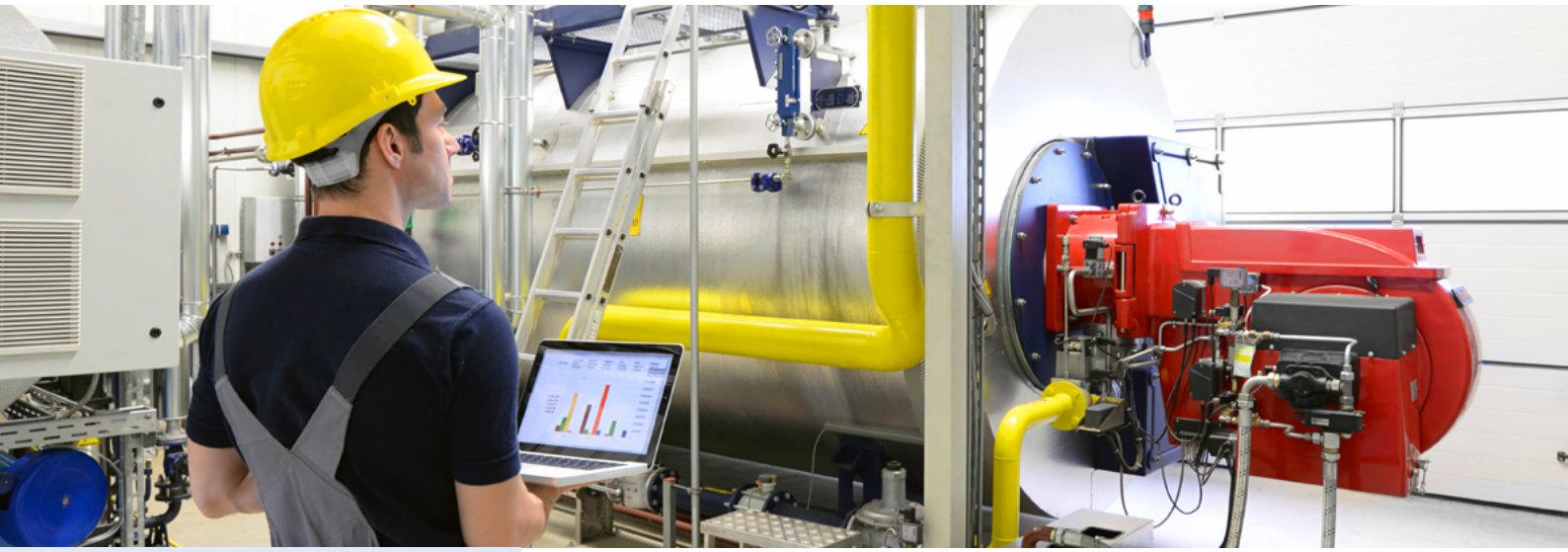
opentext™

Solution overview

Secure Device Management for the Internet of Things

Embracing and extending business applications begins with an identity-centric focus for people, systems and things



31 million digital identities managed—proven scalability

Data has no compass, it goes where it's told—give your IoT data clear direction

Visibility and delegated device administration for fine-grained control

The number of connected things in the world is expected to exceed 20 billion by 2020[1] and the sheer volume of identities will grow in parallel. For a manufacturer, a connected product means building a better, more valuable or sticky product and unlocking new service-based revenue models. For an owner/operator, a connected asset means increasing operational efficiency and improving services by optimizing use of the asset.

The challenge is the need to deliver trusted information to many mission-critical stakeholders. It is essential for owners and operators of product ecosystems to create and manage a network of physical objects that securely connect, communicate, collect data and intelligently distribute this data to create value. Without secure device management, IoT data and the processes that rely on it are at risk.

Business leaders understand that connecting the myriad of people, systems and things that touch the value chain can have a profoundly positive impact. They also know that piecing a solution together with multiple standalone components or building it themselves would take a considerable amount of time and resources, often more than they can spare, resulting in something that is error-prone, challenging to manage and not easily scalable. The solution is to give IoT the same attention and focus as other enterprise applications that drive innovation and enable timely business decisions.

[1]Gartner, Leading the IoT: Gartner Insights on How to Lead in a Connected World (2017) https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

opentext™

A digital twin is a digital representation of a physical object, instantiated as a software object that mirrors a unique physical object's characteristics and its state.

A connected ecosystem of people, systems and things requires intimate knowledge and expertise in each of these areas. It also requires the ability to purchase, code and maintain a string of components. Like organizations, people, applications and devices have a broad spectrum of attributes, and these entities and their relationships need to be carefully managed. Secure Device Management from OpenText standardizes how these device identities are represented, ensuring the highest level of integrity can be maintained at scale. Common entity definitions allow for consistent identity relationship behavior, versioning and extensibility.

