DELL Technologies

Öka cybersäkerheten och stärk nollförtroendeprinciperna.

Täpp till resurs- och kunskapsluckor för att stärka försvaret mot cyberangrepp.

Dagens snabbt föränderliga hot, särskilt med tillkomsten av GenAI, skapar nya och oväntade utmaningar för även de mest erfarna specialisterna på cybersäkerhet. Läs mer om hur samarbete med erfarna säkerhetsspecialister kan hjälpa dig att undvika cyberangrepp och bibehålla robusta säkerhetsrutiner.

Cyberhot är som myror på en picknick

Du avvärjer ett hot. Då är nästa redan på väg.

I en allt mer sammankopplad värld där organisationer i hög grad förlitar sig på digital infrastruktur, och data har blivit en omfattande handelsvara, är det bäst att anta att en sofistikerad angripare redan har gjort intrång i din IT-miljö.

Den goda nyheten är att det finns erfarna partner som är specialiserade på gränslandet mellan teknik och cybersäkerhet.

Dell Technologies tillhandahåller innovativa lösningar och värdefull expertis som kanske inte finns inom företaget för att hjälpa dig navigera i det ständigt föränderliga hotlandskapet.

- Hård- och mjukvarusäkerhet
- Insikter i kommande risker
- Kunskap om avancerade angreppstekniker
- AIOps som kan möta snabbt föränderliga hot
- Nya säkerhetsstrategier och bästa praxis

Bygg upp försvarsskikt som kontinuerligt förbättrar säkerhetsrutinerna och tillämpar en nollförtroendemetod.

Dell Technologies är en cybersäkerhetspartner som erbjuder omfattande professionella tjänster, hård- och mjukvarulösningar och ett robust partnerekosystem som begränsar risken för angrepp, identifierar och minimerar sårbarheter och hjälper dig att snabbt återställa verksamheten.

Minimera angreppsytan →

Upptäck och åtgärda cyberhot →

Återställ snabbt efter angrepp →

Kant **Kärna** **Flermolnsmiljöer**

Professionella tjänster

Ekosystem med företags- och teknikpartner **Säker leverantörskedja**

DELL Technologies

Minska angreppsytan

Stärk försvaret och minska måltavlan genom att minska intrångsvägarna som cyberbrottslingar gillar att använda.

För att stärka säkerheten måste du identifiera och minimera sårbarheter och ingångspunkter som kan äventyra program, system eller nätverk på olika domäner, inklusive kant, kärna och moln.

IDENTIFIERA sårbarhetspunkter

- Sårbarheter i mjukvara
- Felaktiga konfigurationer
- Svaga autentiseringsmekanismer
- System där nya korrigeringsfiler inte har installerats
- Onödigt stora användarbehörigheter
- Öppna nätverksportar
- Bristfällig fysisk säkerhet

IMPLEMENTERA förebyggande åtgärder

- Arbeta med säkra leverantörer
- Tillämpa omfattande nätverkssegmentering
- Isolera viktiga data
- Tillämpa strikta åtkomstkontroller
- Uppdatera och korrigera system och program
- Upptäck och åtgärda sårbarheter med hjälp av AI, regelbundna utvärderingar och tester

Tillämpa en nollförtroendemetod

En nollförtroendearkitektur innebär att organisationen inte automatiskt litar på något i eller utanför dess gränser. Istället verifieras allt som försöker ansluta till systemen innan åtkomst beviljas. Det är en modell som har upprättats och föreskrivs av USA:s försvarsdepartement. Den införlivar **7 sammankopplade delar** som systematiskt stärker säkerheten.

1. Användarförtroende
2. Enhetsförtroende
3. Dataförtroende
4. Program och arbetsbelastning
5. Nätverk och miljö
6. Synlighet och analys
7. Automatisering och orkestrering

DELL Technologies

Minska angreppsytan

Identifiera svaga punkter som underminerar systemen innan problemen uppstår.

Cybersäkerhet är inte en engångsuppgift, utan en kontinuerlig process. Regelbundna granskningar, penetrationstester och sårbarhetsbedömningar med hjälp från en erfaren partner inom säkerhetstjänster kan bidra till att identifiera och täppa till luckorna och minska risken.

