Advanced Endpoint Protection

1 Inleiding

In de huidige dynamische securitywereld wemelt het van de verschillende endpoint beschermingsproducten. Van traditionele standalone antimalware oplossingen voor kleine omgevingen, next generation endpoint protection oplossingen tot uitgebreide Enterprise Connected Advanced Endpoint Protection oplossingen.

Onderstaand document tracht een eerlijk en helder beeld van de eisen welke door organisaties gesteld moeten worden aan endpoint protectie oplossingen, om ook voor de komende jaren van de juiste endpoint bescherming verzekerd te zijn. Deze informatie helpt bij het opstellen van de juiste eisen voor de selectie van een toekomstbestendige endpoint protectie.

1.1 Opmerking

Ondanks dat sommige beschreven eisen en technologieën kunnen overkomen als eisen alleen bedoeld voor de grotere veeleisende of security technisch volwassen organisaties, is echter gebleken dat de bedreigingen en oplossingen ook gelden voor kleinere en/of security technisch minder veeleisende of volwassen organisaties. De bedreigingen en oplossingsmogelijkheden zijn dan ook identiek voor elke IT omgeving.

© 2019, - all rights reserved. No part of this publication may be shared, reproduced or transmitted to third parties in any form or by any means, or stored in any retrieval system of any nature, without the written permission of Amitron, the Netherlands.

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

Inhoudsopgave

1 Inleiding 1
1.1 Opmerking 1
2 Externe factoren 4
2.1 IT omgevingen veranderen 4
2.2 Gebruikers veranderen 4
2.3 Organisaties veranderen 4
2.4 Risico's en bedreigingen veranderen 4
2.5 Wetgevingen veranderen 5
2.6 Cyber Security's 3 paradigmaverschuivingen 5
2.7 Van netwerk- naar endpoint- en databescherming 5
2.8 Geconsolideerde centrale rapportage, beheer en integratie met informatie-systemen 5
2.9 Tooling: van multi-vendor beleid naar geconsolideerd beleid 5
2.10 "Cyber security is een werkwoord" 6
3 De evolutie van endpoint bescherming 7
3.1 Signaturebased endpoint antivirus 7
3.2 Next Generation endpoint protectie oplossing 7
3.2.1 Next Generation Protection alleen voldoende? 7
3.2.2 Oorsprong en toekomst next generation endpoint protectie? 8
3.3 Advanced Endpoint Protection 8
4 Advanced Endpoint Protection 9
4.1 Vulnerabillity shielding tegen application vulnerabilities 9
4.2 Reputation Services (files, app, web & email) 9
4.3 Newly Encountered Program protection enhancement 9
4.4 Traditional AV 9
4.4.1 Smart Scan 9
4.4.2 True file identificatie 9
4.5 Heuristics 10
4.6 Machine learning: pre-execution 10
4.7 Application control 10
4.8 Suspiscious connections 10
4.9 Behavioral analysis 10
4.10 Ransomware bescherming: Cryptokiller 10
4.11 Machine learning: runtime 11
4.12 False positives & Noise Cancellation 11
4.13 Sandbox Suspicious File Sample Submission 12

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

5 Enterprise Connected Advanced Endpoint Protection 13
5.1 DLP 13
5.2 Onpremise Customized Sandbox 13
5.3 Device control 13
5.4 VDI plugin 13
5.5 Hostbased firewall 13
5.6 Hostbased IPS 13
5.7 Endpoint Encryption 13
5.8 Mobile Security 14
5.9 Linux en Mac ondersteuning 14
5.10 Endpoint Detection en Response (EDR) 14
5.11 Centrale beheerconsole met role based admin 14
5.12 Centrale user security rapportage 14
5.13 Edge Relay server 15
5.14 Schaalbaar 15
5.15 Technologie uitbreidbaar 15
5.16 Integratie met externe informatiesystemen 15
5.17 Supportondersteuning 15
6 Marktanalisten 16
6.1 Gartner 16
6.2 Forrester 16
6.3 NSS Labs 17
6.4 AV-test.org 18
6.5 AV-comparatives.org 19

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

2 Externe factoren

Bij een goed doorgronde selectieprocedure hoort ook een goed beeld of visie over de toekomst waarin de securityoplossing dient te functioneren. De volgende veranderingen zouden bij een selectie door een organisatie aan bod moeten komen en onderdeel moeten vormen van de oplossing. Deze moeten tot zover mogelijk afgedekt worden door een toekomstgerichte beveiligingsoplossing.

2.1 IT omgevingen veranderen

IT omgevingen veranderen van traditionele lokale hardware- en software-installaties naar gecombineerde virtuele, hyperconverged infrastructures of Software Defined Networks in private, hybride, publieke of bursting cloud omgevingen. Voor veel organisaties is dit reeds de realiteit geworden door de dynamiek van hun eigen business processen. De securityfocus verschuift hierdoor van het traditionele eigen netwerk- en perimeterniveau naar de richting van de gebruikers en data, onafhankelijk van de fysieke locatie. Hedendaagse security-oplossingen moeten hierbij flexibel ingezet kunnen worden, zowel op technisch, administratief als financieel vlak.

2.2 Gebruikers veranderen

Gebruikers eisen en krijgen steeds meer invloed op de te volgen koers van een IT afdeling. Voorbeelden hiervan zijn processen zoals consumerization, ''Het Nieuwe Werken'' en de wens altijd via elke device met persoonlijke Internetdiensten in contact te kunnen zijn. Het gebruik van mobiele devices, managed laptops, of unmanaged (thuis)werkplekken moeten door securitymaatregelen niet belemmerend maar juist ondersteunend te worden.

2.3 Organisaties veranderen

De groeiende complexiteit van securityproducten in combinatie met de nieuwe bedreigingen eisen een grotere securitykennis en -ervaring van de IT systeembeheerders. De huidige tendens is echter dat binnen vele organisaties de beschikbaarheid van specialistische kennis binnen een krimpende werknemersgroep steeds moeilijker te realiseren valt. Hierdoor ontstaat een risicovolle ''beveiligingslacune''. Dit zal opgevangen dienen te worden door het verminderen van de totale complexiteit van verschillende producten door een geïntegreerde single vendor policy en de regelmatige inhuur van specialistische externe ondersteuning of het gebruik van een managed security partners opgevangen dienen te worden.

2.4 Risico's en bedreigingen veranderen

De securityrisico's voor organisaties zijn veranderd. De globale en massale virusuitbraken van weleer hebben plaats gemaakt voor kleinschalige en gerichte unieke aanvallen.

Gerichte aanvallen hebben niet meer als einddoel om op te vallen of om uw werkzaamheden te verstoren. Het einddoel is nu gericht om na de initiële infiltratie en opvolgende verkenningsperiode voor een onbepaalde periode schade toe te brengen of data te ontvreemden. Hierbij proberen aanvallers juist zolang mogelijk onopgemerkt toegang te hebben tot uw data, systemen en netwerken. Risico's komen niet alleen via web- en emailverkeer op organisaties af, maar ook via allerlei bestaande en nieuwe routes. Bijvoorbeeld via vertrouwde netwerkverbindingen of bewust of onbewust via de eigen medewerkers. Hierdoor zijn de gevaren complexer en de risico's groter geworden. Traditionele preventieve securitymaatregelen zijn dan niet meer toereikend. Additionele geïntegreerde securitymethoden spelen in snel toenemende mate een onomkeerbare rol.

