

DE MYTHE VAN DIGITALE SOEVEREINITEIT

ONDERZOEK SAI.BE: WELKE CLOUD VOOR JOUW ORGANISATIE?

Pag. 8 & 11

SAI RESET IT
4 DECEMBER 2025

BEKIJK [HIER](#) HET
VOLLEDIGE
PROGRAMMA



En verder:



SYSTEM ADMINISTRATORS | AGENTIC AI | PHISHING | OUTSOURCING NAAR EGYPTEN | MEEST GEVRAAGDE IT-SKILLS |
AI & SOFTWARE-ONTWIKKELING | MISLUKTE AI-TESTPROJECTEN | DIGITALE MYTHES



CASE
DATA & AI BIJ CANVA

pag. 16



VIRTUALISATIE
ALTERNATIEVEN VOOR VMWARE

pag. 19



SOFTWARE SECURITY
MET OWASP SAMM

pag. 31

EDITO

DE ROL VAN AI IN HET ONDERWIJS: VANDAAG EN MORGEN

Het nieuwe schooljaar is gestart en tijdens de eerste oudercontactvergadering viel meteen iets op: leerkrachten besteedden opvallend veel aandacht aan het gebruik van AI. In de zaal zag ik verraste blikken bij veel ouders. Alsof ze dachten: "Amai, onze leerkrachten zijn mee met hun tijd. Ze weten niet alleen dat AI bestaat, maar herkennen ook hoe het in de klas kan worden ingezet."

Natuurlijk, sommige studenten misbruiken AI. Dat werd in Vlaanderen pijnlijk duidelijk na het debacle met het toelatingsexamen geneeskunde. Maar tegelijk groeit het aantal leerkrachten dat AI omarmt om hun lessen efficiënter te plannen en inhoud te verrijken.

Het deed me denken aan een recent interview met Salman Khan, oprichter van de gratis **Khan Academy**. Hij ziet AI niet als bedreiging, maar als hulpmiddel. In zijn visie is AI een assistent, geen vervanger. Want leerkrachten brengen unieke menselijke kwaliteiten mee – verbinding, verantwoordelijkheid, empathie – die geen enkele machine ooit zal kunnen repliceren.

Khan verwoordt het treffend: "Wat ik altijd graag doe, is nadenken over de doelstellingen van schrijven en lezen toen die voor het eerst ontstonden." Communicatie en structuur in ons denken zijn essentieel. Net daar kan AI het onderwijs versterken, zonder het menselijke te ondermijnen.

"AI could serve as an invaluable tool, enhancing personalized learning experiences while maintaining the essential human element of teaching."

Salman Khan (2025)

Stel dat een school een miljard euro ontvangt en briljante afgestudeerden inhuurt als persoonlijke assistenten. Niet om leerkrachten te vervangen, maar om hen te ondersteunen. Elke student zou een persoonlijke begeleiding krijgen. Wanneer een assistent merkt dat een leerling minder betrokken is, kan die informatie meteen doorstromen naar de leerkracht. Zo kan het lesmateriaal in real time aangepast worden aan de noden en interesses van de student. Precies dat is wat AI zou kunnen doen – en misschien nog beter.

AI maakt onderwijs niet alleen efficiënter, maar ook aantrekkelijker. Denk aan gepersonaliseerde leerpaden, interactieve simulaties en gesprekken met virtuele historische figuren. Of aan het ervaren van oude beschavingen in 3D. Virtual reality kan een klaslokaal omtoveren tot een ontdekkingsreis door het menselijk lichaam of een wandeling langs de ruïnes van Rome. Zo wordt leren niet alleen effectiever en visueler, maar ook boeiender en betekenisvoller.

Daarnaast kan AI de creativiteit van studenten versterken. Het biedt eindeloze mogelijkheden om te experimenteren, te ontdekken en nieuwe ideeën te verkennen. AI kan dienen als persoonlijke leercoach voor iedere student – voor zover middelen en toegang het toelaten.

Toch blijft één punt overeind: zonder de menselijke factor verliest onderwijs zijn ziel. AI kan ondersteunen, inspireren en personaliseren, maar het is de leerkracht die studenten motiveert, aanspreekt en begeleidt op een manier die technologie nooit kan evenaren.



De uitdaging is dus niet of AI in het onderwijs thuishoort, maar hoe we het inzetten. Mits goed gebruik kan het leren verrijken en de rol van de leerkracht versterken. En denk ten slotte ook aan het continu leren binnen de bedrijfsmuren.

Geniet intussen van het nieuwe schooljaar – mét of zonder AI.

Marc Vael
Voorzitter raad van bestuur SAI.BE

INHOUD

FLASH: MISLUKTE AI-PILOTS, PHISHING, MEEST GEVRAAGDE IT-SKILLS

pag. 3

PROGRAMMA SAI RESET 2025: AFSpraak op 4 DECEMBER

pag. 6

HOE AI DE ZES BELANGRIJKSTE TALEN NOG BELANGRIJKER MAAKT

pag. 7

DE GROTE SOFTWARE DEVELOPMENT UPDATE (DEEL 2): TRENDS, INFRASTRUCTUUR EN ARCHITECTUUR

pag. 8

DE MYTHE VAN DIGITALE SOEVEREINITEIT: WAAROM EUROPA NIET LOSKOMT VAN AMERIKAANSE CLOUDS

pag. 13

CASE: HOE CANVA DATA INZET OM WERELDWIJD 370 DESIGNS PER SECONDE TE VERWERKEN

pag. 16

DE ZEVEN BESTE VMWARE-ALTERNATIEVEN

pag. 19

DE LANGE CARRIÈRE VAN DE SYSTEM ADMINISTRATOR

pag. 24

DAAR ZIJN DE AGENTS: 5 FEITEN OVER AGENTIC AI

pag. 26

EGYPTE IN OPMARS ALS IT-BESTEMMING

pag. 29

A NOVEL APPROACH TO QUANTIFYING SECURITY USING SAMM

pag. 31

BOEK: DE ZEVEN GROOTSTE MYTHES VAN HET DIGITALE TIJDPERK

pag. 35

OPVALLENDE QUOTES: "AGENTS HATE SPAGHETTI"

pag. 37

VOLGENDE EVENTS SAI.BE

pag. 38

“

"WE DACHTEN DAT PYTHON NIET VERDER KON GROEIEN, MAAR AI-CODE-ASSISTENTEN LATEN PYTHON TOCH NOG EEN STAP VOORUITZETTEN."

PAUL JANSEN, CEO VAN TIOBE

OP PAGINA 7.

TECHNOLOGIE IS HET PROBLEEM NIET WAAROM 95% VAN AI-PILOTS MISLUKT

Een nieuw rapport van het MIT Media Lab zet bedrijven op scherp: maar liefst 95% van alle AI-pilotprojecten levert geen merkbare financiële return op. De oorzaak zit in de manier waarop organisaties AI gebruiken.

Volgens de studie **The GenAI Divide: State of AI in Business 2025** is de grootste bottleneck een *learning gap*: bedrijven begrijpen onvoldoende hoe ze AI-tools goed moeten toepassen of verankeren in hun processen. "Grote taalmodellen lijken simpel, omdat je ze in gewone taal kunt aansturen. Maar het vergt expertise en experimenten om ze effectief in workflows te integreren", zo schrijven de onderzoekers. Wharton-professor Ethan Mollick benadrukt dat **bedrijven te vaak proberen AI in te passen in bestaande processen**, die vaak vooral bureaucratie en kantoorpolitiek weerspiegelen. Start-ups, minder gehinderd door verouderde structuren, zien daarom sneller rendement. Of hoe technische kennis alleen niet genoeg is om een AI-project te doen slagen. Er is ook een rol weggelegd als change agent om processen opnieuw te ontwerpen in functie van AI.

BOUWEN VERSUS KOPEN

Een tweede pijnpunt is de strategie: organisaties die AI-oplossingen inkopen, boeken twee derde van de tijd succes, terwijl intern gebouwde systemen slechts in een derde van de gevallen slagen.

Voor al **grote ondernemingen houden vast aan eigen ontwikkeling**, vaak uit zorgen over privacy of een hang naar controle – met dus vaak eerder teleurstellende resultaten als gevolg. IT-professionals komen hier

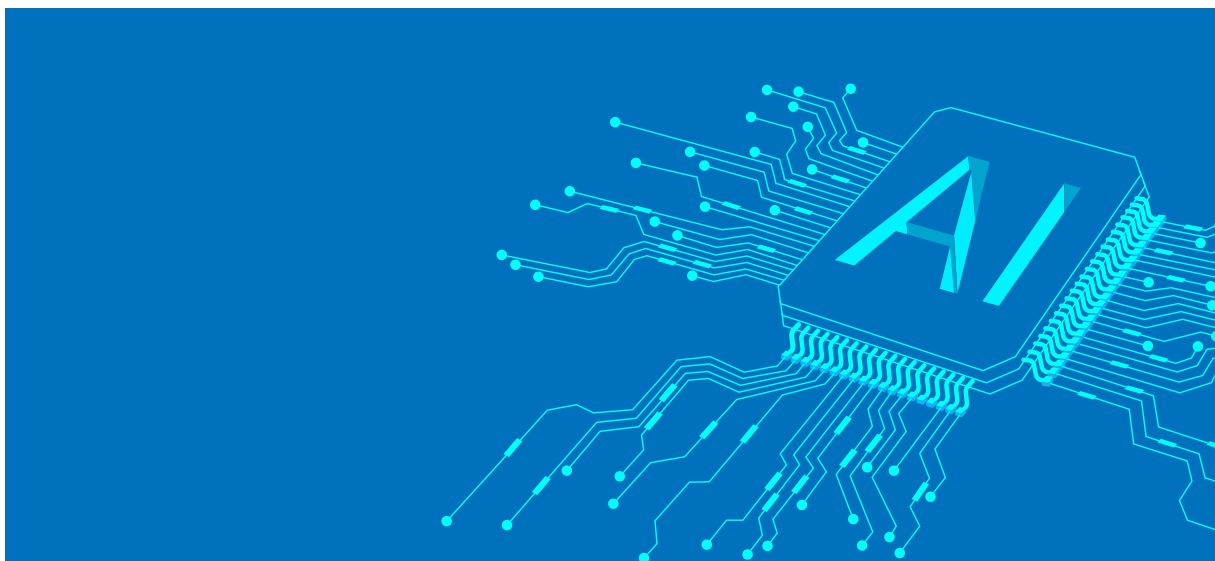
door vaak klem te zitten tussen de strategische keuze voor maatwerk en de realiteit van beperkte middelen en expertise.

Opvallend is ook de keuze van toepassingen. Veel bedrijven zetten AI in bij marketing en sales, terwijl volgens MIT de echte winst ligt in backofficeprocessen, waar kostenreductie en efficiëntie veel groter kunnen zijn. Zo maakt hun onderzoek duidelijk dat maar liefst 50% tot 70% van de AI-budgetten (op basis van de steekproeven onder leidinggevers) naar pilotprojecten op het gebied van verkoop en marketing is gegaan. "Deze projecten zijn intern gemakkelijk te verkopen", zo stellen de onderzoekers vast.

50% TOT 70%

van de AI-budgetten
gaat naar pilots in
sales en marketing

» *Bekijk of herbekijk **hier** de SAI Short over Data & AI.*



PHISHING SUCCESVOLLER VIA PC DAN VIA SMARTPHONE

Phishing gedijt niet overal even vlot. Het toestel waarmee gebruikers online zijn, blijkt een cruciale factor in hun risicomijdend gedrag.

Voor bedrijven blijft phishing een van de hardnekkigste dreigingen: aanval- len zijn (kost)efficiënt uit te voeren, vaak verantwoordelijk voor miljarden- verliezen. Toch laat **nieuw onderzoek** van Carnegie Mellon University en de Ben-Gurion Universiteit zien dat niet alle gebruikers even vatbaar zijn. Smartphonegebruikers blijken vaker niet te klikken op verdachte links dan pc-gebruikers.

Volgens de onderzoekers valt dit ver- schil in klikgedrag vooral te verklaren doordat **mobiele gebruikers zich in een andere mentale toestand bevin- den**. Smartphonegebruik vindt vaak plaats tijdens multitasking of korte interacties, waardoor gebruikers min-

der diep analyseren en sneller voor veiligheid kiezen. Het kleine scherm en de beperkte context versterken dit effect.

Pc-gebruikers nemen doorgaans meer tijd om details te beoordelen, maar lopen daardoor juist meer risico bij slim verpakte phishingbe- richten zonder duidelijke waarschu- wingstekens. Hoewel je zou zeggen dat deze gebruikers zo'n phishinglink beter kunnen inschatten, is besluit-eloosheid dus blijkbaar een betere verdediging tegen phishing dan een weloverwogen keuze.



ANDER APPARAAT, ANDER VERMIJDINGSGEDRAG

De onderzoekers spreken in dit verband van vermijdingsgedrag: de bewuste of onbewuste keuze van gebruikers om geen actie te onder- nemen bij een mogelijk risicovol bericht, zoals het niet openen van een verdachte link. Het besluit is dus dat het gebruikte toestel van invloed kan zijn op dat risicomijdend gedrag, aldus Lior Fink, van de Ben-Gurion Universiteit van de Negev in de Israëlische stad Be'er Sheva en co-auteur van het onderzoek. "Gelet op de grote verscheidenheid aan apparaten die gebruikers ter beschik- king hebben, draagt ons onderzoek ook bij aan een beter begrip van gedragsverschillen per apparaat."

» Bekijk **hier** de SAI Shorts over security.

WANTED



Technology & Data talents

Data&AI, Chatbot,
Security, Cloud, Mobile, ...

belfius.be/ITjobs





VOOR DEZE VIJF IT-VAARDIGHEDEN WILLEN BEDRIJVEN EXTRA BETALEN

Vooraf kennis van cybersecurity en netwerken maakt IT'ers schaars én waardevol. Voor deze specifieke IT-vaardigheden zijn bedrijven bereid om extra te betalen, blijkt uit recent onderzoek van rekruteringsbedrijf Robert Half.

In de voortdurende 'war for talent' zoeken werkgevers heel gericht naar profielen die over kritische digitale vaardigheden beschikken en zijn ze bereid daarvoor dieper in de buidel te tasten.

Uit de survey van rekruteringsbedrijf Robert Half komt naar voren dat cybersecurity dé topprioriteit blijft. "Bijna de helft (46%) van de onderzochte werkgevers zegt bereid te zijn een hoger start- of topsalaris te betalen als een kandidaat cybersecurityvaardigheden bezit", aldus Wout Van de Wijer, manager bij Robert Half.

Ondanks de opmars van AI staat cybersecurity dus bovenaan, maar het verschil met andere vaardigheden is klein. Netwerkbeheer staat op twee en analytische vaardig-

heden op drie. Business intelligence en cloud skills vervolledigen de top vijf. "Wie over deze skills beschikt, kan daar zijn voordeel mee doen op de arbeidsmarkt", stelt Van de Wijer.

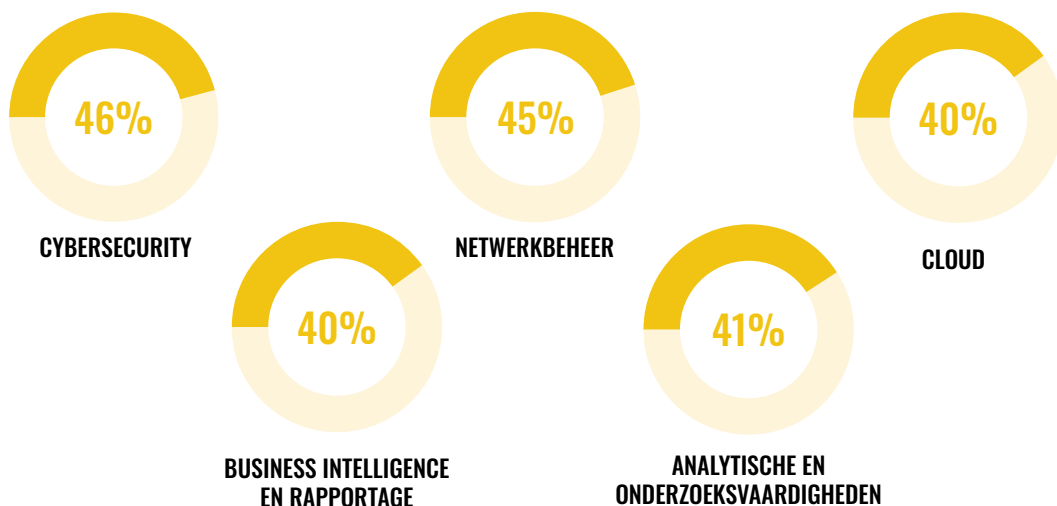
FLEXIBELE ARBEIDSVORWAARDEN

De slotsom is ook: bedrijven blijven het een uitdaging vinden om de juiste mensen te vinden, zeker in IT. "Zo zegt een kwart van hen dat het

hun grootste uitdaging is in 2025", aldus Wout Van de Wijer. AI grijpen bedrijven ook op andere vlakken in. "Eén op de drie kmo's biedt extra flexibele werkomstandigheden bovenop degene die ze al hebben. Bij grote bedrijven loopt dat aantal zelfs op tot 41%." Het onderzoek van Robert Half werd online uitgevoerd onder 500 werkgevers door Rigour Research, een onafhankelijke onderzoekspartner.



