AuthPoint-Datenschutz

Dieser Leitfaden zum Datenschutz beschreibt die Verarbeitung personenbezogener Daten durch WatchGuard Technologies, Inc. („WatchGuard“) in Verbindung mit WatchGuard AuthPoint-Lösungen. Dazu gehören das AuthPoint Multifaktor-Authentifizierungsprodukt („AuthPoint MFA“), die AuthPoint Total Identity Security-Lösung und die als Teil dieser Lösungen angebotenen Verbesserungen, einschließlich der AuthPoint-Verwaltung über WatchGuard Cloud, der mobilen AuthPoint-App, dem Corporate Password Manager, Dark Web Scan, Dark Web Monitor und die hier beschriebenen verwandten Funktionen.

Übersicht über AuthPoint-Lösungen

AuthPoint MFA wird als eigenständiges Produkt oder als Teil von AuthPoint Total Identity Security angeboten. Zusätzlich zu AuthPoint MFA umfasst AuthPoint Total Identity Security den Corporate Password Manager und Dark Web Monitor von WatchGuard. Weitere Informationen zu AuthPoint-Lösungen finden Sie im AuthPoint-Produktdatenblatt.

Umfang

Zur Verwendung der AuthPoint-Lösungen werden Sie möglicherweise aufgefordert, Ihre personenbezogenen Daten anzugeben. Dieser Leitfaden soll die WatchGuard-Datenschutzrichtlinie ergänzen und beschreibt die Verarbeitung personenbezogener Daten durch WatchGuard, die für die Bereitstellung von AuthPoint-Lösungen spezifisch ist. Es wird nicht beschrieben, wie WatchGuard personenbezogene Daten im Zusammenhang mit seinen anderen Produkten und Dienstleistungen (z. B. WatchGuard Cloud) oder allgemeineren Geschäftsaktivitäten von WatchGuard (z. B. Bereitstellung von Kundensupport, Schulungen, Veranstaltungen usw.) verarbeitet.

Die Rolle von WatchGuard in Bezug auf Ihre personenbezogenen Daten

In Rechtsordnungen, in denen zwischen Verantwortlichen und Auftragsverarbeitern (z. B. EWR und Vereinigtes Königreich) oder Unternehmen und Dienstleistern (z. B. in Kalifornien) unterschieden wird, ist WatchGuard der Verantwortliche oder das Unternehmen in Bezug auf die personenbezogenen Daten, die für seine legitimen oder betrieblichen Geschäftszwecke verarbeitet werden, z. B. zur Verwaltung und Steuerung der Kundenbeziehung, zur Sicherung der Services oder zur Produktverbesserung, einschließlich der statistischen Analyse von Nutzungsdaten. Für die meisten der in diesem Datenschutzleitfaden beschriebenen Verarbeitungszwecke fungiert WatchGuard als Auftragsverarbeiter oder Dienstleister und Ihr Unternehmen (das unser Kunde und Ihr Arbeitgeber sein kann) ist der Verantwortliche oder das Unternehmen in Bezug auf Ihre personenbezogenen Daten.

Wenn Sie ein Endbenutzer sind und datenschutzbezogene Fragen oder Bedenken zu den Datenschutzpraktiken oder den Entscheidungen haben, die Ihr Unternehmen (das unser Kunde und Ihr Arbeitgeber sein kann) in Bezug auf die Verwendung Ihrer personenbezogenen Daten getroffen hat, sollten Sie sich an Ihr Unternehmen wenden oder gegebenenfalls deren Datenschutzhinweise lesen.

WatchGuard ist nicht verantwortlich für die Datenschutz- oder Sicherheitspraktiken seiner Kunden, die von denen in diesem Datenschutzleitfaden oder der WatchGuard-Datenschutzrichtlinie abweichen können.

Umfang und Gründe für die von uns erfassten personenbezogenen Daten

In den folgenden Tabellen sind die von WatchGuard gesammelten personenbezogenen Daten aufgeführt, um AuthPoint MFA und Password Manager bereitzustellen und zu beschreiben, warum wir Ihre Daten verarbeiten. Solche Informationen werden in der Regel direkt von Ihnen bereitgestellt, wenn Sie die AuthPoint-Lösungen verwenden, oder von Ihrem Organisationsadministrator, wenn Sie oder Ihre Organisation ein Konto registrieren. Darüber hinaus erfassen wir automatisch bestimmte Geräte-, Nutzungs- und Protokollinformationen, auch wenn Sie die mobile AuthPoint-App verwenden. Wie unten beschrieben, bitten wir Sie möglicherweise um Ihre Zustimmung, bevor wir bestimmte Informationen sammeln (z. B. genaue Geolokalisierungsinformationen).