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

2.5 Wetgevingen veranderen

Nederlands en Europese privacywetgevingen worden vanaf 2018 verscherpt inclusief een meldplicht bij inbraken en hoge boetes. Ook voor vitale infrastructuren zijn er strengere wetten in de maak. Een aantoonbaar inzet van eenvoudige eerste generatie preventieve beveiliging zoals firewall en antimalware zal bij geconstateerde datalekken niet meer toereikend zijn om een organisatie te beschermen tegen serieuze sancties. Endpoints zijn momenteel juist het einddoel en bron van datalekken.

2.6 Cyber Security's 3 paradigmaverschuivingen

Een hedendaagse Cyber security professional houdt rekening met 3 paradigmaverschuivingen:

1) De vraag is niet meer òf er een keer succesvol ingebroken wordt bij een organisatie wordt, maar wannéér.
2) De securityfocus verschuift van de netwerkperimeter (firewall) naar interne/externe cloud infrastructuren, gebruikers en data.
3) De securityfocus verschuift van de traditionele losse producten naar geïntegreerde en connected securitysystemen.

Deze paradigmaverschuivingen hebben invloed op de benaderingswijze van beveiliging, de focus van kennis en aandacht en de budgettoewijzing binnen organisaties.

2.7 Van netwerk- naar endpoint- en databescherming

Door de virtualisatie en netwerk agnostische manier waarnaartoe de IT wereld verschuift is de focus van de bescherming van (gevoelige data) aan het veranderen van de statische netwerk gerelateerde oplossingen naar endpoint en data bescherming. Dit is tevens device-, data en locatie onafhankelijk. De endpoint wordt steeds belangrijker omdat door het toenemende gebruik van versleutelde verbindingen en SaaS diensten, er direct toegang is tot data buiten het netwerk en buiten het zicht van de reeds geïnstalleerde netwerk security tooling.

2.8 Geconsolideerde centrale rapportage, beheer en integratie met informatie-systemen

Naarmate organisaties volwassener worden wordt geconsolideerde security informatie vergaring en presentatie voor zowel de onpremise als cloud/SaaS belangrijker. Dit is van belang om snel en adequaat te kunnen acteren, voorspellen en te rapporteren om aanvallen te kunnen analyseren en neutraliseren en om compliance met regel- en wetgeving aan te kunnen tonen.

2.9 Tooling: van multi-vendor beleid naar geconsolideerd beleid

In het verleden (lees: tot enkele jaren terug) was de techniek van antimalware tooling volledig gebaseerd op basis van herkenning van bedreigingen (virussen, malware) aan de hand van een zo courant mogelijke signature database. Het was daarbij wijselijk om een dual vendor of 2-laagse bescherming te hanteren op basis van minimaal 2 fabrikanten. Zodoende was er in het geval dat een (nieuw) virus nog niet bij de ene fabrikanten in database geüpdatet was, de hoop dat de database van de andere fabrikant dat misschien wel al had. De extra beheerlast die dit met zich meebracht nam men voor lief toe.

Echter zijn er de laatste jaren enkele zaken rigoureus veranderd:

- het type aanvallen zijn anders
- security is complexer
- organisaties veranderen

Momenteel is het relevanter aan het worden om securityoplossingen te integreren of te connecteren met elkaar. Hierna wordt informatie over (nieuwe) aanvallen direct met elkaar gedeeld en kan er organisatie breed op worden geacteerd. Deze connecties bestaan binnen het oplossingsportfolio van één fabrikant en ontstaan in toenemende mate binnen ecosystemen van complementaire producten van verschillende fabrikanten.

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

2.10 “Cyber security is een werkwoord”

Cyber security is een continue proces, door het veranderen van de IT omgevingen, de gestelde eisen en bedreigingen. Cyber security is daarom ook uitdagend. Organisatie en specialisten worden continu uitgedaagd om continu passende en ontzorgende oplossingen te bieden voor de bescherming van de beschikbaarheid, integriteit en vertrouwelijkheid van de digitale informatie van organisaties. Deze bescherming moet van het hoogst mogelijke niveau zijn ongeacht het grootte of type organisatie. De bescherming moet onafhankelijk zijn van tijdstip en plaats van data en persoon.

Door de complexiteit van zaken en de veranderingen in het IT (security) landschap is een voorheen een standaard eenvoudig endpoint antivirus verworden tot een technisch complexer en snel evoluerend product dat niet meer volledig op zichzelf als standalone product functioneert. Om dit effectief te laten functioneren neemt de behoefte aan specialistische (externe) kennis ook toe.

Een cyber security dienstverlener kan contractueel en technische de verantwoording op zich nemen om de operationele security uit te voeren voor elke organisatie. De organisaties zelf blijven echter juridisch altijd eindverantwoordelijk voor de effectieve bescherming van haar eigen informatie. Men voert het beveiligingswerk dus altijd gezamenlijk uit.

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

3 De evolutie van endpoint bescherming

De endpoint protectie oplossingen lijken te kunnen worden verdeeld tussen signaturebased endpoint antivirus (AV), Next Generation endpoint protection (NG) en (Enterpise Connected) Advanced Endpoint protection oplossingen (EPP).

Eenvoudig en grofweg kan men de volgende stelregels hanteren:

3.1 Signaturebased endpoint antivirus

Hiermee is het antivirus product ongeveer 30 jaar geleden mee ontstaan. Van elk ontdekt kwaadaardig bestand (virus, Trojans, spyware, worms, adware, ransomware, etc.) wordt na analyse door de fabrikant een zogenaamde hash/signature gemaakt en centraal wereldwijd gedistribueerd naar al de endpoint oplossingen. Daarna wordt dit bestand in het vervolg herkent door endpoints en gekwalificeerd als virus en opvolgend door de endpoint oplossing gedeletet of in quarantaine geplaatst.

Deze antivirus techniek is, ondanks dat het niet meer toereikend is voor het volledig zelfstandig beschermen van een endpoint tegen de huidige bedreigingen, door de effectiviteit ervan, nog altijd een belangrijk onderdeel van elk goed werkende antimalware endpoint bescherming. Een op zichzelf staande opmerking als ''antivirus is dead'' is onzinnig, maar moet in het licht gezien worden van additionele technieken die nodig zijn voor een hedendaagse bescherming.

3.2 Next Generation endpoint protectie oplossing

De recent veelvuldig gehoorde opkomende zogenaamde Next Generation endpoint protectie oplossingen haken in op het feit dat pure signaturebased antivirusprogramma's niet opgewassen zijn tegen de hoeveelheid nieuwe unieke geïnfecteerde bestanden en andere antimalware o.a. polymorphic malware en malware afgeleverd door zero-day exploits, etc.

Next Generation endpoint protectie oplossingen herkennen niet meer de bestanden via een signature (hash) maar kijken hoofdzakelijk pas naar de processen die bij uitvoer van een kwaadaardig bestand/malware opgestart worden. Deze processen wordt vergeleken dit processen die typisch door malware misbruikt worden. Het kwaadaardig gekwalificeerde proces wordt dan gemeld en eventueel gestopt. Typisch kan de schade van malware hierdoor gestopt worden zonder herkenning van de malware (hash) zelf. Nieuwe onbenoemde malware zou dus zo ook tegengehouden kunnen worden, iets dat een pure signaturebased endpoint antivirus dus niet kon.

