

PARTNER SUCCESS STORY



Aumatics houdt grip op digitale veiligheid klanten met WatchGuard MDR

Volgens de nieuwe Cyberbeveiligingswet zijn managed security service providers (MSSP's) eindverantwoordelijk voor de digitale veiligheid van hun klanten. Ze moeten bij iedere klant snel en adequaat kunnen ingrijpen als er iets mis dreigt te gaan. "Dat lukt niet met alleen een firewall en endpoint protection", zegt Ed van Puffelen, oprichter en directeur van Aumatics. Met WatchGuard Managed Detection & Response (MDR) houdt de MSSP continu grip op security.

Aumatics ontwerpt, implementeert en beheert schaalbare en veilige IT-oplossingen voor met name grotere organisaties met meer dan duizend medewerkers. "Als MSP en MSSP bieden we klanten een totaaloplossing in de vorm van een dienst", vertelt Frank Kemeling, Cyber Security Consultant bij Aumatics dat onderdeel is van de zakelijke ICT-provider Hallo. "We leveren niet alleen een firewall, maar ook netwerkoplossingen, endpoints en de bijbehorende bescherming. Vanuit ons Security Operations Center houden we alles voortdurend in de gaten om cyberaanvallen te detecteren."

"Wanneer ons SOC kwetsbaarheden ontdekt, hangt de aanpak af van de afspraken met de klant", voegt Van Puffelen toe. "Soms patcht onze eigen beheerorganisatie de kwetsbaarheden of worden er andere security-aanpassingen gedaan. In andere gevallen regelt de klant dit zelf. Een groot deel van onze klanten beschikt over een eigen IT-afdeling die wij ondersteunen."

Managed security populair

Deze vorm van dienstverlening wint volgens Van Puffelen snel aan populariteit. "Berichten in de media over ransomware-aanvallen en datalekken vergroten het securitybewustzijn bij bedrijven. Ze realiseren zich steeds meer dat aanvullende beveiligingsmaatregelen noodzakelijk zijn, om geen slachtoffer te worden van dergelijke aanvallen. Multifactorauthenticatie wordt bijvoorbeeld snel de norm, omdat het een extra beveiligingslaag toevoegt die voorkomt dat aanvallers toegang krijgen, zelfs als ze over een wachtwoord beschikken."

"Tegelijkertijd geven bedrijven aan dat ze deze maatregelen vanwege een gebrek aan tijd en kennis niet zelf willen beheren", vervolgt de directeur van Aumatics. "Die beveiliging moet bovendien voldoen aan een groeiend aantal wetten en regels, zoals de Digital Operational Resilience Act (DORA) voor de financiële sector en de aankomende Cyberbeveiligingswet op basis van de NIS2-richtlijn. Met security als een beheerde dienst weten klanten precies waar ze aan toe zijn, voor een vast en goed te budgetteren bedrag per maand."

MSSP Partner



Region:
The Netherlands

Category:
MSP/ MSSP

WatchGuardONE Level:
Gold

WatchGuard Products:

- Managed Detection & Response
- Endpoint Security
- Network Security
- Wi-Fi Access Points

“Aan de selectie van WatchGuard MDR ging een grondig onderzoek van drie maanden vooraf. “Security draait om vertrouwen. Als MSSP verkoop je vertrouwen. Maar dan moeten wij de partners waarmee we samenwerken ook kunnen vertrouwen”, verklaart Van Puffelen. “Dat kan alleen als je de oplossingen die je gebruikt voor je dienstverlening zelf hebt getest. Die moeten bewezen goed en betrouwbaar zijn. En de prijs moet natuurlijk kloppen.”

- Ed van Puffelen, oprichter en directeur van Aumatics

Zware verantwoordelijkheid MSSP's

Security als dienstverlening legt wel een zware verantwoordelijkheid bij de MSSP's. Deze partijen worden - afhankelijk van omvang en omzet - onder de NIS2-richtlijn aangemerkt als een 'belangrijke entiteit'. Daar hoort een zorgplicht bij. MSSP's moeten passende maatregelen nemen om de netwerk- en informatiesystemen van klanten te beschermen. Ze zijn dus niet alleen verantwoordelijk voor de eigen securityomgeving, maar ook eindverantwoordelijk voor de digitale veiligheid van hun klanten.

