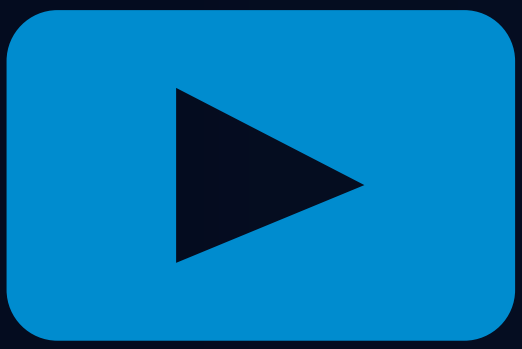
dynatrace

Session Replay privacy excellence

Best-in-class privacy with Session Replay



Overview

Deploy **Session Replay** with ease—learn what you need to know to use Session Replay successfully while respecting and protecting your end users' privacy. Join other Dynatrace customers who use Session Replay in highly regulated sectors, including government, healthcare, and banking.

In this white paper, we'll provide guidelines and answers to your questions on how to roll out Session Replay successfully within your organization. Along the way, we'll show you how you can fine-tune the Session Replay settings so that you get valuable insights into your end users' experiences while respecting their privacy.

The following sections provide you with guidance and answers to essential questions. Feel free to jump to the sections that interest you.

- **What is Session Replay?** See Introduction to Session Replay.
- **Why is Session Replay safe to use?** See Your frequently asked questions about privacy and security answered.

For more information, view the information in this document online.

Introduction to Session Replay

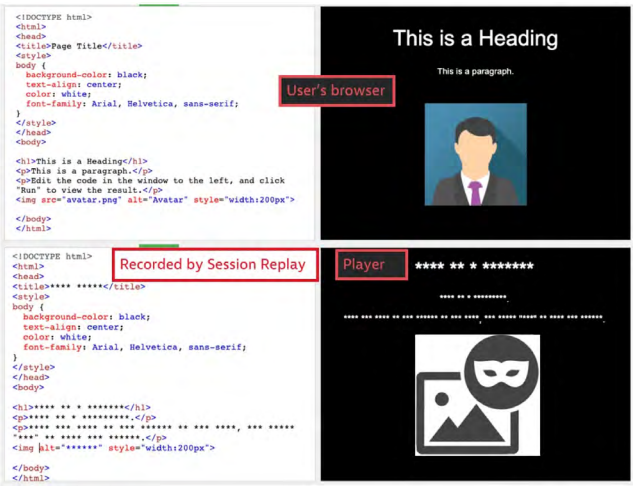
Session Replay extends Dynatrace Real User Monitoring (RUM) as a powerful tool for visually representing the digital experiences of your end users across relevant devices, form factors, personalizations, and responsive UIs. It helps to identify errors, analyze areas of user struggle, and provides analytical data for your testing teams. Development teams use it to proactively analyze new feature adoption and user experience to make smarter investments in their applications while optimizing business success.

Session Replay for web applications

Session Replay for web applications reviews the content and structure of the monitored webpages. It then applies the masking algorithm to anonymize the content, replacing it with asterisks (*) in the user's browser before any session data is sent to Dynatrace.

> **Important**
>
> Session Replay for web applications does not record a video of your end users' screens.

By default, the Session Replay masking algorithm masks all content. See the masked information depicted by asterisks and generic icons in the image below.

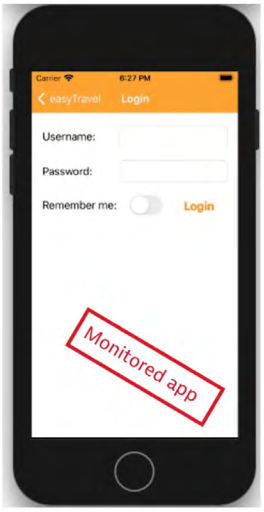


Session Replay for native mobile apps

Session Replay for native mobile apps is available just for those sessions that end in crashes. So, even with Session Replay enabled, not all sessions will be sent to Dynatrace.