3.2.1 Next Generation Protection alleen voldoende?

Er vindt bij de Next Generation endpoint protectie oplossing nog altijd een herkenningsproces plaats (proces), echter is het aantal processen dat jaarlijks nieuw moeten worden toegevoegd tot de lijst van de Next Generation endpoint protectie oplossingen veel lager dan het aantal nieuwe signatures (2-4 per jaar)

Er wordt misleidend nog wel gesproken dat een Next Generation endpoint protectie oplossing efficiënter is dan een signaturebased oplossing en deze ook compleet overbodig maakt. Hier moet men niet in trappen, dat is niet waar: nog steeds maakt een Next Generation endpoint protectie oplossing gebruik van herkennen van processen, welke -weliswaar minimaal- geüpdatet dient te worden. Een Next Generation endpoint protectie oplossing beroept zich o.a. op het whitelisten van al de toegestane programma's welke ook gebruik maken van dezelfde verdachte processen. Dat is arbeidsintensief en in dynamische omgevingen lastig te beheren. Daarnaast levert het in afwijkende (virtuele) omgevingen de nodige performance problemen op.

Elk bestand/programma wordt tijdens de bestandsuitvoering door een Next Generation protection oplossing op procesniveau geanalyseerd, er vindt hier dus geen voorselectie plaats. Vooral in virtuele omgevingen levert dit een performance probleem op.

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

Om een Next Generation endpoint protectie oplossing zoals hierboven beschreven goed te laten werken dient er alsnog een antivirus/antimalware naast te draaien. Het onderhouden van twee oplossingen met twee management, beheer- en rapportageomgevingen is binnen grotere organisaties en dynamische omgevingen een prijs- en beheerstechnische uitdaging.

Next Generation endpoint oplossingen zijn daarnaast vaak gelimiteerd in het leveren van één of enkele technieken: bescherming tegen antimalware via proces herkenning. Dit terwijl de uitgebreide enterprise advanced endpoint protectie oplossingen meerdere geïntegreerde (optionele) security oplossingen bieden welke van toepassing zijn in (grotere) omgevingen.

3.2.2 Oorsprong en toekomst next generation endpoint protectie?

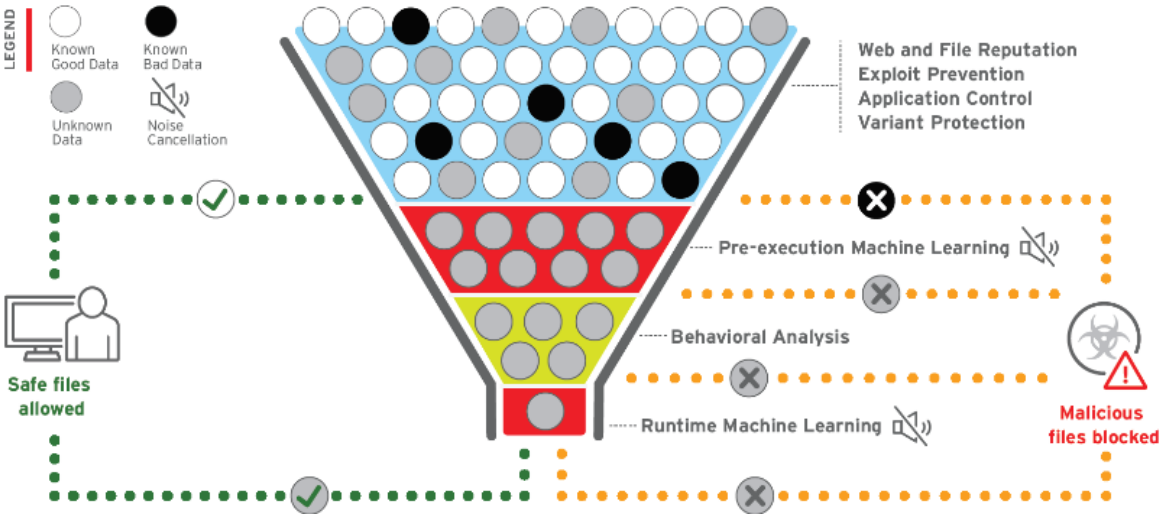
De reden dat deze een Next Generation endpoint protectie oplossingen met redelijk veel bombarie opkomen is hoofdzakelijk omdat het aantrekkelijk is voor nieuwe (firewall)fabrikanten om zonder de jarenlange technische knowhow en ervaring op endpoint protectie gebied, zich eenvoudig te kunnen mengen in deze nog steeds lucratieve endpoint protectie markt.

Men zal echter zien dat de een Next Generation endpoint protectie oplossing uitgroeien tot of als techniek geïntegreerd raken in de bestaande volwaardiger Advanced Endpoint Protection oplossingen.

3.3 Advanced Endpoint Protection

Oplossingen waarbij van meerdere preventieve oplossingen gebruikt worden gemaakt noemt men Advanced Endpoint Protection oplossingen. Beproefde preventie technieken worden hierbij in serie gebruikt waarbij de meest efficiënte preventie techniek als eerste plaatsvindt gevolgd door de volgende, totdat er uitsluitsel plaats heeft gevonden (niet/wel ''goed'' bevonden). Dit betekent dat niet elk scanproces hoeft te worden doorlopen. Deze trechter aanpak bevordert de efficiëntie van de totale oplossing.

Afbeelding 1: Trechter preventie techniek Advanced Endpoint Protection



Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

4 Advanced Endpoint Protection

Een Advanced Endpoint Protection oplossing maakt typisch van de onderstaande volgorde van processen gebruik. Als voorbeeld is het product Trend Micro OfficeScan 12 (XG) ter hand genomen.

4.1 Vulnerabillity shielding tegen application vulnerabilities

Als eerste wordt de virtual patching of vulnerability shielding techniek gebruikt die het endpoint protectie in staat stelt zero day threats en exploits te detecteren en te blokkeren op basis van applicatie kwetsbaarheden welke op de endpoint geïnstalleerd zijn. Processen in gedownloade bestanden welke misbruik proberen te maken van bekende Common Vulnerabilities and Exposures (CVE) kwetsbaarheden in gebruikte producten worden herkend en direct al geblokkeerd.

4.2 Reputation Services (files, app, web & email)

Trend Micro checkt de bron van de bestanden, als deze bekend staan als 'known' malware bronnen worden deze geblokkeerd. Dit bestaat voor files, apps, web URL's en email servers. Voordeel van deze techniek is dat de content niet geïnspecteerd hoeft te worden. Bestanden hoeven niet geopend te worden een hash check is voldoende. De benodigde resources zijn hierdoor erg laag. De Webreputation service zorgt ervoor dat alleen betrouwbare webpagina's bezocht worden waar geen spyware of malware op aanwezig is. Dit gaat per pagina en niet per hele site om een ongewenste totale website blokkade te voorkomen.

