Data Control

Bewaking van gevoelige gegevens op endpoints

panda a WatchGuard brand

Realtime beveiliging, zichtbaarheid en controle over persoonsgegevens. Vereenvoudiging van AGV-naleving.

In mei 2018 is de Algemene verordening gegevensbescherming (AVG) van de Europese Unie van kracht geworden. Deze nieuwe verordening, gericht op de verbetering van gegevensbeveiliging en -behandeling, dwingt alle all organisaties, zonder uitzondering, om de beveiliging van de persoonlijk identificeerbare informatie (PII) te versterken die ze opslaan en/of verwerken, met name gegevens die worden opgeslagen, gebruikt of verzonden op apparaten van werknemers en samenwerkende partijen.

WAAROM MOET U DE PERSOONSGEGEVENS EN GEVOELIGE GEGEVENS VAN UW ORGANISATIE BESCHERMEN?

Bedrijven moeten voldoen aan de nieuwe AVG, die van kracht is gegaan in mei 2018. Niet nakomen hiervan kan enorme boetes opleveren, tot 20 miljoen euro of 4 procent van de jaaromzet van een bedrijf.

De AVG geldt voor alle bedrijven, branches en regio's, met inbegrip van die buiten de EU, die persoonsgegevens van Europese ingezetenen verzamelen en opslaan.

Bedrijven moeten ook klaarstaan om de reputatieschade te voorkomen die een gegevenslek veroorzaakt, en de negatieve effecten daarvan op het vertrouwen van medewerkers en van huidige en potentiële klanten.

Organisaties worden geconfronteerd met belangrijke uitdagingen om te voldoen aan de nieuwe regelgeving: Ze moeten vooral in staat zijn om:

- **De ongebreidelde verspreiding van ongestructureerde gegevens tegen te gaan.** Ongestructureerde gegevens die staan opgeslagen op servers, alsmede op apparaten en laptops van samenwerkende partijen (partners, consultants, enz.) vormen zo'n 80 procent van alle bedrijfsgerelateerde gegevens. En terwijl de hoeveelheid ongestructureerde gegevens elk jaar verdubbelt, gebeurt dat ook met het risico dat bedrijven lopen[1].
- **De exponentiële toename van exfiltratiegevallen te bestrijden.** Het aantal gevallen waarin slecht beheerde en beveiligde gegevens worden geëxfiltreerd uit computersystemen, neemt dagelijks toe. En soms is de betroffen organisatie zich hiervan niet eens bewust. Deze gegevensdiefstallen zijn gewoonlijk te wijten aan externe aanvallen of nalatige of kwaadwillende insiders die worden gedreven door lucratieve oogmerken of wraak.

DE OPLOSSING: PANDA DATA CONTROL

Panda Data Control is een gegevensbeveiligingsmodule die volledig in het Panda Adaptive Defense-platform is geïntegreerd. Data Control is ontworpen om organisaties te helpen bij de naleving van gegevensbeveiligingsverordeningen, en om persoonsgegevens en gevoelige gegevens in kaart te brengen en te beveiligen, zowel in real time als gedurende de levenscyclus ervan op endpoints en servers.

Panda Data Control registreert, controleert en bewaakt **ongestructureerde[2] persoonsgegevens** op endpoints: van rustende gegevens tot in gebruik zijnde gegevens en in beweging zijnde gegevens.

Afbeelding 1 – Algemeen overzicht van de bestanden die persoonsgegevens bevatten en de gebruikers die er toegang tot hebben gehad.

BELANGRIJKSTE VOORDELEN

Registreren en controleren
Bestanden met persoonsgegevens (PII) in kaart brengen, alsmede gebruikers, medewerkers, samenwerkende partijen, endpoints en servers in uw organisatie die toegang hebben tot deze persoonlijk identificeerbare informatie.

Bewaken en detecteren
Proactieve maatregelen implementeren om toegang tot PII te voorkomen met behulp van rapporten en realtime waarschuwingen betreffende onbevoegd en verdacht gebruik, verzending en exfiltratie van bestanden met persoonsgegevens.

Belangrijke bestanden in de gaten houden
Krachtige zoekmogelijkheden stellen beheerders in staat om belangrijke bestanden te vinden op basis van door de gebruiker gedefinieerde zoekcriteria.

