# mesh
## works

TECH BROCHURE

# INSIDE THIS DOCUMENT

# PROBLEM

The current offerings in the market for software management solutions for sourcing, procurement, sales, and engineering are on two extremes of the spectrum: Microsoft Excel, Dropbox and SharePoint which are free and then full-blown ERP/MRP solutions that offer RFQ modules at prices starting in the $50-100K range. Midsize manufacturers have been extremely underserved and have been left behind in terms of their adoption of technology and systems that can help improve operations and efficiency.

The biggest problem that small to midsize industrial manufacturers face right now is that all system functionality and time is spent on the analysis, which is where the real insights can be derived from. This decentralization of data process is much more time-consuming and manual. They offer no ability to collaborate on the projects and very little for management to see what's in pipeline within their sourcing teams. Solutions also lack simple methods to solve supplier management problems—keeping the supplier certifications current.

There are over 280,000 manufacturing sites in North America and over 60,000 manufacturers with 20-500 employees and over 10,000 with more than 500 employees. Tier 2, 3 and 4 manufacturers purchase over 30 different types of raw materials and components from 200-500 suppliers. Their buyers typically issue over 500 RFQs annually. Current solutions which are available to them cost from $60,000 to well over $250,000 and still lack basic engineering intelligence within the system.

In our conversations with subject matter experts in the manufacturing industry, one of the main challenges is managing their RFQ pipeline. Most products have been built to satisfy enterprise customers and their complicated IT requirements, but these complexities are simply not needed for mid-size manufacturers.

# SOLUTION

MESH is a cloud-based portal designed for manufacturers to manage all sourcing, sales, procurement, and engineering in one easy-to-use, online platform. Current enterprise level sourcing systems are designed to be used for special projects and reverse auctions. The MESH Solution is designed to be user friendly and aspires to be a workflow software to be used to send RFQs, update supplier information, analyze quotes, manage quality projects and incidents, and communicate with suppliers.

MESH is designed to have customizable dashboards for buyers as well as managers and has a "workbench" feature, which team members can login to see their task list. MESH has a mobile app to manage APQP projects and quality incidents. MESH is striving to be "4 step" RFQ process which can add efficiency to buying process.

The MESH solution is built on the latest Angular and .Net platforms. It was built using State-of-the-Art micro-services. It is hosted on Azure cloud with various levels of encryption and security.

MESH consists of 3 main solutions to begin with, which will all be separate products that can be used together if desired – MESH SRM, MESH Sourcing, and MESH QMS.

# OVERVIEW

MESH is using a software-as-a-service model (SaaS), where there is nothing to install on individual client machines locally or application servers to maintain on premise. Instead, the application is consumed using a web browser securely accessing MESH application services over the internet. The SaaS model offers a strong value proposition to customers by eliminating significant administrative and IT operational overhead, while still delivering enterprise class functionality, and security for corporate performance management.

\

## No Investments in Hardware, Software, or IT Services

MESH eliminates the need to purchase expensive new hardware, additional software, or even additional maintenance oversight from an already burdened IT department to provide a lower total cost of ownership.

## Rapid Deployment

By eliminating time consuming and expensive infrastructure setup and configuration, you can be up and running immediately to begin solving business problems earlier instead of worrying about dealing with complicated server configurations.

## Seamless Data Integration

Easily import data into MESH as part of your service from either Excel or text files, on premise ERPs and GLs, or other leading cloud services without significant IT involvement for rapid implementations.

## Operating Expense Instead of Capital Costs

As there is no need to purchase new hardware and software licenses upfront, subscription fees make it easier to budget for recurring operating expenses.

## Enhanced Security Posture

MESH has been built since its onset with a robust security framework in mind. In many cases, the security protections implemented in MESH exceed the levels usually implemented at a customers' data center. Instead of having to worry about security across multiple applications consisting of different technology stacks, security protections can be focused entirely on the MESH and implement controls solely for the protection of MESH infrastructure and data.

