Endpoint Security

WatchGuard hat diesen Datenschutzleitfaden erstellt, um unsere Kunden über die Verarbeitung personenbezogener Daten im Zusammenhang mit WatchGuard Endpoint Security Services zu informieren. Die WatchGuard Endpoint Security Services umfassen WatchGuard EPP, EDR, EPDR, Advanced EPDR sowie zusätzliche Sicherheitsmodule wie WatchGuard Patch Management, Full Encryption, Advanced Reporting Tool und Data Control. Eine detaillierte Beschreibung finden Sie hier.

Der vorliegende Datenschutzleitfaden behandelt nicht die Verarbeitung personenbezogener Daten durch WatchGuard im Zusammenhang mit anderen Produkten, Services oder umfassenderen Geschäftstätigkeiten von WatchGuard (z. B. auf unseren Websites, im Rahmen von Lizenzierungen, Schulungen, Veranstaltungen usw.).

Für weitere Informationen zur Verarbeitung personenbezogener Daten im Zusammenhang mit unseren Services, einschließlich WatchGuard Endpoint Security Services, lesen Sie bitte unsere Datenschutzrichtlinie und den Zusatz zur Datenverarbeitung. Außerdem finden Sie in unserem Trust Center alles rund um die Themen Datenschutz und Sicherheit.

Bitte beachten Sie, dass dieser Datenschutzleitfaden weder den E-Mail-Schutz noch PCMS behandelt. Für etwaige Fragen zu diesen Produkten wenden Sie sich bitte an privacy@watchguard.com.

Überblick über die Endpoint Security Services

WatchGuard bietet mit seiner WatchGuard Endpoint Security Suite einen hervorragenden Schutz für Endpoints. Die Suite basiert auf einem mehrschichtigen Ansatz und wird über die WatchGuard Cloud zentral verwaltet. Die Suite umfasst die WatchGuard Endpoint Protection Platform (EPP), eine Cloud-native Lösung, welche einen Antivirus-Schutz der nächsten Generation für Desktops, Laptops, Server und Mobilgeräte (Android und iOS) bereitstellt. Die WatchGuard Endpoint Detection & Response (EDR) basiert auf künstlicher Intelligenz und ist in der Lage, fortschrittliche Bedrohungen sowie Zero-Day-Angriffe zu identifizieren und darauf zu reagieren. Damit stellt sie eine sinnvolle Ergänzung zu herkömmlichen Antivirus-Lösungen dar. Die WatchGuard Endpoint Protection Detection & Response (EPDR) verbindet die Stärken der EPP und des EDR zu einem umfassenden Schutz vor bekannten und unbekannten Bedrohungen, einschließlich Malware-Angriffen. Advanced EPDR ist die nächste Stufe der EPDR. Es bietet Sicherheitsteams zusätzliche Funktionen für eine tiefgreifende Bedrohungsjagd und eine schnellere Reaktion auf Vorfälle. Die zusätzlichen Sicherungsmodule für Endpoints umfassen das WatchGuard Patch Management, welches das Patchen von Schwachstellen auf Endpoints vereinfacht, Full Encryption für sensible Daten, ein Advanced Reporting Tool, das detaillierte Einblicke in Sicherheitsaktivitäten bietet, und Data Control zur Einschränkung der Datenübertragung und Verhinderung von Datenverlusten. Eine ausführlichere Beschreibung dieser Services und Module finden Sie hier.

WatchGuards Rolle bei der Datenverarbeitung

Bei der Bereitstellung von Endpoint Security Services für Kunden nimmt WatchGuard in erster Linie die Rolle eines Service Providers und Auftragsverarbeiters ein. Das heißt, dass wir die personenbezogenen Daten unserer Kunden entsprechend ihrer Anweisung und in ihrem Auftrag verarbeiten. Wir verarbeiten personenbezogene Daten auch in unserem eigenen Namen als Verantwortlicher, um unsere Geschäftszwecke zu verfolgen. Dazu zählen beispielsweise die Verwaltung und Pflege der Kundenbeziehung, die Sicherung der Services oder die Produktverbesserung. Hierfür nutzen wir statistische Analysen von Nutzungs-, Protokoll- oder Telemetriedaten.

