Identity of Things Explained

- Learn why the Internet of Things has an identity problem
- Understand the benefits of an identity centric IoT platform
- Select the right IDoT provider for your business

Contents

Introduction

The Internet of Things (IoT) is rapidly transforming almost every aspect of modern life. From monitoring our health to automating production lines, IoT devices are improving what can be achieved.

In fact, estimates suggest there will be more than 75 billion devices connected to the internet by 2025.[1] That represents 10 IoT devices for every human on earth.

British researcher Kevin Ashton coined the term IoT in 2009, while working on a project to connect different devices to the internet. With billions of devices now attached, the technical challenge has moved from making an effective and reliable connection, to managing and securing IoT devices and the vast amounts of data they create on a daily basis.

The foundation to managing IoT devices is built on uniquely identifying each and every one. This has become known as the Identity of Things (IDoT) and can be thought of as an extension to traditional identity and access management (IAM) for the internet era.

Traditional IAM was designed to manage the identity of users on a company network. It set up secure relationships between each user and corporate application and system. This approach was not designed to deal with the identity of ‘things’ or to manage the more complex relationships of creating an IoT ecosystem of people, systems and things.

IDoT has become essential for any IoT infrastructure to ensure secure connectivity and, most importantly, build trust in the data from IoT devices.

Today, IoT is often split into two separate but related types: consumer IoT, which includes IoT devices, such as smart appliances in the home, connected cars and wearable devices to monitor our health. The second type covers the industrial application of IoT in transforming business areas, such as factories and supply chains. This is known as Industrial IoT, sometimes called Industry 4.0, and is the focus of this guide.

About this guide

Identity of Things Explained, OpenText Special Edition, provides a guide to everything you need to know to start adding identity to the Internet of Things. This guide covers seven informative chapters:

- Introducing the Identity of Things (Chapter 1)
- The core capabilities of an identity driven IoT platform (Chapter 2)
- Challenges involved in IDoT (Chapter 3)
- Applying identity to Industrial IoT (Chapter 4)
- The benefits of IDoT (Chapter 5)
- Selecting the right IDoT provider (Chapter 6)
- The top 10 tips to consider when deploying IDoT (Chapter 7)

Who should read this guide?

This guide is designed to be accessible and readable for everyone, geared towards board-level and senior management of any business where IoT is becoming a major part of operations and business processes. But, it really benefits anyone who wants to understand more about the essential role of IDoT in delivering the opportunities offered by IoT.

1. IHS Technology, IOT platforms: enabling the Internet of Things (2016) https://cdn.ihs.com/www/pdf/enabling-IOT.pdf

Chapter 1

Introducing the Identity of Things

In this chapter

- Learn the definition of the Identity of Things (IDoT)
- Understand the difference between IAM and IDoT
- Learn about the core components of IDoT

The Internet of Things (IoT) has exploded over recent years. It has found practical application in almost every industry sector and walk of life. While the identity management requirements are similar for both consumer IoT and Industrial IoT, this guide is going to look at its application in business.

Today, as we add more and more 'things' to the internet, we are faced with a new set of questions: How do we recognize each device? How do we know what it is doing? And, how do we know who is using it? The Identity of Things (IDoT) is designed to give us the answers.

> ### A simple definition
>
> ***"IDoT assigns unique identifiers and metadata to things— devices, objects, etc.—enabling them to connect and communicate with other entities via the internet."***

This is one of those technology definitions that tells you everything and nothing. It describes how you use identity to connect things to the internet but does not explain how to handle an even more important aspect of IoT: The relationship between people, systems and things.

When you connect a device to the internet, you need to be able to identify it from any other device. You also need to know its purpose and who has the right to use it. That may be a fairly simple task when you only have a handful of devices to manage. But, the task grows exponentially complex as the number of devices multiplies.

The role of the majority of IoT devices is to produce data on a particular activity, function or process. So, now you have to manage that data as well. Who should have access to the data? How should that data be presented? What other systems will interact with that data?