Beheer vereenvoudigen
De Panda Data Control-module maakt standaard deel uit van Panda Adaptive Defense en Panda Adaptive Defense 360. Organisaties hoeven niets anders te implementeren dan de standaardbeveiliging, en de module kan eenvoudig en onmiddellijk worden geactiveerd zonder omslachtige configuraties. Als de module eenmaal is geactiveerd, wordt deze ingeschakeld en beheerd vanaf het cloudplatform.

Naleving aantonen van toepasselijke regelgeving aan het hogere management, de functionaris voor gegevensbescherming[3] en alle andere medewerkers in uw organisatie. De strikte maatregelen tonen die van kracht zijn ter beveiliging van PII buiten gebruik, in gebruik en in gegevensverkeer tussen endpoints en servers.

[1] Carla Arend. IDC Opinion - maart 2017.
[2] Ongestructureerde gegevens zijn gegevens die zich niet in een database of enige andere gegevensstructuur bevinden. Ongestructureerde gegevens kunnen tekstueel of niet-tekstueel zijn. Panda Data Control richt zich op de tekstuele ongestructureerde gegevens die zich bevinden op endpoints en servers.
[3] Functionaris voor gegevensbescherming: De persoon die verantwoordelijk is voor het toezicht op de gegevensbeveiligingsstrategie in een organisatie.

BEVEILIGING EN BEHEER VAN PII

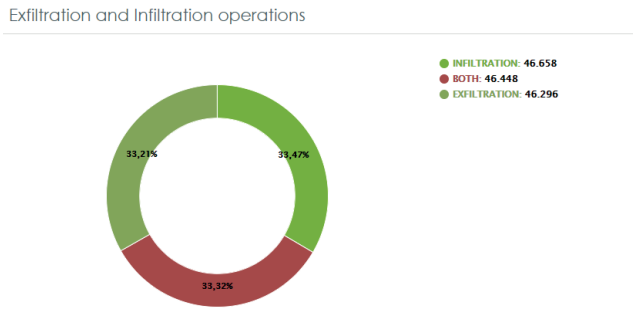
Door **Panda Adaptive Defense** beschermde organisaties kunnen er zeker van zijn dat hun endpoints en servers niet worden geschaad door kwaadaardige programma's afkomstig van externe bronnen, en zullen dus niet het slachtoffer worden van externe gegevensexfiltratie-aanvallen.

De **classificatieservice** van Panda Adaptive Defense **categoriseert 100 procent van alle toepassingen** die op de beveiligde endpoints en servers worden uitgevoerd, en geeft een oordeel over hun betrouwbaarheid of kwaadaardige aard door gebruik te maken van **technieken voor computergestuurd leren** onder supervisie van de malwarespecialisten van Panda Security. Dit systeem garandeert dat **alleen toepassingen die als goodware zijn geclassificeerd**, kunnen worden uitgevoerd.

De **Data Control-module** bevat de EDR-mogelijkheden (Endpoint Detection and Response) van de oplossing voor continue bewaking van de beveiligde endpoints in de organisatie, waarbij de ongestructureerde persoonsgegevens die zich in het netwerk bevinden en binnen het netwerk worden verzonden, in kaart worden gebracht en worden beveiligd.

Tot slot kunnen de **waarschuwingen en rapporten** van Data Control worden aangepast en afgestemd op de specifieke behoeften van elk bedrijf.

Afbeelding 2 - Bewerkingen met bestanden met risico op exfiltratie en infiltratie: Aan de hand van de diagrammen kunt u het risico bewaken en beoordelen van de op PII-bestanden uitgevoerde bewerkingen door gebruikers en computers. Op die manier helpt Data Control organisaties bij het treffen van maatregelen voor het voorkomen en beheersen van gegevensexfiltratie-acties.



BELANGRIJKSTE KENMERKEN

In kaart brengen van gegevens:
Maakt een geïndexeerde inventarisatie van alle bestanden die ongestructureerde persoonsgegevens opslaan (rustende gegevens), met het aantal keren dat elk gegevenstype voorkomt. Alle informatie wordt automatisch geclassificeerd.