To visually recreate the end user's experience with your app before a crash, Session Replay takes screenshots of the monitored app. To ensure maximum data protection, Session Replay applies a masking algorithm before storing images in the local storage of the end user's mobile device.

> **Important**
>
> Session Replay for native mobile apps only captures screenshots and events from the monitored app; it does not record a video of your end user's screen.



Your frequently asked questions about privacy and security answered

Question	Addressed by Session Replay?	Description
Can I exclude personal and confidential information?		Yes. All content is masked by default (text, user input, images, and attributes values) in the end user's browser or device, so only masked data is sent to Dynatrace. You can decide to completely exclude specific URLS from being recorded by using the URL exclusion feature. You can also decide to record additional content by fine-tuning the masking options.
Can I control which sessions are recorded?		Yes. For web applications, use the provided API to carefully select where to start or stop recording. For mobile apps, only sessions ending in crashes are recorded.
Can I control who can change settings?		Yes, by using fine-grained user permissions and management zones.
Can the end user provide informed consent for data collection?		Yes, you can implement this in your web application by using the provided API, which allows you to begin recording once the user consents. The same can be also done for mobile apps.
Can I control who has access to the data?		Yes, by using fine-grained user permissions and management zones.
Can I change the data retention period?		For Dynatrace SaaS, the retention period is 35 days. For Dynatrace Managed, you control the retention period (maximum 35 days).
Can I fulfill data subject requests easily?		By design, no personal data is captured. Furthermore, using anonymization and leveraging our masking capabilities can ensure that no personal data is collected, facilitating the handling of data subject requests.
Can I choose the location where my data is stored?		Yes, you can choose the location when setting up your environment.
Is the data encrypted in transit and at rest?		Yes, here are the details: · In transit · At rest
Can Dynatrace employees play back my end users' sessions?		Yes, Dynatrace employees can view your Session Replay sessions for troubleshooting purposes, and the most restrictive set of defined masking rules is always applied. All access events are registered in audit logs. These audit logs are available to you in an automatable fashion via the REST API.

How Session Replay protects your data

Session Replay and Real User Monitoring offer multiple layers of security and data protection to ensure that only the required information is captured and that unauthorized use and changes are prohibited.

- By default, each user session is anonymized so that the data subject cannot be identified.
- By default, when Session Replay is enabled, Dynatrace anonymizes all content before any session data is sent to Dynatrace.
- Full transparency and control are available to users through the opt-in functionality, which you can integrate with your existing consent solution.
- For Session Replay for mobile apps, only sessions ending in a crash are sent to Dynatrace.
- Session Replay allows for tightly controlled settings for specific purpose-based insights into user experience.
  - **What can be recorded:**
    - You can define specific masking rules for session recording, leveraging pre-configured options.
    - You can exclude specific webpages from being recorded.
  - **What can be played back**— you can define specific masking rules for session playback, leveraging pre-configured options.
  - **Who can see session data:**
    - You can apply fine-grained user permissions to allow session playback, with or without playback masking rules in effect for specific users.
    - Additionally, you can use management zones to carefully and effectively partition your monitoring environment to limit who has access to specific applications that have recorded sessions.
- All changes to the settings—what can be recorded, what can be played back, and by whom—are logged in an audit trail.

To check out videos and see Session Replay in action, learn about rolling out Session Replay for web or mobile apps, explore the settings, and find more resources, view this document online.

About Dynatrace

Dynatrace provides software intelligence to simplify cloud complexity and accelerate digital transformation. With automatic and intelligent observability at scale, our all-in-one platform delivers precise answers about the performance and security of applications, the underlying infrastructure, and the experience of all users to enable organizations to innovate faster, collaborate more efficiently, and deliver more value with dramatically less effort. That's why many of the world's largest enterprises trust Dynatrace® to modernize and automate cloud operations, release better software faster, and deliver unrivalled digital experiences.

dynatrace.com blog @dynatrace

01.03.22 12406_WP_USlet_mt