Managing the identity of IoT goes far beyond the effective identification of things on the internet. It must facilitate a whole host of different relationships across this ecosystem of connected people, systems and things. Relationships can be simple, such as a single device connecting to another device, to highly complex, where multiple users, systems and things are inter-connecting and sharing data.

Identity management has traditionally been seen as an issue of security. IDoT is building upon these security capabilities to include relationship management, data protection, data integrity and business agility.

Moving beyond identity and access management (IAM)

Identity management is hardly a new concept. Organizations have long understood the need to allow privileged access to their staff, while ensuring the corporate network is protected from malicious attack, whether from inside or outside of the corporate firewall.

Identity and access management (IAM) is a technology area that has matured over decades. It is excellent at authorizing and authenticating the rights of people to access and use systems. However, it has always been focused on that closed relationship between people and systems on the corporate network.

In recent years, customer identity and access management (CIAM) has developed to accommodate organizations needing to increasingly give secure access to people on the other side of their firewall. However, CIAM is still primarily about securing the relationship between people and the systems they need.

Traditional IAM was not designed to accommodate the needs of connected devices. IoT has surpassed the capabilities of most IAM solutions. It is no longer enough to manage the identity of a person connected to a system, you have to manage the connection of a user connected to a device, a device connected to another device, a device connected to a system—or any combination in any volume of all those connections.

Traditional IAM cannot cope with the diversity of connections or the explosive growth of IoT networks.

The core components

While IDoT is the term used to describe the ability to manage the identity of all elements on an IoT network, it takes an identity-driven IoT platform (see Chapter 2) to deliver the necessary IDoT capabilities. It is the platform that dynamically connects and manages all the people, systems and things involved in the digital ecosystem of an IoT environment.

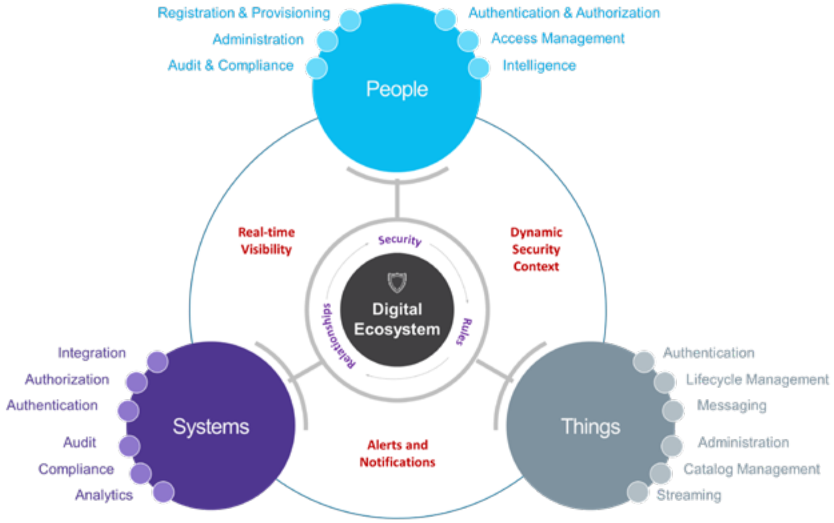


Figure 1-1: The identity-driven IoT platform allows you to manage the digital ecosystem of people, systems and things.

To meet business requirements, the identity-driven IoT platform should contain the following core components:

- **Dynamic client registration:** Every device and user on an IoT network has to be targeted and found. This requires that each element be properly registered on the platform. As the number of devices and users grows rapidly, registration must be dynamic and automated to allow the IoT infrastructure to scale. There are two important aspects to registration:
  - » **Device registration:** Every device must have a global unique identifier, such as the device's serial number, IP address, etc. A single identifier is unlikely to be enough to establish the required level of trust, so a number of identifiers are needed to establish authenticity. These identifiers, and other supporting data, must be captured during the registration process. The IoT platform holds all the registration information and conducts verification and reconciliation services to establish what devices are connected, whether they are the correct devices and what rights they have on the network.
  - » **User registration:** Each new user must be registered on the IoT network. User credentials must be established with strict and secure authorizations and access rights put in place. As customers, suppliers and contract workers demand more direct access to your networks, it becomes increasingly important to enable self-service registration.

