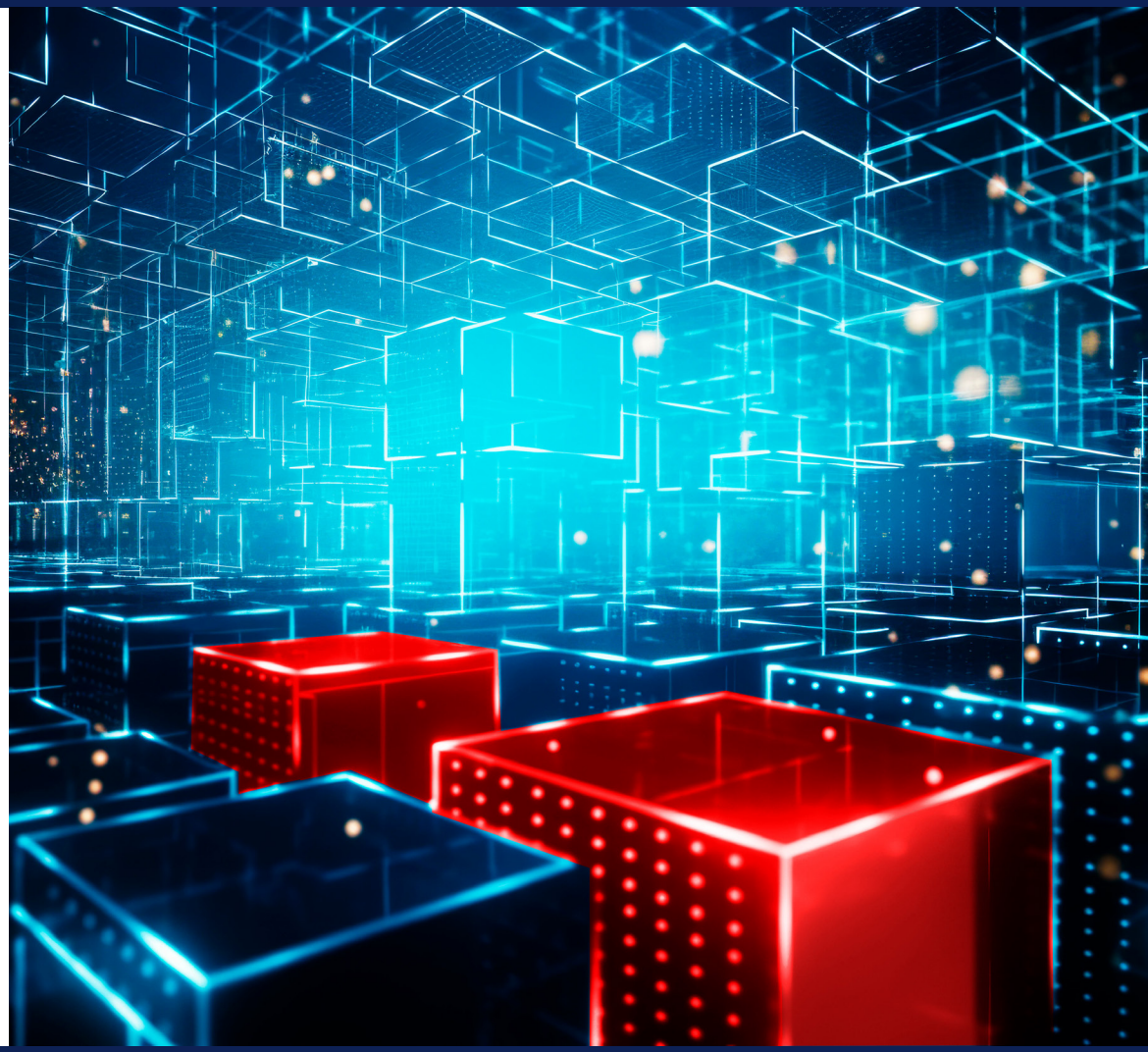
Så här säkrar du användningen av AI vid slutpunkten

Skydda AI-arbetsbelastningar på enheten med säkra och moderna enheter som baseras på angriparens utgångspunkt.



Sammanfattning

AI på enheten har stora fördelar, men det medför även cyberrisker. I den här e-boken går vi igenom hur du ger ditt företag möjlighet att på ett säkert sätt utnyttja AI-innovation vid slutpunkten.

Innehållsförteckning

Angreppsytan för AI på enheten

Vad kan attackeras?

All ny teknik medför cybersäkerhetsrisker av en anledning: det är ett nytt område. Du måste hantera något du inte känner till. Vi har sett detta med molnanvändning, blockkedjor och många andra tekniker. Samma sak gäller för AI på enheten. Därför behöver du lära dig mer om det här för att minska risken.

