

// WHITEPAPER

AI is niet het probleem.

Waarom de meeste organisaties
vastlopen op infrastructuur,
security en governance

Inzichten uit de Cisco AI Readiness Index

Inhoudsopgave

03

Inleiding

De demo draait. En wat nu?

04

Hoofdstuk 1

Iedereen wil AI. Slechts een kleine minderheid is er klaar voor.

06

Hoofdstuk 2

AI is niet het probleem, de funding wel.

08

Hoofdstuk 3

AI Infrastructure Debt

10

Hoofdstuk 4

Security: van kostenpost naar voorwaarde voor innovatie

11

Hoofdstuk 5

Waarom dit nu urgent is

14

Hoofdstuk 6

Wat de 13% succesvolle organisaties anders doen

16

Checklist

Hoe AI-ready is jouw organisatie?

Inleiding

De demo draait. En nu?

AI staat inmiddels hoog op de strategische agenda van vrijwel iedere organisatie. Budgetten worden vrijgemaakt. Pilots worden gestart. Bestuurders spreken vol overtuiging over de transformatieve kracht van AI. Tegelijkertijd blijkt dat veel organisaties moeite hebben om AI echt onderdeel te maken van hun dagelijkse operatie.

Dat ligt meestal niet aan de AI-tool zelf.

In de praktijk lopen organisaties vast op iets veel fundamentele: de kwaliteit van hun IT-omgeving. Denk aan verouderde infrastructuur, versnipperde data, beperkte zichtbaarheid, onvoldoende grip op identiteiten en toegangsrechten of een gebrek aan duidelijke governance. AI maakt die tekortkomingen niet groter, maar wel veel zichtbaarder.

Bij Avit herkennen we dit beeld. Al meer dan twintig jaar helpen we organisaties hun digitale omgeving toekomstbestendig te maken. Daarbij zien we dat organisaties met een solide basis nieuwe technologie sneller en veiliger kunnen inzetten. AI is in eerste plaats een **stresstest** voor de digitale fundering die er al lag. Organisaties waarbij die basis minder sterk is, lopen vroeg of laat tegen dezelfde vraagstukken aan rondom security, beheer en compliance.

Die praktijkervaring sluit naadloos aan op de uitkomsten van de Cisco AI Readiness Index 2025. Uit onderzoek onder ruim 8.000 zakelijke beslissers wereldwijd blijkt dat slechts **13%** van de organisaties klaar is om AI succesvol op schaal toe te passen. De overige 87% investeert wel in AI, maar mist de fundering om die investeringen duurzaam te laten renderen.

In deze whitepaper vertalen we de belangrijkste inzichten uit het onderzoek naar de dagelijkse praktijk. Wat doet de succesvolle 13% structureel anders? Welk risico bouwt de rest op? En welke keuzes helpen om een sterke basis te leggen voor een toekomstbestendig netwerk?

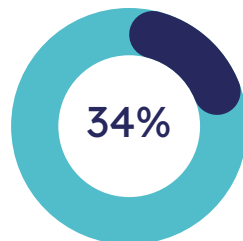
Hoofdstuk 1

Iedereen wil AI. Slechts een kleine minderheid is er klaar voor.

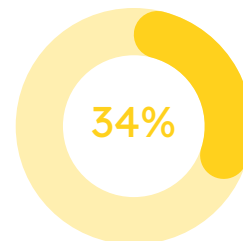
AI is in korte tijd uitgegroeid van experimentele technologie naar strategische prioriteit. Van klantenservice en softwareontwikkeling tot security, procesautomatisering en kennisdeling: de mogelijkheden lijken eindeloos en de verwachtingen zijn hoog. De realiteit blijkt weerbarstig.



klaar voor AI op schaal



infrastructuur AI-ready



data voldoende voorbereid



governance op orde

Bron: Cisco AI Readiness Report, 2025

Deze cijfers laten zien dat een **AI-strategie hebben** en **AI-ready zijn** twee verschillende dingen zijn.

Veel organisaties weten welke rol AI kan spelen binnen hun bedrijfsvoering. Veel minder organisaties beschikken over de technische en organisatorische voorwaarden om AI veilig, beheersbaar en schaalbaar in te zetten. Het verschil tussen die twee is wat de 13% succesvolle organisaties onderscheidt van de rest.

De vraag voor IT-leiders verschuift daarmee fundamenteel.

Niet langer "**welke AI-tool zetten we in?**",
maar "**is onze organisatie klaar om die
tool te ondersteunen?**"

Hoofdstuk 2

AI is niet het probleem, de fundering wel.

