DELL Technologies

Microsoft

Whitepaper

Geavanceerde beveiliging verwerven met de gecombineerde mogelijkheden van Windows Server 2022 en de Dell EMC™ PowerEdge™ servers van de volgende generatie

Versterk bedrijfskritieke workloads met een veiligere hardware-, firmware- en besturingssysteemomgeving

Volgens Cybersecurity Ventures[1] zal cybercriminaliteit in 2021 wereldwijd naar verwachting in totaal 6 biljoen dollar kosten en zal dit bedrag in 2025 groeien tot 10,5 biljoen dollar. Alleen al ransomware-aanvallen zijn in zes jaar tijd met een factor 61 gegroeid tot 20 miljard dollar in 2021, waarbij er elke 11 seconden een aanval plaatsvindt.[1] Uit een IDC-enquête uit 2021 bleek dat meer dan een derde van de ondervraagde organisaties wereldwijd in de afgelopen 12 maanden te maken had gehad met een ransomware-aanval of -inbreuk (en vaak meer dan één aanval).[2] En hoewel IBM schat dat de kosten van een enkel datalek nu USD 4,24 miljoen[3] bedragen, kunnen de werkelijke kosten van inbreuken veel hoger zijn: in sommige gevallen moesten ziekenhuizen in de Verenigde Staten spoedeisende patiënten omboeken naar andere ziekenhuizen en ambulances weigeren vanwege ransomware-aanvallen.[4]

Firmware-aanvallen kunnen een bijzonder ernstige dreiging vormen voor organisaties. Dit komt doordat bij een aanval op firmware malware kan worden geïmplanteerd vóór het besturingssysteem (OS), en dus voordat de softwarematige beveiliging die op dat besturingssysteem wordt uitgevoerd, zelfs maar is gestart. Toch heeft minder dan de helft van de organisaties stappen ondernomen om hun systemen te beschermen tegen firmware-aanvallen, ook al zijn dergelijke aanvallen de afgelopen vijf jaar vijf keer zo frequent geworden.[5] Het resultaat is dat workloads slechts zo veilig zijn als de gehele stack waarop ze worden uitgevoerd.

Om in te spelen op deze exponentiële groei van de frequentie, verscheidenheid en kosten van malwaredreigingen, moet moderne beveiliging uit meerdere lagen bestaan. Dit is nodig omdat malware systemen kan aantasten op hardware- en firmwareniveau, of tijdens het opstarten, allemaal gebieden waarop softwaregedefinieerde beveiliging alleen machteloos is. Om deze kwetsbaarheid het hoofd te kunnen bieden, berust moderne serverbeveiliging niet op een eenzijdige strategie. Beveiliging moet worden ingebouwd in de gehele infrastructuurstack. De combinatie van Dell EMC™ PowerEdge™ servers van de volgende generatie en Windows Server 2022 vereenvoudigt de belangrijke taak van beheerders om hardware, firmware en besturingssysteem op elkaar af te stemmen zodat bedrijfskritieke workloads adequaat zijn beveiligd.

De gecombineerde voordelen van Windows Server 2022 Secured-Core Server en PowerEdge servers van de volgende generatie

Secured-core server is een nieuwe functie in Windows Server 2022 die gebruikmaakt van hardware-, firmware- en OS-mogelijkheden om bescherming te bieden tegen huidige en toekomstige dreigingen. De combinatie van Windows Server 2022 Secured-core serversoftware die wordt uitgevoerd op PowerEdge serverhardware van de volgende generatie biedt drie belangrijke voordelen voor organisaties zoals de uwe:

- Geavanceerde bescherming
- Preventieve verdediging
- Vereenvoudigde beveiliging

Geavanceerde bescherming

Op basis van data over dreigingsinformatie van Microsoft bieden Secured-core pc's meer dan twee keer zoveel bescherming tegen infectie als gewone pc's; Microsoft brengt dezelfde technologie nu naar de serverruimte met Windows Server 2022 Secured-core-servers.[5] Beschermingen die mogelijk worden gemaakt door een Secured core server zijn gericht op het creëren van een veilig platform voor kritieke workloads en data op die server. Secured-core servers gebruiken met name processorondersteuning voor DRTM-technologie (Dynamic Root of Trust for Measurement) om firmware in een op hardware gebaseerde sandbox te plaatsen. Deze isolatie beperkt de impact van beveiligingslekken in miljoenen regels firmwarecode met hoge bevoegdheden.