4.3 Newly Encountered Program protection enhancement

Met deze engine wordt een gedownloade file via HTTP(s), e-mail of Microsoft Office Marco Scripts geclassificeerd door te kijken naar het aantal eerder voorgekomen wereldwijde detecties en de historische leeftijd. Deze worden bijgehouden in het centrale Smart Protection Network met de reputation services.

4.4 Traditional AV

Vervolgens wordt nog steeds een van de efficiëntste beschermingstechnologieën als signaturebased herkenning toegepast. Real-time Scan, Manual Scan, Scheduled Scan van bestanden op basis van blacklisted en white listed hashes. Bij deze techniek wordt de bestandcontent vergeleken met een lijst van bekende malware signatures. Ondanks dat het niet toereikend is voor de totale bescherming is door de efficiëntie ervan dit een belangrijk proces.

4.4.1 Smart Scan

Lokale Trend Micro Smart Scan servers of vanuit de cloud via het Trend Micro Smart Protection Network reduceren de hoeveelheid data in de lokale signature databases op de endpoints en de scansnelheid. Twintig procent van alle signatures die bekend zijn, wordt nog lokaal opgeslagen. Dit omvat circa alle malware die het laatste jaar frequent is voorgekomen. De overige tachtig procent wordt opgeslagen in het Smart Protection Network en zal alleen worden geraadpleegd wanneer dit van toepassing is. De Smart Scan server met deze informatie kan ook als kopie on premise toegepast worden ter bevordering van de distributiesnelheid.

4.4.2 True file identificatie

Een techniek om files te identificeren vóór het scannen. Deze true file type identificatie controleert of een file überhaupt gevoelig is voor een besmetting. Anders dan bij file extensie herkenning wordt bij true file type de eerste 4kB van een file geanalyseerd om te bepalen of een file daadwerkelijk gescand dient te worden. Dit verhoogt de performance van het systeem dramatisch.

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

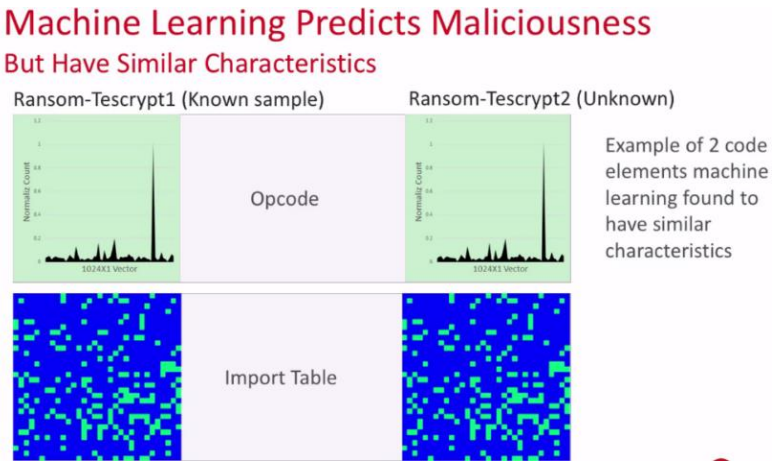
4.5 Heuristics

Heuristic scanning controleert de inhoud van een bestand op system commands, bijvoorbeeld file, I/O & Netwerk commando's. Mochten bepaalde technieken worden ontdekt dan zal op basis van een threshold techniek de severity worden bepaald (low – medium – high). Heuristic scanning voorspelt wat er misschien mis gaat met het systeem wanneer de desbetreffende file wordt geopend. Een heuristic scan wordt uitgevoerd vóórdat het bestand wordt geopend.

4.6 Machine learning: pre-execution

Detecteert in de low level Opcode van bestanden ''pieken'' welke in context met elkaar worden vergeleken met de pieken van bekende malware families. Dit is een zeer efficiënt proces tegen het beschermen tegen de nog onbekende zero days exploits.

Afbeelding 2: Next generation techniek: Machine learning: pre-execution



4.7 Application control

White- en blacklisting van applicaties op basis van naam, path en certificaten. Applicaties zijn gecategoriseerd en worden geadviseerd en automatisch bijgehouden. Handmatig kunnen applicaties worden toegevoegd.

4.8 Suspiscious connections

Controle op aanwezigheid van communicatie op basis van de Command & Control (C&C) IP list en het blokkeren van deze ''calling home'' communicatie, welke duidt op een endpoint infectie. Deze techniek werkt ook op systemen welke wellicht al eerder besmet zijn geraakt of misbruikt worden.

4.9 Behavioral analysis

Bij uitvoeren van het bestand wordt gekeken naar het eigenlijke proces en kwaadaardige acties welke bekend zijn misbruik te worden door malware worden gestopt. Met behavior monitoring worden de belangrijkste bestanden van uw systeem gemonitord zoals; host files, browser settings, start-up programs, services etc. Behavior monitoring vergt meer systeem resources dan alle andere technieken. Daarom is deze techniek gelimiteerd tot het monitoren van de kritische componenten zonder de algehele systeem performance nadelig te beïnvloeden. Daarnaast is deze techniek niet afhankelijk van signature updates. Behavior monitoring is constant actief en monitort dan ook constant niet geautoriseerde veranderingen binnen het systeem.

4.10 Ransomware bescherming: Cryptokiller

Trend Micro's Endpoint Cryptokiller proces detecteert het ongewenste encryptie proces van ransomware op het endpoint. Het stopt na het overschreden van een bepaald aantal encrypties binnen een bepaald tijdbestek het proces om lokale, netwerk en Office365 bestanden te beschermen. Daarnaast kan in combinatie met een beperkte caching tot 100Mb de (door ransomware) versleutelde bestanden hersteld en teruggeplaatst worden.

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

4.11 Machine learning: runtime

Machine learning tijdens de runtime is een typische Next Generation Endpoint scanmethode tegen zero days exploits. Hierbij wordt tijdens de uitvoer van een bestand bepaalde losse processen in memory herkent welke een typische antimalware ook vaak uitvoert. Echter door het low level herkenning is er geen context herkenning wat resulteert in hoger aantal false positives, indien alleen van deze technologie gebruikt gemaakt wordt.

