fullstory

GUIDE

Datenschutz und Sicherheit

Alles was du über Datenschutz und Sicherheit bei FullStory wissen musst

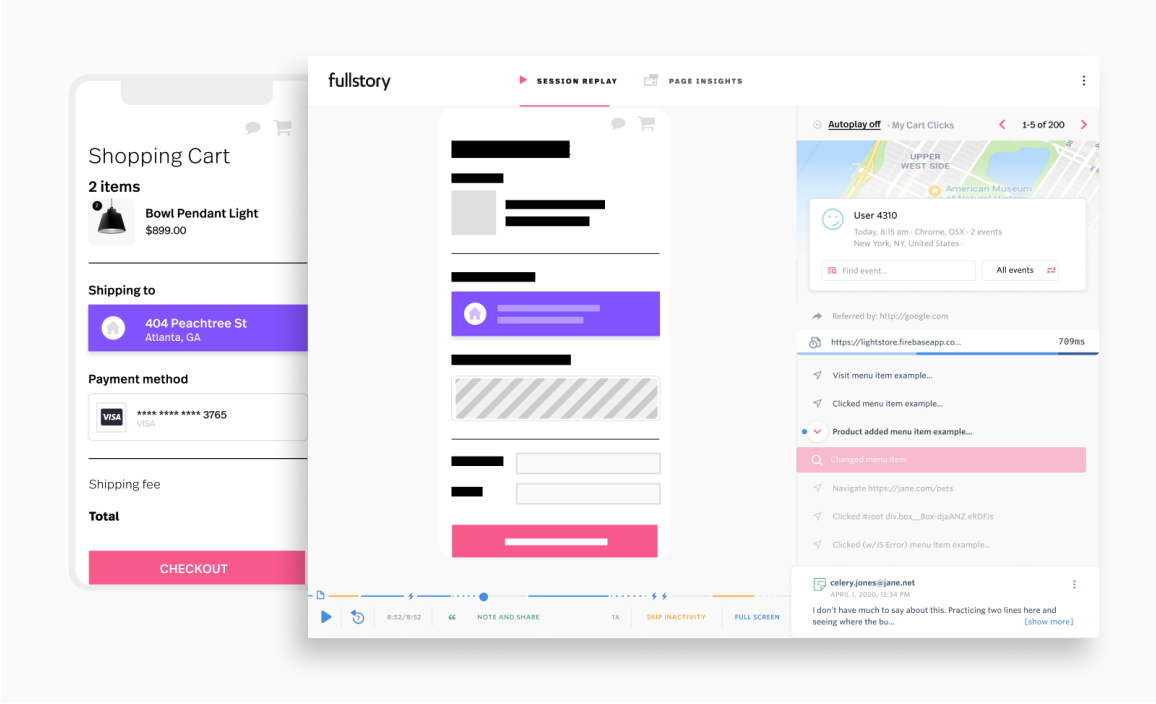
Die Digital Experience Intelligence-Plattform von FullStory ermöglicht es Unternehmen, die digitale Customer Experience über Websites und Apps hinweg kontinuierlich zu verbessern, ohne dabei die Privatsphäre der Endnutzer:innen zu verletzen.

Den Kern der Plattform bildet ein leistungsstarker Analytics-Engine, der digitale Interaktionen mit jenen Metriken zusammenbringt, die für Unternehmen am wichtigsten sind. FullStory zeigt die besten Möglichkeiten zur Optimierung der digitalen Experience proaktiv auf und ermöglicht es den Teams, Probleme zu verstehen, Korrekturen zu priorisieren, Bugs zu beheben und die Auswirkungen dieser Anpassungen zu messen.

Unser in der Branche führender Ansatz zur Datenerfassung, “Private by Default”, maskiert den gesamten Text auf dem Gerät der Endnutzer:innen, sodass er die Server von FullStory gar nicht erst erreicht. Diese einzigartige Verschlüsselungstechnologie bietet genügend Insights, um dabei zu helfen, die digitale Experience zu verbessern und schützt gleichzeitig vor ungewollten Datenlecks und Compliance-Verstößen.

