Aimbetter Security

© Copyright 2017, Aimbetter, Inc. All rights reserved.

AimBetter

OVERVIEW

Aimbetter is committed to the security of your application's performance data. As part of this commitment, we use a variety of industry-standard security technologies and procedures to help protect your information from unauthorized access, use, or disclosure.

Secure and handle the following fields:

- Application Security
- Infrastructure & Network Security
- Compliance
- Privacy
- Corporate Security

Employees are required to attend security awareness training and are informed of their security responsibilities.

CONTENTS

© Copyright 2017, Aimbetter, Inc. All rights reserved.

PRODUCT OVERVIEW

Aimbetter's services provides our customers monitor performance data from their applications and systems. This is accomplished by enabling customers to transmit those monitor data to Aimbetter's services, which presents application performance information through a secure website and user interface.

Aimbetter flow work like this:

• A customer who runs applications and/or servers in data center, cloud, or hybrid environments, installs an “Aimbetter Agent” on a specified server with custom specified servers to monitor.

• Aimbetter Agent transmits monitor data to the Aimbetter service via SSL-encrypted.

• Aimbetter services aggregate and store the application performance information and data in our encrypted data center

• The application performance data are available via Aimbetter SSL-encrypted and password protected website (https://app.aimbetter.com) .

DATA COLLECTION

Aimbetter only monitors performance for the applications and/or servers of the custom database environment specified during the installtion of the Aimbetter Agent. Generally, the monitor collects metadata that includes aggregate time measurements for server resource utilization statistics, server error log, SQL server resources, SQL server queries statistics and SQL errors.

Aimbetter Agent processes:

- Database query activity.
- Database utilization metadata (Database size, SQL response time, Number of request, etc.)
- Database errors (Query error code, Query timeout expired, Duplicate key, etc.)
- Server utilization metadata (CPU usage, Memory utilization, Disk utilization, Network utilization, etc.)
- Server event log.

© Copyright 2017, Aimbetter, Inc. All rights reserved.

PRIVACY

Aimbetter is committed to protect the privacy of our customers. The application data we process as part of our provision of services is primarily used to display application performance information back to the customer's Aimbetter account user.

DATA CENTER SECURITY

Aimbetter is hosted at our Tier3+ certified data center with fully redundant power backup systems, fire suppression systems, security guards, and bio-metric authentication systems.

TECHNICAL FEATURES

Aimbetter has certain technical features built into its offerings to offer its customers flexible security options:

- Aimbetter encrypts performance data in transit. SSL encryption is enabled by default for data being sent to Aimbetter in transit.
- The Aimbetter Agent does not te any vulnerabilites in customers' firewalls. Communication from the Aimbetter Agents to the Aimbetter API is outbound on port 443 by default and can be configured to use a proxy server. Aimbetter Agents do not receive inbound connections.
- Aimbetter does not have the ability to auto-update Agents installed on your servers. All updates must be manually installed by our customers.
- Aimbetter services are protected by firewall, VPN gateway and intrusion detection systems.
- All Aimbetter system databases are encrypted.
- Limited data retention. Upon termination of Aimbetter services, all data will be removed from Aimbetter systems (including backups) within 90 days.

© Copyright 2017, Aimbetter, Inc. All rights reserved.

USER MANAGEMENT

Aimbetter users access the services via an email address and a password. These passwords must contain a minimum of eight characters.

Aimbetter uses the following mechanism to protect access :

- Password retry failure will block the user and enforce the user to identify.
- Optional IP Address restrictions

User passwords are stored in an industry standard encrypted hash format. Customers are responsible for managing their own accounts, including provisioning and de-provisioning their own users.

© Copyright 2017, Aimbetter, Inc. All rights reserved.