"Dit betekent onder andere dat je actief moet monitoren of de endpoints van je klanten worden aangevallen", stelt Van Puffelen. Volgens de directeur van Aumatics is het zelfs geen optie meer om endpointsecurity zonder de monitoringcomponent te verkopen aan klanten. "Ik denk dat wij daar als markt wat harder in moeten worden."

WatchGuard MDR

Voor een snelle detectie van aanvallen op endpoints breidde Aumatics zijn dienstverlening uit met Managed Detection & Response (MDR) van WatchGuard Technologies. Deze dienst wordt beheerd door een team van cybersecurity-experts van WatchGuard. Deze experts gebruiken beveiligingsanalyses, machine learning, AI en dreigingsinformatie om bedreigingen te monitoren, te detecteren en te beheren. Dat doen ze dag en nacht.

De cybersecurity-experts van WatchGuard werken daarbij nauw samen met de securityconsultants van Aumatics. "Dat is ook nodig om een 24-uurs dienst aan te kunnen bieden", stelt Kemeling. "Samen zorgen we op ieder moment van de dag voor een snelle en effectieve respons, in nauwe samenwerking met de klant."

Grondige selectie

Aan de selectie van WatchGuard MDR ging een grondig onderzoek van drie maanden vooraf. "Security draait om vertrouwen. Als MSSP verkoop je vertrouwen. Maar dan moeten wij de partners waarmee we samenwerken ook kunnen vertrouwen", verklaart Van Puffelen. "Dat kan alleen als je de oplossingen die je gebruikt voor je dienstverlening zelf hebt getest. Die moeten bewezen goed en betrouwbaar zijn. En de prijs moet natuurlijk kloppen."

Om de beste oplossing te kiezen, heeft Aumatics drie maanden lang Proof of Concepts (PoC's) uitgevoerd met vier partijen, waaronder WatchGuard. "We richtten geïsoleerde testomgevingen in die een echte klantomgeving nabootsen, compleet met endpoints en firewalls", schetst Kemeling. "Hierin lieten we malware los om te zien hoe de oplossingen reageerden: welke meldingen kwamen binnen, wat belandde in het Security Operations Center, en hoe werd actie ondernomen? Deze tests gaven ons waardevolle inzichten in ondersteuning en effectiviteit."

WatchGuard geeft vertrouwen

WatchGuard kwam als beste uit de bus. "De ondersteuning van WatchGuard is bijzonder sterk", vindt Kemeling. "Bij problemen hebben we binnen enkele minuten iemand aan de lijn. We krijgen duidelijke meldingen in ons SOC: wat er is gebeurd, wat we moeten doen, en of zij ons kunnen ondersteunen. Daarnaast ontvangen we overzichtelijke rapportages met een samenvatting van wat er die week is gedaan, welke bedreigingen zijn gevonden, en welke verbeteringen zijn doorgevoerd. Alles wordt zorgvuldig gecontroleerd."

De PoC's hebben volgens Kemeling geholpen bij een snelle uitrol van WatchGuard MDR. "De procedures voor het onboarden hadden we al gemaakt. De klantspecifieke afspraken zijn dan snel verwerkt. Vervolgens was het een kwestie van het uitrollen van de agents, dan komen ze netjes in de portal en dan ben je in principe on-boarded. Door het volwaardige multi-tier en multi-tenant karakter kunnen we templates hergebruiken en dankzij het gebruik van een doordachte implementatie kunnen we nog steeds klantspecifieke uitzonderingen maken. En alles werkt nu naar tevredenheid. De positieve ervaringen met WatchGuard tijdens de PoC ervaren we nu ook in de praktijk."



WatchGuard® Technologies, Inc. is a global leader in unified cybersecurity. Our Unified Security Platform® approach is uniquely designed for managed service providers to deliver world-class security that increases their business scale and velocity while also improving operational efficiency. Trusted by more than 17,000 security resellers and service providers to protect more than 250,000 customers, the company's award-winning products and services span network security and intelligence, advanced endpoint protection, multi-factor authentication, and secure Wi-Fi. Together, they offer five critical elements of a security platform: comprehensive security, shared knowledge, clarity & control, operational alignment, and automation. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit [WatchGuard.com](https://www.watchguard.com).



©2025 WatchGuard Technologies, Inc. All rights reserved. WatchGuard and the WatchGuard logo are registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other tradenames are the property of their respective owners. Part No. WGCE67813_022025