DATENSCHUTZ: WIE FULLSTORY DATEN ERFASST

Private by Default: Ein in der Branche führender Ansatz

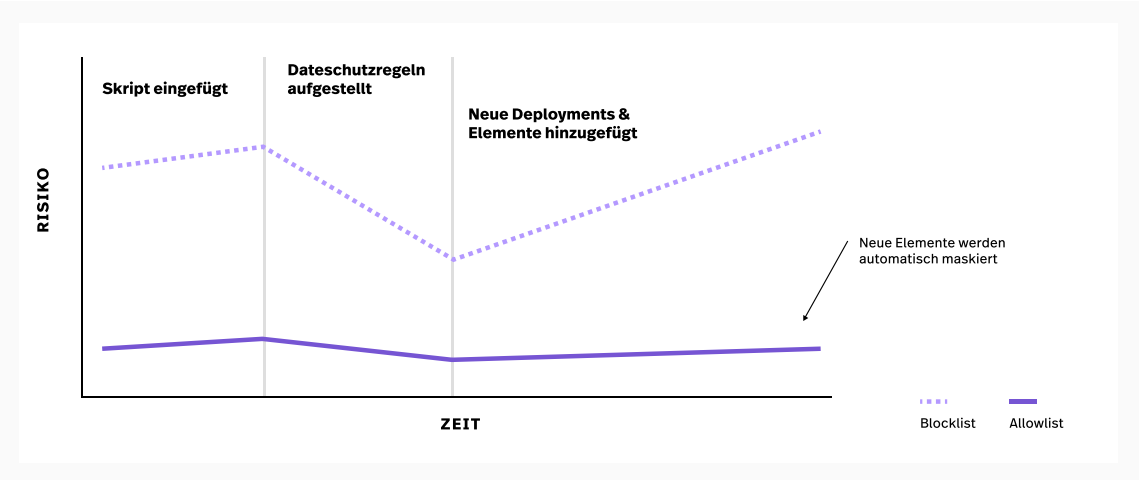


Private by Default ist FullStorys innovativer Ansatz zur Datenerfassung. Diese Funktionsweise ist ein Kernstück von FullStorys Produkt und minimiert das Risiko der unbeabsichtigten Speicherung sensibler Daten. Wenn diese Funktion aktiviert ist, werden alle Textelemente an der Quelle unkenntlich gemacht – und zwar unabhängig davon, wo auf der Seite sie auftauchen. Die Informationen verlassen niemals den Browser oder das Gerät der Kund:innen und werden somit auch nicht auf die Server von FullStory übertragen.

Dieser datenschutzfreundliche Ansatz wird durch eine unternehmenseigene Verschlüsselungstechnologie ermöglicht, die im Wesentlichen alle Elemente deiner Website während des Session Replays in ein Wireframe verwandelt. Der genaue Inhalt der Elemente wird dabei nicht erfasst – außer, du hast Elemente zuvor auf eine gesonderte Allowlist gesetzt. Die Wireframes ermöglichen es dir, wertvolle Nutzerinteraktionen zu sehen – das heißt, selbst wenn du kein einziges Element auf die Allowlist setzt, kannst du trotzdem tiefgehende Einblicke in die User Experience erhalten.

Bei anderen Analytics-Lösungen können unzureichende Aufzeichnungsregeln für die Aufzeichnung dazu führen, dass sensible Daten gesammelt werden. Private by Default bedeutet, dass du FullStory unmittelbar nach der Installation nutzen kannst, während das Risiko, dass dabei unerwünschte Endnutzerdaten erfasst werden, minimal bleibt.

Viele Lösungen machen standardmäßig einige Elemente oder Felder unkenntlich, verlangen dann aber, dass du die restlichen Elemente, die möglicherweise sensible Daten enthalten, manuell auswählst. Dies macht die Umsetzung nicht nur schwieriger und riskanter, sondern verlangsamt auch die Arbeit der Teams, da es bei jedem neuen Update oder einer Veränderung an der Seite sicherstellen muss, dass alle notwendigen Elemente maskiert sind. Dank Private by Default kannst du mit der Aktualisierung der Datenschutzeinstellungen in FullStory bis nach Deployment warten. Das bedeutet, dass dein gesamtes Produktteam schnell und unbesorgt ausliefern kann, ohne ständig kontrollieren zu müssen, ob alle Seiten-Elemente, die von der Datenerfassung ausgeschlossen werden müssen, auch wirklich ausgewählt sind. **Erfahren hier mehr →**



Erfassungsregeln: Sammle nur das, was du brauchst

Mit FullStory kontrollierst du den wichtigsten Sicherheitsaspekt deines Unternehmens: die Entscheidung darüber, welche Daten überhaupt erfasst werden sollen. Private by Default maskiert den gesamten Text bereits an der Quelle. Es kann jedoch Elemente geben, die du dennoch kenntlich machen oder aber völlig von der Erfassung ausschließen möchtest, je nach Inhalt und/oder Zustimmung deiner Nutzer:innen.

FullStory bietet zwei unterschiedliche Ansätze für die Handhabung der Regeln zur Erfassung von Elementen. Der erste involviert die Definierung der relevanten Paremeter in den CSS-Klassen der Web-Elemente, was auch als 'Code First' bezeichnet wird.

Der zweite Ansatz zur Handhabung der Erfassungsregeln von Elementen ist die entsprechende FullStory-Benutzeroberfläche, die sich unter Einstellungen > Datenschutz befindet. Durch die Möglichkeit, Erfassungsregeln direkt in der App zu steuern, kannst du schnell auf notwendige Änderungen reagieren, ohne auf Entwickler-Unterstützung warten zu müssen – eine Option, die nicht von allen Digital Experience-Lösungen angeboten wird.

Ausschließen, maskieren oder demaskieren

Ausschluss von der Erfassung (“Exclusion”) ist die strikteste Form der Datenerfassung. FullStory schließt automatisch sensible Felder wie Passwort- oder Kreditkarteninformationen aus. Da die Regeln für ausgeschlossene Elemente so konzipiert sind, dass sie Maskierungsregeln übertrumpfen, kannst du zusätzliche, benutzerdefinierte Ausschlüsse festlegen, um sicherzustellen, dass bestimmte Daten vollständig blockiert werden – nicht nur von der Wiedergabe, sondern auch von Event-Streams, Suche und Segmentierung. Ausgeschlossene Elemente erfassenn keinerlei Details über das Element, was bedeutet, dass keine Rückschlüsse auf den Nutzer/die Nutzerin oder das Element gezogen werden können.
Erfahre mehr über das Ausschließen von Elementen bei FullStory →

Bei maskierten Elementen verlässt kein Text das Gerät des Endnutzers oder der Endnutzerin, es werden jedoch bestimmte strukturelle Informationen erfasst, darunter Interaktionsdaten und die Größe, Position und Farbe des Elements. Das bedeutet, dass das Element in einer Session Replay als Wireframe dargestellt und für die Analyse ausgewählt werden kann. Dies ist der Standardstatus für alle Textelemente, die Private by Default verwenden. So erhältst du genau die Informationen, die du braucht, um die User Experience zu verstehen, ohne dabei sensible Daten zu erfassen. Mit unmaskierten Elementen kannst du deine Website oder App genau so sehen, wie der Nutzer oder die Nutzerin sie gesehen hat. Das ist eine sehr gute Einstellung für alle sicheren Elemente und gewährleistet, dass deine Teams den vollständigen Kontext haben, wenn sie sich einem Problem nähern. Es gibt einfache Ansätze, um große Teile einer Website mit nur wenigen CSS-Selektoren zu demaskieren.