Innan vi går in på vilken säkerhet som behövs för att minimera attackytan vill vi berätta vad vi säkrar och varför. Tänk dig att det här är ett rörsystem i en kommersiell byggnad som rymmer flera företag. I de här rören flyter vatten, gas och liknande till hela byggnaden för en mängd olika typer av användning. Om innehållet som strömmar genom rören är kontaminerat eller om det stoppas upp kan det inte göra sitt jobb. Om rören som transporterar innehållet är skadade eller korrupta kan de inte utföra sin uppgift. Både rören och innehållet måste vara i bra skick för att uppfylla behoven i respektive användningsfall.►

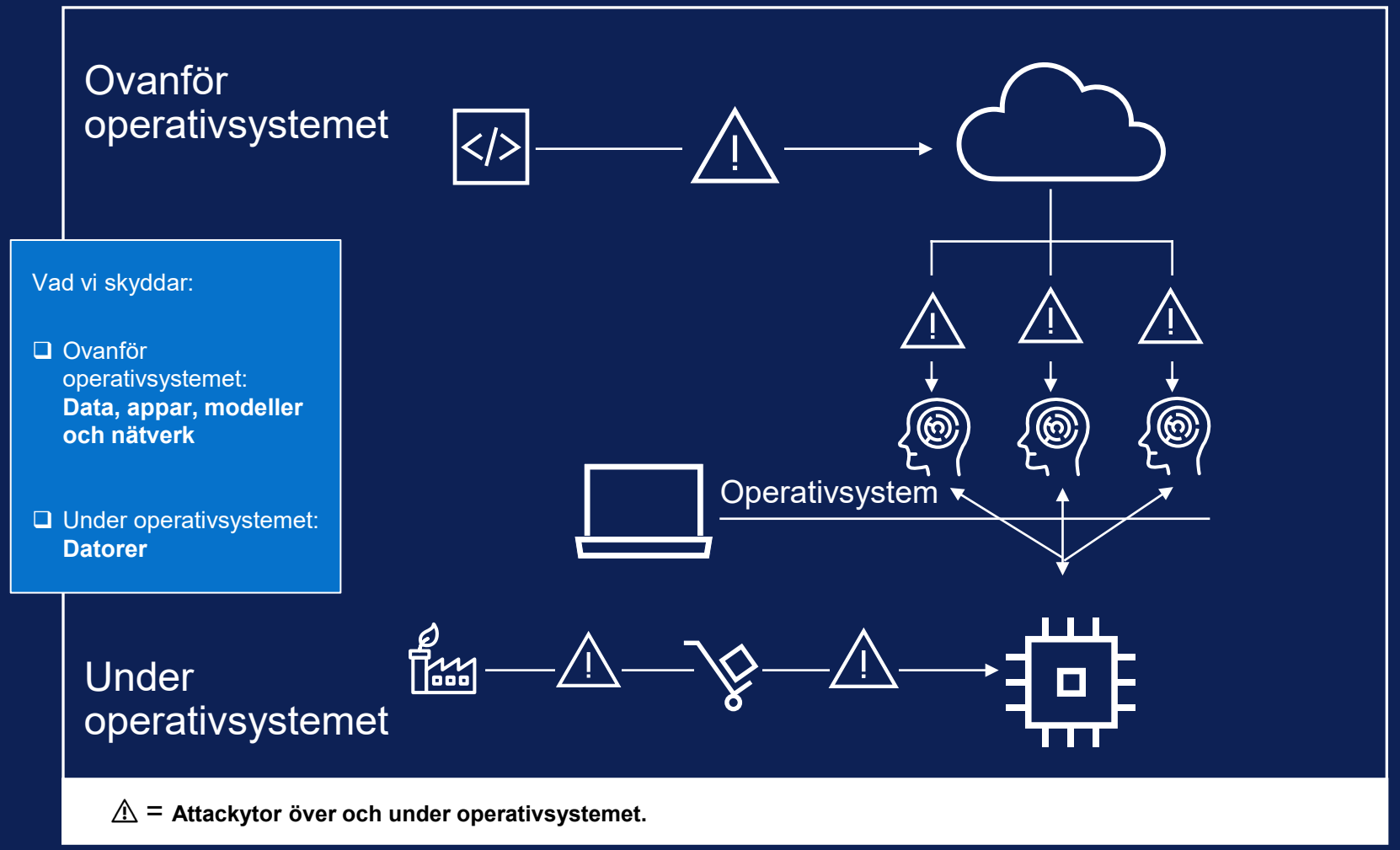
Angreppsytan för AI på enheten, forts.