De eerste stappen met AI zijn vaak snel gezet. Een pilot met Microsoft Copilot, een AI-chatbot voor de klantenservice of een toepassing die documenten samenvat. De technologie werkt, de eerste resultaten zijn veelbelovend en de belangstelling groeit. Pas wanneer organisaties AI breder willen inzetten, wordt duidelijk wat daarvoor nodig is.

AI draait op data. Het vraagt om betrouwbare toegang tot systemen, voldoende netwerkcapaciteit en duidelijke afspraken over wie welke informatie mag gebruiken. AI legt bloot wat organisaties jarenlang hebben uitgesteld: problemen rondom datakwaliteit, toegangsbeheer, zichtbaarheid en security.



Hoofdstuk 2

AI is niet het probleem, de fundering wel.

Dat leidt tot herkenbare vragen.

Mag een AI-assistent toegang krijgen tot SharePoint?

Welke documenten mogen worden gebruikt?

Hoe voorkom je dat vertrouwelijke informatie beschikbaar komt voor medewerkers die daar geen toegang toe horen te hebben?

En hoe blijven we compliant?

Dit zijn geen nieuwe vraagstukken. Ze bestonden al voordat AI zijn intrede deed. Het verschil is dat AI ze niet langer op de achtergrond laat bestaan. Dit creëert spanning tussen ambitie en realiteit. De business wil versnellen. Medewerkers experimenteren. Nieuwe mogelijkheden dienen zich dagelijks aan. Maar de infrastructuur, security en governance zijn niet in hetzelfde tempo meegegroeid.

Bij Avit ondersteunen we organisaties in o.a. zorg, onderwijs en de commerciële sector bij deze uitdaging. We zien structureel dat AI-ambities botsen op een digitale fundering die niet is meegegroeid. AI creëert deze problemen niet, maar het maakt ze onmogelijk te negeren.

Hoofdstuk 3

AI Infrastructure Debt: de schuld die stilletjes groeit

AI versnelt niet alleen innovatie. Het versnelt ook schuldopbouw. Veel organisaties beginnen met AI vanuit een concrete behoefte. Medewerkers ondersteunen, processen versnellen, efficiënter werken. Dat is logisch. Maar wanneer de onderliggende IT-omgeving niet meegroeit, stapelen de uitdagingen zich op.

Cisco noemt dit **AI Infrastructure Debt**.

Een vorm van technische schuld die ontstaat wanneer AI-toepassingen **sneller worden ingevoerd** dan de infrastructuur, security en governance waarop ze draaien.

Deze schuld verschilt van traditionele technische schuld, omdat AI zowel de waardecreatie als de gevolgen van uitgestelde investeringen versnelt. Deze gevolgen worden pas echt zichtbaar wanneer AI breder wordt ingezet:

Hoofdstuk 3

AI Infrastructure Debt: de schuld die stilletjes groeit

- ✓ Meer verkeer over het netwerk dan het aankan
- ✓ Steeds meer data wordt gebruikt zonder duidelijke afspraken over eigenaarschap of kwaliteit
- ✓ AI-toepassingen vragen toegang tot systemen waar het autorisatiebeheer niet op is ingericht
- ✓ Meer risico's die gemonitord moeten worden zonder de juiste visibility-tooling
- ✓ Nieuwe wet- en regelgeving (NIS2, AI Act, CRA) stelt hogere eisen aan beveiliging, documentatie en risicobeheersing

Wat begint als een innovatie-initiatief kan daardoor uitgroeien tot een operationele uitdaging. Maar de organisaties die nu investeren in hun fundering voorkomen dat innovatie wordt afgeremd door hun eigen omgeving.



Hoofdstuk 4

Security: van kostenpost naar voorwaarde voor innovatie

Jarenlang werden innovatie en security als tegengestelde krachten gezien. AI heft dat onderscheid op.

AI-systemen krijgen toegang tot steeds grotere hoeveelheden bedrijfsinformatie. Medewerkers gebruiken publieke AI-tools voor dagelijkse werkzaamheden. AI Agents nemen zelfstandig acties binnen processen en applicaties. In die context is security geen controlemechanisme meer. Het is een randvoorwaarde voor vertrouwen. **En vertrouwen is een randvoorwaarde voor innovatie.**

Wet- en regelgeving versterkt dit. NIS2, de Cyber Resilience Act en de AI Act leggen bestuurders direct verantwoordelijk voor digitale weerbaarheid. Security is niet langer een IT-vraagstuk. Het is een strategisch thema dat op bestuursniveau wordt beoordeeld.

Als Cisco Security Partner of the Year (2024 én 2025) helpen we organisaties security te integreren als fundament, niet als nagedachte. Via Zero Trust-architecturen en onze Managed Security Services creëren we omgevingen waarin innovatie mogelijk is zonder controle te verliezen.

