macaw

Trending Topics

Optimized IT Operations 2022

VIER TRENDING TOPICS VOOR EEN BETERE IT-OPERATIE RICHTING 2022

Management Summary

Bedrijven zijn – enerzijds door technologische ontwikkelingen, anderzijds door de opkomst van het hybride werken - in 2020 en 2021 anders gaan kijken naar hun IT. De optimalisatieslag wordt nu gemaakt. Beheersbaarheid, security, flexibiliteit en (kosten) efficiency zijn daarbij sleutelwoorden.

Macaw signaleert vier belangrijke trends in het optimaliseren van de IT-operatie. Allereerst is dat het verbeteren van security & compliance op basis van een zero trust-fundament. Met Identity First Security creëren bedrijven een extra beveiligingslaag. Gebruikers bevestigen met bijvoorbeeld tweefactorauthenticatie (MFA) hun identiteit. Zij typen geen wachtwoorden meer in, zodat cybercriminelen deze ook niet kunnen achterhalen. Behalve veilig inloggen is het van belang dat dit met de juiste permissies gebeurt. Alleen als het strikt noodzakelijk is, zou iemand in een beheerdersrol actief mogen zijn binnen een netwerk.

Als het gaat om security & compliance-oplossingen is een consolidatieslag gaande in deze markt. Geïntegreerde oplossingen helpen organisaties de complexiteit in hun IT-landschap te verlagen. Vendor consolidatie helpt bovendien het beheer eenvoudiger en goedkoper te maken. Maar liefst 80 procent van alle bedrijven is geïnteresseerd in zo'n strategie. Mede door de opkomst van het hybride werken is er een enorme behoefte aan digitale remote werkplekoplossingen. Met een virtuele werkplek valt dit eenvoudig en veilig in te richten.

Organisaties besparen hiermee op infrastructuurkosten en hebben de mogelijkheid meerdere soorten werkplekken te ontwerpen, die allemaal gebruik maken van dezelfde basis.

Tot slot ontwikkelen steeds meer organisaties een programmeerbare infrastructuur, die het mogelijk maakt de juiste dingen op het juiste moment te doen. Het ontwikkelen en beheren van omgevingen vloeien samen. Om de innovatiesnelheid van met name de open source-wereld bij te houden is het van belang dat organisaties investeren in een goed fundament. Hierin speelt niet alleen de juiste tooling een rol, maar ook de DevOps-mindset rondom zaken als adoptie en agile werken. Want behalve technologie gaat het om mensen en processen.

"Als het gaat om security & compliance-oplossingen is een consolidatieslag gaande in deze markt."

Optimized IT: juist nu veel ruimte voor verbetering

Waar 2020 het jaar was waarin bedrijven – veelal noodgedwongen – écht anders gingen werken, is 2021 het jaar waarin veel organisaties kritischer zijn gaan kijken naar hoe zij dit ondersteunen. Met oog op de opkomst van hybride werken (‘Het Nieuwe Werken 2.0’) zijn vorig jaar veel (technische) maatregelen versneld doorgevoerd om met name remote werken en cloud adoptie beter te faciliteren. Maar op governance gebied zijn onder andere zaken als beheersbaarheid, security & compliance, (kosten)efficiency nog lang niet optimaal geregeld.

Die optimalisatieslag wordt nu gemaakt. Organisaties waar wij als Macaw mee samenwerken kijken onder meer kritisch naar hun leverancierslandschap en de mate van complexiteit die zij wenselijk vinden voor hun IT-omgeving. Maar ook naar het naar een hoger plan brengen van hun security & compliance, iets wat zeker relevant is nu medewerkers een grotere mate van autonomie hebben gekregen (en overigens ook steeds meer verwachten). De rol van de cloud is groter geworden en daarbij komt de vraag ook naar voren wat die cloud nu eigenlijk inhoudt. Bedrijven laten daarbij de vaste contractvormen en traditionele invulling steeds meer los en streven naar een flexibeler model, maar dit is weer een uitdaging op zich: de technologiewereld beweegt snel en dit moet je als organisatie wel bij weten te benen. Hoe doe je dit?
In dit trendrapport brengen wij enkele belangrijke trends onder de aandacht die verband houden met het optimaliseren van IT. Op al deze gebieden ondersteunen wij al verschillende klanten en we kunnen dus gerust zeggen dat veel organisaties kunnen profiteren van best practices die wij inmiddels hebben ontwikkeld. Alle reden dus om dit rapport eens goed door te nemen. In het bijzonder willen we vier trends daarbij graag aan je voorleggen.

> **“De rol van de cloud is groter geworden en daarbij komt de vraag ook naar voren wat die cloud nu eigenlijk inhoudt.”**

Business as usual of juist nú doorpakken?

