DELL Technologies

Zero Trust

Op weg naar betere cyberbeveiliging

Maak kennis met Zero Trust aan de hand van een ervaren technologie- en beveiligingspartner.

Organisaties die de groei van cyberbeveiliging stimuleren, bouwen een uitvoerbare roadmap die manieren identificeert om hun aanvalsoppervlak te verminderen, cyberdreigingen te detecteren en daarop te reageren en om manieren te implementeren voor het herstellen van cyberaanvallen, allemaal met de capaciteiten van Zero Trust.

Om steeds geavanceerdere cyberdreigingen aan te pakken, maakt Dell gebruik van de geïntegreerde beveiligingsmogelijkheden in onze oplossingen en onze partners om onze klanten te helpen Zero Trust te bereiken die is afgestemd op de zakelijke doelstellingen van onze klanten.

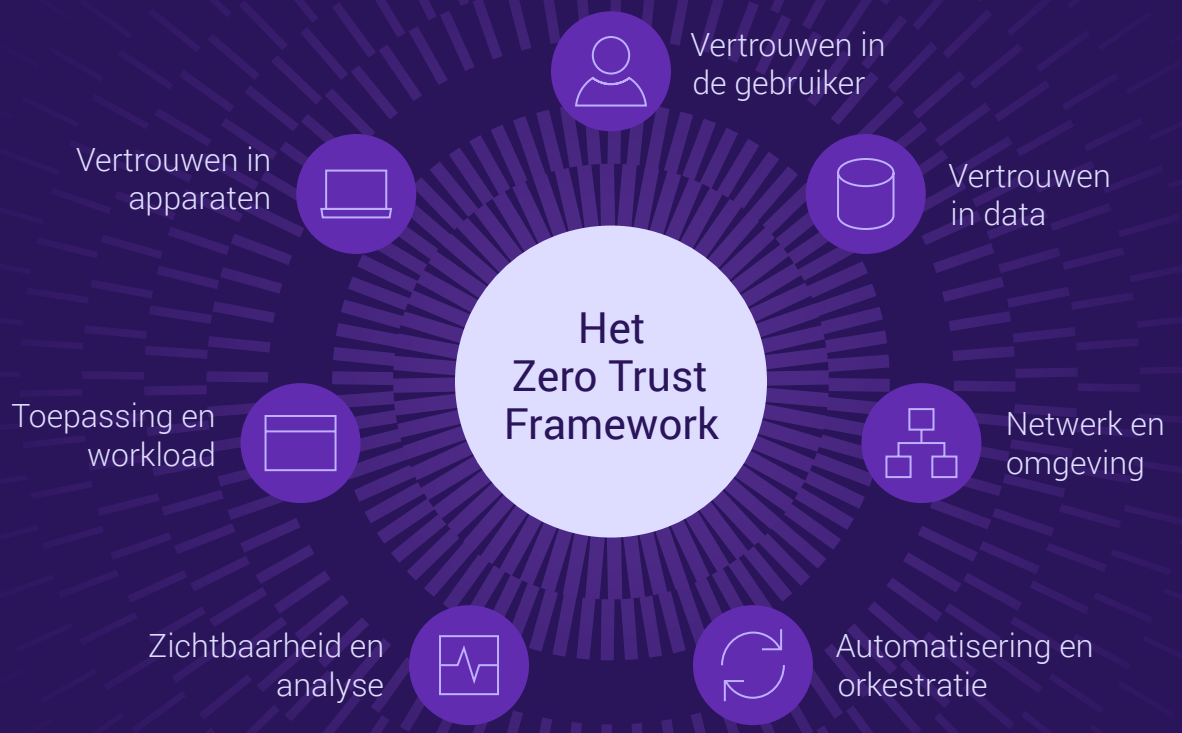
Wat is Zero Trust?

