SupportAssist voor enterprise-systemen

SupportAssist integreert databescherming en risicopreventie tot een beveiligde, geautomatiseerde supportervaring

Tot

85%

van de deelnemers aan het Forrester-onderzoek zijn van plan om meer te investeren in door data gestuurde supporttools en technologieën met AI als basis[1]

Dell Technologies Services is sterk gefocust op de implementatie van beveiligingsfunctionaliteit die zijn gebaseerd op de huidige markt, actuele regelgeving en klantinzichten, zodat onze producten voldoen aan de beveiligingsdoelstellingen en nalevingsvereisten van onze klanten.

Inhoud

1: Inleiding 3

2: SupportAssist voor enterprise-systemen 4

3: Overzicht van beveiligingsarchitectuur 5

4: Gedetailleerde beveiligingsaanpak voor SupportAssist voor enterprise-systemen 6

4-1: Beveiligde onsite-dataverzameling 6

Bekijk hoe SupportAssist functioneert als een veilig communicatiesysteem, waarbij klanten volledige controle houden over autorisatievereisten dankzij verificatieprotocollen met twee factoren en veel meer.

4-2: Beveiligde dataoverdracht en communicatie 9

Leer hoe SupportAssist versleuteling en bilaterale verificatie toepast om een beveiligde TLS-tunnel te creëren voor functies als heartbeat polling, externe meldingen en externe toegang.

4-3: Beveiligde datastorage, gebruik en processen 11

Lees meer over de variëteit aan maatregelen die dagelijks worden geïmplementeerd om uw data veilig te houden, inclusief fysieke beveiliging, risicobeheer van de toeleveringsketen en beveiligde ontwikkelingsprocessen.

5: Conclusie 15

1: Inleiding:

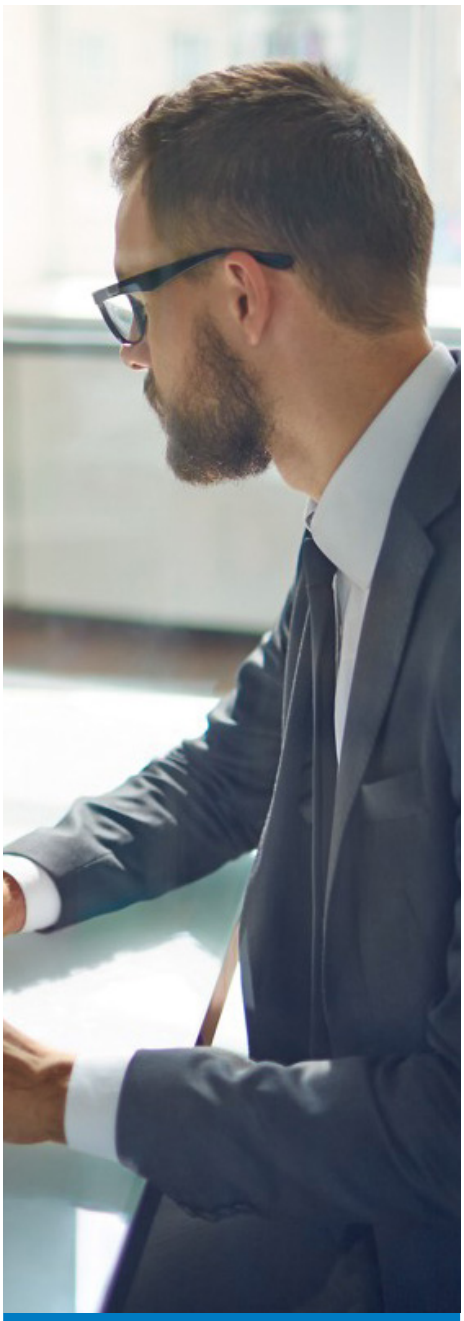
In de hyperdigitale wereld van vandaag richten succesvolle innovatieleiders zich op IT-serviceproviders voor het outsourcen van IT-support. Volgens een onderzoek van Forrester Consulting in opdracht van Dell Technologies Services[1], kunnen bedrijven die in zee gaan met de juiste IT-serviceprovider, tot wel 36% van de tijd van hun IT-personeel richten op innovatie en strategische initiatieven, in plaats van op dagelijkse onderhoudstaken.

Als toonaangevende IT-serviceprovider gaat Dell Technologies Services uiterst zorgvuldig te werk, zodat onze IT-supportservices en technologieën nooit zelf een potentieel beveiligingsrisico kunnen vormen. Elke dag weer doen we er alles aan om dit risico voor onze klanten die in hun bedrijfsomgeving te maken hebben met Dell EMC producten, tot een minimum te beperken. Deze whitepaper laat zien hoe beveiliging is ingebouwd in het ontwerp, de implementatie en de werking van SupportAssist voor enterprise-systemen. Alleen zo kunnen we een veilige en geautomatiseerde IT-supportervaring garanderen voor een complexe datacenterinfrastructuur.

Op basis van meer dan 25 jaar ervaring als pioniers van IT-supporttechnologie is de beveiligingsarchitectuur van SupportAssist speciaal ontworpen om inbreukbedreigingen direct te stoppen en de data-integriteit te beschermen. Met onze technologie kunnen we de apparaten van onze klanten doorlopend controleren op problemen en direct een versnelde herstelprocedure starten. Hierbij geldt bovendien het volgende:

- We gebruiken alleen telemetrie- en gebeurtenisdata van actieve systemen.
- Alle data over de systeemstatus worden versleuteld voordat ze via HTTPS over internet worden verzonden met het TLS-protocol (Transport Layer Security).
- Onze geautoriseerde technische support-engineers passen verificatie met meerdere factoren toe zodat ze problemen op gekoppelde systemen extern kunnen bekijken en oplossen.
- We verwerken, gebruiken en slaan telemetrie- en gebeurtenisdata op onze locaties op met behulp van toonaangevende beveiligingspraktijken in de branche.

Ook worden de beveiligingsmaatregelen die zijn geïntegreerd in de gehele SupportAssist-architectuur en processen rigoureus door ons gecontroleerd. Hierbij maken we gebruik van de diensten van meerdere leidende bedrijven zoals Secureworks, zodat we garant kunnen staan voor een betrouwbare ervaring waarbij alle persoonlijke gegevens veilig zijn afgeschermd.



Cyberaanvallen en datafraude of diefstal staan in de zorgen top vijf van CEO's[2]

2. SupportAssist voor enterprise-systemen

SupportAssist voor enterprise-systemen is een veilige connectiviteitstechnologie die direct zekerheid biedt bij het voorkomen van problemen, zodat u niet meer hoeft te raden waar het probleem ligt, en alle tijd hebt om u te richten op de projecten die er het meest toe doen. De virtuele versie van het apparaat biedt een beveiligde verbinding in twee richtingen tussen uw omgeving en Dell Technologies Services, ideaal voor het centraal controleren van tot wel 4200 apparaten in uw datacenter, waaronder datastorage, servers, networking, CI/HCI en databescherming.