Het roerige jaar 2020 was misschien niet het beste moment voor IT-optimalisatie. Als gevolg van de COVID-19 pandemie was het vooral het jaar van noodgrepen. In veel gevallen trad IT op als redder in nood, toen plotseling veel kantoorwerkers remote moesten gaan werken, veelal gebruikmakend van beschikbare cloud oplossingen. Vooral in organisaties die al gewend waren nieuwe technologie snel te omarmen, leverde de radicale ommezwaai in de lockdown-tijd verbazingwekkend weinig problemen op en de productiviteit ging in veel gevallen zelfs sterk omhoog. Het bleek dat bedrijven zelfs met lege kantoren goed konden opereren.

Inmiddels is de situatie weer anders. De kantoren gaan zo langzamerhand weer open, al is de situatie wel veranderd. Meer dan ooit zijn organisaties flexibel geworden. In hun werkcultuur, waarin hybride werken het nieuwe normaal is, maar ook in de technologie waarmee zij hun business ondersteunen. Dit vraagt om een stevig fundament, zeker op het gebied van security & compliance, andere manieren van werken (bijvoorbeeld DevOps), het consolideren van het IT-landschap en het doorvoeren van nieuwe technologische standaarden als het gaat om het werken in de cloud en de werkplek die daar onderdeel van is.

Er zitten interessante learnings in de talloze gesprekken die we met onze klanten voeren over IT-optimalisatie. In deze gesprekken kwamen duidelijk deze vier trending topics aan bod:

1. Het verbeteren van security & compliance op basis van een zero trust-fundament, waardoor kenniswerkers beter functioneren en de kwetsbaarheid van organisaties afneemt.
2. De beweging naar geïntegreerde security tooling met een daarbij gepaard gaande consolidatie van het leverancierslandschap.
3. Altijd en overal kunnen werken met een virtuele werkplek, die ook geschikt is (veilig en vertrouwd) voor het ontwikkelen van applicaties.
4. De overgang naar een flexibele infrastructuur en het omarmen van een cultuur rondom DevOps, een filosofie die veel verder gaat dan door developers gebruikte tooling en ook zijn weerslag heeft op mensen en processen.

Trend 1: Identity First Security

De trend richting hybride werken bestaat al een tijdje. Steeds meer organisaties hebben afstand genomen van het idee dat elke medewerker één vaste werkplek heeft. Mensen werken afwisselend thuis en op kantoor met flexwerkplekken.

Door de COVID-19 pandemie is die trend in een stroomversnelling geraakt: veel mensen werkten langere tijd volledig remote en zijn eraan gewend geraakt dat zij niet altijd op kantoor hoeven te zijn om productief te zijn. Sterker nog, voor hun eigen welzijn en efficiency (zowel werk als privé) is hybride werken een uitkomst. Het resultaat van deze technische en culturele verschuiving is echter ook dat organisaties moeten werken aan het bouwen van een zero trust-fundament als het gaat om security. Identity First Security staat voor de manier waarop kenniswerkers functioneren, of ze nu op kantoor zijn of ergens anders.

Alles beter dan een wachtwoord

Security is een van de belangrijkste onderwerpen binnen dit trendrapport en binnen het huidige tijdsgewricht. Bij Identity First is het doel dat je als gebruiker nergens meer je wachtwoord hoeft in te typen. Nu nog is de eerste vraag bij het inloggen op diensten in de publieke cloud: ‘Wie ben je?’ Na het opgeven van je username is vervolgens meestal de vraag: ‘Wat is je wachtwoord?’ Dit laatste is echt onwenselijk. Veel beter is het als je als gebruiker bevestigt dat je ook écht bent wie je beweert te zijn. Bijvoorbeeld met tweefactorauthenticatie (2FA) via je mobiele telefoon. Of met een security key op een dongle. Of een vingerafdruk. Er zijn veel manieren om dit in te richten, maar allemaal zijn ze beter dan het intypen van een wachtwoord.

Extra beschermingslaag

Identity First staat voor de gedachte dat je nergens meer je wachtwoord hoeft in te typen. Dit is niet alleen prettig voor de gebruiker zelf, het betekent bovenal dat niemand anders het kan meelezen en/of registreren. En zelfs in het geval dat ongeautoriseerde derde partijen (in het vervelendste geval, cybercriminelen) het wachtwoord achterhalen, dan nog kunnen zij niet inloggen. Met een technologie zoals 2FA is er immers nog eens een bevestiging nodig van de gebruiker zelf. Dit is perfect, want zo is er een extra beveiligingslaag toegevoegd.

Altijd met de juiste permissies

Behalve naar het inloggen zelf valt het aan te raden ook te kijken of dit met de juiste permissies gebeurt. Want eigenlijk wil je niet dat iemand constant ‘admin’ is, terwijl dit niet strikt nodig is. Een rol met verregaande permissies binnen het netwerk is een risico, want deze is immers in staat veel schade aan te richten. Alleen als het strikt noodzakelijk is, zou iemand als admin actief mogen zijn in je netwerk. Dit is een belangrijk principe waar Macaw zelf actief op ‘jaagt’. Een van onze uitgangspunten op het gebied van rollen en rechten is het zorgen dat gebruikers altijd zo min mogelijk (en zo kort mogelijk) rechten gebruiken. Zo is het bijvoorbeeld echt niet nodig dat iemand global admin is voor het aanmaken van een mailbox. Dus niet te veel rechten, maar ook niet te weinig. De rol van ‘e-mailbeheerder’ geeft in dit geval precies de juiste privileges. Bij voorkeur is het ook tijdsgebonden en is de rol actief alleen op de momenten dat iemand aan het werk is. Met de technologie van Azure Active Directory PIM realiseren we deze manier van werken.