TECHNISCHE SKILLS WAARVOOR BEDRIJVEN HOGERE START- EN TOPSALARISSEN WILLEN BETALEN



SAI RESET IT 2025

UW AFSPRAAK OP 4 DECEMBER

SAI.BE presenteert in zijn eindejaarconferentie RESET IT 2025 alle cruciale technologietrends in een boeiende namiddag. Op het programma staan zeven toppresentaties en twee panelgesprekken die alle SAI.BE-thema's zullen behandelen. Deze jaarafsluiter wil je niet missen.

TIJDSTIP	ONDERWERP	SPREKER
12:30 - 13:00	Aankomst en registratie	
13:00 - 13:05	Verwelkoming	Guido Thys Master of Ceremony
13:05 - 13:15	Introductie	Marc Vael Voorzitter SAI.BE
13:15 - 13:45	Keynote 1: On the future of AI	Prof. dr. Tijl De Bie Professor AI UGent 
13:50 - 14:20	Keynote 2: Vision on cybersecurity	Chris Kubecka Chief Hacktress Unit6 Technologies 
14:25 - 14:55	Keynote 3: The future of digital transformation	Prof. dr. Stijn Viaene Head Technology and Operations Management Vlerick Business School 
15:00 - 15:30	Panelgesprek	
15:30 - 16:15	Networking met eten en drank	
16:15 - 16:45	Keynote 4: Application architecture - what's next?	Davide Cioccia Founder en Principal Security Consultant DCDOCX 
16:50 - 17:20	Keynote 5: IT regulations and compliance	Prof. Konstantinos Sergakis Knowledge and Research Director Guberna 
17:25 - 17:55	Keynote 6: The impact of quantum on infrastructure	Ramses Gallego Chief Technologist DXC Technology 
18:00 - 18:30	Panelgesprek	
18:35 - 18:45	SAI Personality Award 2025	Special guest...
18:45 - 19:35	Keynote 7: Technovision 2026 en het Kuramoto Model	Ron Tolido CTO Capgemini 
19:35 - 19:50	Outro	Marc Vael President SAI.BE
19:50 - 20:00	Afsluiter	Guido Thys Master of Ceremony
20:00 - 21:15	Receptie	

LOCATIE

SQUARE Brussels, Mont des Arts,
1000 Brussel, België

DATUM

4 december 2025
12:30 - 21:00

REGISTREREN

- Toegankelijk voor SAI.BE-leden en niet-leden
- Je krijgt **een exclusief SAI.BE-geschenk**
- Early bird (prijs tot oktober 2025): 35 euro (incl. btw)
- Late ticket: 45 euro (incl. btw)
- Betalingen worden verwerkt via **Stripe**. Betalen kan met kredietkaart of Bancontact. Na de betaling krijg je een factuur via e-mail.
- Opgelet: controleer goed je e-mailadres op de betalingspagina!
- Dit evenement kan worden gebruikt voor het vervullen van interne opleidingsdoelen van jouw medewerkers.
- Wil je eerst een factuur ontvangen en dan betalen of meerdere werknemers tegelijk inschrijven? **Contacteer ons.**

*Meer info over de sprekers en het inhoudelijke programma, vind je **hier**.*

Registreren voor RESET IT 2025 kan via **deze link**.

CODECONSOLIDATIE:

HOE AI DE ZES BELANGRIJKSTE TALEN NOG BELANGRIJKEER MAAKT

ABBA zong het jaren geleden al: *the winner takes it all*. De komst van AI-programmeerassistenten had een revolutie kunnen betekenen voor de diversiteit aan programmeertalen. In werkelijkheid gebeurt het omgekeerde: de rijken worden rijker, terwijl nieuwe talen steeds moeilijker doorbreken.

Een analyse van de meest recente edities van populairste programmeertalen toont hoe kunstmatige intelligentie de bestaande hiërarchie in de programmeerwereld verder versteent.

1. DE ONWRIKBARE TOP: ZES ECHTE DOMINANTEN

Python, C++, C, Java, C# en JavaScript (al dan niet met TypeScript) vormen eigenlijk de harde kern van de moderne softwareontwikkeling. Deze zes programmeertalen werden ook in het recente SAI.BE-onderzoek aangehaald als meest gebruikte, zowel in bestaande als nieuwe softwareprojecten.

Deze 'grote zes' houden ook al jaren de eerste posities vast in de bekende Tiobe-index met populairste programmeertalen. Python spant daar overigens de kroon met een recordrating van zowat 26%.

2. AI-ASSISTENTEN VERSTERKEN DE STERKEN

De doorbraak van AI-gebaseerde programmeerassistenten zoals

GitHub Copilot en Google Gemini Code Assist heeft bovendien een onverwacht effect: in plaats van voor diversiteit te zorgen, versterken ze de dominantie van reeds populaire talen. Paul Jansen, CEO van Tiobe, observeert dit fenomeen bij Python: "We dachten dat Python niet verder kon groeien, maar AI-code-assistenten laten Python toch nog een stap vooruitzetten."

De trend wordt ook onderbouwd door research. Stanford-onderzoek toont aan dat AI-programmeerassistenten 20% effectiever zijn bij populaire talen. De verklaring is volgens Jansen logisch: **"Er is simpelweg meer code beschikbaar van deze talen om de onderliggende AI-modellen mee te trainen."**

3. VETERANEN STRIJDEN BIJ DE ACHTERVOLGERS

Onder de gevestigde top woedt een fascinerende strijd tussen programmeertalen uit vervlogen tijden. "Het is een continue strijd tussen de gouden oudjes: Visual Basic, SQL, Fortran, Ada, Perl en

Delphi", analyseert Jansen. En wat verder in de lijst spelen ook talen als Fortran, Cobol en Assembly een rol van betekenis.

Ondanks deze volatiliteit heeft Jansen een duidelijke favoriet: "Ik zou mijn geld op Ada zetten. Met de steeds sterkere eisen op het gebied van beveiliging is Ada, als systeemprogrammeertaal in het veiligheidskritieke domein, waarschijnlijk de beste overlevende."

4. MODERNE TALEN HEBBEN HET MOEILIJK

Opvallend is de afwezigheid bij de stijgers van veel geprezen moderne alternatieven. Rust, Kotlin, Dart en Julia lijken naar adem te happen. Ondanks hun technische voordelen en moderne features, slagen deze nieuwkomers er niet in om door te breken naar de top tien. "Maar blijkbaar zijn vandaag vooral gevestigde talen populair", stelt Jansen vast.

Alleen Go uit 2007 kan nog wat aanklappen bij de grote jongens. "Overigens denk ik dat Go nog lang in de top tien zal blijven", zegt Jansen. "Ik zie steeds meer van onze klanten Go adopteren om snellere back-endcode te ontwikkelen en betere performance te halen."

Voor de software-industrie betekent deze consolidatie een fundamentele verschuiving. **Ontwikkelaars kiezen bewust voor mainstream-talen omdat deze superieure AI-ondersteuning bieden**, wat hun productiviteit aanzienlijk verhoogt. Tegelijkertijd worden nieuwe talen steeds verder naar de marge geduwd, waardoor innovatie paradoxaal genoeg wordt afgeremd door de tools die deze zouden moeten bevorderen.



Paul Jansen,
CEO van Tiobe.

TOP TIEN VAN DE TIOBE-INDEX (september 2025)

1. Python
2. C++
3. C
4. Java
5. C#
6. JavaScript
7. Visual Basic
8. Go
9. Delphi/Pascal
10. Perl



DE GROTE SOFTWARE DEVELOPMENT UPDATE (DEEL 2)

TRENDS, INFRASTRUCTUUR EN ARCHITECTUUR IN BELGISCHE SOFTWAREONTWIKKELING

In het eerste deel van het onderzoek bij SAI.BE-leden ging het onder meer over softwareteams, talen en de intrede van AI in de ontwikkelcyclus.

Nu schuiven we een laag dieper: hoe evolueren bedrijven in hun infrastructuur en architectuur? Welke trends zijn bepalend? De resultaten tonen een duidelijke beweging richting AI en cloud, maar ook een opvallend pragmatisme in de manier waarop bedrijven moderniseren.

1 TRENDS: AI BOVENAAN, BLOCKCHAIN ZAKT WEG

Artificiële intelligentie zet bij de bepalende trends de lijnen uit. Het wordt niet langer alleen gezien als hulpmiddel bij ontwikkeling, maar als bouwsteen van nieuwe toepassingen. Security volgt kort daarop: compliance en privacy blijven bepalend, zeker nu de regelgeving steeds strenger wordt.



Welke technologische trends zullen de komende drie jaar de grootste impact hebben op softwareontwikkeling?

AI/ML-integratie in software	35,8%
Security, privacy en compliance oplossingen	26,8%
Low-code/no-code platformen	14,6%
Serverless architecturen	10,6%
Quantum computing	5,7%
Edge computing	5,7%
Blockchain	0,8%

Low-code/no-code heeft zich intussen stevig gepositioneerd en wijst op een groeiende rol van business-gebruikers in ontwikkeling. Opvallend: blockchain, ooit een hype, speelt vandaag nauwelijks nog een rol van betekenis. Een trend die wel wordt aangehaald, is digitale soevereiniteit. Of zoals één respondent, werkzaam bij een softwarebedrijf, het verwoordde als trend: “Public cloud versus Trump.”

2 CLOUD EN INFRASTRUCTUUR: PUBLIC CLOUD GROEIT, MAAR ON-PREMISES HOUDT STAND

Microsoft Azure is het populairste platform, maar eigen datacenters blijven opvallend sterk aanwezig. Belgische bedrijven hebben dus nog niet massaal de sprong naar de publieke cloud gemaakt. Private cloud en AWS blijven belangrijke alternatieven, terwijl Google Cloud eerder beperkte tractie krijgt in ons land. Vercel duikt op, maar eerder marginaal: Belgische bedrijven experimenteren, maar blijven voorzichtig.

De toekomst ligt anno 2025 voor de meeste organisaties in de publieke cloud. Toch zien we dat hybrid cloud een stevige tweede keuze is: veel bedrijven zoeken flexibiliteit om gevoelige workloads intern te houden en tegelijk te profiteren van schaalbaarheid. Private cloud blijft aantrekkelijk voor specifieke sectoren, terwijl volledig on-premises of klassieke hosting bij minder bedrijven aan de orde is.

Welke infrastructuur-cloudtechnologie gebruikt jouw organisatie momenteel?

Public cloud: Azure	27,2%
On-premises (eigen datacenter)	25,0%
Private cloud (in extern datacenter)	16,2%
Public cloud: AWS	14,7%
Klassieke hosting (in extern datacenter)	11,0%
Public cloud: GCP	4,4%
Public cloud: Vercel	1,5%

Opmerkelijk: de public cloud staat als richting bovenaan, maar een overgrote meerderheid van de organisaties (goed voor zowat 63%) kiest voor opties die een niet-publiek aspect hebben, zoals hybrid cloud, private cloud, on-premises of klassieke hosting. Dit onderstreept de voorzichtige, pragmatische aanpak waarbij gevoelige data en workloads intern worden gehouden. Er wordt in veel gevallen een bewuste keuze gemaakt voor een diverse infrastructuur, in plaats van een integrale sprong naar de public cloud. Het blijkt een thema dat leeft. Een aantal respondenten gaven alvast aan dat ze de richting van hun infrastructuur “actief aan het evalueren zijn.”

In welke richting beweegt jouw organisatie qua infrastructuur en cloudtechnologie?

Meer public cloud	36,9%
Meer hybrid cloud	21,5%
Meer private cloud	20,0%
Meer on-premises	15,4%
Meer klassieke hosting	6,2%

3 ARCHITECTUUR: CONTAINERS EN MICROSERVICES ALS RUGGENGRAAT

Containers en microservices zijn samen met webservices de fundamenteen waarop de meeste applicaties vandaag draaien. Bedrijven willen schaalbaarheid en modulariteit, maar doen dat vooral in beproefde modellen. SOA blijft aanwezig in meer klassieke enterprise-omgevingen. EDA is in opmars, zeker waar realtime data belangrijk wordt. MACH, vaak genoemd in de context van digitale platformen en headless commerce, blijft voorlopig een niche.

Ook OWASP (Open Web Application Security Project) duikt op bij bedrijven. Het is geen klassiek architectuurmodel, maar een vooraanstaande richtlijn voor softwarebeveiliging. Al worden beveiligingsaspecten, zoals OWASP, intussen als een integraal onderdeel van architecturale keuzes beschouwd.

Welke ontwikkelarchitectuurmodellen worden momenteel gebruikt in jouw organisatie?

Containers	25,4%
Microservices	23,7%
Webservices	23,7%
SOA	8,3%
OWASP	8,3%
EDA	7,7%
MACH	3,0%

BESLUIT:

AI, CLOUD EN SCHAALBARE ARCHITECTUUR

Uit deze rondvraag bij 54 Belgische organisaties blijkt dat bedrijven hun softwareontwikkeling moderniseren met drie duidelijke prioriteiten: AI, cloud en schaalbare architectuur.

Dat gebeurt wel stap voor stap. Ze behouden bestaande infrastructuur zolang die waarde biedt, combineren oud en nieuw in hybride modellen en kiezen



vooral voor technologieën die zich in de praktijk al hebben bewezen. Telkens met een pragmatische blik op risico's, kosten en compliance.



DE MYTHE VAN DIGITALE SOEVEREINITEIT

WAAROM EUROPA NIET LOSKOMT VAN AMERIKAANSE CLOUDS

Digitale soevereiniteit is een begrip dat steeds vaker valt in Europese debatten over technologie, veiligheid en geopolitiek. Organisaties willen controle over data, infrastructuur en digitale diensten, vrij van buitenlandse inmenging. Maar wat betekent het werkelijk, en vooral: is het haalbaar? De Amerikaanse wetgeving werpt hier een donkere schaduw over. "Ik wens je veel succes met het begrijpen van die miljard regels broncode."

"No, I cannot guarantee it." Zelfs Microsoft moest het onlangs voor de Franse Senaat toegeven, toen werd gevraagd of data van Franse burgers nooit zonder expliciete toestemming met Amerikaanse autoriteiten zouden worden gedeeld. "Het Cloud Act-risico is hiermee zwart op wit bevestigd, door Microsoft zelf", zegt Eric Primus director Managed Services bij de Belgische dienstverlener Cheops, in een reactie hierop. "Waar data staan, maakt weinig uit als de jurisdictie elders ligt."

CLOUD DRAAIT OM ZEGGENSCHAP

Hiermee komen tot de kern van de zaak. "In een *cloud first*-strategie is het niet de technologie, maar de zeggenschap over jouw data die bepaalt of de cloud een oplossing is of een risico", zegt Peter Witsenburg, regional IT director bij PSA International. **"De cloud draait allang niet meer om de servers en netwerken, maar om de vraag: wie heeft écht toegang tot jouw data?"**

De Microsoft-uitspraak in de Franse Senaat bevestigt niet alleen wat concurrenten maar ook wat andere en juridische experts al langer zeggen: zolang Europa massaal draait op Amerikaanse hyperscalers zoals Microsoft, Google en Amazon, blijft soevereiniteit grotendeels een illusie.