Rutiner för säkra leverantörskedjor	Säkerheten börjar tidigare än du tror. Etablera en betrodd grund med enheter och infrastruktur som utformats, tillverkats och levererats genom en säker leverantörskedja, en säker utvecklingslivscykel och rigorös hotmodellering.
Inbyggd säkerhet	Arbeta med enheter och infrastrukturer med inbyggd hårdvarubaserad säkerhet som utformats för att fånga upp och avvärja angrepp innan de orsakar skada.
Regelbunden installation av korrigeringsfiler och uppdateringar	Åtgärda kända sårbarheter och minimera risken för att de ska utnyttjas genom att uppdatera program, fast mjukvara och operativsystem med de senaste säkerhetskorrigeringarna.
Minsta möjliga behörigheter	Begränsa användar- och systemkonton till minsta möjliga behörigheter som krävs för att utföra respektive uppgifter. Med denna metod begränsas de potentiella konsekvenserna av att en angripare får obehörig åtkomst.
Nätverks-segmentering	Isolera viktiga tillgångar för att begränsa nätverksåtkomsten genom modern nätverkssegmentering för kritiska data samt affärsgrupper och program. Detta begränsar angrepp genom att förhindra sidledes spridning.
Program-säkerhet	Implementera säkra kodningsrutiner, genomför regelbundna säkerhetstester och kodgranskningar, och använd brandväggar för webbprogram (WAF) för att skydda mot vanliga angrepp på programnivå och minska angreppsytan på webbprogram.
Professionella tjänster och samarbeten	Samarbeta med leverantörer av cybersäkerhetstjänster och skapa samarbeten med företags- och teknikpartner för att få expertis och lösningar som kanske inte är tillgängliga internt inom företaget.
Användarutbildning och information	Utbilda medarbetare och användare så att de kan känna igen och rapportera potentiella säkerhetshot, nätfiskeförsök och försök till social manipulering för att minimera de risker som utnyttjar mänskliga sårbarheter.

DELL Technologies

Upptäck och åtgärda cyberhot

Gamla säkerhetsmetoder är som en uppringd internetförbindelse – för långsamt och otillräckligt i dagens krävande miljö.

För att bemöta sofistikerade cyberhot behöver du ha bättre säkerhetsverktyg, till exempel inbyggda AI- och ML-program och metoder som identifierar och agerar utifrån känt och okänt.

Implementera kraftfulla system som detekterar och förebygger intrång

Utnyttja AI och ML för att upptäcka avvikelser

Övervaka nätverkstrafik och användarbeteende i realtid

Öka motståndskraften genom att samarbeta med erfarna professionella tjänster för tillgång till specialistkunskaper.

Som en erfaren teknikpartner kan Dell Technologies hjälpa dig att etablera proaktiva protokoll för åtgärder vid incidenter och återställning efter dem som beskriver roller och ansvarsområden samt säkerställer smidig kommunikation och samordning mellan olika parter.

Förbättra förmågan att proaktivt upptäcka och reagera på cyberhot genom avancerade metoder för:

- Hotinformation
- Åtgärder vid incidenter
- Säkerhetsinformation och händelsehantering
- Slutpunktsskydd
- Beteendeanalys

Förenkla en effektiv, snabb återställning och minimera dataförluster med:

- En väldefinierad åtgärdsplan för incidenter och samarbete
- Regelbundna säkerhetskopieringar av viktiga data och system
- Säkra lösningar för lagring på andra platser och datakryptering

DELL Technologies

Upptäck och åtgärda cyberhot

Var vaksam och agera snabbt.

För att upptäcka och hantera cyberhot behöver du vara alert och planera för det värsta som kan hända. Ta fram en åtgärds- och återställningsplan som kontinuerligt uppdateras och rutinmässigt tillämpas så att hela organisationen vet hur konsekvenserna av ett angrepp kan minskas. Det är en pågående och iterativ process som kräver en kombination av teknik, kunnig personal, väldefinierade processer och lagarbete.