Data is de essentie van SupportAssist. We verzamelen data over de systeemstatus van onze klantomgevingen en correleren die met uitgebreide incident- en engineeringdata van onze teams in het veld en onze technische support-teams, maar ook met data van componentfabrikanten.

Meer informatie over de gedetailleerde systeemstatusinformatie die door SupportAssist wordt verzameld, vindt u hier.

SupportAssist gebruikt geavanceerde AI-modellen, waaronder machine learning, om nauwkeurig patronen te vinden die direct in het herstelproces kunnen worden toegepast. SupportAssist identificeert hardware- en softwareproblemen, opent een case en zorgt ervoor dat wij contact met u opnemen voordat het probleem uit de hand loopt en een kostbare zaak wordt. SupportAssist voorspelt fouten die optreden bij de harde schijfstations van servers en backplanes. Afhankelijk van het type probleem kan de melding ook het startpunt vormen voor het automatisch verzenden van vervangende onderdelen.

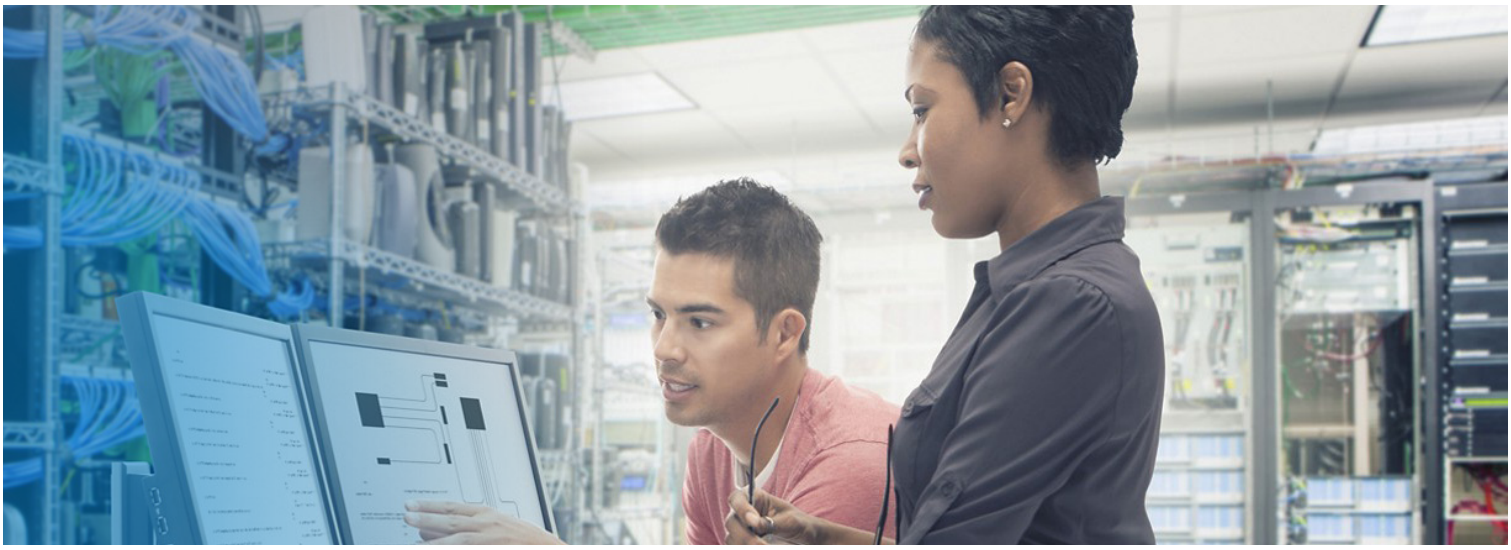
Bovendien biedt de technologie een veilige communicatie in twee richtingen zodat geautoriseerde technische support-agents via externe toegang tot beheerde apparaten kunnen zoeken naar problemen en deze oplossen.

SupportAssist-beveiliging

Beveiligingsbeoordelingen door derden worden regelmatig uitgevoerd op de SupportAssist-applicatie en de ondersteunende infrastructuur.

Applicatiebeoordelingen omvatten dataoverdracht en API-beveiliging, statische en dynamische broncodeanalyse, CVE- en OWASP-controles (respectievelijk Common Vulnerabilities & Exposures en Open Web Application Security Project) en bibliotheken en producten van derden.

Infrastructuurbeoordelingen omvatten interne en externe netwerkapparaten, servers en serviceproviders.



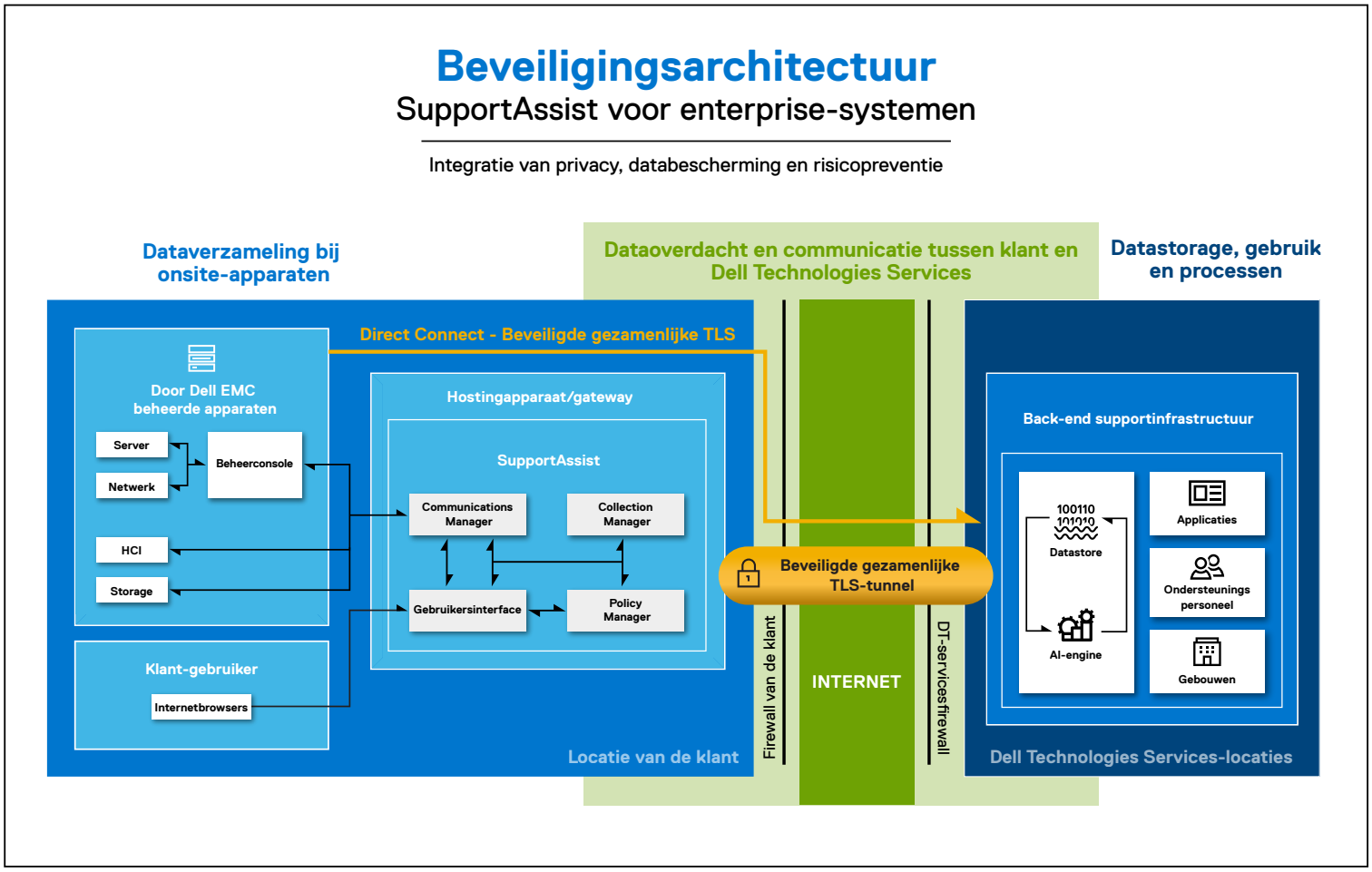
3: Overzicht van beveiligingsarchitectuur

