



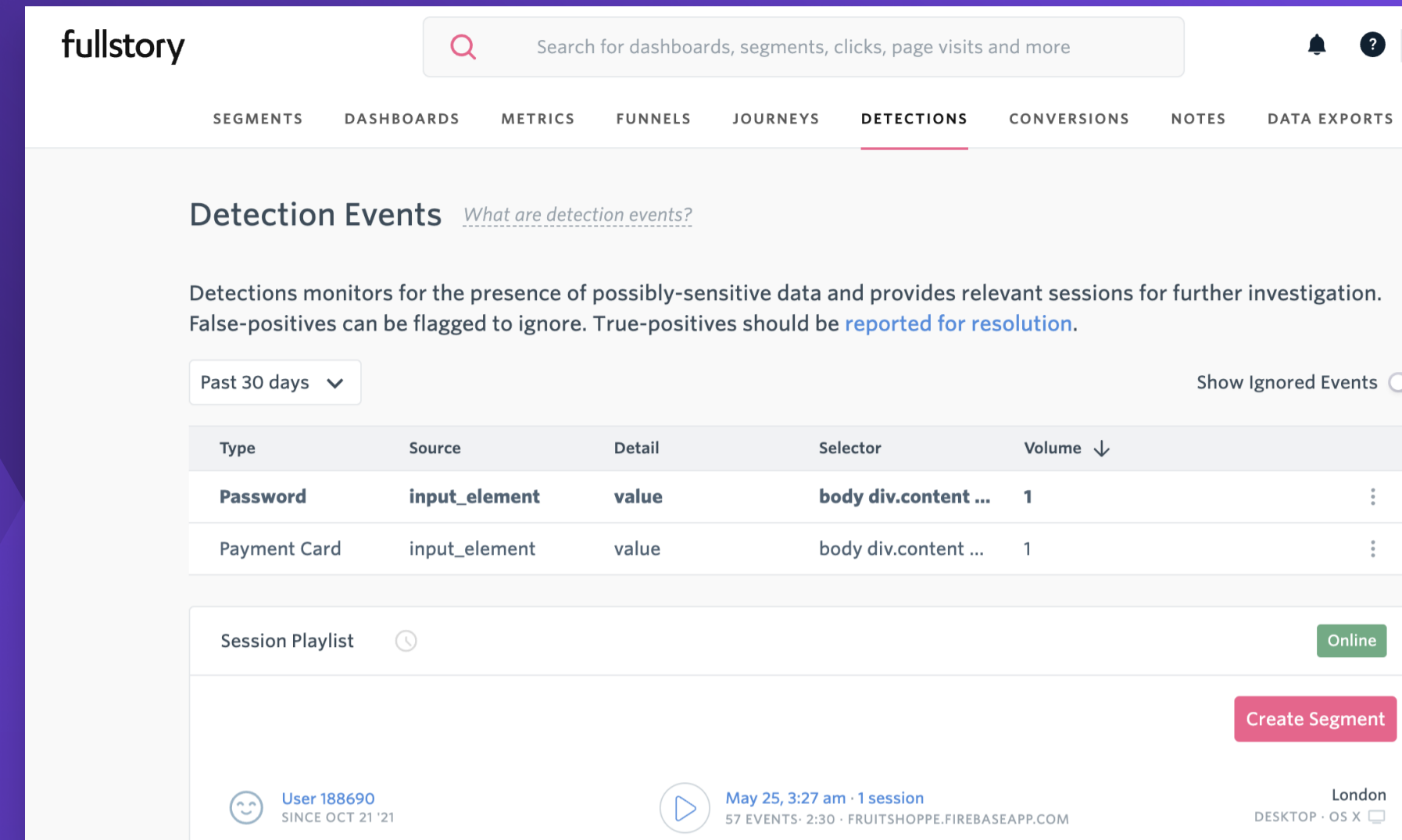
FEATURE OVERVIEW

Proactively preserve user privacy with smart PII monitoring

Automatically detect when, where, and what type of sensitive PII may have slipped through the cracks of your digital experience

Ensure and protect customer privacy from every angle

From first interaction to final transaction, FullStory's robust privacy capabilities are designed to protect you and your end-user. Our Private by Default technology eliminates potential vulnerabilities, and Detections provides an additional layer of protection to make FullStory the most privacy-forward DXI platform.



The screenshot shows the FullStory Detections interface. At the top, there's a search bar and navigation tabs for SEGMENTS, DASHBOARDS, METRICS, FUNNELS, JOURNEYS, DETECTIONS (highlighted), CONVERSIONS, NOTES, and DATA EXPORTS. Below the navigation, there's a section for "Detection Events" with a link "What are detection events?". A text block explains that Detections monitors for sensitive data and provides relevant sessions for investigation, noting that false-positives can be ignored and true-positives should be reported for resolution. A filter dropdown is set to "Past 30 days" and there's a "Show Ignored Events" toggle. A table lists detection events:

Type	Source	Detail	Selector	Volume ↓	
Password	input_element	value	body div.content ...	1	⋮
Payment Card	input_element	value	body div.content ...	1	⋮

Below the table is a "Session Playlist" section with a "Create Segment" button. At the bottom, there are session cards for "User 188690 SINCE OCT 21 '21" and "May 25, 3:27 am · 1 session 57 EVENTS · 2:30 · FRUITSHOPPE.FIREBASEAPP.COM" with a location indicator for "London DESKTOP · OS X".



Gain greater oversight and visibility into your app

With thousands of visitors, complicated web architecture, and ever-changing regulations, ensuring total customer privacy is a huge undertaking. And that's not to mention private information like credit card numbers or passwords that can unintentionally make its way into your DX data. Detections makes the unknown known by monitoring your digital environments and uncovering places (such as DOM sources) where sensitive user data may be buried. Was an account number entered into a chat log with a support agent? Did a user accidentally type their password in a comment field? Did a developer test a new checkout flow and forget to double-check safeguards on payment data? Detections delivers quick access to impacted sessions for further investigation.



Prioritize privacy, proactively and efficiently

When it comes to the digital experience, privacy is a team effort that requires coordination across developer, product, legal, and security teams. To further complicate matters, third-party tools and privacy regulations themselves can change frequently, exposing organizations to the possibility of unknown data leaks. Detections provides an extra layer of support for teams, automatically monitors your site for select categories of sensitive data such as credit card numbers and passwords, and locates issues in real time. As such, Detections empowers teams to take immediate action, minimizing any legal, financial, or security risks associated with sensitive data capture.



Triage and remediate

FullStory makes triaging identified issues easy for your teams by aggregating Detection events in a table with an easily scannable list of corresponding user sessions. Click into any of these sessions to view a Session Replay, which highlights the specific Detection event that occurred. Here, you can determine if the event is a false positive or a true positive, and either create an ignore rule or determine the necessary course of action to remediate the issue.