Vad kan attackeras? forts.

AI vid slutpunkten:

- Rören är din infrastruktur – dina datorer och dina företagsnätverk. Alltså hur och var du arbetar.
- Innehållet som flödar genom rören är data, appar och modeller som driver olika AI-användningsfall. De tillgångar och resurser du behöver för att göra ditt arbete.

Och du gissade helt rätt. Cybermotståndare riktar in sig på båda. De kan stjäla IP för att hålla den som gisslan, förgifta data eller modeller för att påverka verksamheten. Oavsett vilket så kan konsekvenserna bli allvarliga, leda till ekonomiska skador och skador på företagets anseende och/eller utlösa regelgranskningar.►



Säkerhetsrisker vid slutpunkten

Taktiker som angripare använder för att komma in

Nu ska vi prata om metoder som angripare kan använda för att komma åt båda målen.

Kompromitterade enheter. Som vi ser i Endpoint Security Market Insights, Forrester Research, Inc., mars 2025, är datorer bland de ledande målen för moderna cyberhot. Den här typen av attack kan inträffa långt innan AI-arbetet på enheten börjar, alltså en **attack i leverantörskedjan för hårdvara eller mjukvara**. Det finns dussintals, om inte hundratals, punkter i leverantörskedjan där en illvillig part kan manipulera komponenter som kretsar och fast mjukvara – och plantera sårbarheter som kan utnyttjas senare. Föreställ dig katastrofen som väntar om ett värdepappersföretag väntar på en helt ny leverans av datorer, men den innehåller förfalskade komponenter.

Kompromettera identiteter. Intrång som involverar stulna eller komprometterade inloggningsuppgifter är en av de snabbast växande attackvektorerna. Och det är inte så konstigt. Angripare som använder giltiga inloggningsuppgifter kan logga in på en dator, röra sig fritt inom företagsnätverket och förbli oupptäckta under långa perioder. Enligt IBM:s senaste rapport Cost of a Data Breach tog dessa dataintrå`ng i genomsnitt 292 dagar att identifiera och begränsa – den längsta av alla angreppsvektorer som studerades. Åtkomstnivån är alltför värdefull för att hotaktörer ska ignorera det här. Forskning från Zscaler visar faktiskt att skadliga aktörer använder artificiell intelligens för att förbättra och skala upp nätfiskeattacker genom att stjäla inloggningsuppgifter. Denna obehöriga åtkomst som tillämpas på känsliga tränings- eller inferensdata eller direkt på modeller kategoriseras som en **attack mot modelleverantörskedjan**.

Insiderhot. Den senaste forskningen visar att **skadliga insiderattacker** resulterade i de högsta kostnaderna, i genomsnitt 4,99 miljoner USD, jämfört med andra attackvektorer. Tänk på att insiderattacker kan inträffa i hela leverantörskedjan för hårdvara, mjukvara och modelleverantörer.►

Genomsnittstid för en slutanvändare att falla för ett **nätfiskemejl**: <60 sekunder*

I genomsnitt tar det 292 dagar för att upptäcka och hantera **intrång i inloggningsuppgifter** **

Skadliga insiderattacker kostar i genomsnitt 4,99 miljoner USD**

*Källa: Verizon DBIR, 2024
** Källa: IBM Cost of a Data Breach, 2024

Plan för motåtgärder

Det här minskar riskerna

Inget av dessa attackmål är egentligen nya. Det är inte heller attackernas slutmål. Som alltid vill vi fokusera på att hålla din datorflotta säker och tålig. **Att lägga till motåtgärder** kan bidra till att minska angreppsytan och göra det möjligt att omedelbart upptäcka misstänkt beteende.

Nollförtroende minskar riskerna i hela din datorflotta. Genom att använda principerna ”lita aldrig på något, verifiera alltid och övervaka kontinuerligt” kan du ligga steget före angripare. Det är omöjligt att blockera 100 procent av attackerna. Vill du ha en stark säkerhetsställning behöver du **synlighet och kontroll** i hela IT-ekosystemet.

Med det ramverket i åtanke bör du ompröva din infrastruktur – särskilt system och processer som interagerar med AI. Vilka motåtgärder minimerar risken för att enheter äventyras, att du drabbas av identitetsintrång och insiderhot?►

Nollförtroendeprinciper hjälper till att skydda mot risker och minska den snabba spridningen av cyberaktiviteter

Plan för motåtgärder, forts.

Det här minskar riskerna, forts.

Det finns två övergripande motåtgärdskategorier.

