Data Control

Einfachste Überwachung sensibler Daten auf Endpoints

Sicherheit, Transparenz und Kontrolle über personenbezogene Daten in Echtzeit
Vereinfachung der Einhaltung der DSGVO.

Durch das Inkrafttreten der Allgemeinen Datenschutzverordnung (DSGVO) der Europäischen Union zur Verbesserung von Datenschutz und -verarbeitung im Mai 2018 sind ausnahmslos alle Unternehmen dazu verpflichtet, **die Sicherheit** der von ihnen gespeicherten bzw. verarbeiteten **personenbezogenen Daten (PII) zu verstärken,** insbesondere Daten, die auf **Geräten von Arbeitnehmern bzw. Mitarbeitern** gespeichert, genutzt oder übertragen werden.

WARUM MÜSSEN SIE DIE PERSONENBEZOGENEN BZW. SENSIBLEN DATEN IHRES UNTERNEHMENS SCHÜTZEN?

Unternehmen müssen sich selbst auf die Einhaltung der neuen DSGVO vorbereiten, die ab Mai 2018 gilt und im Falle eines Verstoßes Geldstrafen von bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Jahresumsatzes eines Unternehmens mit sich bringt.

Von der DSGVO sind alle Unternehmen, Branchen und Regionen betroffen; selbst jene außerhalb der EU, die personenbezogene Daten von EU-Bürgern erfassen und speichern.

Darüber hinaus müssen sich Unternehmen darauf vorbereiten, die durch ein Datenleck verursachten Reputationsschäden und ihren Auswirkungen auf das Vertrauen der Mitarbeiter sowie der aktuellen und potenziellen Kunden zu verhindern.

Die Erfüllung der Datenschutzgrundverordnung stellt Unternehmen vor großen Herausforderungen. Unter anderem müssen sie in der Lage sein

- **die unkontrollierte Vermehrung unstrukturierter Daten zu verringern.** Unstrukturierte Daten, die sowohl auf Servern als auch auf Geräten und Laptops von Arbeitnehmern bzw. Mitarbeitern (Partner, Berater usw.) gespeichert werden, machen etwa 80 Prozent aller unternehmensbezogenen Daten aus. Und ebenso wie sich die Menge unstrukturierter Daten jedes Jahr verdoppelt, verhält es sich auch mit dem Risiko für Unternehmen[1].

- **gegen die exponentielle Zunahme von Fällen der Datenexfiltration anzugehen.** Die Anzahl der Fälle, bei denen schlecht verwaltete und gesicherte Daten aus den Computersystemen exfiltriert werden, nimmt täglich zu. Dies ist dem betroffenen Unternehmen manchmal nicht einmal bewusst. Die Datendiebstähle sind in der Regel auf externe Angriffe bzw. fahrlässige oder böswillige Insider zurückzuführen, deren Motive finanzieller Gewinn oder Rache sind.

DIE LÖSUNG: PANDA DATA CONTROL

Data Control ist ein Datensicherheitsmodul, das vollständig in die Panda Adaptive Defense-Plattform integriert ist. Data Control wurde entwickelt, um Unternehmen bei der Einhaltung von Datenschutz-bestimmungen zu unterstützen und dabei personen-bezogene und sensible Daten sowohl in Echtzeit als auch während des gesamten Lebenszyklus auf Endpoints und Servern zu ermitteln und zu schützen.

Panda Data Control ermittelt, prüft und überwacht **unstrukturierte[2] personenbezogene Daten auf Endpoints: von ruhenden Daten über verwendete Daten bis hin zu übertragenen Daten.**

Abb. 1 – Allgemeine Übersicht über die Dateien, die personenbezogene Daten enthalten, und die Benutzer, die auf sie zugreifen können.

HAUPTVORTEILE

Ermitteln und Prüfen
Identifizieren von Dateien mit personenbezogenen Daten (PII) sowie Benutzer, Endpoints und Server in Ihrem Unternehmen, die auf diese personenbezogenen Daten zugreifen.

Überwachen und Finden
Implementieren proaktiver Maßnahmen, um den Zugriff auf PII mit Hilfe von Berichten und Echtzeitwarnungen über die unbefugte und verdächtige Verwendung, Übertragung und Exfiltration von Dateien mit personenbezogenen Daten zu verhindern.

Einfaches Management
Das Modul Panda Data Control ist in Panda Adaptive Defense und Panda Adaptive Defense 360 integriert und kann optional hinzugekauft werden. Neben dem Standardschutz kann Data Control einfach und unverzüglich ohne weitere Konfigurationen eingesetzt werden. Nach der Aktivierung ist das Modul freigegeben und wird über die Cloud-Plattform verwaltet.

