Network Security

WatchGuard hat diesen Datenschutzleitfaden erstellt, um unsere Kunden über die Verarbeitung personenbezogener Daten im Zusammenhang mit WatchGuard Network Security Services zu informieren. Unsere Network Security Services umfassen unsere Support-Lizenz, die Basic Security Suite, die Total Security Suite und die im Rahmen dieser Lösungen angebotenen Services , einschließlich Firebox-Verwaltung und Netzwerkkonfiguration über WatchGuard Cloud, WatchGuard Dimension und WatchGuard System Manager.

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 Network 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.

Übersicht über die Network Security Services

WatchGuard bietet zusätzlich zur Standard-Support-Lizenz, die mit unseren Firebox-Geräten geliefert wird, zwei Stufen von Network Security Services an. Die Basic Security Suite beinhaltet traditionelle Services zur Intrusion Prevention, sowie Antivirus- und URL Filtering. Die Total Security Suite beinhaltet Funktionen wie einen KI-gestützten Malware-Schutz, ThreatSync (XDR) sowie Cloud-Sandboxing. Eine ausführlichere Beschreibung dieser Services finden Sie hier.

WatchGuards Rolle bei der Datenverarbeitung

Bei der Bereitstellung von Network 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 Network Security Services und unseren Verarbeitungszwecken erfasst werden. Diese Daten werden in der Regel direkt von einzelnen Endanwendern bereitgestellt, wenn sie Network Security Services verwenden, oder vom Kunden-Administrator, 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 Network Security Services bestimmte Daten auch automatisch.

Die Firebox-Administratoren oder Nutzer der WatchGuard Cloud werden möglicherweise auch gebeten, zusätzliche personenbezogene Daten bereitzustellen. Dies ist notwendig, um Network 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
Firebox® **Fireware®**	• Firebox-Seriennummer • Firebox-IP-Adresse • Geolokalisierungsdaten von Firebox basierend auf der IP-Adresse • Dem Kunden zugewiesene Lizenzschlüssel • Eindeutige Kunden-IDs wie WatchGuard Konto-IDs/Kontonummer • Grundlegendes Geräte-Feedback • Erweitertes Geräte-Feedback • Firebox-Konfigurationsdaten • Fehlerberichte, die das Firebox-Modell, die Firmware-Version, den Zeitstempel des Absturzes, die Traffic- und Ereignisprotokolle zum Zeitpunkt des Absturzes, verarbeitete IP-Adressen und Firebox-Konfigurationsdaten enthalten können • Bedrohungs-Telemetrie (auch „Proxy-Reporting" genannt), die Quell- und Ziel-IP-Adressen und PDF-Statistiken mit PDF-Namen enthalten kann • Authentifizierte Anwenderdaten (Benutzername) • Service-Zeitstempel • Zusätzliche Daten, die für die unten beschriebenen Services spezifisch sind	• Bereitstellung und Betrieb der Services • Erkennung, Analyse und Eindämmung von Bedrohungen und Sicherung der Services • Verbesserung und Entwicklung von WatchGuard Produkten und Services • Durchführung von Analysen und Berichterstattung über Produktnutzungsmuster und -trends • Bereitstellung von technischem Kundensupport und Fehlerbehebung • Einhaltung rechtlicher Verpflichtungen
Authentifizierungsdienste	• Benutzername und Passwort • Art der Benutzerauthentifizierung (Firebox-DB, Radius, Active Directory, LDAP, SAML)	• Bereitstellung und Betrieb der Services • Bereitstellung von technischem Kundensupport und Fehlerbehebung
VPN	**Für MUVPN:** • IP-Adresse des MUVPN-Endanwenders • Einstellungen für Phase I und II (Krypto, Shared Secrets, IP-Adressen) **Für BOVPN:** • E-Mail-Adresse des Anwenders • Zertifikat (wenn der Anwender das Zertifikat importiert hat) • Firebox-Version (wenn der Peer auch eine Firebox ist)	• Bereitstellung und Verwaltung des VPN-Service • Bereitstellung von technischem Kundensupport und Fehlerbehebung

