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 41.5 billion by 2025.[1] This doubles the number of connected devices from the initial 2020 estimate.[2] OpenText believes the 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.

Without secure device management, Internet of Things (IoT) data and the processes that rely on it are at risk.

Stats Source:

1.Worldwide Global DataSphere IoT Device and Data Forecast, 2019-2023, May 2019.

2.Gartner, Leading the IoT: Gartner Insights on How to Lead in a Connected World, 2017.

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.

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

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. Leveraging mobile device provisioning, field deployments of IoT devices is made easy and secure (see figure 1). 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.

The OpenText 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 is accessible to the uninvited or unqualified.