WAT DIGITALE SOEVEREINITEIT WEL EN NIET IS

Volgens Bert Hubert, oprichter van PowerDNS en voormalig toezicht-houder bij de Nederlandse inlichtingendiensten, begint digitale soevereiniteit met drie kernvoorwaarden: vertrouwelijkheid, beschikbaarheid en controle. "Vertrouwelijkheid – hebben andere mensen dan wij toegang tot onze data? Beschikbaarheid – **kunnen we uit de oplossing gegoooid worden door een executive order van Donald Trump?** Controle – als het niet goed gaat, kan ik ingrijpen om de situatie te verbeteren?", zo overloopt Hubert in een blogbericht.

Die voorwaarden zijn concreet. Soevereiniteit is dus niet simpelweg 'een Europees datacenter' of 'een logo met een EU-vlag'. Het gaat om zeggenschap en afdwingbare bescherming.

AMERIKAANSE WETGEVING ALS HARDE GRENS

Een terugkerende realiteit: Amerikaanse bedrijven vallen onder Amerikaanse wetgeving, waar hun servers ook staan. Hubert: "Er is geen manier waarop een Amerikaans bedrijf zichzelf kan omtoveren tot een niet-Amerikaans bedrijf. Ongeacht waar hun servers staan, in de EU of niet. Waar je data staan, maakt voor de Amerikaanse wetgeving echt niet uit."

Dit maakt alle initiatieven van hyperscalers – van 'EU Data Boundaries' tot 'Customer Lockbox' – in essentie tandeloos. Hubert vergelijkt die laatste met een extra slot op je deur. "Terwijl de huisbaas gewoon een kopie van de sleutel heeft."

DE BEFAAMDE SECTION 702

Ook Dave Michels, researcher in cloudcomputingwetgeving, benadrukt dat de juridische constructies

van hyperscalers weinig uithalen zolang FISA Section 702 geldt, wat staat voor *Foreign Intelligence Surveillance Act*. Die impliceert namelijk dat de Amerikaanse overheid zich in bulk toegang kan verschaffen tot onze data.

"Waar je data staat, maakt voor de Amerikaanse wetgeving echt niet uit."

"Geen van de drie hyperscalers legt uit hoe hun nieuwe maatregelen het risico op toegang door de Amerikaanse overheid daadwerkelijk verkleinen", aldus Michels. "Sterker nog, in hun aankondigingen wordt de bevoegdheid van Amerikaanse inlichtingendiensten om gegevens af te dwingen onder FISA Section 702 niet eens genoemd."

DE ILLUSIE VAN EUROPESE ALTERNATIEVEN

Naast Amerikaanse claims zijn er ook Europese bedrijven die zich presenteren als volwaardige alternatieven. Hubert waarschuwt voor *overselling*: "Als je dus een juichende aankondiging ziet van een nieuwe soevereine Europese



Peter Witsenburg, regional IT director bij PSA International: "Vandaag draait de cloud om de vraag: wie heeft écht toegang tot jouw data?"

cloud, check dan of ze bijvoorbeeld een equivalent van Amazon Cognito aanbieden. Dan zouden ze echt meedoen. Zo niet, dan stelt men zich groter voor dan men is.”

Amazon Cognito is een identity-managementdienst die onder meer login, authenticatie en toegangsbeheer voor miljoenen gebruikers afhandelt – precies het soort cruciale bouwsteen dat Europese alternatieven vaak missen.

Met andere woorden: veel Europese aanbieders leveren uitstekende infrastructuur, maar missen de geïntegreerde diensten en ecosystemen die organisaties tegenwoordig verwachten.

AIRGAPPED EN ESCROW: TIJDELIJKE OPLOSSINGEN

Sommige initiatieven proberen afstand te creëren, zoals een ‘air-gapped’ cloud die fysiek ontkoppeld is van Amerikaanse netwerken. Bij Google verwijzen ze naar de Google Distributed Cloud air-gapped als hoogste niveau van soevereiniteit. **“Volledig afgesloten en zonder verbinding met de publieke cloud”**, verduidelijkt Joost Smit, hoofd Google Cloud in de Benelux. “Deze formule krijgt vandaag veel interesse, maar het is complex”, erkent hij. “Ontwikkelingen komen er later beschikbaar, en ondersteuning kan alleen fysiek ter plaatse gebeuren.”

“Juridische constructies van hyperscalers halen weinig uit zolang FISA Section 702 geldt.”

Hubert is sceptisch, vooral als de VS echt de stekker eruit trekt: “Na een paar maanden is het waarschijnlijk toch afgelopen. Er komen dan namelijk geen beveiligingsupdates meer uit Amerika. En na een paar maanden is je cloud dan te onveilig geworden om nog te draaien.”

Ook het idee van broncode in Zwitserse kluizen overtuigt hem niet.

Zonder duizenden getrainde engineers in Europa blijft dit een theoretische noodoplossing. **“In de praktijk mag de kluis met die broncode pas open als er enorme ruzie is.** En dan wens ik je succes met het begrijpen van die miljard regels broncode, waarbij Microsoft je wegens sancties niet meer mag helpen.”

ENCRYPTIE EN CONFIDENTIAL COMPUTING

Technische maatregelen zoals encryptie en confidential computing bieden perspectief, maar blijven beperkt. Dave Michels: “In het slechtste geval geven EKM-oplossingen (*External Key Management*: een techniek waarbij klanten zelf hun encryptiesleutels beheren, maar waarbij de cloudaanbieder in de praktijk vaak nog toegang kan afdwingen) de illusie van klantcontrole, terwijl de provider in werkelijkheid nog altijd in het geheim klantgegevens aan de Amerikaanse overheid kan doorgeven.”

Confidential computing kan, volgens Michels, data in gebruik beschermen, maar laat metadata en veel SaaS-diensten ongemoeid. Het vermindert de risico's, maar lost de kernvraag – zeggenschap tegenover Amerikaanse wetgeving – niet op.

HET FUNDAMENTELE PROBLEEM: GEMAK EN GEWENNING

De afhankelijkheid van Amerikaanse big tech is overigens niet alleen een juridisch probleem, maar ook een cultureel en organisatorisch. Hubert stelt: **“Medewerkers laten switchen van software is onvoorstelbaar moeilijk.** Ook organisaties die geprobeerd hebben te veranderen naar Google Workspace switchen later vaak weer terug: ons personeel eist de echte Microsoft.”

Dat maakt de weg naar echte digitale autonomie lastig. Zolang Europa blijft vertrouwen op Amerikaanse hyperscalers – hoe Europees hun marketing ook klinkt – blijft soevereiniteit eerder een mythe dan een rea-

liteit. De vraag is dus niet of Europa ‘een soevereine cloud’ kan kopen, maar of we bereid zijn te investeren in alternatieven, en vooral, of we de discipline hebben om ze ook echt te gebruiken. Bewustwording is daar het eerste element.

Wat Microsoft hoger al toegaf, geldt natuurlijk ook voor de andere (Amerikaanse) spelers. Zoals Joost Smit van Google Benelux het impliciet erkent: “Ja, we krijgen soms de vraag: wat als de Amerikaanse overheid bepaalde beslissingen neemt? Dat is een complexe discussie, vol hypothesen. Maar de vraag leeft absoluut.”

ZO KAN EEN EUROPESE CLOUD ECHT VAN DE GROND KOMEN

Volgens Peter Witsenburg, regional IT director bij PSA International, ligt de sleutel tot een soevereine Europese cloud in drie domeinen.

1. De handhaving van bestaande EU-wetgeving, zoals GDPR, de Data Act en NIS2, versterken zodat burgers en bedrijven verzekerd zijn van afdwingbare bescherming.

2. Daarnaast moeten Europese aanbieders meer samenwerken en innoveren, onder meer rond identitymanagement en SaaS-oplossingen, zodat zij een volwaardig alternatief kunnen uitbouwen.

3. Tot slot moeten overheden en bedrijven zelf het voortouw nemen door bewust voor Europese cloudoplossingen te kiezen en dit ook te verankeren in hun aanbestedingen.



PLAN B VOOR EUROPA: LOKALE ÉN GLOBALE CLOUDS

“Wat is Plan B? Dat is de grote vraag die we in Europa steeds opnieuw horen”, zegt Rahiel Nasir, research director en European cloud practice lead bij IDC.

“Door alle geopolitieke en economische onrust die we in 2025 hebben gezien, de zorgen over Amerikaanse dominantie in technologie en de angst dat diensten van niet-Europese IT-aanbieders worden ingetrokken door een executive order van de Amerikaanse overheid, is dit dé kwestie.”

Volgens Nasir is de interesse in digitale soevereiniteit in Europa altijd al hoog geweest. “Maar nu geopolitieke spanningen escaleren en de regulatoire onzekerheid verdiept, zien veel organisaties dit als een strategische noodzaak.”

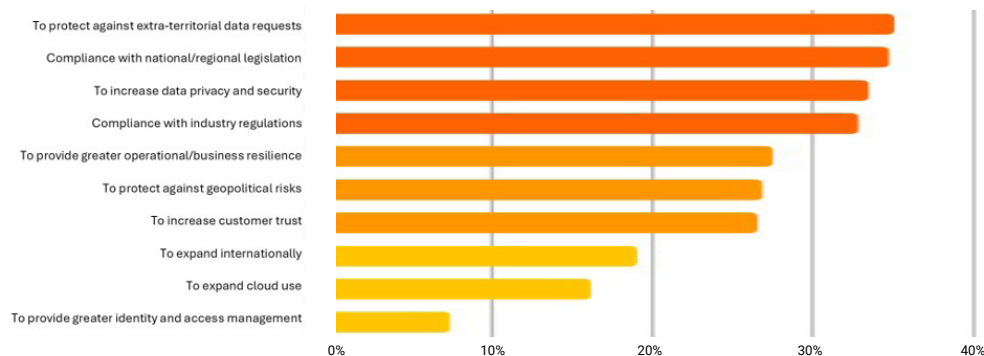
De recente Digital Sovereignty Survey van IDC toont die verschuiving duidelijk. **“Geopolitiek risico stond jarenlang onderaan het lijstje van redenen om voor soevereine oplossingen te kiezen. Nu zien we dat dit**

al meer dan een kwart van de Europese organisaties bezighoudt.” Wat volgens Nasir echter het meest opvalt, is dat bescherming tegen extraterritoriale dataverzoeken de belangrijkste drijfveer is geworden. “Dit weerspiegelt een groeiende angst over buitenlandse toegang tot gevoelige data.”

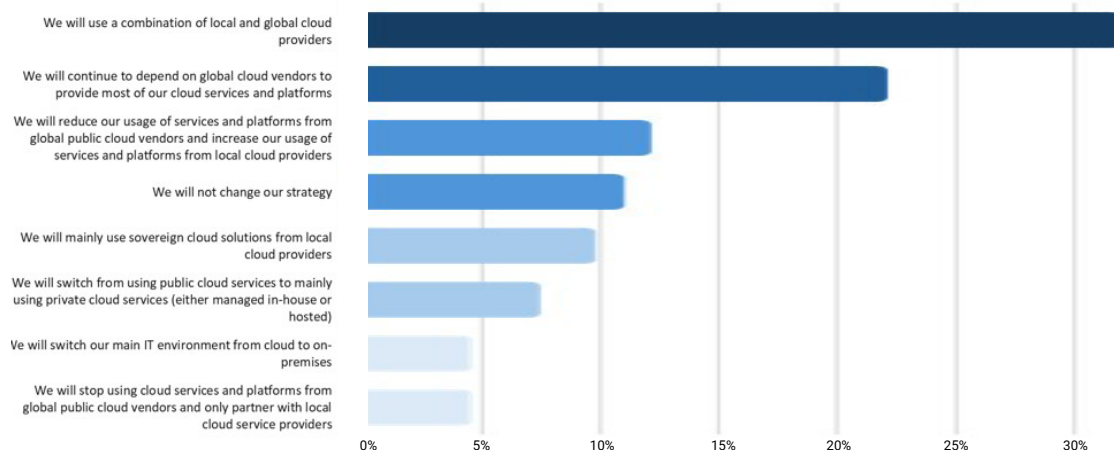
Europa zoekt actief naar alternatieven. Voor het eerst trekken Europese providers proactief samen op en presenteren zij zich, volgens Nasir, zelf als het ‘Plan B’. Voorbeelden zijn EuroStack, dat een Europa-geleide digitale supplychain wil opzetten, virt8ra, Europa’s eerste soevereine edge cloud, en SECA, de door de EU gefinancierde cloud-API.

Maar ook Amerikaanse spelers blijven meebewegen. “Grote namen als Google en Microsoft benadrukken dat soevereiniteit óók met hen kan werken, mits er goede controles en samenwerkingen zijn. Duidelijk is ook dat **net zoals Amerikaanse providers Europa niet verlaten, Europa hen ook niet gaat dumpen.**” De meest geciteerde maatregel is daarom dat organisaties lokale en globale cloudproviders gaan combineren.

What are, or were, the main drivers of your organisation's decision to use sovereign cloud?



How will increased interest in digital sovereignty affect your organisation's cloud and IT usage in the next 12 months?



Bron: IDC, 2025

HET SOEVEREINITEITSOFFENSIEF VAN AWS, GOOGLE EN MICROSOFT

Amazon Web Services heeft deze zomer nieuwe maatregelen aangekondigd voor de AWS European Sovereign Cloud om controle en onafhankelijkheid binnen Europa te vergroten. De zet past in het soevereiniteitsopbod van de hyperscalers.

AWS zette een aparte Europese organisatie op het getouw, gevestigd in Duitsland. De beslissingen worden genomen door een, naar eigen zeggen, onafhankelijk adviesorgaan. De cloud draait volgens de aanbieder volledig op Europese infrastructuur en met een speciaal Europees security operations center (SOC), zonder afhankelijk te zijn van systemen buiten de EU.

Gekwalificeerde medewerkers in de EU hebben toegang tot essentiële software om de diensten draaiende te houden. "De enige volledig uitgeruste, onafhankelijk beheerde

sovereine cloud, ondersteund door strenge technische controles, soevereine garanties en wettelijke bescherming", klinkt het bij AWS.

VIER PIJLERS

Wat is hierbij van tel? Volgens Max Peterson, VP sovereign cloud bij Amazon Web Services, staan enkele pijlers centraal bij soevereiniteit. "De eerste pijler is data. Het draait dus allemaal om datasoevereiniteit, locatie, toegang en gegevensbescherming", vertelt hij. De tweede pijler is toegang voor operators. "Ze willen er zeker van zijn dat alleen zij

toegang hebben tot hun applicaties die in de cloud draaien."

De derde pijler is veerkracht en overlevingsvermogen. Klanten moeten weten dat ze hun digitale activa kunnen blijven gebruiken, ondanks grote natuurrampen of buitenlandse inmenging, zoals we nu zien in Oekraïne." Dat is, volgens Peterson, een van de redenen waarom de Oekraïners de AWS-cloud gebruiken.

En het vierde aspect waar klanten, volgens Peterson, naar op zoek zijn, is transparantie en onafhankelijkheid. "Ze willen precies kunnen begrijpen wat de cloud doet, zodat ze hem kunnen evalueren of beoordelen om er zeker van te zijn dat hij voldoet aan hun specifieke compliance-eisen. Ze willen weten dat ze onafhankelijk kunnen opereren."

EN DE REST?

Microsoft en Google hebben ook maatregelen en lanceringen rond digitale soevereiniteit uitgevoerd, in diverse vormen. Zo is er de *distributed cloud air-gapped*, helemaal afgesloten van het internet, en *cloud dedicated*, waar klanten met regionale data kunnen kiezen waar hun data wordt opgeslagen, vaak via onafhankelijke (Europese) operators. Een instapniveau is vaak *cloud data boundary*, waarbij klanten controle hebben over encryptie en toegangsrechten. Digitale soevereiniteit kent dus vele gradaties.



Max Peterson, VP sovereign cloud bij Amazon Web Services.



HOE CANVA DATA INZET OM WERELDWIJD 370 DESIGNS PER SECONDE TE VERWERKEN

Toen datawetenschapper Moe Kiss in 2019 bij Canva begon, was het Australische grafisch ontwerpplatform nog relatief onbekend. Canva, de uitdager van Adobe, telt inmiddels wereldwijd meer dan 230 miljoen maandelijkse gebruikers. “De schaal en complexiteit van onze dataset is aanzienlijk gegroeid”, zegt Moe Kiss in een gesprek. Om dat te kunnen verwerken, vertrouwt Canva op een moderne data-architectuur.