Netzwerkbetrieb und SD-WAN	• Netzwerk-IP-Adressen
	• PPPoE-Benutzername und -Passwort
	• Informationen des Endanwenders:
	  • IP-Adresse des Endanwenders
	  • MAC-Adressen
	  • Hostnamen
		• Bereitstellung und Verwaltung des Service zur Überwachung der WAN-Verbindung
		• Verbesserung der Anwendungsverfügbarkeit und -leistung
		• Bereitstellung von technischem Kundensupport und Fehlerbehebung

SERVICE	KATEGORIEN PERSONENBEZOGENER DATEN	VERARBEITUNGSZWECKE

Access Portal	• SAML-Konfiguration
	• Server-IP-Adressen des Authentifizierungsservers
	• Informationen des Endanwenders:
	  • Benutzername und Passwort
	  • IP-Adressen
	  • MAC-Adressen
	  • Informationen zur Anwendergruppe
	  • Betriebssystemtyp des Kunden
	  • An-/Abmeldung des Anwenders
	  • Namen der von Endanwendern verwendeten Anwendungen
		• Bereitstellung und Verwaltung des Service durch Ermöglichung eines sicheren Fernzugriffs
		• Bereitstellung von technischem Kundensupport und Fehlerbehebung

Intrusion Prevention Service (IPS)	• Quell- und Ziel-IP-Adressen • Von Endanwendern aufgerufene URLs	• Bereitstellung und Verwaltung des Service • Erkennung, Analyse und Eindämmung von Bedrohungen • Bereitstellung von technischem Kundensupport und Fehlerbehebung

Application Control	• Quell- und Ziel-IP-Adressen
	• Von Endanwendern aufgerufene Anwendungen
	• Bericht zur Identifizierung von Anwendungen:
	  • Top-Anwendungen nach Anwender
	  • Top-Anwendung nach Host
	  • Top-Kunden nach Anwendungsnutzung
	  • Top-Kunden nach blockierten Anwendungen
		• Bereitstellung und Verwaltung des Service zur Netzwerküberwachung und -steuerung
		• Erkennung, Analyse und Eindämmung von Bedrohungen
		• Bereitstellung von technischem Kundensupport und Fehlerbehebung

WebBlocker	• Von Endanwendern aufgerufene URLs • Benutzername des Endanwenders • IP-Adresse des Endanwenders • Von Administrator festgelegtes Passwort, um den Service außer Kraft zu setzen	• Bereitstellung und Verwaltung des Service zur Kontrolle der Internetnutzung • Bereitstellung von technischem Kundensupport und Fehlerbehebung
spamBlocker™	• Name, E-Mail-Adresse, IP-Adresse des Absenders und Empfängers • Inhalt der E-Mails und Anhänge (von WatchGuard verarbeitet, aber auf dem Quarantäneserver im Netzwerk des Kunden gespeichert)	• Bereitstellung und Verwaltung des Services zum Blockieren von Spam-Nachrichten • Durchführung von Datenanalysen und Bewertungen • Bereitstellung von technischem Kundensupport und Fehlerbehebung
Gateway AntiVirus	• Dateien (und Objekte), die auf bekannte Malware gescannt werden	• Bereitstellung und Verwaltung des Service • Erkennung, Analyse und Eindämmung von Bedrohungen • Bereitstellung von technischem Kundensupport und Fehlerbehebung

SERVICE	KATEGORIEN PERSONENBEZOGENER DATEN	VERARBEITUNGSZWECKE
Reputation Enabled Defense	• Quell- und Ziel-IP-Adresse • Geografischer Standort (länderspezifisch) • Von Endanwendern aufgerufene URLs	• Bereitstellung und Verwaltung des Service durch Blockieren bestimmter Websites nach Erkennung der geografischen Standorte von Verbindungen zum und vom Netzwerk des Kunden • Durchführung von Datenanalysen und Bewertung der Websites zur Produktverbesserung • Bereitstellung von technischem Kundensupport und Fehlerbehebung

Network Discovery	• Abbildung der Kundengeräte
	• Informationen des Endanwenders:
	  • Benutzername (wenn der Anwender auf dem Gerät authentifiziert ist)
	  • IP-Adresse des Geräts
	  • Hostname des Geräts
	  • MAC-Adresse des Geräts
	  • Betriebssystem und -dienste des Geräts
	  • Offene Netzwerk-Ports des Geräts
	  • Mobiler Compliance-Status, wenn es sich bei den Geräten um Mobile Security-Geräte handelt
		• Bereitstellung und Verwaltung des Service durch Erkennung von Geräten im Kundennetzwerk und Anzeige der erkannten Geräte auf einer Netzwerkabbildung
		• Bereitstellung von technischem Kundensupport und Fehlerbehebung

