DELL Technologies Microsoft

White Paper

Gain Advanced Security Protection with the Combined Capabilities of Windows Server 2022 and Next-Generation Dell EMC™ PowerEdge™ Servers

Harden business-critical workloads with a more secure hardware, firmware and operating system environment

Global cybercrime is expected to cost a total of USD 6 trillion in 2021, and go on to grow to USD 10.5 trillion in 2025, according to Cybersecurity Ventures.[1] Ransomware attacks alone have grown 61x in six years to USD $20 billion in 2021, with an attack currently occurring every 11 seconds.[1] A 2021 IDC survey found that more than one third of organizations polled worldwide had suffered a ransomware attack or breach in the past 12 months (and often more than one attack).[2] And while IBM estimates that the cost of a single data breach now stands at USD $4.24 million,[3] the true cost of breaches can be much higher: in some instances, hospitals in the United States have had to divert emergency patients to other hospitals and turn away ambulances because of ransomware attacks.[4]

Firmware attacks can be a particularly pernicious threat for organizations. This is because an attack vectored on firmware can implant malware before the operating system (OS)—and thus the software-based security running on that OS—has even started. Yet less than half of organizations have taken steps to harden their systems against firmware attacks, even as such attacks have grown five times more frequent in the last five years.[5] At the end of the day, workloads are only as secure as the entire stacks that they run on.

To meet this exponential growth to the frequency, variety and costliness of malware threats, modern security must be multilayered. This is because malware can compromise systems at the hardware and firmware levels, or during boot up, all areas where solely software-defined security is impotent. To counter this vulnerability, modern server security is not a single-pronged strategy. It must be built into the entire infrastructure stack. The combination of next-generation Dell EMC™ PowerEdge™ servers and Windows Server 2022 simplifies for administrators the important task of aligning hardware, firmware and OS in order to adequately secure business-critical workloads.

The Combined Benefits of Windows Server 2022 Secured-Core Server and Next-Generation PowerEdge Servers

Secured-core server is a new feature in Windows Server 2022 that uses hardware, firmware and OS capabilities to provide protection against current and future threats. The combination of Windows Server 2022 Secured-core server software running on next-generation PowerEdge server hardware provides three substantial benefits for organizations like yours:

- Advanced protection
- Preventative defense
- Simplified security

Advanced Protection

Based on Microsoft threat-intelligence data, Secured-core PCs provide more than twice the protection against infection as regular PCs; Microsoft is now bringing this same technology into the server space with Windows Server 2022 Secured-core servers.[5] Protections enabled by a Secured-core server are targeted to create a secure platform for critical workloads and data on that server. Specifically, Secured-core servers use processor support for Dynamic Root of Trust for Measurement (DRTM) technology to put firmware in a hardware-based sandbox. This isolation helps to limit the impact of vulnerabilities in millions of lines of highly privileged firmware code.

Complementing the firmware-isolation in Windows Server 2022, virtualization-based security (VBS) isolates critical parts of the OS—such as the kernel—from the rest of the system. This helps to ensure that servers remain devoted to running critical workloads, and it helps protect related applications and data from attack and exfiltration.

To further harden the firmware in PowerEdge servers from attack, Dell Technologies helps secure the supply chain for PowerEdge servers to help ensure that no one has tampered with the server while in transit from the factory to the customer site (explained in greater detail in Additional Security Through Dell Technologies Supply-Chain Integrity below).

Preventative Defense

Secured-core functionality helps proactively defend against and disrupt many of the paths that attackers might use to exploit your systems. Hypervisor-protected code integrity (HVCI) in VBS isolates the code integrity (CI) decision-making function from the rest of the Windows OS, which helps ensure that the only way kernel memory can become executable is through a CI verification. VBS also enables the use of Windows Defender Credential Guard, in which user credentials and secrets are stored in a virtual container that the OS cannot access directly.