OpenText: Delivering the promise of an Intelligent and Connected Enterprise

As the basis of a transformational digital strategy, Enterprise Information Management (EIM) helps consolidate information internally across silos and applications and digitize processes from end to end. Operations are more easily coordinated and streamlined throughout an ecosystem with digital consumers at its hub. At every stage in a product's lifecycle, operations can be automated and analyzed for deeper insights to improve efficiencies and output, as well as engagement with customers, partners and suppliers. Empowered with intelligence and connectivity from IoT, organizations can compete with agility, adapt to market changes and respond to opportunities for growth.

31+ million digital identities for proven scalability

OpenText, the market leader in EIM, understands digital and with the OpenText™ Covisint Internet of Things Platform, is uniquely equipped to deliver solutions to enable and empower the Intelligent and Connected enterprise. Managing more than 31 million digital identities, the Covisint IoT Platform has the proven scalability to deliver the Secure Device Management necessary for today's complex ecosystems of people, systems and things. It is this identity-centric approach to IoT and Secure Device Management that allows for the extension and integration of enterprise applications.

Data has no compass, it goes where it's told—give your IoT data clear direction

Managing, governing and auditing data, especially IoT data, is not easy—but getting started can be. Secure Device Management from OpenText makes it possible to create templates for devices, events, commands and even entire solutions. These digital twins of physical objects make it easy to visualize contextual data no matter where the device is located. Templates also make it easy to onboard new devices quickly, catalog attributes for future use and allow users to instantiate entire solutions based on prior models that have proven to be effective.

Gain visibility and delegated device administration for fine-grained control

As IoT deployments move from simple monitoring and failure alerts to more complex and sophisticated solutions, such as digital twins, organizations need to adopt an identity-first approach to ensure the data and devices they are extending are not at risk. Failure to adequately attest and verify the IoT device could lead to too much or too little access, hampering integration or possibly exposing data or the device to cyberattacks.

opentext™

The Covisint IoT Platform enables fine-grained control of IoT devices and data as new capabilities are developed and deployed. An example of this can be seen through the design, operation and augmentation of a manufactured product using a digital twin. As a product is in the design phase, data can be gathered, managed and analyzed by the appropriate personnel as defined by the product owner. This delegated device administration allows for specified data flows to be routed to where it delivers the expected results without extending the data broadly. Clearly defining the product's IoT data paths ensures data access is not considered noise by the uninterested or a security risk that accessible to the uninvited.

An identity-centric platform, designed with security for scalability

OpenText's identity-centric approach to IoT makes the Covisint 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 strained IT budgets.

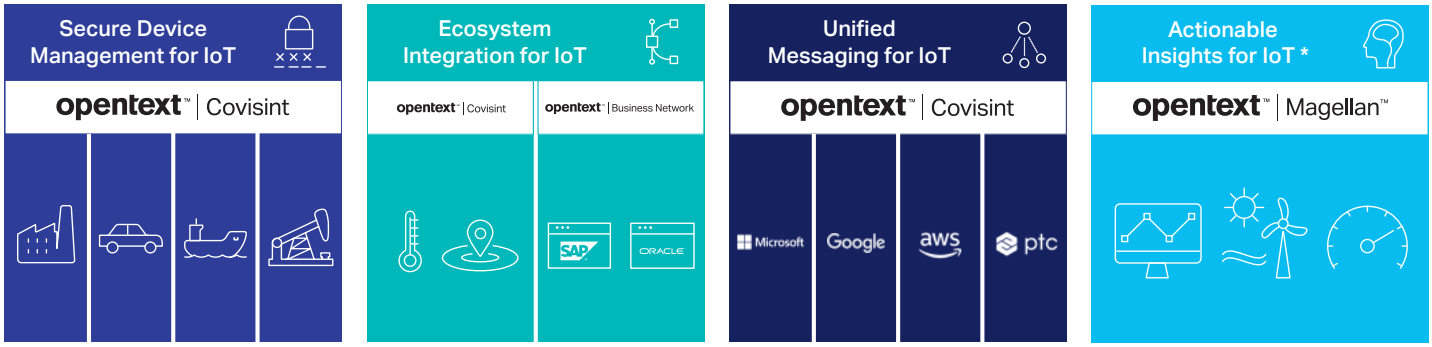
This is possible through relationship and lifecycle management, enabling organizations to register, authenticate and authorize all interactions across the entire lifecycle of people, systems and things. The ability to manage the identity of a device throughout its lifecycle is critical to the security across the entire ecosystem. Managing the relationship that a device has with anyone or anything is what makes the Covisint IoT Platform uniquely capable of handling IoT initiatives that require the highest level of security.