Form Privacy

Persönliche Informationen finden sich am häufigsten in Eingabefeldern auf einer Website. Form Privacy hilft, die Privatsphäre der Nutzer:innen proaktiv zu schützen, indem es FullStory daran hindert, potenziell sensible Nutzerdaten zu protokollieren, die in Eingabefeldern auf deiner Website eingegeben werden.

Form Privacy aktiviert eine Reihe von Erfassungsregeln, die Formular-Elemente maskieren oder ausschließen. Du kannst die Feinheiten der in Formularen erfassten Daten kontrollieren und bestimmte Elemente, die kein Datenschutzrisiko darstellen, demaskieren, indem du Ausnahmen von den Standardregeln festlegst. Dieser Ansatz ermöglicht es, alle weiteren Formular-Elemente standardmäßig privat zu halten, inklusive derer, die in Zukunft noch hinzugefügt werden.
Erfahre hier mehr über Form Privacy →

Vorschaumodus

FullStory enthält den Vorschaumodus, eine Funktion, die es dir ermöglicht, Änderungen an deinen Erfassungsregeln lokal nur in deinen eigenen Sessions durchzuführen. So können Änderungen überprüft werden, bevor sie für die Produktion freigegeben werden, ohne mehrere Umgebungen einrichten zu müssen.
Erfahre mehr über den Vorschaumodus →

Zustimmungsbasierte Erfassung

Die FS.consent API von FullStory bietet dir die Möglichkeit – basierend auf der ausdrücklichen Zustimmung der Nutzer:innen, die normalerweise mit deinem Cookie oder DSGVO-Banner einhergeht – Teile deiner Website oder App selektiv auszuschließen, zu maskieren oder zu demaskieren. So kommst du den Datenschutzwünschen deiner Kund:innen nach und hältst dich gleichzeitig an die Datenschutzbestimmungen.
Erfahre mehr über die Aktivierung von FS.consent →

FullStory, die DSGVO und der CCPA

Die Datenschutzrechte deiner Nutzer:innen sind durch Gesetze wie die Datenschutz-Grundverordnung (DSGVO; englisch GDPR) in Europa und den California Consumer Privacy Act (CCPA) in Kalifornien geschützt. FullStory steht uneingeschränkt für die Einhaltung dieser Rechte ein und bietet eine Reihe von Tools für das Einwilligungsmanagement, mit denen du die Einhaltung der Vorschriften sicherstellen und die Daten deiner Nutzer:innen bei Bedarf kontrollieren und löschen kannst. Mehr Informationen über die **DSGVO** und den **CCPA**.

Rechtliche Dokumente von FullStory

Datenschutzrichtlinie →
Acceptable Use-Richtlinie →
Allgemeine Geschäftsbedingungen →
Vereinbarung zur Datenverarbeitung →

Bescheinigungen und Zertifizierungen

FullStory übertrifft die strengen internationalen Sicherheitsstandards in Bezug auf Vertraulichkeit, Integrität und Verfügbarkeit. Viele SaaS-Anbieter verlassen sich auf die Zertifizierungen ihrer Cloud-Anbieter, was nichts über ihre internen Sicherheitsstandards und -praktiken aussagt. FullStory verfügt über eine SOC 2 Typ II-Bescheinigung, einen SOC 3-Bericht, ist ISO 27001-zertifiziert und speichert Daten sicher mit der **Google Cloud Plattform**. FullStory hält sich auch an die Grundsätze des EU-U.S. und Swiss U.S. Privacy Shield Framework und ist entsprechend zertifiziert.

FullStory Anwendungssicherheit

FullStory bietet Nutzer:innen und Administrator:innen die Möglichkeit zu kontrollieren, wie ihre Daten erfasst und abgerufen werden. Die oben beschriebenen Datenschutzkontrollen – die Möglichkeit, Elemente auszuschließen, zu maskieren und zu demaskieren – sind ein wesentlicher Bestandteil sicherer Analytics.

Für FullStory ist Sicherheit eine Kernkomponente der Analytics-Plattform. Das Programm zur Anwendungssicherheit von FullStory stellt sicher, dass alle kundenorientierten Bereiche der Anwendungsoberflächen – einschließlich unserer Web-App, APIs und Integrationen – zuverlässig gegen Sicherheitslücken geschützt sind.

Der Client-Code verwendet mehrere Techniken, um sicherzustellen, dass die Nutzung der FullStory-Anwendung sicher ist und die Anfragen authentisch sind, darunter:

- IFRAME-Sandboxing
- XSS- und CSRF-Schutz
- Signierte und verschlüsselte Benutzerauthentifizierungs-Cookies
- Deaktivierung bestehender Sessions bei Passwortwechsel/Benutzerdeaktivierung

Ort der Datenspeicherung

US-Rechenzentrum
Die FullStory-Produktionsdaten werden in den Rechenzentren der Google Cloud Platform verarbeitet und gespeichert. Alle Google-Rechenzentren, die FullStory-Daten verarbeiten, befinden sich in den USA, zusätzlich zur Google Cloud-Region europe-west3 (Frankfurt). Die Rechenzentren von Google sind weltweit für ihre hochmodernen Sicherheitssysteme bekannt.

EU-Rechenzentrum
Kunden können eine Version von FullStory nutzen, bei der alle Endnutzerdaten ausschließlich in der EU gespeichert sind.