Kontinuerlig övervakning	Med säkerhetsverktyg som intrångsdetekteringssystem (IDS), intrångsförebyggande system (IPS), logganalys och hotinformation kan du identifiera tecken på obehörig åtkomst, intrång, infektioner orsakade av skadliga program och dataintrång.
Hot-detektering	Dra nytta av AI och ML för att analysera data i syfte att identifiera mönster, avvikelser och angreppsindikatorer som kan tyda på hot. Det omfattar identifiering av kända angreppssignaturer och identifiering av avvikande beteende.
Varningar och aviseringar	Tillhandahåll tidiga varningar för snabba utredningar och svar. Synliggör varningar och aviseringar för snabba åtgärder med inbyggd säkerhet. Skicka telemetri på enhetsnivå uppströms från operativsystemet för att bidra till snabbare hotdetektering och sätt säkerhetspersonal eller ett säkerhetscenter (SOC) i arbete när potentiella hot eller incidenter upptäcks.
Åtgärder vid incidenter	Initiera en åtgärdsplan för att undersöka och minska bekräftade säkerhetsincidenter. Det omfattar att begränsa effekterna, identifiera grundorsaken och implementera nödvändiga åtgärder för att återställa system och förhindra ytterligare skador.
Teknisk analys	Utför detaljerade analyser av incidenter för att förstå angreppsmetoder, fastställa intrångets omfattning, identifiera berörda system eller data och samla in bevis för att hitta och åtgärda säkerhetsbrister.
Problemlösning och återställning	Agera för att åtgärda sårbarheter, korrigera system, ta bort skadliga program och implementera förbättrade säkerhetsåtgärder för att förhindra liknande incidenter. Återställ berörda system och data till deras normala tillstånd för att slutföra återställningsprocessen.

Återskapa från cyberangrepp

Kör hårt och se till att ditt företag kan fortsätta i snabbfilen.

Cyberelasticitet är nödvändigt i dagens datadrivna värld och förväntas av både kunder och partner. Flera skyddsskikt krävs för att säkerställa att viktiga data skyddas och isoleras på ett bra sätt så att de snabbt kan återställas tryggt efter ett angrepp.
Utvärdera din cyberelasticitet ›

- Agera för att minska skadan som orsakas av ett cyberangrepp
- Återskapa tjänster och enheter som äventyrats eller drabbats av störningar
- Analysera incidenten för att förhindra framtida angrepp
- Tillgodose företagets SLA och återställ driften till det normala

Skapa en heltäckande strategi för cybersäkerhet så att organisationen kan återställas effektivt.

IT-teamet, cybersäkerhetspersonalen, ledningen och ibland externa experter måste samarbeta kring återställningen efter ett cyberangrepp. Nyckeln till återställning är att snabbt få system och drift att fungera igen medan man lär sig av incidenten med målet att minska störningar och driftavbrott, återställa tjänster och dataintegritet, minimera ekonomiska och anseendemässiga konsekvenser och stärka cybersäkerheten för att förhindra liknande angrepp i framtiden.

- Utvärdera konsekvenserna av ett angrepp på affärsverksamheten
- Prioritera kritiska tjänster
- Driftsätt dataskyddssystem
- Kommunicera kring incidenter och framsteg i återställningen
- Ta fram en plan som verkställs noga för att säkerställa kontinuiteten

DELL Technologies

Återskapa från cyberangrepp

Ge dig tillbaka in i leken genom att granska system, nätverk och data efter en incident.

En strategi för cyberelasticitet införlivar människor, processer och teknik i ett helhetsramverk som skyddar hela organisationen.

Begränsa incidentens effekter

Det första steget är att isolera och begränsa cyberangreppets effekter. Det innebär att koppla bort angripna system från nätverket, inaktivera konton som har äventyrats och implementera åtgärder för att förhindra ytterligare spridning eller skador.

System- eller enhetsåterställning

När en incident är under kontroll återställs berörda system och nätverk till ett opåverkat och säkert tillstånd. Det kan handla om att återskapa komprometterade system, installera om mjukvara och tillämpa säkerhetskorrigeringar och uppdateringar. Automatisering och självåterställning kan vara viktiga komponenter för att återuppta driften.

Data-återställning

Data som kan ha äventyrats, krypterats eller tagits bort under angreppet måste återskapas. Det kan handla om att återskapa data från säkerhetskopior eller använda specialiserade dataåterställningstekniker för att återfå förlorade eller krypterade filer.

Teknisk analys

Efter ett angrepp är det viktigt att förstå hur intrånget inträffade, vilka sårbarheter som användes och vilka åtgärder som behöver vidtas för att förhindra liknande angrepp. System som säkerhetsinformations- och händelsehanteringssystem (SIEM) och funktioner som externa BIOS-jämförelser kan ge värdefulla insikter.

