DELL Technologies

Microsoft

Informationsdokument

Få avancerat säkerhetsskydd med kombinerade funktioner från Windows Server 2022 och nästa generations Dell EMC™ PowerEdge™-servrar

Stärk företagskritiska arbetsbelastningar med en säkrare miljö för hårdvara, fast mjukvara och operativsystem

Kostnaden för global cyberbrottslighet förväntas uppgå till totalt 6 biljoner USD 2021 och fortsätta växa till 10,5 biljoner USD 2025, enligt Cybersecurity Ventures.[1] Enbart attacker med utpressningsvirus har ökat med 61 gånger på sex år till 20 miljarder USD 2021, med en attack som för närvarande inträffar var 11:e sekund.[1] En IDC-undersökning från 2021 visade att mer än en tredjedel av de tillfrågade organisationerna världen över hade drabbats av en attack eller ett intrång från utpressningsvirus under de senaste 12 månaderna (och ofta mer än en attack).[2] Och även om IBM uppskattar att kostnaden för ett enda dataintrång nu uppgår till 4,24 miljoner USD[3] kan den verkliga kostnaden för intrång vara mycket högre: i vissa fall har sjukhus i USA varit tvungna att omdirigera akutpatienter till andra sjukhus och avvisa ambulanser på grund av utpressningsvirusattacker.[4]

Attacker mot fast mjukvara kan vara ett särskilt skadligt hot för organisationer. Det beror på att en attack mot fast mjukvara kan implantera skadliga program innan operativsystemet (OS) – och därmed den mjukvarubaserade säkerhet som körs – ens har startat. Ändå har mindre än hälften av organisationerna vidtagit åtgärder för att skydda sina system mot attacker på fast mjukvara, trots att sådana attacker har blivit fem gånger vanligare under de senaste fem åren.[5] När allt kommer omkring är arbetsbelastningar bara så säkra som alla stackar som de körs på.

För att kunna möta denna exponentiella tillväxt till frekvensen och variationen och kostnaden av hot från skadliga program måste modern säkerhet ha fler lager. Det beror på att skadliga program kan kompromettera system på hårdvaru- och fast mjukvarunivå, eller under start, alla områden där enbart mjukvarudefinierad säkerhet är kraftlös. För att motverka denna sårbarhet är modern serversäkerhet inte en entydig strategi. Den måste byggas in i hela infrastrukturstacken. Kombinationen av nästa generations Dell EMC™ PowerEdge™-servrar och Windows Server 2022 förenklar administratörens viktiga uppgift att anpassa hårdvara, fast mjukvara och operativsystem för att skydda affärskritiska arbetsbelastningar på ett adekvat sätt.

De kombinerade fördelarna med Windows Server 2022 Secured-core-server och nästa generations PowerEdge-servrar

Secured-core-server är en ny funktion i Windows Server 2022 som använder hårdvara, fast mjukvara och OS-funktioner för att skydda mot nuvarande och framtida hot. Kombinationen av mjukvara i Windows Server 2022 Secured-core-server som körs på nästa generations PowerEdge-serverhårdvara ger tre betydande fördelar för organisationer som din:

- Avancerat skydd
- Förebyggande försvar
- Förenklad säkerhet

Avancerat skydd

Baserat på Microsofts hotinformationsdata ger Secured-core-datorer mer än dubbelt skydd mot infektioner jämfört med vanliga datorer. Microsoft tar nu med samma teknik till servrar med Windows Server 2022 Secured-core-servrar.[5] Skydd som aktiveras av en Secured-core-server inriktade på att skapa en säker plattform för kritiska arbetsbelastningar och data på den servern. Mer specifikt använder Secured-core-servrar processorstöd för DRTM-teknik (Dynamic Root of Trust for Measurement) för att placera fast mjukvara i en hårdvarubaserad sandbox. Med isoleringen begränsas effekten av sårbarheter i miljontals rader med mycket privilegierad fast mjukvara.