Stelt u zich uw netwerk voor als een kasteel. Zodra de brug is neergelaten en iemand binnenkomt, kunnen ze vrij rondlopen. Het is tijd om het beveiligingsmodel voor beveiliging op basis van perimeters bij te werken naar het modernere, veiligere Zero Trust-framework.

Zero Trust is een architectuurgerichte benadering van beveiliging versus een product dat u aanschaft. Het vertrouwt nooit en controleert altijd legitiem zakelijk gebruik voordat het iemand of iets toegang geeft tot bronnen. Dit betekent dat gebruikers en apparaten niet standaard worden vertrouwd, zelfs als ze zijn verbonden met een goedgekeurd netwerk en zelfs als ze eerder zijn geverifieerd.

Vertrouw nooit blind, verifieer altijd.

Fundamentele principes voor een veilig IT-ecosysteem.



Het Zero Trust-framework, zoals gedefinieerd door het National Institute of Standards and Technologies (NIST), is door het Amerikaanse Department of Defense (DoD) overgenomen en geïntegreerd in een architectuur.

Het omvat zeven met elkaar verbonden pijlers die Dell Technologies begeleiden in alle beveiligingsdomeinen. In combinatie bieden de pijlers een veelzijdige, geïntegreerde architectuur voor een uitgebreide beveiligingsaanpak die de data en infrastructuur van uw organisatie beschermt.

De invoering van Zero Trust is een uitdaging vanwege de complexe integratie van diverse beveiligingsmogelijkheden en navigatie door gefragmenteerde opties van een aantal beveiligingsleveranciers.

NIST

U.S. Department of Defense

DELL Technologies

Laat uw Zero Trust verder groeien.

Waar u ook bent op uw reis, Dell heeft oplossingen om u te helpen.

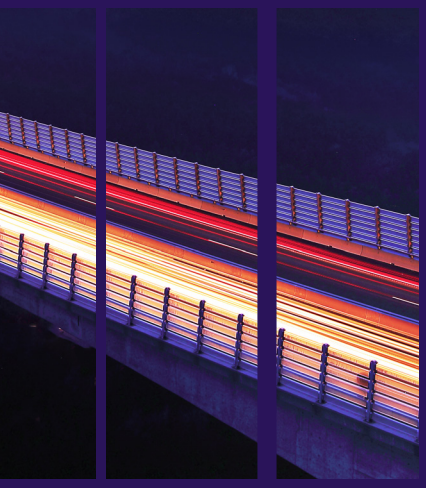
Dell Technologies biedt keuzes en flexibiliteit voor uw organisatie. Als u de volwassenheid van uw cyberbeveiliging wilt verbeteren, kunnen we beveiligingsoplossingen leveren met Zero Trust-mogelijkheden om uw vermogen om kwaadaardige cyberactiviteiten op te vangen, te detecteren, te verdedigen en te herstellen, te vergroten.

Zero Trust-principes toepassen.

Maak keuze en flexibiliteit mogelijk voor het bevorderen van de groei van cyberbeveiliging.

Dell Technologies biedt beveiligingsoplossingen en Zero Trust-mogelijkheden waarmee u uw vermogen om kwaadaardige cyberactiviteiten op te vangen, te detecteren, te verdedigen en te herstellen, kunt vergroten. Dit is hoe:

- Geïntegreerde beschermingen die automatisering, bedreigingsinformatie, authenticatie, zichtbaarheid en meer verbeteren
- Services om een roadmap te ontwikkelen, belangrijke technologieën te integreren en proactief te beheren ter ondersteuning van Zero Trust
- Professionele, beheerde en veilige adviesservices
- Uitgebreid partner ecosysteem



Vereenvoudig de invoering van Zero Trust drastisch.

Ga voluit met een volledig geïntegreerde architectuur.

Omdat Zero Trust een architectuurmatige benadering van beveiliging is, is het niet een enkel product en vergt het een zorgvuldig geplande afstemming van oplossingen. Dell neemt de last van Zero Trust-integratie weg. Zo werkt het:

- Dell bouwt aan de eerste en enige volledig geïntegreerde Zero Trust-architectuur die is ontworpen, getest en gevalideerd door het Amerikaanse Department of Defense

DELL Technologies

Zero Trust-principes toepassen.

