DELL Technologies

Nollförtroende
En väg till bättre cybersäkerhet

Gör resan mot nollförtroende med en erfaren teknik- och säkerhetspartner.

Organisationer som främjar sin cybersäkerhetsmognad bygger en användbar handlingsplan som identifierar sätt att minska angreppsytan, upptäcka och reagera på cyberhot och implementera sätt att återställa efter cyberattacker, allt med funktioner för nollförtroendeaktivering.

Dell använder de inbyggda säkerhetsfunktionerna i våra lösningar och våra partner för att hantera alltmer sofistikerade cyberhot och hjälpa våra kunder att uppnå nollförtroende som anpassar sig till kundernas affärsmål.

Vad är noll-förtroende?

Föreställ dig ditt nätverk som ett slott. När bryggan är nere och någon kommer in kan de röra sig fritt. Det är dags att uppdatera den perimeterbaserade säkerhetsmodellen för försvar till ett mer modernt och säkrare nollförtroenderamverk.

Nollförtroende är en arkitekturmetod för säkerhet jämfört med en produkt som du köper. Det litar aldrig på något och verifierar alltid äkta affärsanvändning innan någon eller något ges åtkomst till resurser. Det innebär att användare och enheter inte är betrodda som standard, även om de är anslutna till ett behörighetsnätverk och även om de har verifierats tidigare.

Lita aldrig på något, verifiera alltid.

Grundläggande för ett säkert IT-ekosystem.

Nollförtroenderamverket, enligt definitionen från National Institute of Standards and Technologies (NIST), har införts och byggts in i en arkitektur av det amerikanska försvarsdepartementet (DoD).

Det omfattar sju sammanhängande grundpelare som styr Dell Technologies i alla säkerhetsdomäner. När de kombineras ger grundpelarna en integrerad arkitektur med flera gränssnitt för en omfattande säkerhetsstrategi som skyddar organisationens data och infrastruktur.

Implementering med nollförtroende har varit en utmaning på grund av komplexiteten i att integrera olika säkerhetsfunktioner och navigera fragmenterade alternativ från ett antal säkerhetsleverantörer.

NIST

U.S. Department of Defense

DELL Technologies

Öka din nollförtroendemognad.

Dell har lösningar som kan hjälpa dig, oavsett var du är på din resa.

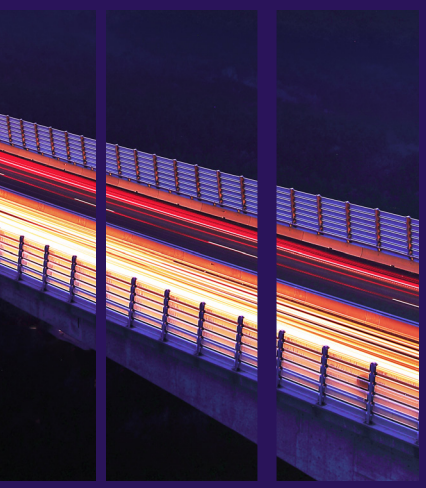
Dell Technologies ger din organisation valfrihet och flexibilitet. Om du vill förbättra din cybersäkerhetsmognad kan vi tillhandahålla säkerhetslösningar med nollförtroendekapacitet för att förbättra din förmåga att härda, upptäcka, försvara och återskapa efter en skadlig cyberaktivitet.

Aktivera nollförtroendeprinciper.

Möjliggör valmöjligheter och flexibilitet för att främja cybersäkerhetsmognad.

Dell Technologies erbjuder säkerhetslösningar och nollförtroendefunktioner för att förbättra din förmåga att härda, upptäcka, försvara och återställa efter skadlig cyberaktivitet. Så här fungerar det:

- Inbyggt skydd som förbättrar automatisering, hotinformation, autentisering, synlighet och mycket mer
- Tjänster för att utveckla en handlingsplan, integrera viktiga tekniker och proaktivt hantera till stöd för nollförtroende
- Professionella, hanterings- och säkerhetsrådgivningstjänster
- Omfattande partnersystem



Förenkla implementeringen av nollförtroende dramatiskt.

Gå all-in med en helt integrerad arkitektur.

Eftersom nollförtroende är en arkitekturmetod för säkerhet är det inte en enskild produkt som kräver en noggrant planerad lösning. Dell tar bort integreringsbördan för nollförtroende. Så här går det till:

- Dell bygger den första och enda helt integrerade nollförtroendearkitekturen som utformats, testats och validerats av amerikanska försvarsdepartementet

DELL Technologies

Aktivera nollförtroendeprinciper.

Uppnå nollförtroende på ett sätt som bygger på ditt specifika säkerhetsekosystem.

