

Windows Server 2022 Launched: Numerous Security Improvements, Extended Support for 10 Years

Microsoft has begun rolling out Windows Server 2022. This is a Long Term Servicing Channel (LTSC) release, which comes with a host of enhanced security improvements.

Microsoft has begun rolling out Windows Server 2022. This is a Long Term Servicing Channel (LTSC) release, which comes with a host of enhanced security improvements.

Notably, this version will also mark the first time Secured-core has been included on the Windows Server platform to enhance protection against a range of threats.

At Microsoft Ignite 2021, Microsoft stated that Windows Server 2022 offers secure connectivity enabled by industry-standard AES 256 encryption . " Furthermore, this release will also include significant improvements to the Windows container runtime. For example, virtualized time zones and IPV6 support for globally scalable applications, as well as container engines for .NET, ASP.NET, and IIS applications ."

Windows Server 2022 comes in three variants: Standard, Datacenter, and Datacenter: Azure Edition. Starting August 21st, Windows Server 2022 will be available to customers on Volume Licensing Server Center. Server 2022 images are also available on Azure, the Product Evaluation Center, and Visual Studio.

Windows Server 2022 Languages and Optional Features	Description	Download	Key
Version 2022			Release Date 8/19/2021
Product Description			
Windows Server 2022 introduces advanced multi-layer security, hybrid capabilities with Azure, and a flexible application platform.			
As part of this release, we are bringing secured-core capabilities to help protect hardware, firmware, and Windows Server OS capabilities against advanced security threats. Secured-core server builds on technologies such as Windows Defender System Guard and Virtualization-based Security to minimize risk from firmware vulnerabilities and advanced malware. The new release also provides secured connectivity that introduces several new capabilities such as faster and more secure encrypted HTTPS connections, industry standard SMB AES 256 encryption and more.			
Windows Server 2022 improves hybrid server management with significantly improved VM management, an enhanced event viewer, and many more new capabilities in Windows Admin Center. Furthermore, this release includes significant improvements to Windows containers, such as smaller image sizes for faster download, simplified network policy implementation and containerization tools for .NET applications.			
System Requirements			
None Provided.			

Microsoft Server 2022 will have primary support for 5 years (ending October 13, 2026) and extended support for 10 years (ending October 14, 2031).

Secured-core servers with built-in threat protection.

Secured-core PCs are now considered a viable solution to the growing number of firmware vulnerabilities. Attackers can exploit these vulnerabilities to bypass Windows Secure Boot . This also addresses the lack of security-level management capabilities in many current endpoint security solutions.

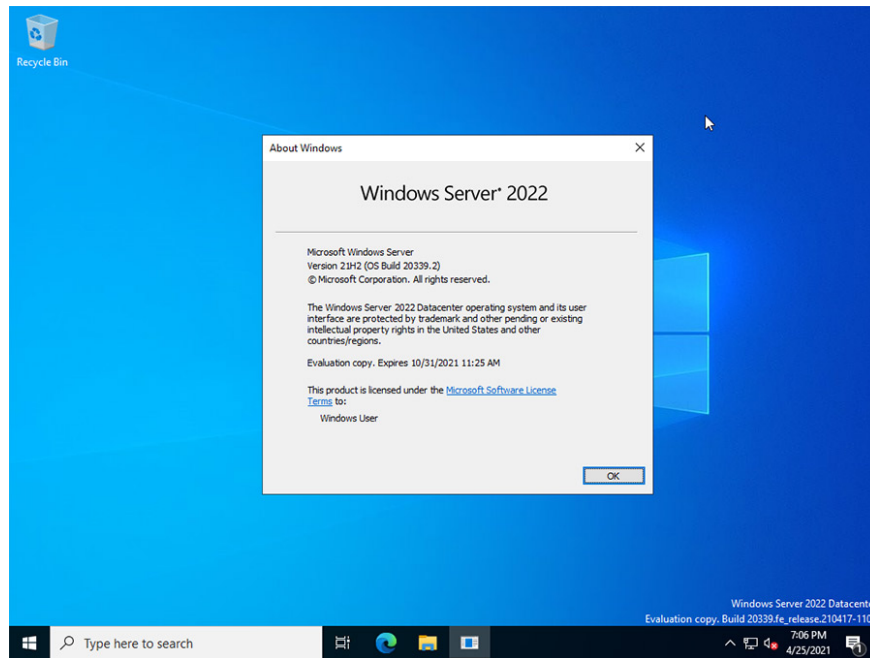
The built-in protection is designed to safeguard users from threats of exploiting firmware vulnerabilities and driver security flaws, and has been included in all Secured-core PCs since October 2019.