Som ett komplement till isoleringen av fast mjukvara i Windows Server 2022 isolerar virtualiseringsbaserad säkerhet (VBS) kritiska delar av operativsystemet, till exempel kärnan, från resten av systemet. Detta hjälper till att säkerställa att servrarna förblir dedikerade att köra kritiska arbetsbelastningar, och det skyddar relaterade program och data från attacker och exfiltration.

För att göra den fasta mjukvaran i PowerEdge-servrar ännu mer motståndskraftig mot angrepp skyddar Dell Technologies leverantörskedjan för PowerEdge-servrar för att säkerställa att ingen har manipulerat servern under transporten från fabriken till kundplatsen (förklaras mer detaljerat i Ytterligare säkerhet genom integritet i leverantörskedjan från Dell Technologies nedan).

Förebyggande försvar

Funktionen Secured-core hjälper till att proaktivt försvara sig mot och störa många av de vägar som angripare kan använda för att utnyttja dina system. Hypervisor-skyddad kodintegritet (HVCI) i VBS isolerar beslutsfunktionen för kodintegritet (CI) från resten av Windows OS, vilket säkerställer att det enda sättet som kernelminnet kan bli körbart är genom en CI-verifiering. VBS möjliggör också användning av Windows Defender Credential Guard, där användarautentiseringsuppgifter och hemligheter lagras i en virtuell behållare som operativsystemet inte kan komma åt direkt.

Trusted Platform Module 2.0 (TPM 2.0) levereras som standard med Secured-core-servrar och tillhandahåller en skyddad lagring av känsliga nycklar och data, t.ex. mätningar av de komponenter som läses in under start. Att kunna verifiera att fast mjukvara som körs under start är giltigt signerad av den förväntade författaren och inte har manipulerats bidrar till att förbättra säkerheten. Denna hårdvarubaserade Root of Trust höjer även skyddet som tillhandahålls av funktioner som BitLocker-diskkryptering, som använder TPM 2.0 och underlättar skapandet av attesteringsbaserade arbetsflöden som kan införlivas i säkerhetsstrategier med nollförtroende. Sammantaget ger de här försvaren era IT- och SecOps-team möjlighet att fördela tiden på de olika säkerhetsområdena på ett bättre sätt.

Nästa generations PowerEdge-servrar har stöd för UEFI Secure Boot (Unified Extensible Firmware Interface) som är branschstandard. UEFI Secure Boot kontrollerar de kryptografiska signaturerna för UEFI-drivrutiner och annan kod som läses in innan operativsystemet körs för att säkerställa att skadliga program inte har manipulerat den fasta mjukvaran. Dessutom har PowerEdge-servrar stöd för TPM 2.0 för att öka säkerheten för den fasta mjukvaran och operativsystemet.

Förenklad säkerhet

När du skaffar en PowerEdge-server med Secured-core kan du vara säker på att Dell Technologies har tillhandahållit hårdvara, fast mjukvara och drivrutiner som uppfyller Secured-core-löftet. Microsoft har ett nära samarbete med Dell Technologies för att förenkla säkerhetsaktiveringen på PowerEdge-servrar.

Nya funktioner i Windows Admin Center gör det enkelt för administratörer att konfigurera OS-säkerhetsfunktionerna i Windows Server 2022 Secured-core-servrar. Med den nya säkerhetsfunktionen i Windows Admin Center kan administratörer aktivera avancerad säkerhet genom att klicka på en knapp. Windows Admin Center visar status för alla nödvändiga säkerhetsfunktioner för Windows Server 2022 Secured-core-servrar och gör det möjligt för administratörer att aktivera funktioner efter behov från en enda plats.

