Einführung in die Datensicherheit bei Matterport

Version 1.8, Dezember 2018

Matterport Sicherheitsüberblick

Einführung

Matterport verpflichtet sich, die Kundendaten sicher aufzubewahren und sicherzustellen, dass private Daten geschützt sind. Dieses Dokument gibt eine Übersicht über die Sicherheitsmaßnahmen bei Matterport in einer Form, die zwischen beteiligten Unternehmen keiner Geheimhaltungsvereinbarung (Non-Disclosure Agreement, NDA) bedarf. Die Informationen in diesem Dokument sind daher als nicht vertraulich einzustufen. Detailliertere Informationen und Dokumentationen sind nach Abschluss eines NDAs erhältlich und können über ein Online-Portal auf www.whistic.com abgerufen werden. Wenden Sie sich bitte an den Vertrieb von Matterport, das Business Development oder das Customer Success Team, um hierfür eine Zugangsberechtigung zu erhalten.

Überblick über das Informationssicherheits- und Datenschutzprogramm von Matterport

Matterport unterhält ein offizielles Programm für Informationssicherheit und Datenschutz. Dessen Eckpunkte sind wie folgt:

- Eine dokumentierte Informationssicherheitsrichtlinie, die administrative, technische und physikalische Kontrollen beschreibt, die bei Matterport implementiert wurden.
- Selbstbewertungen zur Einhaltung der Vorschriften und Nachweise, die nach Abschluss eines NDAs verfügbar sind.
- Jährlich durchgeführte Schwachstellen- und Penetrationstests von Drittanbietern - Berichte sind unter NDA verfügbar.
- DSGVO-Konformität
- Selbstzertifizierung gemäß EU-US und Swiss-US Datenschutzschild: https://www.privacyshield.gov/participant?id=a2zt00000008RnWAAU&status=Active
- Beauftragter Mitarbeiter, der für Informationssicherheit und Datenschutz zuständig ist.

Personal

- Alle Mitarbeiter und Auftragnehmer von Matterport unterliegen einem Background-Check bei der Einstellung oder zu Beginn eines Auftragnehmerverhältnisses.
- Die Mitarbeiter sind verpflichtet, zu bestätigen, dass sie das Mitarbeiterhandbuch und den Verhaltenskodex gelesen haben.
- Der Zugang zu den Räumlichkeiten von Matterport wird durch Keycards gesichert und ist videoüberwacht. Für geschützte Bereiche sind zusätzliche Kontrollen vorhanden. Beachten Sie, dass der Zugriff auf das Rechenzentrum von Amazon Web Services

(AWS) verwaltet wird und dass weder Produktivsysteme noch Produktionsdaten in den eigenen und kontrollierten Einrichtungen von Matterport verarbeitet oder gespeichert werden.
- Im Falle von Kündigungen erfolgt ein formalisierter Offboarding-Prozess unter der Aufsicht der IT- und Personalabteilung.
- Unternehmensweite Schulungen zu Informationssicherheit und Datenschutz werden zu Beginn des Arbeitsverhältnisses sowie jährlich durchgeführt.

Matterport Infrastruktur

Alle Matterport-Anwendungen werden von Amazon Web Services (AWS) gehostet und basieren auf einer gemeinsamen Infrastruktur / mandantenfähigen Architektur.

Im Folgenden erhalten Sie einen Überblick über die Produktionsinfrastruktur von Matterport:

- Die Anwendungen werden in der AWS us-east-1 Region in Virginia, USA, gehostet.
- Der Zugriff auf die Produktivsysteme erfolgt über Bastion-Hosts und wird von AWS IAM mit sicheren Passwörtern, MFA-Token und Okta Einmalanmeldungen (Single Sign-Ons, SSOs) verwaltet. Rollenerweiterungen werden verwendet, wenn temporär erweiterte Benutzerrechte erforderlich sind.
- API-Schlüssel und SSH-Schlüssel werden über eine Secrets-Management Plattform verwaltet.
- AWS Root Accounts sind durch Hardware-MFA-Schlüssel geschützt, die physikalisch in einem Safe mit eingeschränktem Zugriff gesichert sind.
- Alle ruhenden Daten werden mit AES-256 verschlüsselt, wobei AWS KMS für die Schlüsselverwaltung verwendet wird.
- Alle Daten, die im öffentlichen Internet übertragen werden, sind mit HTTPS/TLS 1.2 verschlüsselt.
- Die Mitarbeiter von Matterport erhalten nur dann Zugang zu Produktivsystemen, wenn dies für die Ausübung ihrer Tätigkeit erforderlich ist, und nur dann, wenn der Zugang von der Geschäftsleitung genehmigt wurde.
- Alle AWS-API-Aufrufe und alle AWS-Konsolen-/CLI-Aktivitäten werden über AWS Cloud Trail protokolliert.
- Application Audits und Fehlerprotokolle werden 90 Tage lang in einem Protokollverwaltungsdienst gepflegt.
- Die AWS-Infrastruktur wird mit AWS Guard Duty und Cloud Health auf Schwachstellen und verdächtige Aktivitäten überwacht.
- Datenbanken werden täglich mithilfe von in AWS RDS integrierten Snapshots gesichert und in Amazon S3 gespeichert. Alle Backups sind verschlüsselt. Backups erfolgen alle 24 Stunden und werden für 7 Tage aufbewahrt.
- Die Daten werden in AWS S3 gespeichert, das 99,999999999 %ige (11-9's) Beständigkeit bietet.
- Die Leistung und Betriebsverfügbarkeit der Infrastruktur wird mit Datadog (umgebungsintern) und Site24x7 (umgebungsextern) überwacht.

