DATENBLATT

WATCHGUARD DATA CONTROL

Monitoring für sensible Daten an allen Endpoints

SICHERHEIT, TRANSPARENZ UND KONTROLLE IN ECHTZEIT MIT NUR EINEM PRODUKT

Der unkontrollierte Zugriff auf personenbezogene und sensible Unternehmensdaten ist ein alltägliches Sicherheitsrisiko, das schwerwiegende finanzielle Verluste und Rufschädigungen bedeuten kann. Möchten Sie dieses Risiko wirklich eingehen?

SCHUTZ FÜR PERSONENBEZOGENE UND SENSIBLE DATEN

Unternehmen sind gezwungen, verbesserte oder neue Maßnahmen zu ergreifen, um die von ihnen gespeicherten personenbezogenen oder sensiblen Daten zu schützen. Hauptfaktoren für diese Transformation sind:

- **Exponentielle Zunahme von Exfiltrationsfällen und Datenlecks**. Daten werden üblicherweise durch externe Angriffe, böswillige Insider mit Bereicherungs- oder Racheabsichten oder einfach Fahrlässigkeit gestohlen. Oft bemerken betroffene Organisationen solche Vorfälle nicht einmal.
- **Behördliche Auflagen wie z. B. der Datenschutz-Grundverordnung.** Verstöße gegen diese Vorschriften können hohe Geldstrafen nach sich ziehen, ggf. in Form eines Prozentanteils des weltweiten Umsatzes.
- **Enormer Zuwachs unstrukturierter Daten.** Rund 80 % des Gesamtdatenbestands von Unternehmen sind unstrukturierte Daten. Ihre Menge verdoppelt sich ungefähr von Jahr zu Jahr.

DIE LÖSUNG: WATCHGUARD DATA CONTROL

WatchGuard Data Control ist ein vollständig in WatchGuard EDR und WatchGuard EPDR integriertes Datensicherheitsmodul. Es unterstützt Organisationen dabei, die geltenden Datenschutzvorschriften einzuhalten.

Watchguard Data Control identifiziert, prüft und überwacht unstrukturierte[1] personenbezogene Daten auf Endpoints – von inaktiven Daten über Daten in Verarbeitung bis hin zu Daten bei der Übertragung. Mit dem leistungsfähigen anpassbaren Suchmodul finden Administratoren jede Datei in der Organisation, die zu kontrollierende Daten enthält (urheberrechtlich geschütztes Material, vertrauliche Informationen usw.).

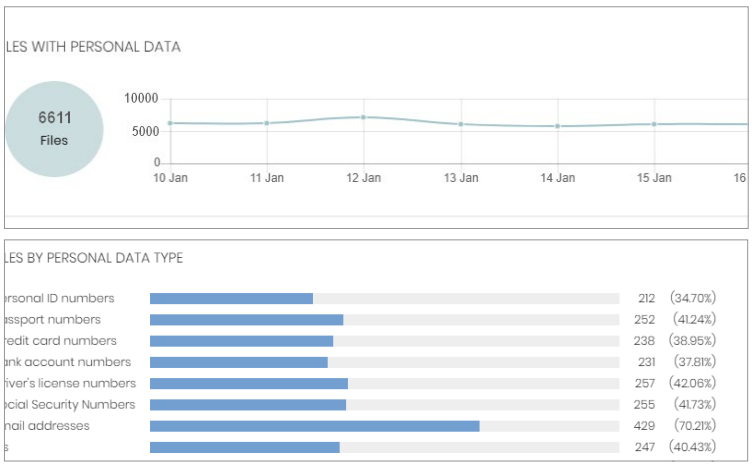


Abbildung 1: Zentrales Dashboard. Zugriff auf verschiedene Bereiche zur Anzeige von Dateien und Computern mit personenbezogenen Daten und von Dateien nach Kategorie personenbezogener Daten.

HAUPTVORTEILE

Identifizierung und Prüfung

Dateien, die personenbezogene Daten enthalten, und die Nutzer, Mitarbeiter, Partner, Workstations und Server in der Organisation, die auf personenbezogene Daten[2] zugreifen, werden automatisch erkannt.

Monitoring und Erkennung

Mit Berichten und Echtzeit-Warnmeldungen zur unbefugten oder verdächtigen Verwendung, Übertragung und Exfiltration von Dateien mit personenbezogenen Daten ergreifen Sie proaktiv Maßnahmen, die den Zugriff auf personenbezogene Daten verhindern.