Dell bidrar till att förbättra cybersäkerhetsmognaden med stöd för nollförtroendestrategier som hjälper till att minska angreppsytan, förbättra upptäckt och snabb återställning från cyberhot.

Inom var och en av grundpelarna för nollförtroende finns tekniker, processer och personer som anpassat sig till viktiga områden där säkerhets- och affärspolicyer behövs för att skydda din organisation. Dells säkerhetstjänster kan hjälpa dig med:

- Säkerhetsmognad, nollförtroende och riskbedömningar
- Utveckling av strategi och handlingsplan
- Hanterade tjänster för viktiga nollförtroendefunktioner

DELL Technologies

Grunderna för nollförtroende.

Vi tillhandahåller avancerade inbyggda säkerhetslösningar som ger dig en fördel på vägen till nollförtroende.

Dell Data Protection

Cyber Recovery-valv | PowerProtect Data Manager | CyberSense transparenta ögonblicksbilder | Cloud IQ | Systemlåsning | Drift-upptäckt | Säker Enterprise-nyckelhantering | TLS 1.3 | IPv6 | Flerfaktorautentisering | Enkel inloggning | Rollbaserad åtkomst | Cloud IQ

Dell PowerEdge-servrar

Materialsedel för mjukvara | Säker komponentverifiering | Silicon Root of Trust | Systemlåsning | Drift-upptäckt | Säker Enterprise-nyckelhantering | TLS 1.3 | IPv6 | Flerfaktorautentisering | Enkel inloggning | Rollbaserad åtkomst | Cloud IQ

Dells lagringsplattformar

Dataisolering | Dataoföränderlighet | Hotidentifiering | Autentisering av åtkomstkontroll | Datakryptering | STIG-härdning | HW Root of Trust | Säker start | Digitalt signerad inbyggd mjukvara | Rollbaserad åtkomst | Säkra ögonblicksbilder

Dell HCI/CI

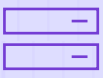
Hårdvarubaserad förtroenderot | Säker startkedja | Digitalt signerade uppdateringar | Nyckelhantering | Säkra loggar | Distribuerade virtuella switchar | VM-isolering | Autentisering och auktorisering | Ekosystemsanslutningar | Kontinuerligt validerade tillstånd | Mjukvarukodsintegritet | Matris för elektronisk kompatibilitet

Dells kommersiella stationära datorer

Säkerhet för BIOS/inbyggd mjukvara | Hårdvarusäkerhet | Försäkring av leverantörskedjan | mjukvara för hothantering (EDR, XDR, VDR) | mjukvara för nätverks- och molndataskydd

Dell Edge-lösningar

HW/SW/VM-attestering | Säker onboarding | Certifikatkedja | Säker OS-/applikationsleverans | Hantering av datarättighet



Dells nätverksswitchar

SmartFabric | Cloud IQ | SD-WAN | VLAN-segmentering | Enterprise SONiC | Åtkomstkontrollistor | RADIUS | TACACS+ | Kryptografi | Switch-härdning | Mikrosegmentering | Virtuell routning och vidarebefordring

DELL Technologies

Vårt accelererade tillvägagångssätt.

Project Fort Zero är snabbt och grundligt och integrerar nollförtroende i hela din organisation från ett helhetsperspektiv.

Project Fort Zero erbjuder en validerad metod för omedelbar avancerad mognad i nollförtroende, vilket minskar implementeringstiden, störningar och hanterar kostnader.

På grund av vår expertis och räckvidd inom branschen bad det amerikanska försvarsdepartementet Dell Technologies att hjälpa till att accelerera implementeringen av nollförtroende. För att hjälpa privata och offentliga organisationer att förenkla implementeringen och globalt skala arkitekturen för nollförtroende bygger Dell ett ekosystem och leder integreringen av mer än 30 ledande teknik- och säkerhetsföretag. Vi är ledande inom utveckling och global skalning av arkitektur för nollförtroende för både privata och offentliga organisationer över hela världen. Det här visar Dells engagemang för att uppnå nollförtroende som kommer från det amerikanska försvarsdepartementet.

På plats

I datacenter för organisationer där datasäkerhet och regelefterlevnad är av största vikt.

Fjärranslutet eller regionalt

På platser som butiker där säker analys i realtid av kunddata kan ge konkurrensfördelar.

Den löstagbara kanten

På platser som flygplan eller fordon med intermittenta anslutningsmöjligheter där tillfällig implementering behövs för driftkontinuitet.

DELL Technologies

Vi hjälper dig att accelerera implementering av nollförtroende genom att driftsätta alla **152** aktiviteter som tagits fram av det amerikanska försvarsdepartementet för en avancerad nivå av nollförtroende.