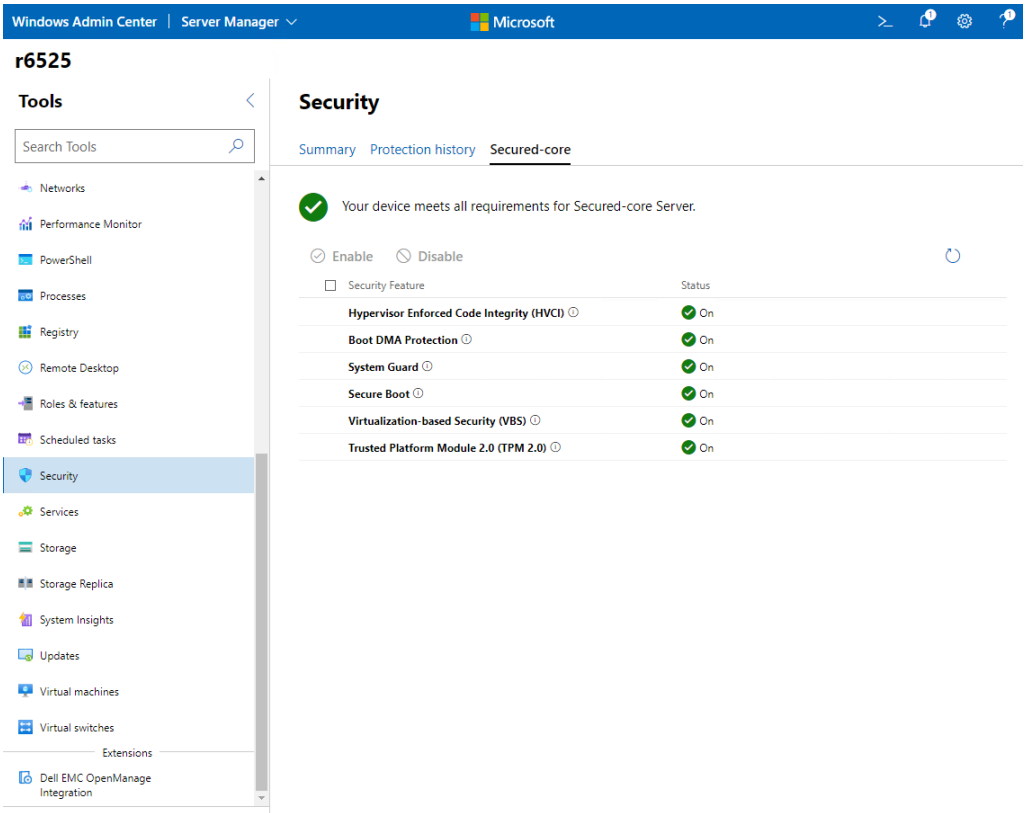


Bild 1 Bekräftelseskärm med Secured-core i Windows Admin Center

Dell EMC™ OpenManage™ Integration med Windows Admin Center är ett tillägg till Windows Admin Center som förenklar hanteringen av Secured-core-servrar ytterligare. Det här Windows Admin Center-tillägget förenklar (bland annat) IT-administratörernas säkerhetsuppgifter genom att fjärrhantera PowerEdge-servrar. Inom ramen för Windows Server 2022 Secure-core-servrar kan du använda tillägget OpenManage Integration med Windows Admin Center för att visa dina PowerEdge-servrar inifrån Windows Admin Center. Det ger en enhetlig vy över PowerEdge-serverkomponenternas hälsotillstånd samt information om hårdvara och fast mjukvara.