4.12 False positives & Noise Cancellation

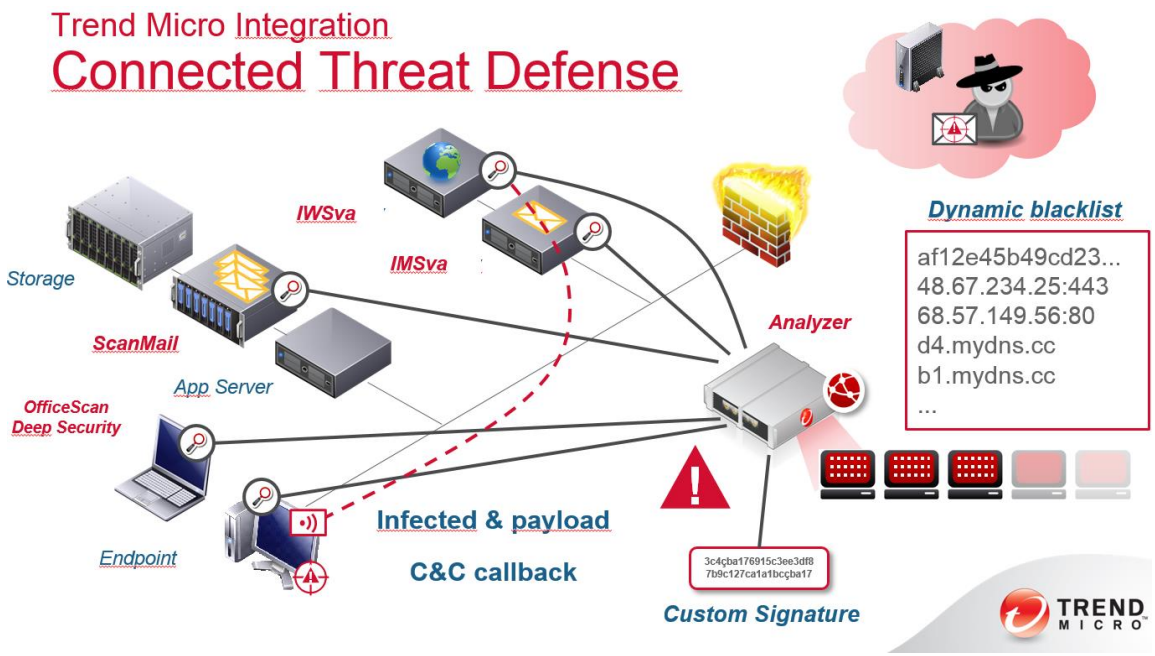
Bij het gebruik van Net Generation technieken moet er een zogenaamde noise cancellation gebruikt worden om het aantal false positives te verminderen. Trend Micro scoort door gebruik te maken van noise cancellation en in combinaties van de verschillende ander scantechnieken zeer goed op het gebied van False Positives. Zie hiervoor de onafhankelijke testresultaten.

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

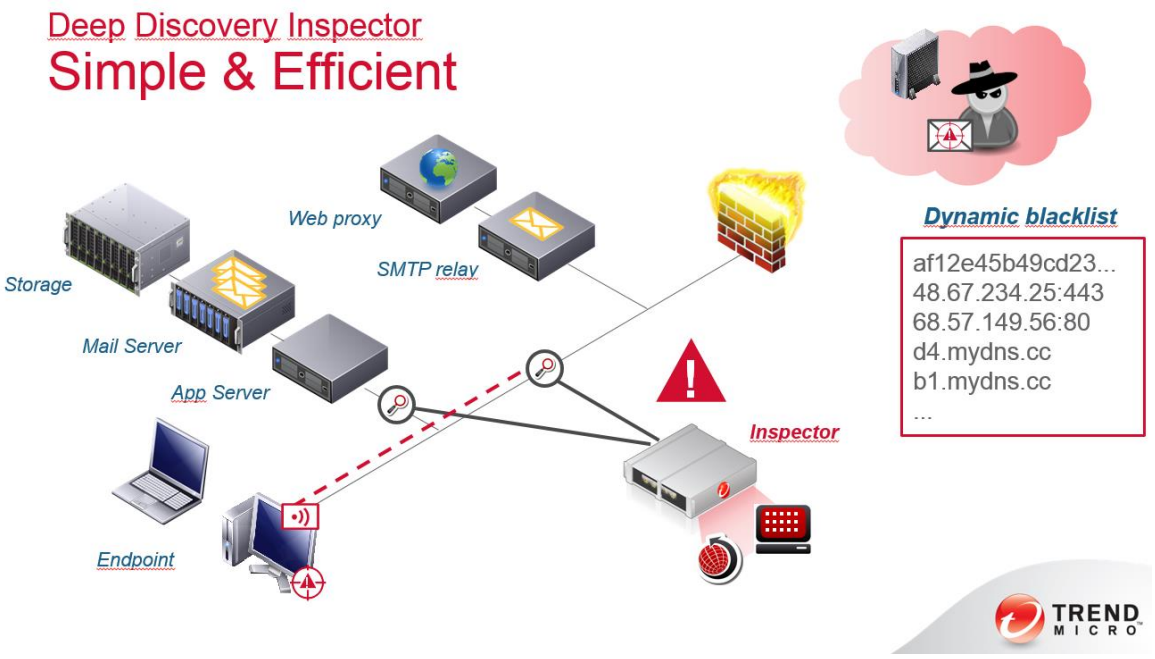
4.13 Sandbox Suspicious File Sample Submission

Endpoint agents kunnen na alle uitgevoerde controles de alsnog resterende verdachte files doorsturen naar de optionele centrale sandbox voor een definitieve 100% analyse, o.a. is dit sandbox-analyse op basis van het gedrag tijdens de daadwerkelijke file executie binnen veilige customized nagebootste omgevingen van de organisatie. Allerlei technieken om de malware te triggeren worden toegepast en het resultaat wordt geanalyseerd. Mocht hieruit alsnog blijken dat er inderdaad een (zero day) risico aanwezig is, dan krijgt de agent dit door en vervolgens worden alle agents (en eventueel andere geconnecteerde Trend Micro en 3de partij producten) automatisch geüpdatet met de adhoc gegenereerde hash van dit object. Hierdoor wordt uw organisatie beschermd nog vóórdat er een wereldwijde update komt van de signature database. Als voorbeeld zal het gebruik van de sandbox in combinatie met email het aantal geslaagde ransomware infecties via email naar 0% kunnen reduceren.

Afbeelding 3: Trend Micro Connected Threat Defense in combianitie met andere producten



Afbeelding 4: Trend Micro Connected Threat Defense met netwerk analyse



Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

5 Enterprise Connected Advanced Endpoint Protection

Om een Advanced Endpoint protection tot Enterprise Connected Advanced Endpoint protection te kwalificeren zullen de volgende (optionele) technieken ter beschikking moeten zijn in de oplossing. Als voorbeeld is het product Trend Micro OfficeScan 12 (XG) ter hand genomen, met complementaire modules en producten.

5.1 DLP

Centraal aangestuurde Data Loss Prevention oplossing. Specifiek voor het tegen gaan van datalekken en de eventueel erbij horende meldplicht/boete. Centraal beheerd en gerapporteerd.

5.2 Onpremise Customized Sandbox

Centrale onpremise sandbox technologie in het eigen netwerk met customized sandboxes. Hierdoor worden bestanden voor de sandbox analyse niet gedeeld met de cloud. Door het gebruik van customized sandboxes is de analyse exacter. De resultaten worden gedeeld ten behoeve van het delen van scan resultaten aan andere producten (connected). Trend Micro maakt onder andere van dezelfde sandbox oplossing gebruik in combinatie met haar volgende beveiligingsoplossingen:

- cloud beveiligingsoplossingen (Office365, Google, Dropbox, Hosted Email, Azure, AWS)
- gateway beveiligingsoplossingen (SMTP en web gateway)
- mailserver beveiligingsoplossingen (Exchange en Domino)
- storage beveiligingsoplossingen (NetApp, EMC en Hitachi)
- endpoint beveiligingsoplossing (Windows, Linux en Mac)
- netwerkanalyse beveiligingsoplossing oplossing (Netwerk Inspector (sniffer))

5.3 Device control

De endpoint protectie oplossing biedt device control mogelijkheden. Policies voor het gebruik van externe media opslag, zoals USB memory sticks kunnen hierbij ingesteld worden. Bijvoorbeeld wordt het gebruik ervan toegestaan, niet toestaan of selectief toegestaan op basis van specifieke USB- of bestandtype.