Werk veiliger samen met ‘externen’

Het doorvoeren van een Identity First-strategie is overal relevant, maar al helemaal voor organisaties die werken met veel ‘externen’. Veel bedrijven werken wel op de een of andere manier samen met mensen buiten hun organisatie. Dit gaat vaak verder dan alleen het uitwisselen van mails; het betreft ook het samenwerken aan documenten en het delen van data. Onderling vertrouwen is hierbij essentieel. Technologie helpt daarbij, maar let op: het is óók een governance-vraagstuk. Wat B2B-samenwerkingen met Identity First aantrekkelijk maakt voor iedereen - van IT-afdeling tot HR - is dat het mogelijk is mensen uit te nodigen met hun eigen bedrijfsaccount. Dit gaat een wildgroei van accounts tegen met de bijbehorende beheerlast. Technisch kan het eenvoudig, maar dan moet een organisatie wel haar governance op orde hebben.

Identity First in de praktijk

Een waterbedrijf is een belangrijke spil in de waterketen met wateraannemers zoals beheerders van sluizen en duingebieden, maar ook met overheden zoals de gemeente en projectontwikkelaars. Het bedrijf werkt aan het verbeteren van de waterkwaliteit. Deze samenwerkingen zijn veilig ingericht met een Identity First-oplossing met behulp van Azure Active Directory. Dit maakt toegang tot de applicaties en geo-data makkelijk, veilig en schaalbaar. Daarbij is de governance in orde door onder andere regelmatige reviews op gebruikte accounts, met name gast-accounts.

“Technologie helpt daarbij, maar let op: het is óók een governance-vraagstuk.”

Trend 1: Identity First Security

Gartner noemt Identity-First Security als een van de belangrijkste trends voor 2021 op het gebied van security en risk management.

Multifactorauthenticatie (MFA) kan meer dan 99,9% van de aanvallen op gebruikersaccounts afweren.

Om het belang van MFA nog verder te illustreren: dit zijn wereldwijd de tien meest gebruikte wachtwoorden door aanvallers:

1. 123456
2. password
3. 000000
4. 1qaz2wsx
5. a123456
6. abc123
7. abcd1234
8. 1234qwer
9. qwe123
10. 123qwe

Volgens het Verizon 2020 Data Breach Investigation rapport maakt 4 van de 5 geslaagde aanvallen door hackers gebruik van gestolen of zwakke wachtwoorden. Dit onderstreept de noodzaak voor MFA als onderdeel van cybersecurity-strategieën.

Trend 2: Vendor Consolidatie

Door de opkomst van hybride werken is het aantal cyberdreigingen alleen maar toegenomen: waar organisaties voorheen vooral bezig waren met het inregelen van security & compliance binnen de bedrijfsmuren, zullen zij dit nu ook moeten doen vanuit het oogpunt van remote en hybride werken. Een integrale aanpak vermindert de complexiteit in het IT-landschap en maakt het beheer ervan eenvoudiger en goedkoper.

Van deeloplossing naar integratie

De realiteit in veel bedrijven is dat er sprake is van te veel verschillende oplossingen, zo ook op security & compliance gebied. Een IT-landschap met (deel)oplossingen van uiteenlopende vendoren resulteert veelal in een complexe operatie en een behoefte aan meer (dure) specialisten. De meeste organisaties zien daarom de consolidatie van het leverancierslandschap als een manier om zowel hun kosten te verlagen als hun security & compliance situatie te verbeteren. Maar liefst 80 procent van alle bedrijven is geïnteresseerd in een strategie van vendor consolidatie. Dit is iets wat vooraanstaande IT-leveranciers ook zien gebeuren en zij reageren met completere, beter geïntegreerde producten.

Verschillende krachten

De trend naar vendor consolidatie is leveranciers-, technologie- en klantgedreven. Leveranciersgedreven omdat grote vendoren zoals Microsoft inzetten op het bieden van een geïntegreerde set van security & compliance oplossingen. Microsoft heeft de slagkracht in de markt om dit te kunnen doen én is al de partij achter veelgebruikte oplossingen zoals Azure en Microsoft 365, die onlosmakelijk met elkaar verbonden zijn. Technologiegedreven omdat het technologielandschap zich heeft ontwikkeld, en de cloud daar een steeds prominentere rol in speelt. Klantgedreven, omdat dit voorziet in de behoefte aan een integrale (holistische) aanpak en om complexiteit te verminderen.