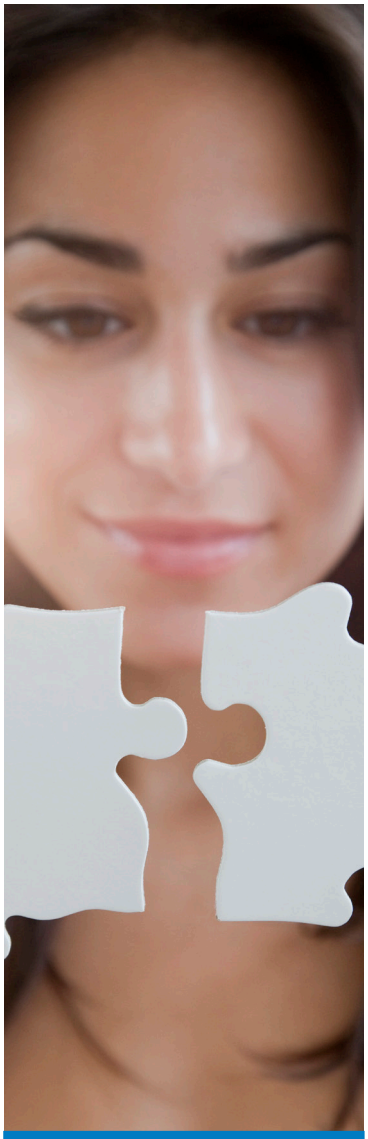
Dell Technologies Services streeft naar het minimaliseren van het aantal risico's op beveiligingsbedreigingen in onze geautomatiseerde, proactieve en voorspellende SupportAssist-technologie. De beveiligingsarchitectuur van SupportAssist voor enterprise-systemen is ontworpen op basis van strikte industriestandaarden en voldoet aan meetbare en herhaalbare beveiligingspraktijken in elke stap van de productontwikkeling en implementatie.

Diagram A hieronder biedt een overzicht van de SupportAssist-beveiligingsarchitectuur. In de volgende secties laten we zien hoe SupportAssist alleen die systeemdata van de door Dell EMC beheerde apparaten ophaalt die nodig zijn voor probleemdiagnose en -herstel, en hoe deze data met de hoogst mogelijke veiligheids- en privacyvereisten worden verwerkt in alle onderstaande stappen:

- Dataverzameling bij onsite-apparaten
- Dataoverdracht en -communicatie
- Datastorage, gebruik en processen bij Dell Technologies Services

Diagram A:





Klanten krijgen een extra beveiligingslaag voor onsite-dataverzameling via de auditfuncties van Policy Manager in SupportAssist

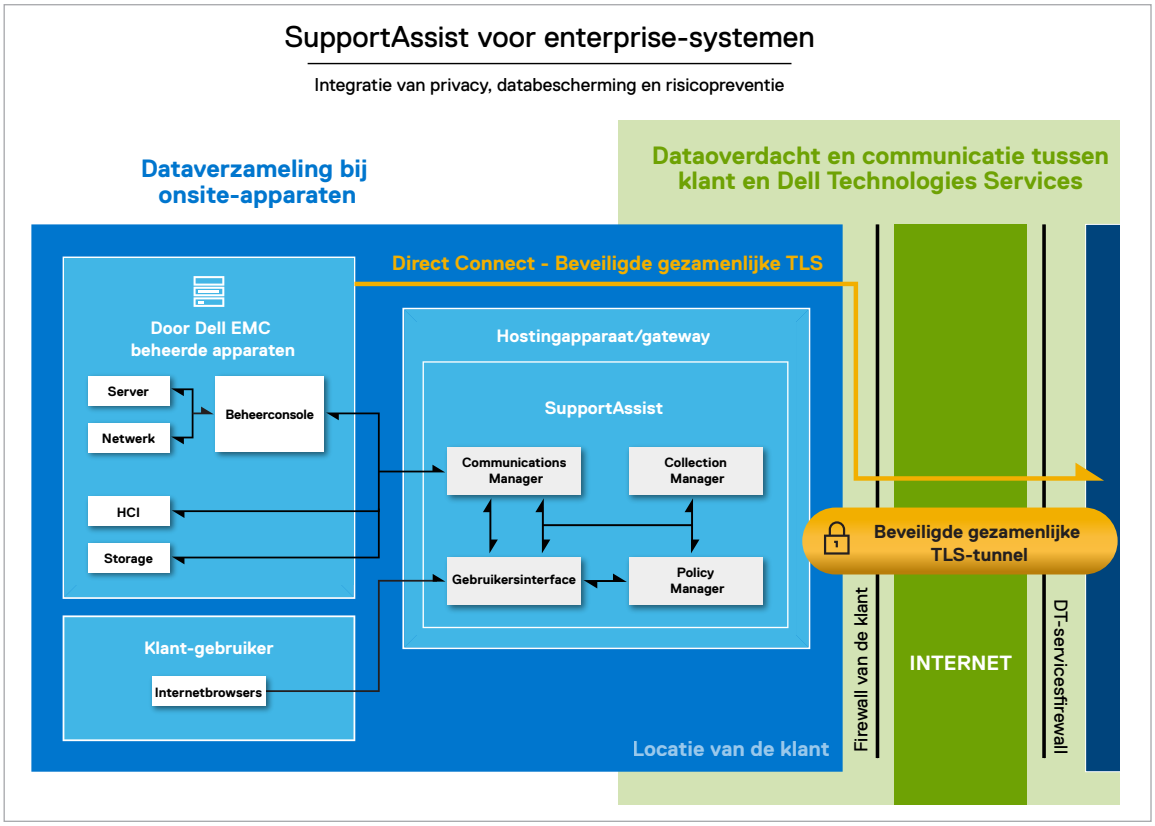
4: Gedetailleerde beveiligingsaanpak voor SupportAssist voor enterprise-systemen

4-1: Beveiligde onsite-dataverzameling

Minimaal aantal access points in firewall

SupportAssist voor enterprise-systemen aggregeert de communicatie tussen Dell EMC apparaten en fungeert als een single access point (zowel ingang als uitgang) in de firewall van de klant voor alle externe IP-serviceactiviteiten. Zie diagram B. Door het aantal access points in de firewall voor externe IT-supporttechnologie te minimaliseren, verlaagt SupportAssist het beveiligingsrisico voor ongewenste toegang via de bedrijfsfirewall.