Nachweis der DSGVO-Konformität
Ermöglicht der Geschäftsführung, dem DSB[3] und allen anderen Arbeitnehmern in Ihrem Unternehmen die **Einhaltung** der geltenden Vorschriften aufzuzeigen. Darüber hinaus zeigt sie die Sicherheitsmaßnahmen an, die zum Schutz von ruhenden, verwendeten und zwischen Endpoints und Servern übertragenen PII vorhanden sind.

SICHERHEIT UND KONTROLLE PERSONENBEZOGENER DATEN

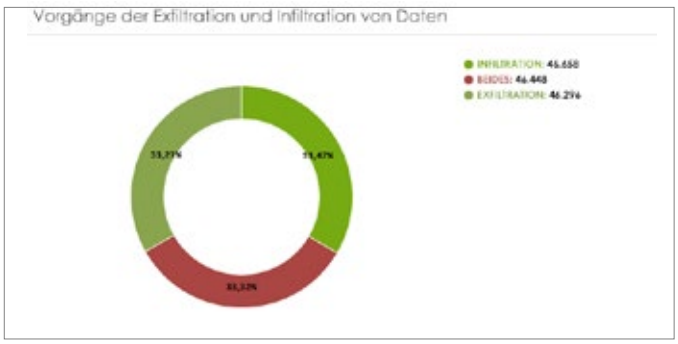
Durch **Panda Adaptive Defense** geschützte Unternehmen können sicher sein, dass ihre Endpoints und Server nicht durch bösartige Programme gefährdet und daher nicht Opfer von externen Angriffen zur Exfiltration von Daten werden.

Panda Adaptive Defense **kategorisiert 100 Prozent aller Anwendungen,** die auf den geschützten Endpoints und Servern ausgeführt werden, und beurteilt ihre Vertrauenswürdigkeit. Dafür werden Verfahren des **maschinellen Lernens** genutzt und von PandaLabs-Spezialisten überwacht. Dieses System stellt sicher, dass **nur Anwendungen** ausgeführt werden können, die als **„Goodware" eingestuft** wurden.

Das **Data Control-Modul** nutzt die EDR-Funktionen (Endpoint Detection and Response) von Adaptive Defense, um die geschützten Endpoints im Unternehmen kontinuierlich zu überwachen. Dabei werden die unstrukturierten personenbezogenen Daten ermittelt, die über das Netzwerk gespeichert und übertragen werden.

Die **Warnmeldungen und Berichte** von Data Control können individuell gestaltet und an die spezifischen Bedürfnisse jedes Unternehmens angepasst werden.

Abb. 2 - Vorgänge mit Dateien, für die ein Risiko der Exfiltration und Infiltration von Daten besteht: Mithilfe der Diagramme können Sie das Risiko von Vorgängen überwachen und bewerten, die von Benutzern und Geräten an PII-Dateien ausgeführt werden. Dadurch werden Unternehmen von Data Control bei der Einführung von Maßnahmen zur Verhinderung und Kontrolle von Vorgängen zur Exfiltration von Daten unterstützt.



HAUPTMERKMALE

Datenermittlung:
Erstellt ein indiziertes Inventar aller Dateien, in denen unstrukturierte personengebundene Daten (ruhende Daten) gespeichert sind, mit der Anzahl des Vorkommens der verschiedenen Datentypen (inklusive automatischer Klassifizierung aller Informationen).

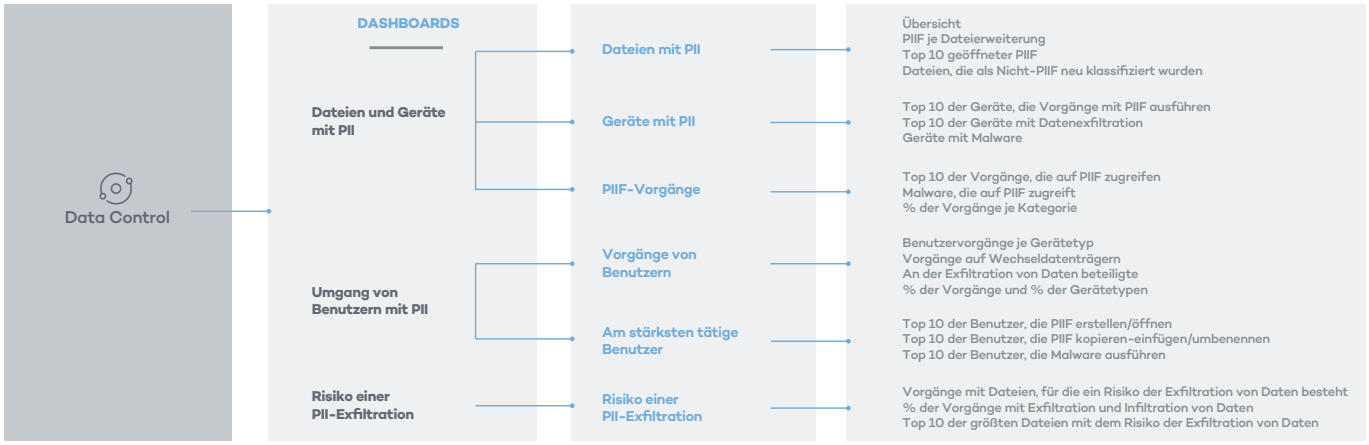
Die Klassifizierung kombiniert verschiedene Techniken und Algorithmen des maschinellen Lernens, die die Ergebnisse optimieren und gleichzeitig Fehlalarme und Ressourcenverbräuche auf den Geräten verringern.