Positie Microsoft

Microsoft heeft enorm geïnvesteerd in security- en compliance-kennis en -technologie. Het bedrijf kan zich inmiddels meten met specifieke security & compliance oplossingen van andere leveranciers in de markt. Microsoft brengt de verschillende security activiteiten samen met niet alleen koppelingen naar verschillende producten, activiteiten en tools, maar ook met een overzicht in een centraal dashboard dat in één oogopslag de status weergeeft van uiteenlopende security & compliance-activiteiten.

“De motivaties om veiligheid en naar een hoger niveau te brengen verschillen soms per sector.”

Overwegingen

Er valt veel te zeggen voor vendor consolidatie, maar er zijn zeker ook argumenten om te kiezen voor een best-of-breed strategie. Het voorkomen van vendor lock-in bijvoorbeeld. Ook kan het zijn dat specifieke oplossingen functionaliteiten bieden die net iets beter passen bij de situatie waarin een bedrijf zich bevindt. Een klant van Macaw kiest bijvoorbeeld voor zo’n specifieke oplossing die hen in staat stelt snel en eenvoudig nieuwe bedrijfsonderdelen te koppelen met hun bestaande IT-omgeving (carve in) en in omgekeerde richting af te stoten onderdelen te ontkoppelen (carve out). De keerzijde van zo’n strategie is natuurlijk wel dat je mensen moet bekwamen in verschillende deeloplossingen. Het dreigingslandschap ontwikkelt zich bovendien snel. Kun je zelf, met gedifferentieerde oplossingen, het tempo bijhouden met de mensen die je aan boord hebt?

Quick wins

Het gebruik van een geïntegreerde security & compliance-oplossing kan leiden tot snelle verbeteringen op gebieden die tot op heden te weinig aandacht kregen. Zo zijn er bijvoorbeeld nog steeds veel bedrijven die nog niet heel goed naar Identity & Access Management hebben gekeken. Door te gaan werken met technologieën als Single Sign-On (SSO) en Multi-Factor Authentication (MFA) zijn hier snel stappen te maken. Een andere groep bedrijven is, vanuit Threat Protection perspectief, gebaat bij een Security Information and Event Management oplossing (SIEM) voor het verzamelen en analyseren van bedreigingen als onderdeel van een Security Operations Center (SOC). De keuze voor een leverancier die een geïntegreerde oplossing met deze functies biedt, betekent daarmee een forse stap in de juiste richting.

Sectoroverstijgend

De drijfveren om security en compliance naar een hoger plan te brengen verschillen soms per sector. De maakindustrie is bijvoorbeeld sterk gericht op de bescherming van intellectueel eigendom en het tegengaan van bedrijfsspionage. Bij financiële instellingen heeft men juist vooral te maken met wetgeving zoals de AVG en richtlijnen van DNB. Ook nutsvoorzieningen zoals waterschappen en energiebedrijven hebben te maken met strenge richtlijnen, omdat zij verantwoordelijk zijn voor een kritische infrastructuur. Maar wat de achtergrond ook is, geïntegreerde oplossingen zijn relevant voor alle sectoren, omdat deze over de gehele breedte leiden tot het op orde brengen van security & compliance. De discussie rond vendor consolidatie speelt dan ook overal. Iedereen is op zoek naar een geoptimaliseerde IT-operatie, met als voornaamste argumenten: betere beheersbaarheid, minder complexiteit en de realisatie van kostenefficiëntie.

Business, Bytes & Behaviour

In relatie tot de klantbehoefte aan een integrale aanpak op het gebied van security & compliance zijn er drie facetten van belang die wij benoemen als Business, Bytes en Behaviour. Naast de technologie (Bytes) is het namelijk ook nodig aandacht te besteden aan het treffen van eventuele organisatorische (Business) maatregelen. Daarnaast zijn we van mening dat het creëren van het gewenste gebruikersgedrag- en bewustzijn (Behaviour) met betrekking tot cyber security eveneens essentieel is om de security & compliance situatie bij onze klanten te verbeteren. We hebben de overtuiging dat het onmogelijk is om security & compliance goed in te richten zonder aandacht voor al deze facetten. Alle drie de B’s zullen op orde moeten zijn.