De classificatie combineert verschillende technieken en algoritmen van computergestuurd leren die de resultaten optimaliseren en tegelijkertijd valse positieven en het gebruik van bronnen op apparaten verminderen.

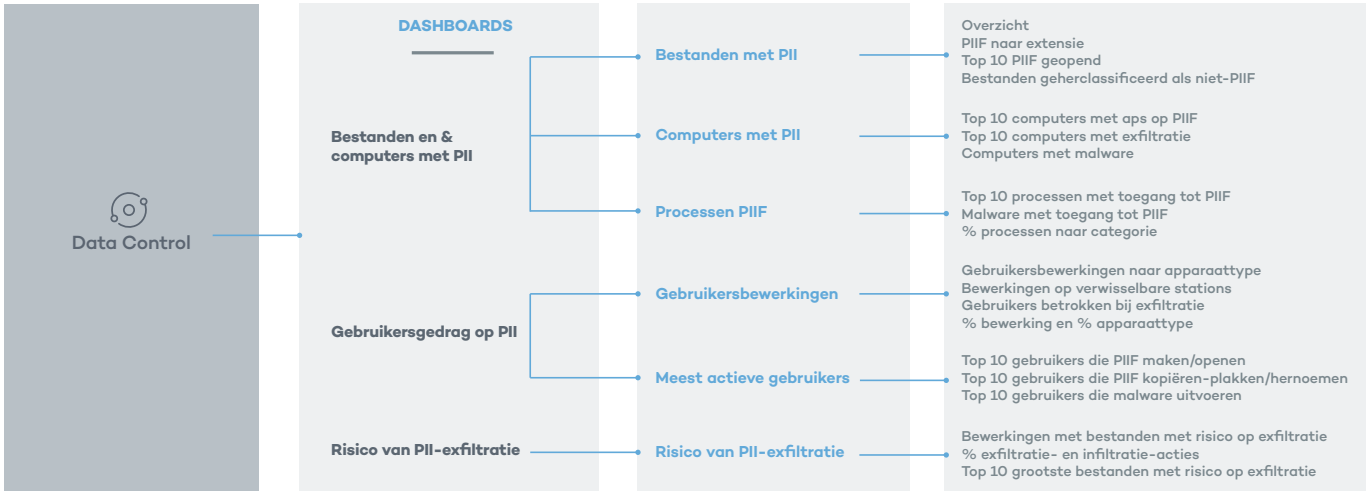
Gegevens zoeken:
De door de gebruiker gedefinieerde vrije zoekopdracht creëert een lijst van de bestanden waarin de gezochte informatie is opgeslagen. Deze lijst kan worden geëxporteerd voor een eenvoudigere verwerking.

Bewaking van gegevens:
Bewaakt de verschillende typen bewerkingen die worden uitgevoerd op ongestructureerde bestanden (gegevens in gebruik), terwijl de inventarisatie van bestanden met persoonsgegevens volledig actueel wordt gehouden. Elke poging om een van deze bestanden te kopiëren of uit het netwerk te verplaatsen via e-mail, webbrowsers of FTP (gegevens in beweging) wordt door de module geregistreerd.

Visualisatie van gegevens:
De resultaten van de gegevensbewakings- en -registratietaken worden continuegesynchroniseerd op het Adaptive Defense-platform en in de module Advanced Visualization Tool. Deze module biedt tools voor het onderzoeken van alle gebeurtenissen die betrekking hebben op gegevens in rust, in gebruik en in beweging, zowel in real time als achteraf gedurende de levenscyclus ervan op apparaten.

De dashboards en voorgedefinieerde rapporten en waarschuwingen van Data Control helpen bij het onderzoeken van gebruiksgevallen en de waarborging van het beveiligingsbeheer van de ongestructureerde persoonsgegevens die zich op de beveiligde apparaten van de organisatie bevinden.

Afbeelding 3 – Panda Data Control - dashboards, secties, diagrammen en voorgedefinieerde query's.