Utvärdering av åtgärder vid incidenter

Efter återställning är det viktigt att utvärdera de åtgärder som vidtogs vid incidenten och identifiera förbättringsområden. Lärdomar från angrepp kan användas för att förbättra säkerhetsrutiner, uppdatera åtgärdsplaner för incidenter och ge bättre skydd mot framtida incidenter.

Professionella tjänster och samarbeten

Leverantörer av cybersäkerhetstjänster och teknikpartner tillhandahåller värdefull expertis och resurser som hjälper organisationen att återhämta sig. De kan bland annat hjälpa till att analysera spåren, identifiera var intrånget har skett och rekommendera åtgärder för att förhindra framtida incidenter.

DELL Technologies

Utöka cybersäkerheten till kanter och molnmiljöer

När nätverken sprider sig från kärnan till kanten till molnet har miljöerna blivit en viktig sårbarhetspunkt.

När cybersäkerhetsstrategin implementeras bör organisationen utvidga nollförtroendeprincipen till kanten och molnet för att säkerställa noggranna åtkomstkontroller, kontinuerlig autentisering och omfattande synlighet och kontroll över nätverkstrafiken. Eftersom hotlandskapet ständigt utvecklas är det bra att distribuera AI-funktioner som en första försvarslinje. Dessutom är en strategi bara komplett om kärnnätverk och molnmiljöer har säkerhetsåtgärder, till exempel nätverkssegmentering, kryptering och kontinuerlig övervakning.

Professionella cybersäkerhetstjänster kan hjälpa dig att få ett helhetsperspektiv.

Det kan vara en utmaning att koppla ihop olika säkerhetslösningar. Samarbete med professionella tjänster som är specialiserade på kant-, kärn- och molnsäkerhet ger expertis nog att vidta effektiva åtgärder som skyddar organisationen från alla håll.

Kant

Etablera flera säkerhetsskikt i kanten, i nätverket och i hårdvara och mjukvara.

Kärna

Anpassa infrastrukturen till en nollförtroendemetod med hjälp av AI, ML och automatisering.

Flermolnsmiljöer

Skydda alla arbetsbelastningar i alla miljöer, inklusive offentliga moln, behållare och molnintegrerade arbetsbelastningar.

DELL Technologies

GenAI: Ett dubbelsidigt svärd för cybersäkerhet

Nästa generation av AI medför i snabb takt nya risker, men även förbättrad säkerhet.

GenAI – nästa fas inom AI – omfattar system som kan förstå, lära sig, anpassa sig och implementera kunskap inom en rad olika uppgifter.

Å ena sidan utlovas förbättrad hotdetektering och åtgärder, prediktiva funktioner och driftseffektivitet. Å andra sidan medför det nya utmaningar som kräver utvecklade cybersäkerhetsstrategier som hanterar risker genom robusta säkerhetsåtgärder, kontinuerlig övervakning, regelbundna uppdateringar och korrigeringar samt metoder för datasekretess och etik som ständigt utvecklas.

Skydda organisationer med GenAI

GenAI har blivit ett viktigt verktyg inom cybersäkerhet som öppnar upp för nya skyddsmöjligheter.

- Öka effektiviteten i hotidentifiering och åtgärder.
- Förutsäg framtida hot eller identifiera potentiella sårbarheter.
- Automatisera hotidentifieringen och öka effektiviteten.
- Tillämpa teknisk analys för att snabbt identifiera mönster, avvikelser och tecken på intrång.
- Anpassa säkerhetsutbildningar.
- Skala säkerhetsåtgärder med snabbare åtkomst till större insikter.