Als aanvulling op de firmware-isolatie in Windows Server 2022 isoleert Virtualization-Based Security (VBS) essentiële onderdelen van het besturingssysteem, zoals de kernel, van de rest van het systeem. Dit zorgt ervoor dat servers kritieke workloads blijven uitvoeren en gerelateerde applicaties en data beschermd zijn tegen aanvallen en exfiltratie.

Om de firmware in PowerEdge servers verder te beveiligen tegen aanvallen, beveiligt Dell Technologies de leveringsketen voor PowerEdge servers om ervoor te zorgen dat niemand de server kan manipuleren tijdens het transport van de fabriek naar de locatie van de klant (uitgebreider uitgelegd in Extra beveiliging dankzij integriteit van de leveringsketen van Dell Technologies hieronder).

Preventieve verdediging

Secured-core-functionaliteit verdedigt proactief tegen veel van de paden die aanvallers kunnen misbruiken om uw systemen uit te buiten en deze te verstoren. Hypervisor-protected Code Integrity (HVCI) in VBS isoleert de besluitvormingsfunctie voor code-integriteit (CI) van de rest van het Windows-besturingssysteem, wat ervoor zorgt dat kernelgeheugen alleen uitvoerbaar kan worden via een CI-verificatie. VBS maakt ook het gebruik van Windows Defender Credential Guard mogelijk, waarin gebruikersreferenties en -geheimen worden opgeslagen in een virtuele container waartoe het besturingssysteem geen directe toegang heeft.

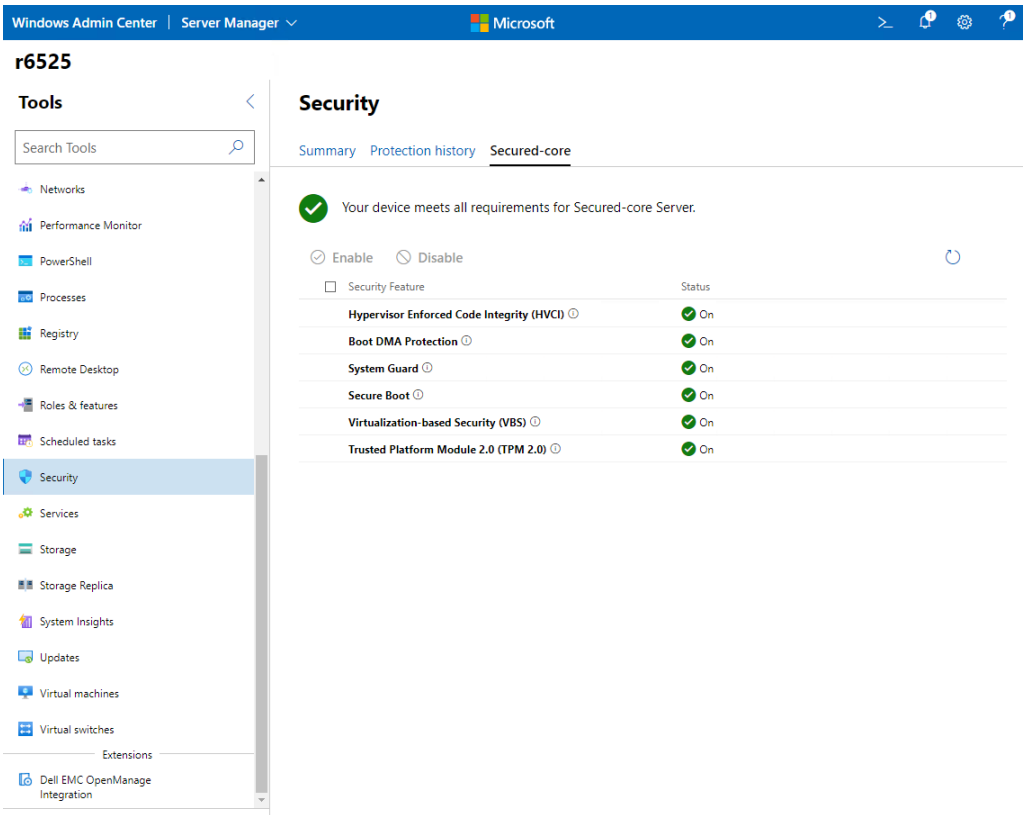
Trusted Platform Module 2.0 (TPM 2.0) wordt standaard geleverd met Secured-core servers en biedt een beschermd archief voor gevoelige sleutels en data, zoals metingen van de componenten die tijdens het opstarten worden geladen. De mogelijkheid om te controleren of firmware die tijdens het opstarten wordt uitgevoerd, geldig is ondertekend door de verwachte auteur en dat deze niet is gemanipuleerd, verbetert de beveiliging. Deze hardwarematige root-of-trust verhoogt ook de bescherming die wordt geboden door mogelijkheden zoals BitLocker Drive Encryption, dat TPM 2.0 gebruikt en het maken van op attests gebaseerde workflows vergemakkelijkt die kunnen worden opgenomen in zero-trust beveiligingsstrategieën. Samen stellen deze verdedigingen uw IT- en SecOps-teams in staat om hun tijd beter te gebruiken voor de vele beveiligingsgebieden die hun aandacht nodig hebben.