Datenüberwachung:
Überwacht die verschiedenen Arten der Vorgänge, die an unstrukturierten Dateien (verwendete Daten) ausgeführt werden, während das Inventar der personenbezogenen Daten auf dem neuesten Stand gehalten wird. Jegliche Versuche, diese Dateien zu kopieren oder per E-Mail, Webbrowser oder FTP aus dem Netzwerk zu verschieben (übertragene Daten), werden vom Modul aufgezeichnet.

Datenvisualisierung:
Die Ergebnisse der Datenüberwachung und -ermittlung werden kontinuierlich auf der Adaptive Defense-Plattform sowie im optional hinzubuchbaren Advanced Visualization Tool synchronisiert. Dieses Modul bietet die Möglichkeit, alle Ereignisse, die ruhende, verwendete und übertragene Daten betreffen, sowohl in Echtzeit als auch retrospektiv bis zu einem Jahr auf den Geräten auszuwerten.

Die Dashboards und vordefinierten Berichte und Warnungen von Data Control gewährleisten die Sicherheitskontrolle der unstrukturierten personenbezogenen Daten auf den geschützten Geräten des Unternehmens.

Abb. 3 – Panda Data Control - Dashboards, Bereiche, Diagramme und vordefinierte Abfragen.



WIE PANDA DATA CONTROL DIE EINHALTUNG DER DSGVO UNTERSTÜTZT

DSGVO-Artikel	Funktion von Panda Data Control
Art. 32: Sicherheit der Verarbeitung *„Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.“*	Panda Data Control stellt Unternehmen Tools zur Verfügung, mit denen sie sowohl in Echtzeit als auch retrospektiv beurteilen können, ob nur autorisiertes Personal auf die in ihrem Netzwerk gespeicherten Dateien zugegriffen haben und ob die vorhandenen Sicherheitsrichtlinien angemessen sind. Verfügbare Berichte umfassen: • Geräte mit PII, PII-Dateien, Geräte, die die meisten Vorgänge mit PII-Dateien ausführen, und Malware-Vorgänge, die auf PII-Dateien zugreifen. • Verteilung der Vorgänge mit PII, Benutzer, die an Vorgängen mit personenbezogenen Daten beteiligt sind, und Benutzer, die Malware ausführen, in den Benutzervorgängen auf dem PII-Datei-Dashboard.
Art. 33: Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde *„Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde. Diese Meldung enthält die Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze.“*	Panda Data Control bietet zusätzlich zu allen detaillierten Grafiken zu Artikel 32 eine Reihe von Berichten, die sich speziell auf die PII-Exfiltration konzentrieren: • Vorgänge mit Dateien, für die ein Risiko der Exfiltration und Infiltration von Daten besteht. • Dateien mit dem Risiko der Exfiltration von Daten. • Benutzer/Geräte, die an Vorgängen zur Exfiltration von Daten beteiligt sind.
Art. 35: Datenschutz-Folgenabschätzung *„Hat eine Form der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.“*	Das Data Control-Modul dient der Identifizierung von Dateien, in denen personenbezogene Daten gespeichert werden, der Überwachung von Vorgängen, die an ihnen ausgeführt werden sowie der daran beteiligten Benutzer. Durch diese Daten sind Unternehmen in der Lage, die Menge, den Typ und die Verwendung der in ihrem Netzwerk vorhandenen personenbezogenen Daten zu ermitteln und damit die Auswirkungen und das Risiko der Verarbeitung derartiger Daten zu beurteilen.
Art. 39: Aufgaben des Datenschutzbeauftragten (DSB) *„Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:* *Überwachung der Einhaltung dieser Verordnung.* *Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35.“*	Alle oben genannten Dashboards und Berichte, insbesondere jene, die sich auf Artikel 35 beziehen, sind wesentliche Instrumente, die den DSB bei der Erfüllung seiner Aufgaben unterstützen.