AuthPoint MFA

DATENTYP	DATENKATEGORIEN	VERARBEITUNGSZWECKE
Endbenutzer-Registrierungsinformationen	• Name • Benutzername • E-Mail-Adresse • Passwort • Token-gerechtes Bild (optional und nur bei Erteilung von Foto- oder Kameraberechtigungen) • Geschäftsanschrift (optional) • Telefonnummer (optional)	• Benutzererstellung und Token-Aktivierung • Serviceauthentifizierung und Anmeldung • Ermöglicht dem Administrator des Kunden, Endbenutzer zu unterstützen und Helpdesk-Support bereitzustellen
Endbenutzer-Mobilgeräteinformationen	• Mobilgerätname • Marke und Modell des Geräts • Betriebssystem und -version des Geräts • Geräteversion und andere Gerätemerkmale (z. B. ein Gerät mit Jailbreak oder wenn es sich anderweitig in einem kompromittierten Zustand befindet, eine Bildschirmsperre vorhanden ist, der Emulator ausgeführt wird oder böswillige Software installiert ist) • Gerätekennungen (z. B. Gerätename, Prozessor-ID, Seriennummern) zum Erstellen einer eindeutigen Kennung – der sogenannten Geräte-DNA, die einen Hash der Gerätekennungen umfasst • Browsertyp, Browserversion • Öffentliche IP-Adresse • Genaue Geolokalisierungsinformationen (GPS) von Ihrem Mobilgerät, aber nur, wenn Sie Ihre Zustimmung zu einer solchen Erfassung erteilt haben • Name der Anwendung, auf die der Benutzer über AuthPoint MFA zuzugreifen versucht • PIN zum Schützen und Entsperren mobiler Token	• Bereitstellung und Erhaltung der Services • Verbesserung der Benutzererfahrung, Qualität und Benutzerfreundlichkeit der Services • Verbesserung der Sicherheitsfunktionalität durch Berechnung der mit der Geolokalisierung verbundenen Risiken • Sicherung der Services (z. B. wird DDID verwendet, um die Authentizität des Geräts zu überprüfen, indem sichergestellt wird, dass es nicht geklont wird) • Verwendung der öffentlichen IP-Adresse zur Bestimmung des ungefähren Gerätestandorts für Risiko- und Richtlinienzwecke • Durchführung statistischer Analysen mit pseudonymisierten und/oder aggregierten Nutzungsdaten zur Verbesserung der Services • Schutz der Token vor unbefugter Verwendung/Missbrauch • Fehlerbehebung bei Kompatibilitätsproblemen mit Versionsverwaltung, Updates und Hardware
Endbenutzer-Computerinformationen	• Computername • Marke und Modell des Computers • Betriebssystem und -version des Computers • Browsertyp, Browserversion • Öffentliche IP-Adresse • Genaue Geolokalisierungsinformationen (GPS) von Ihrem Computer, aber nur, wenn Sie Ihre Zustimmung zu einer solchen Erfassung erteilt haben • Name der Anwendung, auf die der Benutzer über AuthPoint MFA zuzugreifen versucht	• Bereitstellung und Erhaltung der Services • Verbesserung der Benutzererfahrung, Qualität und Benutzerfreundlichkeit der Services • Verbesserung der Sicherheitsfunktionalität durch Berechnung der mit der Geolokalisierung verbundenen Risiken • Sicherung der Services (z. B. wird DDID verwendet, um die Authentizität des Geräts zu überprüfen, indem sichergestellt wird, dass es nicht geklont wird) • Verwendung der öffentlichen IP-Adresse zur Bestimmung des Gerätestandorts für Risiko- und Richtlinienzwecke • Durchführung statistischer Analysen mit pseudonymisierten und/oder aggregierten Nutzungsdaten zur Verbesserung der Services • Fehlerbehebung bei Kompatibilitätsproblemen mit Versionsverwaltung, Updates und Hardware

