opentext™

Solution overview

Unified Messaging for the Internet of Things

Extend business applications with messaging and orchestration to translate, route and govern disparate and legacy technology and gain visibility into enterprise IoT data

Integrate legacy and modern messaging technologies with any-to-any communication protocol from MQTT to FTP and many more

Automate processes and advanced rules on people, system and thing messages for greater business value

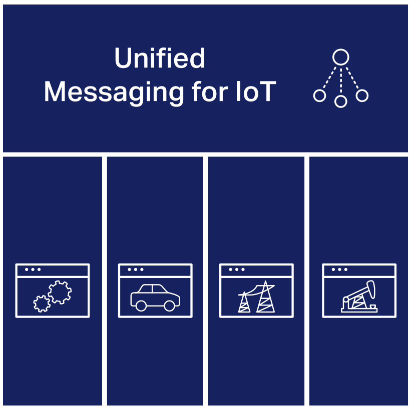
Ease IoT operations with transparency, governance, complete data tracking and visibility

Achieve enterprise-level performance and scale for millions of messages per second with no down time

Digitally transforming a business process is not easy. Connecting machines to systems and systems to people requires a methodical, purposeful approach to data management. As machines and things generate more and more data and new business models are realized, it is essential to secure and unify this critical information. Failing at this step is not an option if organizations want to maintain a competitive edge.

Forward-thinking leaders understand that connecting the myriad of people, systems and things that interact with the value chain can have a profound and positive impact on business. But, piecing together a solution with multiple standalone components or building their own solution takes a considerable amount of time and IoT expertise and often results in an error-prone system that is challenging to manage and not easily scalable.

Alternately, a cloud Platform-as-a-Service (PaaS) can be set up to manage entities and their relationships, the lifecycle of all connected entities, the orchestration of data streams and messaging for integration of systems and devices. The OpenText IoT Platform takes an identity-centric approach to IoT and enables enterprises to integrate legacy and modern messaging technologies and gather and track IoT data, avoiding the operational nightmare commonly associated with piece-meal IoT systems.



Aggregate information from disparate systems to obtain a single data feed for analysis or archive

Bridge the integration of legacy and modern messaging technologies

With any-to-any communication protocol from MQTT to FTP, Unified Messaging enables enterprises to perform rapid, secure and flexible integration of structured and unstructured data. This eliminates the cost and complexity of changing document types, data formats and protocols. It also removes the need for creating and syndicating integrations for machine-to-machine and application-to-application scenarios. With Unified Messaging, enterprises no longer need to create composite applications or manage disparate provisioning, authentication and authorization processes across complex ecosystems.

Achieve greater business value

A key component of Unified Messaging is an event data hub and processing engine that receives multiple streams of data with different protocols, persists the data, applies business logic and automatically routes it to the right recipient or application. As an IoT deployment grows or new services that require access to the IoT-sourced data are offered, organizations can leverage a pub-sub model for Unified Messaging that publishes data into a public queue to which new entities can subscribe.

Gain transparency, governance, complete data tracking and visibility

Secure Device Management and Unified Messaging enable the authorization security layer that acts as the gatekeeper for access to protected resources. When an application calls any API exposed through the OpenText IoT Platform on behalf of a user, system or thing, the authorization policy framework evaluates that API request and manages the authorization and access. This authorization security layer enables fine-grained traceability of messages for troubleshooting, auditing and billing. The platform captures IoT communications and transactions or system state changes and makes them available for replay and audit. With Unified Messaging, enterprises have visibility into what IoT data is doing and where it is going.

Get enterprise-level performance and scalability

The OpenText IoT Platform infrastructure-agnostic architecture is built on Cloud Foundry, which allows for solutions to scale dynamically, ingest data rapidly, upgrade with no downtime and run on any Infrastructure-as-a-Service (IaaS). Fine-grained audit and tracking for every event associated with a device provide complete transparency across the ecosystem.