## Automatic Upgrades

All customers are on the same version of MESH. Regularly scheduled upgrades are implemented safely and automatically without customer intervention, ensuring that all customers have access to the latest capabilities without having to wait for IT departments to apply upgrades. Upgrades are performed away from busy month-end periods and during non-business hours.

## Anywhere Availability

All that is required to access MESH is an internet connection. The software can be accessed from any web browser capable device including desktops, laptops, tablets, and phones. Customers with multiple corporate locations do not need VPNs or additional investments remote desktop or virtualization architectures.

## High Degree of Flexibility

MESH offers the same powerful and comprehensive capabilities as an on-site system. Budgeting, planning models, reports, forecasts, and business processes can all be configured and maintained by the business user.

## Elastic Scalability

One of the primary benefits of SaaS is the ability to be nimble when necessary, and quickly scale if there is additional demand, a feature that is not enjoyed with on premise applications. Additional users can be quickly accommodated by MESH without the need to procure and manage additional servers.

# A Consumer User Experience

The rise of highly functional, visually rich, and easy to use consumer applications has put increasing pressure on business applications to also deliver equivalent experiences. Historically, business applications have suffered from a lack of attention to the details required by regular business users and instead focused on technical aspects geared towards IT developers, highly trained power users, and consultants.

To meet the expectations of modern business users in the age of consumer applications that deliver high-fidelity user experiences, MESH has always focused on ease of use for all users in the budgeting, planning, forecasting, and reporting ecosystem. All users want to be empowered to use the business application rather than engaging with IT to perform routine tasks like running reports or updating calculations in budgeting and forecasting models.

The MESH design team regularly benchmarks the MESH user experience against consumer cloud applications that most business users are accustomed to using.

### HTML5 User Interface

The MESH user interface is written to be fully compatible across all modern web browsers such as Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari, and Internet Explorer. Since we use industry standard HTML5/ CSS3 and JavaScript to create our user interface, no additional plug-ins or add-ons are necessary.

### Mobile App

The mobile user experience is a core principle in the overall design of the MESH user interface. Mobile users have access to key functionality and data as they do on their desktop. For example, a report on the desktop can be accessed containing live data (and can even be updated) on any mobile device, with no data stored on the device.