- Matterport strebt eine Verfügbarkeit von 99,9 % oder mehr über alle produktiven Dienstleistungen an und bietet einen Wiederherstellungspunkt (RPO) von 24 Stunden sowie eine Wiederherstellungszeit (RTO) innerhalb von 4 Stunden.

AWS verfügt über umfassende Sicherheitskontrollen und mehrere Compliance-Zertifizierungen. Diese können hier eingesehen werden: https://aws.amazon.com/security/

Matterport Cloud-Sicherheit

Matterport Cloud (unter https://my.matterport.com) authentifiziert Benutzer mittels Benutzernamen und Passwörtern. Multi-Faktor-Authentisierung (MFA) und Single Sign-On (SSO) werden derzeit nicht unterstützt, werden aber für eine zukünftige Produktfreigabe in Betracht gezogen.

Matterport-Benutzer haben entweder eine Administrator- oder eine reguläre ("Collaborator") Benutzerrolle. Die Funktionalität der Benutzerrollen geht jedoch über den Rahmen dieses Dokuments hinaus und ist in der Online-Benutzerdokumentation von Matterport unter https://support.matterport.com/hc/en-us/articles/115004080628-Learn-about-Collaborators beschrieben.

Space Access Control

3D-Räume und zugehörige Assets, die auf der Matterport Cloud-Plattform erstellt wurden, verfügen über ein einfaches öffentliches/privates Zugangskontrollmodell wie nachfolgend beschrieben:

- Alle Assets, die zu einem Raum gehören, sind standardmäßig privat und können nur von autorisierten Benutzern innerhalb der Matterport Cloud aufgerufen werden.
- Wenn ein Bereich nicht auf 'öffentlich' gesetzt ist, ist er nur für 1) Mitarbeiter zugänglich, denen der Zugriff auf das Modell gewährt wurde, oder 2) Kontoadministratoren in Ihrem Konto, 3) Mitarbeiter von Matterport, wenn nötig.
- Wenn ein Raum auf 'öffentlich' gesetzt ist, können Benutzer mit entsprechendem URL-Link darauf zugreifen.
- Der Zugriff auf einen Raum wird protokolliert und mit mindestens der Quell-IP-Adresse und dem Zeitstempel versehen, jedoch sind diese Protokolle unter normalen Umständen nur den Mitarbeitern von Matterport zugänglich.

Matterport Sicherheit FAQs - Häufig gestellte Fragen zur Sicherheit

Zusätzlich zu den in den vorangegangenen Abschnitten beschriebenen Informationen enthält die folgende Tabelle Antworten auf häufig gestellte Fragen zur Informationssicherheit und zum Datenschutz bei Matterport:

Fragen	Antwort
Wo befindet sich die Infrastruktur von Matterport?	Amazon Web Services us-east-1 Region in Virginia, USA.
Können Kundendaten in einem anderen Land oder einer anderen AWS-Region gespeichert werden?	Nein
Kann die Matterport Cloud im Kunden-eigenen Rechenzentrum gehostet werden?	Nein - Matterport wird als SaaS bereitgestellt.
Kann Matterport Cloud auf AWS GovCloud gehostet werden, um FedRAMP, NIST SP 800 und andere von der US-Regierung vorgeschriebene Standards für Controlled Unclassified Information (CUI) zu erfüllen?	Nein. AWS-Hosting ist nur in einer Nicht-GovCloud-Region verfügbar.
Wie ist der Technologie-Stack aufgebaut?	Linux, Python, Django, WebGL, Javascript/React, C++, Postgres, Kubernetes.
Verwendet Matterport ein CDN?	Ja, Fastly (www.fastly.com)
Werden sowohl öffentliche als auch private Räume im Fastly CDN zwischengespeichert?	Ja
Können Kunden steuern, in welchen Ländern ihre Räume zwischengespeichert werden?	Nein, das CDN ist jedoch nicht vorinstalliert, sodass Modelldaten nur am geografisch nächsten Fastly-Präsenzpunkt (POP) zwischengespeichert werden.
Gibt es Einschränkungen bei der Skalierbarkeit der Raum-(3D-Modell)-Verteilung?	Nein, es gibt keine praktischen Obergrenzen, jedoch können vertragliche und "fair-use" Nutzungsgrenzen gelten.
Hat jeder Kunde eine eigene, physikalisch getrennte Umgebung?	Nein, die Matterport Cloud ist eine gemeinsame, mandantenfähige Umgebung, die logisch getrennt ist.
Wie werden Produktivsysteme getrennt und isoliert?	Die Isolierung der Produktivsysteme erfolgt über AWS VPCs, der öffentliche Internetzugang wird durch NAT-Gateways und AWS Security Groups (Firewalls) gesteuert. Logische Funktionen werden in separaten VPCs bereitgestellt und jegliche Kerninfrastrukturkomponenten haben keine öffentlichen IP-Adressen. Öffentliche IP-Adressen werden nur den AWS ELBs