Behaal Zero Trust op een manier die wordt gebouwd op uw specifieke beveiligingsecosysteem.

Dell helpt de groei van cyberbeveiliging te verbeteren ter ondersteuning van Zero Trust-strategieën, die helpen het aanvalsoppervlak te verminderen, detectie te verbeteren en herstel van cyberdreigingen te versnellen.

Binnen elk van de afgebeelde Zero Trust-pijlers zijn technologieën, processen en personen afgestemd op kritieke gebieden waar beveiliging en bedrijfsbeleid nodig zijn om uw organisatie te beschermen. Dell Security Services kan u helpen met:

- Groei van beveiliging, Zero Trust en risicobeoordelingen
- Ontwikkeling van strategie en roadmap
- Beheerde services van belangrijke Zero Trust-mogelijkheden

DELL Technologies

Zero Trust-basis.

Wij bieden geavanceerde, geïntegreerde beveiligingsoplossingen die u een voorsprong geven op uw pad naar Zero Trust.

Dell Data Protection

Kluis voor Cyber Recovery | PowerProtect Data Manager | CyberSense transparante snapshots | Cloud IQ | Systeemvergrendeling | Driftdetectie | Veilig beheer van bedrijfssleutels | TLS 1.3 | IPv6 | Meervoudige verificatie | Eenmalige aanmelding | Op rollen gebaseerde toegang | Cloud IQ

Dell PowerEdge servers

Softwarefactuur van materialen | Verificatie van veilige onderdelen | Silicon Root of Trust | Systeemvergrendeling | Driftdetectie | Veilig beheer van bedrijfssleutels | TLS 1.3 | IPv6 | Meervoudige verificatie | Eenmalige aanmelding | Op rollen gebaseerde toegang | Cloud IQ

Dell storageplatforms

Dataisolatie | Onveranderlijkheid van data | Bedreigingsdetectie | Verificatie van toegangscontrole | Gegevenscodering | STIG-versteviging | HW-basis van vertrouwen | Secure Boot | Digitaal ondertekende firmware | Toegang op basis van rollen | Veilige snapshots

Dell HCI/CI

Vertrouwde hardwareroot | Veilige opstartketen van vertrouwen | Digitaal ondertekende updates | Sleutelbeheer | Beveiligde logboekregistratie | Gedistribueerde virtuele switches | VM-isolatie | Verificatie en autorisatie | Ecosysteemconnectoren | Continu gevalideerde statussen | Integriteit van softwarecode | Elektronische compatibiliteitsmatrix

Commerciële PC's van Dell

BIOS-/firmwarebeveiliging | Hardwarebeveiliging | Leveringsketengarantie | Software voor bedreigingsbeheer (EDR, XDR, VDR) | Data Protection Software in het netwerk en de cloud

Dell edge-oplossingen

HW/SW/VM attestatie | Veilige onboarding | Vertrouwensketen | Veilige levering van besturingssystemen/applicaties | Beheer van datarechten

Dell networking switches

SmartFabric | Cloud IQ | SD-WAN | VLAN-segmentatie | Enterprise SONiC | Toegangscontrolelijsten | RADIUS | TACACS+ | Cryptografie | Switchversterking | Microsegmentatie | Virtuele routering en doorsturen

DELL Technologies

Onze versnelde aanpak.

Project Fort Zero is snel en grondig en integreert Zero Trust in al uw organisatie op holistische wijze.

Project Fort Zero biedt een gevalideerde methode voor directe geavanceerde groei in Zero Trust, waardoor de acceptatietijd wordt verkort, onderbrekingen worden verminderd en de kosten worden beheerd.

