AimBetter Security Specification

OVERVIEW

AimBetter is committed to the security of our own and our customers' data. As part of this commitment, we use a variety of leading-edge security technologies and procedures to help protect your information from unauthorized access, use, or disclosure.

Our promise is to provide full security in the following areas:

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

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

CONTENTS

PRODUCT OVERVIEW

AimBetter's services provides our customers with performance data from their applications and systems. This is accomplished by means of our specialized on-site agent that performs the data collection, consolidation and transmission over secure channels into our proprietary servers.

AimBetter’s workflow goes like this:

• AimBetter Agent is installed on one of the customer’s own servers to monitor servers in a local data center, cloud, or hybrid environment.

• AimBetter Agent collects and transmits monitored data to our remote servers via secure SSL-encrypted channels.

• AimBetter servers aggregate and store the application performance information and data in our secure data center.

• The resulting server performance reports are made available via AimBetter’s 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 installation 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.

PRIVACY

AimBetter is committed to protect the privacy of our customers. The application data we process as part of our provision of services is only used to display application performance information back to the customer's AimBetter account user. We undertake never to provide data to third-parties without the explicit approval of the customer.

DATA CENTER SECURITY

AimBetter is hosted at our Tier3+ certified data center. Physical access to this location is restricted to people with authenticated credentials and all access/egress is reported.

The center is equipped with fully redundant power backup systems, fire suppression systems, security guards, and bio-metric authentication systems.

ADDITIONAL SECURITY FEATURES

AimBetter has certain technical features built into its design to offer its customers additional security options:

- AimBetter encrypts all data in transit. SSL encryption is enabled by default for data being sent to AimBetter.
- The AimBetter Agent does not create any vulnerabilities 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 allow inbound connections.
- AimBetter does not have the ability to auto-update software installed on your servers. All updates must be manually installed by your own administrators.
- AimBetter services are protected by firewall, VPN gateway and intrusion detection systems.
- All AimBetter system databases are locally encrypted and cannot be accessed except via username/password access.
- Data retention persists only during the period of service. Upon termination of AimBetter services, all data will be removed from AimBetter systems (including backups) within 90 days.

USER ACCESS MANAGEMENT

AimBetter users access the services by means of their unique username (usually email address) and password. These passwords must contain a minimum of eight characters.

AimBetter uses the following mechanism to protect against access violation:

- Multiple login failures will block the user and enforce re-authentication.
- Optionally, customers can specify a range of valid IP Address from which access is permitted.

User passwords are stored by us in an advanced, industry standard encrypted hash format.

Customers are responsible for managing their own accounts, including provisioning and de-provisioning their own users.

SUMMARY

AimBetter guarantees complete security of your on-site data. No data content is passed between your site and the AimBetter processing center.

AimBetter guarantees the integrity of your site. There is no channel for data to be uploaded into your location from our service.

AimBetter uses leading-edge data encryption technology in all traffic movement between your site and our center.

AimBetter's own data center is protected physically and logically to prevent access except by authenticated users.

Access to our service is restricted to authenticated users, with measures to detect and prevent attempted hacking.