Säkerhet ”under operativsystemet” skyddar de AI-enheter du arbetar på. Vi kan dela upp detta i två delar:

- Försvara din datorflotta med enheter som är **byggda på ett säkert sätt**. Det innebär att använda AI-datorer som är säkra till sin utformning – att de har utvecklats med principer för säker design och i en säker leverantörskedja.
- Skydda din datorflotta med enheter som har **inbyggd säkerhet**. Säkra AI-datorer innehåller lager av inbyggt skydd som ger insyn ner till BIOS- och kisellagren – och fungerar direkt från leverans.

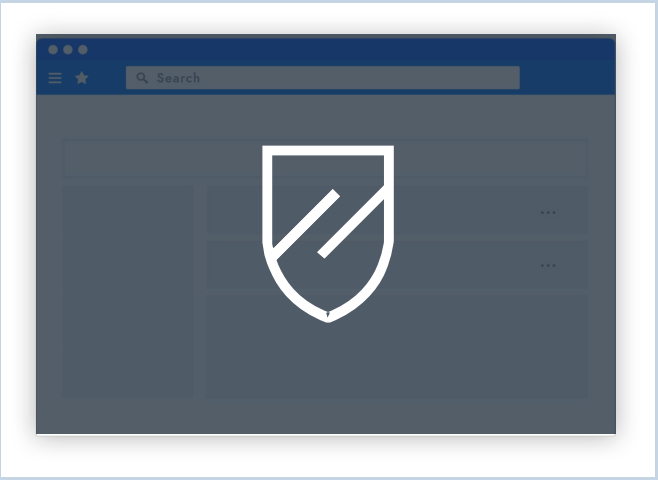