Diagram B: (Extract van diagram A – Beveiligingsarchitectuur):



Als onsite-gateway, wordt SupportAssist virtueel geïmplementeerd op een hypervisor die door de klant wordt aangeleverd. Elke gatewayserver werkt als een proxy voor het overdragen van informatie van en naar de beheerde apparaten. Bij tijdelijke netwerkfouten kan SupportAssist ook een wachtrij instellen voor gekoppelde thuisgebeurtenissen. Deze gatewayservers beschikken over een eigen webgebruikersinterface dat is gebaseerd op het onderliggende besturingssysteem.

Voor sommige klanten is de Direct Connect-versie ideaal geschikt voor de heterogene implementatie van meerdere hardwareproducten van Dell EMC. Deze oplossing vormt dan één enkel beveiligd communicatiepunt via de firewall van de klant, volledig geïntegreerd in de besturingsomgeving van het product. Zo is er ook geen noodzaak voor een afzonderlijke server die inkomende externe support en een Call Home-functie zou moeten bieden.

Een veilig communicatiemiddel

SupportAssist fungeert als communicatiemiddel tussen beheerde apparaten, de Policy Manager en de back-end supportinfrastructuur van Dell Technologies Services. De gatewayservers waarop het systeem is geïmplementeerd zijn feitelijk HTTPS-handlers. SupportAssist maakt optimaal gebruik van meerdere communicatiemethoden waaronder apparaatdetectie, gebeurtenisbeheer en de verzameling en het beheer van telemetriedata. De volgende berichttypen zijn mogelijk:

- "Heartbeat polling" voor status van apparaat
- Overdracht van databestanden (thuisverbinding)
- Overdracht van data over licentiegebruik
- Verzoeken voor gebruikersverificatie
- Synchronisatie van apparaatbeheer

Alle berichten zijn veilig versleuteld met standaardapplicatieprotocollen. In een van de volgende secties kijken we in meer detail naar de extra beveiliging die is ingebouwd in de SupportAssist-functies voor datacommunicatie en -transport, waaronder het gebruik van het HTTPS-protocol met end-to-end TLS-tunneling (Transport Layer Security) en versleuteling via industrienormen.

Klantcontrole over autorisatievereisten en toegangsrechten

Als apparaten worden gecontroleerd door SupportAssist in het datacenter van een klant, kan de klant desgewenst Policy Manager gebruiken om de autorisatievereisten voor externe toegangsverbindingen te controleren, naast de uitvoering van diagnostische scripts en andere bijbehorende activiteiten. Ook kan de klant toegangsrechten instellen voor personeel en technische support-engineers die zich extern aanmelden voor diagnose en probleemoplossing.

De beveiliging voor autorisatie- en rechtenbeheer wordt gegarandeerd door de volgende functies van Policy Manager:

- SupportAssist pollt de Policy Manager regelmatig voor wijzigingen met betrekking tot de rechten en slaat de rechten lokaal op in een cachegeheugen. In het geval van Policy Manager geldt het volgende:
  - De regelsetcache wordt automatisch bijgewerkt met configuratie-updates na de laatste pollingcyclus.
  - De cache wordt als HTTPS-listener geconfigureerd voor het ontvangen van berichten op een specifieke, vooraf geaccordeerde poort.
- Wanneer SupportAssist een extern toegangsverzoek of een andere actie ontvangt, dwingt het het beleid af dat SupportAssist heeft gekregen vanuit de Policy Manager-cache.
  - De rechten van Policy Manager kunnen hiërarchisch worden toegewezen met beleid dat is gebaseerd op apparaattypen of specifieke modellen binnen een apparaattype.
  - Klanten kunnen de verzochte actie accepteren of afwijzen via de webgebruikersinterface van Policy Manager. Met behulp van filters kunnen ze ook verdere beperkingen voor autorisatie en acties instellen.

Logboeken en audittrails

Klanten beschikken over een toegevoegde beveiligingslaag voor onsite-dataverzameling via de controlefuncties van Policy Manager in SupportAssist. Policy Manager legt alle externe servicegebeurtenissen en verbindingen vast, samen met alle diagnostische scriptuitvoeringen en overdrachtsbewerkingen van supportbestanden. Deze worden vervolgens opgeslagen in de Policy Manager-database als niet-opgemaakte auditlogboeken (als tekstindeling). De Policy Manager houdt ook bij wanneer er toegang is gevraagd voor de Policy Manager zelf, alsook beleidswijzigingen en alle autorisaties of afwijzingen van toegangsactiviteiten.

Deze informatie is direct en altijd beschikbaar voor de klant:

- Audits kunnen worden ingezien via de webgebruikersinterface van Policy Manager. Deze kunnen niet worden bewerkt.
- Auditlogboeken kunnen worden geconfigureerd voor streaming naar een syslog-server in hun omgeving.

Beveiligingsoptie via apparaatcontrole

Aangezien klanten niet altijd de Policy Manager inschakelen voor autorisatie- en rechtenbeheer, biedt SupportAssist een aantal verwante functies via de apparaatcontroleoptie.

Klanten kunnen het volgende uitvoeren:

- Aangepaste groepen maken op basis van apparaattype, beheerdersgroep, organisatie- of bedrijfseenheid, fysieke locatie van het apparaat of elke ander gekozen criterium
- Specifieke machtigingen en toegangsrechten definiëren op basis van deze apparaatgroepen

Alle bewerkingen voor apparaatbeheer worden vastgelegd, en dat is inclusief externe activiteiten van technische support-engineers. Deze moeten ook in de back-end worden goedgekeurd door een technische support-agent.

Op deze manier behouden klanten de volledige controle en transparantie over de apparaten die via SupportAssist worden beheerd.

Verificatie met twee factoren en beheer van digitale certificaten

Verificatie vormt een belangrijke onderdeel van het beveiligde onsite-dataverzamelingsproces. SupportAssist gebruikt een digitaal certificaat als identificatiemiddel bij de implementatie op de gatewayserver van de klant. Het certificaat bindt de identiteit van de gatewayserver aan een sleutelpaar waardoor alle communicatie met de back-end wordt versleuteld en geverifieerd. Dell Technologies Services' Certificate Authority (CA) is de centrale opslaglocatie voor de SupportAssist-sleutelinfrastructuur.

Door beheer van digitale certificaten kan de ingebruikname van het digitale certificaat worden geautomatiseerd via onze privécertificeringsinstantie. Met de volgende mogelijkheden als gevolg:

- Mogelijkheid tot programmatisch aanmaken en verifiëren van elk certificaatverzoek.
- Garantie dat het certificaat alleen is uitgegeven voor en geïnstalleerd op de gatewayserver. Het certificaat kan niet worden gekopieerd of gebruikt op een andere machine.