APT Blocker	• IP-Adresse des Endanwenders • Dateien (oder Objekte), die auf Malware und Zero-Day-Exploits gescannt werden (WatchGuard sucht nach Links und Anhängen zu den Dateien. Nur die Dateisignatur (nicht aber die Datei selbst) wird gespeichert, wenn eine Erkennung erfolgt.)	• Bereitstellung und Verwaltung des Service • Erkennung, Analyse und Eindämmung von Bedrohungen • Verbesserung und Entwicklung des Produkts • Bereitstellung von technischem Kundensupport und Fehlerbehebung

DNSWatch®	• Verbindungsinformationen einschließlich Netzwerkprotokoll
	• Informationen des Endanwenders:
	  • Benutzername
	  • E-Mail-Adresse
	  • IP-Adresse
		• Bereitstellung und Verwaltung des Service
		• Erkennung, Analyse und Eindämmung von Bedrohungen
		• Verbesserung und Weiterentwicklung des Produkts zur Steigerung der Effizienz des Service
		• Bereitstellung von technischem Kundensupport und Fehlerbehebung

IntelligentAV®	• IP-Adresse des Endanwenders • Dateien (oder Objekte), die auf bekannte und unbekannte Malware gescannt werden	• Bereitstellung und Verwaltung des Service • Erkennung, Analyse und Eindämmung von Bedrohungen • Bereitstellung von technischem Kundensupport und Fehlerbehebung

ThreatSync® (XDR)	• Informationen des Endanwenders:
	  • Benutzername
	  • IP-Adresse
	  • Gerätedaten (z. B. Hostname, MAC-Adresse, Gerätekennungen)
	  • Nutzungsdaten (z. B. verwendete Funktionen, Anzahl der Anwender)
	  • Anwendergenerierte Inhalte (wie Dateipfade und in Dateien enthaltene Informationen)
	• Andere technische Informationen, die möglicherweise personenbezogene Daten enthalten, wie z. B. Prozess-IDs, Prozessbäume, Dateisystemereignisse, Windows-Registrierungsereignisse
		• Bereitstellung und Verwaltung des Service
		• Erkennung, Analyse und Eindämmung von Bedrohungen
		• Verbesserung und Entwicklung des Produkts
		• Bereitstellung von technischem Kundensupport und Fehlerbehebung

SERVICE	KATEGORIEN PERSONENBEZOGENER DATEN	VERARBEITUNGSZWECKE

EDR Core	• Informationen des Endanwenders:
	  • Name (als Teil von Pfaden und Dokumentnamen)
	  • Benutzername
	  • E-Mail-Adresse
	  • IP-Adresse
	  • Gerätedaten (wie Hostname, MAC-Adresse, Hardware-Details, Gerätekennungen)
	  • Aufgerufene URLs
		• Bereitstellung und Verwaltung des Service
		• Erkennung, Analyse und Eindämmung von Bedrohungen
		• Verbesserung und Entwicklung des Produkts
		• Bereitstellung von technischem Kundensupport und Fehlerbehebung

Data Loss Prevention	• Informationen des Endanwenders:
	  • Benutzername
	  • IP-Adresse
	  • Daten in Kundendateien
	• Serviceprotokolle (die DLP-Regeln/Muster, die abgeglichen wurden, und Dateinamen, aber nicht die Datei oder Daten in der Datei enthalten)
		• Bereitstellung und Verwaltung des Service
		• Erkennung, Analyse und Eindämmung von Bedrohungen
		• Bereitstellung von technischem Kundensupport und Fehlerbehebung

Support	• Alle vom Kundenadministrator bereitgestellten Informationen	• Bereitstellung technischer Unterstützung auf Kundenwunsch