5.4 VDI plugin

Endpoints agents zijn ‘virtualisatie aware’ ten behoeve van performance winst in virtuele omgevingen. Hierbij worden via een gegenereerde hash de scanresultaten gedeeld tussen de agents op een host, waardoor bestanden éénmalig gescand hoeven te worden. Scheduled scans worden daarnaast gecontroleerd in serie opgestart om overbelasting van de host te voorkomen.

5.5 Hostbased firewall

De endpoint protectie oplossing biedt een granulair instelbare Hostbased Firewall.

5.6 Hostbased IPS

De endpoint protectie oplossing biedt een Hostbased Intrusion Prevention, inclusief een recommendation scan ten behoeve van het eenvoudig adviseren en instellen van de IPS policyset.

5.7 Endpoint Encryption

De endpoint protectie oplossing biedt file-, fulldisk, folder en USB encryptie.

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

5.8 Mobile Security

De endpoint protectie oplossing biedt mobile security, waarbij de organisatie in staat wordt gesteld om security policies af te dwingen op de meest voorkomende mobiele devices (o.a.: Blackberry, Windows, Android en iOS). Hierbij kunt u denken aan anti-malware op Android, App reputation, Web reputation en encryptie. Tevens biedt de endpoint oplossing de standaard MDM functionaliteiten aan zoals het afdwingen van de pincode, remote wipe en remote lock, etc.

5.9 Linux en Mac ondersteuning

De endpoint protectie oplossing biedt ook ondersteuning voor Linux en Mac endpoints.

5.10 Endpoint Detection en Response (EDR)

De endpoint protectie oplossing biedt EDR uitbreidingsmogelijkheden ten behoeve van forensisch onderzoek om een aanval of besmetting te kunnen herleiden naar systeem, gebruiker, bron en route.

5.11 Centrale beheerconsole met role based admin

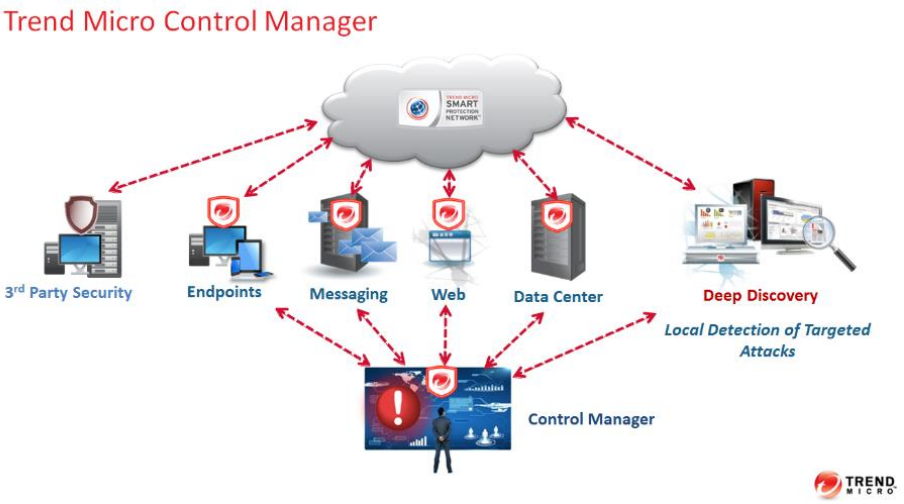
Het centrale management console geeft de mogelijkheid om in het dashboard een persoonlijk en individueel overzicht te maken met gebruik van widgets. Tevens kunnen hele specifieke uitvoerende en leesrechten worden toegekend. Het centrale management heeft 3 standaard rollen: Operator, Power user en Administrator/Root. Zowel additionele rechten als customised rollen kunnen toegevoegd worden.

De rollen kunnen verschillende rechten krijgen om de connected consoles (dashboard) aan te passen of om acties zoals scan, agent update etc. uit te voeren. Men kan ook per user het producten type en onderliggende product management systeem specificeren met betrekking tot wat die user mag zien. Bijvoorbeeld: beheerder A mag alleen de test- of acceptatieomgeving zien, maar beheerder B alleen de productieomgeving, etc. De AD integratie kan gebruikt worden om groepen te creëren van beheerders. Bijvoorbeeld om notificaties te sturen.

5.12 Centrale user security rapportage

De Control Manager centrale rapportage biedt een platform waarmee u een centraal totaaloverzicht krijgt van de security 'status' van al uw connected Trend Micro omgeving en gebruikers (user centric). Naast de manageability van uw on-premise security oplossingen kunt u met de Control Manager ook de 'cloud' security oplossingen van Trend Micro managen en configureren. Bijvoorbeeld voor Azure, AWS en Office 365. Hiermee ontstaat een totaalbeeld van uw interne en externe securitybeleid. Tevens beschikken alle Trend Micro producten over een product specifieke beheerconsole, die door de product specialisten binnen uw organisatie gebruikt kunnen worden voor hun dagelijkse beheerwerkzaamheden.

Afbeelding 5: Trend Micro Connected Control Manager



Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

5.13 Edge Relay server

De Edge Relay server connecteert de remote endpoints die het lokale network veelvuldig verlaten, zoals laptops en andere remote gebruikers met de management server om communicatie tussen de twee mogelijk te maken, zonder hiervoor een VPN verbinding op te hoeven zetten. Dit maakt het volgende mogelijk:

a. Delen van logfiles met de OfficeScan management server
b. Updates van de agents status (pattern files en versie) met de OfficeScan server
c. Synchronisatie van de Suspicious Object lijst met de Control Manager
d. Sandbox connectie voor de analyse van verdachte bestanden met de Deep Discovery Analyzer (additioneel)

5.14 Schaalbaar

De Trend Micro endpoint protectie oplossing is bewezen schaalbaar te zijn binnen grote en complexe omgevingen.

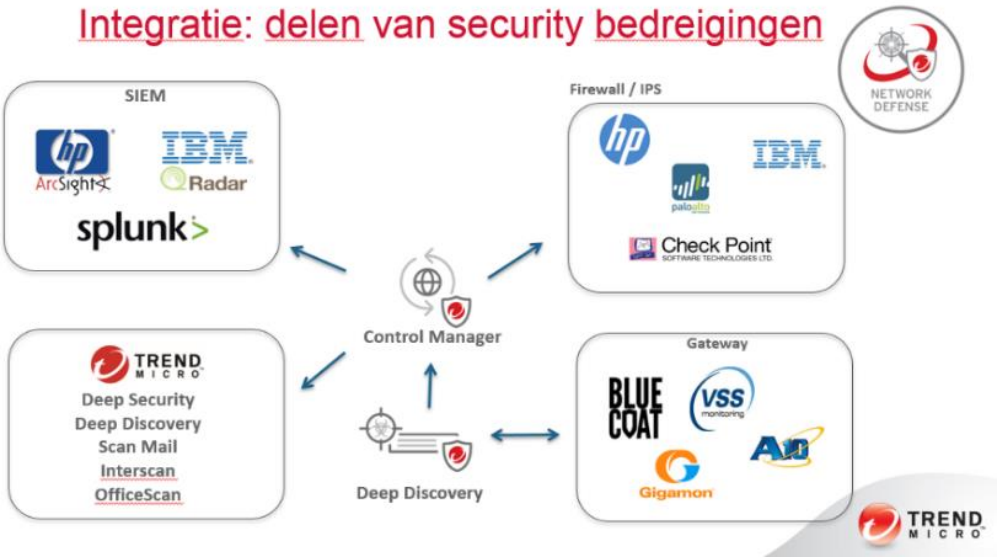
5.15 Technologie uitbreidbaar

Een endpoint oplossing staat niet op zichzelf en kan uitgebreid kunnen worden en samenwerken met oplossingen voor de bescherming van de emailgateway, webgateway, mailserver, firewall, storage, cloudoplossingen, Office365, etc.