SupportAssist maakt en verifieert verbindingen via het digitale certificaat dat is geïmplementeerd op onze back-endsupportinfrastructuur. Technische support-agents koppelen SupportAssist in de klantomgeving door middel van een verificatieproces met twee factoren.

4-2: Beveiligde dataoverdracht en communicatie

Beveiligde communicatietunnel

Alle communicatie tussen de klant en de back-endsupportinfrastructuur van Dell Technologies Services wordt op uitgaande basis gestart door SupportAssist vanaf de locatie van de klant. Hiervoor wordt een beveiligde secure end-to-end communicatietunnel gemaakt met gebruik van een TLS-internetverbinding met 256-bits versleuteling conform de industrienormen, naast verificatie met een digitaal certificaat dat is ondertekend door Dell Technologies Services. Dit laatste wordt uitvoerig besproken in de voorgaande sectie over beveiligde onsite-dataverzameling.

Als gevolg hiervan beschikken SupportAssist-verbindingen over de volgende eigenschappen:

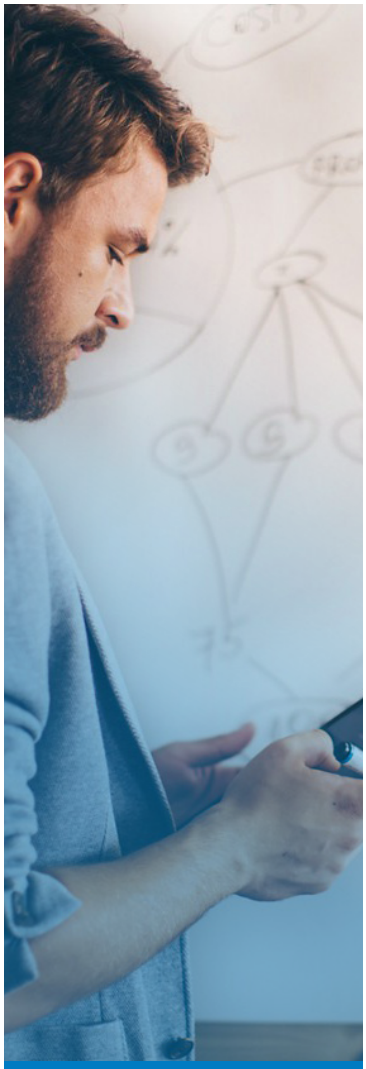
- **Betrouwbare dataoverdracht:** Elk bericht dat wordt verzonden, bevat een integriteitscontrole via een berichtverificatiecode. Dit voorkomt dat een bericht ongezien verloren gaat of dat data tijdens de overdracht worden gewijzigd.
- **Privé en beveiligde sessie via TLS:** via symmetrische versleuteling met algoritmen conform de industrienormen worden unieke sleutels gegenereerd voor elke verbinding. De communicatiewijze kan tijdens de onderhandelingen niet worden gewijzigd zonder dat dit wordt gedetecteerd.
- **Geverifieerde partijen:** aangezien het om een beveiligde verbinding gaat, worden de communicerende partijen geïdentificeerd en geverifieerd via cryptografie met openbare sleutels. Zo worden spoofing en man-in-the-middle (MITM)-aanvallen voorkomen.

Communicatie via de beveiligde TLS-tunnel

De gatewayserver gebruikt de TLS-tunnel om een beveiligde omgeving te garanderen voor de volgende functies: heartbeat polling, externe meldingen en externe toegang. In deze sectie en diagram C gaan we dieper in om deze basiscommunicatieprocessen en protocollen voor de geautomatiseerde, proactieve en voorspellende gebruikerservaringen van SupportAssist.

“Heartbeat-polling”

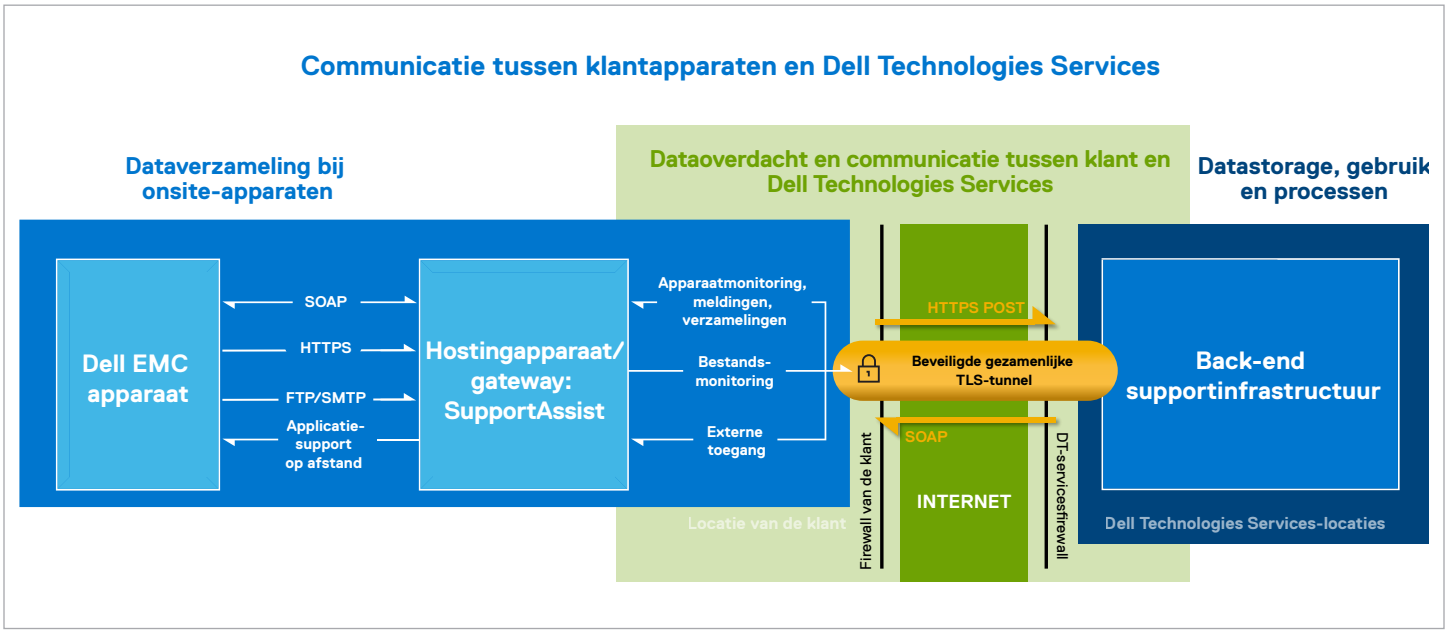
Voor een optimale werking van SupportAssist moeten klantsystemen gekoppeld zijn. Met heartbeat-polling wordt de connectiviteitsstatus van apparaten getest en worden telemetriedata regelmatig doorgegeven aan de back-end. Met de data wordt ook de gatewayserver geïdentificeerd waarop SupportAssist wordt geïmplementeerd. Bovendien kan heartbeat-polling worden gebruikt om bestanden over te dragen naar de back-end.



