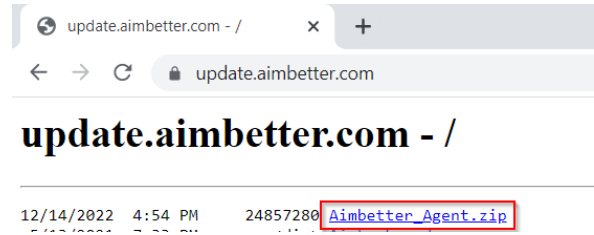# Secure-by-Design Architecture Details

CUSTOMERS SERVERS' ENVIRONMENT - Single Agent

The Agent program is downloaded from the secured URL update.aimbetter.com to **only one of the customer's servers**. This server must have Windows OS (check the Requirements for the Agent Server). The Agent program code is in C#.


A **unique License key and Identifier** are requested for the installation, which are received after account creation and email verification.
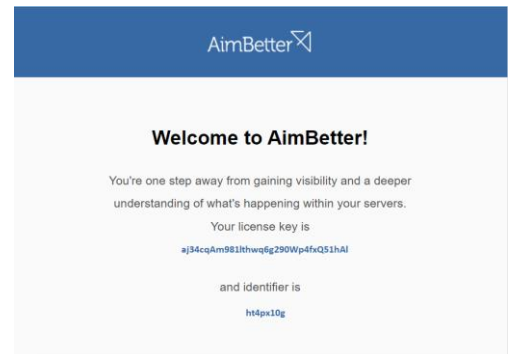
A Windows service is created in the Agent server after running the Agent program. The user that runs this service needs minimal Windows OS credentials which enables collecting OS performance metrics from the monitored servers.
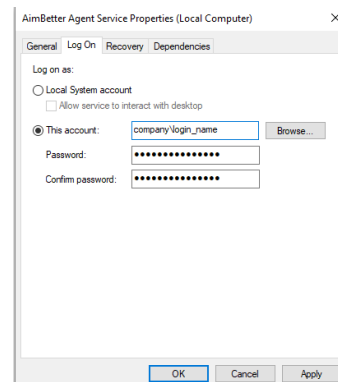
In order to connect to the Database server in the monitored server, a Database Server user must be created with **minimal permissions** as detailed in the Monitored Servers Requirement Table. This user has READ-ONLY permission to collect Metadata, Statistics and Performance metrics. It has no access to the Database content whatsoever.
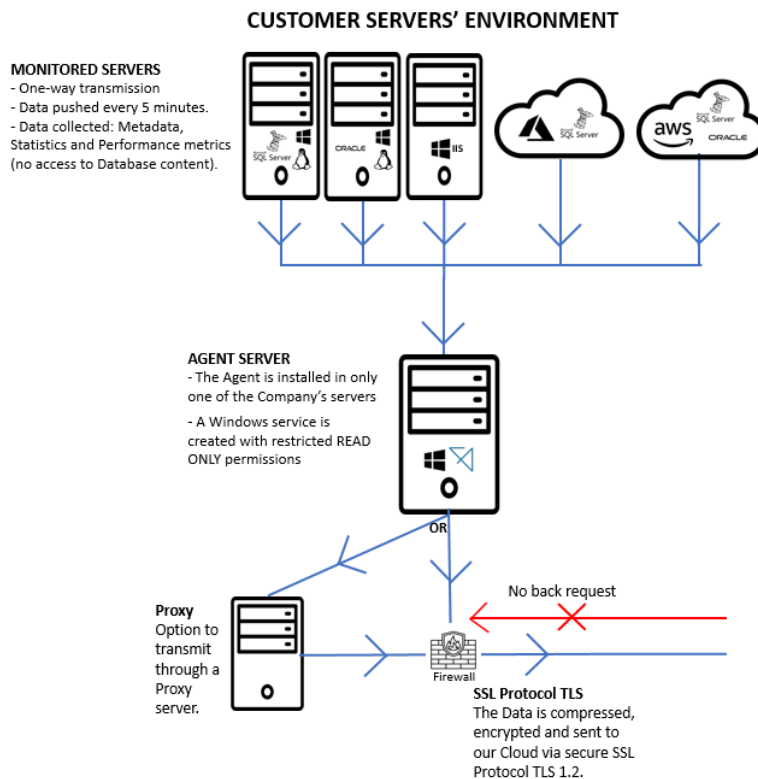
The Agent collects **WMI and System queries data** and sends to our API Cloudflare-secured address api.aimbetter.com via **SSL** ports through **secure Protocol TLS 1.2** after the Data **is encrypted** and compressed. The default outbound port is 443.

There is no transmission of data from our API to the Agent. The Agent only waits for confirmation that the data was properly transmitted.