Hoofdstuk 5

Waarom dit nú urgent is

De druk om nú te handelen komt niet alleen van AI zelf. Er zijn minstens drie parallelle ontwikkelingen die de urgentie tegelijkertijd vergroten en die samen een tijdsdruk creëren die organisaties niet kunnen negeren.

Regelgeving staat niet stil

Wetgeving rondom digitale veiligheid en AI wordt steeds concreter. NIS2 is per oktober 2024 van kracht en legt organisaties in kritieke sectoren directe verplichtingen op rond risicobeheer, incidentrapportage en beveiliging van de toeleveringsketen. De Cyber Resilience Act (CRA) stelt aanvullende eisen aan digitale producten en diensten. De AI Act, de eerste bindende AI-wetgeving ter wereld, treedt gefaseerd in werking en vereist dat organisaties aantoonbaar grip hebben op de AI-systemen die zij inzetten.

Organisaties die dit niet op orde hebben, lopen niet alleen operationeel risico maar ook juridisch en reputatierisico. En dat risico ligt inmiddels op het bord van de boardroom, niet alleen bij IT.



Waarom dit nú urgent is

Cyberdreigingen groeien mee met AI

AI maakt aanvallen goedkoper, sneller en gericht. Phishing-campagnes die vroeger weken kostten, worden nu in minuten gegenereerd. Deepfakes ondermijnen vertrouwen in communicatie. AI-gestuurde analyses vinden kwetsbaarheden sneller dan menselijke analisten ze kunnen dichten.

Tegelijkertijd biedt AI juist ook nieuwe mogelijkheden om dreigingen eerder te herkennen en sneller te reageren, maar alleen voor organisaties die beschikken over de juiste monitoring, data en architectuur. Wie die fundering mist, geeft het initiatief weg aan de aanvaller.



Hoofdstuk 5

Waarom dit nú urgent is

De concurrentiekloof wordt groter

De 13% die vandaag AI succesvol inzet, bouwt een voorsprong op die moeilijk te overbruggen is. Zij automatiseren processen die bij concurrenten nog handmatig verlopen. Zij reageren sneller op dreigingen. Zij schalen hun operaties zonder evenredige groei in personeelskosten. En zij doen dat op een fundering die verdere innovatie mogelijk maakt.

Voor de 87% die nog niet klaar is, geldt het omgekeerde. Elke maand uitstel vergroot niet alleen de technische schuld, het vergroot ook de afstand tot de koplopers.

De komende jaren worden niet bepaald door wie de meeste AI-tools inzet. Ze worden bepaald door wie de sterkste basis heeft om die technologie veilig, compliant en op schaal te benutten. Die basis bouwen kost tijd. En die tijd is nu.



Hoofdstuk 6

Wat de 13% succesvolle organisaties anders doen

Uit de Cisco AI Readiness Index blijkt dat succesvolle organisaties zich niet onderscheiden door duurdere AI-tools, maar door keuzes die zij jaren eerder maakten. Dat zie je terug in vier kenmerken:

Zij investeren eerst in hun fundering

Netwerk, cloudplatform en de digitale werkplek zijn voorbereid op de extra belasting die AI met zich meebrengt. Een schaalbare, veilige en goed beheerde infrastructuur vormt de basis voor iedere succesvolle AI-strategie.

Zij nemen security mee in het ontwerp

Security is geen laag die achteraf wordt toegevoegd. Door Zero Trust toe te passen als architectuurprincipe creëren organisaties een omgeving waarin innovatie mogelijk is zonder controle te verliezen.

Hoofdstuk 6

Wat de 13% succesvolle organisaties anders doen

Ze hebben inzicht in hun IT-omgeving

AI vergroot de afhankelijkheid van data, applicaties en digitale processen. Succesvolle organisaties beschikken over real-time inzicht in prestaties, risico's en afwijkingen. Zonder visibility wordt innovatie een risico. Met visibility wordt het beheersbaar. Continu inzicht maakt het mogelijk om sneller bij te sturen en problemen te voorkomen voordat gebruikers er last van hebben.

Zij combineren governance met innovatie

Succesvolle organisaties weten wie verantwoordelijk is voor data, AI-toepassingen en besluitvorming. Daardoor kunnen nieuwe initiatieven sneller worden beoordeeld en ingevoerd, zonder steeds opnieuw het wiel uit te vinden. Governance is geen rem op AI. Het is de voorwaarde voor verantwoorde AI op schaal.

Bij Avit zien we dat organisaties die succesvol met AI werken meestal geen fundamenteel andere technologie gebruiken dan de rest van de markt. Het verschil zit in de kwaliteit van de onderliggende IT-omgeving. Wie daar de afgelopen jaren in heeft geïnvesteerd, kan nieuwe ontwikkelingen sneller en met minder risico omarmen.