DATENTYP	DATENKATEGORIEN	VERARBEITUNGSZWECKE
Ereignisse und Nutzungsdaten	• Wie Endbenutzer Anwendungen und Services über AuthPoint MFA verwenden und darauf zugreifen • Wenn Endbenutzer über AuthPoint MFA auf Services zugreifen (z. B. Datum und Uhrzeit des Zugriffs) • Von wo aus der Zugriff auf die Services basierend auf der öffentlichen IP-Adresse erfolgt • Geräteereignisse und Protokolle im Zusammenhang mit Fehlern und Abstürzen • Sicherheitsrelevante Ereignisse, wie eine verweigerte Authentifizierung oder unbefugte Zugriffsversuche • Lizenzstatus (aktiv/abgelaufen)	• Bereitstellung und Erhaltung der Services • Bessere Erfahrungen für Anwender • Verbesserung der Sicherheitsfunktionalität • Verbesserung der Servicequalität • Durchführung statistischer Analysen mit pseudonymisierten und/oder aggregierten Nutzungsdaten zur Verbesserung der Services • Vorbeugung, Erkennung, Reaktion auf und Schutz vor potenziellen oder tatsächlichen Ansprüchen, Verbindlichkeiten, verbotenem Verhalten, Sicherheitsrisiken und kriminellen Aktivitäten
Aktivitätsprotokolle	• Welche Endbenutzer auf die Services zugreifen • Welche Geräte auf die Services zugreifen • Durch die Services geschützte Anwendungen • Zeitpunkt des Zugriffs auf die Services • Öffentliche IP-Adresse des Endbenutzers beim Zugriff auf die Services • Welche Administratoren (d. h. Administratoren, die zur Verwaltung des Kundenkontos berechtigt sind) auf die Verwaltungsoberfläche zugreifen • Verwaltungs- und managementbezogene Aktivitäten (z. B. Maßnahmen des Kundenadministrators)	• Bereitstellung und Erhaltung der Services • Bereitstellung von Prüfprotokolldaten für die Administratoren des Kunden • Benachrichtigungen über sicherheitsrelevante Ereignisse, z. B. eine verweigerte Authentifizierung • Bessere Erfahrungen für Anwender • Verbesserung der Sicherheitsfunktionalität • Verbesserung der Servicequalität • Durchführung statistischer Analysen mit pseudonymisierten und/oder aggregierten Nutzungsdaten zur Verbesserung der Services • Vorbeugung, Erkennung, Reaktion auf und Schutz vor potenziellen oder tatsächlichen Ansprüchen, Verbindlichkeiten, verbotenem Verhalten, Sicherheitsrisiken und kriminellen Aktivitäten

AuthPoint Password Manager

DATENTYP	DATENKATEGORIEN	VERARBEITUNGSZWECKE
Daten, die während des Password Manager-Kontoerstellungsprozesses gesammelt wurden	• E-Mail-Adresse • Tresor-Passwort	• Kontoerstellung • Bereitstellung des Password Manager-Services • Serviceauthentifizierung und Anmeldung • Servicesicherung • Sichern und Verwahren von in Password Manager gespeicherten Anmeldedaten
Anmeldedaten für den Unternehmenstresor	• Titel der Website oder App-Name • URL der Anmeldeseite (mit Miniaturansicht) • PIN zum Schützen und Entsperren mobiler Token • Benutzeranmeldedaten (z. B. E-Mail-Adresse oder eine andere vom Benutzer verwendete Anmeldung) • Verschlüsseltes Passwort • Hinweisfeld (freier Text)	• Bereitstellung des Password Manager-Services • Automatisches Ausfüllen von Anmeldedaten und automatisches Anmelden bei Websites und Anwendungen, die eine formularbasierte Eingabe über Password Manager ermöglichen • Analyse der Passwortqualität (z. B. Überprüfung auf wiederverwendete, schwache oder kompromittierte Passwörter)

