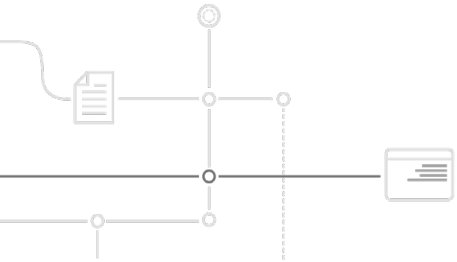

Lakeside®

SysTrack Cloud Edition

Security Overview

Lakeside Software takes data protection and privacy very seriously

What is SysTrack Cloud Edition?

SysTrack Cloud Edition is a digital experience monitoring solution that gathers and analyzes data on everything that may impact end-user experience and business productivity, in any EUC environment. To do this, SysTrack gathers these details using an endpoint agent and periodically summarizes and sends that data to a SysTrack master. For SysTrack Cloud Edition, that master, and the collected environment data, live in Azure. Other cloud providers could be supported.

What is SysTrack collecting?

By the very nature of the solution, SysTrack captures performance and usage data on thirteen KPIs totaling tens of thousands of data points: CPU, memory, disk, network, latency, startup time, virtual memory, virtual machine data, software installment and usage, software updates, events, faults and hardware.

When it comes to user-specific data, SysTrack captures the following user details in an effort to provide Lakeside Software customers with visibility into which end users are experiencing problems and why: user names, active directory details, site visits, application activity, and the hours during which a user is active throughout the week. Should it be a requirement or preference of the customer, this data can be easily anonymized within the solution.

Alternatively, SysTrack is NOT collecting sensitive data like keystrokes and screen captures or email and file contents. In fact, anything that might be considered protected intellectual property or sensitive user information is avoided to protect privacy. Many other metadata classes, like user names or website visitation tracking, can also be disabled or tuned for countries or companies with stricter requirements on what data collection is acceptable.

How is user data protected within SysTrack Cloud Edition?

SysTrack Cloud Edition uses HTTPS and SSL connections. Given the master and the collected environment data are housed in the cloud, data protection and security compliance are reliant on the cloud provider's information security standards. As it pertains to Azure, the offering is ISO27001 and SOC 1, 2 and 3 compliant. Below are other helpful links pertaining Microsoft Security and Compliance:

Microsoft's full list of compliance offerings

Microsoft's compliance overview

Microsoft security site

Microsoft's privacy overview

Additionally, SysTrack is designed to be customizable so that Lakeside customers can configure the solution in order to fit their security standards. To do this, three critical areas can be enabled and customized: User name anonymization, tuning or disabling collection of specific data points, and permissions configuration.

How does Lakeside comply with the GDPR and other data protection law?

Lakeside is committed to providing its customers the capabilities needed to keep their SysTrack investment GDPR compliant. As such, the company is certified under the EC- and Swiss-approved Privacy Shield program administered by the U.S. Department of Commerce and enforced by the U.S. Federal Trade Commission.

In order to facilitate GDPR compliance, SysTrack configurations allow for user anonymization and extensive limits to be placed on what data is being processed, with things like web history being a popular option. To learn more, please read our GDPR statement. Below are Lakeside compliance information resources:

Lakeside 's Privacy Shield Privacy Statement

Lakeside's Privacy Statement

Lakeside's GDPR statement

Can user names be anonymized?

Yes. This can be done either by replacing user names with terminal names or using an MD5 hash with or without a lookup table or reference.

Can data collection be customized to exclude certain data points?

Yes. SysTrack is built to be customizable. You can limit or disable web browser tracking, data related to application usage, and the collection of any data.

Who has access to SysTrack-collected data?

Access to data collected by SysTrack Cloud Edition is dependent on what is configured via security controls. Only those within the same tenant have access to SysTrack data.

What is used for authentication in SysTrack Cloud Edition?

Active Directory is used, with policies enforced via (GPO).

Is my data encrypted in the cloud?

All data is encrypted during transit and at rest.

Is the data collected by SysTrack Cloud Edition separate from other people's data?

Yes. Customer data is isolated in separate databases.

If you have any further questions, please contact your sales representative.