Checklist

Hoe AI-ready is jouw organisatie?

Beantwoord onderstaande vragen met een score van 1 tot 5 (1 = niet ingericht, 5 = volledig ingericht). De totaalscore geeft een indicatie van jullie startpositie voor AI op schaal.

Infrastructuur

Ons netwerk, datacenter en cloudplatform zijn voorbereid op AI-workloads en de extra capaciteit die daarvoor nodig is.

Score: _____

Security & Identity

Wij hebben inzicht in gebruikers, apparaten en toegangsrechten en passen moderne beveiligingsprincipes, zoals Zero Trust, toe.

Score: _____

Governance

Er zijn duidelijke afspraken over het gebruik van AI, eigenaarschap van data en verantwoordelijkheden binnen de organisatie.

Score: _____

Checklist

Hoe AI-ready is jouw organisatie?

Beantwoord onderstaande vragen met een score van 1 tot 5 (1 = niet ingericht, 5 = volledig ingericht). De totaalscore geeft een indicatie van jullie startpositie voor AI op schaal.

Visibility

Wij hebben real-time inzicht op prestaties, risico's en afwijkingen binnen onze IT-omgeving.

Score: _____

Automation & Operations

Operationele processen en securitytaken zijn waar mogelijk geautomatiseerd, zodat beheerteams zich kunnen richten op uitzonderingen en verbeteringen.

Score: _____

Hoe AI-ready is jouw organisatie?

Resultaten

5 – 10 punten: Startfase

AI kan zeker waarde opleveren, maar de onderliggende IT-omgeving vraagt eerst aandacht. Investerings in infrastructuur, security en beheer vormen hier de grootste stap vooruit.

11 – 18 punten: In ontwikkeling

Er is een basis, maar kritische gaps in governance, visibility of security beperken het AI-potentieel.

19 – 25 punten: Klaar voor de volgende stap

Jullie organisatie beschikt over een solide uitgangspunt om AI verder op te schalen. De uitdaging ligt vooral in het blijven ontwikkelen van de omgeving, zodat nieuwe toepassingen veilig en beheersbaar kunnen worden toegevoegd.

Geen enkele organisatie is volledig 'klaar'. Technologie, wetgeving en dreigingen blijven zich ontwikkelen. Regelmatig toetsen waar de grootste verbeterkansen liggen, helpt om gericht te blijven investeren.

Iedere organisatie kent aandachtspunten. Tijdens Avit Live op 17 september 2026 laten wij zien hoe organisaties hiermee omgaan en welke keuzes zij maken om hun IT-omgeving klaar te maken voor AI.

Avit Live 2026

Op 17 september 2026 brengen we IT-leiders, security-specialisten en digitale beslissers samen om te bespreken hoe organisaties hun digitale fundering versterken voor een toekomst waarin AI een steeds grotere rol speelt.

Aanmelden kan via:
www.avitgroup.com/avit-live

Dag programma

Avit Live
2026



De Landgoederij
Camminghalaan 30, 3981 GH Bunnik

Inloop en lunch	12:00
Welkomstwoord	12:45
Keynote	13:00
Avit Expertsessie: State of the Hack	14:15
Avit Expertsessie: Digitale weerbaarheid begint bij inzicht	15:15
Panel: De bouwstenen van een AI-ready organisatie	16:15
Afsluiting	16:45
1-op-1 sessies & Borrel	17:00

Tijdens de sessies is er volop ruimte om ervaringen uit te wisselen en in gesprek te gaan over de vraagstukken die binnen jouw eigen organisatie spelen.

avit
part of  springboardnetwork

Over Avit

Bij Avit helpen we organisaties bij het ontwerpen, realiseren en beheren van veilige en toekomstbestendige IT-omgevingen. Dat doen we op het gebied van networking, cybersecurity, cloud, AI en managed services. Al meer dan twintig jaar werken we samen met Cisco aan complexe IT-vraagstukken binnen onder meer de zorg, het onderwijs, de overheid en het bedrijfsleven. Vanuit die praktijk ondersteunen we organisaties bij het versterken van hun digitale weerbaarheid en het creëren van een omgeving waarin nieuwe technologie verantwoord kan worden toegepast.

Als Cisco Preferred Partner, Overall Partner of the Year Nederland 2024 en Security Partner of the Year 2024 en 2025 combineren we diepgaande technische kennis met ruime ervaring in ontwerp, implementatie en beheer.

 www.avitgroup.com

 info@avitgroup.com

avit

part of  springboardnetwork