WATCHGUARD TECHNOLOGIES: ÉÉN FULL-STACK UNIFIED SECURITY PLATFORM

‘Het nieuwe werken, end-to-end beveiligd voor iedere organisatie’

Thuiswerken is inmiddels de gewoonste zaak ter wereld geworden. Of beter gezegd, de situatie waarbij medewerkers afwisselend vanuit huis en kantoor werken. De security van zulke hybride werkplekken is daarmee belangrijker dan ooit tevoren. Martijn Nielen, Senior Sales Engineer bij WatchGuard, belicht in vleugelvlucht de effectiviteit van Endpoint Protection, Detection & Response (EPDR) en de voordelen van WatchGuard Cloud. *Tekst: Arnold le Fèbre*

In 2020 rondde WatchGuard Technologies de overname af van Panda Security. Alle Panda-producten werden als onderdeel van de integratie opgenomen in het endpointportfolio van WatchGuard. Dit portfolio bestaat nu uit EPP (EndPoint Protection), WatchGuard EDR (Endpoint Detection and Response) en WatchGuard EPDR (Endpoint Protection Defense and Response). De endpointsecurity is volledig geïntegreerd in het nieuw ontworpen WatchGuard Cloud.

Martijn Nielen: “Deze producten maken ons portfolio compleet en sluiten aan op onze visie dat je enterprise-grade security supereenvoudig moet maken voor iedere organisatie. We beveiligen niet alleen de Windows- en MacOS-endpoint tegen ransomware-aanvallen, maar je kunt door multifactorauthenticatie (MFA) ook veilig inloggen op die endpoint of applicaties. Alle oplossingen zijn te managen vanuit de centrale bedieningsconsole WatchGuard Cloud. Dankzij de integratie van netwerk-, identiteits- en endpointbeveiliging verenigen we diverse beveiligingsproducten in één full-stack Unified Security Platform.”

Vijf schillen

WatchGuard EPDR werkt met vijf schillen, die steeds een ander securityprobleem ondervangen en tegelijk of afzonderlijk van elkaar opereren, legt Nielen uit. De eerste schil is de antiviruslaag, die - al dan niet geholpen door heuristische technieken - nieuwe bedreigingen opspoort. De tweede en derde laag zijn respectievelijk de contextuele laag (die onder meer exploits tegenhoudt) en de anti-exportlaag. De vierde laag speelt een grote rol, benadrukt Nielen. “Deze laag wordt ook wel de ‘100% attestation’-laag genoemd en wordt door ons omschreven als ‘zero trust application service’. Hierbij wordt op basis van een groot aantal criteria uiteenlopende software gescand en waar nodig onschadelijk gemaakt. 99.98% van de business-applicaties wordt automatisch herkend. Deze laag is enorm belangrijk om malware en goodware (en alles wat daartussen zit) te identificeren en te classificeren. Als niet direct duidelijk is of iets malware of goodware is, gebruiken we machine learning om dit op basis van AI volledig geautomatiseerd vast te stellen.”

Tot slot is er de vijfde schil, waarbij via cloudconnectiviteit onze threat hunting-experts snel kunnen schakelen om het minieme aantal ongeïdentificeerde zaken in (verzamelingen van) endpoints nader te bekijken.

Alles via de cloud

Nielen: “Alles wat we doen, is volledig via de cloud te managen voor alle platformen (Windows, Mac, Android en zeer binnenkort iOS). Onze oplossingen vragen bovendien weinig CPU-kracht op de endpoint. De footprint van onze securityoplossingen is zeer beperkt, vooral omdat alle functies zijn uit te voeren met één agent. Belangrijk om te benadrukken is dat we de cloud als middel gebruiken om onze security makkelijker te kunnen uitrollen, te beheren en te automatiseren, en niet als doel op zich. Wat er gebeurt als de cloud niet beschikbaar is? Er staat ook een grote hoeveelheid informatie lokaal in de cache; als er geen internetverbinding is, kunnen we dit in de meeste gevallen lokaal afvangen.”

Veel securityrisico’s vinden hun oorsprong in niet-gepatchte systemen, die draaien op een oude Windows-versie of op applicaties die niet zijn bijgewerkt. “Heel veel patchoplossingen zijn afhankelijk van een verbinding met een on-premise server”, vertelt Nielen. “WatchGuard heeft ervoor gekozen – in 2016 al, dus nog ver voor we massaal moesten thuiswerken - om alle securityfunctionaliteit inclusief de patches en updates, volledig via de cloud te draaien. Kortom, WatchGuard biedt een compleet securitypakket voor het nieuwe werken, end-to-end beveiligd en voor iedere organisatie.” ■