●	●
SMB Compression. SMB compression allows an administrator, user, or application to request on-the-fly compression of files as they transfer over the network. Compressed files will consume less network bandwidth and take less time to transfer.	○	○	●
Storage Migration Service (SMS). Helps inventory and migrate data, security, and configurations from legacy systems to Windows Server or a cloud virtual machine. Starting with Windows Server 2022, customers can integrate SMS with Azure File Sync and migrate to low-latency private cloud servers or the bottomless cloud storage in Azure while reducing on-premises storage footprint. SMS migrates file servers from Windows Server, Windows clusters, Samba, and starting in Windows Server 2022—NetApp FAS arrays.	○	◔	●

Feature and description	Windows Server 2016	Windows Server 2019	Windows Server 2022
Unified management with Windows Admin Center. Deploy Admin Center locally or in Azure to manage Windows Server instances running anywhere—on-premises or in the cloud. Seamlessly manage infrastructure with features for Hyper-V management, role-based access control, and security. Includes significant performance and accessibility improvements with an upgrade to HTTP/2. Customize the tool with a publicly available SDK toolkit.	●	●	●
Azure File Sync. Centralize your organization's file shares in Azure Files while keeping the flexibility, performance, and compatibility of an on-premises file server.	●	●	●
System Insights. Brings local predictive analytics capabilities native to Windows Server. These predictive capabilities—each backed by a machine-learning model—locally analyze Windows Server system data to provide high-accuracy predictions that help reduce the operational expenses associated with reactively managing Window Server instances.	○	●	●

Flexible application platform

Empower your developers and IT pros to create applications quickly without worrying about the production environment. Windows Server 2022 offers enhanced platform capabilities and tools that improve developer velocity and increase support for key workloads. Run business-critical and large-scale applications like SQL Server that require 48TB of memory and 2,048 logical cores running on 64 physical sockets.

Feature and description	Windows Server 2016	Windows Server 2019	Windows Server 2022
Windows Container overall. Create an isolated application environment to run applications across diverse environments without fear of changes due to applications or configuration.	◔	◔	●
Image Size reduction. Improvements to Server Core container image, which is recommended for lift and shift scenarios.	◔	◔	●
Group Managed Service Accounts (gMSA). This special type of service account enables containers to share an identity without needing to know its password, allowing containerized applications to enable Active Directory authentication. Recent improvements no longer require domain-join container hosts.	○	◔	●
Kubernetes experience. Adds support for industry standard containerd.	○	◔	●

Feature and description	Windows Server 2016	Windows Server 2019	Windows Server 2022
Hyper-V isolation. Provides a highly isolated container environment in which the host operating system cannot be affected in any way by any other running container.	●	●	●
Virtualized time zone. Improvements enable configuration of the time zone of a container without requiring access to the host.	○	●	●
Scalability improvements enhancing overlay networking support. Aggregates several performance and scale improvements which have been made across the last 4 Semi-Annual Channel (SAC) versions after Windows Server 2019.	○	◕	●
Direct Server Return (DSR) routing for overlay and l2bridge networks. Reduces latency and removes extra load from load balancers.	○	○	●
Multi-subnet support for Windows worker nodes with Calico for Windows. More flexible Kubernetes container endpoint configurations via Calico for Windows.	○	●	●
HostProcess containers for node management. Extends the Windows container model to enable a wider range of Kubernetes cluster management scenarios.	○	●	●
Server Core Features on Demand. Features on Demand (FoD) significantly improve the app compatibility of Windows Server Core by including a set of binaries and packages from Windows Server with Desktop without adding any of the Windows Server Desktop GUI or Windows 10 GUI experiences.	○	●	●
PowerShell scripting and automation. Now open-source and cross-platform in version 7.0, which provides enhanced scripting capabilities for configuration, management, and deployment of software-defined datacenter components.	◔	◕	●
Nested Hyper-V virtualization supports AMD EPYC and Ryzen processors in Windows Server 2022.	◔	◔	●
Single node caching and tiering for single node servers is new with Windows Server 2022.	◔	◔	●
Scalability improvements. Windows Server 2022 supports 48TB memory highly optimized for large memory systems, and 64 sockets/2048 logical processors for massive scaleup systems.	◔	◕	●

Feature and description	Windows Server 2016	Windows Server 2019	Windows Server 2022
Networking UDP/TCP Performance. Improvements in Windows Server 2022 include support for UDP Segmentation Offload and UDP Receive Side Coalescing. Windows Server 2022 adds support for TCP HyStart++ and RACK-TLP. TCP HyStart++ reduces packet loss during connection start-up and RACK (Recent Acknowledgement Tail Loss Probe) reduces Retransmit TimeOuts (RTO). These features are enabled in the transport layer by default and provide a smoother network data flow with better performance at high speeds.	◔	◔	○
Microsoft Edge browser support.	○	○	○
PowerShell Desired State Configuration (DSC). Provides a set of PowerShell language extensions and cmdlets to declaratively specify how you want your software environment to be configured.	○	○	○
Visual Studio Code. Supports development operations such as debugging, task running, and version control to provide the tools a developer needs for a quick code-build-debug cycle.	○	○	○
.NET Core. Helps create modern web apps, microservices, libraries, and console applications that run on Windows, Mac, and Linux.	○	○	○

Get started

Built your future with Windows Server

Evaluate Windows Server 2022

Download Windows Admin Center