

Interview | Foto Karianne Hoekstra

# Datacenters openen de deuren voor nieuwe diensten in de cloud

Organisaties gebruiken steeds vaker cloudapplicaties voor directe toegang tot online datasystemen of als back-endoplossingen voor zakelijke toepassingen. Dat bedrijven hun data en applicaties in de cloud zetten, betekent niet dat alles maar ergens rondzweeft. De cloud staat gewoon op hardware, ergens in een datacenter. Wat de cloud de cloud maakt, is dat data verspreid is over veel verschillende datacenters. Dat brengt beveiligingsrisico's met zich mee, en dus ook kansen voor ICT-dienstverleners die gedegen kennis hebben van securitytoepassingen, zegt Marc Jepkes, sales manager bij Fortinet.



Marc Jepkes

Bij de cloud denken veel mensen aan de datacenters van de grote publieke cloudaanbieders: Microsoft (Azure), Amazon (AWS) en Google (Cloud Platform). Zij voorzien in de infrastructuur waar bedrijven hun data opslaan. Vervolgens kiest men uit 'marktplaatsen' aanvullende diensten voor migratie, opslag, beveiliging, etc. van deze data. Zo bouwt men zijn eigen ICT-omgeving helemaal naar wens op.

Nemen de 'grote jongens' daarmee de plaats in van de vertrouwde en bekende ICT-partner van een organisatie? Niet volgens Marc Jepkes: "De cloud bestaat niet alleen uit de datacenters van de grote cloud- en SaaS-aanbieders, maar omvat ook datacenters bij serviceproviders

en, nog steeds, bij bedrijven op locatie. Dat noemen we respectievelijk public en private clouds. In de praktijk is er meestal sprake van een combinatie: de zogenoemde multicloud. Het beheren, en vooral het beveiligen van data in al deze verschillende datacenters biedt nieuwe kansen voor IT-partners van bedrijven."

## Rol van resellers

Hoe kunnen resellers een rol spelen bij de stap naar de public cloud? Jepkes: "Het lijkt alsof Microsoft, Amazon en Google alles bieden wat een organisatie nodig heeft. De infrastructuur in de cloud is echter totaal anders dan die in de traditionele omgeving. Als je een bepaalde omgeving wilt opbouwen, moet je uit

de marketplaces van de cloudaanbieder bepaalde componenten bestellen. Dat varieert van storage en business intelligence tot en met security. Dat kan uitermate complex worden als je niet weet wat je doet. Het is verstandig om daar een ICT-partner met kennis van zaken bij te halen."

## Spanningsveld tussen CIO en CISO

Bovendien betekent het wijdverspreide karakter van de hybrid cloud dat bedrijven andere prioriteiten moeten stellen in hun keuze om naar de cloud te migreren. "De infrastructures in de datacenters zijn wel beveiligd, maar de componenten en applicaties die bedrijven daar bovenop installeren zijn dat niet", zegt Jepkes. "Dat creëert een spanningsveld tussen de CIO, die zo snel mogelijk naar de cloud wil, en de CISO die de controle dreigt te verliezen. Hij weet vaak niet wat voor policies daar worden ingebracht en hoe veilig het is. Fortinet kan daarbij helpen. Met een centraal platform zoals FortiManager kan een CISO de beleidsregels en oplossingen waarmee zij de omgeving op de eigen locatie beveiligen, doortrekken naar de cloud, uniform houden en beheren, met inzicht. Het is belangrijk om rekening te houden met het feit dat niet het netwerk, maar de beveiliging leidend is in de transformatie naar de cloud. Daarvoor is een kennispartner essentieel."

Managed Service Providers (MSPs), aan wie bedrijven al langer de ICT-omgeving uitbesteden, zijn uitstekend gepositioneerd om die rol op zich te nemen. "MSP's werken al vanuit datacenters", zegt Jepkes. "Fortinet heeft een heel interessant portfolio om hen te helpen nieuwe diensten te ontwikkelen waarbij security leidend is. Daarmee kunnen zij hun klanten ontzorgen en hen voorzien van een securitylevel dat de klant zelf niet kan invullen. Door de stap te maken van MSP naar MSSP (Managed Security Service Providers, red.) kunnen zij zich differentiëren."