Umfang und Gründe für die von uns erfassten personenbezogenen Daten

In der folgenden Tabelle finden Sie eine Übersicht über die personenbezogenen Daten, die von WatchGuard im Zusammenhang mit unseren Endpoint Security Services und unseren Verarbeitungszwecken erfasst werden. Diese Daten werden in der Regel direkt von einzelnen Endanwendern bereitgestellt, wenn sie Endpoint Security Services verwenden, oder vom Kunden-Kontoadministrator, wenn dieser ein WatchGuard-Konto erstellt und verwaltet, sowie Services im Namen der Kundenorganisation und ihrer Endanwender konfiguriert. Wir erfassen im Rahmen der Bereitstellung unserer Endpoint Security Services bestimmte Daten auch automatisch.

Die Nutzer der WatchGuard Cloud werden möglicherweise auch gebeten, zusätzliche personenbezogene Daten bereitzustellen. Dies ist notwendig, um Endpoint Security Services im Auftrag der Kundenorganisation zu verwalten.

Des Weiteren erfolgt eine automatische Erfassung spezifischer Servicedaten (siehe unten), welche der Behebung von Fehlern sowie der Sicherstellung der Einhaltung gesetzlicher Vorgaben dient. Zudem werden dadurch die Sicherheit und die kontinuierliche Verbesserung der Services gewährleistet.

SERVICE	KATEGORIEN PERSONENBEZOGENER DATEN	VERARBEITUNGSZWECKE
EPP, EDR, EPDR, Advanced EPDR	• Name des Endanwenders (als Teil von Pfaden und Dokumentnamen) • Benutzername des Endanwenders • E-Mail-Adressen des Endanwenders und des Absenders/Empfängers • IP-Adresse des Endanwenders • Gerätedaten des Endanwenders wie Hostname, MAC-Adresse, Hardware-Details, andere eindeutige Gerätekennungen • URLs	• Bereitstellung und Betrieb des Service • Erkennung, Analyse und Eindämmung von Bedrohungen und Sicherung der Services • Bereitstellung von technischem Kundensupport und Fehlerbehebung
DNSWatch® GO	• Benutzername des Endanwenders • E-Mail-Adresse des Endanwenders • IP-Adresse des Endanwenders • Gerätedaten des Endanwenders wie Hostname, MAC-Adresse, Hardware-Details, andere eindeutige Gerätekennungen • Berichte mit Diagnosedaten (Hostname, Benutzername, Zeitstempel)	• Bereitstellung und Betrieb des Service • Erkennung, Analyse und Eindämmung von Bedrohungen und Sicherung der Services • Bereitstellung von technischem Kundensupport und Fehlerbehebung
SIEMFeeder	• Name des Endanwenders (als Teil von Pfaden und Dokumentnamen) • Benutzername des Endanwenders • IP-Adresse des Endanwenders • Gerätedaten des Endanwenders wie Hostname, MAC-Adresse, Hardware-Details, andere eindeutige Gerätekennungen • URLs (in der Regel nur auf Domains beschränkt)	• Bereitstellung und Betrieb des Service • Erkennung, Analyse und Eindämmung von Bedrohungen und Sicherung der Services • Bereitstellung von technischem Kundensupport und Fehlerbehebung
Patch Management	• Name des Endanwenders (als Teil von Pfaden und Dokumentnamen) • IP-Adresse des Endanwenders • Gerätename des Endanwenders (kann den Benutzernamen enthalten)	• Bereitstellung und Betrieb des Service • Erkennung, Analyse und Eindämmung von Bedrohungen und Sicherung der Services • Bereitstellung von technischem Kundensupport und Fehlerbehebung
Full Encryption	• Name des Endanwenders (als Teil von Pfaden und Dokumentnamen) • IP-Adresse des Endanwenders • Gerätename des Endanwenders (kann den Benutzernamen enthalten)	• Bereitstellung und Betrieb des Service • Erkennung, Analyse und Eindämmung von Bedrohungen und Sicherung der Services • Bereitstellung von technischem Kundensupport und Fehlerbehebung