Körningsaktiverare

Doktrin | Företag | Utbildning | Material | Ledarskap och utbildning | Personal | Anläggningar | Policy

Målnivå för nollförtroende

Användar-förtroende

- Användarinventering
- Appbaserad behörighet
- Regelbaserad dynamisk åtkomst, del 1
- Organisatoriska MFA/IDP
- Implementera system och minimera privilegierade användare, del 1
- Hantering av organisationens identitetslivscykel
- Neka användaren med standardpolicy
- Enkel autentisering
- Implementera system och minimera privilegierade användare, del 2
- Hantering av organisationens identitetslivscykel, del 1
- Genomföra UEBA-verktyg
- Periodisk autentisering
- Enterprise PKI/IDP, del 1

Enhets-förtroende

- Hjälpverktyg för enheter: analys av mellanrum
- Integrera NextGen AV-verktyg med C2C
- NPE/PKI-enhet under hantering
- Neka enhet som standardpolicy
- Implementera UEDM eller motsvarande verktyg
- Enhetshantering för företag, del 1
- Implementera EDR-verktyg och integrera med C2C
- Implementera verktyg för tillgångs-, sårbarhets- och korrigeringshantering
- Enterprise-IDP, del 1
- Implementera C2C/efterlevnadsbaserad nätverksauktorisering, del 1
- Implementera appkontrolls- och FIM-verktyg
- Hanterad och begränsad BYOD- och IOT-support
- Enhetshantering för företag, del 2
- Implementera XDR-verktyg och integrering med C2C, del 1

Program och arbetsbelastning

- Program-/kodidentifiering
- Resursauktorisering, del 1
- Bygga DevSecOps-mjukvarufabrik, del 1
- Godkända binärfiler/kod
- Programmet Vulnerability Management, del 1
- SDC-resursauktorisering, del 1
- Resursauktorisering, del 2
- Bygga DevSecOps-mjukvarufabrik, del 2
- Automatisera program-säkerhet och kodåtgärder, del 1
- Programmet Vulnerability Management, del 2
- Kontinuerlig validering
- SDC-resursauktorisering, del 2

Data-förtroende

- Dataanalys
- Loggning och analys av DLP-verkställningspunkter
- Loggning och analys av DRM-verkställningspunkter
- Definiera data-märkningsstandarder
- Implementera datamärknings- och klassificeringsverktyg
- Filaktivitetsövervakning, del 1
- Implementera DRM och skyddsverktyg, del 1
- Implementera verkställningspunkter
- Interoperabilitets-standarder
- Utveckla SDS-policy
- Manuell data-märkning, del 1
- Filaktivitetsövervakning, del 2
- Implementera DRM- och skyddsverktyg, del 2
- DLP-verkställning via dataggar och analys, del 1
- Integrera DAAS-åtkomst med SDS-policy, del 1
- DRM-verkställning via dataggar och analys, del 1
- Integrera SDS-lösning(ar) och -policy med Enterprise IDP, del 1

Nätverk och miljö

- Definiera detaljerade kontrollåtkomstregler och -policyer, del 1
- Definiera SDN-API:er
- Definiera detaljerade kontrollåtkomstregler och -policyer, del 2
- Implementera programmerbar SDN-infrastruktur
- Makrosegmentering av datacenter
- Implementera mikrosegmentering
- Segmentera flöden till kontrollhantering och dataplan
- Segmentering av B/C/P/S-makro
- Program- och mikrosegmentering för enhet
- Skydda data under överföring

Automatisering och orkestrering

- Policyinventering och utveckling
- Analys av uppgiftsautomatisering
- Svarsautomatiserings-analys
- Analys av verktygsefterlevnad
- Organisationens åtkomstprofil
- Implementera SOAR-verktyg
- Standardiserade API-anrop och -scheman, del 1
- Arbetsflödes-berikande, del 1
- Företagssäkerhetsprofil, del 1
- Etablering av företagsintegrering och arbetsflöde, del 1
- Implementera ML-verktyg för datamärkning och klassificering
- Standardiserade API-anrop och -scheman, del 2
- Arbetsflödes-berikande, del 2

Synlighet och analys

- Skalningsöverväganden
- Loggparsning
- Korrelation mellan tillgångs-ID och varningar
- Hotvarning, del 1
- Implementera analysverktyg
- Cyber Threat Intelligence-program, del 1
- Logganalys
- Hotvarning, del 2
- Användar-/enhetsreferensvärden
- Etablera användarens referensvärdesbeteende
- Referensvärde och profilering, del 1
- Cyber Threat Intelligence-program, del 2