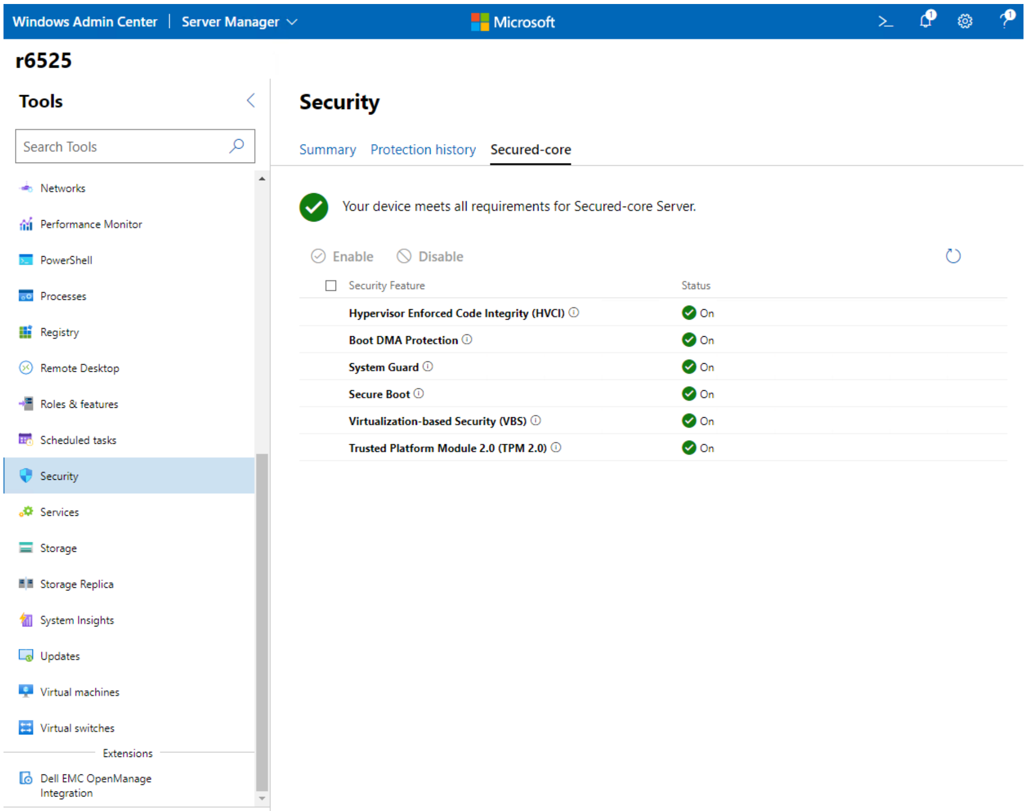
Trusted Platform Module 2.0 (TPM 2.0) comes standard with Secured-core servers, and it provides a protected store for sensitive keys and data, such as measurements of the components loaded during boot. Being able to verify that firmware that runs during boot is validly signed by the expected author and has not been tampered with helps improve security. This hardware root-of-trust also elevates the protection provided by capabilities like BitLocker Drive Encryption, which uses TPM 2.0 and facilitates the creation of attestation-based workflows that can be incorporated into zero-trust security strategies. Taken together, these defenses enable your IT and SecOps teams to better use their time across the many areas of security that need their attention.

Next-generation PowerEdge servers support industry-standard Unified Extensible Firmware Interface (UEFI) Secure Boot. UEFI Secure Boot checks the cryptographic signatures of UEFI drivers and other code loaded prior to the OS running to help ensure that malware has not tampered with the firmware. Moreover, PowerEdge servers support TPM 2.0 in order to elevate security for firmware and the OS.

Simplified Security

When you acquire a Secured-core PowerEdge server, you have an assurance that Dell Technologies has provided a set of hardware, firmware and drivers that satisfy the Secured-core promise. Microsoft collaborates closely with Dell Technologies to simplify security enablement on PowerEdge servers.

New functionality in Windows Admin Center makes it easy for administrators to configure the OS security features of Windows Server 2022 Secured-core servers. The new Windows Admin Center security functionality allows administrators to enable advanced security with a click of a button. Windows Admin Center presents the status of all of the required security features for Windows Server 2022 Secured-core servers and enables administrators to turn on features as necessary from a single location.



Your device meets all requirements for Secured-core Server.

Security Feature	Status
Hypervisor Enforced Code Integrity (HVCI)	On
Boot DMA Protection	On
System Guard	On
Secure Boot	On
Virtualization-based Security (VBS)	On
Trusted Platform Module 2.0 (TPM 2.0)	On

Figure 1. Secured-core confirmation screen in Windows Admin Center

Dell EMC™ OpenManage™ Integration with Windows Admin Center is an extension for Windows Admin Center that further simplifies management of Secured-core servers. This Windows Admin Center extension simplifies the security tasks (among others) of IT administrators by remotely managing PowerEdge servers. Within the context of Windows Server 2022 Secure-core servers, the OpenManage Integration with Windows Admin Center extension enables you to view your inventory of PowerEdge servers from within Windows Admin Center, and it provides a unified view of health, hardware and firmware inventory information of the PowerEdge server components.