5.16 Integratie met externe informatiesystemen

De oplossing dient informatie te kunnen delen met centrale of externe informatiesystemen zoals Security Information and Event Management (SIEM) in bijvoorbeeld een Security Operations Center (SOC). Dit kan onder ander op basis van syslog.

Afbeelding 6: integratie met derde partij informatiesystemen



5.17 Supportondersteuning

Elke security oplossing is net zo effectief als de wijze waarop deze geïmplementeerd en onderhouden wordt. De gehele oplossing kan en moet daarom ondersteund worden door een securityproduct specialist partner met aantoonbare ervaring. Supportmogelijkheden zoals: servicedesk, periodieke health checks, co-managed en fully-managed beheer moeten tot de supportmogelijkheden behoren.

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

6 Marktanalisten

De beste en bekendste advanced endpoint protectie oplossingen worden door verschillende min of meer onafhankelijke marktanalisten en testbureaus gekwalificeerd. Een oplossing is ter overweging waard mits het op meerdere recente onafhankelijke testen/marktanalyses voorkomt en uiteraard goed gekwalificeerd wordt. De volgende marktanalisten zijn veruit de belangrijkste:

6.1 Gartner

"Trend Micro has shown consistent leadership in ability to execute since 2002 and remains a good shortlist candidate for all kinds of buyers"

Afbeelding 7: Gartner Magic Quadrant for Endpoint Protection Platforms 2018

6.2 Forrester

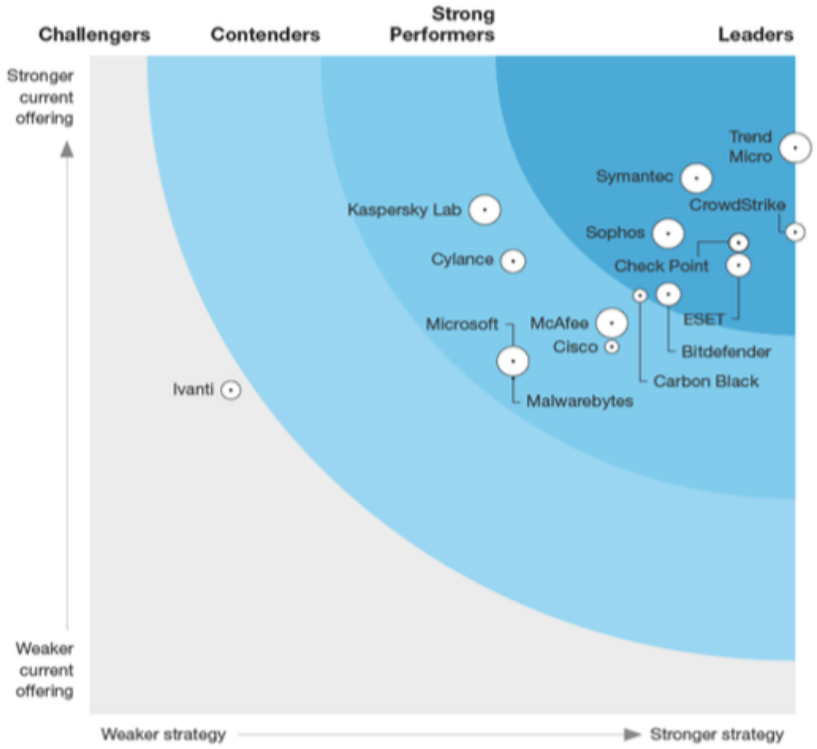
Trend Micro is top ranked in the "Current Offering" category and received the highest score possible in the "Strategy" category in The Forrester Wave™: Endpoint Security Suites, Q2 2018.

Trend Micro's customers give the product high marks for its malware and exploit prevention efficiency, with a low negative impact on endpoint user experience."

"Admins appreciate the product's high level of automation along with its flexibility and scalability to adapt to different operating environments."

Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

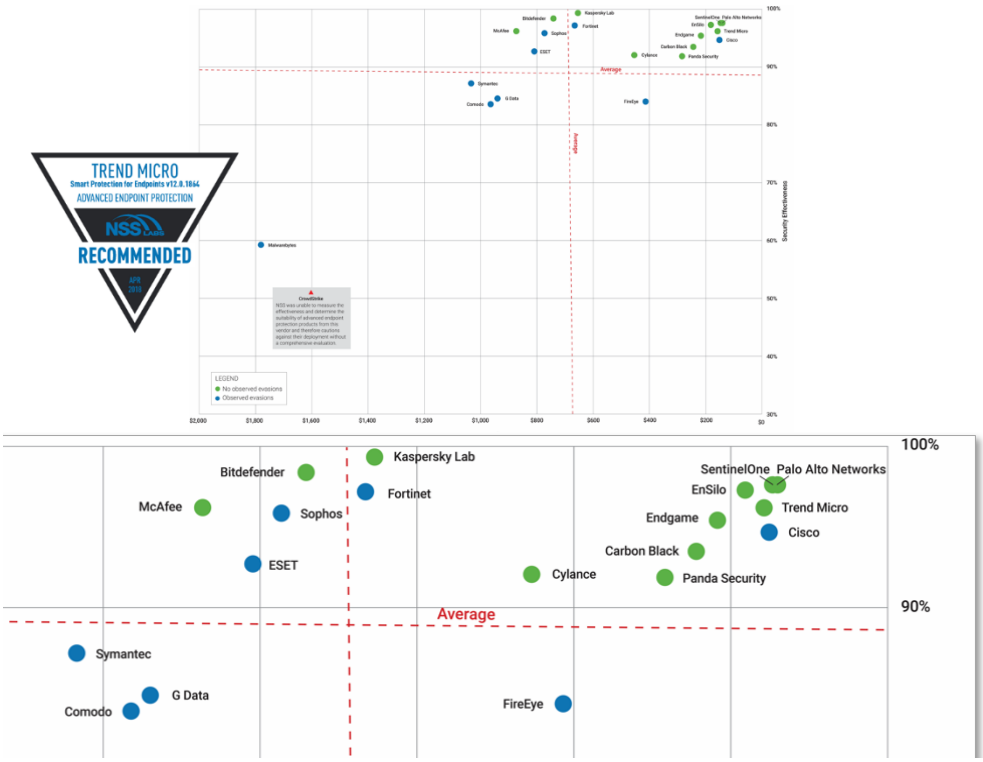
Afbeelding 8: Forrester Wave Endpoint Security Suites 2018



6.3 NSS Labs

''The OfficeScan Agent achieved a Security Effectiveness rating of 98.29%. The OfficeScan Agent did not alert on any false positive samples after the initial tuning. The OfficeScan Agent blocked all of the tested evasions.''

