Security and Data Protection

VM Products ensures system safety by implementing specific security protocols.

The system is built using Microsoft's technology stack of development tools, servers, and database utilizing the **Microsoft Azure cloud** services (https://azure.microsoft.com). This allows tight integration among components.

Microsoft Azure cloud

The system is installed on three Azure services:

1. App Service—Used for Web API that are consumed by the mobile app, Web app and IoT devices.
2. VM (Virtual Machines)—Used as an "application server" (the application uses SOA to implement some of the system's "business logic").
3. Database and Storage—"Azure SQL Database" is the system database for storing all the structured data while Blob storage is used for large amounts of unstructured object data, such as images. This database implements a variety of methods to keep the data secured and protected, such as 99.99% availability, built-in geo-replication, failover options, multiple layers of data protection, and much more....
   Azure SQL Database has the largest compliance portfolio in the industry.

   Read more about Azure security, privacy, and compliance features at:
   https://www.microsoft.com/en-us/TrustCenter/CloudServices/Azure

Software

1. The source code and design documents are managed by the development team using a private account of Bitbucket (see http://www.bitbucket.org) and access is allowed only to authorized users.
2. The system is built with "Visual Studio 2015" using C# programming language for the backend server. The frontend web application is built using Angular (Created by Google) and the mobile app are developed by Xamarin (Created by Microsoft) complied to native code for both Android and iOS.
3. The following guidelines are kept during the development process to ensure a high level of security:
   - **a.** Validate and sanitize the input data to avoid cross-site scripting.
   - **b.** All data access is done via "Stored Procedure" to reduce the risk for SQL injection.
   - **c.** All sensitive data, such as passwords, are encrypted in the database.
   - **d.** The application is tested for security issues by the QA team and reviewed during code-review sessions.
   - **e.** All the communication between frontend (Web and Mobile apps) and backend (Server) is encrypted using SSL.
   - **f.** Hardware (PestOptix®) - All the communication between endpoints and backend (Server) is encrypted using the AES-256.

PestOptix Data Protection

Overview[1]

Cloud Architecture	Microsoft Azure
Service	SaaS (Software-as-a-Service)
System	App Service, VM (Virtual Machines) Server, Azure SQL Database, Bitbucket
Software	.NET, Angular, Xamarin
Hardware	Wi-Fi protocol 802.11 B/G/N between Router and Endpoint

Variation Specifications

Normal operating	Standby mode "Sleep" is the normal state after initial turn on with 10 KB (+/-) of data from any message (once-a-day heartbeat "keep alive" or an alert message).
Security	SSL, AES-256
Wi-Fi notes	**1.** After install is verified for client's peace of mind, you can choose "Forget Network" from the phone's Wi-Fi network list. **2.** During an outage, the PestOptix system Wi-Fi retention will auto-reconnect to the router, sending any messages during stand by occurrence(s). **3.** Pressing the button will also auto-reconnect if the password has not changed and check if you're in range of the Router or range extender.

[1] The above is a brief overview. Detailed information is available upon request.