Door toonaangevende verificatie in de branche worden verbindingen beveiligd tegen spoofing en “man-in-the-middle”-aanvallen

Communicatie via de beveiligde TLS-tunnel (vervolg)

Diagram C: Beveiligingsarchitectuur



Externe meldingen of Connect Home-functie

SupportAssist dient als een beveiligde toegangspassage voor apparaten om hun gebeurtenisbestanden naar de back-end te sturen. Hieronder vallen foutmeldingen, voorwaarden voor waarschuwingen, prestatierapporten, configuratiedata en de status van scriptuitvoeringen.

- Met elke melding wordt ook een gebeurtenisbestand gegenereerd en verzonden naar SupportAssist.
- Het bestand ontvangen door SupportAssist ontvangen via de HTTPS-listenerservices.
- Bij verouderde producten die FTP en/of SMTP-listeners gebruiken voor SupportAssist, worden de bestanden versleuteld voor overdracht.
- SupportAssist comprimeert het bestand en stuurt het via de TLS-tunnel naar de back-end. Hierna wordt het bestand verwijderd uit de listener-directory.
- Tot slot wordt het bestand in de back-end gedecomprimeerd voor analyse.
- SupportAssist kan de bestanden ook via de versleutelde communicatietunnel versturen naar de back-end. Bovendien kan SupportAssist worden geconfigureerd voor gebruik van de failover-kanalen, namelijk FTPS of de e-mailserver van de klant.

Data over systeemcontrole worden van meerdere componenten van het actieve systeem verzameld, zodat Dell Technologies Services adaptief, slim en versneld support kan bieden. De systeem-id, nodig om het specifieke systeem dat in behandeling is te identificeren, is de enige informatie over het bedrijf dat van apparaten wordt opgehaald. Wanneer SupportAssist bepaalt dat er proactief een vervangend onderdeel moet worden verzonden, gebruiken we hiervoor bestaande contactgegevens die veilig zijn opgeslagen op Dell Technologies servers.

De volledige lijst met systeemcontroledata die van een actief systeem worden verzameld (inclusief data die worden verzameld buiten de routinecyclus van 24 uur), is hier beschikbaar.

Externe toegang

Onze technische supportteams hebben ook externe toegang tot de apparaten op de locatie van de klant om problemen op te lossen of apparaatspecifieke handelingen uit te voeren. Via asynchrone messaging wordt gegarandeerd dat de externe toegangssessie door SupportAssist wordt gestart vanaf de klantlocatie. Hierna kan als volgt een beveiligde toegangssessie worden ingesteld:

- Nadat de sessie is geverifieerd op de Dell Technologies Services back-end, wordt door een technische support-agent een toegangsverzoek tot een apparaat ingediend in combinatie met een serviceverzoeknummer (indien beschikbaar) en andere id's voor het apparaat of de gebruiker.
- Het externe toegangsverzoek wordt in een wachtrij op de back-end geplaatst totdat SupportAssist een heartbeat-melding van het apparaat naar de back-end stuurt voor ophalen.
- Als reactie stuurt de back-endserver een bericht met informatie over het verzoek, het adres van de back-endserver en een unieke sessie-id om verbinding te maken met SupportAssist.
- SupportAssist gebruikt zijn lokale opslaglocatie om het lokale IP-adres van het apparaat vast te stellen. Vervolgens wordt het cachebeleid van Policy Manager gecontroleerd op de verbindingsrechten.
- Indien toegestaan zorgt SupportAssist voor een afzonderlijke, permanente TLS-verbinding met de back-endserver.

Communicatie vindt plaats via de tunnel tussen SupportAssist en de back-endserver totdat de sessie wordt beëindigd of er een time-out is na een periode van inactiviteit.

Netwerkbeveiliging

Alle componenten voor netwerkcontrole bevinden zich achter een firewall en worden beheerd door ons netwerkbeveiligingsteam. Netwerkverkeer wordt strikt gecontroleerd. De overdracht van al het binnenkomend verkeer gebeurt via specifieke poorten en gaat alleen naar de daartoe aangewezen adressen van het doelnetwerk.

4-3: Beveiligde datastorage, gebruik en processen

Beveiliging voor storage en gebruik

Fysieke beveiliging

Dell Technologies Services fungeert als host voor de meeste SupportAssist-data, inclusief applicaties, systemen, netwerk- en beveiligingsonderdelen. Het datacenter bevindt zich in de Verenigde Staten en is speciaal ontworpen voor een uitermate hoog niveau van beschikbaarheid en beveiliging. De SupportAssist-data worden beschermd door een groot aantal verschillende maatregelen, zoals fysieke beveiliging en onder meer de volgende kenmerken:

- Bewakers on-premise
- Camera's
- Valse toegangspoorten
- Blokkades voor voertuigen
- Speciaal ontworpen parking
- Kogelvrij glas en kogelvrije muren
- Gebruik van regulier uitziende gebouwen

De toegang tot datacenters met systeeminfrastructuur wordt beperkt tot geautoriseerd personeel. Toegangscontrole via smartcard.

Logistieke beveiliging

De door SupportAssist gegenereerde data worden opgeslagen volgens het Dell privacybeleid.

De logische toegang tot de Dell Technologies Services infrastructuur (servers, loadbalancers, netwerkshares, etc.) wordt beperkt door interne tools die conform de IT-richtlijnen worden gecontroleerd en geëvalueerd:

Logistieke beveiliging (vervolg)

- **Server- en databasebeveiliging:** Onderdelen van servers en besturingssystemen staan op standaardimages die zijn gecontroleerd op beveiligingsaspecten. Er zijn regelmatige controles van beveiligingsupdates die door de applicatie worden gebruikt, inclusief updates die zijn uitgebracht door Microsoft en andere softwareleveranciers. Wanneer essentiële beveiligingsupdates worden uitgebracht, worden deze eerst getest op niet-productie-images en dan tijdig en algemeen toegepast op live servers om risico's te vermijden.
- **Audits:** Controlelogboeken voor apparaten worden onderhouden en zijn eigendom van en alleen toegankelijk door Dell Technologies Services. In deze logboeken worden alle pogingen voor aanmelden of om toegang te krijgen tot het besturingssysteem of de webserverconsole van SupportAssist opgenomen.

Door IT-beheerde builds worden versterkt met CIS-aanbevelingen (Center for Internet Security). Ook worden industrienormen en richtlijnen op het gebied van beveiliging geïmplementeerd op alle servers en netwerkapparatuur.

Tot slot maakt het SupportAssist-ecosysteem gebruik van zowel lokale hoge beschikbaarheid in het eigen datacenter als van een identieke infrastructuur in een afzonderlijk datacenter. De enige uitzonderingen hierop vormen technologieën die intrinsiek hoog beschikbaar zijn, zoals big data-clusters en private clouds. Voor data-analytics gebruikt Dell Technologies Services cloudomgevingen die we volledig zelf controleren en beheren, inclusief private, hybride en public clouds.

Verificatie

SupportAssist gebruikt Dell MyAccount voor verificatie bij Dell Technologies Services en OS-aanmeldingsgroepen voor “on-the-box”-verificatie.