### No Additional Learning Curve on Difference Devices

Additional user training is not required to utilize the application on different devices. The same user experience is consistent across all platforms to maximize the value to users.
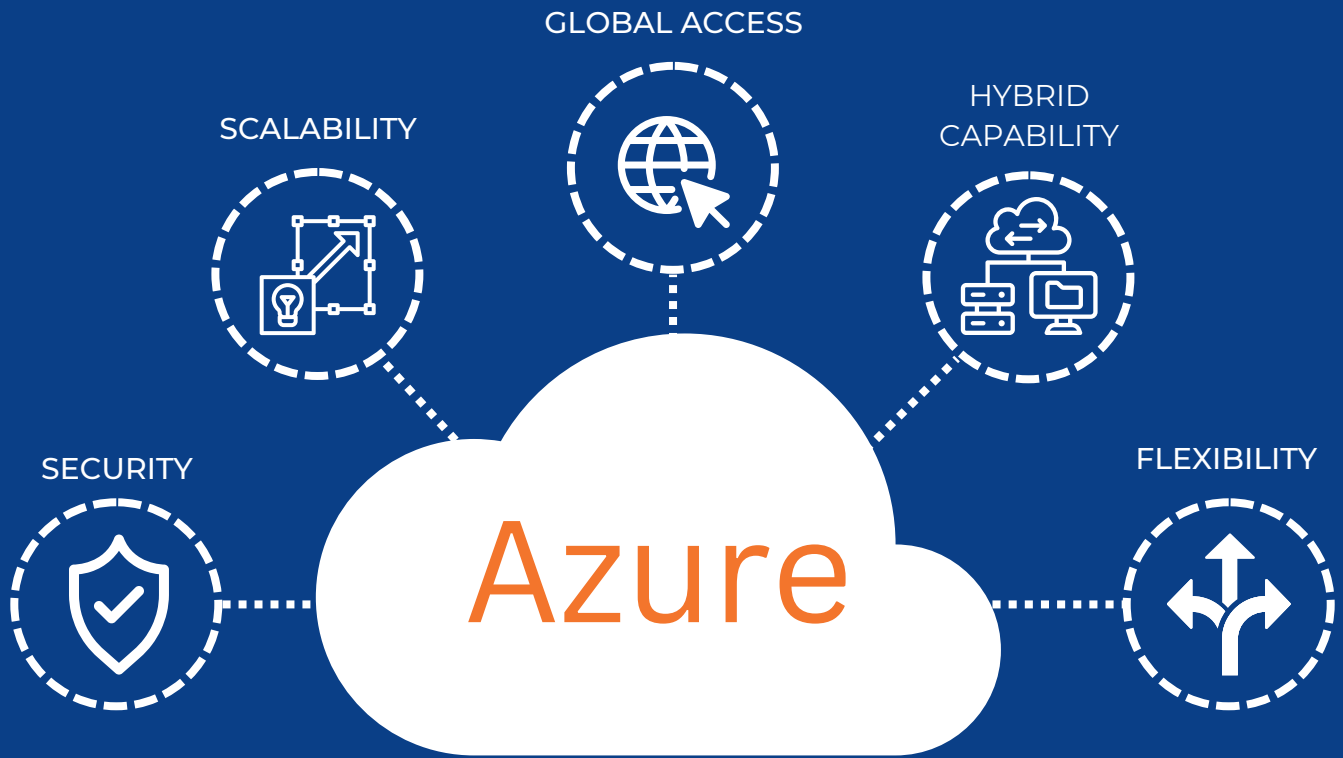
# Application Architecture

MESH is a native web application based on an ASP.NET MVC using RESTful APIs, and Microsoft SQL Server, with a browser-based user interface.

There is logical separation of data and application instances between customers to ensure total data isolation, access control, and performance. Through this level of isolation, the behavior of a single MESH customer can never affect the performance of another customer. For example, no individual customer can flood the service with expensive queries which impact the level of service delivered to another customer.

# World Class Cloud Infrastructure

The MESH application is hosted within Azure Web Services (Azure), the largest provider of cloud infrastructure in the world. MESH selected Azure for both its breadth of infrastructure, flexible management tools, and strong commitment to security. The scale and sophistication of controls for Azure far exceeds any known private hosting provider. The result is a robust cloud service that can ensure uptime availability levels of at least 99.5%, consistent performance, and a high security posture for our customers.

Azure offers cloud infrastructure services from 21 geographic locations around the world, with each location consisting of multiple physically distinct availability zones to ensure the highest levels of service access. Availability zones offer the ability to operate production applications, databases, and networks in a highly available, fault tolerant and scalable manner as availability zones are connected via fast, private fiber-optic networking that enable fail-over between availability zones without interruption. Currently, the primary points of delivery for MESH services in the United States are from Azure US regions located in Virginia, Oregon, and Ohio. MESH makes use of multiple availability zones within a region. Outside of the US, MESH services are delivered from Azure regions in Montreal, Frankfurt, London, São Paulo Singapore, and Sydney.

GLOBAL ACCESS

SCALABILITY

HYBRID CAPABILITY

SECURITY

Azure

FLEXIBILITY

AWS, other cloud providers, and SaaS apps

Azure

VMs WITH ASC AGENTS INSTALLED

Collector Proxy (Optional)

