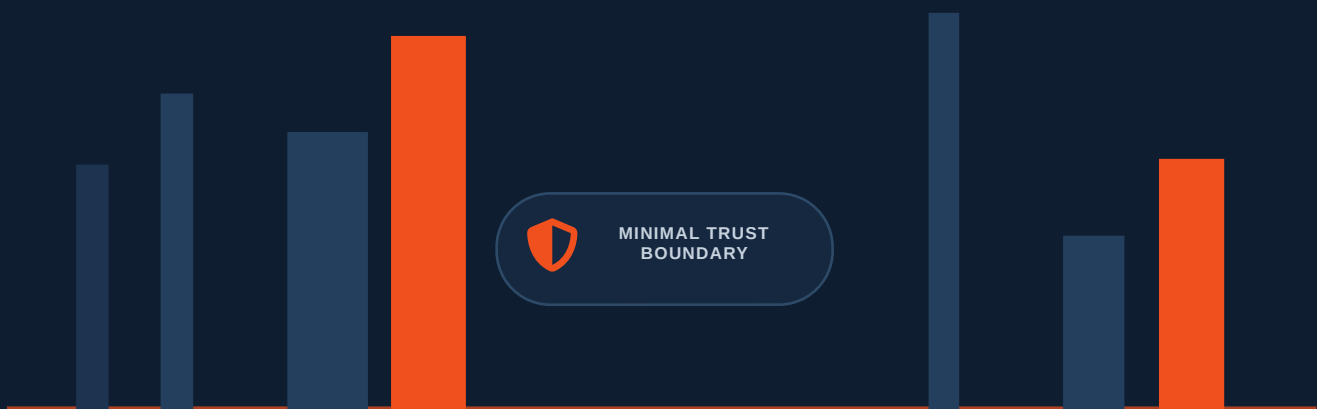




SECURITY & ACCESS ARCHITECTURE

A minimal-access approach to turnaround software.

No ERP credentials. No inbound firewall access. No OT connectivity required.





JUSTIFY THE ACCESS. NOT JUST THE CONTROLS.

Refinery IT and cybersecurity teams should scrutinize every external application introduced into the environment. The review should begin with one architectural question: what access does the application actually require?



SAP OR ERP CREDENTIALS

NOT REQUIRED



CUSTOMER-ENVIRONMENT SERVICE
ACCOUNT

NOT REQUIRED



INBOUND FIREWALL ACCESS

NOT REQUIRED



PERSISTENT ERP CONNECTIVITY

NOT REQUIRED



OT OR CONTROL-SYSTEM CONNECTIVITY

NOT REQUIRED



A third-party application should justify the access it requires, not simply the controls surrounding that access.

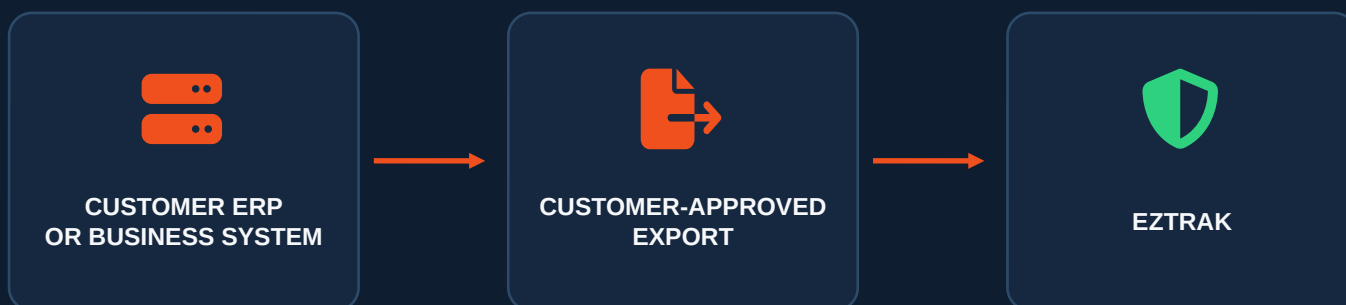
Customer-approved export/import is the default model. Automated integration is optional.



CUSTOMER-CONTROLLED BY DEFAULT.

EZTRAK does not require direct access to a customer's ERP or other enterprise systems to function. Authorized customer personnel decide what information crosses the boundary, when it is transferred, and who is permitted to provide it.

DEFAULT DEPLOYMENT MODEL



NO EZTRAK ERP CREDENTIALS REQUIRED



OPTIONAL INTEGRATION

CUSTOMER DECISION

When automation provides value, interfaces are limited to the workflows and data exchanges authorized by the customer. Broad access into the source environment is not required.

ACCESS REQUIREMENTS

SAP / ERP credentials

NOT REQUIRED

OT connectivity

NOT REQUIRED

Service account

NOT REQUIRED

Persistent ERP connection

NOT REQUIRED

Inbound firewall access

NOT REQUIRED

Automated integration

OPTIONAL

SEPARATE FROM OT. BY DESIGN.

EZTRAK supports planning, readiness, material management, cost control, field execution, equipment management, and contractor coordination. Those business workflows do not require connectivity to refinery operational technology.



EZTRAK BUSINESS APPLICATION

- Planning & readiness
- Material management
- Cost control
- Field execution
- Equipment & contractors



NO CONNECTION
REQUIRED



REFINERY OT / CONTROL SYSTEMS

- Distributed control systems
- Safety instrumented systems
- Process control systems
- Other OT environments

WHAT THIS MEANS FOR THE SECURITY REVIEW

The platform is evaluated as a business application without introducing required connectivity into the refinery OT environment.