Unser EU Data Residency-Angebot nutzt die Region europe-west3 (Frankfurt) von Google Cloud. Deutschland ist aufgrund seines guten Rufs in Bezug auf den Datenschutz eine beliebte Wahl für Unternehmen, die ihre Daten in der EU speichern wollen.

Hinweis: Bei einigen Diensten, wie z. B. Google Cloud Storage, bietet GCP die Möglichkeit, Daten in einer bestimmten Region (z. B. europe-west3) oder in einer Konfiguration mit mehreren Regionen, die über die gesamte EU verteilt sind, zu speichern. In diesen Fällen entscheiden wir uns dafür, Daten nur in europe-west3 zu speichern.

Bearbeitung von FullStory-Kundenzahlungen

Der Zugriff auf jeden FullStory REST API Endpoint erfordert einen Zugangsschlüssel, der bei Bedarf von Kund:innen neu generiert werden kann.
Erfahre mehr über den API-Zugangsschlüssel →

Integrationen mit anderen Anwendungen erfordern alle einen Opt-in und authentifizieren sich über OAuth oder andere Tools, die von der Drittanwendung gefordert werden. Integrationen können jederzeit deaktiviert werden.

APIs und Integrationen

Bei FullStory verwenden wir Stripe – einen bewährten Level 1 PCI Service Provider – für die Zahlungsabwicklung. Wir nutzen die direkte Stripe-JavaScript-Integration, sodass die Kreditkarteninformationen direkt vom Browser an Stripe gesendet werden und zu keinem Zeitpunkt mit FullStory-Servern in Berührung kommen.
Erfahre mehr über die Sicherheitspraktiken von Stripe →

Sicherer Single Sign-On und Geräteüberprüfung

FullStory kann in die Single Sign-On (SSO) Lösung deines Unternehmens integriert werden, sodass sich Teammitglieder mit ihren SSO-Anmeldedaten bei FullStory anmelden können. Dadurch benötigen die Nutzer:innen keine separaten FullStory-Anmeldedaten mehr, nur die gewünschten Nutzer:innen haben Zugriff auf die Daten und du kannst für FullStory die gleichen Authentifizierungsrichtlinien anwenden wie für deine anderen Unternehmensanwendungen.

Die Timeouts für inaktive Sessions sind konfigurierbar, um sicherzustellen, dass keine vergessenen Sessions auf den Geräten der Mitarbeitenden offen bleiben. FullStory bietet auch die Möglichkeit, eine E-Mail-basierte Kontoverifizierung durchzuführen, wenn ein Nutzer oder eine Nutzerin von einem neuen Gerät aus auf FullStory zugreift.

Sicherheit geht nicht auf Kosten der Nutzerfreundlichkeit; FullStory bietet Just-in-Time (JIT) Provisioning, womit berechtigte neue Nutzer:innen automatisch freigeschaltet werden können, wenn sie sich zum ersten Mal über die SAML SSO-Anmeldeseite des Unternehmens anmelden.
Erfahre mehr über die Single Sign-On-Optionen von FullStory →

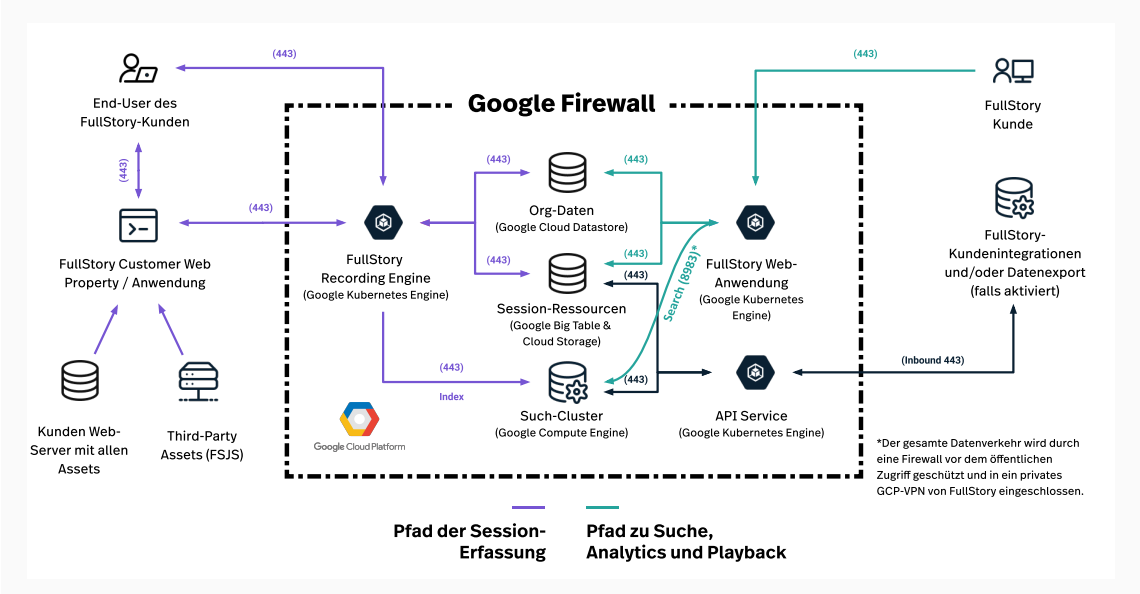
FullStory Systemsicherheit

Sicherheitsarchitektur

Wenn es um die Sicherheitsarchitektur von FullStory geht, betrachten wir vier Wege des Datenzugriffs

- Kundenzugriff auf die FullStory-Anwendung
- Erfassung von Endnutzerdaten durch den Kunden/die Kundin
- Erfassung der Webanwendungsressourcen (Bilder, CSS) des Kunden/der Kundin
- Integration und programmatischer API-Zugang des Kunden/der Kundin

Das folgende Diagramm zeigt, wie jede dieser Interaktionen mit der FullStory-Engine verknüpft ist:



Servers

Wie im obigen Diagramm zu sehen ist, wird fast die gesamte Infrastruktur von FullStory über Microservices implementiert, die innerhalb des Google Kubernetes Engine (GKE) laufen. Wöchentlich erstellt FullStory ein neues Base-Image aus der neuesten Version von Debian, das als Base-Image für alle Container verwendet wird.