DATENTYP	DATENKATEGORIEN	VERARBEITUNGSZWECKE
Anmeldedaten für privaten Tresor (Gilt nur, wenn die Verwendung des privaten Tresors gemäß den internen Richtlinien Ihres Unternehmens zulässig ist)	• Website oder App-Name • URL der Anmeldeseite (mit Miniaturansicht) • Benutzeranmeldung (z. B. E-Mail-Adresse oder eine andere vom Benutzer verwendete Anmeldung) • Verschlüsselte Passwörter • Hinweisfeld (freier Text)	• Bereitstellung von Password Manager • Automatisches Ausfüllen von Anmeldedaten und automatisches Anmelden bei Websites und Anwendungen, die eine formularbasierte Eingabe über Passwort-Manager ermöglichen • Analyse der Passwortqualität (z. B. Überprüfung auf wiederverwendete, schwache oder kompromittierte Passwörter)
Daten des Endbenutzers für das Unternehmenszentrum zur Anmeldedatenfreigabe	• Anzeigename für gemeinsam genutzte Anmeldedaten	• Sichere Freigabe von Anmeldedaten zwischen zwei oder mehr registrierten/aktivierten Benutzern desselben Kontos für eine Anwendung oder Website (falls vom Endbenutzer initiiert)
Daten zur Anmeldedatenfreigabe für Bediener/MSP	• Im Verwaltungsportal erstellte und zu Gruppen von Endbenutzern zugewiesene Links für den Zugriff über das Anwendungsportal	• Sichere Freigabe von Anmeldedaten zwischen Gruppen von registrierten/aktivierten Benutzern desselben Kontos für eine Anwendung oder Website (falls vom Administrator des Kunden initiiert)
Prüfung, Ereignisse, Aktivitätsprotokolle und andere automatisch gesammelte Daten	• Protokollierung und Prüfung von Administratorkonfigurationen • Geräteereignisse und Protokolle im Zusammenhang mit Fehlern und Abstürzen • Lizenzstatus (aktiv/abgelaufen) – Protokoll der kompromittierten Anmeldedaten (Warnung) • Version der installierten mobilen App • Version der verwendeten Browsererweiterung	• Bereitstellung und Erhaltung des Password Manager-Services • Bereitstellung von Prüfprotokolldaten für die Administratoren des Kunden • Verbesserung der Benutzererfahrung und der Servicequalität • Verbesserung der Sicherheitsfunktionalität • Fehlerbehebung und Lösung von Kompatibilitätsproblemen

Um zu erfahren, wie Ihre Daten von Dark Web Monitor von WatchGuard verarbeitet werden können, lesen Sie die Datenschutzerklärung zu Dark Web Scanner und Dark Web Monitoring von WatchGuard.

Berechtigungen der mobilen AuthPoint-App von WatchGuard

Im Allgemeinen kann WatchGuard nicht auf Dinge wie Ihre Kontakte, Telefondateien, Textnachrichten und E-Mails zugreifen. Wir verfügen jedoch über einige Berechtigungen für Gerätedaten, die wir anfordern, wenn Sie die mobile AuthPoint-App verwenden, um Ihnen die Multifaktor-Authentifizierung zu erleichtern oder bestimmte Funktionen zu aktivieren.

- **Berechtigung zum Senden von Push-Benachrichtigungen.** Push-Benachrichtigungen versenden wir nur zu zwei Zwecken: (1) Um Ihnen eine Anmeldeanfrage zur Genehmigung oder Ablehnung zu senden, oder (2) um Sie auf ein Sicherheitsproblem aufmerksam zu machen, das wir auf Ihrem Gerät feststellen. Wir werden niemals Spam oder irrelevante Push-Benachrichtigungen senden. Sie können diese Berechtigung ablehnen, müssen dann jedoch eine andere Methode verwenden, z. B. die Eingabe eines Einmalpassworts (One-Time Password, OTP), um eine Anmeldung über AuthPoint MFA durchzuführen.

- **Kamerazugriff**. Diese Berechtigung erfordert, dass Sie der mobilen AuthPoint-App ausdrücklich die Berechtigung erteilen, QR-Codes, die zum Aktivieren eines AuthPoint-Tokens verwendet werden, mit Ihrer Kamera zu scannen, ein persönliches Multifaktor-Authentifizierungskonto wie Social-Media-Token hinzuzufügen und eine QR-Code-basierte Authentifizierung durchzuführen. Sie können diese Berechtigung ablehnen, aber ohne diesen Zugriff müssen Sie AuthPoint-Token aktivieren, indem Sie auf eine in der Aktivierungs-E-Mail enthaltene Schaltfläche klicken, Zeichenfolgen und Daten manuell eingeben, um ein persönliches Token hinzuzufügen, und Sie können keine QR-Code-basierte Authentifizierung verwenden. Die mobile AuthPoint-App verwendet Ihre Kamera nur, wenn Sie einen QR-Code scannen. Wir können auch den Zugriff auf Ihre Kamera anfordern, wenn Sie ein Bild aufnehmen möchten, um Ihr Profil für die mobile AuthPoint-App zu füllen.