MANAGEMENTSYSTEM	KATEGORIEN PERSONENBEZOGENER DATEN	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:** Konfigurationen, Verbindungen und Protokolle, die personenbezogene Daten von Endanwendern des Kunden enthalten können, wie z. B.: • IP-Adressen von Endanwendern • Benutzername • Dateiname • URLs und verwendete Anwendungen • Von einem bestimmten Endanwender aufgerufene URLs und Anwendungen • Je nach Konfiguration, Aktionen des Endanwenders und/oder Passwörtern **WGC-Auditprotokolle:** Daten von WGC-Nutzern: • Konto-ID/Kontonummer • Benutzername • IP-Adresse • Zeitpunkt/Datum des Zugriffs • Quelle (Produkt, mit dem interagiert wurde) • Ausgeführte Aktivitäten **Diagnosetools:** • Wenn Diagnosetools innerhalb von WGC verwendet werden, können TCP-Pakete alle personenbezogenen Daten enthalten, die als Teil von Netzwerkpaketen verarbeitet werden, die von den Services verarbeitet werden.	• Bereitstellung und Verwaltung des Service • Erkennung, Analyse und Eindämmung von Bedrohungen und Sicherung der Services • Bereitstellung von technischem Kundensupport und Fehlerbehebung • Einhaltung rechtlicher Verpflichtungen

MANAGEMENTSYSTEM	KATEGORIEN PERSONENBEZOGENER DATEN	VERARBEITUNGSZWECKE
WatchGuard Dimension®	**Dimensions-Feedback:** • Dimension IP-Adresse (ISP-IP-Adresse) und Geolokalisierung • Seriennummern der verbundenen Fireboxes • WatchGuard Dimension wird lokal vom Kunden installiert und verwaltet. WatchGuard hat über WatchGuard Dimension keinen Zugriff auf Visualisierungsdaten von Services, es sei denn, der Kunde fordert technische Unterstützung an und gewährt Zugriff.	• Bereitstellung und Verwaltung des Service • Erkennung, Analyse und Eindämmung von Bedrohungen • Analyse von Produktnutzungsmustern und -trends und Berichterstattung darüber • Bereitstellung von technischem Kundensupport und Fehlerbehebung
WatchGuard® System Manager	• WatchGuard System Manager wird lokal vom Kunden installiert und verwaltet. WatchGuard hat über WatchGuard System Manager keinen Zugriff auf Visualisierungsdaten von Services, es sei denn, der Kunde fordert technische Unterstützung an und gewährt Zugriff.	• Bereitstellung von technischem Kundensupport und Fehlerbehebung

Von WatchGuard erfasste Servicedaten

Während der Nutzung von Network Security-Produkten und -Services durch unsere Kunden erfasst WatchGuard automatisch bestimmte Geräte-, Protokoll- und Nutzungsdaten (wir nennen diese „Servicedaten“) (weitere Informationen siehe unten). Diese Daten werden von WatchGuard zur Bereitstellung, Wartung und Unterstützung der Services sowie für eigene Geschäftszwecke verwendet, z. B. zur Verwaltung von Kundenlizenzen, zur Fehlerbehebung, zur Verbesserung und Entwicklung neuer Produkte und Services, zur Einhaltung gesetzlicher Vorschriften wie z. B. Exportkontrollbestimmungen sowie zur Durchführung von Analysen und Erstellung von Berichten zu Produktnutzungsmustern und -trends.

Protokolle der Diagnoseanwendung. WatchGuard erfasst Anwendungsprotokolle, um Serviceprobleme zu diagnostizieren und zu beheben, die von unseren Systemen oder denen unserer Kunden gemeldet werden, und um unsere Produkte und Services weiter zu verbessern. Die in internen Anwendungsprotokollen erfassten Informationen können Daten enthalten, die als personenbezogene Daten gelten, wie z. B. WatchGuard Konto- und Benutzer-IDs oder IP-Adressen. Die Verarbeitung der Daten erfolgt unter Berücksichtigung der Anonymisierung oder, sofern dies nicht möglich ist, der De-Identifizierung und Aggregation. In jedem Fall werden die Daten auf der Ebene der Produktionsdaten gesichert. Die Erfassung von Diagnoseprotokollen kann nicht deaktiviert werden.