Op basis van onze expertise en bereik binnen de branche, heeft het Amerikaanse Department of Defense Dell Technologies gevraagd om te helpen bij het versnellen van de acceptatie van Zero Trust. Om organisaties in de particuliere en publieke sector te helpen de ingebruikname te vereenvoudigen en de Zero Trust-architectuur wereldwijd op te schalen, bouwt Dell een ecosysteem en leidt het de integratie van meer dan 30 toonaangevende technologie- en beveiligingsbedrijven. Wij leiden de ontwikkeling en wereldwijde opschaling van Zero Trust-architectuur voor zowel particuliere als publieke organisaties wereldwijd. Dit is een bevestiging van de toewijding van Dell aan de Amerikaanse DoD-doelstellingen om zero trust te bereiken.

On-premises

In datacenters voor organisaties waar databeveiliging en naleving van het grootste belang zijn.

Extern of regionaal

Op locaties zoals winkels waar veilige, realtime analyse van klantdata een concurrentievoordeel kan opleveren.

De verwijderbare edge

Op plaatsen zoals vliegtuig of voertuigen met onregelmatige connectiviteit waar tijdelijke implementatie nodig is voor operationele continuïteit.

DELL Technologies

We helpen u bij het versnellen van de ingebruikname van Zero Trust door alle **152** activiteiten van de Amerikaanse DoD te implementeren voor een geavanceerd niveau van Zero Trust.

Uitvoeringsbevorderende factoren

Leer | Organisatie | Training | Materiaal | Leiderschap en onderwijs | Personeel | Faciliteiten | Beleid

Zero Trust-doelniveau

Vertrouwen in de gebruiker

- Gebruikersinventaris
- Toestemming op basis van app
- Op regel gebaseerde Dynamische Toegang tot pt. 1
- Organisatorische MFA/ IDP
- Systeem implementeren en gebruikers met privileges beperken pt. 1
- Levenscyclusbeheer organisatie-identiteit
- Standaardbeleid voor weigeren gebruiker
- Enkele verificatie
- Systeem implementeren en gebruikers met privileges beperken pt. 2
- Levenscyclusbeheer bedrijfsidentiteit pt. 1
- UEBA tooling implementeren
- Periodieke verificatie
- Enterprise PKI/IDP pt. 1

Vertrouwen in apparaten

- Apparaathulpprogram-ma Analyse van hiaten
- NextGen AV-tools integreren met C2C
- NPE/PKI-apparaat onder beheer
- Standaardbeleid voor weigeren apparaat
- UEDM of soortgelijke tools implementeren
- Beheer voor bedrijfsapparaat pt. 1
- EDR-tools implementeren en integreren met C2C
- Tools voor asset-, beveiligingslekken en patchbeheer implementeren
- Enterprise IDP pt. 1
- Implementatie van C2C/ Compliance Based Network Authorization pt. 1
- App Control en FIM Tools implementeren
- Beheerd en beperkt BYOD en IOT-ondersteuning
- Beheer voor bedrijfsapparaat pt. 2
- XDR-tools implementeren en integreren met C2C pt. 1

Toepassing en workload

- Identificatie van applicatie/code
- Bronautorisatie pt. 1
- Build DevSecOps Software Factory Pt. 1
- Goedgekeurd Binaire bestanden/code
- Programma kwetsbaarheidsbeheer pt. 1
- SDC Bronautorisatie Pt. 1
- Bronautorisatie pt. 2
- Build DevSecOps Software Factory Pt. 2
- Applicatie automatiseren Security en Code oplossing Pt. 1
- Programma kwetsbaarheidsbeheer pt. 2
- Continue validatie
- SDC Bronautorisatie Pt. 2

