Total ETO Managed Cloud Deployments

Platform Overview

Version 1
June 2026

Executive Summary

Total ETO is a software platform built specifically for engineer-to-order (ETO) manufacturers. It is delivered as a fully managed, cloud-based service. Your team uses the software while we manage the underlying infrastructure, security, backups, monitoring, and platform maintenance.

This document provides an overview of how the Total ETO Managed Cloud platform is hosted, operated, and secured.

In summary:

1. Customer environments are hosted entirely within Microsoft Azure.
2. Customer environments are isolated from one another.
3. Production environments target 99.9% uptime.
4. Backups and recovery processes are automated and monitored continuously.
5. Data is encrypted both in transit and at rest.
6. Administrative access is tightly controlled, time-limited, and logged.
7. Monitoring and incident response processes operate 24/7 for production systems.
8. Infrastructure changes are performed through controlled deployment pipelines rather than manual server configuration.

1. The Total ETO Managed Cloud Service

Total ETO Managed Cloud delivers the Total ETO application as a fully managed service. Each customer receives their own application instance and dedicated database, accessed securely through a web browser at their own site address.

Our team manages the servers, networking, security, backups, monitoring, and application updates behind the service, so your team can focus on using the software.

Customers with specific isolation or compliance requirements can be hosted on dedicated infrastructure.

2. Where Your Data Lives

Total ETO environments are hosted exclusively on Microsoft Azure. Azure provides the underlying physical infrastructure, networking, and datacenter operations used by the platform.

Microsoft Azure maintains a broad set of industry certifications and compliance programs, including SOC 1, SOC 2, SOC 3, ISO 27001, and FedRAMP authorizations.

Key details about customer environments:

1. Each customer environment operates in logically isolated infrastructure and databases separate from other customers.

2. Customer environments are hosted in Microsoft Azure in the customer's country where a suitable supported region is available. Where no suitable in-country region is available, customer environments may be hosted in a geographically nearby region.
3. Backups are retained within the same geographic region as the primary environment unless otherwise requested or contractually required.
4. Infrastructure configuration is managed through version-controlled deployment pipelines and infrastructure-as-code processes. Production infrastructure is not routinely modified through direct manual server administration.
5. Production, QA, and Development environments are isolated from one another with separate credentials and permissions.

At this time, Total ETO does not operate or manage physical datacenter infrastructure directly. Physical security controls are managed by Microsoft Azure as part of the underlying cloud platform.

3. Availability & Uptime

Total ETO targets 99.9% uptime for production environments, excluding scheduled maintenance windows and external dependency failures outside our operational control.

A 99.9% availability target corresponds to approximately:

* Less than 44 minutes of unplanned downtime per month

Planned maintenance windows are communicated in advance whenever practical.

Availability targets are operational objectives unless otherwise defined in customer agreements or service-level contracts.

4. Backups & Recovery

Total ETO maintains layered backup and recovery processes intended to support operational recovery from infrastructure failure, corruption, accidental deletion, or other service-impacting events.

Backup Type	Frequency	Retention
Full VM Backup	Daily	14 days daily, 4 weeks weekly
Full Database Backup	Daily	14 days daily, 12 weeks weekly
Database Transaction Log	Every 2 hours	7 days
Instant Recovery VM Snapshots	Daily (with each backup)	7 days

Backups are monitored automatically. Failed or incomplete backup operations generate alerts for operational review.

Recovery Objectives

Our current operational targets are:

1. Recovery Point Objective (RPO): up to 2 hours of potential data loss in a severe recovery scenario.
2. Recovery Time Objective (RTO): restoration of core production services within approximately 2 hours following confirmation of a qualifying infrastructure or platform incident.

These values are operational targets rather than guaranteed service-level commitments unless otherwise specified in customer agreements.

Recovery capabilities are validated through routine operational restore activity and ongoing operational review.

5. How We Protect Your Data

Network Protection

Traffic destined for customer environments passes through multiple layers of Azure network and edge protection before reaching the application.

These protections include:

1. Distributed Denial of Service (DDoS) mitigation through Microsoft Azure network protections.
2. Web Application Firewall (WAF) filtering to help identify and block malicious or abnormal HTTP traffic patterns.
3. Network access restrictions and filtering rules based on approved services, ports, and protocols.
4. Geographic traffic restrictions where appropriate to reduce exposure from regions where customer users do not operate.
5. Default-deny network rules. Services and ports must be explicitly permitted before traffic is allowed.
6. Administrative management ports are not exposed directly to the public internet.

Where possible, administrative operations are performed through secured management workflows rather than persistent externally accessible administrative endpoints.

Encryption

Customer data is encrypted both while in transit and while stored.

Data in Transit

1. Communication between users and the platform uses TLS 1.2 or higher.
2. Older or deprecated encryption protocols and cipher suites are disabled where supported by the platform and Azure services.
3. Administrative and service-to-service communications also use encrypted transport methods.