Canva verwerkt elke seconde 370 nieuwe ontwerpen. Dat betekent miljoenen datapunten per dag – van gekozen lettertypes en templates tot complete video's. "We moeten niet alleen met veel verschillende bestandsformaten omgaan. Ook **opslag is een behoorlijke uitdaging, vooral als je kijkt naar de verschillende bestandsformaten** en de grootte ervan", vertelt Moe Kiss, director of data science in marketing bij Canva, wanneer we haar spreken tijdens de Snowflake Summit, waar data en AI centraal stonden. Ze heeft het over inzet van data in haar eigen marketingdomein en bij Canva in het algemeen. Moe Kiss is als datawetenschapper ook host van de internationale data podcast **The Analytics Power Hour**.

"Toen ik in 2019 begon, zeiden mensen: 'Wat is Canva?' En nu lijkt wel iedereen het te gebruiken."

Databeheer is niet alleen cruciaal maar ook sterk geëvolueerd bij het Australische bedrijf. Waar het Canva-platform vroeger te maken had met uitval en vertragingen, draait het nu op een robuuste infrastructuur, met Snowflake als clouddataplatform, dat schaalbaar en betrouwbaar is. Kiss benadrukt dat dit een wereld van verschil heeft gemaakt: "De grootste winst voor mij is gewoon de betrouwbaarheid van ons platform. Als dingen werken en het moeiteloos gaat, vergeet je soms hoe moeilijk het vroeger was."

DATA MESH ALS FUNDAMENT

De datagroei dwong Canva om zijn architectuur fundamenteel anders in te richten. In plaats van enkele centrale datamodellen werkt het bedrijf nu met een data-mesh-aanpak. Hierbij worden **datasets opgesplitst in domein-specifieke tabellen**, waardoor verschillende teams zelfstandig kunnen werken. "In totaal gaat het om meer dan 70.000 tabellen. Dit maakt onze organisatie wendbaarder en zorgt ervoor dat data sneller beschikbaar zijn voor uiteenlopende toepassingen, van productontwikkeling tot marketinganalyse."

Naast Snowflake gebruikt Canva ook geïntegreerde data uit Google Analytics en andere bronnen om gebruikers-



Moe Kiss, director of data science in marketing bij Canva.

gedrag over verschillende klantsegmenten heen te begrijpen. Die inzichten beïnvloeden rechtstreeks productbeslissingen, zoals de introductie van Canva Sheets, een visueel-first spreadsheetapplicatie. "Het toont hoe data-analyse, verspreid over meerdere platforms, de koers van productontwikkeling kan bepalen."

AI ALS VERSNELLER

Naast de schaalbaarheid van de infrastructuur staat artificiële intelligentie centraal in Canva's datastrategie. "We zijn een AI-first company", omschrijft Moe het. Binnen marketing wordt AI bijvoorbeeld gebruikt voor lead routing: nieuwe leads worden automatisch geclassificeerd en zo snel mogelijk doorgestuurd naar hun CRM- en marketingplatform Salesforce. Hiervoor maakt Canva gebruik van Snowflake Cortex, een suite van AI-mogelijkheden die direct op de data kan worden toegepast. **"Een van de belangrijkste gebruiksscenario's in mijn team was voor onze B2B-leadrouting.** Het doel is om de snelheid naar lead te versnellen en ervoor te zorgen dat de gegevens van iemand die een formulier invult zo snel mogelijk bij Salesforce terechtkomen."

Een ander element is AI SQL, waarmee AI SQL-queries kan genereren en uitvoeren. Voor Canva opent dit de mogelijkheid om sneller beslissingen te nemen, bijvoorbeeld om te bepalen of een binnengekomen contact van hoge kwaliteit is of niet. Voorts kijkt Canva vooruit naar de inzet van semantic layers. Zo'n **semantic layer vertaalt complexe data naar zakelijke termen die voor iedereen begrijpelijk zijn.** "Zo ontstaat één eenduidige en betrouwbare laag voor analytics en AI, een 'single source of truth' die cruciaal is in onze omgeving met tienduizenden tabellen."

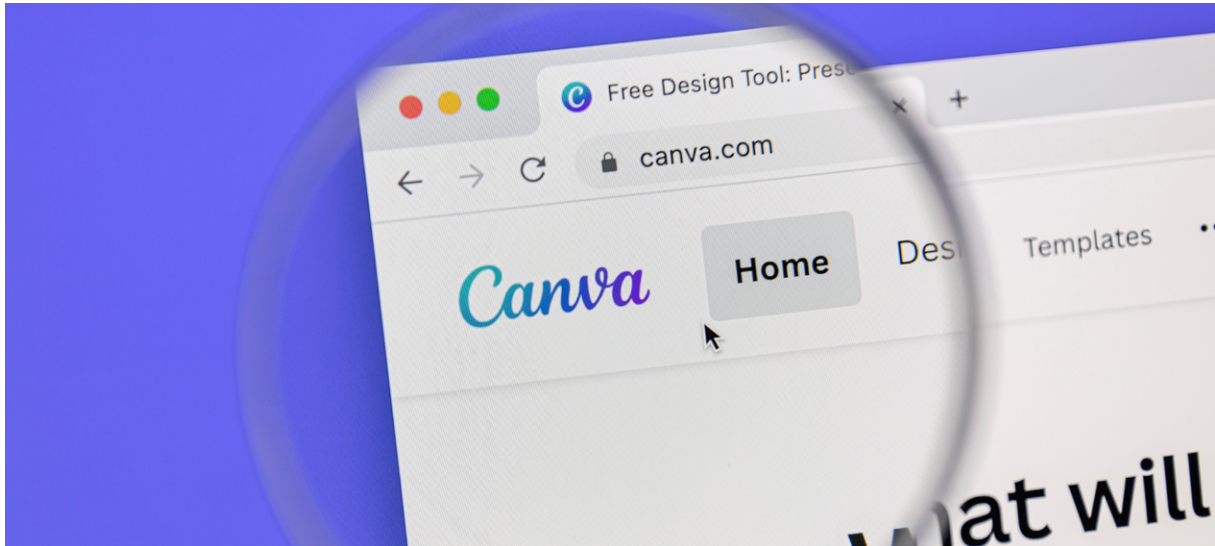
CANVA IN CIJFERS

Maandelijks actieve gebruikers: **230 miljoen**

Ontwerpen per seconde: **370**

Werknemers: **5.000**

Tabellen in data mesh: **70.000**



DE HOCKEYSTICKGROEI VAN CANVA

De technische fundamenteën maken het mogelijk om zowel consumenten als grote ondernemingen te bedienen. 95% van de Fortune 500 zijn klant, met prominente klanten zoals FedEx, Salesforce, Expedia, Reddit en Zoom. Toch blijft de consumenten-tak van het bedrijf heel belangrijk. “We willen absoluut niet de focus op onze kerngebruikers verliezen. En hun feedback is altijd heel belangrijk om de richting van het product te bepalen.”

Moe Kiss is zelf ook altijd een fervent gebruiker geweest. **“Ik begon bij Canva te werken omdat ik Canva gebruikte.** Ik organiseerde vroeger data-meetups. Ik zette het in voor mijn werk. Daarvoor gebruikte ik andere presentatieplatformen.”

“In totaal gaat het bij Canva om meer dan 70.000 tabellen in een data mesh-architectuur.”

Intussen is Canva een danige challenger voor bestaande grafische pakketten (lees: Adobe). “Toen ik in 2019 begon, vroegen mensen nog wat Canva eigenlijk was. Nu hoor ik vaak dat kinderen het voor school gebruiken, of zelfs dat een grootmoeder het onlangs heeft uitgeprobeerd”, vertelt ze. Het platform is ongelooflijk gegroeid. “Het is niet vaak dat je bij een bedrijf werkt waar je daadwerkelijk die hockeystickgroei ziet.”

DATAPERSONEN ZIJN WÉL CREATIEF

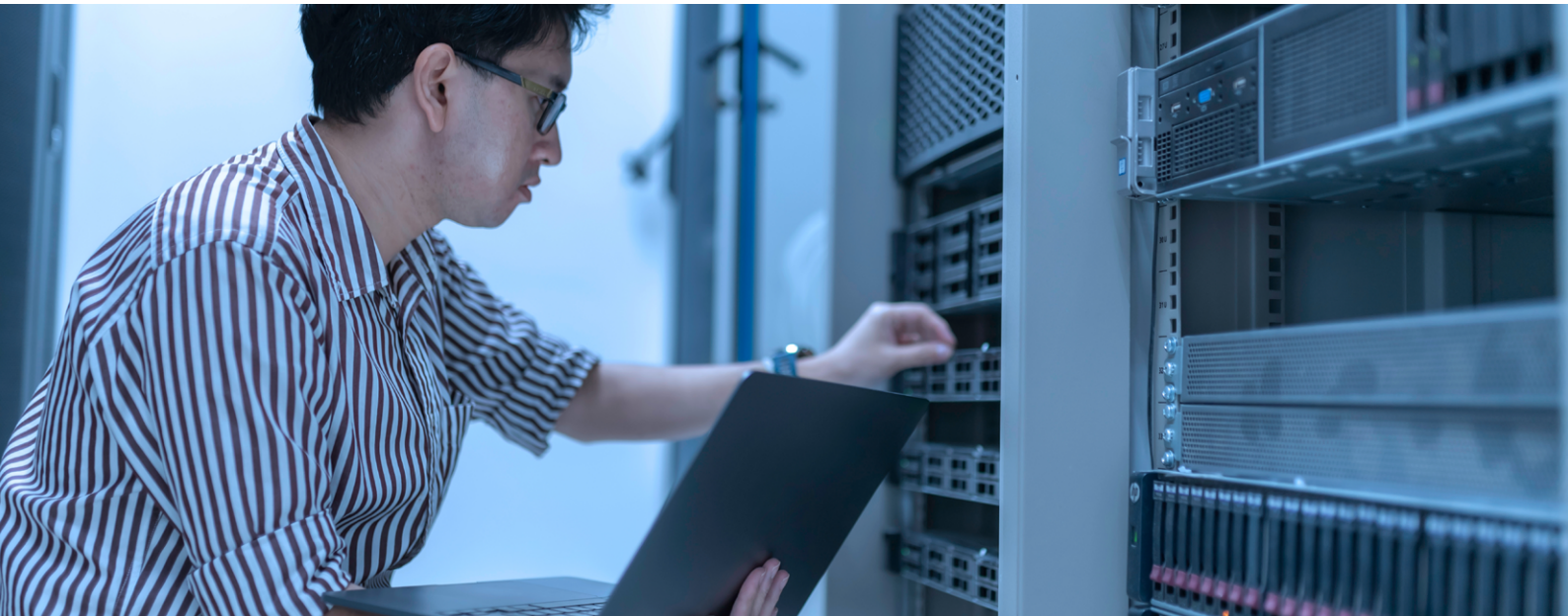
Canva laat zien dat een schaalbare data-architectuur en slimme inzet van AI onmisbaar zijn om hypergrowth te ondersteunen. Toch blijft de mens de kern. “Werken bij Canva heeft me **echt laten inzien dat je als data-persoon**

wel een visueel of creatief persoon kunt zijn. Het is nu zelfs iets waar ik diep om geef, vooral in functie van datavisualisatie.” Of zoals Kiss het samenvat: “Het zijn de tools die ons helpen sneller te werken, maar de mens staat nog altijd centraal.”

CANVA DATA-TECHNISCH

- De data-infrastructuur van Canva draait op **Snowflake** als clouddataplatform, waarbij zowel first-party als third-party data worden ingeladen in **AWS S3** voor opslag en verwerking. **Fivetran** verzorgt de integratie van third-party data, terwijl first-party data via een change-data-capture (CDC)-systeem wordt geëxtraheerd. **dbt** wordt ingezet voor data-transformatie, en via **Census** worden data gesynchroniseerd naar externe systemen.
- Voor visualisatie en exploratie gebruikt Canva **Looker** en **Mode**. Daarnaast wordt geëxperimenteerd met nieuwe AI-mogelijkheden zoals Snowflake Cortex Analyst.
- Ook gebruikt Canva geïntegreerde data uit **Google Analytics** en andere bronnen om gebruikersgedrag over verschillende klantsegmenten te begrijpen en productontwikkeling te sturen.

» Herbeluister **hier** de recente SAI Shorts-podcast over Data & AI.



VAN VSPHERE NAAR VRIJHEID

DE ZEVEN BESTE VMWARE- ALTERNATIEVEN

Sinds Broadcom de overname van VMware twee jaar geleden afrondde, staat de virtualisatiewereld op zijn kop. De overgang heeft geleid tot ingrijpende wijzigingen in het licentiemodel die voor veel organisaties forse kostenstijgingen opleverden. Maar wat is er precies veranderd en vooral: welke alternatieven bieden uitkomst? We vroegen het aan enkele specialisten.

VMware heeft zich de afgelopen jaren ontwikkeld tot een brede infrastructuurleverancier. Het portfolio omvat vSphere (servervirtualisatie en ESXi-hypervisor), vSAN (software-defined storage), NSX (netwerkvirtualisatie en security) en Aria (cloud management). Daarmee bood VMware een complete stack voor datacenters en hybride cloud. Het is al jaren een gevestigde waarde, maar sinds de overname door Broadcom is er veel veranderd voor de klanten. “De ingrepen door Broadcom hebben veel klanten wakker geschud”, stelt Stéphane Lahaye, managing director BeLux bij HPE.

WAT IS DE NIEUWE REALITEIT ONDER BROADCOM?

Het belangrijkste punt van verandering is de afschaffing van perpetual licenties voor nieuwe klanten. Waar organisaties vroeger eenmalig een licentie konden kopen, eventueel aangevuld met onderhoudscontracten, dwingt Broadcom nu een abonnementsmodel af. Bestaande perpetual licenties blijven wel geldig, maar kunnen na afloop niet meer worden verlengd of uitgebreid.

De aanpassingen veroorzaakten een aardverschuiving. “Al vanaf de prille geruchten op Reddit was het voor onze

licentiespecialisten alle hens aan dek. Door snel te schakelen, hebben we nog zoveel mogelijk klanten in de oude prijsformule kunnen verlengen, waardoor de druk van de ketel was”, vertelt Roel Van Looy, CTO bij VanRoey. “Zo kregen zij een extra jaar de tijd om – indien gewenst – een grondig beredeneerd migratietraject te plannen.”

“Het mag wel duidelijk zijn dat Microsoft de grote winnaar is in dit hele verhaal.”

De prijsstelling onderging dus een metamorfose. Hoewel Broadcom beweert dat de prijzen van abonnementen zijn verlaagd, rapporteren vele organisaties juist een **kostenstijging van 150 tot 300%** bij vernieuwing.

GEEN LICENTIES, MAAR BUNDELS

Dit komt niet alleen door de overstap van core- naar socket-licenties (VMware rekende al per socket), maar vooral doordat Broadcom losse licenties heeft vervangen door bundels zoals hun Cloud Foundation. **Klanten worden hierdoor gedwongen meer functionaliteit af te nemen dan ze nodig hebben**, wat de kosten fors opdrijft.

“Veel organisaties voelen zich door Broadcom met de rug tegen de muur gezet”, vindt Wesley Kerrebrouck, IT-consultant bij Network-IT. “Waar men vroeger zelf kon kiezen welke modules men nodig had, worden klanten nu verplicht tot dure bundels. Dat zet bedrijven aan het denken over hun afhankelijkheid van één leverancier.” Bovendien vereist het nieuwe model doorgaans een commitment van drie jaar in plaats van de gebruikelijke één jaar.



Het productportfolio is drastisch vereenvoudigd. Veel gespecialiseerde producten en diensten zijn geschrapt, waardoor organisaties gedwongen worden naar duurdere enterprise-versies te migreren, ook al hebben ze de extra functionaliteit niet nodig. Erik Moreau, technical supervisor field system engineers bij Aurelium, vat het als volgt samen: “Wat vroeger een transparant licentiemodel was, is **nu een bundelstructuur die niet altijd aansluit bij de noden van onze klanten**. Dat maakt kosteninschatting en budgettering complexer.”