Säkerhet ”ovanför operativsystemet” skyddar åtkomsten till AI-modeller. Skydda de data och modeller som du arbetar *med* och företagsnätverk du arbetar *i* med **mjukvarusäkerhet**. Det är viktigt att skydda säkerhetsåtgärder för maskininlärning och övervaka nätverkstrafiken för distribuerade AI-arbetsbelastningar.►

Säkerhet under operativsystemet

Säkra AI-datorer

Säkerhet i hårdvara och fast mjukvara, säkerhet i leverantörskedjan, kärnsilikon

Säkerhet ovanför operativsystemet



Mjukvarusäkerhet

Ytterligare säkerhetslager för slutpunkter, nätverk och molnmiljöer

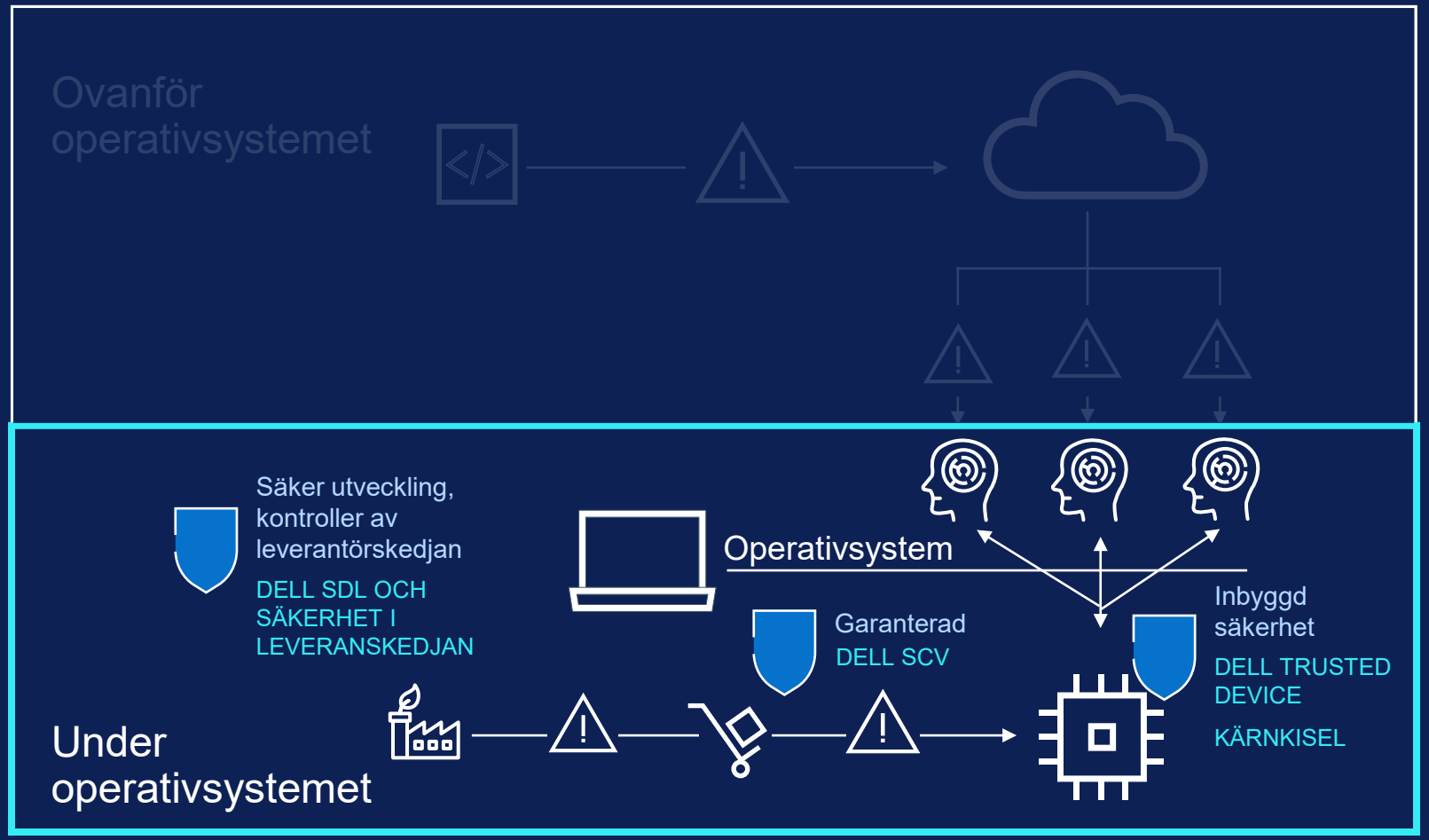
Säkerhetstjänster och expertis finns tillgängliga för att knyta ihop allt.