Skydda GenAI-system

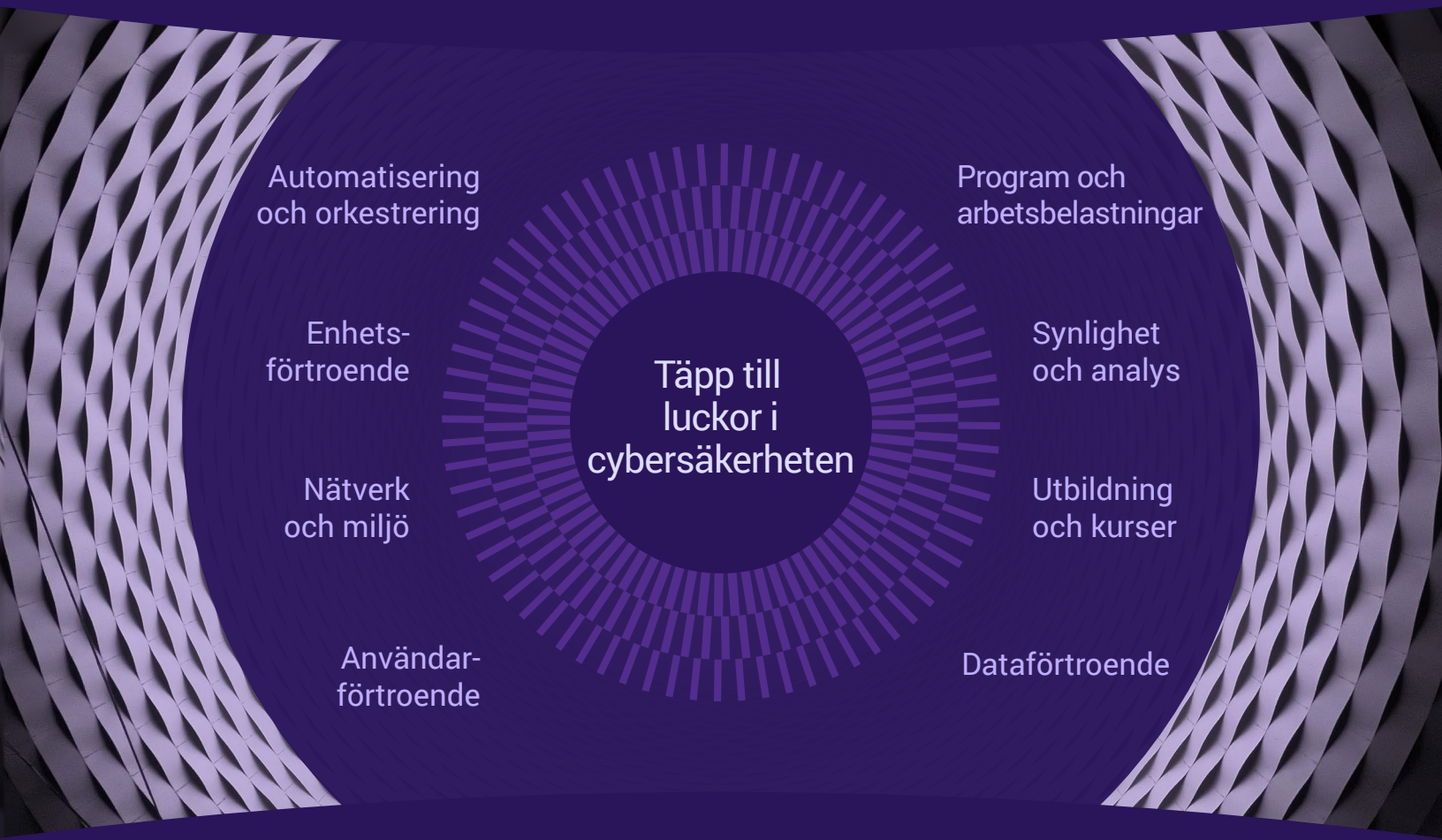
GenAI erbjuder betydande säkerhetsfördelar, men funktionerna kan användas på skadliga sätt om de inte skyddas på lämpligt sätt.

- Säkerställ datasekretess och integritet.
- Minska fientliga angrepp avsedda att lura AI-system och orsaka fel.
- Upptäck och reagera på felaktig systemanvändning från skadlig AI-användning.
- Granska och minska etiska problem och partiskhet.
- Implementera starka åtkomstkontroller för AI-system.
- Skydda och återställ stora språkmodeller (LLM) på ett säkert sätt.

DELL Technologies

Modern cybersäkerhet bör vara smart, skalbar och automatiserad

Dell Technologies kan hjälpa dig att skapa heltäckande säkerhet som skyddar mot ständigt föränderliga cyberhot. När tekniken utvecklas ligger vår strategi för cybersäkerhet steget före och utnyttjar kraften i AI och ML för att skydda dina digitala infrastrukturer och bibehålla förtroendet för den digitala världen. Oavsett var du befinner dig på resan mot cybersäkerhet kommer vi att samarbeta med dig för att inte bara skydda organisationen, utan vidta åtgärder som ser till att den alltid är flexibel och motståndskraftig.



DELL Technologies

Dell.com/SecuritySolutions
Vill du att vi ringer upp dig?
Chatta med en säkerhetsrådgivare
Ring 1-800-433-2393