DE ALTERNATIEVENRACE: VOOR WIE WIL OVERSTAPPEN

Overstappen naar een nieuwe hypervisor-leverancier is helaas niet zo eenvoudig als wisselen van energieleverancier bijvoorbeeld, vergelijkt Roel Van Looy van VanRoey. “Het gaat gepaard met een heus migratietraject waarbij iedere virtuele machine zorgvuldig overgezet moet worden. De hamvraag bij de meeste bedrijven is dan ook: **wegen de kosten, impact en mogelijke risico's van dit traject op tegen de gestegen kosten van VMware?** Broadcom anticipeert natuurlijk dat organisaties de weg van de minste weerstand kiezen en gewoon meer betalen.”

“De keuze voor een alternatief platform hangt sterk af van de interne expertise. Een oplossing als Proxmox vraagt een ander profiel dan Nutanix of Hyper-V.”

Organisaties die zoeken naar een uitweg uit deze kostenstijging, kunnen verschillende paden bewandelen.

1

MICROSOFT HYPER-V

Microsoft Hyper-V vormt voor Windows-gecentreerde omgevingen een logische keuze. De Hyper-V-rol is al opgenomen in Windows Server en biedt een solide virtualisatieoplossing zonder extra licentiekosten voor de hypervisor zelf. Organisaties betalen alleen voor de Windows Server-licenties van hun virtuele machines.

“Gezien onze jarenlange specialisaties in Microsoft en HPE zijn Hyper-V en Morpheus (zie 4) logische keuzes. Zelf hadden wij al jaren ervaring met Microsoft Hyper-V waardoor vele klanten inmiddels overgeschakeld zijn”, weet Roel Van Looy. **“AI is het (nog) geen perfect alternatief**, het mag wel duidelijk zijn dat Microsoft de grote winnaar is in dit hele verhaal.”

Hyper-V integreert naadloos met het ecosysteem van Microsoft en biedt goede prestaties voor Windows-workloads. Voor organisaties met gemengde Linux/

Windows-omgevingen kan het echter beperkingen hebben in geavanceerde functies die VMware wel biedt. Kostentechnisch kan dit zeer aantrekkelijk zijn, vooral voor bedrijven die al zwaar investeren in Microsoft-licenties. “Hyper-V is een solide keuze voor Windows-omgevingen”, erkent Erik Moreau van Aurelium. “Maar we merken dat **Hyper-V minder geschikt is voor gemengde Linux-workloads** zonder extra tuning.”

2

PROXMOX

Proxmox biedt een opensourcealternatief dat vooral aantrekkelijk is voor kostenbewuste organisaties of die met sterke Linux-competenties. Het platform ondersteunt zowel KVM-virtualisatie als LXC-containers.

Het is misschien minder bekend, maar wel van tel. “Proxmox zien we vaak terug bij organisaties die maximale flexibiliteit willen behouden en kosten willen drukken”, zegt Wesley Kerrebrouck van Network-IT. “Maar men moet zich bewust zijn dat dit ook meer Linux-knowhow vereist en minder enterprise-support biedt dan VMware.”

Voor organisaties met sterke Linux-kennis is Proxmox een verrassend krachtig alternatief, vult Erik Moreau aan. “Het vraagt wel meer technische maturiteit, maar biedt ongeziene vrijheid.”

3

NUTANIX

Nutanix positioneert zich als de enterprise-vervanger bij uitstek. Het platform combineert compute, storage en virtualisatie in één hyperconverged infrastructure (HCI)-oplossing. Nutanix biedt een eigen hypervisor (AHV) die gratis wordt geleverd, waardoor kosten voornamelijk zitten in de hardware en managementsoftware.

Voor middelgrote tot grote organisaties die een volledig geïntegreerde oplossing met enterprise-support zoeken, vormt Nutanix een aantrekkelijk alternatief. De totale eigendomskosten liggen vaak lager dan bij VMware, vooral bij schaalvergroting.

4

HPE & MORPHEUS

HPE biedt meerdere opties voor virtualisatie en cloud-beheer. HPE SimpliVity vertegenwoordigt de hyperconverged infrastructuur (HCI) van HPE, terwijl HPE Morpheus fungeert als onafhankelijk multi-cloudmanagement- en automationplatform is. “Dankzij onder meer de overname van Morpheus profileren wij ons als geloofwaardig VMware-alternatief”, aldus Stéphane Lahaye.

Voor organisaties die hun IT-omgeving willen standaardiseren en automatiseren, vormt Morpheus een krachtig



“Bij cloud gaat het om het vinden van de juiste balans tussen schaalbaarheid, kosten en controle”, stelt Erik Moreau van Aurelium.

alternatief, met name voor vSphere. Het platform is niet hardwaregebonden, al positioneert HPE het vooral in combinatie met de eigen infrastructuur.

5

RED HAT OPENSIFT VIRTUALIZATION

Red Hat OpenShift Virtualization combineert traditionele VM-workloads met moderne containerorkestratie op Kubernetes. “De onzekerheid rond de nieuwe tarifiering van VMware heeft ons bevestigd in onze keuze voor OpenShift”, erkent Steven Van Peteghem, I&T operations directeur bij VDAB dat OpenShift gebruikt.

Dit platform is vooral interessant voor organisaties die zowel legacy-applicaties als moderne cloud-native workloads draaien. De licentiekosten zijn gebaseerd op het aantal nodes, vergelijkbaar met andere enterprise Kubernetes-distributies. Voor organisaties die inzetten op modernisering en DevOps-praktijken biedt dit een toekomstbestendige optie, al vereist het wel significante expertise in Kubernetes-technologieën.

6

CITRIX HYPERVISOR

Citrix Hypervisor is een krachtige type-1-hypervisor die een VMware vSphere kan vervangen. Het is vooral een populair alternatief voor organisaties die zwaar leunen op Virtual Desktop Infrastructure (VDI).

Hoewel het ook functionaliteit biedt voor servervirtualisatie, wordt Citrix Hypervisor in de praktijk vooral ingezet door organisaties die al sterk investeren in het Citrix-ecosysteem.

7

CLOUD (AWS, AZURE & GOOGLE CLOUD)

Cloudmigratie naar een van de grote hyperscalers vormt een fundamenteel ander pad. Amazon Web Services (AWS) biedt naast VMware Cloud on AWS ook native diensten zoals EC2. Microsoft Azure heeft vergelijkbare diensten met Azure Virtual Machines, terwijl Google Cloud inzet op containergebaseerde workloads.

Daarnaast kan OpenStack een alternatief zijn voor organisaties die een eigen private cloud willen opbouwen. Het opensourceplatform bestaat uit modulaire componenten voor computing, storage en netwerken.

Het model van cloud is uiteraard anders. "Cloud is geen goedkoop alternatief voor VMware, tenzij je workloads variabel en schaalbaar zijn", merkt Wesley Kerrebrouck van Network-IT op. "Voor stabiele omgevingen blijft on-premises vaak financieel voordeliger. Het gaat dus om de juiste balans tussen flexibiliteit en kostenefficiëntie."

Erik Moreau van Aurelium sluit zich hierbij aan: "Cloud is niet altijd de heilige graal", stelt hij. "Voor voorspelbare workloads blijft on-premises vaak efficiënter. Het gaat om het vinden van de juiste balans tussen schaalbaarheid, kosten en controle."



"De beslissingen van Broadcom zetten bedrijven aan het denken over hun afhankelijkheid van één IT-leverancier", zegt Wesley Kerrebrouck van Network-IT.



CONTRACTBREUK? BRITSE SUPERMARKT EIST 126 MILJOEN EURO VAN VMWARE

De Britse supermarktketen Tesco eist 110 miljoen pond (zo'n 126 miljoen euro) van Broadcom wegens contractbreuk met betrekking tot VMware-licenties. Tesco kocht in 2021 permanente licenties voor vSphere en Cloud Foundation, samen met abonnementen op Veeva's Tanzu-producten, en sloot een contract voor software-updates en ondersteuning tot 2026.

Na de overname van VMware door Broadcom stopte Broadcom echter de verkoop van ondersteuning voor deze permanente licenties. Volgens Tesco moeten ze hierdoor nu 'buitensporige prijzen' betalen voor software waarvoor ze eigenlijk al hebben betaald.

VIRTUALISATIE-ALTERNATIEVEN: WAARVOOR KIEZEN?

De keuze tussen alternatieven hangt af van verschillende factoren: de huidige VMware-investering, technical debt, beschikbare expertise, budget en strategische IT-richting. Organisaties met zware Windows-omgevingen zullen anders afwegen dan Linux-first bedrijven.

Een overstap moet je niet puur op prijs baseren, benadrukt Wesley Kerrebrouck. "Hyper-V is bijvoorbeeld interessant in Windows-omgevingen, maar voor Linux-zware workloads is Proxmox vaak logischer. Het gaat erom dat je **een platform kiest dat past bij je lange-termijnstrategie**, niet alleen bij je kortetermijnbudget."

KWESTIE VAN EXPERTISE

Experts raden vaak een hybride aanpak aan. In de praktijk blijkt dat vaak het meest realistisch: behoud VMware voor kritieke workloads op korte termijn, maar migreer geleidelijk naar alternatieven waar dat kosteneffectief en operationeel verantwoord is. Dit vermijdt big-bangmigraties, maar geeft wel tijd om expertise op te bouwen en ervaringen op te doen met nieuwe platforms.

Uiteindelijk draait het om de kennis (lees: de mensen) die je in huis hebt. "De keuze voor een alternatief platform hangt sterk af van de interne expertise", beaamt Erik Moreau. "Een oplossing als Proxmox is technisch sterk, maar vraagt een ander profiel dan bijvoorbeeld Nutanix of Hyper-V."

GEFASEERDE MIGRATIE

Wat duidelijk is: de overname van VMware door Broadcom heeft de virtualisatiemarkt opengebroken. "Organisaties doen er goed aan hun infrastructuurs-trategie kritisch te herbekijken. **Er bestaat geen one-size-fits-all-alternatief**. De keuze hangt af van workloadprofiel, expertise en budget", stelt Wesley Kerrebrouck van Network-IT.

De overstap van VMware naar een alternatief is bovendien zelden plug-and-play, haalt Moreau aan. "We merken dat een gefaseerde aanpak met duidelijke workloadanalyse het verschil maakt tussen succes en frustratie."

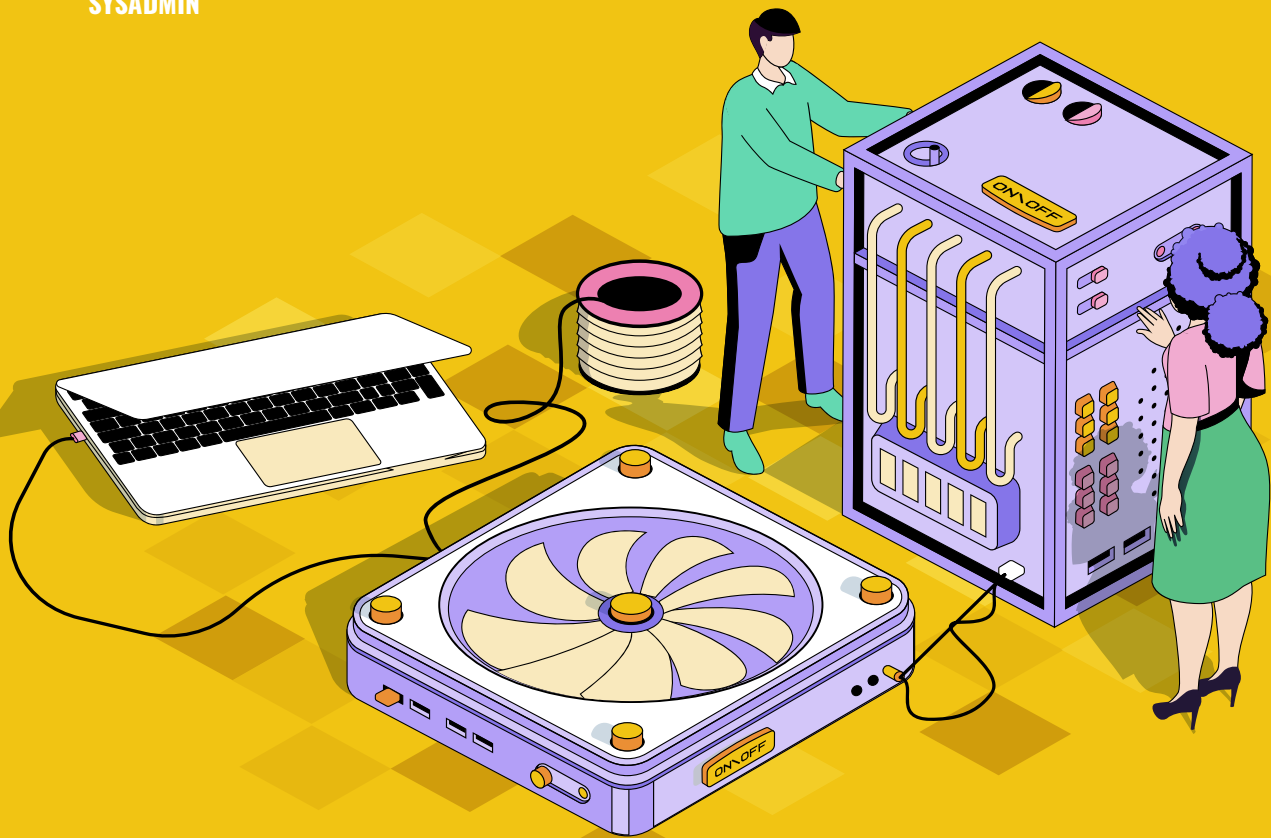
Wat Kerrebrouck in de praktijk ziet, is een gefaseerde migratie. "Die is het meest realistisch en kosten-efficiënt. Bedrijven die vandaag al alternatieven testen, hebben morgen de vrijheid om onafhankelijk te beslissen – en dat is precies de les die Broadcom ons onbedoeld geleerd heeft."

PIJNLIJKE VASTSTELLING

Roel Van Looy sluit nog af met een uitsmijter. "Het blijft het een pijnlijke vaststelling om te zien hoe afhankelijk we blijven van niet-Europese spelers", meent hij. "Het zou mooi zijn mochten we vroeg of laat ook een lokale speler kunnen aanbieden."

Alternatief	Mate van VMware-ervanging	Primaire focus	Kostenstructuur
VMware (vSphere, vSAN, NSX, Aria)	Referentie (volledig stack)	Servervirtualisatie, storage, netwerk, cloudbeheer	Abonnementen via VMware Cloud Foundation (driejarig commitment, bundelprijzen)
Microsoft Hyper-V	Hoog voor Windows-workloads	Windows-centrische datacenters	Hypervisor inbegrepen in Windows Server-licenties
Nutanix (AHV)	Hoog	Hyperconverged infrastructuur (HCI)	Licenties voor management + hardware
HPE Morpheus / SimpliVity	Middelhoog	Cloud management (Morpheus) + HCI (SimpliVity)	Softwarelicenties + hardware (SimpliVity)
Proxmox VE	Middel	Open source, KVM/LXC	Gratis (open source) + optionele support
Red Hat OpenShift Virtualization	Middelhoog	Kubernetes + VM-integratie	Node-gebaseerde abonnementen
Citrix Hypervisor	Middel	VDI en Citrix Virtual Apps & Desktops	Abonnementen/licenties via Citrix
Public Cloud (AWS, Azure, GCP)	Hoog (maar fundamenteel anders)	IaaS, schaalbaarheid, modernisering	Pay-as-you-go (op basis van verbruik)
OpenStack	Middel	Private cloud, vendor-neutraal	Open source, implementatie + beheercomplexiteit

» Bekijk of herbekijk **hier** de SAI Shorts over infrastructuur.



DE LANGE CARRIÈRE VAN DE SYSTEM ADMINISTRATOR

Moeten er in een tijdperk waarin cloudplatformen en artificiële intelligentie het IT-landschap domineren nog system administrators zijn? De rol van de sysadmin is niet simpelweg verdwenen, maar radicaal veranderd. "Het is een kwestie van aanpassen om relevant te blijven."