Tillämpa bästa praxis för din datorflotta

Så ger Dells AI-datorer grundläggande säkerhet till din datorflotta

Det är här Dell Trusted Workspace kan hjälpa dig. Våra tekniker utformar och konstruerar säkerheten för våra kommersiella AI-datorer med en djup förståelse för angriparnas tillvägagångssätt.

Under operativsystemet, säker utformning, robusta kontroller i leverantörskedjan och säkerhet i leverantörskedjan som tillval ser till att datorerna är säkra från första start. Inbyggd säkerhet för hårdvara och fast mjukvara skyddar datorn när den används, exempelvis Dells unika* manipuleringsdetektering på BIOS-nivå (Dell SafeBIOS) och lösenordsfri säkerhet för inloggningsuppgifter (Dell SafeID) för att skydda mot obehörig åtkomst. Intel® har kiselteknik som dessutom bidrar till att ge en grund för att skydda olika aspekter av AI när den används av AI PC-klienter. Intel hjälper till exempel till att skydda AI-data som finns på klienten med acceleration för modellkryptering på disk.►

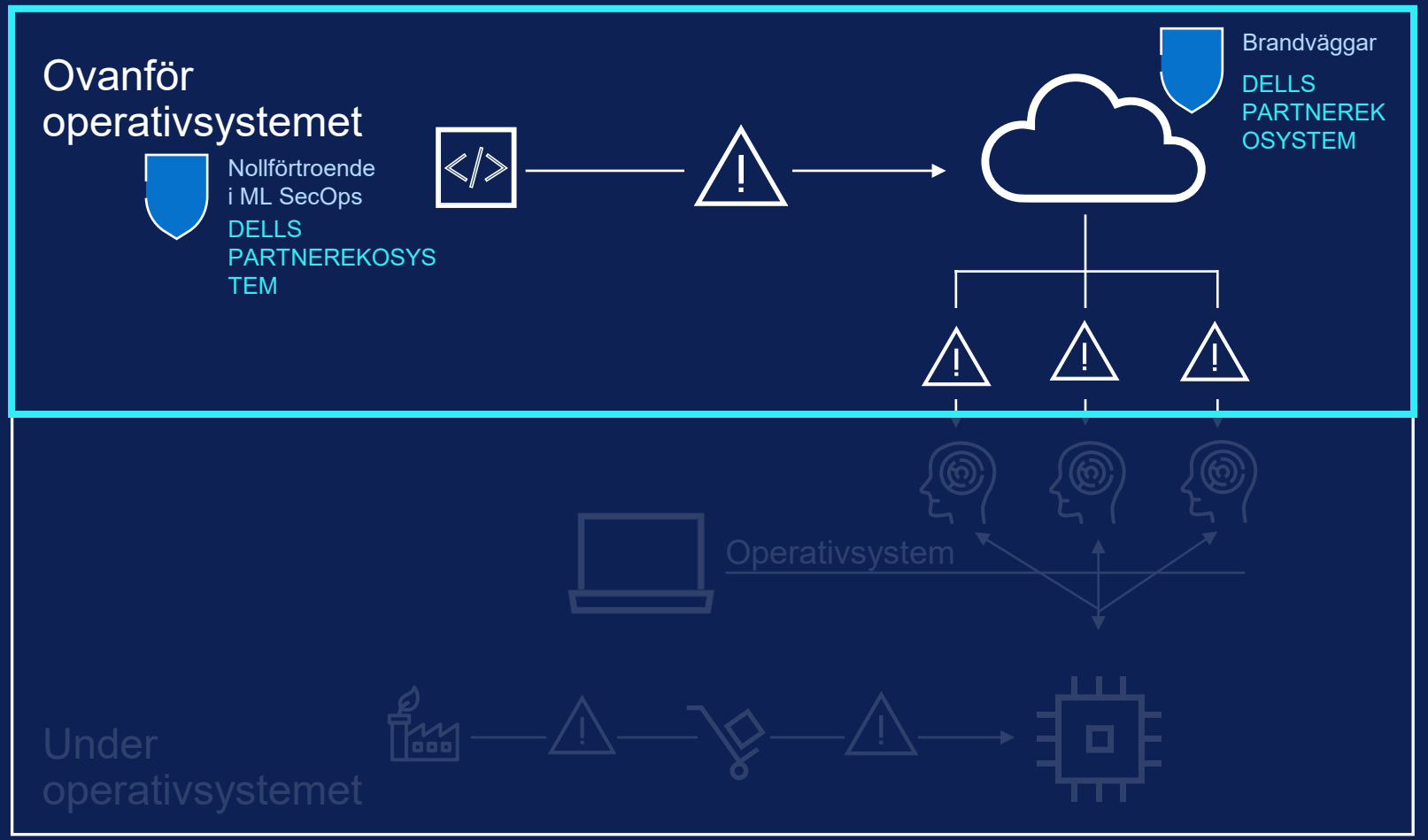


Tillämpa bästa praxis för din datorflotta, forts.

Så ger Dells AI-datorer grundläggande säkerhet till din datorflotta, forts.

Det går att komplettera säkerheten ”under operativsystemet” med hjälp av teknik från vår partner Absolutes Persistence som bäddas in redan på fabriken för ännu större synlighet och kontroll över datorns livscykel. Det möjliggör bland annat geolokalisering för enheter på väg och självläkning av kritiska appar i värsta tänkbara scenario.

Dell har sammanställt ett ekosystem av mjukvarupartnerlösningar som CrowdStrike Falcon XDR och Absolute Secure Access. De aktiverar nollförtroendeprinciper för att skydda leverantörskedjan från obehörig åtkomst **ovanför operativsystemet**. Med dessa lösningar kan du skapa och upprätthålla policyer med detaljerade åtkomstkontroller (exempelvis rollbaserad åtkomstkontroll eller RBAC) för att minska risken för att skadliga insiders kommer åt eller manipulerar dina AI-modeller.►