Jeder Microservice kann vom zuständigen Team in Übereinstimmung mit unserem Software Development Lifecycle (siehe "Softwareentwicklung und -überwachung") unabhängig bereitgestellt werden. Die meisten Dienste werden mehrmals pro Woche aktualisiert; normalerweise ist kein laufender Container älter als eine Woche.

Es gibt Sicherheitsvorkehrungen, die gewährleisten, dass die laufende Software immer aktuell ist. Für den Fall, dass ein Dienst 28 Tage lang nicht neu ausgerollt wurde (und somit sein Base-Image auf die neueste Version aktualisiert wurde), erhält das Team, das ihn betreibt, Warnungen, dass seine Container veraltet sind. Darüber hinaus identifizieren Nessus-Scans alle Schwachstellen, die sofort behoben werden müssen, und senden entsprechende Warnungen.

Einige wenige Dienste benötigen einen dauerhaften Datenspeicher und werden auf virtuellen Maschinen im Google Compute Engine (GCE) ausgeführt. Diese VMs werden kontinuierlich ausgeführt, aber Patches (und Neustarts) mindestens einmal wöchentlich über einen Ansible-Auftrag eingespielt. Zusätzliche gehostete Dienste, wie z. B. Google Cloud Storage, sind umfassend geschützte Google Infrastruktur-as-a-Service-Plattformen.

Transport Layer Security

FullStorys Richtlinien sehen vor, dass alle TLS-Endpoints, auf die ausschließlich FullStory-Mitarbeiter:innen zugreifen, TLS 1.2+ und nur TLS-Chiffren des Profils "RESTRICTED" von Google unterstützen. Endpoints, auf die FullStory-Kund:innen zugreifen, unterstützen TLS 1.2+ und nur TLS-Chiffren im Google Profil "MODERN". **Erfahre mehr über die SSL-Richtlinien von Google →**

Datenspeicherung

Alle beständigen Daten werden im Ruhezustand mit AES-128 oder vergleichbaren Standards verschlüsselt. Dies wird von Google Cloud verwaltet, deren Sicherheitspraxis erfolgreich nach ISO 27001, SSAE-16, SOC 1, SOC 2 und SOC 3 zertifiziert wurde.

Aufbewahrung und Löschung von Daten

FullStory speichert die Daten verschlüsselt für die Dauer des Vertrages mit dem jeweiligen Kunden/der jeweiligen Kundin. Sobald die Daten ablaufen, werden sie aus den FullStory-Systemen gelöscht. Wenn ein Kunde oder eine Kundin die Löschung bestimmter Daten verlangt (im Rahmen einer Zugriffsanfrage gemäß DSGVO oder aus anderen Gründen), können die Daten selektiv mit einem granularen Ansatz gelöscht werden, wobei der Rest der aufgezeichneten Daten intakt bleibt. In einigen Fällen kann die Löschung eines breiteren Umfangs an Daten empfohlen werden, um die Privatsphäre der Endnutzer:innen und die Einhaltung der Kundenvorschriften zu schützen.
Erfahre mehr über die Löschung von Sitzungen →

Service-Level, Backups und Wiederherstellung

Die FullStory-Infrastruktur nutzt unterschiedliche, mehrschichtige Techniken um für eine optimale Zuverlässigkeit zu sorgen, einschließlich automatischer Skalierung, Lastausgleich, Task-Warteschlangen und rollierender Bereitstellungen. Die Daten von Kundenkonten, Organisationen und Konfigurationen werden täglich gesichert. Eine automatische Überprüfung des Backups wird ebenfalls täglich durchgeführt.

Aufgrund der sehr großen Menge an aufgezeichneten Kundendaten, die FullStory speichert, führen wir derzeit keine isolierten Point-in-Time-Backups durch. Wir verwenden jedoch hochredundante Datenspeicher und eine schnelle Wiederherstellungsinfrastruktur, was einen ungewollten Verlust von Daten aufgrund von Hardwareausfällen sehr unwahrscheinlich macht.

Softwareentwicklung und -überwachung

FullStory speichert Quellcode und Konfigurationsdateien in privaten GitHub-Repositories. Vertrauliche Informationen wie Authentifizierungsschlüssel im Klartextformat werden nicht im Repository gespeichert. Die Sicherheits- und Entwicklungsteams von FullStory führen Code-Reviews durch und wenden bei jedem Code Commit statische Code-Analyse-Tools an. Dabei wird sichergestellt, dass die Programmierungs-Konventionen und Stile von FullStory befolgt werden, außerdem wird auf mögliche Fehler oder Leistungsprobleme überprüft, damit der Code-Commit sich nur auf den vorgesehenen Zweck bezieht.

Sicherheitsüberprüfungen werden bei jedem Code-Commit für sicherheitsrelevante Module durchgeführt. Zu diesen Modulen gehören solche, die sich direkt auf Authentifizierung, Autorisierung, Zugriffskontrolle, Auditing und Verschlüsselung beziehen.