Ooit was de sysadmin het kloppend hart van een IT-afdeling. Vanaf de jaren tachtig tot ver in de jaren 2000 waren zij verantwoordelijk voor zo-wat alles wat met (back-end)computers en infrastructuur te maken had:

servers installeren, updates uitrollen en storingen oplossen. Sysadmins beheerden fysieke machines en draaiden commando's in command line-omgevingen om systemen overeind te houden.

DAAR IS DE CLOUD

Maar vanaf 2010 veranderde hun rol fundamenteel. Cloud computing maakte fysieke hardware grotendeels overbodig. Automatisering en infrastructuur-als-code zorgden

ervoor dat één sysadmin niet langer tien, maar honderden servers kon beheren. En met de opkomst van DevOps werden de muren tussen ontwikkeling en beheer gesloopt: sysadmins werden geacht ook code te schrijven en mee te draaien in softwareteams.

Volgens Eamonn O'Neill, mede-oprichter en CTO van Lemongrass, betekende dit voor velen het einde van een carrière, en voor anderen een doorstart. "Voor sommige sysadmins waren deze veranderingen positief. Wie wat codeerervaring had en infrastructuur-als-code kon inzetten, automatiseerde de saaie taken en verhoogde tegelijk zijn waarde voor de organisatie."

DAAR IS AI

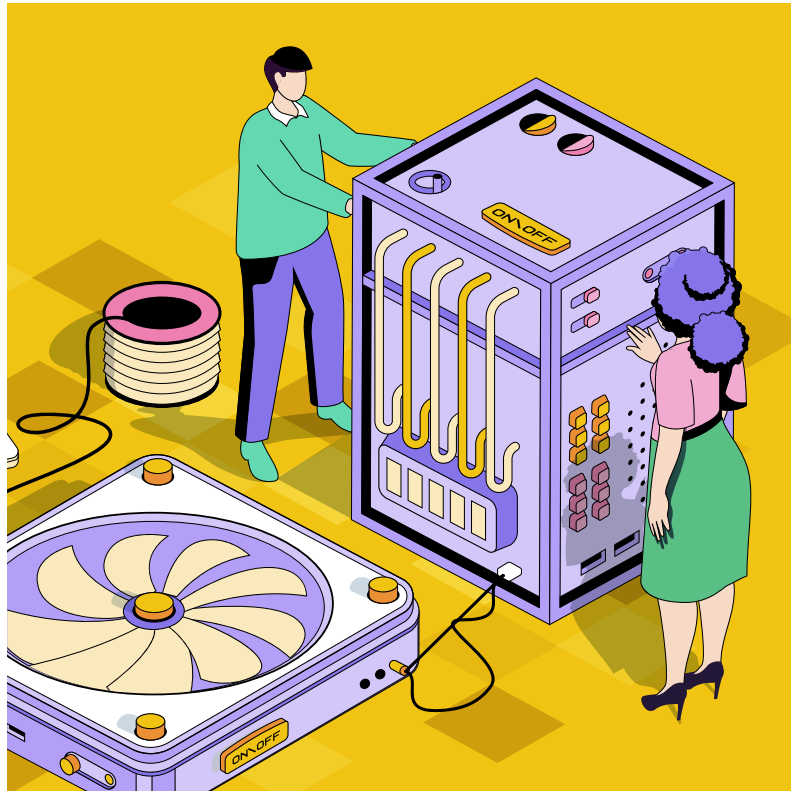
Vandaag ondergaat de IT-sector opnieuw een disruptie, dit keer door artificiële intelligentie. En ook hier zal de sysadmin mee moeten leren omgaan. **"IT-professionals die AI leren inzetten als 'sidekick', in plaats van het te zien als vervanger, zullen floreren"**, zegt O'Neill. "Het idee dat technologie IT-rollen volledig zou elimineren, zoals ooit voorspeld werd met het concept 'NoOps', is nooit uitgekomen. Artificiële intelligentie zal IT'ers niet vervangen, maar net krachtiger maken."

"Automatisering, cloud, AI en security hebben de rol van system administrator totaal doen veranderen."

Het verleden leert volgens O'Neill dus: wie vasthoudt aan oude routines, verliest terrein. Maar wie zich openstelt voor nieuwe tools en leert samenwerken met technologie, versterkt zijn positie.

DAAR IS CYBERSECURITY

En dan is er nog een andere trend, die impact heeft op de job, naast automatisering, cloud en AI. Flink



wat system administrators hebben hun job naar security zien evolueren. Zo liet het vakblad *Silicon Republic* recent John Donohoe, nu senior cybersecurity engineer bij Fidelity Investments, aan het woord. Hij startte er als sysadmin, beheerde duizenden computers, rolde patches en software uit en leerde zichzelf automatiseren met scripts.

Toch koos hij enkele jaren geleden voor een overstap naar cybersecurity én een andere invulling. "Als system administrator dacht je vooral aan technische problemen, hun oplossingen en hoe je die toepast", vertelt hij. "In cybersecurity denk je aan problemen, oplossingen én de risico's. Dat maakt dat je IT-systemen op een heel andere manier moet bekijken. Het kostte me **tijd om me dat nieuwe denkpatroon eigen te maken.**"

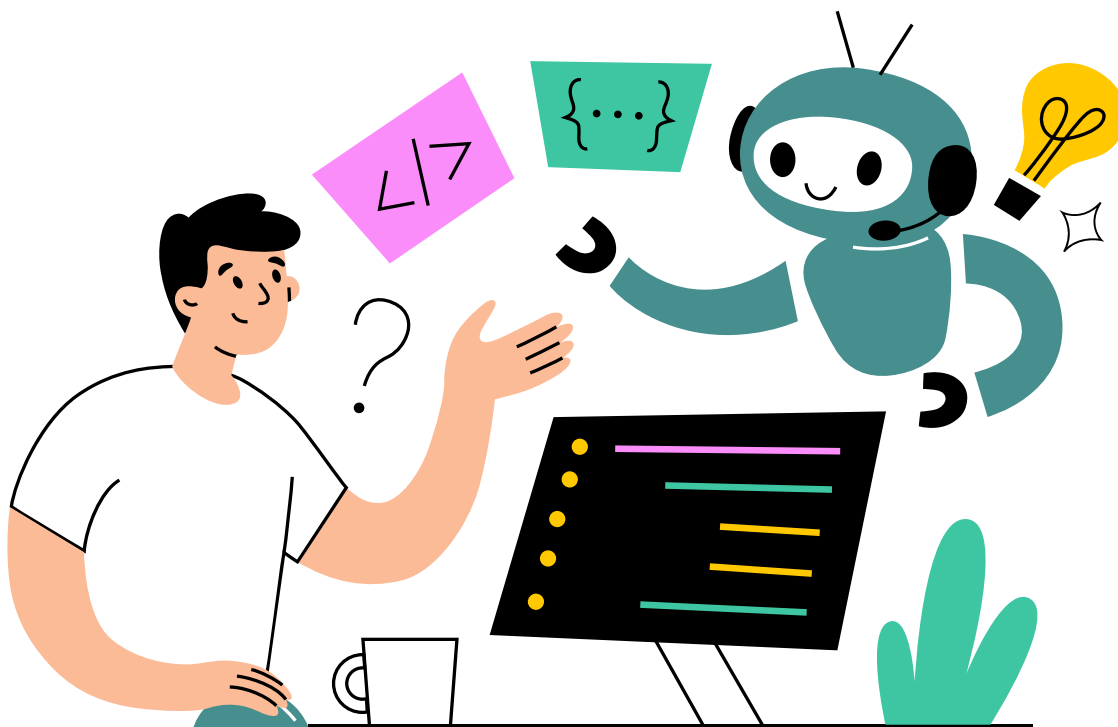
De sysadmin-taken die hij ooit deed, bestaan volgens hem nog altijd, maar vaak in andere functies of geïntegreerd in bredere rollen.

NIET VERDWIJNEN, WEL TRANSFORMÉREN

Kortom, de klassieke sysadmin, die servers in het eigen datacenter patcht, is zeldzaam geworden. Maar de kern van het werk – systemen draaiend houden, problemen oplossen, risico's afwegen – leeft vooral voort in nieuwe functies: cloud engineer, DevOps-specialist of zelfs cybersecurity-expert.

"De vraag is niet of de sysadmin nog bestaat, maar hoe snel IT-professionals zich aanpassen om relevant te blijven."

Net zoals de rol van de sysadmin ooit werd heruitgevonden door cloud en automatisering, zal AI een volgende gedaantewisseling afdwingen, schat Eamonn O'Neill in. "De vraag is niet of de sysadmin nog bestaat, maar hoe snel IT-professionals zich aanpassen om relevant te blijven."



DAAR ZIJN DE AGENTS

5 FEITEN OVER AGENTIC AI

Sinds een jaar trekt agentic AI steeds meer aandacht en duiken er steeds meer testprojecten op. Volgens Capgemini zien bedrijven de eerste concrete toepassingen vooral in klantenservice, IT en sales – domeinen waar agents processen kunnen automatiseren en versnellen. Maar wat maakt een AI-agent nu écht anders? En waar zitten de risico's die vaak onderbelicht blijven?

FEIT 1 AGENTIC AI IS GEEN DURE CHATBOT

De eerste verwarring ontstaat al bij de naam. Veel leveranciers voorzien hun chatbots of gescripte workflows van het label 'agentic', in de hoop mee te liften op de hype. Toch is er een wezenlijk verschil. Een chatbot of beslisboom kan prima antwoorden geven, maar zodra de gebruiker buiten het script gaat, loopt het systeem vast. Agentic AI hoort juist **zelfstandig** te redeneren en beslissingen te nemen die niet expliciet zijn geprogrammeerd.

Glenn Nethercutt, CTO van Genesys, zegt hierover: **"Veel leveranciers plakken nu al het label 'agentic' op systemen die niet meer zijn dan gescripte workflows of beslisbomen."** Wie dus denkt dat een slimmere chatbot of voicebot al meteen een AI-agent is, zit ernaast. Echte agentic AI onderscheidt zich doordat het de context begrijpt, beslissingen onderbouwt én actie onderneemt zonder dat iedere stap vooraf vastligt.

FEIT 2 AGENTS HEBBEN NIET ALTIJD LLM'S NODIG

Een tweede hardnekkige misvatting is dat AI-agents per definitie draaien op large language models. Zeker sinds de opkomst van ChatGPT lijkt het alsof alle vooruitgang in AI rond LLM's draait. In werkelijkheid vormen enterprise data en bestaande AI-modellen vaak de basis. **"Een AI-agent is een systeem dat verschillende intelligente modules aan elkaar koppelt en gebruikt om je zo goed mogelijk te assisteren"**, stelt Véronique Van Vlasselaer, analytics & AI lead bij SAS. "Een LLM heeft geen toegang tot tools en het ontbreekt ook aan connectie met data, analytische rapporten of AI-modellen."

Fraudebestrijding is een goed voorbeeld, vindt Véronique Van Vlasselaer. Banken gebruiken al decennia systemen die patronen en afwijkingen in transacties detecteren. Vandaag noemen we dat een AI-agent, terwijl het in de jaren negentig 'data mining' heette. **"Voor het detecteren van fraude is een LLM niet noodzakelijk"**, merkt Van Vlasselaer op. "Toch kan een bank in bepaalde toepassingen wel profiteren van integratie met zo'n LLM." Ze illustreert dit met een toepassing bij de National Bank of Greece waarbij een model de vertaalslag maakt naar het Grieks. "Hierdoor kunnen agents in de moedertaal van klanten communiceren en analyseren."

"In wezen verschillen enterprise AI-agents niet veel van de modellen die we al jaren gebruiken."

Véronique Van Vlasselaer, analytics & AI lead bij SAS

De les voor IT'ers: kijk niet alleen naar de hype rond taalmodellen, maar naar de kwaliteit van je data en de bestaande assets waarop een agent kan steunen. "In wezen verschillen enterprise AI-agents niet veel van de modellen die we al jaren gebruiken", benadrukt Véronique Van Vlasselaer. De kern van de gebruikte modellen kan volgens haar vergelijkbaar zijn, maar **de 'agentic' eigenschap zit juist in de extra autonomie en redeneringslaag**. "Zodra ze meer autonomie krijgen en verrijkt worden met LLM-toepassingen, moeten we voldoende aandacht besteden aan governance."

FEIT 3 DE ECHTE UITDAGING IS GOVERNANCE EN ACCOUNTABILITY

Dat brengt ons meteen bij feit 3. In discussies rond agentic AI gaat de aandacht vaak naar technische vragen: welk platform kies je, welke API's gebruik je, welke frameworks zijn er beschikbaar? Maar de grootste uitdaging ligt bij proces en governance. Hoe stel je grenzen? Hoe maak je beslissingen traceerbaar? En hoe zorg je dat iemand altijd verantwoordelijk blijft voor wat een agent uitvoert?

Véronique Van Vlasselaer,
Analytics & AI Lead bij SAS.



DRIE KLASSIEKE TOEPASSINGEN VAN AGENTIC AI

1. Klantenservice: Een agent die niet alleen antwoord geeft op een vraag over een bestelling, maar ook zelfstandig de tracking-informatie opzoekt, een verzendvertraging signaleert en direct een compensatievoorstel naar de klant stuurt, zonder menselijke tussenkomst.

2. IT: Een agent die een storingsmelding krijgt over een server, zelf de logs analyseert, de oorzaak identificeert, een herstart uitvoert en daarna automatisch een rapport opstelt voor het IT-team.

3. Sales: Een agent die de verkoophistorie en online activiteit van een prospect analyseert, automatisch een persoonlijk aanbod genereert, en proactief een opvolg-e-mail verstuurt en contactmomenten plant. Zodat de menselijke salesmedewerker zich kan richten op het afronden van de deal.

Van Vlasselaer benadrukt het belang van vangrails: “Net zoals menselijke collega’s heeft ook AI bepaalde regels nodig waarbinnen het systeem mag functioneren. **Governance is nodig om de grenzen van die omgeving vast te leggen**”, benadrukt ze. “Wat mag een AI-agent doen? En vooral, wat mag hij niet doen?”

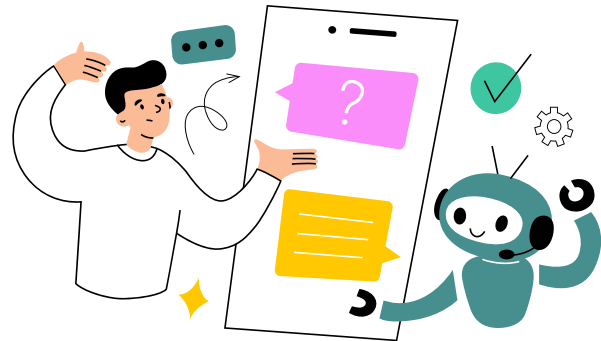
Denk aan beleidslijnen, logsystemen en monitoring waarmee beslissingen herleidbaar zijn, of beleid dat expliciet vastlegt welke acties een agent wél of niet mag uitvoeren. Governance gaat dus niet alleen over techniek, maar ook over accountability en procesafspraken die bijvoorbeeld menselijke controle verankeren.

FEIT 4 AUTONOMIE BETEKENT NIET ONBEGRENSD

Het woord ‘autonomie’ klinkt aantrekkelijk, maar roept ook misverstanden op. Een AI-agent die volledig zelfstandig zijn gang gaat, is in de praktijk eerder een risico dan een kans. Waar governance draait om beleid en verantwoordelijkheid, gaat het hier om operationele beperkingen in de praktijk.

Te veel vrijheid leidt tot fouten die mensen vanzelfsprekend vermijden. Vaak gaat het om banale zaken. Aravind Chandramouli, vice president AI Center of Excellence bij Tredence, wijst in *Infoworld* op een concreet probleem: “In sommige tests waren meer dan 30% van de *multi-agent failures* het gevolg van agents die dachten dat de taak voltooid was terwijl dat niet zo was.”

Zulke operationele fouten tonen dat autonomie altijd gradueel moet worden opgebouwd en gecontroleerd getest. IT-teams doen er, volgens hem, goed aan de bevoegdheden van een agent in eerste instantie scherp af te bakenen en pas later uit te breiden. Dat voorkomt dat projecten mislukken en dat vertrouwen vroegtijdig verdamppt.