MSP's begrijpen dat en mede daardoor is Fortinet zo sterk vertegenwoordigd in datacenters, zegt Jepkes. "Een aanzienlijk gedeelte van onze omzet komt van serviceproviders. Dat zal nog groter worden, want de traditionele reseller wordt ook een partij die klanten volledig ondersteunt als het gaat om de complexiteit die de cloud met zich meebrengt. Dat is de evolutie van de markt, klanten vragen daar tegenwoordig om." Voor datacenters die voorheen voornamelijk 'housing' oftewel onderdak voor hardware boden, geldt deze evolutie ook. Jepkes: "Hun klanten willen niet alleen spullen bij hen neerzetten, maar vragen ook om een dienst daaromheen, zoals voor security. Dat begon als een managed firewalldienst of een managed maildienst, maar tegenwoordig omvat dat veel meer."

Daarnaast ontwikkelt er dankzij de cloud een nieuwe dienstverlener, de zogenoemde cloud enablement partner. "Dit zijn partijen die bedrijven helpen om naar de cloud te gaan", weet Jepkes. "Veel bedrijven die dit zelf wilden realiseren zijn gestruikeld door gebrek aan competentie of door een verkeerd beeld van wat ze daar aantreffen. Competentie is superbelangrijk en cloud enablement partners blinken daarin uit."

**Minder complexiteit en meer inzicht**  
Al deze partners kunnen, door het uitbreiden of initiëren van diensten, bedrijven helpen om de reis naar de cloud te maken. Waarom zouden zij deze reis aangaan met Fortinet? Jepkes: "Fortinet biedt een uitgebreid palet aan geïntegreerde security-oplossingen en services. Daardoor hoeven bedrijven in de datacenters niet te kiezen voor allerlei losse componenten die allemaal afzonderlijk beheerd moeten worden. Als je een efficiënte MSSP-propositie in het

die bedrijven al gemaakt hebben in hun bestaande omgeving. De wereld is nu eenmaal opgebouwd uit diversiteit. Het zou een desinvestering zijn om daar een streep door te zetten. Als een omgeving al een oplossing van een andere partij heeft die perfect werkt, waarom zou je die dan weghalen? Daarom bieden we API's om een koppeling te maken ons portfolio, rekening houdend met het fundament dat al geslagen is." Partners kunnen met Fortinet een efficiënte, differentiërende, managed-security-

## De totaalbenadering maakt een centraal beheerde end-to-end-security mogelijk

leven wilt roepen, moet deze niet bestaan uit een mengeling van verschillende technologieën. Die problemen hebben we in het verleden al genoeg gezien bij de eindgebruikers. Met Fortinet werken men met een framework waarbij de onderliggende securitycomponenten met elkaar samenwerken. Via API's bieden we ook de mogelijkheden voor automation, orchestration en de koppeling met oplossingen van derden. Uniek voor Fortinet is dat men dat allemaal centraal beheert vanuit één enkel dashboard."

Het volledige securityconcept, waarbij alle aspecten van het netwerk beveiligd worden, wordt door de leverancier de Fortinet Security Fabric genoemd. Deze totaalbenadering maakt een centraal beheerde end-to-end-security mogelijk.

"We beveiligen data in het datacenter, op weg daar naartoe en binnen de applicaties die het gebruiken. Ongeacht of de data nu in een datacenter on premise staat of in een private of public cloud, of in combinaties daarvan. Dat betekent ook dat we rekening houden met keuzes

dienst aanbieden, stelt Jepkes. "Die staat voor minder complexiteit, meer inzicht en meer controle. Want voor alle oplossingen die we hebben – FortiGate, FortiMail, FortiCASB, et cetera – kun je het woordje 'managed' zetten. Het licentiemodel van Fortinet ondersteunt managed-securityoplossingen voor de MSSP-dienst."

Hoe doet het licentiemodel van Fortinet dat? Jepkes: "Een MSSP legt een beveiligingsschil rondom een infrastructuur waar hij soms zelf geen controle over heeft. Veel licentiemodellen zijn nog steeds gebaseerd op prijs per user, per node, per device: dat zijn lastige elementen om een efficiënte dienst van te maken. Een MSSP ziet tenslotte alleen performance en wil dáár rekening mee houden en afrekenen op basis van toename en afname van die performance. Niet op basis van de apparatuur die daaronder ligt, want die kent hij niet altijd. Fortinet biedt een MSSP-ready-oplossing: van technologie en oplossing tot en met het hele licentiemodel. Inzichtelijk én schaalbaar."