Nachweisliche Einhaltung von Vorschriften

Belegen Sie gegenüber Unternehmensleitung, DSB[3] und allen anderen Mitarbeitern in der Organisation, dass Sie die geltenden Vorschriften einhalten. Weisen Sie die angewendeten strengen Sicherheitsmaßnahmen zum Schutz personenbezogener Daten auf Workstations und Servern nach.

Auffindung aller zu schützenden Daten

Mit einer angepassten Suche finden Sie alle Datenkategorien in den Dateien in Ihrem Netzwerk. So identifizieren Sie doppelte persönliche Dateien, um sie zu löschen und so das Risiko der Datenexfiltration zu reduzieren.

Einfache Verwaltung

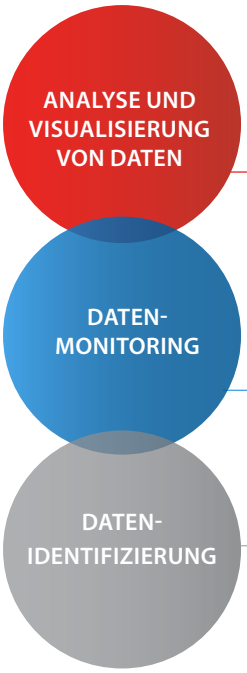
Sie müssen keine zusätzliche Software oder Hardware bereitstellen. Die Lösung lässt sich einfach und direkt ohne Konfigurationsaufwand aktivieren. Nach der Aktivierung wird das Modul über die Cloud-Plattform genutzt und verwaltet.

GESCHÄFTSDATEN-GOVERNANCE

Eine solide Daten-Governance erlaubt es Unternehmen, alle Fragen zu personenbezogenen Daten zu beantworten, die von Mitarbeitern verwendet werden: Welche Daten sind auf den Mitarbeiter-Endpoints gespeichert? Wer kann auf die Daten zugreifen und welche Aktionen können Zugriffsberechtigte damit ausführen? Entsprechen diese Aktionen den Unternehmensrichtlinien?

- Identifizieren Sie unstrukturierte personenbezogene Daten und verschaffen Sie sich transparenten Einblick. Markieren, gruppieren und klassifizieren Sie die Daten nach dem Grad ihrer Vertraulichkeit.
- Erstellen Sie Sicherheits- und Zugriffsrichtlinien, um Datenzugriff und -verwendung durch befugte Nutzer zu kontrollieren.
- Sensibilisieren Sie Ihre Mitarbeiter, um zu gewährleisten, dass sie Daten im Einklang mit externen Vorschriften und internen Richtlinien verwenden.
- Sorgen Sie mit Dashboards, Berichten und angepassten oder vorkonfigurierten Warnmeldungen für Daten-Governance.
- Analysieren Sie die Ursachen von Datensicherheitsverletzungen und passen Sie die Unternehmensrichtlinien entsprechend an. Legen Sie das Vorgehen bei Verletzungen des Schutzes personenbezogener Daten fest.

WATCHGUARD DATA CONTROL – HAUPTFUNKTIONEN



Transparenter Einblick in Echtzeit und nachträglich zu personenbezogenen Daten im Ruhezustand, in Verwendung und bei der Übertragung

Vorkonfigurierte Dashboards und Warnmeldungen

Monitoring[4] von Daten in Verwendung

Monitoring ein- und ausgehender[5] Vorgänge für Daten bei der Übertragung

Monitoring von Dateien mit personenbezogenen Daten[6] und Dateien, die angepassten Regeln entsprechen

Angepasste freie Suche nach Dateien anhand von Suchkriterien (Dateien mit und ohne personenbezogene Daten)

Bericht mit Möglichkeit, die Ergebnisse der angepassten Suche zu exportieren

Klassifizierung personenbezogener Daten (im Ruhezustand) mithilfe von maschinellem Lernen

Bestand der Dateien mit personenbezogenen Daten in WatchGuard Cloud verfügbar

WatchGuard Data Control – unterstützte Länder

Verfügbar in Spanien, Deutschland, Großbritannien, Schweden, Frankreich, Italien, Portugal, Holland, Finnland, Dänemark, der Schweiz, Norwegen, Österreich, Belgien, Ungarn und Irland.