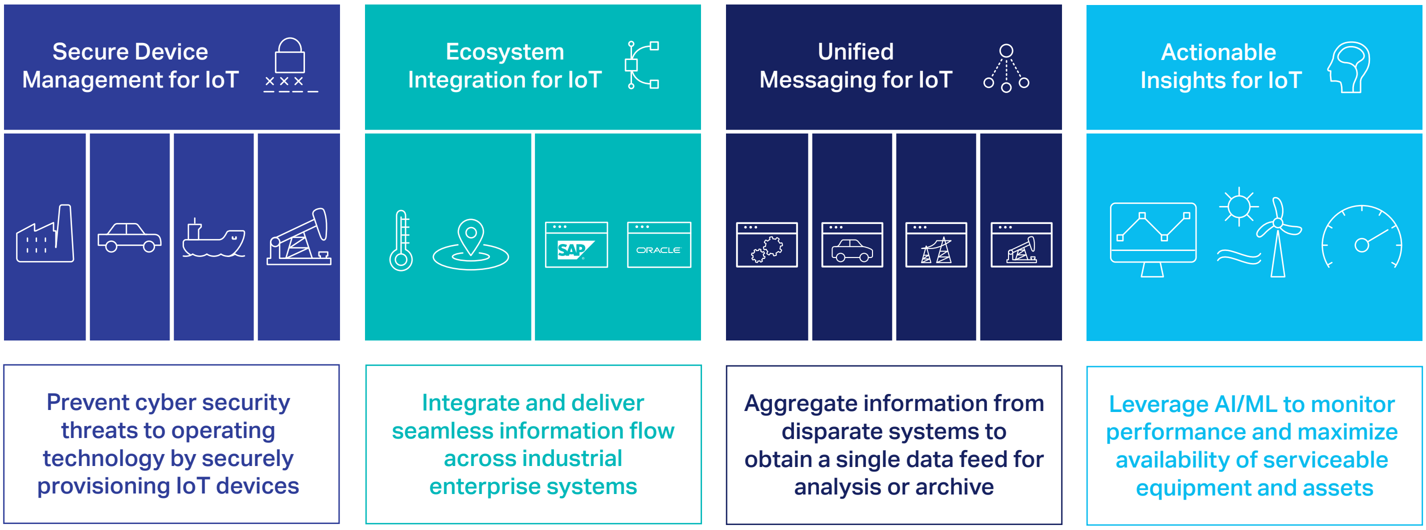
An identity-centric platform, designed with security for scalability and integration

OpenText's identity-centric approach to IoT makes its IoT platform unique and ready for integration with enterprise applications. The platform comes with advanced out-of-the-box identity and access management functionality, which would otherwise have to be built from scratch, consuming development time and taxing already strained IT budgets.

With the OpenText IoT Platform, organizations can register, authenticate and authorize all interactions across the entire lifecycle of people, systems and things. The ability to manage the identity of a device, sensor or machine throughout its lifecycle is critical to security across the entire ecosystem. Managing the relationship that an IoT data source or operator has with anyone or anything that it interacts with is what makes the OpenText IoT Platform uniquely capable to handle IoT initiatives requiring the highest level of security.

OpenText IoT

Embracing and extending business applications through an identity-centric approach provisioning people, systems and things



Secure Device Management for IoT

Prevent cyber security threats to operating technology by securely provisioning IoT devices

Ecosystem Integration for IoT

Integrate and deliver seamless information flow across industrial enterprise systems

Unified Messaging for IoT

Aggregate information from disparate systems to obtain a single data feed for analysis or archive

Actionable Insights for IoT

Leverage AI/ML to monitor performance and maximize availability of serviceable equipment and assets

Figure 1: In addition to Unified Messaging for IoT, the OpenText IoT Platform can also deliver Secure Device Management, Ecosystem Integration and Actionable Insights.

Unified Messaging seamlessly integrates enterprise data

Routing and orchestration

Robust enterprise service bus to transfer, route, prioritize and orchestrate messages

Transformation

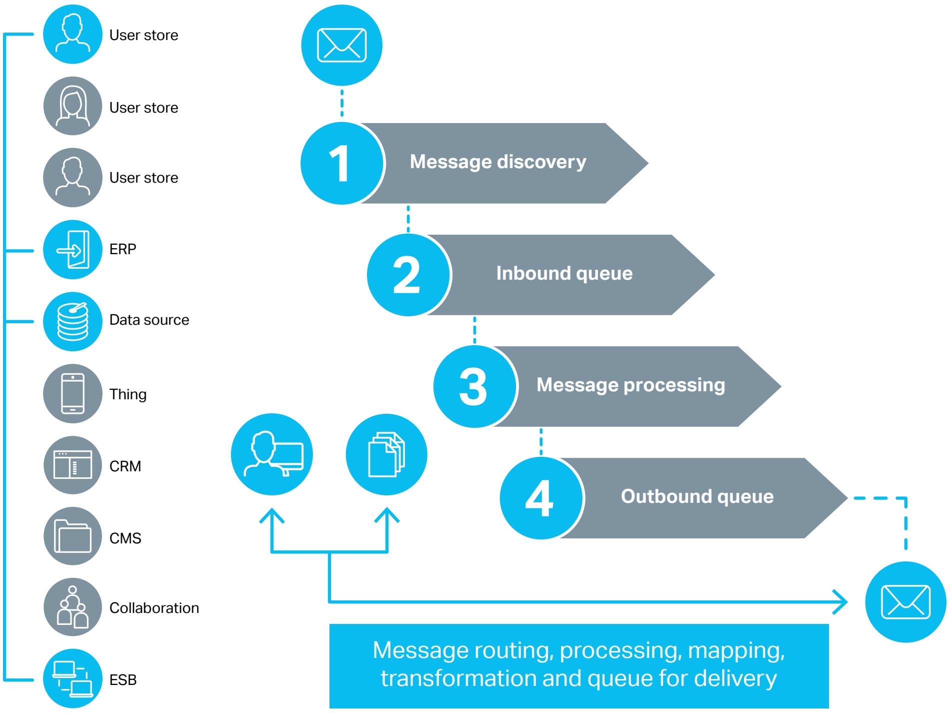
Flexible transformation of message payloads across document types, data formats and protocols

Integration

Enterprise adapters to ingest and publish data from/to third-party data stores and enterprise systems

Syndication

Synchronize and consolidate information across applications and sources



Message routing, processing, mapping, transformation and queue for delivery

Figure 2: A simple enterprise integration use case and sample capabilities of Ecosystem Integration.
Once the integration endpoint is set up, customers can manage integrations and track messages and failures.