Aan groepen die toegang hebben tot SupportAssist-componenten, zoals het databasebeheerteam en het operationele supportteam, worden afzonderlijke toegangsrechten en plichten toegewezen. Alle updates voor de productieomgeving doorlopen een duidelijk beschreven wijzigingscontroleproces waarin de benodigde controles en maatregelen zijn opgenomen.

Beveiliging voor processen

Community bewust van het belang van beveiliging

We bieden een op rollen gebaseerd trainingscurriculum om nieuwe en bestaande werknemers te informeren over de best practices voor beveiliging op basis van hun functie, en hoe ze relevante resources kunnen gebruiken. Dell Technologies streeft naar een cultuur waarin het belang van beveiliging in de gehele community wordt gedeeld.

Ontwikkeling

Onze interne **SDL-standaard (Secure Development Lifecycle Standard)** vormt een algemeen referentiekader voor Dell Technologies productorganisaties voor de benchmarking van onze ontwikkelingsactiviteiten voor de beveiliging van producten en applicaties, zodat deze conformeren aan de verwachtingen in de markt en de praktijken in de branche. De SDL-standaard definieert beveiligingscontroles waaraan productteams zich dienen te houden bij de ontwikkeling van nieuwe kenmerken en functionaliteit. SDL bevat zowel analyseactiviteiten als voorspellende proactieve controles voor belangrijke risicogebieden. De analyseactiviteiten, zoals bedreigingsmodellering, statische codeanalyse, en het scannen en testen op beveiliging, zijn bedoeld om kwetsbare beveiligingsplekken in de volledige ontwikkelingscyclus te ontdekken en op te lossen. De voorspellende controles vormen een garantie dat ontwikkelingsteams defensief coderen om bepaalde veel voorkomende beveiligingsproblemen te voorkomen, zoals problemen die zijn opgenomen in de top 10 van het OWASP (Open Web Application Security Project) of de top 25 van SANS.

We gebruiken een herhaalbaar en beveiligd ontwikkellings-proces voor producten en applicaties

Ontwikkeling (vervolg)

De SupportAssist-code is ontworpen volgende Agile-ontwikkelingsmethodiek waarbij code continu wordt geïntegreerd op basis van automatiseringssoftware die voldoet aan de industrienormen. Codeversies worden ingecheckt en gecontroleerd via beveiligde groepsmachtigingen.

Elke softwarerelease ondergaat een beveiligingscheck die in lijn ligt met ons beveiligingsbeleid en die de volgende punten omvat:

- Beoordeling van kwetsbaarheden met behulp van penetratietesten
- Testen op beveiliging door meerdere externe "best-in-class"-leveranciers zoals Secureworks
- Beoordeling van oplossingen voor verificatie, autorisatie en identiteitsbeheer
- Controle en goedkeuring van opensourcebibliotheken door ons juridisch team
- Dataclassificatie met onze Global Security-organisatie. Dit proces combineert privacy- en beveiligingsaspecten met als resultaat de bescherming van elektronische data.

Applicaties worden gecontroleerd op beveiliging en governance.

Wijzigingsbeheer

Het wijzigingsbeheerproces van Dell Technologies volgt de best practises van de ITIL Foundation, zoals voorgeschreven door de bestuurders in ons Corporate Change Management Board. Alle wijzigingen worden beheerd via aanvraagtickets. Iedereen die ons systeem gebruikt om wijzigingen aan te vragen ondergaat verplicht ITIL-training en dient bekend te zijn met de SDL-standaard. Voor alle updates en upgrades die worden toegepast op de back-endinfrastructuur is versiebeheer actief zodat wijzigingen correct kunnen worden gevolg en bijgehouden. Het team gebruikt een geautomatiseerd build-proces om nieuwe builds toe te passen of om builds of hot-fixes die al zijn geïmplementeerd, indien nodig, terug te rollen.

De applicatie die op de klantlocatie is geïnstalleerd kan worden geüpgraded indien de klant dit wenst. Elke release die beschikbaar is op Dell.com/support bevat informatie over nieuwe wijzigingen en eventuele beperkingen die op dat moment bekend zijn.

Alle nieuwe functies en wijzigingen worden uitvoerig gecontroleerd door ons productmanagementteam en geprioriteerd volgens een POR-wijzigingsproces (plan-of-record) waarbij controle en goedkeuring door de Change Control Board en essentieel onderdeel is.

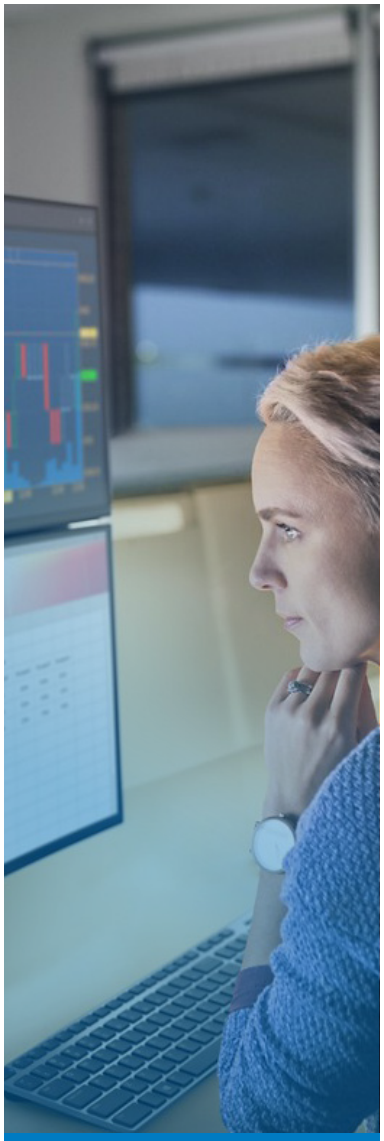
Risicobeheer van toeleveringsketen

Dell Technologies volgt de toonaangevende best practices voor onze branche in elke fase van de "plannen-sourcen-maken-leveren-retourneren"-levenscyclus. We streven een alomvattende aanpak na bij de beveiliging van onze toeleveringsketen, zoals de toepassing van internationale SCRM-standaarden en best practices. Alleen zo behouden we onze reputatie als een betrouwbare en vertrouwde ICT-leverancier op de wereldmarkt.

Meer informatie over onze Supply Chain Assurance-praktijken vindt u hier.

Incidentenrapportage

Iedereen bij Dell Technologies die een verdachte activiteit ontdekt of meent dat er sprake is van een cybersecurityprobleem of bedreiging, is verplicht om het incident direct te rapporteren aan ons Security Response Center (SRC). Hierbij gaat het bijvoorbeeld om een kwetsbaarheid of hiaat in een beveiligingsproces die een impact heeft op onze omgeving of die kan leiden tot een systeem- en/of datalek. Het SRC start vervolgens een volledig onderzoek naar het incident en de persoon die het incident heeft gerapporteerd, verstrekt alle benodigde artefacten en details, zodat het SRC het onderzoek correct kan uitvoeren. Het SRC en cybersecurityorganisaties bieden hun klanten inzage in het rapport en de details van het lek, afhankelijk van de ernst van het incident en de aard van het lek.