Vertrouwen in data

- Data-analyse
- DLP-handhavingspunt logging en analyse
- DRM-handhavingspunt logging en analyse
- Data definiëren tag-normen
- Tools voor datataggen en classificatie implementeren
- Controle op bestandsactiviteit pt. 1
- DRM en beschermingstools pt. 1 implementeren
- Handhavingspunten implementeren
- Interoperabiliteitsnor-men
- SDS-beleid ontwikkelen
- Handmatig data taggen pt. 1
- Controle op bestandsactiviteit pt. 2
- DRM implementeren en bescherming Hulpprogramma's pt. 2
- DLP-handhaving via datatags en analyse pt. 1
- Daas-toegang integreren met SDS-beleid pt. 1
- DRM-handhaving via datatags en analyse pt. 1
- SDS-oplossing(en) en beleid met Enterprise IDP pt. 1 integreren

Netwerk en omgeving

- Definieer regels en beleid voor fijnmazige toegangscontroles pt. 1
- SDN APIs definiëren
- Definieer regels en beleid voor fijnmazige toegangscontrole pt. 2
- SDN programmeerbare infrastructuur implementeren
- Datacenter macrosegmentatie
- Microsegmentatie implementeren
- Segmentstroom naar controlebeheer en datavlakken
- B/C/P/S macrosegmentatie
- Microsegmentatie voor applicaties en apparaten
- Gegevens tijdens transport beschermen

Automatisering en orkestratie

- Beleidsinventaris en ontwikkeling
- Analyse van taakautomatisering
- Responsautomatisering Analyse
- Analyse van naleving van tools
- Organisatie Toegangsprofiel
- SOAR-tools implementeren
- Gestandaardiseerde API-oproepen en schema's pt. 1
- Workflow verrijking pt. 1
- Enterprise-beveiligingsprofiel pt. 1
- Bedrijfsintegratie en workflowprovisioning pt. 1
- Datataggen en -classificatie implementeren ML-tools
- Gestandaardiseerde API-oproepen en schema's Pt. 2
- Workflow Verrijking pt. 2

Zichtbaarheid en analyse

- Overwegingen bij opschalen
- Logboekparseren
- Asset-ID en correlatie van waarschuwingen
- Bedreigingswaarschu-wing pt.1
- Implementeren analysetools
- Informatie over programma cyberdreigingen pt. 1
- Analyse van logboeken
- Bedreigingswaarschu-wingen pt. 2
- Basislijnen gebruiker/ apparaat
- Basisgedrag van de gebruiker vaststellen
- Basislijn en Profilering pt. 1
- Informatie over programma cyberdreigingen pt. 2

Totale doelactiviteiten: 91

Bron: DoD Zero Trust Strategy publicatie, 7 november 2022

DELL Technologies

Geavanceerde Zero Trust

Vertrouwen in de gebruiker

- Op regel gebaseerde dynamische toegang pt. 2
- Bedrijfsrollen en -machtigingen Pt. 1
- Alternatieve flexibele MFA pt. 1
- Real-time Goedkeuringen en JIT/ JEA analyse pt. 1
- Levenscyclusbeheer bedrijfsidentiteit pt. 2
- Controle op gebruikersactiviteiten pt. 1
- Continue verificatie pt. 1
- Continue verificatie pt. 2
- Enterprise PKI/IDP pt. 3
- Bedrijfsrollen en -machtigingen Pt. 2
- Alternatieve flexibele MFA pt. 2
- Real-time Goedkeuringen en JIT/ JEA analyse pt. 2
- Levenscyclusbeheer bedrijfsidentiteit pt. 3
- Controle op gebruikersactiviteiten pt. 2
- Enterprise PKI/IDP pt. 2

Vertrouwen in apparaten

- Enterprise IDP pt. 2
- Implementatie van C2C/ Compliance Based Network Authorization Pt. 2
- Controle op entiteitsactiviteiten pt. 1
- Volledig integreren van Slack apparaatbeveiliging met C2C
- Enterprise PKI pt. 1
- Beheerd en Volledige BYOD- en IOT-ondersteuning pt. 1
- XDR-tools implementeren en integreren met C2C pt. 2
- Controle op entiteitsactiviteiten pt. 2
- Enterprise PKI pt. 2
- Beheerd en volledige BYOD- en IOT-ondersteuning pt. 2