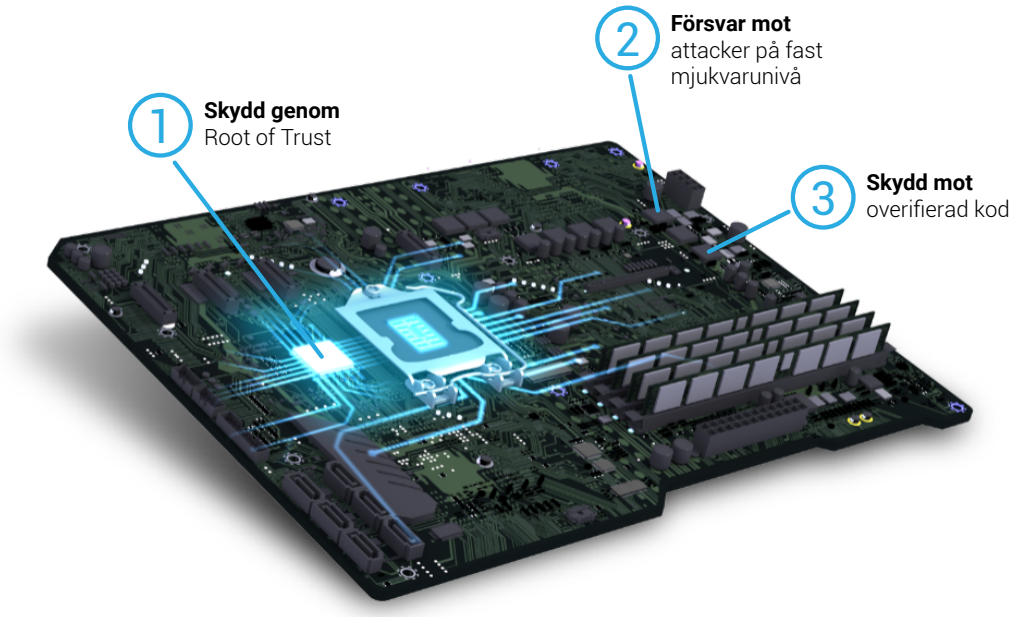
Stöd för PowerEdge-servrar för Secure-core-servrar i Windows Server 2022

Eftersom försvaret i Secured-core-servern består av flera lager är det viktigt med stöd från din hårdvaru-OEM. PowerEdge-servrar testas och certifieras av Dell Technologies för att säkerställa att hårdvara och fast mjukvara uppfyller kraven på säkerhetsfunktioner i Windows Server 2022. Dessutom är hårdvara och fast mjukvara i PowerEdge-servrar konfigurerade för Secure-core-servern i Windows Server 2022. I Tabell 1 beskrivs hur hårdvaran i PowerEdge-servrar förstärker funktionerna i Windows Server 2022.

Tabell 1 Mappning av säkerhetsfunktioner i Windows Server 2022 och viktiga stödfunktioner i nästa generations Dell EMC™ PowerEdge™-servrar

	Windows Server 2022	Nästa generations Dell™ PowerEdge™-servrar
Avancerat skydd	Secured-core-system placerar den fasta mjukvaran i en hårdvarubaserad sandbox, vilket begränsar effekten av sårbarheter baserade på fast mjukvara. VBS isolerar kritiska delar av operativsystemet från avancerade skadliga program.	Dell Technologies bidrar till att säkra leverantörskedjan för PowerEdge-servrar för att säkerställa att ingen har manipulerat servern eller komprometterat den fasta mjukvaran under transporten från fabriken till kundplatsen.
Förebyggande försvar	VBS-funktioner som HVCI och Windows Defender Credential Guard förhindrar hela klasser av sårbarheter och skyddar bättre känsliga tillgångar som inloggningsuppgifter. TPM 2.0 tillhandahåller hårdvarubaserad Root of Trust som används som en säker grund.	PowerEdge-servrar stöder UEFI Secure Boot av branschstandard för att kontrollera kryptografiska signaturer för UEFI-drivrutiner och annan kod som läses in innan operativsystemet körs. PowerEdge-servrar har stöd för TPM 2.0.
Förenklad säkerhet	Windows Admin Center ger enkel åtkomst till att konfigurera Secured-core-servrar.	Microsoft samarbetar med Dell Technologies för att förenkla säkerhetsaktiveringen på PowerEdge-servrar. Integreringen av Windows Admin Center med Dell EMC™ OpenManage™ förenklar hanteringen av Secured-core-servrar ytterligare.

Uppbyggnaden av avancerad säkerhet i flera lager



1 Skydd genom Root of Trust

Secured-core-servrarna samarbetar med ledande OEM-tillverkare som Dell Technologies och kiselleverantörer som Intel och AMD och använder en Root of Trust av branschstandard för hårdvara tillsammans med säkerhetsfunktioner som är inbyggda i dagens moderna processorer.