PANDA DATA CONTROL-DASHBOARDS

Art. 32: Sicherheit der Verarbeitung

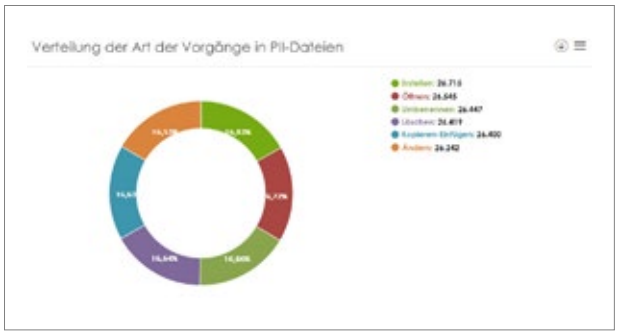
Data Control Dashboard über Dateien und Geräte mit PII: Geräte mit Malware, die auf PII-Dateien zugreifen

Dieses Dashboard zeigt die Top 10 der Computer, auf denen bösartige Prozesse aufgedeckt wurden, die auf personenbezogene Daten zugreifen. Durch diese Informationen sind Sicherheitsbeauftragte in der Lage, wiederkehrende Malware-Infektionen und andauernde Bedrohungen auf bestimmten Computern aufzudecken und die Auswirkungen dieser Bedrohungen auf die personenbezogenen Daten zu bewerten, die von dem Unternehmen gemäß der DSGVO gespeichert werden.

Art. 33: Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

Data Control Dashboard über Benutzervorgänge auf PII-Dateien: Verteilung der Art der Vorgänge in PII-Dateien

Dieses Dashboard stellt die Arten der Vorgänge dar, die an den von Ihrem Unternehmen bearbeiteten Dateien mit personenbezogenen und sensiblen Daten (PIIFs) ausgeführt werden. Eine signifikante Zunahme oder Abnahme der Anzahl dieser Vorgänge kann auf einen Vorfall oder ein Ereignis in Bezug auf die Datensicherheit hindeuten.



Art. 35: Datenschutz-Folgenabschätzung

Dashboard über Benutzervorgänge auf PII-Dateien: Top 10 der Benutzer, die an Vorgängen des Copy/Paste beteiligt sind

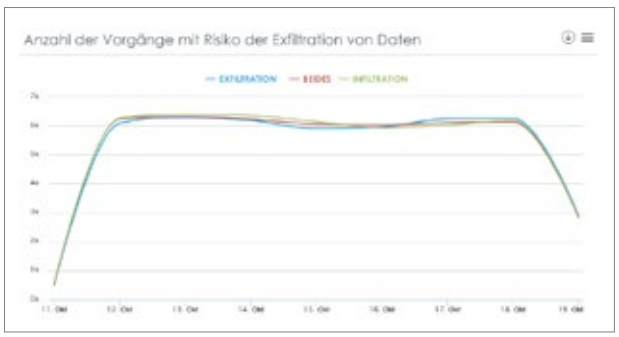
Dieses Widget listet die Top-Benutzer auf, die an Dateien mit personenbezogenen Daten (PII) Vorgänge zum Kopieren und Einfügen ausgeführt haben. Data Control überwacht auch andere Arten von Vorgängen: Zugreifen, Erstellen, Öffnen, Umbenennen, Löschen usw.

Art. 39: Aufgaben des Datenschutzbeauftragten (DSB)

Dashboard über das Risiko einer PII-Exfiltration: Anzahl der Vorgänge mit Dateien, für die ein Risiko der Exfiltration von Daten besteht

Dieses Widget unterstützt Unternehmen dabei, die Bewegungen von personenbezogenen Daten zu überwachen, indem die Anzahl der Vorgänge zur Exfiltration von Daten dargestellt wird, die an im Netzwerk vorhandenen Dateien mit sensiblen Daten ausgeführt werden.

Diese Informationen ermöglichen es dem DSB, die übliche Anzahl von Exfiltrationsvorgängen zu ermitteln und Abweichungen zu erkennen, die durch Sicherheitsvorfälle verursacht werden.



[1] Carla Arend. IDC Opinion - März 2017.
[2] Unstrukturierte Daten sind Daten, die sich nicht in einer Datenbank oder einer anderen Datenstruktur befinden. Unstrukturierte Daten können textliche oder nicht textliche Daten darstellen. Panda Data Control legt den Schwerpunkt auf textliche unstrukturierte Daten, die auf Endpoints und Servern gespeichert sind.
[3] DSB (Datenschutzbeauftragter): Person, die für die Überwachung der Datenschutzstrategie in einem Unternehmen verantwortlich ist.

Das Modul Panda Data Control ist ein Add-On für Panda Adaptive Defense oder Panda Adaptive Defense 360. Erhältlich in den folgenden Ländern: Spanien, Deutschland, Großbritannien, Frankreich und Schweden.