Adaptive Defense 360

Antwoorden vinden, problemen oplossen

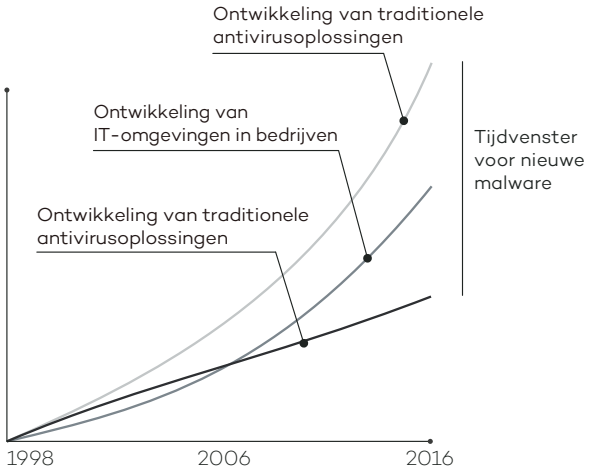
MAXIMALE BEVEILIGING DOOR EEN COMBINATIE VAN EPP- EN EDR-TECHNOLOGIEËN

Endpoints tegen aanvallen beschermen is moeilijk en omslachtig. Een beveiligingsoplossing dient een brede reeks aan beveiligingsmaatregelen te bevatten, inclusief traditionele antivirus- en antimalwarebeveiliging, Personal Firewall, web- en mailfilters evenals Device Control. Elke vorm van afweer dient additionele beveiliging te bieden tegen moeilijk te herkennen zero-day- en doelgerichte aanvallen.

Tot nog toe moesten IT-afdelingen een hele reeks verschillende producten van verschillende producenten kopen en bewaken om endpoints te beschermen. **Adaptive Defense 360** is de eerste en enige oplossing die **Endpoint Protection Platform (EPP)-** en **Endpoint Detection & Response (EDR)-**technologieën combineert. Bovendien automatiseert **Adaptive Defense 360** veel processen en vermindert op die manier de werkdruk van de IT-afdelingen.

Adaptive Defense 360 behelst de modernste EPP-oplossing van Panda, welke eenvoudige en gecentraliseerde veiligheid, herstelmaatregelen, realtime-bewaking en reports, profiel gebaseerde beveiliging, gecentraliseerde Device Control, evenals webbewaking en -filtering biedt.

Zowel het malware- als het IT-security landschap zijn in de afgelopen 20 jaar enorm veranderd. Door de opkomst van gemiddeld 225.000 nieuwe virussen per dag (1e kwartaal 2015) en de steeds complexer en uitgekiender wordende malware zijn netwerken in ondernemingen gevoeliger voor zero-day en doelgerichte aanvallen, zogenaamde targeted attacks, dan ooit.



Beschermingsoplossingen voor endpoints, die gebaseerd zijn op signature files en heuristische algoritmes, bieden effectieve bescherming tegen bekende malware. Ze bieden echter geen bescherming tegen zero-day en doelgerichte aanvallen, die misbruik maken van „het tijdvenster voor nieuwe malware„. Dit „tijdvenster“ duidt de periode tussen het verschijnen van een nieuw virus en de ontwikkeling van een tegenmiddel door de security ondernemingen aan. Een groeiende leemte waarvan hackers misbruik maken om virussen, ransomware, trojans en andere soorten van malware de bedrijfsnetwerken binnen te sluizen. Dergelijke steeds verder verspreide bedreigingen kunnen vertrouwelijke documenten versleutelen om losgeld te eisen of gevoelige data te verzamelen met industriële spionage doeleinden.

Adaptive Defense 360 is het antwoord van Panda op dit soort aanvallen. Adaptive Defense 360 biedt een EDR-service die elke binnen een onderneming draaiende applicatie nauwkeurig kan classificeren zodat alleen betrouwbare processen worden uitgevoerd. De EDR-vaardigheden van Adoptive Defense 360 resulteren uit een veiligheidsmodel dat is gebaseerd op drie beginselen: (1) voortdurende bewaking van alle op de bedrijfscomputers en servers draaiende applicaties (2) automatische classificering door Collective Intelligence en (3) analyse van niet automatisch geclassificeerde applicaties door technici van de PandaLabs. Op die manier kunnen we het gedrag van elke binnen een onderneming draaiende applicatie controleren.

Automatische preventie
Blokkeert applicaties en isoleert systemen om toekomstige aanvallen te voorkomen.

Automatische herkenning
Targeted Attacks en zero-day aanvallen worden in realtime en zonder signature files geblokkeerd.

Automatische desinfectie
Verwijdering van malware door middel van een muisklik of automatisch om de werkdruk van de administrators te verlagen.