Trend 2: Vendor Consolidatie

78% **van alle CISO's heeft 16 of meer tools in hun cybersecurity vendor portfolio.**

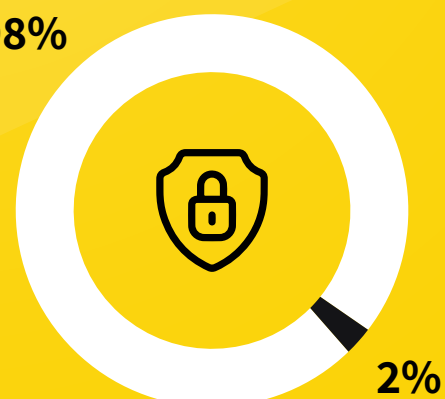
12% **heeft er zelfs 46 of meer. Het grote aantal securityproducten in organisaties leidt tot een toegenomen complexiteit, integratiekosten en toegenomen personeelskosten.**

80%

80% **van alle organisaties is geïnteresseerd in een vendor consolidatie-strategie**

Wereldwijd onderzoek in 2020 uitgevoerd in opdracht van security-dienstverlener Check Point onder 400 'global security leaders' wees het volgende uit:

- **98%** van de organisaties beheren hun beveiligingsproducten met meerdere consoles, waardoor zichtbaarheidssilo's ontstaan
- **79%** van de beveiligingsprofessionals zegt dat het werken met meerdere leveranciers aanzienlijke uitdagingen met zich meebrengt
- **69%** is het ermee eens dat prioriteit geven aan consolidatie van leveranciers zou leiden tot betere beveiliging



Trend 3: Anywhere Operations

Anywhere Operations staat voor altijd en overal kunnen werken. Mede door de opkomst van het hybride werken is er een enorme behoefte aan digitale remote werkplekoplossingen. Logistiek is het immers een behoorlijke operatie om remote fysieke werkplekken goed op orde te krijgen. Onnodig bovendien, inefficiënt en een verspilling van de hardware. De medewerker heeft immers vaak al de beschikking over goede hardware en is snel geholpen met een virtual desktop-oplossing.

Azure Virtual Desktop

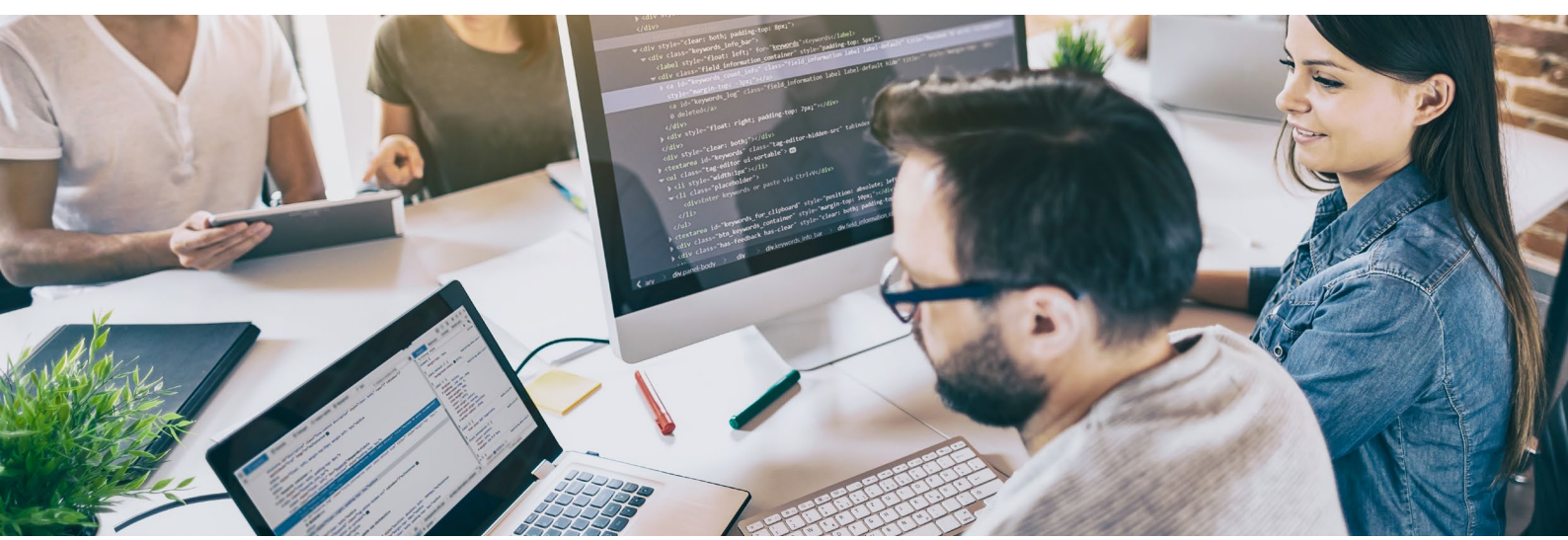
Met Azure Virtual Desktop geeft Macaw invulling aan de behoefte om eenvoudig en veilig op afstand te kunnen werken. In het bijzonder doen wij dit voor werkplekken voor developers. Een van de redenen om dit voor deze doelgroep goed in te richten is dat zij werken aan platformen met veel gevoelige data, bijvoorbeeld in de zorg of voor financiële instellingen. Deze klanten letten scherp op security en bovendien gaat het om intensief ontwikkelwerk, waarbij gebruiksvriendelijkheid en een goede performance belangrijkzijn.