FEIT 5 AGENTS ZIJN GEEN VERVANGING VAN MENSELIJKE DENKKRACHT

Misschien wel de grootste misvatting is dat AI-agents de mens zullen vervangen. In werkelijkheid ligt hun kracht in herhaalbare, doelgerichte taken: IT-verzoeken afhandelen, softwareontwikkeling versnellen of datasets analyseren. Ze nemen repetitieve stappen weg, maar missen diep begrip, context en het vermogen om complexe afwegingen te maken.

Aravind Chandramouli verwoordt het scherp: “**Agents zijn sterk met doelgerichte en herhaalbare taken. Ze zijn niet klaar om diep menselijk denken te vervangen.**” Dat betekent dat ook de rol van IT’ers niet verdwijnt, maar verschuift. Ze worden regisseurs die bepalen welke taken een agent krijgt, welke kaders gelden en waar menselijk oordeel onmisbaar blijft. Daarmee is de toekomst van agentic AI niet die van de digitale werknemer die de mens verdringt, maar die van de digitale collega die processen versnelt – mits iemand de regie stevig in handen houdt.

AGENTIC AI IN CIJFERS

- **450 miljard dollar** potentiële economische waarde tegen 2028, via omzetgroei en kostenbesparing.
- **93%** van leidinggevendenden verwacht binnen twaalf maanden concurrentievoordeel door AI-agents.
- **14%** van de organisaties gebruikt AI-agents al (12% deels, 2% volledig).
- **23%** is bezig met proefprojecten, 61% onderzoekt of bereidt toepassing voor.
- **82%** mist nog een volwassen AI-infrastructuur, minder dan 20% heeft data op orde.
- Vertrouwen daalt: slechts **27%** vertrouwt volledig autonome agents (vorig jaar nog 43%).
- Grootste zorgen: privacy (**51%**), bias en transparantie.
- Ook medewerkers zijn ongerust: **61%** vreest dat agents hun job zullen beïnvloeden.

Bron: Capgemini, 2025



VAN PIRAMIDES NAAR PLATFORMS

EGYPTE IN OPMARS ALS IT-BESTEMMING

Egypte rukt snel op als een onverwachte groeier in de wereld van IT-outsourcing. Het land investeert massaal in datacenters en digitale infrastructuur en profileert zich als een stabiel alternatief in een onrustige regio. Multinationals als Capgemini zien Egypte inmiddels niet meer alleen als goedkope uitvalsbasis, maar als serieuze hub voor innovatie en AI.

Als het over IT gaat, duikt Egypte amper op in het nieuws. Een uitzondering was een brand deze zomer in een datacenter van Telecom Egypt in Caïro. Vier medewerkers kwamen om, 22 anderen raakten gewond door rookinhalatie.

Het incident leidde tot storingen in telefoonverkeer en online-bankdien-

sten, al werden die binnen een dag grotendeels hersteld. Een tragische klap, en een erg valse noot in de plannen van Egypte om zich als IT-locatie te positioneren.

Vandaag telt Egypte meer dan 260 outsourcingcentra, waarvan 190 onder beheer van internationale spelers.

GROEIENDE DATACENTERHUB

Vergis je niet: Egypte is bezig aan een inhaalrace, te beginnen met de uitbouw van de infrastructuur. Het land is na Zuid-Afrika het tweede datacenterland van het continent. Zowel de overheid als internationale bedrijven als Orange Business en Khazna Data Centers steken miljarden in nieuwe capaciteit. Op dit

moment wordt het eerste nationale overheidsdatacenter gebouwd, gericht op cloud computing en met aandacht voor duurzame energie.

De ambitie is duidelijk: Egypte wil zich ontwikkelen tot regionaal digitaal knooppunt en tegelijk zijn digitale soevereiniteit vergroten. **“Egypte blijft ook aantrekkelijk dankzij zijn neutrale positie in conflicten.** De regio maakt momenteel een periode van grote onrust door, gekenmerkt door aanhoudende conflicten in en tussen landen als Israël, Libanon en Iran. Of denk aan de spanningen tussen Syrië en Jemen”, stellen Kanishka Chakraborty en Parul Jain van Everest Group. “Maar het land heeft geen verstoringen gekend in servicelevering.”

OUTSOURCING IN DE LIFT

Volgens cijfers van de Egyptische overheid hebben 74 outsourcing-bedrijven tussen 2022 en 2024 in totaal 60.000 IT-profielen aangeworven. Vandaag telt Egypte meer dan 260 outsourcingcentra, waarvan 190 onder beheer van internationale spelers.

In Kearney's Global Services Location Index 2023 staat het land op de 23ste plaats van 78 markten, waarbij India op de eerste plek staat.

Minister van Communicatie Amr Talaat benadrukte de ambitie van Egypte recent in een gesprek met de Indiase ambassadeur Suresh Reddy. De aanleiding was de uitbreiding van de bilaterale ICT-samenwerking tussen beide landen. “Onze **ICT-sector heeft een groeiende rol als belangrijke motor van de Egyptische economie**, met name op het gebied van outsourcing.”

KRITIEK BLIJFT

Toch zijn er kanttekeningen. Research manager Arjun Singh van Kearney wijst op structurele uitdagingen: de munt verzwakte fors tegenover de dollar, de publieke



Hossam Seifeldin, de CEO van Capgemini Egypte

schuld loopt op en Egypte scoort laag op technologische innovatie-intensiteit.

“Egypte positioneert zich niet alleen als low-costlocatie, maar ook als innovatiehub.”

Kanishka Chakraborty en Parul Jain van Everest Group

Al zijn er volop inspanningen om dat te keren. Via publiek-private samenwerkingen worden jonge IT'ers beter voorbereid op de arbeidsmarkt en krijgen ze toegang tot opleidingen in opkomende technologieën.

CAPGEMINI KIEST EGYPTE VOOR AI

Het meest zichtbare bewijs van Egypte's transformatie komt van **Capgemini, dat in april 2025 aankondigde een AI Center of Excellence te openen in Caïro.** Het Franse adviesbureau wil er zijn personeelsbestand verdubbelen tot 1.200 medewerkers en generatieve AI-projecten ontwikkelen voor sectoren als energie, farma en luchtvaart.

Hossam Seifeldin, de CEO van Capgemini Egypte, is er alvast enthousiast over. “Egypte bevindt zich op een indrukwekkend groeipad, gedreven door digitalisering en uitzonderlijk AI-talent”, zo stelde hij in de persmededeling naar aanleiding van de plannen.

Volgens Kanishka Chakraborty en Parul Jain (Everest Group) is de zet van Capgemini geen toeval: “Egypte positioneert zich niet alleen als low-costlocatie, maar ook als innovatiehub die waarde toevoegt aan complexe projecten”, stellen ze. “Egypte combineert geopolitieke rust, een jonge talentenpool van 250.000 professionals en tijdzonevoordelen met Europa en het Midden-Oosten.”

IT IN EGYPTE IN CIJFERS

- Tweede grootste datacenterland in Afrika, na Zuid-Afrika
- Investeren van Orange Business, Telecom Egypt en Khazna Data Centers
- Eerste nationale overheidsdatacenter in aanbouw
- ICT-sector met dubbele groeicijfers
- 74 outsourcingbedrijven scheppen 60.000 banen (2022-2024)
- 260 outsourcingcentra, waarvan 190 internationaal
- 23ste plaats in Kearney's Global Services Location Index 2023
- 250.000 FTE's actief in IT- en BPO-diensten



A NOVEL APPROACH TO QUANTIFYING SECURITY USING SAMM

Application security has never been more business-critical, yet security often comes too late in the development process. This article explores how the *OWASP Software Assurance Maturity Model (SAMM)* helps organizations measure, improve, and align application security with business goals.

According to the **2024 Data Breach Investigations Report**, applications are the most common method used by a cyber attacker to gain unauthorized access to IT systems. Despite awareness, the number of breaches is rising, especially in sectors like healthcare. One reason is that security is intangible. Other (IT) investments usually have a quantifiable benefit. For security, this is much

more difficult until the business suffers. Additionally, startups and agile teams often skip security because it's not in the top 10 priorities.

The traditional software development lifecycle (SDLC) is predominantly focused on building software. Security is only introduced at specific stages of the development

pipeline. Thus, this reactive methodology often comes in when it is too late and too expensive to properly implement changes.

SECURE SDLC

Secure SDLC (SSDLC) is an idea to incorporate security in the software development lifecycle. It integrates security proactively into all phases of the development. An example of SSDLC is the recent rise of DevSecOps where organizations would augment the existing collaboration between developers and operations staff (DevOps) with security tooling as well as the security team thereby creating DevSecOps.

Integrating security throughout the development pipeline is a proactive approach. This method is concerned with laying a solid foundation rather than patching cracks. It is not only more effective in reducing risk but also more cost-efficient. As it allows teams to identify and address issues earlier, changes are easier and less expensive to implement.

APPSEC CORNERSTONES

The application security (AppSec) cornerstones are people, processes, knowledge and tools. The *people*-aspect means that security roles and responsibilities should be clear and the people responsible should be capable of fulfilling their role. The process-aspect includes having clear control gates, deliverables and activities enforcing security measures in the business. The knowledge-aspect is about implementing standards & guidelines, compliance, transfer methods. The last aspect encapsulates the tools used to implement security. An example of this is development tools, like an IDE, which can be employed by a programmer to write more secure code. Other tools are assessment tools and management tools.

More importantly though, all of these cornerstones revolve around the notion and understanding of risk. The framework doesn't assume that every control, process, or activity has the same importance for every organization. Different application risk profiles may apply. For instance, a bank app must have all-round security measures in place. This means that the SAMM maturity goals will be deep and extensive. By contrast, an internal accountant's tool in a restricted environment with limited access may not require the same level of security investment as the bank app.

SECURITY IS EVERYONE'S CONCERN

When implementing security in a business it should be clear that it is everyone's concern. It is not just something for the security team, but developers, testers, operators and business leaders need to play a role. Many stakeholders still see security only as the responsibility of

the security team. As security is often a matter of the weakest link, it should be shared in reality across roles: business analysts must capture security requirements, architects should apply secure design principles, developers need to write secure code, and testers and quality-assurance must validate that security features work as intended.

Of course, not all security measures are equally important in every context. For the business to remain efficient and competitive it is crucial to align the security efforts with what matters the most to the organization. When these specific goals have been established, feedback loops and metrics can be leveraged. By measuring KPIs a business can adjust and improve security over time.

SOFTWARE ASSURANCE MATURITY MODEL

However, as with implementing any new technology in the business, it is difficult to know where to start. For a business, a proper starting point might be the software assurance maturity model (SAMM), a flagship project of the Open Worldwide

Application Security Project (OWASP). Its purpose is to help organizations measure, improve, and mature their software security practices. The model addresses the key issues with security as it provides an approach to measure security and make risk driven decisions that align with the business needs.

Thus, it can be considered for a wide range of companies. The model considers the business functions governance, design, implementation, verification and operations. Each function has three security practices, and each practice has two business processes that can reach three maturity levels. Examples of maturity levels for the business processes Education and Guidance (Governance) and Secure Build (Implementation) are in table 1.

TABLE 1: EXAMPLES OF MATURITY LEVELS FOR EDUCATION AND SECURE BUILD

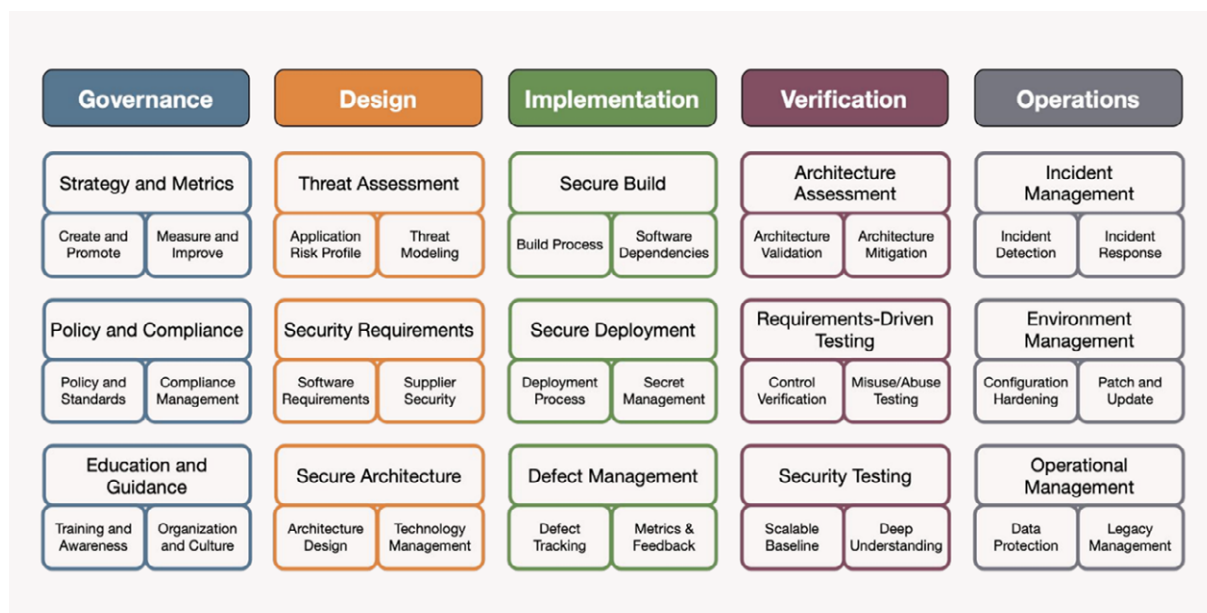
Maturity Levels (Example: Education) – table 1

- **Level 1:** Provide awareness training for devs.
- **Level 2:** Role-specific guidance and tools.
- **Level 3:** Fully standardized internal training with updates and metrics.

Maturity Levels (Example: Secure Build)

- **Level 1:** Define a consistent build process.
- **Level 2:** Automate builds, secure tools, add checks.
- **Level 3:** Enforce mandatory checks, reject non-compliant builds.

FIGURE 1: SAMM V2 MODEL OVERVIEW



Considering their risk profile, each organization decides how deep and in which way they apply the model. For instance, both a bank and a startup may consider verification but the bank might extensively simulate attacks while the startup might only run a few automated scans. The framework is the same, but the maturity targets differ per company.

Based on a questionnaire, companies are assigned to a maturity level for each business function described in SAMM. After completing the questionnaire, a total score for how secure a company is on each business function is obtained. The five business processes governance, operations, verification, implementation and design are ranked and compared to where the company wants to be in the future. These scorecards show how secure your organization is for each business function.

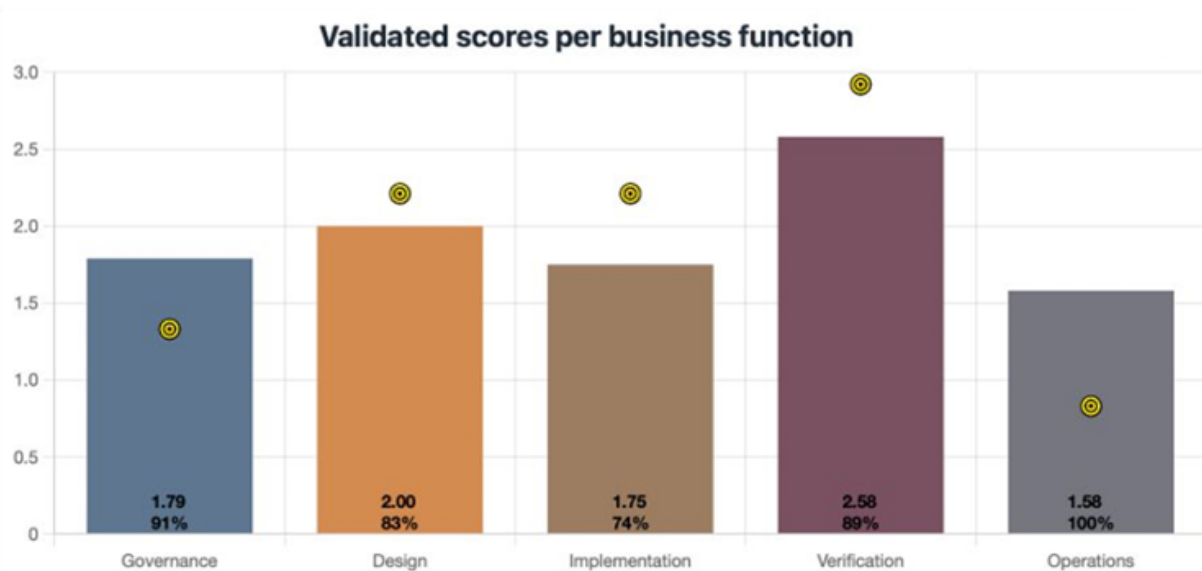
The scores make it possible to do gap analysis. Hence, target postures can then be used to gain an idea of how far teams have progressed in implementing security. In addition, the current and future state of a company can be compared and concrete roadmap building can be done. It also gives a clear overview of progress over time, showing an evolution of the security of your company.