Alle Hauptkomponenten von integrierten Open-Source-Softwarebibliotheken und -Werkzeugen werden auf Robustheit, Stabilität, Leistung, Sicherheit und Wartbarkeit geprüft. Die Sicherheits- und Entwicklungsteams legen einen formalen Softwarefreigabeprozess fest und befolgen diesen.

Code Reviews und Produktionsfreigabe

Alle Änderungen am Quellcode von FullStory, die für Produktionssysteme bestimmt sind, werden vor dem Einsatz einer Codeprüfung durch einen qualifizierten technischen Mitarbeiter/eine qualifizierte technische Mitarbeiterin unterzogen, die eine Analyse der Sicherheit, der Leistung und des Potenzials für Datenmissbrauch umfasst.

Vor der Aktualisierung von Produktions-Services müssen alle, die an der aktualisierten Software-Version mitarbeiten, bestätigen, dass ihre Änderungen auf den Staging-Servern wie vorgesehen funktionieren. Dies wird durch Systeme gewährleistet, die die Zustimmung eines zweiten Entwicklers/einer zweiten Entwicklerin erfordern, der oder die den geplanten Einsatz überprüft hat.

FullStory Betriebssicherheit

Ausstattung der Mitarbeitenden

Die Computer der Mitarbeitenden verfügen über sichere Passwörter, verschlüsselte Festplatten, Firewalls und gegebenenfalls über eine Überwachung des ein- und ausgehenden Netzwerkverkehrs und entsprechende Warnmeldungen. Außer in isolierten Testumgebungen werden überhaupt keine Windows-Computer oder -Server verwendet. Ein großer und zunehmender Prozentsatz der Mitarbeitenden verwendet ausschließlich Chromebooks, um maximalen Schutz vor Schadsoftware sicherzustellen, einschließlich leistungsfähiger Sicherheitsmaßnahmen wie ein **Verified Boot**.

Zugang für Mitarbeitende

FullStory verfolgt das Least-Privilege-Prinzip, wenn es um das Schreiben von Software, die Diagnose und Lösung von Problemen und die Unterstützung von Kund:innen geht. Die Mitarbeitenden erhalten nur so viel Zugriff, wie sie für die jeweilige Aufgabe benötigen, und nicht mehr.

Wir verwenden die Google-Konto-Infrastruktur, um die Identität der Mitarbeiterkonten zu überprüfen und verlangen physische Sicherheitsschlüssel und/oder Zwei-Faktor-Authentifizierung für alle internen Anwendungen, ohne Ausnahme. Administrative Berechtigungen werden bei Bedarf festgelegt, alle administrativen Zugriffe werden protokolliert und lassen sich sowohl über traditionelle Webserverprotokolle als auch über FullStory selbst prüfen. Für SaaS-Drittanbieter verwenden wir Google als Identitätsprovider, um eine zentrale Zugriffskontrolle für alle Anwendungen zu ermöglichen, auf die Mitarbeitende im Rahmen ihrer Arbeit zugreifen.

HR-Prozesse

Background-Checks

Alle Mitarbeitenden werden vor ihrem Einstieg einem Background-Check unterzogen. Falls diese Background-Checks problematische Ergebnisse erzeugen, können die Folgen von einer Einschränkung der Sicherheitsrechte bis hin zum Widerruf von Stellenangeboten reichen.

Unsere Background-Checks umfassen je nach Region und Gesetzeslage:

- Strafrechtliche Überprüfung auf Bezirksebene (letzte 7 Jahre)
- Nationale Suche nach Straftätern
- Suche nach Sexualstraftätern
- SSN Rückverfolgung
- Global Watchlist Suche

Sobald der Kandidat/die Kandidatin sein/ihr Angebot unterschrieben hat, startet der/die Personalverantwortliche die Suche. Der Bericht wird von unserem Anbieter, Checkr, an FullStory zurückgesendet. Angebotsschreiben weisen darauf hin, dass sie von einem erfolgreichen Background-Check abhängig sind.

Wenn die Überprüfung nicht erfolgreich ist, untersuchen wir die Auffälligkeiten als Team und entscheiden über das weitere Vorgehen. Wenn es sich um etwas handelt, das die Fähigkeit der Person zur Ausübung ihrer Tätigkeit beeinträchtigt oder ein ethisches oder Sicherheitsrisiko darstellt, ziehen wir das Angebot zurück.

Sicherheitsschulung

Das Sicherheitsteam pflegt ein unternehmensweites, computerbasiertes Sicherheits-Schulungsprogramm, das mindestens einmal jährlich von allen FullStory-Mitarbeitenden durchlaufen wird. Das Programm umfasst Sicherheitsbewusstsein, Richtlinien, Prozesse und Übungen, um sicherzustellen, dass die Mitarbeitenden ausreichend informiert sind, um ihren Verpflichtungen nachzukommen. Zusätzlich wird vierteljährlich ein obligatorisches All-Hands-Meeting für alle Mitarbeitenden abgehalten, um das Sicherheitsbewusstsein zu stärken und zusätzliche relevante Themen zu behandeln.

Die Mitarbeitenden des Engineering-Teams erhalten zusätzlich eine vierteljährliche Pflichtschulung, die sich speziell auf Software-Sicherheitsthemen konzentriert. Diese Schulung findet im Abstand von sechs Wochen zu der unternehmensweiten Schulung statt, um zu gewährleisten, dass die Sicherheit kontinuierlich ausgebaut wird.

Das Sicherheitsteam erstellt und vermittelt computerbasierte Schulungen zu verschiedenen Sicherheitsthemen. Die Hauptverantwortlichen für die Aufrechterhaltung der Sicherheit bei FullStory – darunter das Sicherheitsteam sowie wichtige Mitarbeitende aus dem Bereich Engineering/Operations – nehmen an weiteren technischen Fortbildungen teil.