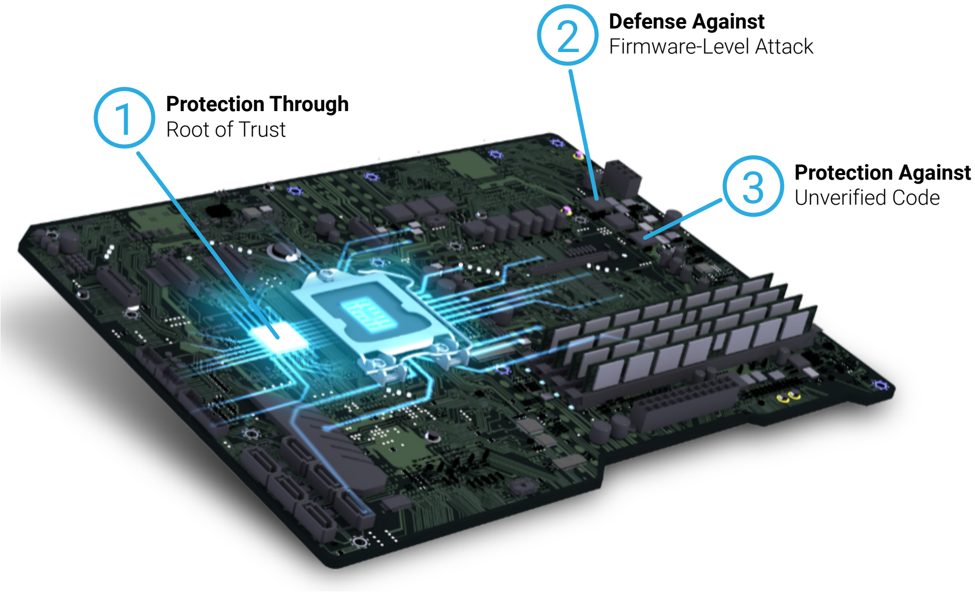
PowerEdge Server Support for Windows Server 2022 Secure-Core Servers

Because of the multi-layered nature of Secured-core server defenses, support from your hardware OEM is crucial. PowerEdge servers are tested and certified by Dell Technologies to ensure that hardware and firmware satisfy the requirements of Windows Server 2022 security features. In addition, the hardware and firmware in PowerEdge servers are configured to enable Windows Server 2022 Secure-core server. Table 1 details how hardware in PowerEdge servers undergirds Windows Server 2022 features.

Table 1. Mapping of Windows Server 2022 security features and key supporting features in next-generation Dell EMC™ PowerEdge™ servers

	Windows Server 2022	Next-generation Dell EMC™ PowerEdge™ servers
Advanced protection	Secured-core systems put firmware in a hardware-based sandbox helping to limit the impact of firmware-based vulnerabilities. VBS isolates critical parts of the OS from advanced malware.	Dell Technologies helps secure the supply chain for PowerEdge servers to help ensure that no one has tampered with the server or compromised the firmware while in transit from the factory to the customer site.
Preventative defense	VBS features such as HVCI and Windows Defender Credential Guard prevent entire classes of vulnerabilities and better protect sensitive assets like credentials. TPM 2.0 provides hardware root-of-trust used as a secure foundation.	PowerEdge servers support industry-standard UEFI Secure Boot to check the cryptographic signatures of UEFI drivers and other code loaded prior to the OS running. PowerEdge servers support TPM 2.0.
Simplified security	Windows Admin Center provides easy access to configure Secured-core servers.	Microsoft collaborates with Dell Technologies to simplify security enablement on PowerEdge servers. Windows Admin Center integration with Dell EMC™ OpenManage™ further simplifies management of Secured-core servers.

Anatomy of Advanced, Multilayered Security



1

Protection Through Root of Trusts

Partnering with leading OEMs like Dell Technologies and silicon vendors like Intel and AMD, Secured-core servers use industry-standard hardware root of trust coupled with security capabilities built into today's modern CPUs.

Secured-core servers use TPM 2.0 and a modern CPU with DRTM to boot up servers more securely and minimize firmware vulnerabilities.

2

Defense Against Firmware-Level Attacks

Secured-core servers use hardware-rooted security in the modern CPU to launch the system into a trusted state, preventing advanced malware from tampering with the system and attacking at the firmware level.

System Guard Secure Launch uses the CPU to validate the device to boot more securely, helping prevent advanced firmware attacks.

3

Protection Against Unverified Code

Code running within the trusted computing base runs with integrity and is not subject to exploits or attacks. Enabled with HVCI, a Secured-core server only starts executables signed by known and approved authorities.

The hypervisor sets and enforces permissions to prevent malware from attempting to modify the memory and make it executable.

Next-Generation PowerEdge Server Support for Secure Connectivity in Windows Server 2022

Next-generation PowerEdge servers support Server Message Block (SMB) AES-256 encryption for security-conscious workloads. This support means that PowerEdge servers running Windows Server 2022 can provide end-to-end encryption for workload data for extra security. The 256-bit AES encryption used for SMB in Windows Server 2022 is also robust enough to be resistant even to brute-force attacks by quantum computers if strong enough passwords are used.

PowerEdge servers and Windows Server 2022 further extend end-to-end SMB encryption from individual servers to the internal communications of clusters with AES-256 encryption for East-West SMB data traffic. These additional SMB encryption controls further harden workloads and close avenues of attack.