	zugewiesen.
Ist eine DMZ zur Trennung von Produktivsystemen implementiert?	Die Nutzung einer AWS VPC-basierten Infrastruktur erspart die Notwendigkeit einer traditionellen demilitarisierte Zone (DMZ).
Wer kann auf die Produktivsysteme von Matterport zugreifen?	Nur Matterport-Mitarbeiter mit erweiterten Berechtigungen, die von der Geschäftsleitung genehmigt wurden, haben Zugang zur Umgebung.
Ist Matterport ISO 27001 zertifiziert?	Nein. Obwohl formelle Audits nicht durchgeführt wurden, folgt Matterport vielen der ISO 27001 Anforderungen.
Kann ein Kunde ein Vor-Ort-Audit der Produktivinfrastruktur von Matterport durchführen?	Nein. Die gesamte Infrastruktur befindet sich in den Rechenzentren von Amazon Web Services und Amazon erlaubt keine Besuche oder Audits vor Ort.
Hat Matterport eine Informationssicherheitsrichtlinie?	Ja. Sie ist nach Abschluss eines NDA verfügbar.
Werden Verschlüsselungstechnologien verwendet?	Ja, ruhende Daten werden AES-256 mit AWS KMS für die Schlüsselverwaltung verschlüsselt, mit einer automatisierten einjährigen Rotationsperiode. Alle bewegten Daten, die im öffentlichen Internet übertragen werden, sind mit HTTPS mit TLS 1.2 verschlüsselt.
Entsprechen die Verschlüsselungswerkzeuge den FIPS 140-2-Standards?	Nein. FIPS 140-2-Endpunkte sind nur in der AWS GovCloud verfügbar, die derzeit nicht unterstützt wird.
Hat Showcase Javascript Zugriff auf die Host-Webseite?	Nein. Ein Showcase Modell ist in einem Iframe eingebunden und hat eine von der Host-Webseite separate Domain.
Unterstützt Matterport Cloud SSO / SAML 2.0 / ADFS / Okta etc.?	Nein, SSO wird nicht unterstützt.
Erzwingt Matterport Cloud starke Passwörter?	Ja - Passwörter müssen mindestens 8 Zeichen lang sein und drei der folgenden Komponenten enthalten: Großbuchstaben, Kleinbuchstaben, Zahlen und Symbole.
Lässt Matterport Schwachstellen-/Penetrationstests von Drittanbietern	Ja, es werden jährliche Tests durchgeführt - die Ergebnisse sind nach Unterzeichnung

durchführen?	eines NDAs verfügbar.
Wie schützt Matterport seine Umgebung vor DDoS-Angriffen?	Die gesamte Web-Infrastruktur von Matterport befindet sich hinter dem Fastly CDN, das alle Anfragen verwaltet und so die Infrastruktur vor DDoS-Angriffen schützt.
Werden Protokolle gepflegt?	Es werden Protokolle für alle AWS-internen Aktivitäten sowie alle Zugriffe auf Matterport-Anwendungen und -Räume gepflegt, sind aber in der Regel für Kunden nicht einsehbar. Die Protokolle werden 90 Tage lang verwaltet.
Gibt es einen formalen Change-Management Prozess?	Alle Software- und Infrastrukturänderungen werden mit Jira verwaltet und erfordern mehrere Genehmigungsstufen.
Wie werden Betriebssystem- und Patch-Updates durchgeführt und wie oft?	Produktivanwendungen werden mit Docker-Containern bereitgestellt, deren Basis-Images nachts mit den jeweils neuesten Betriebssystem-Updates neu erstellt werden. Infolgedessen werden Betriebssystem-Updates mit jedem Anwendungsrelease bereitgestellt, typischerweise alle 4 Wochen. Notfall-Patches für identifizierte Sicherheitsschwachstellen und Stabilitätsprobleme werden innerhalb von 24 Stunden bereitgestellt.
Werden Antiviren- und Anti-Malware-Produkte verwendet?	Antiviren- und Anti-Malware-Produkte werden auf Büro-/Firmen-PCs eingesetzt, aber nicht auf Linux-basierter Produktionsinfrastrukturen, da das Risiko von Viren auf Linux-Systemen gering ist.
Hat Matterport ein formales Datenschutzprogramm?	Ja, Matterport unterhält ein formales Programm und erfüllt die DSGVO und alle anderen geltenden US-amerikanischen und internationalen Vorschriften. Dokumentierte Nachweise sind unter NDA verfügbar.
Gibt es eine formelle Datenschutzerklärung?	Ja, unter https://matterport.com/legal/privacy-policy/
Gibt es eine Richtlinie zur Reaktion auf Vorfälle?	Ja - Diese Richtlinie kann unter NDA eingesehen werden.