SonicWall: Voor de reseller die MSSP wil worden

Begin januari werd ChannelConnect bijgepraat over de producten en strategie van SonicWall. Het is een bedrijf dat bijna iedereen van naam kent en dankzij duizenden partners in de Benelux ook een groot marktaandeel heeft. Dat laatste wil SonicWall vanzelfsprekend verder uitbouwen.

Tekst Rashid Niamat

De afgelopen tijd is het redelijk rustig geweest rond SonicWall. Michael Berg, verantwoordelijk voor de EMEA-sales, is daar direct vanaf de start van het gesprek open over. “Zoals bekend is Sonicwall in 2012 door Dell overgenomen. We hebben vanaf dat moment deel uitgemaakt van de Dell Software Groep. Het bedrijfsonderdeel Sonicwall is in 2016 verkocht aan Francisco Partners met de doelstelling om te analysen waar de behoefte van de markt ligt en om zich te kunnen profileren als een pur sang securityvendor.”

Het blijkt dat SonicWall die periode heeft benut om de bestaande diensten verder te ontwikkelen en het portfolio uit te breiden. Daardoor kan het op dit moment voor specifieke doelgroepen en verticals tal van diensten en producten aanbieden die allemaal via een en hetzelfde panel, het CSC (Capture Security Center), kunnen worden bediend. Het maakt daarbij niet uit of het gaat om fysieke devices, zoals next gen firewalls, malwareprotectie-appliances of de virtuele uitvoeringen daarvan. SonicWall kan zowel lokaal worden ingezet als off-premise, wat een datacenter kan zijn, een private of public cloud.

100% kanaal en mkb

Het portfolio wordt nog steeds op basis van een honderd procent channelmodel in de markt gezet, waarbij voor de Nederlandse markt gebruik wordt gemaakt van vier distributeurs.

De focus van SonicWall is altijd geweest het maximaal faciliteren van de partners met als eindgebruikers het mkb. Tot die groep worden profit als non-profit organisaties gerekend die maximaal 1.500 werkplekken groot zijn. Bij die omvang spreekt het voor zich dat in het SonicWall-portfolio producten en diensten te vinden zijn voor organisaties met meerdere vestigingen. Om de implementaties over verschillende locaties te simplificeren zijn de SonicWall-appliances allemaal geschikt voor zero touch deployment. De partner kan de appliance laten bezorgen zonder daarbij aanwezig te hoeven zijn.

> SonicWall heeft de luwte benut om diensten te ontwikkelen

De klant hoeft de appliance slechts te voorzien van stroom en connectiviteit. Remote kan de reseller of de centrale IT-afdeling, al dan niet door gebruik te maken van pre defined settings, voor activatie en naadloze integratie binnen de infra zorgen.

TCO

Naast het mkb is SonicWall sterk vertegenwoordigd in delen van het onderwijs en bij overheden. Dat heeft alles te maken met de vraag van deze specifieke klantgroepen naar high performance appliances, dus hoge throughput en lage latency. Voorbeelden hiervan zijn te vinden bij de roc’s en vmbo-instellingen, waar de wens is meer dan 10GB aan traffic real time te kunnen inspecteren tegen een lage TCO. De TCO voor SonicWall-appliances is zo laag omdat SonicWall een afwijkend pricingmodel hanteert. Bij twee boxes in een active-passive-opstelling geldt dat alleen voor de actieve box de licenties, services en support in rekening worden gebracht. Voor de passive appliance geldt alleen de aanschafprijs van de tweede box.

Real time tegen Meltdown en Spectre

SonicWall maakt voor de detectie en preventie van malware uiteraard gebruik van sandboxing. De techniek is zelf ontwikkeld en maakt real time deep-memory-inspectie mogelijk. De toevoeging real time is hier cruciaal. SonicWall claimt hierdoor beter te presteren dan andere vendoren, die werken met memory-snapshottechnieken, waarbij Sonicwall Real Time Deep Memory Inspectie levert binnen een honderdste van een nanoseconde. Sonicwall RTDMI is in staat bedreigingen die werken op basis van side channel attacks, de welbekende Spectre, Meltdown, Foreshadow en Portsmesh te kunnen detecteren en blokkeren. Belangrijk in deze techniek is dat varianten op basis van de bestaande side channel attack patronen worden gedetecteerd en geblokkeerd.

Real time detectie biedt dan ook de mogelijkheid om elke CPU-instructie te kunnen detecteren voordat malware wordt uitgevoerd. Die aanvallen zijn geen theorie: volgens Berg zijn er inmiddels meer dan 60.000 verschillende en voorheen onbekende aanvaltypes aan het licht gekomen door RTDMI.

Van losse oplossingen naar platform

Berg heeft een uitgesproken mening over dat deel van de markt dat vertrouwt op een multi layered security approach waarbij een veelvoud van vendoren essentieel is. De gedachte bij eindklanten en resellers werkt volgens hem juist meer onveiligheid in de hand. “De praktijk is dat silo’s slecht met elkaar communiceren”, stelt hij en vervolgt: “Ze vergroten de veiligheid van een netwerk of infrastructuur ook niet, omdat de performance van de slechtst werkende component de werking van de rest ondermijnd.” Verder is er wat hem betreft nog te weinig oog voor de gebrekkige efficiency. “Een multi layered- en multi-vendorbenadering betekent dat de reseller of IT-afdeling de kennis van meerdere vendoren en producten moet bijhouden en de gebrekkige communicatie tussen die losse silo-oplossingen moet managen.

Zowel de resellers als de eindklanten hebben daar de zelfde problemen. Het kost steeds meer geld en de mensen die dat kunnen zijn er amper.” Wat Berg betreft moet dat anders. “CSC is het logische antwoord. Dat is een platform waar je alle SonicWall securitydiensten integreert, via één single pane of glass beheert en de data kunt analyseren. Als iets de firewall raakt dan worden de andere componenten automatisch gealarmeerd. Binnenkort wordt aan de CSC ook de access-securityoplossing toegevoegd waardoor het overzicht en de veiligheid nog verder toeneemt.”

Van MSP naar MSSP

Een bijkomend voordeel van het CSC-platform is dat het de partner de mogelijkheid geeft zich te ontwikkelen van een Managed Service Provider naar een Managed Security Service Provider. “Het CSC-platform biedt de beste diensten en het gebruik daarvan door partners en klanten is logisch en simpel”, zegt Berg en voegt daar aan toe dat een goed doordachte en simpele bediening de veiligheid van de IT-omgeving bij de klant verhoogt. “In design investeren we permanent, we zijn de enige organisatie met een CDO, een Chief Design Officer.”

> Lage TCO door afwijkend pricingmodel

De focus op gebruiksgemak zorgt er ook voor dat nieuwe diensten sneller door de partners en eindklanten worden ingezet. Daarmee kan de MSP zich ontwikkelen tot een MSSP, een leverancier die op basis van een uitgebreid veiligheidspakket de beste oplossing voor zijn klanten samenstelt, beheert en uitbouwt. SonicWall ziet dat partners die als MSSP opereren en het leveren van diensten centraal stellen in plaats van hardwareverkoop, beloond worden met een hogere klantloyaliteit. Dat draagt structureel bij aan gezondere business en maakt de stap van MSP naar MSSP iets dat veel lezers zou moeten aanspreken. Voor resellers die meer willen weten over zowel de commerciële als technische mogelijkheden van het CSC-platform heeft SonicWall een kort en helder introductieprogramma. Deze jumpstarttraining wordt meerdere keren per jaar gegeven en men kan zich daarvoor opgeven via mail benelux@sonicwall.com of telefonisch 00353212377037. «