HOE PANDA DATA CONTROL BIJDRAAGT AAN NALEVING VAN DE AVG

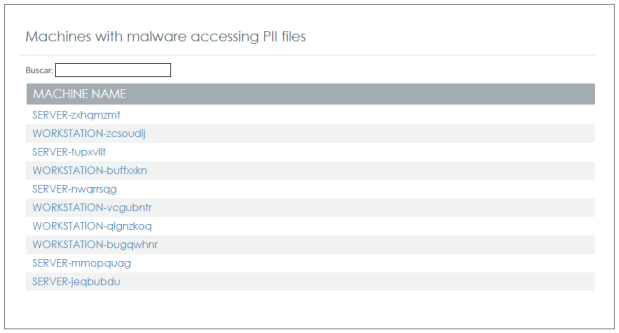
AVG-artikel	Functie Panda Data Control
Art. 17: Recht op gegevenswissing ("recht om te worden vergeten"). *"De betrokkene heeft het recht van de voor de verwerking verantwoordelijke te verlangen dat hij of zij onverwijld de hem of haar betreffende persoonsgegevens wist en de voor de verwerking verantwoordelijke is verplicht de persoonsgegevens onverwijld te wissen...."*	Met Panda Data Control kunnen organisaties aangepaste zoekopdrachten configureren om bestanden in het netwerk te vinden die de persoonlijke informatie bevatten van mensen die hun recht op verwijdering willen claimen.
Art. 32: Beveiliging van de verwerking. *"De verwerkingsverantwoordelijke en de verwerker treffen passende technische en organisatorische maatregelen om te zorgen voor een beveiligingsniveau dat passend is voor het risico, met inbegrip van een proces voor periodieke tests, waarbij de effectiviteit van technische en organisatorische maatregelen om te zorgen voor de beveiliging van de verwerking wordt vastgesteld en beoordeeld."*	Panda Data Control biedt organisaties tools om te beoordelen, zowel in real time als achteraf, of alleen bevoegd personeel toegang heeft tot de op hun netwerk opgeslagen bestanden met persoonsgegevens en of het geldende beveiligingsbeleid al dan niet adequaat is. Beschikbare rapporten zijn: • Computers met PII, PII-bestanden, Computers met de meeste bewerkingen op PII-bestanden en Malwareprocessen met toegang tot PII-bestanden, op het dashboard Bestanden en computers met PII. • Verdeling van typen bewerkingen op PII, Bij persoonsgegevensbewerkingen betrokken gebruikers, en Gebruikers die malware uitvoeren, op het dashboard Gebruikersbewerkingen op PII-bestanden.
Art. 33: Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit. *"Indien een inbreuk in verband met persoonsgegevens heeft plaatsgevonden, meldt de verwerkingsverantwoordelijke deze zonder onredelijke vertraging en, indien mogelijk, uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan de bevoegde toezichthoudende autoriteit. Deze melding beschrijft de aard van de inbreuk in verband met persoonsgegevens, waar mogelijk onder vermelding van de categorieën van betrokkenen en persoonsgegevensregisters in kwestie en, bij benadering, het aantal betrokkenen en persoonsgegevensregisters in kwestie."*	Panda Data Control biedt, naast alle diagrammen zoals beschreven voor Artikel 32, een reeks gegevens die speciaal zijn gericht op exfiltratie van PII: • Bewerkingen met bestanden met risico op exfiltratie en infiltratie. • Grootste bestanden met risico op exfiltratie. • Gebruikers betrokken bij exfiltratie-acties: Risico van PII-exfiltratie.
Art. 35: Privacyeffectbeoordelingen. *"Wanneer een bepaald soort verwerking waarschijnlijk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen, voert de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens."*	De module Data Control is gericht op het in kaart brengen van de bestanden waarin persoonsgegevens zijn opgeslagen, en op het bewaken van de acties die op de bestanden worden uitgevoerd en de daarbij betrokken gebruikers. Op basis van deze gegevens kunnen organisaties hoeveelheid, type en gebruik van de zich op hun netwerk bevindende persoonsgegevens in kaart brengen, zodat ze de gevolgen en het risico van de verwerking van dergelijke gegevens kunnen beoordelen. De voornoemde dashboards en rapporten zijn ook van toepassing op dit artikel.
Art. 39: Taken van de functionaris voor gegevensbescherming. *"De functionaris voor gegevensbescherming vervult ten minste de volgende taken:* *Toezien op naleving van deze verordening.* *Desgevraagd advies verstrekken met betrekking tot de gegevensbeschermingseffect-beoordeling en toezien op de uitvoering daarvan in overeenstemming met Artikel 35."*	Alle voornoemde dashboards en rapporten, met name diegene die betrekking hebben op Artikel 35, zijn essentiële tools om de functionaris voor gegevensbescherming te helpen bij de uitvoering van zijn taak.