Geräte-Feedback. Das Geräte-Feedback hilft WatchGuard bei der Fehlerbehebung und Sicherung unserer Services, bei der Bewertung der Bedrohungslandschaft und bei der Einhaltung gesetzlicher Auflagen wie Exportkontrollvorschriften. Es wird auch verwendet, um unsere Produkte und Services zu verbessern. Das Geräte-Feedback kann Informationen darüber enthalten, wie die Firebox verwendet wird und welche Probleme unsere Kunden mit der Firebox haben, aber es enthält keine Informationen über unsere Kunden und deren Endanwender oder Kundendaten, die über die Firebox gesendet werden. Daher besteht das Geräte-Feedback hauptsächlich aus technischen Informationen und enthält möglicherweise nur begrenzte personenbezogene Daten (wenn überhaupt) wie die Seriennummer der Firebox, die IP-Adresse und die Geolokalisierung auf Länderebene. Die Firebox sendet zwei Arten von Geräte-Feedback-Daten an WatchGuard: (1) Grundlegendes Geräte-Feedback, das immer aktiviert ist und nicht deaktiviert werden kann, und (2) erweitertes Geräte-Feedback, das unsere Kunden durch Ablehnung deaktivieren können. Weitere Informationen zum Geräte-Feedback und zur Deaktivierung des erweiterten Geräte-Feedbacks finden Sie hier.

Bedrohungs-Telemetrie (auch „Proxy-Reporting“ genannt). WatchGuard erfasst Telemetriedaten zu Bedrohungen, um diese zu untersuchen und die aktuelle Bedrohungslandschaft zu analysieren. Anschließend verwenden wir die anonymisierten und aggregierten Daten, um Trends bei der Erkennung von Bedrohungen im vierteljährlichen Internet Security Report von WatchGuard und auf unserer Cybersecurity Hub-Seite aufzuzeigen. Die Bedrohungs-Telemetrie kann Vorfallsberichte enthalten, die begrenzte personenbezogene Daten wie Quell- und Ziel-IP-Adressen und PDF-Dateistatistiken mit PDF-Dateinamen (jedoch nicht den Inhalt der Dateien) umfassen. Wenn Ihre Organisation Fireboxes mit Fireware v12.11 verwendet, können Sie die Erfassung von Bedrohungsdaten deaktivieren, indem Sie das Kontrollkästchen „Send Threat Telemetry to WatchGuard“ deaktivieren. Bei älteren Geräten ist dies durch Deaktivierung der Erfassung des erweiterten Geräte-Feedbacks möglich (siehe oben).

Fehlerberichte. WatchGuard erfasst Fehlerberichte, um Fehler zu beheben und unsere Produkte und Services zu verbessern. Die in den Fehlerberichten enthaltenen Informationen können die Seriennummer der Firebox, das Modell, die Firmware-Version, den Absturz-Zeitstempel, die Traffic- und Ereignisprotokolle zum Zeitpunkt des Absturzes, die verarbeiteten IP-Adressen und die Firebox-ID enthalten. Einige dieser Informationen können personenbezogene Daten enthalten oder darstellen. Fehlerberichte werden nur gesendet, wenn der Kunde das Kästchen „Send Fault Reports to WatchGuard“ markiert.

WatchGuard Cloud-Nutzungsdaten. Wir verwenden ein Tool namens Pendo, um unseren WatchGuard Cloud-Anwendern (den WatchGuard Cloud-Nutzern unserer Kunden) In-App-Anleitungen zur Verfügung zu stellen und Nutzungsdaten zu erfassen, die zur Erstellung statistischer Analysedaten verwendet werden, um Benutzerprobleme besser diagnostizieren und die Benutzererfahrung verbessern zu können. Pendo zeichnet Anwenderereignisse auf und speichert diese, um Anwenderaktionen wie Mausklicks, Bewegungen, Aktionen in der Konsole, Verweildauer auf verschiedenen Seiten und anonyme Einzelbesucher zu überwachen. Die erfassten Daten werden in aggregierter und anonymisierter Form verarbeitet. Wenn der WatchGuard Cloud-Nutzer die Cookies in der WatchGuard Cloud ablehnt, werden seine Daten nicht erfasst, er verliert jedoch den Zugriff auf die In-App-Anleitungen. Wir verwenden außerdem Google Analytics, um in begrenztem Umfang Nutzungsdaten direkt von den Browsern der Anwender zu erfassen, um Ihre Nutzung der WatchGuard Cloud Services besser zu verstehen, Probleme zu diagnostizieren und zu beheben sowie die Services zu verbessern. Lehnt der WatchGuard Cloud-Nutzer die Cookies innerhalb der WatchGuard Cloud ab, werden seine Daten nicht erfasst.