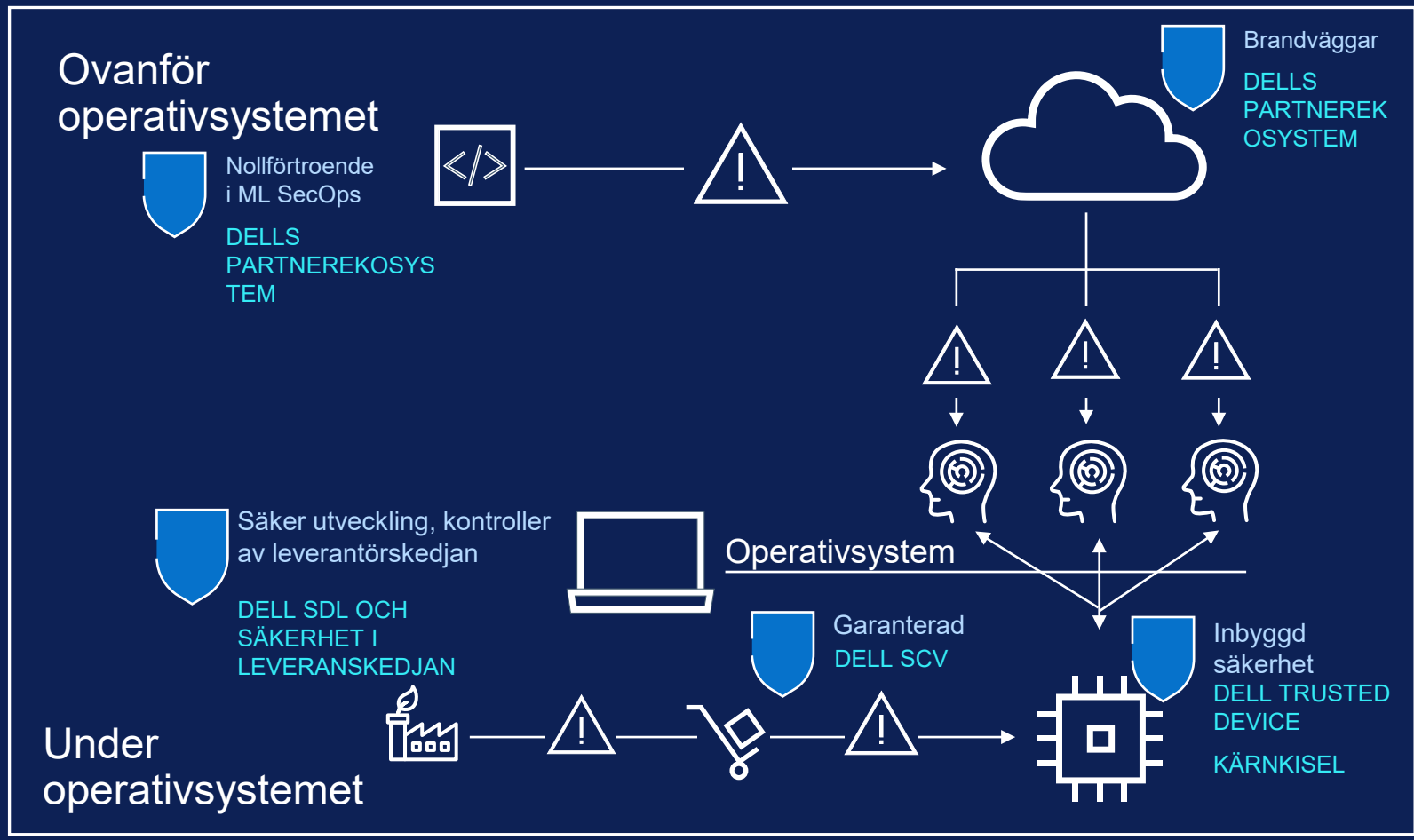
Tillämpa bästa praxis för din datorflotta, forts.

Så ger Dells AI-datorer grundläggande säkerhet till din datorflotta, forts.

Allt det här kombinerat är ***säkerhet för AI.*** Dessa funktioner skyddar AI-arbetsbelastningar på enheten från cyberattacker, så att du kan fokusera på innovation och stärka ditt företag.►

Förhindra avancerade slutpunktsattacker med koordinerat hårdvaru- och mjukvaruförs

Dell samarbetar med Intel och CrowdStrike för att integrera lagren under och ovanför operativsystemet med hårdvaruassisterad säkerhet.
Mer information >



Viktiga lärdomar och nästa steg

Säkra AI i slutpunkten med Dell

Företag ökar glatt användningen av AI men säkerhetsberedskapen släpar efter enligt en nyligen genomförd undersökning av CISOs utförd av Absolute. En analys av miljontals enheter visade att många datorer inte kunde absorbera nya AI-funktioner på ett bra sätt. **Dell kan hjälpa till att föra samman allt.**

Utveckla och driftsätt AI-modeller på en säker och modern grund. Support för Windows 10 upphör i oktober 2025. Datorer får inte längre några säkerhetsuppdateringar, inga funktionsuppdateringar och inget stöd för Windows 10. Äldre enheter kanske inte uppfyller kraven för Windows 11 och kan sakna de senaste inbyggda prestanda-, säkerhets- och AI-förbättringarna. Uppgradera till **Dell Pro** eller **Dell Pro Max baserat på Intel® Core™ Ultra processorer med Intel vPro®** för att frigöra säkerhetsfördelar och försvara AI-arbetsbelastningar med **världens säkraste kommersiella AI-datorer.*** ►

Support för Windows 10 upphör i oktober.

Uppgradera till Dells senaste AI-datorer på Intel för att få tillgång till säkerhetsfördelar och AI-förbättringar:

Köp Dell Pro ● Dell Pro Max.