Switchpod

Voor de duidelijkheid: de virtuele werkplek zal niet de traditionele fysieke werkplek vervangen. Het is geen vervanging voor je laptop. Het is juist een extra middel, een ‘switchpod’ die het gemakkelijk maakt om te schakelen tussen virtuele omgevingen. In het verleden was het inrichten van een remote werkplek namelijk lang niet altijd even efficiënt. Organisaties maakten bijvoorbeeld gebruik van een opstapserver waar alle medewerkers mee verbonden, maar waar niemand een eigen werkplek had. En ook andere oplossingen zorgden vaak voor klachten onder gebruikers: niet snel genoeg, omslachtig in gebruik.

Geen irritaties meer

Deze irritaties zijn er bij Azure Virtual Desktop niet. Geen gedoe, niet lastig en ondertussen wél extra security. Verschillende technische belemmeringen die oplossingen in het verleden parten speelden, zijn weggehaald. Dus geen VPN’s, tokens en/of dongels voor het inloggen en werken. Je logt simpelweg in met de tools die je al kent, bijvoorbeeld tweefactorauthenticatie (2FA) via je telefoon. Met de Azure Virtual Desktop bespaart een organisatie op de infrastructuurkosten door alleen te betalen tijdens het gebruik. En dat geeft de mogelijkheid om meerdere soorten werkplekken te ontwerpen voor teams in de organisatie. Allemaal maken ze gebruik van dezelfde basis. Wie Windows kent (en wie kent het niet), kan ermee aan de slag.



Lage beheerlast en kosten

Kortom, een eigen werkplek die altijd in de cloud beschikbaar is. In Nederland ontdekken steeds meer organisaties de virtuele desktop. Hier houden we immers wel van zulke efficiency. Het product is eenvoudig uit te rollen en kent weinig beheerlast. Inmiddels is ook duidelijk dat de kosten van een werkplek in de praktijk gunstig zijn. De gebruiker heeft zelf geen zware hardware nodig (de werkplek draait vanuit de cloud op het Azure-platform) en je kunt gemakkelijk met meerdere mensen tegelijk inloggen. Daarbij betaal je alleen voor wat je werkelijk gebruikt, weliswaar met een vaste prijs voor de licentie, maar verder alleen voor daadwerkelijk afgenomen resources. Een ideale oplossing voor veel bedrijven. Immers, hoeveel hebben er wel niet hele serverfarms met remote werkplekomgevingen zelf moeten optuigen om deze maar steeds verder te upgraden voor meer performance. Dit probleem is in één keer opgelost met een publieke cloudoplossing.

Integraties met (klant)omgevingen

Belemmeringen voor de virtuele desktop zijn zeldzaam, maar het kan zijn dat het gebruik van een bepaalde bedrijfsapplicatie reden is om toch te kiezen voor Citrix of een VMware-oplossing. Aan de andere kant brengt Azure Virtual Desktop juist ook gebruiksgemak en security in balans. Macaw doet dit met Microsoft 365 E5-software, waarmee gebruikers beschikken over een volledig pakket aan cloud security-producten. Developers die werken met de virtuele desktop-oplossing kunnen hierdoor in veel vrijheid hun werk doen. Bijvoorbeeld grote bestanden downloaden met snelle (10 Gb/s) verbindingen zonder dat zij meteen geblokkeerd worden. Bovendien kan Macaw de virtuele werkplek integreren met netwerk- en backend-systemen van de klantorganisatie, van SAP tot Oracle-databases en Sitecore. Het beheer van een werkplek - élke werkplek - is bepalend voor de effectiviteit van een oplossing. Het beheer moet gemakkelijk en efficiënt zijn. Daarom automatiseert Macaw het patchen en updaten van de virtuele werkplek zoveel mogelijk via scripts. Onder meer met Infrastructure-as-a-Code, DevOps-tooling én de DevOps-mindset die zo mogelijk nog belangrijker is. Met security als prioriteit moet alles goed in orde zijn en goed werken. Door te scripten verkort de time-to-market van de virtuele werkplek aanzienlijk. Het is daarmee ook een schaalbaar product; Macaw kan gelijktijdig meerdere aanvragen voor werkplekken verwerken en is niet beperkt door de capaciteit van beschikbare cloud engineers.

Virtuele desktops in de praktijk

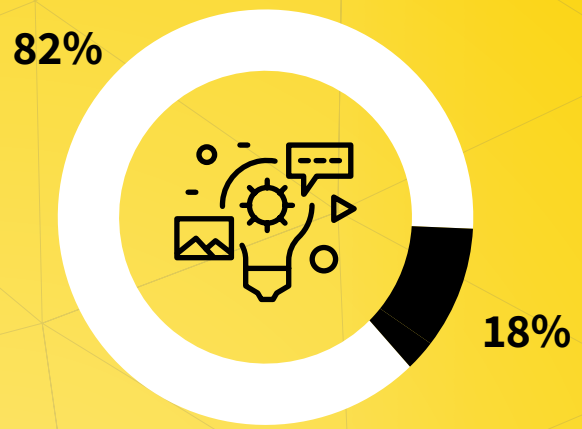
Een samenwerking van zeven ziekenhuizen gebruikt een gemeenschappelijke voorziening voor het analyseren van behandelinformatie. Het is niet alleen een gezamenlijk platform, maar ook een gezamenlijke werkplek voor developers, mogelijk gemaakt met
Azure Virtual Desktop. De overstap van lokale werkplekken naar een centrale werkplek versnelt het ontwikkelproces aanzienlijk.