Schutz Ihrer personenbezogenen Daten

WatchGuard hat technische und organisatorische Maßnahmen ergriffen, um personenbezogene Daten vor versehentlichem Verlust und unbefugtem Zugriff, unbefugter Verwendung, Änderung und Offenlegung zu schützen. Wir unterhalten ein robustes Sicherheits- und Datenschutzprogramm, das sich mit dem Sicherheitsmanagement befasst. WatchGuard hat die ISO/IEC 27001:2013-Zertifizierung seines Informationssicherheits-Managementsystems (ISMS) erhalten. ISO 27001 ist eine weltweit anerkannte Norm, die die Anforderungen für die Einrichtung, Implementierung, Wartung und kontinuierliche Verbesserung eines ISMS festlegt. Die Details der Zertifizierung sind unter https://www.schellman.com/certificate-directory öffentlich zugänglich. Der Sicherheitsansatz von WatchGuard umfasst Richtlinien, Verfahren und Kontrollen mit dem Ziel, die Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten, die in den Systemen und Netzwerken von WatchGuard gespeichert sind.

Cookies und ähnliche Technologien

Wir verwenden gängige Datenerfassungstools wie Cookies, Web Beacons und ähnliche Technologien, um automatisch bestimmte Informationen zu erfassen, wenn Kunden die WatchGuard Cloud nutzen, einschließlich der WatchGuard Cloud-Nutzungsdaten (siehe oben). WatchGuard Cloud-Nutzer können die Verwendung von Cookies in der WatchGuard Cloud ablehnen oder diese löschen. Wenn der WatchGuard Cloud-Nutzer die Verwendung von Cookies in der WatchGuard Cloud ablehnen möchte, kann er diese im Cookie-Banner der Plattform deaktivieren, indem er auf „Manage Cookies" klickt. Weitere Informationen zu Cookies und ähnlichen Technologien in der WatchGuard Cloud finden Sie in unserem Cookie-Hinweis für den WatchGuard Cloud-Service.

Informationen zur Verwendung von Tools zur Datenerfassung auf unseren Websites finden Sie in unserer Datenschutzrichtlinie und Cookie-Richtlinie.

Verarbeitungsstandorte und Datenübermittlungen

Die von uns erfassten personenbezogenen Daten werden in der Region des Kunden, in den USA oder in einem anderen Land gespeichert und verarbeitet, in dem wir oder unsere Tochtergesellschaften, Niederlassungen oder Dienstanbieter Einrichtungen unterhalten. Weitere Informationen finden Sie in der Liste der Unterauftragsverarbeiter von WatchGuard.

Unabhängig davon, wo personenbezogene Daten verarbeitet werden, ergreifen wir Maßnahmen, um sicherzustellen, dass die Verarbeitung personenbezogener Daten in Übereinstimmung mit diesen Datenschutzbestimmungen, der WatchGuard Datenschutzrichtlinie, unserem Zusatz zur Datenverarbeitung und den geltenden Datenschutzgesetzen erfolgt. Weitere Informationen finden Sie in den FAQs zu den Datenübermittlungen von WatchGuard.

Rechte der betroffenen Personen

Wenn WatchGuard der für die Verarbeitung Verantwortliche ist, haben Endanwender und alle anderen Personen, deren personenbezogene Daten von den Network Security Services verarbeitet werden, das Recht, Auskunft über die von den Network Security Services verarbeiteten personenbezogenen Daten zu verlangen und diese Daten berichtigen zu lassen, ihre Verarbeitung auszusetzen oder die Löschung der Daten zu verlangen. Weitere Informationen darüber, wie diese Rechte ausgeübt werden können, finden Sie im Abschnitt „Ihre Datenschutzrechte" in der Datenschutzrichtlinie von WatchGuard.

Wenn WatchGuard personenbezogene Daten als Auftragsverarbeiter im Auftrag und auf Anweisung seines Kunden verarbeitet, werden betroffene Personen an den jeweiligen für die Verarbeitung Verantwortlichen (unseren Kunden) verwiesen.