Toepassing en workload

- Verrijk attributen voor bronautorisatie pt. 1
- Verrijk attributen voor bronautorisatie pt. 2
- Continue autorisatie om te werken (ATO) pt. 1
- Applicatie automatiseren Security en Code oplossing Pt. 2
- REST API microsegmenten
- Continue autorisatie om te werken (ATO) Pt. 2

Vertrouwen in data

- Handmatig data taggen pt. 2
- Controle op databaseactiviteit
- Geautomatiseerde datataggen en ondersteuning pt. 1
- DRM-handhaving via datatags en analyse pt. 2
- DLP-handhaving via datatags en analyse pt. 2
- Daas-toegang integreren met SDS-beleid pt. 2
- SDS-oplossing(en) en beleid integreren met Enterprise IDP pt. 2
- SOS Tool integreren en/ of integreren met DRM Tool Pt. 1
- Geautomatiseerde Data taggen en ondersteuning pt. 2
- Uitgebreide controle op data-activiteit
- DRM-handhaving via datatags en analyse pt. 3
- DLP-handhaving via datatags en analyse pt. 3
- Daas-toegang integreren met SDS-beleid pt. 3
- SDS Tool integreren en/ of integreren met DRM Tool Pt. 2

Netwerk en omgeving

- Detectie en optimalisatie van netwerkactiva
- Real-time toegangsbeslissingen
- Microsegmentatie van processen

Automatisering en orkestratie

- Beveiligingsprofiel voor ondernemingen pt. 2
- Bedrijfsintegratie en workflowprovisioning pt. 2
- AI-automatiseringstool implementeren
- Workflow verrijking pt. 3
- AI aangedreven door analyses besluit over A&O-wijzigingen
- Playbooks implementeren
- Geautomatiseerde workflows

Zichtbaarheid en analyse

- Bedreigingswaarschuwingen pt. 3
- Basislijn en Profilering pt. 2
- UEBA basisondersteuning pt. 1
- UEBA basisondersteuning pt. 2
- AI ingeschakeld netwerktoegang
- AI-ingeschakelde dynamische toegangscontrole

Totale geavanceerde activiteiten: 61

Dell Technologies kan de complexiteit van het snel bereiken van Zero Trust volwassenheid vereenvoudigen.

Bron: DoD Zero Trust Strategy publicatie, 7 november 2022

DELL Technologies

Voldoen aan de behoeften van alle organisaties.

Laat uw Zero Trust verder groeien.

Zero Trust is een gedefinieerd framework en een reeks principes die bepalen hoe beveiliging moet worden benaderd en die kan worden geïmplementeerd met behulp van verschillende capaciteiten. Dell is een ervaren beveiligingspartner die u kan helpen bij het bevorderen van uw beveiligingstraject, of u nu volledig op Zero Trust vertrouwt of gericht bent op gerichte verbeteringen, die zijn afgestemd op de Zero Trust-principes.

Chemie	Informatie-technologie	Communicatie	Hulpdiensten
Voedsel en Landbouw	Defensie	Gezondheidszorg en volksgezondheid	Productie
Financieel	Nucleaire Reactoren	Commercieel	Overheid
Energie	Transport	Water en afvalwater	Dammen

DELL Technologies

DELL Technologies

Een ervaren technologie- en beveiligingspartner voor het Zero Trust-traject van uw organisatie.

Verbeter cyberbeveiliging op de lange termijn door Zero Trust te implementeren.

Dell Security Services biedt:

Deskundige beoordeling van de groei van de beveiliging en het algehele risico.

Ontwikkeling van een Zero Trust-roadmap.

Doorlopend beheer van beveiligingsactiviteiten.

DELL Technologies

Dell.com/SecuritySolutions

Laat u terugbellen

Chatten met een beveiligingsadviseur

Bel 1-800-433-2393