AZURE SECURITY CENTER

AZURE SECURITY CENTER DASHBOARDS

HTTPS USED BY AGENTS

LOG ANALYTICS WORKSPACE

On Premises

AZURE STACK

OTHER SYSTEMS WITH ASC AGENTS INSTALLED
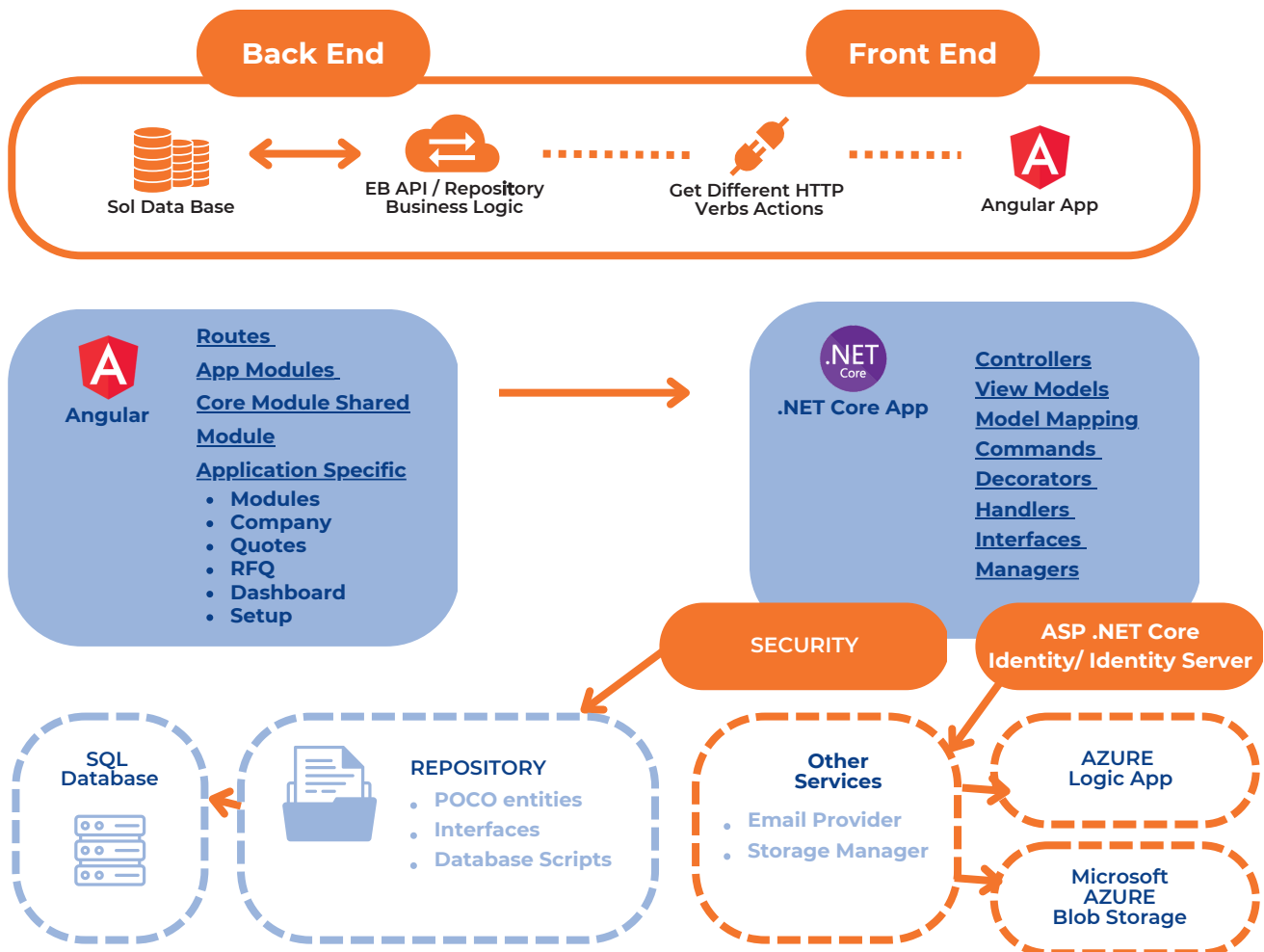
AZURE SENTINEL (SIEM & SOAR)

# Security

MESH takes the responsibility of ensuring the protection of customer data very seriously and is the reason why we have created comprehensive information security and privacy programs to safeguard your data and the systems used to process data. MESH undergoes regular external audits designed to thoroughly test our systems and internal control.