PowerEdge servers van de volgende generatie ondersteunen de industriestandaard Unified Extensible Firmware Interface (UEFI) Secure Boot. UEFI Secure Boot controleert de cryptografische handtekeningen van UEFI-drivers en andere code die wordt geladen voordat het besturingssysteem wordt uitgevoerd om er zeker van te zijn dat malware de firmware niet heeft gemanipuleerd. Bovendien ondersteunen PowerEdge servers TPM 2.0 om de beveiliging van firmware en het besturingssysteem te verbeteren.

Vereenvoudigde beveiliging

Wanneer u een PowerEdge Secured-core server aanschaft, weet u zeker dat Dell Technologies een set hardware, firmware en drivers heeft geleverd die voldoen aan de belofte van Secured-core. Microsoft werkt nauw samen met Dell Technologies om de beveiliging van PowerEdge servers te vereenvoudigen.

Dankzij nieuwe functionaliteit in Windows Admin Center kunnen beheerders gemakkelijk de OS-beveiligingsfuncties van Windows Server 2022 Secured-core servers configureren. Met de nieuwe beveiligingsfunctionaliteit van Windows Admin Center kunnen beheerders met één klik op een knop geavanceerde beveiliging inschakelen. Windows Admin Center geeft de status weer van alle vereiste beveiligingsfuncties voor Windows Server 2022 Secured-core servers en stelt beheerders in staat om functies zo nodig vanaf een enkele locatie in te schakelen.



Afbeelding 1. Bevestigingsscherm Secured-core in Windows Admin Center

Dell EMC™ OpenManage™ integratie met Windows Admin Center is een uitbreiding voor Windows Admin Center die het beheer van Secured-core servers verder vereenvoudigt. Deze Windows Admin Center-extensie vereenvoudigt onder andere de beveiligingstaken van IT-beheerders door PowerEdge servers op afstand te beheren. Binnen de context van Windows Server 2022 Secure-core servers kunt u met de extensie OpenManage integratie met Windows Admin Center uw inventaris van PowerEdge servers bekijken vanuit Windows Admin Center. Deze biedt een uniforme weergave van de status-, hardware- en firmware-inventarisinformatie van de PowerEdge servercomponenten.