Een zorgverzekeraar heeft circa 120 developers verdeeld over meerdere teams, die elk een eigen focus hebben. Voorheen was er sprake van verschillende werkplekoplossingen, afhankelijk van de behoefte van de teams. Met de door Macaw geleverde Azure Virtual Desktop kan deze zorgverzekeraar eindelijk alle exoten uit de IT-omgeving verwijderen en resources rationaliseren tot één centrale werkplekoplossing.

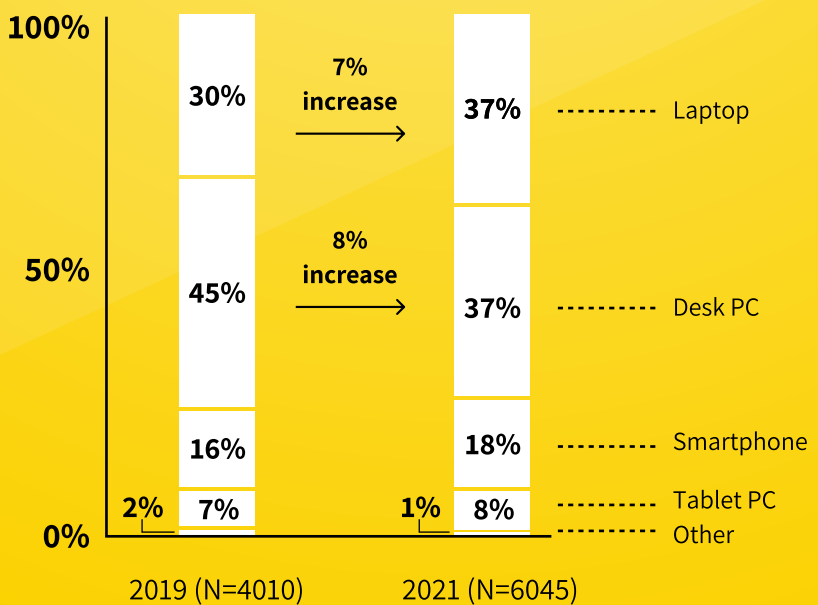
Een marktleidend bouwbedrijf heeft de beschikking over een groot dataplatform voor onder meer het beheer van gebouwen en IoToplossingen. Voorheen werd deze benaderd via een virtual machine in Azure, maar een virtuele desktop is beter gebleken. In plaats van een server met serversoftware hebben gebruikers de beschikking

Trend 3: Anywhere Operations

Toename in vertrouwen van digitale technologieBijna één op de vijf werknemers (18%) beschouwt zichzelf sinds de COVID-crisis als een expert op het gebied van digitale technologie, terwijl meer dan de helft zichzelf als bekwaam beschouwt, zo blijkt uit een nieuw onderzoek van Gartner. De toegenomen afhankelijkheid van digitale samenwerkingstools en het gebrek aan persoonlijke IT-ondersteuning bij het werken op afstand hebben de relatie van veel werknemers tot technologie veranderd.



Vertaling Onderzoek van Gartner wijst ook uit dat bij 36% van de werknemers van wie de thuiswerktijd sinds januari 2020 is toegenomen, ook ,de productiviteit is toegenomen. 35% gaf aan dat zij geen verandering in productiviteit ervaren. Flexibiliteit in de werktijden was de meest genoemde factor die een hogere productiviteit mogelijk maakte, gaf maar liefst 43% van de ondervraagden aan.



Trend 4: Operational Excellence

Steeds meer organisaties zien het als noodzakelijk om een programmeerbare infrastructuur te ontwikkelen, die het mogelijk maakt de juiste dingen op het juiste moment te doen. DevOps gaat daarbij een veel grotere rol spelen, waarbij met name open source-toepassingen de weg wijzen. Ook Macaw zet hier vol op in. Vooral het gebruik van GitHub neemt toe en Macaw zal deze technologie integreren met bestaande processen, bijvoorbeeld door source control hier neer te zetten en de developers-community te stimuleren.

Dev en Ops schuiven in elkaar

Binnen DevOps is het technology-aspect (GitHub/Azure DevOps) al redelijk voorzien. Maar qua people en process vraagt DevOps op het terrein van cloudmigratie meer aandacht. Organisaties zullen hier de komende tijd meer de focus op gaan leggen. Wat vooral inhoudt dat hun werkwijze en mindset zullen gaan veranderen. Vanuit het perspectief van veel bedrijven zijn ‘Dev’ en ‘Ops’ nu nog sterk gescheiden. Maar met het steeds meer naar de cloud migreren vloeien Development en Operations in elkaar over en zullen bedrijven steeds meer zelf hun DevOps gaan doen. Dat betekent dat ontwikkelteams ook operationele zaken gaan opzetten. Dit is in de praktijk best lastig.