*Världens säkraste kommersiella AI-datorer**

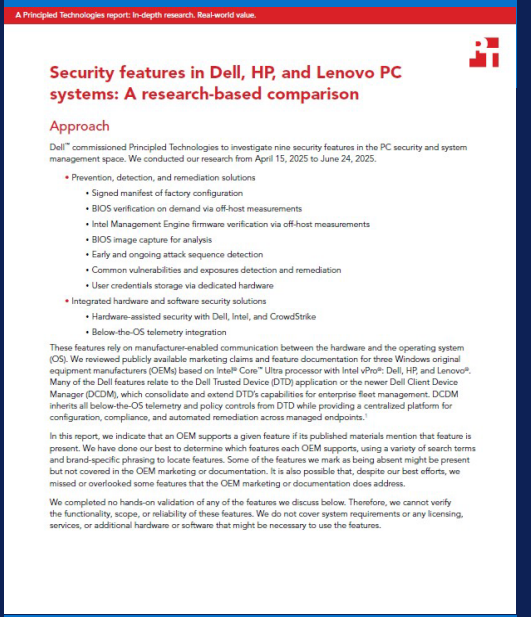
Utforska mervärdesprogram och tjänster för att förbättra din säkerhetsställning:

Mjukvara och integreringar

Tjänster

LEDANDE I BRANSCHEN

Principled Technologies visade att säkerhet på Dell och Intels kommersiella AI PC-säkerhet vinner jämfört med andra


A Principled Technologies report: In-depth research. Real-world value.

Security features in Dell, HP, and Lenovo PC systems: A research-based comparison

Approach

Dell™ commissioned Principled Technologies to investigate nine security features in the PC security and system management space. We conducted our research from April 15, 2025 to June 24, 2025.

- Prevention, detection, and remediation solutions
  - Signed manifest of factory configuration
  - BIOS verification on demand via off-host measurements
  - Intel Management Engine firmware verification via off-host measurements
  - BIOS image capture for analysis
  - Early and ongoing attack sequence detection
  - Common vulnerabilities and exposures detection and remediation
  - User credentials storage via dedicated hardware
- Integrated hardware and software security solutions
  - Hardware-assisted security with Dell, Intel, and CrowdStrike
  - Below-the-OS telemetry integration

These features rely on manufacturer-enabled communication between the hardware and the operating system (OS). We reviewed publicly available marketing claims and feature documentation for three Windows original equipment manufacturers (OEMs) based on Intel® Core™ Ultra processor with Intel vPro®: Dell, HP, and Lenovo®. Many of the Dell features relate to the Dell Trusted Device (DTD) application or the newer Dell Client Device Manager (DCDM), which consolidate and extend DTD's capabilities for enterprise fleet management. DCDM inherits all below-the-OS telemetry and policy controls from DTD while providing a centralized platform for configuration, compliance, and automated remediation across managed endpoints.[1]

In this report, we indicate that an OEM supports a given feature if its published materials mention that feature is present. We have done our best to determine which features each OEM supports, using a variety of search terms and brand-specific phrasing to locate features. Some of the features we mark as being absent might be present but not covered in the OEM marketing or documentation. It is also possible that, despite our best efforts, we missed or overlooked some features that the OEM marketing or documentation does address.

We completed no hands-on validation of any of the features we discuss below. Therefore, we cannot verify the functionality, scope, or reliability of these features. We do not cover system requirements or any licensing, services, or additional hardware or software that might be necessary to use the features.

Läs undersökningen

Friskrivningar

*Baserat på en tredjepartsanalys utförd av Principled Technologies vid en jämförelse av Dells kommersiella AI-datorer med Intel processorer jämfört med HP och Lenovo, juli 2025. Uppbackad av Dells interna analys av den globala datormarknaden, oktober 2024. Gäller datorer med Intel processorer. Alla funktioner är inte tillgängliga för alla datorer. För vissa funktioner krävs ytterligare köp.

För mer information:

Kontakta oss: Global.Security.Sales@Dell.com

Besök oss: Dell.com/Endpoint-Security

Följ oss: LinkedIn @DellTechnologies | X @DellTech

Om Dells slutpunktssäkerhet

Säkerhet är ett överväldigande ämne för organisationer av alla storlekar. **Samarbeta med en erfaren säkerhets- och teknikpartner för att modernisera slutpunktssäkerheten**.

Dell Trusted Workspace hjälper till med att säkra slutpunkter för en modern, nollförtroende-redo IT-miljö. Minska attackytan och förbättra cyberelasticiteten med en heltäckande portfölj av hård- och mjukvaruskydd – bara hos Dell. Vår mycket koordinerade och försvarsbaserade strategi avvärjer hot genom att kombinera inbyggda skydd med kontinuerlig vaksamhet. Slutanvändare håller produktiviteten uppe och IT-avdelningen känner sig trygg med säkerhetslösningar som är byggda för dagens molnbaserade värld.