Finally, Windows Server 2022 makes use of Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) included in 3rd Generation Intel® Xeon® Scalable processors and vectorized AES encryption for 256-bit (vAES256) included in AMD EPYC™ Zen 3 processors. These advanced processors' instruction sets boost performance for AES-256 encryption in PowerEdge servers. By making use of these advanced security technologies, Dell Technologies and Microsoft help ensure that you don't have to choose between robust security and responsiveness for business-critical workloads.

Additional Security Through Dell Technologies Supply-Chain Integrity

Dell Technologies supply-chain integrity protects hardware and firmware components from compromise during manufacturing and shipping. In the domain of hardware integrity, Dell Technologies works to ensure that there is no product tampering or insertion of counterfeit components before shipping products to customers. The controls that Dell Technologies has in place span supplier selection, sourcing, production processes and governance through auditing and testing. Material inspections during production help identify components that are mismarked, deviate from normal performance parameters or contain an incorrect electronic identifier.

For software integrity, Dell Technologies seeks to ensure that no malware gets inserted in firmware or device drivers before shipping a product to customers, in addition to preventing any coding vulnerabilities. Dell Technologies maintains ISO 9001 certification for all global manufacturing sites. Strict adherence to these processes and controls helps minimize the risk of counterfeit components being embedded among the Dell Technologies™ products and of malware getting inserted into firmware or device drivers. Moreover, Dell Technologies implements these measures as part of the Software Development Lifecycle (SDLC) process.

Dell Technologies also works to help ensure the physical security of manufacturing facilities and transportation chains. Dell Technologies requires certain factories where Dell Technologies products are built to meet specified Transported Asset Protection Association (TAPA) facility security requirements, including the use of monitored closed-circuit cameras in key areas, access controls and continuously guarded entries and exits. Dell Technologies has also put in place protective measures to guard products against theft and tampering during transport as part of an industry-leading logistics program. Finally, Dell Technologies Secured Component Verification (SCV) for PowerEdge servers enables Dell Technologies customers to verify that a PowerEdge server received by the customer matches what was manufactured in the factory.

Protect Your Vital Workloads with a Better Security Foundation from Windows Server 2022 and Next-Generation Dell EMC PowerEdge Servers

Workloads are only as secure as the foundation that they run on. The threat from malware and data breaches will only continue to grow in the future, particularly as malicious actors continue to explore avenues of attack immune to traditional, software-based security. Firmware attacks specifically target servers during the boot process, before software-based security has even begun protecting systems. Modern server protection requires multi-pronged security that spans hardware, firmware and the OS.

Upgrading to Windows Server 2022 can make more sense now than ever. The Secured-core server feature in Windows Server 2022 helps organizations counter threats to both firmware and the OS. When paired with the hardware- and software-integrity protections of Dell Technologies, next-generation Dell EMC PowerEdge servers running Windows Server 2022 can provide modern security to the entire stack for hardware, firmware and the OS. And the secure-connectivity features in Windows Server 2022 and supported in next-generation PowerEdge servers extend this security beyond individual servers to entire clusters within your data center. Moreover, support for Windows Server 2012 ends in October 2023, which means it is time to start making upgrade plans.[6]

To learn more about how Windows Server 2022 and next-generation Dell EMC PowerEdge servers can help secure your critical workloads and data, visit www.delltechnologies.com/en-us/solutions/microsoft-oem/.

[1] Cybersecurity Ventures. “Cybercrime To Cost The World $10.5 Trillion Annually By 2025.” November 2020. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

[2] IDC. “IDC Survey Finds More Than One Third of Organizations Worldwide Have Experienced a Ransomware Attack or Breach.” August 2021. www.idc.com/getdoc.jsp?containerId=prUS48159121.

[3] IBM. “How much does a data breach cost?” 2021. www.ibm.com/security/data-breach.

[4] Dan Goodin. “Hospitals hamstrung by ransomware are turning away patients.” *Ars Technica*. August 2021. https://arstechnica.com/gadgets/2021/08/hospitals-hamstrung-by-ransomware-are-turning-away-patients/.

[5] Microsoft. “New Security Signals study shows firmware attacks on the rise; here’s how Microsoft is working to help eliminate this entire class of threats.” March 2021. www.microsoft.com/security/blog/2021/03/30/new-security-signals-study-shows-firmware-attacks-on-the-rise-heres-how-microsoft-is-working-to-help-eliminate-this-entire-class-of-threats/.

[6] As of the writing of this paper. For the latest information about end of support for Windows Server 2012, visit the Windows Server 2012 lifecycle page: https://docs.microsoft.com/en-us/lifecycle/products/windows-server-2012.

The information in this publication is provided as is. Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Dell Inc. believes the information in this document is accurate as of its publication date. The information is subject to change without notice.