SERVICE	KATEGORIEN PERSONENBEZOGENER DATEN	VERARBEITUNGSZWECKE
Advanced Reporting Tool (ART)	• Name des Endanwenders (als Teil von Pfaden und Dokumentnamen) • Benutzername des Endanwenders • IP-Adresse des Endanwenders • Gerätedaten des Endanwenders wie Hostname, MAC-Adresse, Hardware-Details, andere eindeutige Gerätekennungen	• Bereitstellung und Betrieb des Service • Erkennung, Analyse und Eindämmung von Bedrohungen und Sicherung der Services • Bereitstellung von technischem Kundensupport und Fehlerbehebung
Data Control	• Name des Endanwenders (als Teil von Pfaden und Dokumentnamen) • Benutzername des Endanwenders • E-Mail-Adresse des Endanwenders • IP-Adresse des Endanwenders • Gerätedaten des Endanwenders wie Hostname, MAC-Adresse, Hardware-Details, andere eindeutige Gerätekennungen • Suchanfragen des Nutzers, die personenbezogene Daten enthalten können	• Bereitstellung und Betrieb des Service • Erkennung, Analyse und Eindämmung von Bedrohungen und Sicherung der Services • Bereitstellung von technischem Kundensupport und Fehlerbehebung
Remote Control (nur Advanced EPDR)	• Anfragen und Befehle des Nutzers, die personenbezogene Daten enthalten können, werden als Teil der Serviceprotokolle gespeichert. • Die Nutzer haben Zugriff auf die Details und die Verwaltung der Endpoints (einschließlich der Möglichkeit, Endpoint-Dateien herunterzuladen). Die Daten werden über einen sicheren Kanal gesendet, der ausschließlich vom Kunden initiiert werden kann und auf den WatchGuard keinerlei Zugriff hat. Auch eine Speicherung der Daten durch uns ist ausgeschlossen.	• Bereitstellung und Betrieb des Service • Erkennung, Analyse und Eindämmung von Bedrohungen und Sicherung der Services • Bereitstellung von technischem Kundensupport und Fehlerbehebung

MANAGEMENTSYSTEM	DATENKATEGORIEN	VERARBEITUNGSZWECKE
WatchGuard® Cloud (WGC)	**WGC-Kontodaten:** Umfasst die folgenden Daten der WGC-Nutzer: • Vollständiger Name • E-Mail-Adresse • Benutzername • IP-Adresse • Firmenname • Firmen-Telefonnummer • Zugangsdaten **Visualisierungsdaten zu WGC-Services:** • Verbindungen und Protokolle, die personenbezogene Daten von Endanwendern und Nutzern des Kunden wie oben beschrieben enthalten können. • Statusdaten, die Servicefehler auf bestimmten Geräten anzeigen und Angaben zum Gerät und zum letzten angemeldeten Anwender enthalten können. **WGC-Auditprotokolle:** Daten von WGC-Nutzern: • Konto-ID/Kontonummer/Benutzer-ID • Benutzername • IP-Adresse • Hostname • Zeitpunkt/Datum des Zugriffs • Quelle (Produkt, mit dem interagiert wurde) • Ausgeführte Aktivitäten	• Bereitstellung und Betrieb des Service • Erkennung, Analyse und Eindämmung von Bedrohungen und Sicherung der Services • Bereitstellung von technischem Kundensupport und Fehlerbehebung