They can protect users against malware designed to exploit driver security vulnerabilities to disable security solutions.

Secured-core PCs are typically developed in collaboration with Microsoft and its OEM partners and silicon chip manufacturers. Secured-core PCs protect users against attacks by adhering to the following requirements:

1. **Securely boot Windows** : With integrated Hypervisor Enforced Integrity, Secured-core PCs only boot executables signed by known and approved entities. Additionally, the supervisor can set and enforce necessary permissions to prevent malware from attempting to modify memory and execute malicious code. Refer to how to download Windows 10 ISOs from Microsoft .
2. **Firmware-level protection** : System Guard Secure Launch uses the CPU to authenticate secure boot devices, preventing advanced firmware attacks.
3. **Identity protection** : Windows Hello allows you to log in without a password , while Credential Guard leverages helps prevent identity attacks.
4. **A secure operating environment, isolated from hardware** : Utilizing Trusted Platform Module 2.0 and a modern CPU with Trusted Dynamic Range Measurement (DRTM) to securely boot your PC and minimize firmware vulnerabilities.

Today's Secured-core servers adhere to these guidelines for secure boot-ups, self-protection against firmware security flaws, protection of the operating system from attacks, prevention of unauthorized access, and security of user identities and domain login credentials.



Security features on Windows Server 2022

Windows Server 2022, along with Secured-core, will add the following preventative protection capabilities to servers:

Enhance protection against vulnerability exploitation:

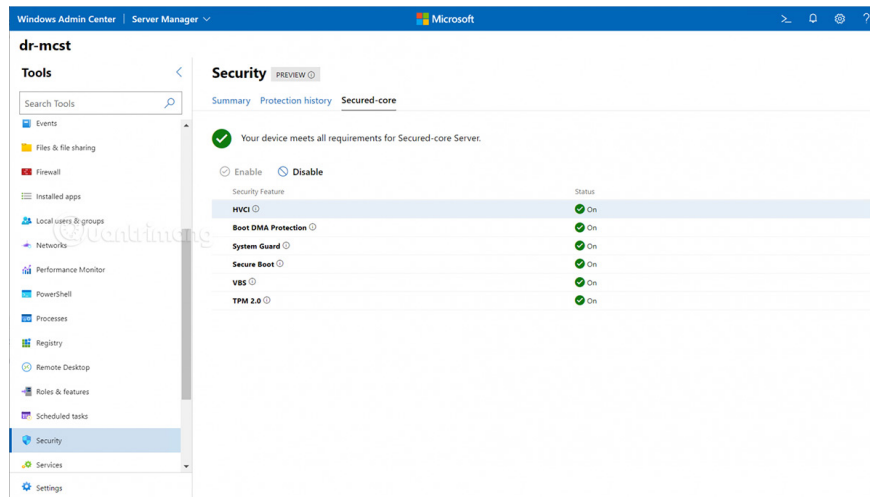
Hardware innovations enable the robust and effective deployment of vulnerability mitigation measures. Windows Server 2022 and critical applications will be secured from a common exploitation technique – return-directed programming (ROP) – often used to hijack a program's intended control flow.

Secure connection :

Secure connectivity is central to today's interconnected systems. Transport Layer Security (TLS) 1.3 is the latest version of the most widely deployed security protocol on the internet, supporting data encryption to provide a secure communication channel between two endpoints.

TLS 1.3 eliminates outdated cryptographic algorithms, enhancing security compared to older versions. Windows Server 2022 comes with TLS 1.3 enabled by default, helping to protect data on client machines connecting to the server.

HTTPS is also enabled by default, adding an extra layer of security when connecting to critical data, making data transfers more secure.



Several other new features of Windows Server 2022 have been announced:

1. Advanced multi-layered protection against threats can be easily enabled from the secured-core server.
2. Manage and control on-premise Windows Server with Azure Arc.
3. Manage virtual machines better with the latest Windows Admin Center.
4. Migrate your file server from on-premises to Azure with the new support script in Storage Migration Service.
5. Improved implementation of containerized applications with smaller image file sizes for faster downloads and simplified network policy enforcement.
6. Update .NET applications using the new containerization tool in Windows Admin Center.

According to Microsoft, in the future, the company will only release LTSC versions of Windows Server and will not release Semi-Annual Channel versions. These LTSC Windows Server releases will receive 10 years of support, including 5 years of official support and 5 years of extended support. Officials said Microsoft plans to release new versions of Windows Server every two to three years.

Microsoft will hold its Windows Server Summit online on September 16th, featuring the first public demos of the product.

You finished reading the article "**Windows Server 2022 Launched: Numerous Security Improvements, Extended Support for 10 Years**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.