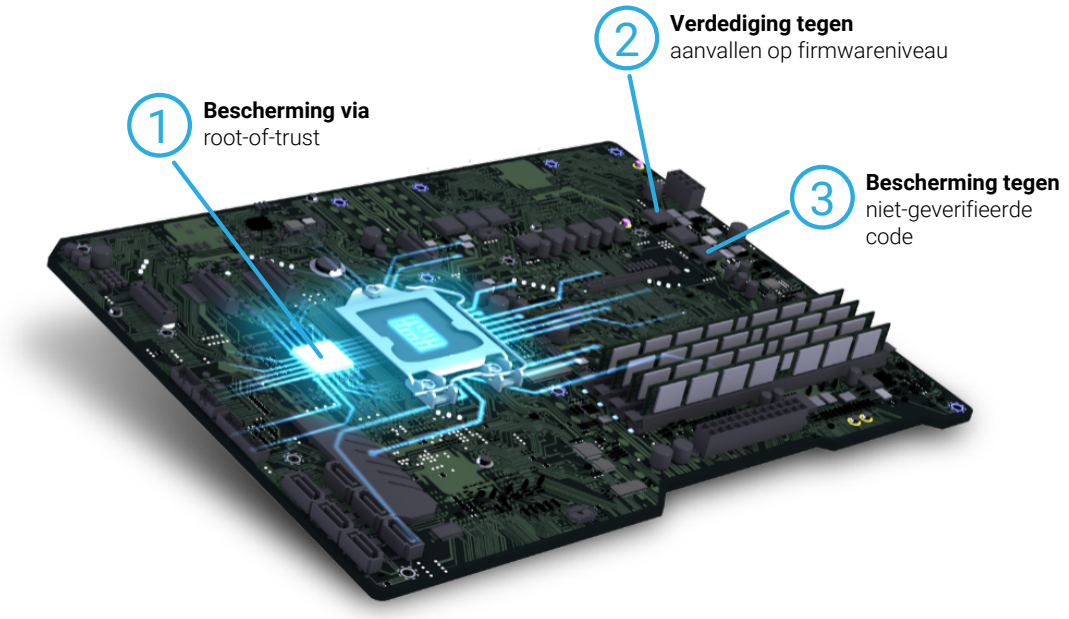
PowerEdge serverondersteuning voor Windows Server 2022 Secured-core servers

Vanwege de meerlaagse aard van Secured-core serververdediging, is ondersteuning van uw hardware-OEM cruciaal. PowerEdge servers worden getest en gecertificeerd door Dell Technologies om ervoor te zorgen dat hardware en firmware voldoen aan de vereisten van Windows Server 2022-beveiligingsfuncties. Bovendien zijn de hardware en firmware in PowerEdge servers geconfigureerd om Windows Server 2022 Secured-core server in te schakelen. In tabel 1 wordt beschreven hoe hardware in PowerEdge servers de functies van Windows Server 2022 ondersteunt.

Tabel 1. Toewijzing van Windows Server 2022-beveiligingsfuncties en belangrijke ondersteunende functies in Dell EMC™ PowerEdge™ servers van de volgende generatie

	Windows Server 2022	Dell EMC™ PowerEdge™ servers van de volgende generatie
Geavanceerde bescherming	Secured-core systemen plaatsen firmware in een op hardware gebaseerde sandbox, waardoor de impact van beveiligingslekken in de firmware wordt beperkt. VBS isoleert kritieke onderdelen van het besturingssysteem tegen geavanceerde malware.	Dell Technologies beveiligt de leveringsketen van PowerEdge servers door ervoor te zorgen dat niemand de server kan manipuleren of de firmware kan wijzigen tijdens het transport van de fabriek naar de locatie van de klant.
Preventieve verdediging	VBS-functies zoals HVCI en Windows Defender Credential Guard voorkomen hele klassen van beveiligingslekken en beschermen gevoelige productiemiddelen zoals referenties beter. TPM 2.0 biedt hardwarematige root-of-trust die als veilige basis wordt gebruikt.	PowerEdge servers ondersteunen industriestandaard UEFI Secure Boot om de cryptografische handtekeningen te controleren van UEFI-drivers en andere code die wordt geladen voordat het besturingssysteem wordt uitgevoerd. PowerEdge servers ondersteunen TPM 2.0.
Vereenvoudigde beveiliging	Windows Admin Center biedt eenvoudige toegang tot het configureren van Secured-core servers.	Microsoft werkt samen met Dell Technologies om het inschakelen van beveiliging op PowerEdge servers te vereenvoudigen. De integratie van Windows Admin Center met Dell EMC™ OpenManage™ vereenvoudigt het beheer van Secured-core servers nog verder.

De anatomie van geavanceerde, meerlaagse beveiliging



1 Bescherming via root-of-trust

In samenwerking met toonaangevende OEM's zoals Dell Technologies en siliciumleveranciers zoals Intel en AMD, maken Secured-core servers gebruik van industriestandaard hardwarematige root-of-trust in combinatie met beveiligingsmogelijkheden die zijn ingebouwd in de moderne CPU's van vandaag.