Unified Messaging components

Routing and orchestration: A robust enterprise service bus transfers, routes, prioritizes and orchestrates messages

Rules and workflows	Configure rules and workflow to prioritize and trigger actions on messages (transformations, duplication checking, copying, enrichment) and route to appropriate channels
Dedicated queues	Manage customer and application-specific traffic using dedicated queues to isolate customer traffic, effectively manage customer-specific load and prevent erratic volumes by one customer from impacting other customers
Batch processing	Batch process multiple messages (zip, flat file, XML) into a single scheduled delivery with configurable delivery intervals and reporting capabilities on job execution
API orchestration	Create custom batching modules with simple Java coding Orchestrate API execution based on a customer-specific logic, e.g., API publishing, authentication and throttling
Business process management	Orchestrate seamless integration of business processes spanning multiple applications, harmonizing workflows independent of the underlying infrastructure and ensuring the right information is sent securely to the relevant processes on time
Event and notification hub	Collect, process, publish and/or route events and alerts based on threshold policies

Transformation: Flexible transformation of message payloads across document types, data formats and protocols

Protocol translation	Manage any-to-any protocol transformation and enable easy to configure, simple to use, scalable applications
Data translation	Translate data with a predefined library of existing data format converters Manage custom transformations (e.g., using XSLT) for conversion between formats, such as XML, JSON, CSV, X12, EDIFACT and HL7, for receiver and sender wires and encrypt and decrypt data
Copy and split	Create copies of a message and use parallel processing with rules for delivery to multiple systems Configure record terminators and delimiters for custom message splitting
Data enrichment	Configure lookup tables to pre-process, parse, map, package, post process, add or swap data on in-flight messages and view audit history of changes to the configuration
Multiple channel support	Configure and manage inbound and outbound communication channels with support for standards, such as SFTP, FTPS and HTTPS. The HTTPS channel also supports REST and SOAP variants
Synchronous and asynchronous processing	Process messages in a sequential or parallel manner for harmonized workflow execution

Integration: Use enterprise adapters to ingest and publish data from/to third-party data stores and enterprise systems

Enterprise adapters	Adapters ingest and publish data from/to third-party data stores and enterprise systems and integrate third-party web services Use the custom app protocol service (CAPS) endpoint to write custom adapters using the pub-sub model
Pub-sub engine	Publish and subscribe to events and exchange messages via this realtime messaging service, for example, the initiation of a device can generate an event with a payload to which a device or an API can subscribe Subscribers receive a subset of the total messages based on the filtering approach
Trading partner management	Configure and manage collaborating entities as trading partners, logically separate message traffic and establish messaging privileges between trading partners
File management	Manage file exchanges in multiple ways: Agent-based file transfer (SCOUT) enables automated file exchanges with external sites and periodic heartbeats enable the creation, installation and monitoring of SCOUTs and system health verification Other file management options include API-based file transfer, Messaging Hub (up to 10 MB) and the enterprise message bus (for EDI files)
Audit and traceability	Use the operations console to view messages, metadata, routing and control information, before and after transformations, command acknowledgments, detailed timestamps for all processing steps and root cause and traces of failed messages Messages are stored online for 15 days and offline for one year
Monitoring, metering and throttling	Configure monitors to track and alert on failures Alerting policies are configurable based on message type and priority Customizable groups allow failed messages to be routed to separate support teams and notifications can be delivered by email or REST-style HTTP callouts Monitoring supports policies around scheduled jobs and API throttling uses Apigee to manage load
Electronic data interchange (EDI)	Electronic interchange of business information uses a standardized format with support for machine-to-machine (traditional EDI), web EDI and a CSV messaging solution that translates CSV files to EDI

Syndication: Synchronize and consolidate information across applications and sources	
Event source hub	Use a pub-sub model for app-to-app data synchronization where a change in data triggers an event and event subscribers get the latest data
Authorization policy framework	An authorization security layer acts as the gatekeeper for access to protected resources When an application calls any API exposed through the OpenText IoT Platform on behalf of a user of the application, the authorization policy framework evaluates that API request and manages the authorization and access
Provisioning	Provisioning enables syndication of user, application and device profiles and authorizations across the digital ecosystem
Composite service creation	Service syndication implies that services do not act in isolation but interact and operate in concert with other services Smaller, lower-level services may aggregate to form a composite service that provides a composite unit of functionality to the consumer Composite services are created with the custom app protocol service (CAPS) and an orchestration engine
API security and syndication	API syndication allows enterprises to create and manage APIs once and then syndicate them into various internal and external developer communities, each with their own branding, licensing, security and other localized attributes Token services, such as JSON Web Token (JWT), Oauth and OpenID Connect (Oauth and SAML), can be made available to other services for authorization

Download the Identity of Things guide

Learn more

opentext.com/contact Twitter | LinkedIn