Automatiseren, automatiseren, automatiseren

Voor een deel zit de ‘angst’ van organisaties met het samenvloeien van Dev en Ops in security. Met manuele processen is het inderdaad lastig om dit op een goed niveau te houden. Maar in de cloud is het sowieso goed om meer te denken vanuit het automatiseren van workloads. Dit begint al met een fundament waarin omschreven is aan welke specifieke eisen workloads in de cloud moeten voldoen. Het vereist het gebruik van scripts voor het afdwingen van standaarden en het schaalbaar maken van de infrastructuur.

Infrastructuur als flexibele resource

Het bij elkaar brengen van Dev en Ops vraagt erom dat organisaties zelf in control zijn. De mindset is dat zij infrastructuur managen als een flexibele resource. Deze moet nu werken, maar ook over pakweg tien jaar. Met workloads die draaien op een fundament met duidelijke policies, die zijn neergezet om het werk van mensen binnen de gewenste kaders (security!) te houden. Dat brengt dus Development en Operations bij elkaar. Development wordt kort-cyclisch en Operations komt veel sneller om de hoek kijken (‘Shift Left’). En het monitoren van de infrastructuur levert inzichten op voor de backlog, waarmee je diensten steeds verder gaat verbeteren.

Denk verder dan technologie

Met infrastructuur als flexibele resource is snelheid bepalend voor de effectiviteit van organisaties. Het is lastig de ontwikkelsnelheid in de open source-wereld bij te houden, maar dit is wel belangrijk. Om klanten hierbij te helpen biedt Macaw de mogelijkheid om blueprints te gebruiken, gebaseerd op best practices die zich onder andere vertalen naar effectieve scripts. Met Infrastructure-as-a-Code verzekeren bedrijven zich van standaard bouwblokken die zorgen voor een goed ingeregeld fundament, efficiënte monitoring en dashboards. Maar de belangrijkste trend is dat DevOps véél meer is dan de CI/CD pipelines waar men het nu vooral mee in verband brengt. Dit is inderdaad een onderdeel, maar DevOps is juist een mindset rondom zaken als adoptie en agile werken. Behalve technologie gaat het om mensen en processen.

Zorgverzekeraar **Menzis** omarmt steeds meer de DevOps-filosofie van you build it, you run it. De manier waarop Macaw hierbij ondersteunt is volgens het principe van 'voordoen, samen doen, zelf doen'.

Trend 4: Operational Excellence

De vijf belangrijkste pijlers onder een DevOps-strategie volgens Gartner (2020)

"Met infrastructuur als flexibele resource is snelheid bepalend voor de effectiviteit van organisaties."

Samenvattend kunnen we het volgende stellen:

Door vendor consolidatie en integratie van security-oplossingen verminderen organisaties de complexiteit van hun IT-landschap. Dit leidt tot meer efficiency, een verhoogde security en lagere kosten voor beheer.

Door de opkomst van hybride werken is er meer aandacht voor het inbouwen van een extra beveiligingslaag waardoor IT-gebruikers altijd veilig kunnen inloggen, waar zij zich ook bevinden. Technologieën als tweefactorauthenticatie vormen een verbetering ten opzichte van de situatie waarbij gebruikers inloggen met alleen hun inlognaam en wachtwoord. Daarnaast is het belangrijk dat gebruikers niet actief zijn binnen een netwerk met verhoogde privileges (admin-rechten) op momenten dat dit niet strikt noodzakelijk is.

Ook een gevolg van het hybride werken zijn ontwikkelingen op de markt van remote werkplekoplossingen. Een virtuele werkplek biedt gebruikers een volwaardige (Windows-) desktopomgeving die bovendien efficiënt is met resources, met een lagere beheerlast en lagere kosten tot gevolg.
Om de juiste dingen te blijven doen op de juiste momenten, speelt DevOps een steeds grotere rol. Met infrastructuur als flexibele resource is snelheid bepalend voor de effectiviteit van organisaties. Het is lastig de ontwikkelsnelheid in de open source-wereld bij te houden, maar dit is wel belangrijk. Macaw helpt klanten in control te zijn van hun infrastructuur, met een werkwijze gebaseerd op best practices in verschillende sectoren.

Zit je na het lezen van dit trendrapport met vragen?

Stel ze dan gerust via één van onze consultants of via

contact@macaw.nl

Of ben je benieuwd wat andere bedrijven al hebben gedaan om hun digital workplace toekomstbestendig te maken? In onze cases, in samenwerking met onder andere **financieel dienstverlener CED** (data in de cloud) en **staalproducent Tata Steel** (applicaties m.b.v. Microsoft Power Platform), vertellen we er meer over!