Offboarding

Im Falle einer Kündigung oder eines Austritts eines Mitarbeitenden koordiniert das Sicherheitsteam mit der Personalabteilung einen standardisierten Offboarding-Prozess, der sicherstellt, dass alle Konten, Anmeldeinformationen und Zugriffe des austretenden Mitarbeitenden zuverlässig deaktiviert werden.

Physische Sicherheit bei FullStory

Sicherheit im Büro

Der Zugang zu den FullStory-Büros erfolgt über ein elektronisches Kontrollsystem, das einen identitätsgesteuerten Zugang, eine programmierbare Kontrolle der Zugangszeiten und eine Überprüfung der Nutzung ermöglicht. Alle Türen bleiben unter normalen Betriebsbedingungen stets verschlossen, mit Ausnahme der Eingangstür, an der während der normalen Geschäftszeiten Wachpersonal anwesend ist. Das Sicherheitsteam kann die Genehmigung erteilen, die Türen für kurze Zeiträume zu öffnen, sollte das aufgrund besonderer Umstände nötig sein. Internetbasierte Sicherheitskameras zeichnen mit Zeitstempel versehene Videos vom Betreten und Verlassen auf; diese Videos werden auf einem externen Server gespeichert.

Sicherheit im Rechenzentrum

Die FullStory-Produktionsdaten werden in den renommierten Google Cloud Platform-Rechenzentren verarbeitet und gespeichert, die sich in den USA sowie in der Google Cloud-Region Europa-West3 (Frankfurt) befinden. In den Rechenzentren werden modernste und mehrschichtige Zugangs-, Alarmierungs- und Kontrollmaßnahmen verwendet. Dazu gehören:

- Umzäunung
- Zugangssperren für Fahrzeuge
- Individuell gestaltete elektronische Zugangskarten
- Biometrische Kontrollen
- Lasergesteuerte Einbruchssicherung
- Ständige Überwachung durch externe und interne Sicherheitskameras
- 24x7 geschultes Sicherheitspersonal

Erfahre mehr über die zuverlässige Infrastruktur und die physischen Sicherheitsmaßnahmen von GCP →

IT-Sicherheit

Büro-Netzwerk

Der Zugang der FullStory-Mitarbeitenden zu den Informationsressourcen erfolgt zu 100 Prozent remote. Es gibt kein FullStory-eigenes Rechenzentrum oder FullStory-Netzwerk. Die Büros von FullStory bieten einen Arbeitsplatz für die Mitarbeitenden sowie eine Internetverbindung. Der Internetzugang wird den Geräten über kabelgebundenes Ethernet und WPA2-WLAN zur Verfügung gestellt.

Die Netzwerk-Switches und -Router befinden sich in einem verschlossenen Netzwerkschrank, der nur dem Sicherheitsteam zugänglich ist. FullStory-Führungskräfte und das Sicherheitsteam können Personen im Einzelfall und bei Bedarf Zugang zum Netzwerkschrank gewähren. Außerdem blockiert eine Netzwerk-Firewall den gesamten über das WAN laufenden Verkehr. WAN-zugängliche Netzwerkdienste werden nicht in der Büroumgebung gehostet.

Zugriffsverwaltung

FullStory hält sich an das Least-Privilege-Prinzip, und jede Aktion, die von einem Benutzerkonto ausgeht, unterliegt einer Zugriffskontrollprüfung.

Rollenbasierte Zugriffskontrolle

FullStory wendet ein rollenbasiertes Zugriffskontrollmodell (RBAC) an, das von Google bereitgestellte Einrichtungen wie Organisationseinheiten, Nutzerkonten, Nutzergruppen und Freigabekontrollen nutzt.

Webbrowser und Erweiterungen

FullStory kann die Verwendung eines bestimmten Webbrowsers für die reguläre geschäftliche Nutzung und für den Zugriff auf Unternehmensdaten wie E-Mail verlangen. Für bestimmte Rollen – wie z.B. Softwareentwicklung und Webdesign – können bestimmte Tätigkeiten die Verwendung einer Vielzahl von Browsern erforderlich machen und diese Rollen sind im Bedarfsfall dazu berechtigt, dies zu tun.

Jeder Browser, der für den Zugriff auf Unternehmensdaten wie E-Mail zugelassen ist, unterliegt einer Whitelist-basierten Beschränkung, was die Installation von Browser-Erweiterungen angeht.

Administrativer Zugang

Der Zugang zu administrativen Vorgängen ist streng auf die Mitglieder des Sicherheitsteams beschränkt und kann in Abhängigkeit von der Betriebszugehörigkeit und entsprechend des Least-Privilege-Prinzips noch weiter eingeschränkt werden.

Regelmäßige Überprüfung

Die Zugangskontrollrichtlinien werden vierteljährlich überprüft, mit dem Ziel, den Zugang wo immer möglich zu reduzieren oder zu verfeinern. Änderungen in der Tätigkeit des Personals lösen ebenfalls eine Überprüfung des Zugangs aus.

Krisen- und Incident-Management

Sicherheits-Vorkommnisse erkennen und richtig reagieren

FullStory hat ein Programm zur verantwortungsvollen Offenlegung von Sicherheitslücken. Dieses Programm wird von demselben Drittanbieter verwaltet, der auch unser Bug Bounty-Programm verwaltet und unseren jährlichen Penetrationstest durchführt.

Geschäftsfortführung und Wiederherstellung im Krisenfall

Die in der Google Cloud Platform (GCP) gehosteten FullStory-Dienste sind so konfiguriert, dass sie langfristigen Ausfällen in einer GCP-Verfügbarkeitszone standhalten. Kontrollen wie automatische Replikation oder automatisierte Datenwiederherstellungsprozesse können verwendet werden, um dieses gewünschte Verfügbarkeitsniveau zu erreichen.