Industriële samenwerking over de best practices voor product-beveiliging

Respons bij kwetsbaarheden

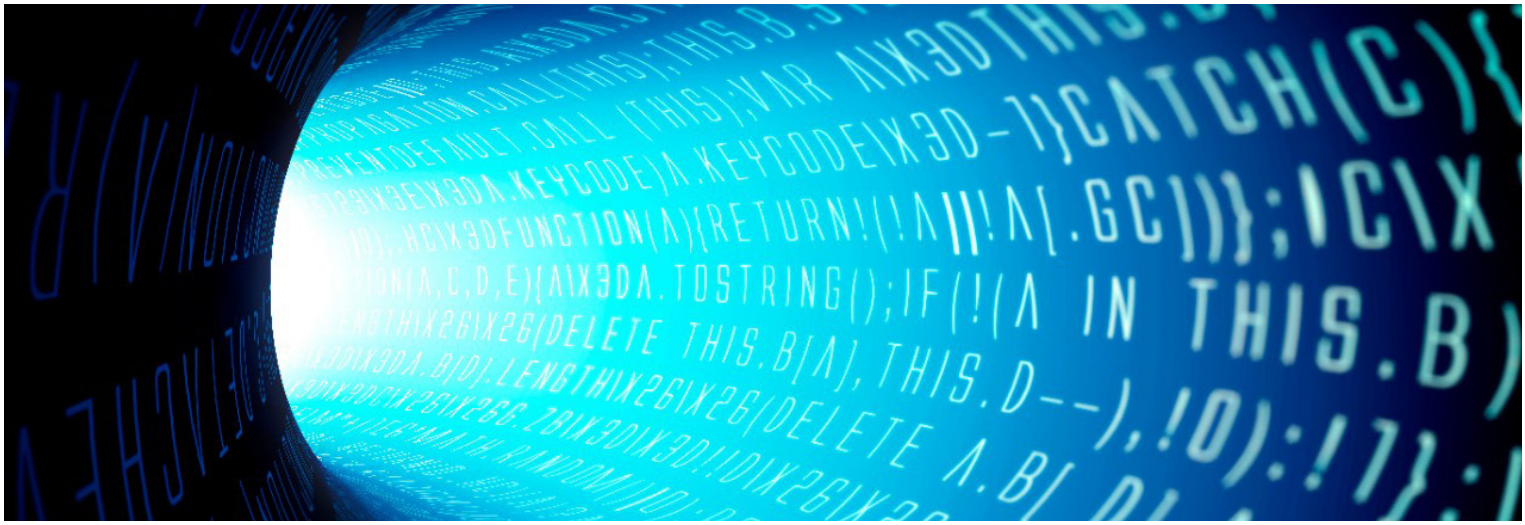
Dell Technologies streeft ernaar om onze klanten zo goed mogelijk te helpen bij het minimaliseren van risico's en kwetsbaarheden ten aanzien van onze productbeveiliging. Daarom bieden we klanten tijdige informatie, richtlijnen en opties voor risicobeperking om bedreigingen door kwetsbaarheden aan te pakken. Ons PSIRT-team (Product Security Incident Response Team) is verantwoordelijk voor de coördinatie van deze respons en voor het openbaar maken van alle productkwetsbaarheden die aan ons worden gerapporteerd.

Meer informatie over ons Vulnerability Response-beleid

Samenwerking in de branche

Dell Technologies neemt samen met andere toonaangevende leveranciers deel aan een aantal samenwerkingsinitiatieven in de branche met het oog op het definiëren, uitwerken en delen van de best practices voor productbeveiliging, en om de veilige ontwikkeling van producten vooruit te helpen. Voorbeelden van deze samenwerking zijn onder meer:

- Via onze EMC-entiteit is Dell medeoprichter en momenteel voorzitter van de Board of Directors van The Software Assurance Forum for Excellence in Code (SAFECode). Overige raadsleden zijn vertegenwoordigers van Microsoft, Adobe, SAP, Intel, Siemens, CA en Symantec. Leden van SAFECode delen en publiceren informatie over de beste praktijken en training voor de kwaliteitsborging voor software.
- Dell Technologies is actief lid van het Forum for Incident Response and Security Teams (FIRST). FIRST is een toonaangevende organisatie en erkend wereldwijd leider in de aanpak van incidenten en kwetsbaarheden.
- We nemen actief deel in het Open Group Trusted Technology Forum (OTTF). OTTF leidt de ontwikkeling van een wereldwijd integriteitsprogramma en framework voor de toeleveringsketen.
- Dell was in 2008 een van de eerste 9 bedrijven die werden beoordeeld door het Building Security In Maturity Model-project (BSIMM) en is sindsdien actief deelnemer in het project. Een Dell Technologies vertegenwoordiger is lid van de BSIMM Board of Advisors.
- Dell werknemers waren medeoprichters van het IEEE Center for Secure Design, dat werd gestart als onderdeel van het IEEE-initiatief voor cybersecurity om softwarearchitecten meer inzicht te bieden in veel voorkomende ontwerpfouten ten aanzien van beveiliging en om deze fouten te voorkomen.



Industrienormen voor beveiliging

Onze werknemers zijn actief betrokken bij instanties voor standaarden en bij industriële consortiums die zich richten op het ontwerp van beveiligingsstandaarden en de definitie van beveiligingspraktijken in de gehele branche, waaronder de volgende:

- Cloud Security Alliance (CSA)
- Distributed Management Task Force (DMTF)
- Forum for Incident Response and Security Teams (FIRST)
- International Committee for Information Technology Standards (INCITS)
- Internationale Organisatie voor Standaardisatie (ISO)
- Internet Engineering Task Force (IETF)
- The Open Group
- Organization for the Advancement of Structured Information Standards (OASIS)
- Software Assurance Forum for Excellence in Code (SAFECode)
- Storage Networking Industry Association (SNIA)

ISO 9001-certificering

Dell Technologies is gecertificeerd voor ISO 9001. Het bedrijf voert elk kwartaal vaste audits en nalavingsbeoordelingen uit voor alle ontwikkelings- en productiecenters.

5: Conclusie

SupportAssist voor enterprise-systemen biedt moeiteloze IT-support met geautomatiseerde proactieve en voorspellende meldingen waardoor maximale uptime voor essentiële datacenterinfrastructuur gegarandeerd is. Klanten die kiezen voor Dell Technologies Services kunnen zeker zijn van onze betrokkenheid bij het bieden van een betrouwbare, privacygevoelige en veilige ervaring bij de collectie, communicatie, overdracht, gebruik en storage van hun telemetriedata.

Voor vragen en meer informatie gaat u naar **DellTechnologies.com/SupportAssist**

1 Bron: "Innovation Leaders Need IT Services To Drive Transformative Outcomes"-onderzoek uitgevoerd door Forrester Consulting namens Dell EMC, oktober 2018.

2 Bron: World Economic Forum Global Risks Report 2019. http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

April 2020 | SupportAssist Enterprise Security-whitepaper