To properly use SAMM, first a scope should be set. Maybe you are concerned with security in the whole organization or just one department. Usually, teams following the same development process can be grouped together. When assessing security, a smaller scope will be more precise than a larger scope. The next step of the process is to gather stakeholders, including all sorts of roles like developers, testers, operations team, Security Champions and GRC staff to create an initial assessment of the selected scope. After this assessment, the gaps between current position and future objective are considered to build an improvement plan. Finally, the teams will have to work on these improvements and roll them out across the planned scope.

Additionally, it's important to note that many SAMM activities require a continuous effort, especially at higher maturity levels. Due to the evolution of technology, security will always be a race between attackers and defenders. This means that achieving a certain score is one thing, but constant investments are needed to maintain that score. SAMM models this effect using score expiration, where the score automatically drops unless activities are maintained.

1. According to the OWASP SAMM framework, Security Champions serve as the primary security contact within their team. They meet with the security team for guidance and help bridge communication gaps between development and security. Because they understand their teammates' codebases and working culture, Security Champions can align security such that it resonates with the team. This makes them a key enabler of application security maturity.
2. Governance, Risk, and Compliance (GRC) professionals are dedicated to a company-wide approach to managing decision-making, risk, and regulatory compliance.

FIGURE 2: SAMM ENABLES GAP ANALYSIS BETWEEN FUTURE OBJECTIVES AND CURRENT POSITION



From <https://sammy.codific.com>

CONCLUSION

Security is a continuous journey, not a one-time fix. The central attacking point of adversaries has shifted to applications. Hence, pre-emptive security approaches are receiving more attention to integrate security practices earlier in the software development lifecycle, rather than treating it as a separate phase at the end. In addition, no company is 100% secure. However, as running a business intrinsically comes with trade-offs it is important to assess which security aspects are the most crucial.

For companies it is difficult to adapt to the vastly changing security environment. Adding to the challenge are the specific security needs of a company. This is where SAMM comes in. Just like a Swiss Army knife, it will provide a tailored risk-driven approach to implement security in your organization based on what it means for the organization to be secure. It considers security over many business functions and not just development. OWASP SAMM is free, open, and designed to help all types of

teams. The model helps bridge the gap between business goals and technical practices. As each SAMM activity has clear maturity levels to grow into, businesses can define clear objectives to reach. Lastly, the model also comes in handy for audits or Mergers and Acquisitions assessments. For instance, when one company merges with or acquires another, the security maturity and risk can be verified and evaluated. Hence, OWASP SAMM can evaluate AppSec maturity before a merger closes, reducing integration risk.



This article is based on a presentation by Aram Hovsepyan (CEO Codific and OWASP SAMM core team member). Article written by Jasper Visterin (KU Leuven).

DE ZEVEN GROOTSTE MYTHES VAN HET DIGITALE TIJDPERK

Zelfs voor doorgewinterde IT-professionals is het soms moeilijk om te weten wat ze nog moeten geloven over digitale media en internet. Het recente boek van Mediawijs met de titel *Mijn smartphone luistert mij af* zet 23 hardnekkige mythes op een rijtje. Wij schatten ze naar waarde.

MYTHE 1 MIJN SMARTPHONE LUISTERT MIJ AF

De eerste mythe is dus meteen de titel van het boek. Praat je soms met vrienden of familie en zie je nadien plots tientallen advertenties over datzelfde onderwerp in je feed, dan denk je misschien dat je toestel je af luistert. Als je bepaalde apps op je smartphone toegang gaf tot je microfoon, dan is dat in theorie inderdaad mogelijk.

Maar: "In de praktijk is dat voor bedrijven een erg dure en tijdrovende manier om informatie over jou te verzamelen", klinkt het bij Mediawijs. "Daar hebben ze veel gemakkelijkere trucjes voor."

MYTHE 2 BEN JE ONLINE OPGELICHT, DAN IS HET JE EIGEN SCHULD

Valse e-mails, frauduleuze berichtjes of bizarre betaalverzoeken: online kun je op verschillende manieren een oplichter tegen het lijf lopen. Cybercriminelen bedenken allerlei trucjes om je vertrouwen te winnen.



Maar: "Krijgen ze jou te pakken, dan is dat zeker niet omdat je dom of onoplettend bent geweest. Of om het met een vergelijking te zeggen: ook op de fiets kun je weleens een lelijke val maken en draag je best een helm. Toch doet zo'n val niets af aan de heerlijke avonturen die je al fietsend kunt beleven."

MYTHE 3 ANTIVIRUSPROGRAMMA'S ZIJN OVERBODIG GEWORDEN

Computervirussen lijken iets van een ver verleden. Veel apps en toestellen voorzien vandaag automatische updates die je beschermen tegen nieuwe bedreigingen.

Maar: "Ook vandaag vormen virussen nog altijd een risico voor je bestanden. Vooral op laptops of vaste computers bewijst zo'n programma nog altijd zijn nut."

MYTHE 4 NEPNIEUWS ONTMASKER JE METEEN

Niet alle vormen van fake news zijn gemakkelijk te herkennen. Sommige berichten zijn zo professioneel geschreven en vormgegeven dat je ze amper kunt onderscheiden van betrouwbare bronnen.

Maar: "Toch hoeft je niet alles op het internet met een korrel zout te nemen. Als je kritisch bent en alert blijft, kun je online perfect betrouwbare informatie vinden."

MYTHE 5 ONLINE BANKIEREN IS ONVEILIG

Sommige mensen mijden online bankieren, omdat ze niet goed weten hoe het juist werkt, bang zijn om iets fout te doen of erger nog: hun geld kwijt te raken. Bovendien verschilt de beveiliging van bank tot bank.

Maar: "Banken, en zeker de Belgische, doen er alles aan om je transacties veilig te houden. En als je zelf nog eens goed oplet, als je bijvoorbeeld geld overmaakt, dan ben je dubbel beschermd."

MYTHE 6 ALS JE OVERLIJDT VERLIEZEN JE DIERBAREN JE ONLINE DATA

Je huis, je fiets of je boekencollectie... die zijn van jou en gaan naar je erfgenamen wanneer jij er niet

meer bent. Maar voor gegevens die je verzamelt in online accounts en opslagdiensten, zoals foto's, chatgesprekken, e-mails of afspeellijsten lijkt dat minder evident. Het kan in de praktijk voor je erfgenamen moeilijk zijn om je digitale eigendommen in handen te krijgen.

Maar: "Het kan geen kwaad om je erfgenamen na je dood toegang te geven tot je accounts of gegevens. In accounts op platformen van Google, Meta of Apple kun je bijvoorbeeld keuzes aanduiden, zoals om je account na je dood volledig door te geven, te verwijderen, toegang te geven tot een deel van de gegevens op je account of je account een herdenkingsstatus te geven."

MYTHE 7 COMPUTERS ZIJN INTUSSEN SLIMMER DAN MENSEN

Al decennialang proberen we onze intelligentie over te dragen aan machines, zodat die kunnen kopiëren hoe ons brein werkt. Intussen worden ze daar dankzij artificiële intelligentie ook steeds beter in.

Maar: "De sterkte van computers ligt vooral in hun rekenkracht. Ze kunnen een veel grotere hoeveelheid informatie veel sneller verwerken. Strikt genomen zijn computers dus niet slimmer dan wij. Ze vullen onze tekortkomingen gewoon mooi aan."



'Mijn smartphone luistert mij af' en 22 andere mythes over het digitale tijdperk, Mediawijs, Borgerhoff & Lamberigts, 275 pagina's, 2024, ISBN: 9789463938327

OPVALLENDE QUOTES

“Agents hate spaghetti.”

Dave Lardinois, head of data & integrations bij Boels Rental, bij Tweakers. Als je data verspreid zijn en je integraties niet kloppen, kun je geen agent goed laten functioneren.

“We hebben 950 beroepen ontleed en geen enkele job gevonden waarbij AI alles kan overnemen.”

Econoom en auteur Erik Brynjolfsson van het bedrijf Workhelix in De Tijd.

“Er wordt vaak geschreven over ‘een datalek hier en een datalek daar’, maar wat momenteel gaande is, tart elke verbeelding.”

Cybersecurity-ondernemer Erik Westhovens op LinkedIn over de gerichte voice phishing-aanvallen op Salesforce-omgevingen door hackersgroep ShinyHunters. Medewerkers worden telefonisch misleid om hun Salesforce-inloggegevens prijs te geven.

“Learn Linux before Kubernetes. Learn Linux before Docker. Learn Linux before AWS. Learn Linux before anything else.”

Bill Buchanan, professor computerwetenschappen aan de Edinburgh Napier University op LinkedIn.

“Chinese hackers, gelinkt aan de overheid, hebben zich ingegraven in Amerikaanse kritieke infrastructuur en wachten op het juiste moment om een verwoestende slag toe te brengen.”

FBI-directeur Christopher Wray aan Reuters via ICT Magazine.

“Bedrijven als Facebook of Google denken altijd dat wat goed is voor hen, ook goed is voor de wereld.”

AI-experte Karen Hao over de race richting superintelligentie in De Standaard.



VOLGENDE EVENTS VOOR SAI.BE

6
10
OKT
2025

Partner event
<>
DEVOXX
Meer info vind je [hier](#)

22
OKT
2025

Partner event
<>
ANNA CON
Meer info vind je [hier](#)

4
DEC
2025

12.30 – 21.00 uur
☀️
SAI RESET IT 2025
SQUARE Brussels
Meer info vind je [hier](#)

BEKIJK **HIER** DE VOORBIJE EVENTS
VAN SAI.BE

VOOR NIEUWE EVENTS: NEEM ZEKER
EEN KIKJE OP **WWW.SAI.BE**



IN MEMORIAM - BART BAESENS

SAI.BE nam deze zomer met pijn in het hart afscheid van Bart Baesens, professor big data & analytics aan de KU Leuven. Bart heeft in het verleden heel veel cursussen verzorgd voor SAI.BE. Hij was zo de eerste om het prille begin van AI binnen te brengen in ons aanbod. We wensen de familie veel sterkte met het zware verlies. En danken Bart voor al wat hij voor SAI.BE heeft weten te bewerkstelligen.



Beluister [hier](#) ook de extra edities van **SAI.NT**, de podcast van **SAI.BE**. De SAI.NT-podcast bespreekt de laatste thema's en actualiteit binnen het IT- en technologielandschap.

ADVERTEREN IN SAI UPDATE?

Stuur een mail naar
communicatie@sai.be

INTERESSE IN ONS PRIJSVOORDELIJ LIDMAATSCHAP?

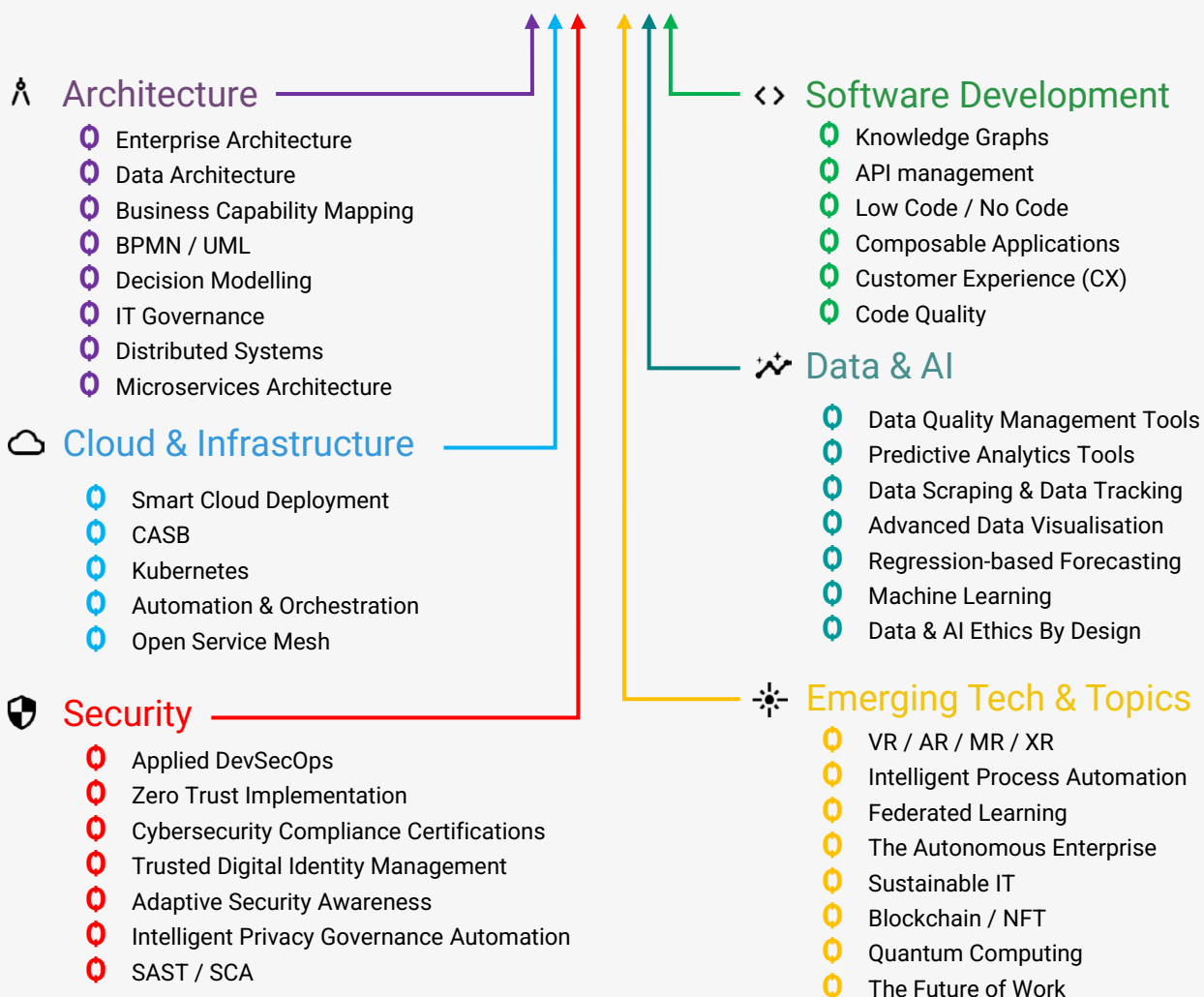
Kijk op www.sai.be/pagina/lidmaatschap/

Voor de bestaande leden: de meldingen voor het vernieuwen van het SAI.BE-lidmaatschap zijn begin november uitgestuurd. **Aarzel niet om uw lidmaatschap te verlengen en ook nieuwe SAI.BE-leden zijn uiteraard altijd welkom.**

COLOFON

Werkten mee aan dit nummer: William Visterin (coördinatie), Robin Van den Bogaert, Stef Gyssels, Jasper Visterin, Aram Hovsepyan en Marc Vael.

De missie van SAI.BE is om actuele en relevante IT kennis te delen op een objectieve en kwalitatieve manier met alle informatici in Vlaanderen en Brussel



- ✓ SAI.BE begeleidt duizenden informatici **sinds 1967** doorheen een immer wijzigend IT landschap
- ✓ SAI.BE organiseert jaarlijks **gemiddeld 50 events**, waaronder avondconferenties, workshops, webinars, focus-meetings, speciale events en ook podcasts



SAI.BE publiceert elk kwartaal **het tijdschrift "SAI Update"** voor informatici, IT-experten, en IT beslissings-makers

MEER WETEN OF LID WORDEN?

Ga naar www.sai.be/pagina/lidmaatschap/

NEEM CONTACT OP

voorzitter@sai.be