[1]**Unstrukturierte Daten** sind Daten, die sich nicht in einer Datenbank oder einer anderen Datenstruktur befinden. Unstrukturierte Daten können textbasiert oder nicht textbasiert sein. WatchGuard Data Control legt den Schwerpunkt auf textbasierte unstrukturierte Daten auf Endpoints und Servern.
[2]**Personenbezogene Daten:** Ausweisdokumente, Führerschein, Reisepass, Sozialversicherungsnummer, E-Mail, Steuernummer, IPs, Vornamen, Nachnamen, Telefonnummern, Bankkonten, Kreditkarten.
[3]**Datenschutzbeauftragter:** Die Person, die für die Datenschutzstrategie einer Organisation verantwortlich ist.
[4]**Verwendete Daten.** Monitoring von Aktionen zu Dateien mit personenbezogenen Daten: Zugriff, Öffnen, Erstellung, Bearbeitung, Löschung, Umbenennung, Kopieren und Einfügen.
[5]**Daten bei der Übertragung** mit Risiko von Datenlecks über Outlook, Webbrowser, FTP oder externe USB-Laufwerke.
[6]**Dateien mit personenbezogenen Daten**: unstrukturierte Dateien mit personenbezogenen Daten, z. B. Office, OpenOffice, PDF, TXT usw.

FUNKTIONEN

Datenidentifizierung

Alle Dateien mit unstrukturierten personenbezogenen Daten (Daten im Ruhezustand) werden automatisch klassifiziert und mit der Anzahl der Vorkommen jeder Datenkategorie in ein Bestandsverzeichnis aufgenommen. Darin sind auch Duplikate enthalten. Diese Dateien können aus dem Bestand gelöscht werden. Die Planungsfunktion legt fest, wann eine vollständige Festplattenanalyse gestartet wird (für Bestand und Suchvorgänge erforderlich).

Die Klassifizierung erfolgt anhand einer Kombination unter anderem von Regeln, regulären Ausdrücken und maschinellem Lernen, die die Klassifizierungsergebnisse optimiert und die Zahl der False Positives und den Ressourcenverbrauch von Geräten senkt.

Datensuche

Mit der angepassten freien Suche finden Sie Dateien mit spezifischen Inhalten. **WatchGuard Data Control** erstellt eine Liste aller Dateien, die die betreffenden Informationen enthalten. Um die Verwaltung zu erleichtern, können Sie die Liste exportieren.

Monitoring und Kontrolle von Daten

Überwachen Sie die verschiedenen Arten von Vorgängen, die mit unstrukturierten Dateien (Daten in Verwendung) durchgeführt werden, und halten Sie den Bestand der Dateien mit personenbezogenen Daten auf dem neuesten Stand. Das Modul dokumentiert jeden Versuch, entsprechende Dateien per E-Mail, Webbrowser, FTP oder Wechseldatenträger (Daten
bei der Übertragung) zu kopieren oder zu verschieben. Informationen werden nur in verschlüsselter Form
auf Wechsellaufwerken gespeichert.

Datenvisualisierung

Die Ergebnisse der Überwachung und Identifizierung der Daten werden fortlaufend mit der Endpoint Security-Plattform und dem Advanced Visualization Tool-Modul synchronisiert. Dieses Modul stellt Tools für die Analyse aller Ereignisse im Zusammenhang mit Daten im Ruhezustand, in Verwendung und bei der Übertragung bereit – in Echtzeit und nachträglich und über den gesamten Datenlebenszyklus auf den Geräten.

Die Dashboards und vorkonfigurierten Berichte und Warnmeldungen von **WatchGuard Data Control** decken unterschiedlichste Anwendungsfälle ab und gewährleisten die Governance der Sicherheit unstrukturierter personenbezogener Daten.

Unterstützte Plattformen und Systemanforderungen für Watchguard Data Control

Mit folgenden Lösungen kompatibel: WatchGuard EPDR und WatchGuard EDR.

Unterstützte Betriebssysteme: Windows.

Liste kompatibler Browser: Google Chrome und Mozilla Firefox (weitere Browser ggf. kompatibel).

Deutschland, Österreich, Schweiz +49 700 92229333 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB: www.watchguard.de WatchGuard Technologies, Inc.