Totala målaktiviteter: 91

Källa: Publicering av DoD Zero Trust Strategy, 7 november 2022

DELL Technologies

Avancerat nollförtroende

Användar-förtroende	Enhets-förtroende	Program och arbetsbelastning	Data-förtroende	Nätverk och miljö	Automatisering och orkestrering	Synlighet och analys
Regelbaserad dynamisk åtkomst, del 2	Företags-IDP, del 2	Berika attribut för resursauktorisering, del 1	Manuell data-märkning, del 2	Identifiering och optimering av nätverkstillgång	Företagssäkerhetsprofil, del 2	Hotvarning, del 3
Företagsroller och behörigheter, del 1	Implementera C2C/ efterlevnadsbaserad nätverksauktorisering, del 2	Berika attribut för resursauktorisering, del 2	Övervakning av databasaktivitet	Beslut om åtkomst i realtid	Etablering av företagsintegrering och arbetsflöde, del 2	Referensvärde och profilering, del 2
Alternativ flexibel MFA, del 1	Övervakning av enhetsaktivitet, del 1	Kontinuerlig auktorisering för drift (ATO), del 1	Automatiserad datamärkning och support, del 1	Behandla mikrosegmentering	Implementera AI-automatiseringsverktyg	UEBA-referensvärdesstöd, del 1
Godkännanden i realtid och JIT-/JEA-analys, del 1	Helt integrerad enhetssäkerhetsstack med C2C	Automatisera program-säkerhet och kodåtgärder, del 2	DRM-verkställning via dataaggar och analys, del 2		Arbetsflödes-berikande, del 3	UEBA-referensvärdesstöd, del 2
Livscykelhantering av företagsidentitet, del 2	Enterprise-PKI, del 1	REST API-mikrosegment	DLP-verkställning via dataaggar och analys, del 2		AI driven av analys fastställer A&O-ändringar	AI-aktiverad nätverksåtkomst
Övervakning av användaraktivitet, del 1	Hanterad och fullständig BYOD- och IOT-support, del 1	Kontinuerlig auktorisering för drift (ATO), del 2	Integrera DAAS-åtkomst med SDS-policy, del 2		Implementera playbooks	AI-aktiverad dynamisk åtkomstkontroll
Kontinuerlig autentisering, del 1	Implementera XDR-verktyg och integrering med C2C, del 2		Integrera SDS-lösning(ar) och policy med företags-IDP, del 2		Automatiserade arbetsflöden	
Kontinuerlig autentisering, del 2	Övervakning av enhetsaktivitet, del 2		Integrera SOS-verktyg och/eller integrera med DRM-verktyg, del 1			
Företags-PKI/IDP, del 3	Företags-PKI, del 2		Automatiserad datamärkning och support, del 2			
Företagsroller och behörigheter, del 2	Hanterad och fullständig BYOD- och IOT-support, del 2		Omfattande övervakning av dataaktivitet			
Alternativ flexibel MFA, del 2			DRM-verkställning via dataaggar och analys, del 3			
Godkännanden i realtid och JIT-/JEA-analys, del 2			DLP-verkställning via dataaggar och analys, del 3			
Livscykelhantering av företagsidentitet, del 3			Integrera DAAS-åtkomst med SDS-policy, del 3			
Övervakning av användaraktivitet, del 2			Integrera SDS-verktyg och/eller integrera med DRM-verktyg, del 2			
Företags-PKI/IDP, del 2						

Totalt antal avancerade aktiviteter: 61

Dell Technologies kan förenkla komplexiteten med att uppnå nollförtroendemognad snabbt.

Källa: Publicering av DoD Zero Trust Strategy, 7 november 2022

DELL Technologies

Tillgodose alla organisationers behov.

Öka din nollförtroendemognad.

Nollförtroende är ett definierat ramverk och en uppsättning principer som vägleder hur säkerheten ska hanteras, och det kan implementeras med hjälp av en mängd olika funktioner. Oavsett om du är all-in på nollförtroende eller fokuserar på riktade förbättringar som anpassar sig till principerna för nollförtroende så är Dell en erfaren säkerhetspartner som hjälper dig på din säkerhetsresa.

Kemi	Informationsteknik	Kommunikation	Räddningstjänster
Livsmedel och jordbruk	Försvar	Hälso- och sjukvård och folkhälsa	Tillverkning
Ekonomi	Kärnreaktorer	Kommersiella	Myndigheter
Energi	Transport	Vatten och avlopp	Dammar

DELL Technologies

DELL Technologies

En erfaren teknik- och säkerhetspartner för organisationens resa mot nollförtroende.

Förbättra cybersäkerheten långsiktigt genom att implementera nollförtroende.

Dells säkerhetstjänster erbjuder:

Expertutvärdering av säkerhetsmognad och övergripande risk.

Utveckling av en handlingsplan för nollförtroende.

Löpande hantering av säkerhetsaktiviteter.

DELL Technologies

Dell.com/SecuritySolutions

Vill du att vi ringer upp dig?

Chatta med en säkerhetsrådgivare

Ring 1-800-433-2393