In unserem Büronetzwerk befinden sich keine kritischen Server. Für den Fall, dass unser Büro plötzlich nicht mehr erreichbar ist, suchen sich die Mitarbeitenden alternative remote Arbeitsplätze und koordinieren gegebenenfalls die physische Zusammenarbeit, um die Produktivität zu optimieren.

Sollte eine Krise eintreten – sei es ein Brand, ein Unwetter, eine politische Katastrophe oder eine Pandemie – durch die FullStorys Büros betroffen sind, werden die lokalen Behörden um Hilfe gebeten, um die Sicherheit unserer Mitarbeitenden zu gewährleisten.

Sicherheitsvorteile bei der Verwendung von FullStory

FullStory kann nicht nur deine digitale Experience verbessern, sondern auch deine eigenen Sicherheitspraktiken erheblich verbessern.

Überwachung und Überprüfung verdächtiger Aktivitäten

Kund:innen sind sich einig, dass FullStory eine zusätzliche und neuartige Form der Anwendungssicherheit bietet. Mit einer vollständigen Erfassung der Nutzerinteraktionen und einer Reproduktion dieser Aktionen in Form von Session Replay, haben Unternehmen aus allen Branchen FullStory als sehr nützlich empfunden, wenn es um rechtliche und sicherheitsrelevante Audits und Überprüfungen geht.

Mit FullStory kannst du Behauptungen validieren, betrügerische Akteure identifizieren und dein Unternehmen auf eine neue Weise schützen. Mit FullStory kannst du verdächtige Sitzungen in nahezu Echtzeit einsehen, durchsuchen und überprüfen. Das Einsehen von Sitzungen ist eine viel schnellere und informativere Methode, eine Situation zu beurteilen, als sich durch umfangreiche Systemprotokolle zu wühlen.

FullStory ist einer der wenigen Anbieter, der jede Interaktion von Nutzer:innen mit deiner Website oder App erfasst, ohne dass eine spezielle Ereignis-Instrumentierung erforderlich ist. Somit kannst du sicher sein, dass du über eine umfassende Erfassung jeder Interaktion verfügst, um deine Sicherheitsmaßnahmen zu unterstützen.

Weniger administrative Befugnisse für Mitarbeitende

Um die eigenen Kund:innen optimal zu unterstützen, ist es gängige Praxis, dass vertrauliche, administrative Passwörtern unter Kolleg:innen geteilt werden – insbesondere bei SaaS-Anbietern. Diese Passwörter werden oft im gesamten Unternehmen weitergegeben, um die Behebung von Nutzerproblemen durch autorisierten Datenzugriff oder das Ausgeben von Nutzeridentitäten innerhalb der eigenen Anwendung zu erleichtern. Diese Praxis erhöht das Risiko einer versehentlichen Datenbeschädigung, eines Diebstahls und des Eindringens in die Privatsphäre, wenn sich Support-Mitarbeiter:innen anmelden und in Benutzerkonten stöbern.

FullStory bietet einen Einblick in die Sitzungen der Nutzer:innen in nur einer Richtung. Session Replay ruft vergangene Sitzungen ab (natürlich schreibgeschützt), was bedeutet, dass Informationen ermittelt werden können, ohne mit den Live-Anwendungen zu interagieren. Buttons können nicht gedrückt werden. Einstellungen können nicht geändert werden. Dateien können nicht exportiert werden.

So bietet FullStory eine Möglichkeit, deine Nutzer:innen besser zu unterstützen und gleichzeitig die Anzahl der Personen mit administrativen Rechten im Unternehmen auf sichere Weise zu reduzieren.

SCHLUSSFOLGERUNG

Jede:r verdient eine optimierte digitale Experience

Dennoch sollte die Verbesserung der digitalen Experience niemals auf Kosten der Privatsphäre der Nutzer:innen gehen.

FullStory ist den Kund:innen unserer Kund:innen und deren Datensicherheit verpflichtet. Und wir sind entschlossen, die gesamte Branche durch kontinuierliche Forschung und Entwicklung von führenden Datenschutzmechanismen und Sicherheitsprotokollen voranzutreiben.

Deine Digital Experience Intelligence-Plattform sollte dir helfen, noch bessere digitale Erlebnisse zu schaffen – und zwar schnell und zuverlässig, mühelos und sicher. Unser Ziel ist es, Erkenntnisse zu liefern, die dabei helfen, deine Kund:innen zu begeistern und gleichzeitig ein vertrauenswürdiger Partner zu sein, der deine Daten sicher aufbewahrt.

Wenn du mehr darüber erfahren möchtest, wie FullStory deinem Unternehmen helfen kann, **kontaktiere deine:n Ansprechpartner:in oder fordere eine Demo an →**

Du hast weitere Fragen oder Bedenken? Schicke uns eine E-Mail an **security@fullstory.com.**

Über FullStory

Die Digital Experience Intelligence-Plattform von FullStory ermöglicht es Unternehmen, ihr digitales Kundenerlebnis auf Websites und in mobilen Apps kontinuierlich zu verbessern. Die Plattform liefert proaktiv Erkenntnisse aus Milliarden von Datenpunkten, die unmittelbar in Optimierungen umgesetzt werden können. FullStory hilft so Tausenden von Unternehmen, darunter Fortune-100-Unternehmen und die innovativsten Verbrauchermarken der Welt, evidenzbasierte digitale Verbesserungen vorzunehmen, die Kosten senken und Umsätze zurückgewinnen. Weitere Informationen findest du auf **www.fullstory.com**.