LABSTATS

LABSTATS CLOUD SECURITY OVERVIEW

LabStats is a software package which collects data on hardware and software usage and offers utilization statistics and analytics on that usage to permitted users via the LabStats Portal. Portions of the LabStats software package can be hosted in the cloud and this Security & Compliance Overview provides details of this arrangement.

Service Provider

LabStats utilizes the Microsoft Azure cloud platform for delivering the LabStats product in the cloud. The highly trusted platform was chosen for a variety of reasons including: their multi-decade long history of being a software solutions provider, their industry recognition as being the leading cloud platform provider, their world class security and risk mitigation, their high-availability offerings, and because they have the most compliance certifications and attestations of any cloud provider.

Collected Data

Hardware

LabStats collects information on specified computers only, and currently includes information such as manufacturer, model, serial number, host name, operating system, processor details, memory details, IP addresses, MAC addresses, graphics card details, hard drive capacity/availability. Host name values can be manually overridden to obfuscate the identity of some or all computers.

Hardware Usage

LabStats collects usage information of specified computers only, such as when a computer was powered on and off, and when the computer was logged in and out of and by which user account.

Applications

LabStats collects information about software installed on and/or ran from specified computers only, and currently includes information such as name, process name pattern for desktop applications, and URL pattern for web applications. Application name values can be manually

overridden to obfuscate the identity of some or all applications.

Application Usage

LabStats collects information of specified software only which is installed on and/or ran from specified computers, such as when the application was launched and closed and by which user account, and the duration in which it was in focus.

User Accounts

LabStats collects information of all user accounts which are used to log into specified computers, and currently includes information such as username. Username values can be manually overridden to obfuscate the identity of some or all user accounts.

Access to Data

Permitted Users

Your organization is responsible for granting access to your LabStats Portal and the data contained within it. As such, your organization will decide who should be given access and what level of access they should have. Your organization has complete control of this at all times and can make changes as needed with immediate effect.

LabStats Employees

As necessary to perform their job functions and support you in your use of the LabStats product, certain LabStats employees may have some level of access to your data, including customer service, support, and software development employees. Access is limited, is intermittent, and is given only to required employees which have undergone a formal vetting and have signed confidentiality and non-disclosure agreements.

Raw Access

While a subscription is active, Permitted Users have access to data within the LabStats Portal, however, you may also periodically request access to your raw data to facilitate any secondary backup, audit, or other needs.

Data Policies

Ownership

Your organization retains ownership of the data collected by LabStats. LabStats maintains a

license to use the data for the purpose of providing utilization statistics and analytics to your organization.

Storage

Data collected by LabStats is stored in the nearest cloud data center to your physical location in which LabStats has a presence, which currently includes data centers in the United States (California), Canada (Ontario), Netherlands, and Singapore. If your organization does not reside within one of these countries, you may contact LabStats Support to find out specifically which data center your data is or would be stored in.

Retention

Data collected by LabStats is retained while an active subscription is maintained and has a schedule for destruction at the expiration of the subscription. After a short period of time following subscription expiration, unless instructed otherwise, the primary data source is backed up and the original is destroyed. The backup is held in the cloud but is offline for another period of time and can be restored in the event that you wish to reinstate your account. After this period of time has elapsed, your database backup is permanently destroyed and is unrecoverable.

System Access

Computers

The LabStats client is installed on specified physical or virtual computers, most likely within your organization's network. This client runs under standard, un-elevated privileges, and is required for data collection (which is outlined in Collected Data).

Active Directory

Integrating with Active Directory is optional and allows computers to automatically organize into groups in LabStats which mimic the organization in Active Directory. The integration can also be used to collect the user account display name in place of the username. Both of these integration options are opted into independently. Access to Active Directory is performed by the LabStats application via an account with read-only permission and can be revoked at any time; permission can be limited to a subset of OUs. Account credentials are encrypted and cannot be viewed by any Portal users or LabStats employees. Connection to AD server is done through port 389 using the "Directory Services" .NET library authored by Microsoft by default, however, if the AD server supports SSL connections, port 636 can be used instead to establish a secure connection.

Azure Active Directory

Integrating with Azure Active Directory is optional and allows users of the LabStats Portal to login using their organization provided account, puts access control to LabStats and its data in the hands of your IT or security department, and enforces your password and security policies on the LabStats Portal. User passwords are not shared with LabStats and authentication is handled by Microsoft.

Security

Physical & Digital

For its cloud offering, LabStats utilizes Microsoft Azure data-centers which employ many measures to protect operations and data from physical or virtual threats or intrusions. The data centers comply with industry standards (such as ISO 27001) for physical security and availability. Data centers are hardened and their exact locations are not published. They have extensive physical security in place, which include perimeter fencing, video cameras, security personnel, secure entrances, real-time communication networks, etc.

Data in Transit

Data is transmitted to and from the LabStats Portal, Client Service, API, and LabFind using TLS 1.0, 1.1, and 1.2 encryption with an SSL certificate utilizing a SHA-256 algorithm and an RSA 4096 bit key. Certificates are kept current such that they won't expire.

Data at Rest

Certain sensitive data is encrypted at rest for an additional layer of security using 256 bit AES encryption with a private password and salt. The encryption is reversible by the LabStats Portal as is required to present data back to authorized Portal Users or to perform authentication against integrated network assets (in the case of Active Directory integration).

Isolation

Data is stored in isolation via separate databases and is not co-mingled with data from other organizations. Access from one database to another database is prohibited by design.

Code Execution

The LabStats Portal and its supporting systems are developed and deployed with strong security controls. The application is pre-compiled, peer reviewed, and is developed with strict standards and controls so no unauthorized code is allowed to execute against your data or your network.

Security Updates & Patches

LabStats uses a platform-as-a-service (PAAS) provider for hosting the LabStats Portal, and as such, security updates and patches are installed promptly by Microsoft as they become available for operating systems, server, and other supporting software. The level of responsiveness to these security updates and patches is unparalleled and provides the best prevention against malware and unauthorized access.

Monitoring

The cloud infrastructure which LabStats runs on is physically monitored continuously by Microsoft employees and contractors and virtually by Microsoft employees and contractors and LabStats engineers.

Breach

No breaches of any kind have previously occurred and LabStats will notify organizations if there are real or perceived breaches in the future.

Compliance

LabStats strives to achieve and maintain compliance with all relevant guidelines, standards, and legislation, including the Family Educational Rights and Privacy Act (FERPA), the American Disabilities Act (ADA), section 508 of the Rehabilitation Act, and the EU General Data Protection Regulation (GDPR). A voluntary product accessibility template (VPAT) is available by request.

This document is for informational purposes only and is not a guarantee or contract between any two parties. Information is subject to change.

Last updated: November 2019