Secured-core servers gebruiken TPM 2.0 en een moderne CPU met DRTM om servers veiliger op te starten en kwetsbaarheden in de firmware te minimaliseren.

2 Verdediging tegen aanvallen op firmwareniveau

Secured-core servers maken gebruik van hardwarebeveiliging in de moderne CPU om het systeem in een vertrouwde staat te starten, zodat geavanceerde malware het systeem niet kan manipuleren en geen aanvallen op firmwareniveau kan uitvoeren.

System Guard Secure Launch maakt gebruik van de CPU om te valideren dat het apparaat veiliger opstart, waardoor geavanceerde firmware-aanvallen worden voorkomen.

3 Bescherming tegen niet-geverifieerde code

Code die wordt uitgevoerd binnen de vertrouwde computingbasis wordt met integriteit uitgevoerd en is niet onderhevig aan exploits of aanvallen.

Een Secured core-server met HVCI start alleen uitvoerbare bestanden die zijn ondertekend door bekende en goedgekeurde instanties. De hypervisor stelt machtigingen in en dwingt deze af om te voorkomen dat malware probeert het geheugen te wijzigen en uitvoerbaar te maken.

Ondersteuning voor PowerEdge servers van de volgende generatie voor veilige connectiviteit in Windows Server 2022

De volgende generatie PowerEdge servers ondersteunt Server Message Block (SMB) AES-256-versleuteling voor beveiligingsbewuste workloads. Deze ondersteuning betekent dat PowerEdge servers met Windows Server 2022 end-to-end versleuteling kunnen bieden voor workloaddata voor extra beveiliging. De 256-bits AES-versleuteling die wordt gebruikt voor het mkb in Windows Server 2022 is dusdanig robuust dat deze zelfs bestand is tegen brute-force-aanvallen door kwantumcomputers als er sterke wachtwoorden worden gebruikt.

PowerEdge servers en Windows Server 2022 breiden end-to-end SMB-versleuteling verder uit van afzonderlijke servers naar de interne communicatie van clusters met AES-256-versleuteling voor dataverkeer van server naar server binnen een datacenter. Deze extra SMB-versleutelingscontroles versterken workloads verder en sluiten aanvalsmogelijkheden uit.

Tot slot maakt Windows Server 2022 gebruik van Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) dat is opgenomen in de 3e generatie Intel® Xeon® schaalbare processors en gevectoriseerde 256-bits AES-versleuteling (vAES256) die is opgenomen in AMD EPYC™ Zen 3-processors. De instructiesets van deze geavanceerde processors verhogen de prestaties voor AES-256-versleuteling in PowerEdge servers. Door gebruik te maken van deze geavanceerde beveiligingstechnologieën zorgen Dell Technologies en Microsoft ervoor dat u niet hoeft te kiezen tussen robuuste beveiliging en responstijd voor bedrijfskritieke workloads.

Extra beveiliging dankzij integriteit van de leveringsketen van Dell Technologies

De integriteit van de leveringsketen van Dell Technologies beschermt hardware- en firmwarecomponenten tegen inbreuken tijdens productie en verzending. Op het gebied van hardware-integriteit doet Dell Technologies er alles aan om ervoor te zorgen dat het product niet wordt gemanipuleerd en dat er geen vervalste onderdelen in worden geplaatst voordat producten naar klanten worden verzonden. De controles die Dell Technologies heeft ingesteld, omvatten een strenge selectie van leveranciers, inkoop- en productieprocessen, en governance door middel van audits en tests. Bij materiaalinspecties tijdens de productie worden componenten geïdentificeerd die mogelijk verkeerd zijn gemarkeerd, afwijken van de normale prestatieparameters of een onjuiste elektronische ID hebben.