- **Foto/Medienspeicher/Dateien/Speicherzugriff.** Wenn Sie Ihre Token für die mobile AuthPoint-App mit einem Bild personalisieren möchten, bitten wir Sie um Zugriff auf Ihr Foto oder andere Dateien, damit Sie ein Bild Ihrer Wahl hochladen können.

- **Zugriff auf exakte Geolokalisierungsdaten (GPS).** Wir fordern möglicherweise den Zugriff auf Ihre exakten Geolokalisierungsdaten (GPS) an, wenn Sie die mobile AuthPoint-App verwenden. Sie können es ablehnen, dass wir derartige Daten sammeln. In diesem Fall können wir Ihnen bestimmte Funktionen oder Funktionalitäten nicht zur Verfügung stellen, z. B. Geofencing mit exakter GPS-Position.

- **Zugriff mit biometrischer ID.** Diese Berechtigung erfordert, dass Sie der mobilen AuthPoint-App ausdrücklich die Berechtigung erteilen, Sie mit Ihrer aktivierten biometrischen Authentifizierung (Fingerabdruck oder Gesichtserkennung) über den Betriebssystemdienst Ihres mobilen Geräts zu authentifizieren. Wir erhalten keinen Zugriff auf die biometrischen Daten selbst oder verarbeiten diese auf andere Weise.

- **Sicherung/Wiederherstellung von Drittanbieter-Token.** Diese Berechtigung ermöglicht es Ihnen, Drittanbieter-Token in der mobilen AuthPoint-App automatisch auf Google Drive und iDrive mit passwortgeschützten Anmeldedaten zu sichern.

Nutzungsdaten, die von WatchGuard für eigene Zwecke gesammelt und verwendet werden

Wir verwenden einen pseudonymisierten mobilen Service für Absturzmeldungen namens Firebase Crash Reporting. Firebase sammelt Informationen über App-Abstürze, die wir verwenden, um die Stabilität der mobilen AuthPoint-App zu überwachen und Fehler in der App zu beheben.

Wenn Sie sich im EWR, im Vereinigten Königreich oder in der Schweiz befinden, beachten Sie, dass WatchGuard für die in diesem Abschnitt beschriebenen Nutzungs- und Absturzdaten verantwortlich ist.

Schutz Ihrer personenbezogenen Daten

WatchGuard hat geeignete 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 Computersystemen und Netzwerken von WatchGuard gespeichert sind.

Cookies und ähnliche Technologien

Wir verwenden gängige Tools zum Sammeln von Informationen, z. B. Tools zum Sammeln von Nutzungsdaten, Cookies, Web-Beacons und ähnliche Technologien, um automatisch Informationen zu sammeln, die personenbezogene Daten von Ihrem Computer oder Mobilgerät enthalten können, wenn Sie die AuthPoint-Lösungen verwenden. Weitere Informationen zur Verwendung von Tools zur Datensammlung finden Sie in unserer hauptsächlichen Datenschutzrichtlinie und unserer Cookie-Richtlinie.

Übermittlung Ihrer personenbezogenen Daten

Von uns erfasste personenbezogene Daten werden in Ihrer Region, in den USA oder in einem anderen Land gespeichert und verarbeitet, in dem wir oder unsere Tochtergesellschaften, Niederlassungen oder Dienstanbieter Einrichtungen unterhalten. Unabhängig davon, wo sich Ihre Daten befinden, ergreifen wir Maßnahmen, um Ihre personenbezogenen Daten in Übereinstimmung mit diesem Datenschutzleitfaden, der WatchGuard-Datenschutzrichtlinie und dem geltenden Datenschutzrecht zu verarbeiten.

Ihre Datenschutzrechte

In den meisten Fällen verarbeitet WatchGuard personenbezogene Daten von AuthPoint-Benutzern als Auftragsverarbeiter, der im Auftrag und auf Anweisung seiner Kunden handelt. Wenn Sie Ihre Datenschutzrechte wahrnehmen möchten, sollten Sie sich an Ihre Organisation (unseren Kunden) wenden, die in Bezug auf Ihre personenbezogenen Daten als Verantwortlicher oder Unternehmen fungiert.

Um zu erfahren, wie Sie Ihre Datenschutzrechte in den Fällen wahrnehmen können, in denen WatchGuard für Ihre personenbezogenen Daten in Verbindung mit den AuthPoint-Lösungen verantwortlich ist, lesen Sie die Datenschutzrichtlinie von WatchGuard.