## Logical Data Separation

The data of every customer is completely separated from another customer. This includes all application data, databases, log data, and backup data. This total separation makes it impossible for one customer to accidentally access another customer's data.

## Data Encryption

MESH uses industry standard TLS encryption for data in transit. All connections from the web browser to the application are via secure HTTPS TLS 1.2 connections. Key exchanges done via the web browser are based on 2048-bit certificates (SHA256withRSA). Industry leading AES 256-bit encryption is used for data at rest, including any replicated archived backup data. Encryption keys are managed using enterprise grade cloud HSMM, rotated on a regular basis and under continuous monitoring.

**Back End** **Front End**

Sol Data Base ⟷ EB API / Repository Business Logic ⋯ Get Different HTTP Verbs Actions ⋯ Angular App

**Angular**

Routes
App Modules
Core Module Shared
Module
Application Specific
- Modules
- Company
- Quotes
- RFQ
- Dashboard
- Setup

**.NET Core App**

Controllers
View Models
Model Mapping
Commands
Decorators
Handlers
Interfaces
Managers

SECURITY

ASP .NET Core Identity/ Identity Server

SQL Database

REPOSITORY
- POCO entities
- Interfaces
- Database Scripts

Other Services
- Email Provider
- Storage Manager

AZURE Logic App

Microsoft AZURE Blob Storage

# Application Security

MESH is delivered as a web application which requires no elevation of privileges on the client machine to install additional software.

## User Authentication

Access to MESH requires that all users authenticate themselves using a business email address from their organization and a secret password known only to the user. All failed login attempts are logged with mechanisms in place to prevent brute force attacks by locking down accounts after multiple failed login attempts.

## Single Sign On Through SAML

For organizations who have their own identity provider, MESH supports identity federation through SAML2. Using SAML2, organizations can centralize their management of users to the application and permit single sign on capabilities.

## Password Policy

MESH also enforces minimum password length, complexity, and reusability rules in accordance with ISO 27001 standards. By default, passwords set by the user must contain at least 10 characters, contain an uppercase, lowercase character, and numbers. Passwords are never stored in plain text. Instead a salted hash is stored in the MESH database.

## Authorization

Role-based application level security is a core component of MESH which permits the assignment of functional roles to users by application administrators. MESH administrators can designate specific application functions to users based on roles and define data access permissions.

## Secure Cookie Management

MESH requires the use of secured cookies by default and directs browsers not to expose cookies through channels other than HTTPS requests.

## Audit Logging

MESH offers a robust logging framework for security events including the addition or removal of users, changes to user access levels, roles, and access to functional capabilities. This is in addition to recording all logins, logoffs, and failed logins.

## Backups, Redundancy, and Recovery

All application data in the MESH is automatically backed up at least twice daily to multiple regions. Full system-level backups are performed daily and weekly with 30 days of retention to ensure a recovery point objective (RPO) of no more than 12 hours. In the unlikely event of a total service disruption in an entire AWS region, an alternate geographic region can be used to provide continuity of services. A full system recovery at the alternate disaster recovery region will take place in no more than 6 hours (Recovery Time Objective).

## Data Encryption

MESH uses industry standard TLS encryption for data in transit. All connections from the web browser to the application are via secure HTTPS TLS 1.2 connections. Key exchanges done via the web browser are based on 2048-bit certificates (SHA256withRSA). Industry leading AES 256-bit encryption is used for data at rest, including any replicated archived backup data. Encryption keys are managed using enterprise grade cloud HSMM, rotated on a regular basis and under continuous monitoring.

## Network Security

MESH utilizes a layered network security architecture which includes perimeter/edge firewalls, web application firewalls (WAF), instance-based firewalls, and intrusion detection systems (IDS).