Automatische forensics
Forenische informatie voor een gedetailleerde analyse van elke aanvalspoging. Traceerbaarheid en transparantie van elke actie die door de draaiende applicaties wordt uitgevoerd.

Door de combinatie van deze EDR-vaardigheden met de modernste EPP-oplossing van Panda maakt Adaptive Defense 360 malwarebescherming mogelijk die automatische preventie, herkenning, forensics en desinfectie in één enkele oplossing biedt.

DE ENIGE OPLOSSING VOOR DE OPTIMALE VEILIGHEID VAN ALLE DRAAIENDE APPLICATIES

VEELOMVATTENDE EN STABIELE BEVEILIGING

Panda **Adaptive Defense 360** biedt twee bedrijfsmodi:

• **Hardening-Modus:** Er mogen alleen applicaties draaien die zijn geclassificeerd als goodware, evenals de programma's die nog door Panda Security en de geautomatiseerde systemen geanalyseerd dienen te worden. Echter worden alle onbekende programma's die van het internet gedownload zijn of van een extern medium afkomen, geblokkeerd.

• **Lock-Modus:** Er mag alleen goodware uitgevoerd worden. Dit is de beste beveiligingsvorm voor ondernemingen, die wat de veiligheid betreft, van een "nul-risico"-benadering gebruik maken.

FORENSISCHE INFORMATIE

• **Overzichten van alle uitgevoerde acties** geven een duidelijk overzicht over alle gebeurtenissen die zijn veroorzaakt door malware.

• **Heatmaps** geven visuele informatie over de geografische locatie van de malware verbindingen, opgezette bestanden en nog veel meer.

• Software met bekende zwakke punten, die in het netwerk is geïnstalleerd, wordt gelokaliseerd.

BEVEILIGING VAN KWETSBARE BESTURINGSSYSTEMEN EN APPLICATIES

Systemen zoals Windows XP, die niet langer worden ondersteund door de producent en derhalve ongepatcht en onbeveiligd zijn, vallen makkelijk ten prooi aan zero-day aanvallen en bedreigingen van de nieuwste generatie. Bovendien maakt 90 procent van de malware gebruik van zwakke punten in applicaties zoals Java, Adobe, Microsoft Office evanals in browsers.

Adaptive Defense 360 maakt gebruik van context- en gedragsregels om te waarborgen dat ondernemingen in een veilige omgeving kunnen werken, zelfs wanneer deze gebruik maken van besturingssystemen die niet meer worden geactualiseerd.

VEELOMVATTENDE EPP-VAARDIGHEDEN

Adaptive Defense 360 bevat Panda Endpoint Protection Plus, de meest geavanceerde EPP-oplossing van Panda, waaronder begrepen:

- Herstelmaatregelen
- Gecentraliseerde Device Control: Voorkoming dat malware binnen-komt en gegevens verloren gaan door middel van blokkering van bepaald soorten apparatuur
- Webfiltering en bewaking
- Emailfiltering en bewaking
- Endpoint firewall en nog veel meer

VOORTDURENDE INFORMATIE OVER DE NETWERK STATUS

Er worden onmiddelijk waarschuwingen gegeven zodra malware in het netwerk wordt geïdentificeerd. Een veelomvattend bericht geeft informatie over de locatie, de aangevallen computers en de door malware uitgevoerde acties.

Berichten over de dagelijkse service-activiteiten worden per email verstuurd.

INTEGRATIE IN SIEM

A**daptive Defense 360** integreert zich in SIEM (Security Information and Event Management)-oplossingen om gedetailleerde gegevens over de activiteiten van alle op het systeem draaiende applicaties te leveren.

Voor klanten zonder SIEM bevat Adaptive Defense 360 optioneel een complete SIEM-tool ter visualisering en voor de forensische analyse van hetgeen alle processen in het systeem c.q. netwerk veroorzaken.

100 % MANAGED SERVICE

Er zijn geen investeringen in technisch personeel noodzakelijk om quarantaine, verdachte bestanden of besmette computers te managen. **Adaptive Defense 360** classificeert alle applicaties automatisch met behulp van zelflerende systemen in Big Data-omgevingen en onder continu toezicht van gespecialiseerde technici van de PandaLabs.

TECHNISCHE EISEN

Webconsole

- Internetverbinding
- Internet Explorer 10
- Firefox (laatste versie)
- Google Chrome (laatste versie)

Agent

- Besturingssystemen (workstations): Windows XP SP2 en later, Vista, Windows 7,8 & 8.1, 10
- Besturingssystemen (server): Windows Server 2003, Windows Server 2008, Windows Server 2012, Windows Server 2016
- Internetverbinding (rechtsstreeks of via een proxy)

Gedeeltelijk ondersteund (alléén EPP):

- Linux, Mac OS X en Android