The platform is not designed to operate industrial equipment or communicate with process-control infrastructure.





ACCESS FOLLOWS THE ROLE.

Users receive access according to their responsibilities within the platform rather than unrestricted access to every function and record.



ROLE-BASED ACCESS

Permissions are scoped to the user's responsibilities within the platform.



SAML SINGLE SIGN-ON

Authentication can be managed through the customer's identity provider.



MULTI-FACTOR AUTHENTICATION

An additional authentication factor strengthens account access.

TEMPORARY AND CONTRACTOR ACCESS



01

APPROVAL REQUEST

Access is requested for a defined operational need.



02

DEFINED DURATION

The authorized period is established in advance.



03

ACCESS EXPIRES

Access ends when the approved period concludes.



04

NEW APPROVAL

Continued access requires a new request and approval.

A defined lifecycle reduces reliance on manual account cleanup after the event.



PROTECT THE DATA. RECORD THE ACTION.

Security controls apply to customer information in storage, in transit, and during authorized platform activity.



ENCRYPTION

AES-256

AT REST

TLS 1.2+

IN TRANSIT



USER TRANSACTION AUDIT TRAIL



WHO

The user performing the action



WHAT

The affected record or transaction



WHEN

The time the action occurred



INTERNAL PRODUCTION ACCESS

RESTRICTED BY ROLE

Production access by EZTRAK personnel is restricted by role and limited to authorized personnel with an operational need.

These controls limit unnecessary access within both the customer user population and EZTRAK's production-support environment.



U.S.-HOSTED. RECOVERABLE. MONITORED.

EZTRAK is hosted in Microsoft Azure in the United States, with production customer data hosted in U.S. environments.



AZURE

HOSTING PROVIDER

Microsoft Azure is EZTRAK's hosting subprocessor. A complete subprocessor list is available during security review.



U.S.

DATA RESIDENCY

Production customer data is hosted in U.S.-based environments.



DAILY

PRODUCTION BACKUPS

Production customer data is backed up daily.



24 HRS

RECOVERY POINT OBJECTIVE

The stated Recovery Point Objective is 24 hours.



CONTINUOUS AUTOMATED VULNERABILITY SCANNING

Dedicated customer environments are available where separation from a shared application environment is required.

**DEDICATED
ENVIRONMENT AVAILABLE**



ACT FAST. KEEP CONTROL.

EZTRAK maintains an incident-response process for suspected or confirmed security events affecting customer information.



72 HOURS

INCIDENT NOTIFICATION

Designated customer contacts are notified within 72 hours after EZTRAK confirms customer-data impact, or sooner where required by contract or law.



CUSTOMER-OWNED DATA

Information can be exported in standard formats, and EZTRAK supports the required transition process if the relationship ends.



DESKTOP, MOBILE & OFFLINE

Role-based permissions continue to govern access for field users in warehouses, laydown yards, fabrication areas, and execution environments.

INCIDENT-RESPONSE PROCESS



INVESTIGATE



ESCALATE



CONTAIN



REMEDiate



COMMUNICATE

Customer-specific notification requirements may also be incorporated into the applicable agreement or security addendum.

Data portability should not be used to create artificial commercial dependency.



CHALLENGE THE ARCHITECTURE.

EZTRAK does not expect IT or cybersecurity teams to rely on broad marketing statements. Customers should evaluate the actual architecture, access requirements, controls, and operating model.

01

Required and excluded system access

02

Data flows and integration architecture

03

Identity, permissions, and temporary access

04

Logging and internal production access

05

Hosting, residency, and environment separation

06

Encryption, vulnerability management, and recovery

07

Incident response, retention, deletion, and subprocessors

08

Data ownership and export



THE QUESTION BEHIND THE QUESTION

What systems, credentials, connections, and trust relationships must the customer expose for the application to function?



SECURITY FACTS

THE ANSWERS IN ONE PLACE.

A concise reference for architecture, access, hosting, identity, recovery, incident response, and customer control.

Hosting provider	Microsoft Azure
------------------	-----------------

Production data residency	United States
---------------------------	---------------

SAP or ERP credentials	Not required
------------------------	--------------

Customer service account	Not required
--------------------------	--------------

Inbound firewall access	Not required
-------------------------	--------------

OT connectivity	Not required
-----------------	--------------

Persistent ERP connection	Not required
---------------------------	--------------

Automated integration	Optional
-----------------------	----------

Role-based access control	Supported
---------------------------	-----------

SAML SSO	Supported
----------	-----------

Multi-Factor Authentication	Supported
-----------------------------	-----------

Temporary access expiration	Supported
-----------------------------	-----------

Encryption at rest	AES-256
--------------------	---------

Encryption in transit	TLS 1.2 or higher
-----------------------	-------------------

User transaction audit trail	Yes
------------------------------	-----

Internal production access	Restricted by role and operational need
----------------------------	---

Vulnerability scanning	Continuous automated scanning
------------------------	-------------------------------

Production backups	Daily
--------------------	-------

Recovery Point Objective	24 hours
--------------------------	----------

Incident notification	Within 72 hours of confirmed impact
-----------------------	-------------------------------------

Subprocessors	Azure hosting; complete list during review
---------------	--

Dedicated environment	Available
-----------------------	-----------

Mobile access	Supported
---------------	-----------

Offline operation	Supported
-------------------	-----------

Customer data ownership	Customer
-------------------------	----------

Standard-format data export	Supported
-----------------------------	-----------

SECURITY BEGINS BY MINIMIZING THE ACCESS AN APPLICATION REQUIRES IN THE FIRST PLACE.