Secured-core-servrarna använder TPM 2.0 och en modern processor med DRTM för att starta servrar på ett säkrare sätt och minimera sårbarheter i den fasta mjukvaran.

2 Försvar mot attacker på fast mjukvarunivå

Secured-core-servrar använder hårdvarubaserad säkerhet i den moderna processorn för att starta systemet i ett betrott tillstånd, vilket förhindrar att avancerade skadliga program manipulerar systemet och attackerar på fast mjukvarunivå.

System Guard Secure Launch använder processorn för att validera enheten så att den startar säkrare, vilket förhindrar avancerade attacker på fast mjukvara.

3 Skydd mot overifierad kod

Kod som körs i den betrodda beräkningsbasen körs med integritet och är inte föremål för kryphål eller attacker.

Secured-core-servern med HVCI startar endast körbara filer som signerats av kända och godkända utfärdare. Hypervisor ställer in och tillämpar behörigheter för att förhindra att skadliga program försöker ändra minnet och göra det körbart.

Stöd för nästa generations PowerEdge-server för säker anslutning i Windows Server 2022

Nästa generations PowerEdge-servrar har stöd för SMB:s (Server Message Block) AES-256-kryptering för säkerhetsmedvetna arbetsbelastningar. Det här stödet innebär att PowerEdge-servrar som kör Windows Server 2022 kan tillhandahålla heltäckande kryptering för arbetsbelastningsdata för extra säkerhet. Den 256-bitars AES-kryptering som används för SMB i Windows Server 2022 är också tillräckligt robust för att vara motståndskraftig även mot brute force-attacker från kvantdatorer om tillräckligt starka lösenord används.

PowerEdge-servrar och Windows Server 2022 utökar den heltäckande SMB-krypteringen från enskilda servrar till den interna kommunikationen i kluster med AES-256-kryptering för öst-västlig SMB-datatrafik. Dessa ytterligare SMB-krypteringskontroller härdar arbetsbelastningar ännu mer och stänger angreppsvägar.

Slutligen använder Windows Server 2022 Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) som ingår i 3:e generationens skalbara Intel® Xeon®-processorer och vektoriserad AES-kryptering för 256-bitars (vAES256) som ingår i AMD EPYC™ Zen 3-processorer. De här avancerade processorernas instruktionsuppsättningar ökar prestandan för AES-256-kryptering i PowerEdge-servrar. Genom att använda dessa avancerade säkerhetstekniker gör Dell Technologies och Microsoft att du inte behöver välja mellan robust säkerhet och svarstider för affärskritiska arbetsbelastningar.

Ytterligare säkerhet genom integritet i leverantörskedjan från Dell Technologies

Dell Technologies integritet i leverantörskedjan skyddar hårdvara och komponenter i fast mjukvara från att äventyras under tillverkning och frakt. När det gäller hårdvaruintegritet arbetar Dell Technologies för att säkerställa att inga produkter manipuleras eller att förfalskade komponenter sätts i innan produkter levereras till kunder. De kontroller som Dell Technologies har omfattar val av leverantör, inköp, produktionsprocesser och styrning genom granskning och testning. Materialinspektioner i produktionen kan identifiera komponenter som är felmärkta, avviker från normala prestandaparametrar eller innehåller en felaktig elektronisk identifierare.

För mjukvaruintegritetens skull strävar Dell Technologies efter att se till att inga skadliga program förs in i den fasta mjukvaran eller enhetsdrivrutinerna innan en produkt levereras till kund, samt att förhindra eventuella sårbarheter i kodningen. Dell Technologies är ISO 9001-certifierat för alla globala tillverkningsanläggningar. Att strikt följa dessa processer och kontroller bidrar till att minimera risken för att förfalskade komponenter bäddas in i Dell Technologies™-produkterna och att skadliga program förs in i fast mjukvara eller enhetsdrivrutiner. Dessutom implementerar Dell Technologies dessa åtgärder som en del av SDLC-processen (Software Development Lifecycle).