Wat betreft software-integriteit probeert Dell Technologies ervoor te zorgen dat er geen malware in firmware of apparaatdrivers wordt geplaatst voordat producten naar klanten worden verzonden en dat eventuele kwetsbaarheden in de codering worden voorkomen. Dell Technologies beschikt over ISO 9001-certificering voor alle wereldwijde productielocaties. Strikte naleving van deze processen en controles minimaliseert het risico dat er vervalste componenten in de producten van Dell Technologies™ worden geïntegreerd en dat er malware in de firmware of apparaatdrivers wordt geplaatst. Bovendien implementeert Dell Technologies deze maatregelen als onderdeel van het SDLC-proces (Software Development Lifecycle).

Dell Technologies zet zich daarnaast in voor de fysieke beveiliging van productiefaciliteiten en transportketens. Dell Technologies vereist dat bepaalde fabrieken waar producten van Dell Technologies worden gemaakt, voldoen aan de gespecificeerde beveiligingsvereisten van de TAPA (Transported Asset Protection Association), waaronder het gebruik van bewakingscamera's met een gesloten circuit op belangrijke locaties, toegangscontroles en continu bewaakte in- en uitgangen. Dell Technologies heeft als onderdeel van een toonaangevend logistiek programma ook beschermende maatregelen getroffen om producten te beschermen tegen diefstal en sabotage tijdens transport. Tot slot kunnen klanten van Dell Technologies met SCV (Secured Component Verification) voor PowerEdge servers controleren of een PowerEdge server die door de klant wordt ontvangen, overeenkomt met de server die in de fabriek is geproduceerd.

Bescherm uw vitale workloads met een betere beveiliging tegen Windows Server 2022 en de volgende generatie Dell EMC PowerEdge servers

Workloads zijn slechts zo veilig als het fundament waarop ze worden uitgevoerd. De dreiging van malware en datalekken zal in de toekomst alleen maar blijven toenemen, vooral omdat kwaadwillenden aanvalsmogelijkheden blijven verkennen die immuun zijn voor traditionele, softwarematige beveiliging. Firmware-aanvallen richten zich specifiek op servers tijdens het opstartproces, voordat softwarematige beveiliging zelfs maar is begonnen met het beschermen van systemen. Moderne serverbescherming vereist meervoudige beveiliging die hardware, firmware en besturingssysteem omvat.

Upgraden naar Windows Server 2022 kan nu logischer zijn dan ooit. Met de Secured-core-functie in Windows Server 2022 kunnen organisaties dreigingen voor zowel firmware als besturingssysteem tegengaan. In combinatie met de hardware- en software-integriteitsbescherming van Dell Technologies kunnen Dell EMC PowerEdge servers van de volgende generatie met Windows Server 2022 moderne beveiliging bieden voor de hele stack voor hardware, firmware en besturingssysteem. En de functies voor veilige connectiviteit in Windows Server 2022 die worden ondersteund in PowerEdge servers van de volgende generatie breiden deze beveiliging uit van individuele servers naar volledige clusters binnen uw datacenter. Bovendien eindigt de ondersteuning voor Windows Server 2012 in oktober 2023, wat betekent dat het tijd is om upgradeplannen te gaan maken.[6]

Ga naar www.delltechnologies.com/en-us/solutions/microsoft-oem/ voor meer informatie over hoe Windows Server 2022 en de volgende generatie Dell EMC PowerEdge servers kunnen helpen bij het beveiligen van uw kritieke workloads en data.

[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. "Uit onderzoek van IDC blijkt dat meer dan een derde van de organisaties wereldwijd te maken heeft gehad met een ransomware-aanval of inbreuk." Augustus 2021.
[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.* Augustus 2021. https://arstechnica.com/gadgets/2021/08/hospitals-hamstrung-by-ransomware-are-turning-away-patients/.
[5] Microsoft. "Nieuw onderzoek van Security Signals toont aan dat firmware-aanvallen toenemen. Microsoft doet het volgende om een einde te maken aan deze hele klasse van bedreigingen." Maart 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] Op het moment van schrijven van dit artikel. Ga voor de meest recente informatie over het einde van de ondersteuning van Windows Server 2012 naar de levenscycluspagina voor Windows Server 2012: https://docs.microsoft.com/en-us/lifecycle/products/windows-server-2012.

DELL Technologies

Microsoft

Moderniseer met Windows Server 2022.
Het besturingssysteem dat klaar is voor de cloud en on-premise investeringen een boost geeft met hybride opties.