Data at Rest

1. Databases, storage volumes, backups, and temporary storage locations are encrypted at rest using Azure-managed encryption capabilities.
2. Backup data remains encrypted during storage and recovery operations.

Secrets and Credentials

1. Passwords, API keys, certificates, and application secrets are stored in Azure Key Vault or equivalent protected secret-management systems.
2. Secrets are not stored in source code repositories.
3. Sensitive credentials are masked or restricted within operational tooling where possible.
4. Privileged credentials are rotated periodically or regenerated as part of operational maintenance activities.

6. Administrative Access & Privileged Operations

Total ETO operates using a least-privilege access model.

Team members do not maintain unrestricted standing administrative access to customer production environments. Access to production systems is controlled through approval workflows, time-limited elevation, and audit logging.

When administrative access is required:

1. A request must be submitted with a documented operational or support reason.
2. Access requests require authentication and approval through administrative workflows.
3. Access is time-limited and automatically expires after a defined period.
4. Administrative activity is logged and retained for operational review, investigation, and audit purposes.

Privileged access usage is reviewed regularly through automated reporting and operational monitoring.

Application and Database Access

Applications use dedicated service accounts with scoped permissions appropriate for their operational role.

Application service credentials are configured to:

1. Access only required systems and services.
2. Avoid unnecessary administrative permissions where possible.
3. Prevent direct modification of database structure or platform administration functions from standard application credentials.

7. Monitoring & Incident Response

Platform Monitoring

Production systems are monitored continuously for operational health, availability, and security-related events.

Monitoring includes:

1. Infrastructure resource utilization and performance
2. Application errors and service degradation
3. Azure platform health notifications
4. Backup failures
5. Security-related alerts generated through Microsoft Defender for Cloud and related tooling

Operational alerts are routed through on-call escalation processes for investigation and response.

Automated application-layer security testing is also performed as part of ongoing security operations.

Incident Classification & Response

Incidents are prioritized based on operational severity and customer impact.

Severity	Response Target	Escalation
Critical — outage, data-loss risk, or security event	Immediate response and escalation	Phone, SMS, email, PagerDuty
High — significant degradation of normal use	Response same business day	Ticket system and operational escalation
Medium — limited-impact issues	Next business day	Ticket system
Low — minor or routine items	Scheduled operational handling	Ticket system

For significant operational or security incidents:

1. Internal incident tracking and review processes are initiated.
2. Corrective actions are documented and tracked.
3. Post-incident reviews are conducted for major incidents to identify contributing factors and preventative improvements.

If a customer-impacting security incident occurs, customer notification procedures are handled in accordance with contractual and legal obligations applicable to the affected environment.

For service-affecting incidents, status updates are available through our standard support channels.

8. System Maintenance & Change Management

Scheduled Maintenance

Security and infrastructure updates are applied on a scheduled maintenance cycle.

Standard maintenance windows currently occur:

* Wednesdays between 2:00 AM and 5:00 AM, local time for your hosting region

Maintenance activities may include:

1. Operating system security updates
2. Infrastructure component updates
3. Critical vulnerability remediation
4. Platform reliability improvements

Emergency security updates may be deployed outside standard maintenance windows when required to address elevated risk or active vulnerabilities.

Patch compliance and update status are monitored through automated reporting processes.

Servers or services are restarted only when required by the update or remediation process.

Change Management

Infrastructure and platform changes follow a controlled deployment process intended to reduce operational risk and maintain deployment consistency.

The general deployment workflow includes:

1. Planning and scope definition
2. Peer review and approval
3. Automated validation and testing checks
4. Controlled deployment through deployment pipelines
5. Post-deployment verification and monitoring

Changes to production systems are tracked through operational change records and deployment history.

9. Customer Responsibilities

Total ETO manages the underlying platform infrastructure and operational environment. Customers remain responsible for certain areas within their own organization, including:

1. Managing internal user access approvals
2. Maintaining secure endpoint devices used to access the platform
3. Using strong passwords and multi-factor authentication where enabled

4. Reviewing user permissions periodically
5. Managing exported data outside the platform environment

Security is a shared responsibility between the platform provider and the customer organization.

10. Support & Contact Information

For operational support, security questions, or incident reporting:

Channel	Details
Support Email	support@totaleto.com
Support Portal	https://totaleto.itclientportal.com
Support Phone	1.855.780.8973 ext. 2
Standard Support Hours	Monday–Friday, 8:00 AM – 5:00 PM ET
Critical Incident Monitoring	24/7/365

Document Notes

This document is intended as a general overview of the Total ETO Managed Cloud platform and its operating practices as of the publication date.

Security controls, operational processes, infrastructure architecture, and recovery procedures may evolve over time as part of ongoing platform improvements and changing security requirements.

Additional documentation, policies, or security review materials may be available under NDA or during formal customer onboarding and procurement processes.