Firewalls are set to deny traffic by default, and will only accept traffic on designated open ports and whitelisted IP addresses. The principle of least privilege is enforced on firewall rules to ensure that unused ports are closed and protocols are denied.

The WAF's ruleset aligns to OWASP Top 10 issues based on both standard rulesets. The WAF is actively monitored, with alerts going to the security operations team in real-time for analysis and action.

## Advanced Threat Detection, Monitoring, and Alerting

A dedicated security team monitors all network and system activity in the MESH Cloud. An advanced Security Information and Event Management (SIEM) system is leveraged to provide full visibility into the MESH infrastructure. This centralized system aggregates all logs created by host operating systems, network firewalls, load balancers, cloud infrastructure events, and installed software. The collected data is correlated and analyzed in real-time against known and emerging threats to provide total security awareness.

Advanced threat detection and analysis helps safeguard data and provides a level of threat intelligence that is often beyond what customers are capable of receiving in their own IT environments, as SIEMS are costly to deploy, and operate with limited trained resources.

As the SIEM is operating in real-time, any anomalous activity is immediately highlighted and security personnel are alerted to conduct further analysis. The real-time nature of threat analysis ensures that security incidences are detected as early as possible to prevent and minimize any potential data exfiltration. For example, if a MESH user is known to login from Los Angeles, and suddenly on the same day logs in from South Africa, the SIEM generates an alert which is investigated by the security team.

## Production Infrastructure Access Control

Strict controls are in place to limit access to the MESH production infrastructure. MESH incorporates the concepts of 1) least privilege access, 2) separation of duties, and 30 information classifications as part of its information access and control policy. Management of access controls includes executive management approval for all access to the MESH infrastructure and regularly scheduled reviews, to ensure they are accurate and up to date. Two-factor authentication is required to access and manage the cloud infrastructure at all times.

## Operational Security

MESH has implemented extensive operational controls to address requirements for the timely execution of activities and the ability to review operational effectiveness. Operational controls include:

- Up-to-date documentation and runbooks on critical processes and procedures.

- A formal change management process based on ISO27001:2013 ISMS standards with a dedicated change review board.

- Fully isolated production, pre-production, and UAT infrastructures with strict access controls prevent unauthorized or accidental changes being propagated to production.

- Automated and scheduled tasks.

- Continuous infrastructure, application, and task monitoring.

- Extensive employee background checks and mandatory security awareness training.

## Infrastructure Best Practices

The MESH production infrastructure has been hardened against baselines established by the Center for Internet Security (CIS). Active anti-virus software is deployed and updated regularly to ensure the latest malware is detected. Regularly scheduled patching of the OS and dependent application software is practiced.

## Penetration & Vulnerability Prevention

MESH leverages a variety of technologies, tools, and techniques to provide broad coverage against various types of threats. The MESH environment and application code base is regularly scanned for vulnerabilities. Third party vendors are also contracted to perform regular security vulnerability assessments and annual penetration testing on the MESH infrastructure.

# Development Process

## Agile Development

To support the rapid pace of development necessary for delivering a SaaS solution, MESH has embraced an agile development methodology, and its principles of continuous integration and continuous development. This is the only way to support the MESH commitment to delivering regular, high-quality updates multiple times a year to the MESH Cloud.

## Automated Testing

A large automated test infrastructure with broad testing coverage supports the development of MESH Cloud. Through test automation, thousands of tests are run each time code is updated to ensure that new features perform to specifications and no regression to existing functionality is introduced.

## Secure Development Methods

MESH includes security resources and reviews as part of the development process. Security vulnerabilities are regularly monitored using automated static code analysis tools with results analyzed by the internal information security team. No code is released to production without undergoing a code analysis.

## Secure Developer Training

The development and QA employees at MESH have undergone certified secure software lifecycle training that includes:

- Secure software concepts
- Secure software design
- Secure software coding
- OWASP (Open Web Security Project) Top 10
- Defending .NET