Dell Technologies arbetar även för att garantera den fysiska säkerheten vid tillverkningsanläggningar och transportkedjor. Dell Technologies kräver att vissa fabriker där Dell Technologies-produkter byggs uppfyller specificerade säkerhetskrav från Transportasset Protection Association (TAPA), inklusive användning av övervakade övervakningskameror i viktiga områden, åtkomstkontroller och kontinuerligt bevakade in- och utgångar. Som en del av ett branschledande logistikprogram har Dell Technologies även infört skyddsåtgärder för att skydda produkter mot stöld och manipulering under transport. Genom Dell Technologies verifiering för komponentsäkerhet (SCV) för PowerEdge-servrar kan Dell Technologies-kunder verifiera att en PowerEdge-server som tas emot av kund överensstämmer med den som tillverkades i fabriken.

Skydda dina viktiga arbetsbelastningar med en bättre säkerhetsgrund från Windows Server 2022 och nästa generations Dell EMC PowerEdge-servrar

Arbetsbelastningar är bara så säkra som grunden de körs på. Hotet från skadliga program och dataintrång kommer bara att fortsätta att växa i framtiden, särskilt när skadliga aktörer som vill orsaka skada fortsätter att utforska angreppsvägar som är immuna mot traditionell, mjukvarubaserad säkerhet. Attacker mot fast mjukvara riktar sig specifikt mot servrar under startprocessen, innan mjukvarubaserad säkerhet ens har börjat skydda systemen. Modernt serverskydd kräver mångsidig säkerhet som omfattar hårdvara, fast mjukvara och operativsystem.

Det har aldrig varit så här logiskt att uppgradera till Windows Server 2022. Med funktionen Secured-Core-server i Windows Server 2022 kan organisationer motverka hot mot både fast mjukvara och operativsystemet. När de kombineras med Dell Technologies integritetsskydd för hårdvara och mjukvara kan nästa generations Dell EMC PowerEdge-servrar som kör Windows Server 2022 tillhandahålla modern säkerhet för hårdvara, fast mjukvara och operativsystem. Och de säkra anslutningsfunktionerna i Windows Server 2022 som stöds i nästa generations PowerEdge-servrar utökar detta skydd från enskilda servrar till hela kluster i ditt datacenter. Dessutom upphör supporten för Windows Server 2012 i oktober 2023, vilket innebär att det är dags att börja göra uppgraderingsplaner.[6]

Mer information om hur Windows Server 2022 och nästa generations Dell EMC PowerEdge-servrar kan skydda dina kritiska arbetsbelastningar och data finns på www.delltechnologies.com/en-us/solutions/microsoft-oem/.

[1] Cybersecurity Ventures. ”Kostnaden för cyberbrott uppgår till 10,5 biljoner dollar per år för hela världen fram till 2025” (på engelska). november 2020. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.
[2] IDC. ”IDC:s undersökning visar att mer än en tredjedel av alla organisationer världen över har drabbats av en attack eller ett intrång av utpressningsvirus” (på engelska). Augusti 2021.
[3] IBM. ”Hur mycket kan en dataläcka kosta?” (på engelska). 2021. www.ibm.com/security/data-breach.
[4] Dan Goodin. ”Sjukhus som är lamslagna av utpressningsvirus avvisar patienter” (på engelska). *Ars Technica*. Augusti 2021. https://arstechnica.com/gadgets/2021/08/hospitals-hamstrung-by-ransomware-are-turning-away-patients/.
[5] Microsoft. ”En ny studie av säkerhetssignaler visar att attacker på fast mjukvara ökar. Så här arbetar Microsoft för att eliminera hela den här hotklassen” (på engelska). Mars 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] När artikeln skrevs. Den senaste informationen om att supporten för Windows Server 2012 upphör finns på livscykelsidan för Windows Server 2012: https://docs.microsoft.com/en-us/lifecycle/products/windows-server-2012.

DELL Technologies

Microsoft

Modernisera din utrustning med Windows Server 2022.
Det molnförberedda operativsystemet effektiviserar investeringar på plats med hybridfunktionalitet.