ENDPOINT SECURITY

Endpoint security; deze term is één van de meest gehoorde in de afgelopen jaren tijdens grote security-events, -conferenties, -webinars en in -blogs. De een noemt het een verplicht onderdeel van het securityplatform, de ander zegt dat het slechts een nieuwe term voor antivirus is en weer anderen noemen het een overschatte aanpak. Een ding is duidelijk: het is een term die niet direct duidelijk maakt wat er van moet worden verwacht.

In deze blog zal ik het hebben over endpoint security, wat het echt betekent, en **waarom organisaties dit zonder twijfel nodig hebben.**

Endpoint security beveiligt apparaten van eindgebruikers, zoals mobiele apparaten, laptops, desktop-pc's en servers. Kortom: elk apparaat dat is verbonden met uw bedrijfsnetwerk. Deze apparaten kunnen worden beschouwd als een **toegangspunt tot het netwerk**.

Gartners definitie van endpoint security

Gartner brengt elk jaar diverse Magic Quadrants uit, waaronder die voor endpoint security, welke voor de meeste bedrijven een basislijn vormt voor diens beveiligingsstrategie. In hert Magic Quadrant voor endpoint security wordt elk jaar de sterke en zwakke punten van 21 Endpoint Protection Platform (EPP) leveranciers geëvalueerd. In 2018 definieert Gartner endpoint security als een "*solution deployed on endpoint devices to prevent file-based malware, to detect and block malicious activity from trusted and untrusted applications, and to provide the investigation and remediation capabilities needed to dynamically respond to security incidents and alerts.*" Ik vind het belangrijk om deze definitie hier te plaatsen omdat, zoals dit altijd gaat in de informatiebeveiliging, deze benadering hoogstwaarschijnlijk tijdelijk is en in de loop van de tijd zal veranderen. De bovenstaande definitie staat bijv. in contrast met de definitie van 2017. Zo werd Endpoint Detection and Response (EDR) in 2017 essentieel geacht, maar in 2018 wordt het volgens Gartner als een welkome aanvulling beschouwd.

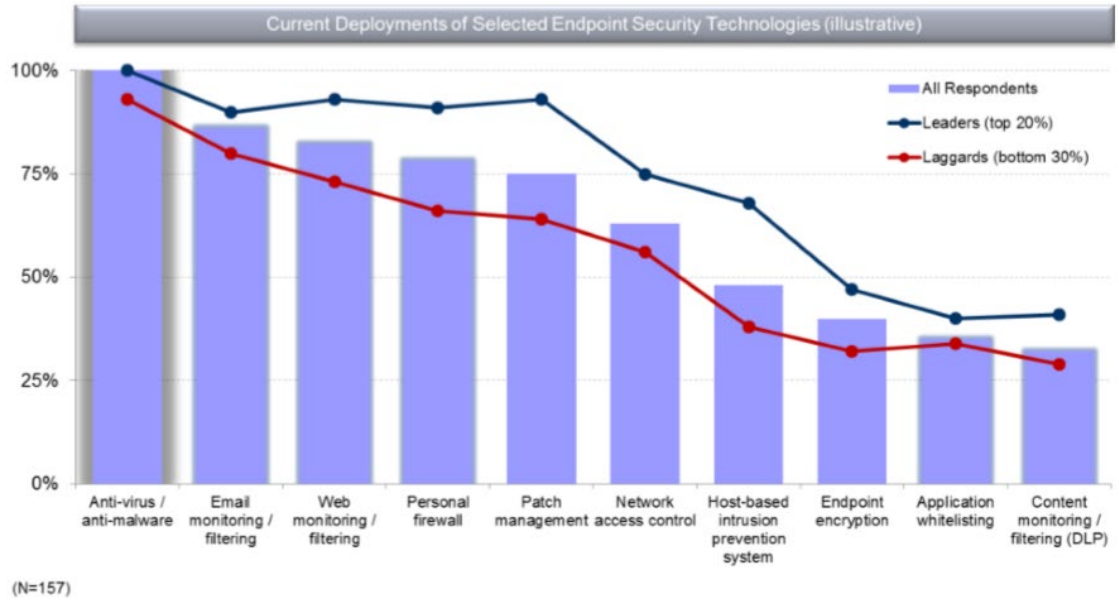
Evolutie van systemen en veiligheidsmaatregelen

Waarom moet u in het bezit zijn van een gedegen endpoint beveiliging? Is end-to-end monitoring van packet transfers en het 'dichtzetten' van het

hele netwerk middels firewall-regels niet voldoende? Het antwoord is: **nee, dat is het absoluut niet!**

Naarmate bedreigingen in de afgelopen jaren evolueerden, kon de aanpak van endpoint security ook niet achter blijven. De basisvereisten voor een relatief klein bedrijf kunnen misschien bestaan uit een firewall en een antivirusoplossing, waarmee zij zichzelf als veilig beschouwen. Echter, de beveiliging in het echte leven waar het gehele risico bestaat, **daar zou de aanpak technologisch wat volwassener moeten zijn**. Niet zo complex zodat het hele proces onmogelijk wordt, maar complex genoeg om veilig te blijven. Antivirussoftware en persoonlijke firewalls kunnen worden beschreven als eenvoudige vormen van endpoint security. Moderne endpoint security maakt echter gebruik van meer geavanceerdere methodologieën. Deze omvatten detectieve mechanismen die **bedreigende acties en gedrag identificeren en blokkeren**, hetzij van eindgebruikers, hetzij van indringers.

Figure 2: All Organizations Have Deployed Anti-Virus Software



Het zijn niet alleen bedreigingen of veiligheidsrisico's die in de loop van de tijd **evolueren**. Het zijn ook systemen, IT-structuren die worden gebruikt, de evolutionaire verschuiving van datacenters met op hardware gebaseerde systemen naar virtuele omgevingen, private/public cloud infrastructuur, etc. Bijvoorbeeld: de term 'backend-systeem' verwijst allang niet meer alleen naar hosts, opslag en applicaties binnen een datacenter,

maar tegenwoordig ook naar gevirtualiseerde resources in het datacenter of in de cloud. Zo is het ook met endpoints; deze term heeft niet alleen betrekking op traditionele apparaten, maar **ook op mobiele apparaten als telefoons en tablets.** Netwerken verwijzen niet alleen naar elektronische interconnecties en protocollen tussen systemen, maar ook naar sociale verbindingen tussen mensen, zowel binnen als buiten de grenzen van de organisatie.

Dit betekent dat er **verschillende beveiligingsvereisten zijn.** Met de **toename van mobiele dreigingen** en gebruik van mobiele apparaten, is de behoefte aan effectieve endpoint security maatregelen navenant toegenomen. Mobiliteit van medewerkers maakt dat de effectiviteit van netwerkbeveiliging minder wordt, omdat de controle over het netwerk **via firewalls niet meer voldoende is**. Ook hebben we te maken met endpoints in geïsoleerde netwerken die sommige bedrijven gebruiken voor speciale doeleinden en het feit dat deze niet verbonden zijn met een netwerk of zeer beperkte connectiviteit hebben. Het updaten, monitoren en beheren van dergelijke endpoints wordt daarmee bemoeilijkt en dit stelt dus ook weer andere eisen aan de beveiliging ervan.

Bron: Orange Cyberdefense