Power an intelligent supply chain

Leverage AI and IoT to create an intelligent supply chain that is at the heart of the digital ecosystem. In this white paper, learn:

- Six core services every IoT platform should deliver to drive security, innovation and connectivity.
- Eight benefits of integrating identity and access management (IAM) into an IoT platform.
- Three use cases: proactive replenishment, predictive maintenance and supply chain visibility.
- The latest IoT and IAM trends and best practices.
- The core capabilities that separate an industry-leading IoT platform from the rest.

Get the white paper, How IoT enables an Intelligent and Connected Supply Chain



Prevent cyber security threats across different industries by securely provisioning devices

Integrate to standard sensors and ensure seamless information flow across enterprise systems

Aggregate information from different IoT providers to obtain a single data feed for analysis or archive

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

* Future roadmap offering

opentext™

Learn more

OpenText Internet of Things »

Intelligent and Connected Enterprise »

Deliver a connected and intelligent customer experience

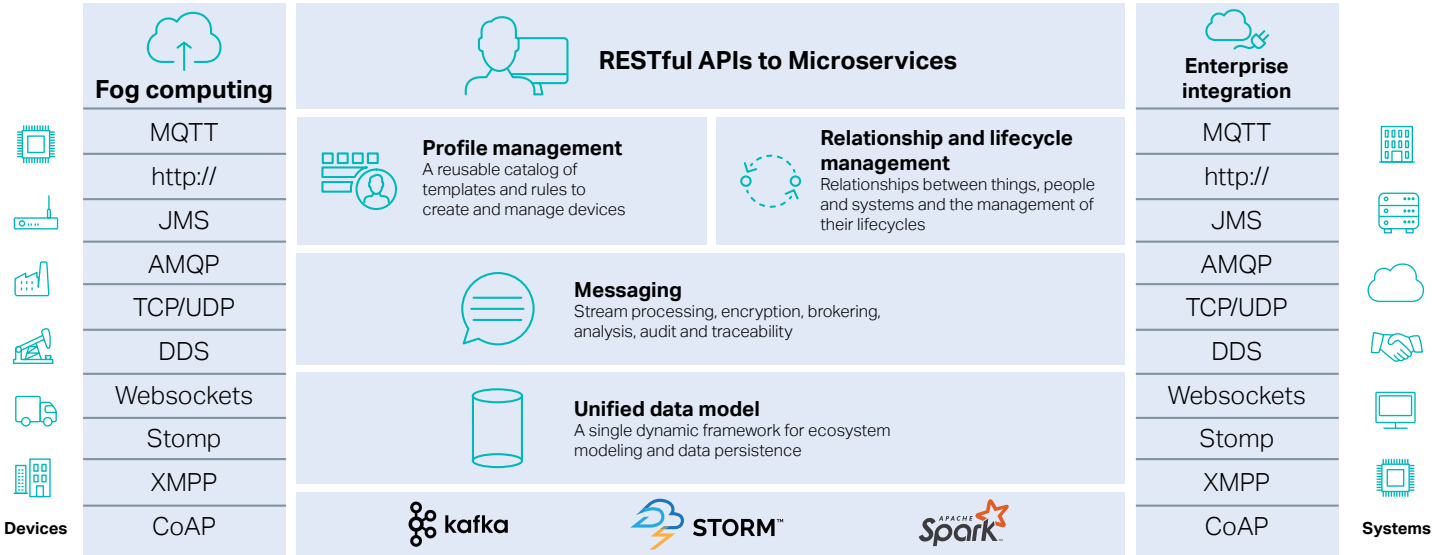
Today's manufacturers are sitting on a gold mine of IoT data that can be sent automatically from vehicles to numerous entities to enhance offerings and improve customer experience (CX). Through a combination of AI, IoT and analytics, automotive manufacturers and service providers can:

- Enable OEMs to quickly onboard partners, third-party application providers and systems that interact with the connected vehicle.
- Allow OEMs to centralize critical data about the connected vehicles for CRM, CX and quality monitoring purposes.
- Ensure the security of the data stream being transmitted to and from the vehicle, promoting customer safety and loyalty.
- Predict potential failure points and install proactive alerts that reduce vehicle downtime to improve customer satisfaction.

Download the guide

Secure Device Management components

Profile management	A reusable catalog of templates and rules to create and manage devices
Relationship and lifecycle management	Relationships between people, systems and things and the management of their lifecycles
Messaging	Stream processing, encryption, brokering, analysis audit and traceability
Unified data model	A single dynamic framework for encryption modeling and data persistence



Covisint IoT architecture

opentext.com/contact Twitter | LinkedIn