DASHBOARDS VAN PANDA DATA CONTROL

Art. 32: Beveiliging van de verwerking.

Bestanden en computers met PII Data Control Dashboard - computers met malware met toegang tot PII-bestanden:

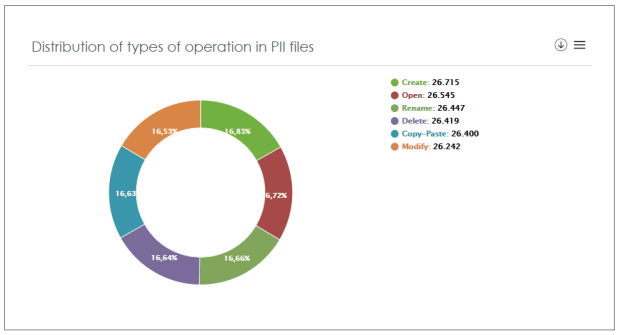
Dit dashboard toont de top 10 computers waarop kwaadaardige processen zijn gedetecteerd die toegang proberen te krijgen tot persoonsgegevens. Op basis van deze informatie kunnen beheerders terugkerende malware-infecties en aanhoudende dreigingen op bepaalde computers detecteren, en kunnen ze vaststellen wat de impact van deze dreigingen is op de persoonsgegevens die in bezit zijn van de organisatie, zoals vereist door de AVG.



Art. 33: Melding van een inbreuk in verband met persoonsgegevens aan de toezichthoudende autoriteit.

Data Control Dashboard Gebruikersbewerkingen op PII-bestanden - Verdeling van typen bewerkingen in PII-bestanden.

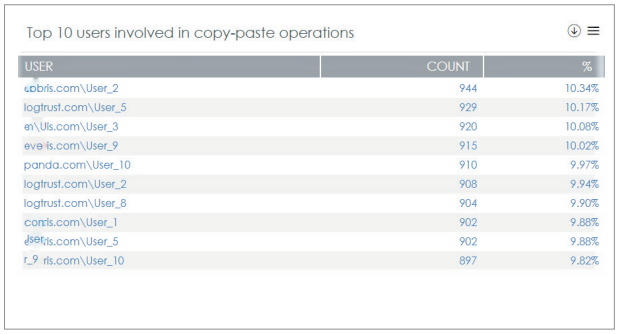
Dit dashboard toont de typen bewerkingen, uitgevoerd op bestanden met persoonsgegevens en gevoelige gegevens (PIIF's) waarmee uw organisatie werkt. Een significante toename of afname in het aantal bewerkingen, van welk type dan ook, kan duiden op een gegevensbeveiligingsincident of -gebeurtenis.



Art. 35: Privacyeffectbeoordelingen.

Dashboard Gebruikersbewerkingen op PII-bestanden - Top 10 gebruikers betrokken bij kopieer-plakbewerkingen.

Deze widget toont de topgebruikers die kopieer-plakbewerkingen hebben uitgevoerd op bestanden met persoonlijk identificeerbare informatie (PII). Data Control bewaakt ook andere bewerkingstypen: toegang, maken, openen, hernoemen, verwijderen, enz...



Art. 39: Taken van de functionaris voor gegevensbescherming.

Dashboard Risico van PII-exfiltratie - Aantal bewerkingen met bestanden met risico op exfiltratie:

Deze widget helpt organisaties bij het bewaken van persoonsgegevensstromen door het aantal exfiltratie-acties weer te geven dat is uitgevoerd op bestanden met gevoelige gegevens in het netwerk.

Op basis van deze informatie kan de functionaris voor gegevensbescherming het gebruikelijke aantal exfiltratie-acties vaststellen en afwijkingen constateren die worden veroorzaakt door beveiligingsincidenten.