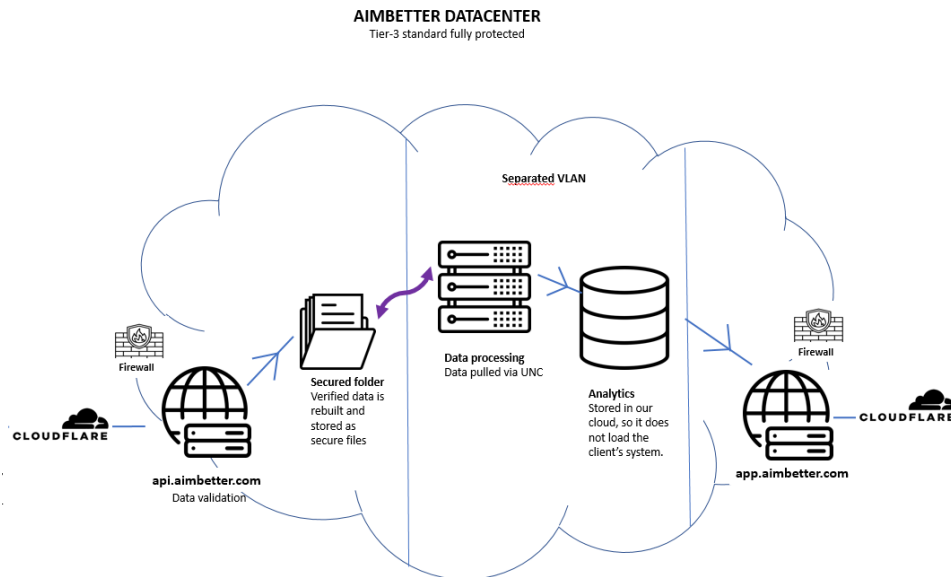**No data flows from our API to the companies' servers.**

During the installation process, there is an option to restrict the Database Server access selecting "**Secured**" and/or "**Reserved Connection**".
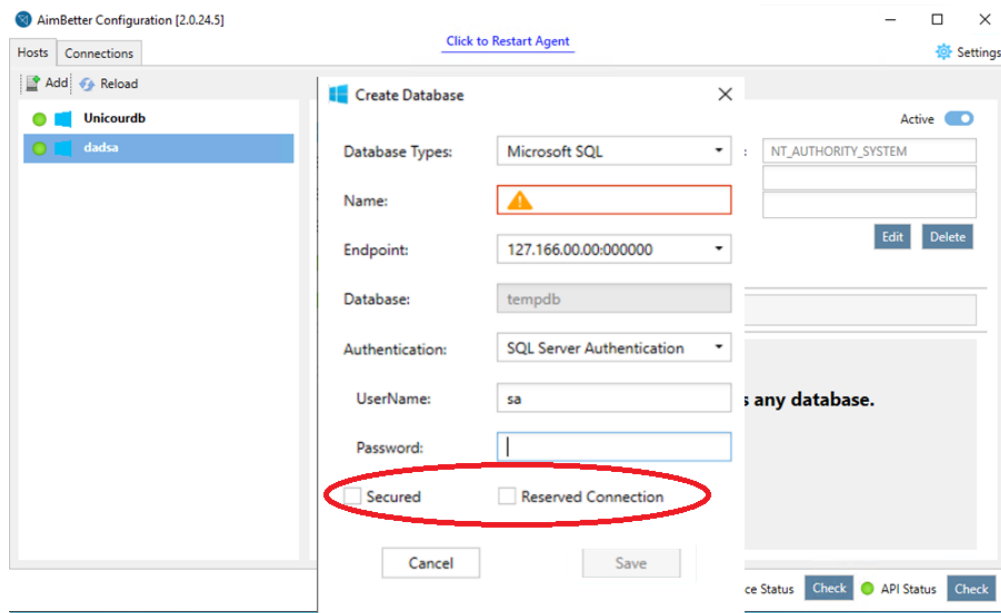
The "Secured" option prevents the collection of parameters that may be included in queries' plans and the "Reserved Connection" guarantees a unique and exclusive connection to the Database Server.

AIMBETTER DATACENTER

Our Datacenter operates on **Tier-3 standard**, equivalent to banking and insurance. Data is fully secured both physically and logically. It is **hosted on leading Israeli Service Provider** which guarantees full compliance with GDPR standards.

AIMBETTER DATACENTER
Tier-3 standard fully protected

Separated VLAN

Firewall

Secured folder
Verified data is
rebuilt and
stored as
secure files

Data processing
Data pulled via UNC

Analytics
Stored in our
cloud, so it does
not load the
client's system.

Firewall

CLOUDFLARE

api.aimbetter.com
Data validation

CLOUDFLARE

app.aimbetter.com

After the Performance metrics are received and validated by our API, the data is rebuilt and stored as **secured files**.

Our Applications servers pull the data **via UNC** from the specific secured folder path and process it.

All the analytics are then stored in our Database servers. That means that there is no load on the customers' servers caused by the monitoring.

Both Application and Database servers are located in a separate villa inside the Datacenter, protected by **firewall**, **VPN gateway** and high-level **access restrictions**.

CUSTOMER BROWSER - User Access

The platform UI is accessible through the Cloudflare-secured address app.aimbetter.com through any browser and can be restricted for specific IPs.

The user access is **login-based** with a strong password required and can be configured to have **2 factor authentication, IP restriction**. It can also be integrated with the customer's **Identity Provider via SSO** if it supports the SAML 2.0 protocol.

After **5 failed login attempts**, the user is blocked, and it can be released only though our support team.

The user access is **session protected**, which means that the system automatically logs out upon any IP change.

User access:
- Login based
- IP restricted
- 2-FA authenticated
- Session protected
- Blocked after 5 failed login attempts

CLOUDFLARE

app.aimbetter.com