Afbeelding 9: The NSS Labs Security Value Map (SVM).



Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

6.4 AV-test.org

Afbeelding 10: AV-test.org test - april 2018, The best antivirus software for Windows Client Business User.

Producer		Certified	Protection	Performance	Usability
TREND MICRO	Office Scan 12.0		6	6	6
Symantec	Endpoint Protection Cloud 22.12		6	6	5.5
Symantec	Endpoint Protection 14.0		6	6	6
SOPHOS	Endpoint Security and Control 10.8		5.5	5.5	6
SECRITE	Endpoint Security 17.00		5.5	6	5
paloalto	Traps 4.1		3	5	5
Microsoft	Windows Defender Antivirus 4.12		5.5	5.5	5.5
McAfee	Endpoint Security 10.5		6	5.5	6
KASPERSKY	Small Office Security 5		6	5.5	6
KASPERSKY	Endpoint Security 10.3		6	6	6
G DATA	AntiVirus Business 14.1		6	5	5
F-Secure	PSB Computer Protection 18.3 & 18.4		6	5	3.5
Bitdefender	Endpoint Security Elite 6.2		6	6	5.5
Bitdefender	Endpoint Security 6.2		6	6	5.5
avast	Antivirus Business 18.1 & 18.2		5.5	5.5	6

Afbeelding 11: AV-test.org test. Protection score

	Industry average	March	April
Protection against 0-day malware attacks, inclusive of web and e-mail threats (Real-World Testing) 196 samples used	99.5%	100%	100%
Detection of widespread and prevalent malware discovered in the last 4 weeks (the AV-TEST reference set) 5,484 samples used	99.9%	100%	100%
Protection Score	6.0/6.0		

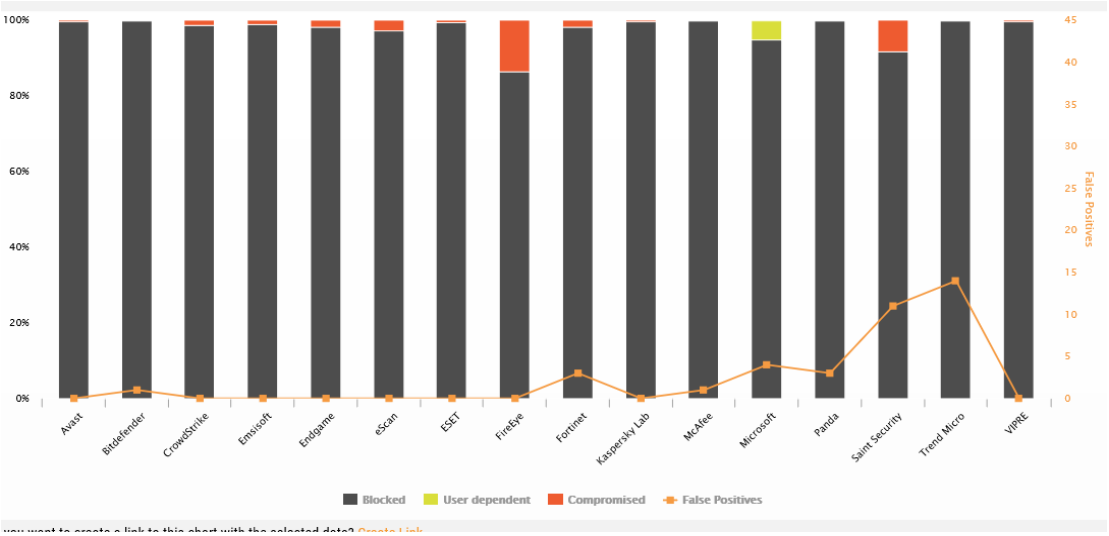
Afbeelding 12: AV-test.org test. Usability (False positives)

	Industry average	March	April
False warnings or blockages when visiting websites 500 samples used	0	0	0
False detections of legitimate software as malware during a system scan 1,615,681 samples used	6	0	1
False warnings concerning certain actions carried out whilst installing and using legitimate software 42 samples used	0	0	
False blockages of certain actions carried out whilst installing and using legitimate software 42 samples used	0	0	
Usability Score	6.0/6.0		

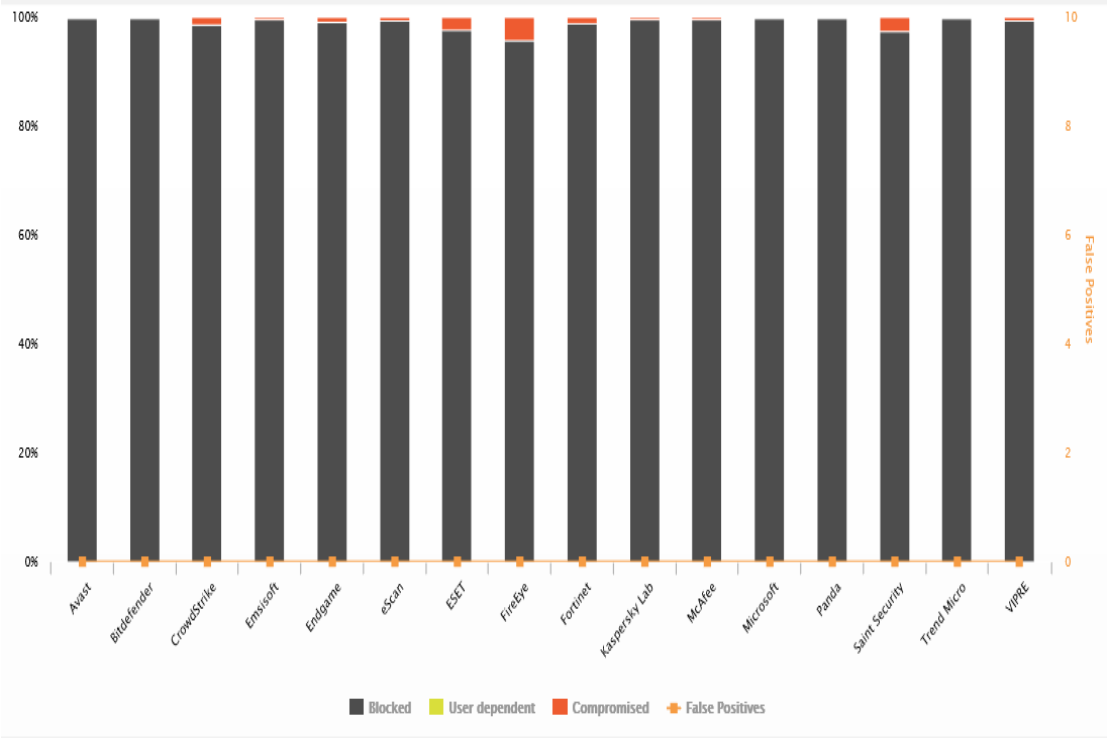
Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl

6.5 AV-comparatives.org

Afbeelding 13: maart 2018 AV-comparatives.org. Real World protection test.



Afbeelding 14: maart 2018 AV-comparatives.org. Malware protection



Amitron BV
Maasstraat 15
3016 DB
Rotterdam
+31 (0)10 870 01 50
info@amitron.nl
www.amitron.nl