- **Authentication:** Devices, users and systems must authenticate onto your IoT network. However, the type of authentication that you can use for each differs. The IoT platform must be able to accommodate the following types of authentication:

  - » **Device authentication:** When a device connects or transfers data, it needs to authenticate to prove it is real and has the rights to conduct that task. Credentials, symmetric keys or certificates can be used for authentication. Certificates, or tokens, offer high levels of security with long, unique identification numbers that can be automatically assigned and involve little human administration or computational power. Device authentication can be further strengthened using geo-location and behavioral analysis.
  - » **User authentication:** Users also need to authenticate when connecting to the network and accessing IoT devices. Simple credentials, such as user name and password, are vulnerable. Multi-factor authentication allows several different facets—for example, password, SMS notifications and biometric details—to be applied in combination to build trust that the user is who they say they are and that they have the correct rights.
  - » **System authentication:** System authentication is very similar to user authentication. Multi-factor authentication ensures that only the users and devices with correct rights and access can communicate with the system. It is likely that you will decide the level of authentication needed for a system based on how important that system is to your business and the sensitivity of the data that it contains.

- **Device data sharing:** The role of any IoT device is to capture and transmit data. You have to be sure the data is coming from a trusted source. Moreover, you must ensure that only authorized users and systems can gain access to that data. Data sharing rights can be established at registration and access control can be established through authentication. The platform has to ensure that these rights are easy for both humans and devices to understand, can be quickly changed or revoked and are sustainable throughout the lifecycle of the device.
- **Privacy management:** The data created by connected devices and shared across your IoT environment can include personal data on users and customers that has to be protected. You have to be able to set the correct privacy levels on all data created. Where appropriate, it may be possible to enable users to establish and manage their own data privacy preferences. However, these capabilities still have to be centrally managed to ensure you stay in compliance with your data management obligations.
- **Multi-layer relationships:** IoT creates a digital ecosystem that spawns new types of relationships, including device-to-device, device-to-user, user-to-user, device-to-system, etc. A user may own more than one device and a device may have more than one owner. IoT creates many-to-many relationships. For example, groups of devices can work together to provide a complete picture of a production line. In addition, relationships can be permanent or only temporary. The IoT platform must be able to manage all the concurrent relationships that happen on an IoT network at scale.

- **Certificate Management:** The use of certificates, or tokens, is a popular way to authenticate devices as it can build solid trust between the device and other elements connected to the network. The certificate management capabilities of the IoT platform should include:

  - » Platform-generated certificates: The IoT platform generates a unique certificate that is then loaded onto the device. In some cases, the IoT platform can relate the certificate to other device credentials to enhance security.
  - » Device-generated keys: The IoT platform generates the certificate and issues it to the device. In return, the device creates an asymmetric key that it shares with the platform to build greater trust.
  - » Third-party certificates: In some cases, IoT devices will use certificates from third parties. For example, some IoT devices will have certificates loaded at the factory. The IoT platform should be able to check and verify certificates issued by third parties and take over the management of those certificates.

- **Authorization:** The IoT platform must be able to maintain strict access control to everything attached to an IoT network. Authorizations have to be established at the device, data, user and system levels. Authorization has to be able to be granted, changed and revoked as required and at scale. In all instances, the minimum amount of access has to be granted in order for that function or task to be completed successfully.
- **Credential rotation:** Where a device is connected to your IoT network over extended periods of time, it is important to be able to rotate its credentials. For most IoT networks, the process of credential rotation will need to be automated. The IoT platform must, after a set period of time, install new credentials and disable the old credentials after the first instance of the new credentials being used.
- **Lifecycle management:** End-to-end lifecycle management is an essential capability of an identity-driven IoT platform. It must be able to quickly onboard new devices and users, assign their rights, monitor and manage their activities and de-provision devices and users to revoke all rights and permissions as soon as they do not need to be connected to the network.
- **Analytics and reporting:** All connections, interactions and transactions that take place over your IoT network must be monitored and analyzed to ensure security and network performance. The IoT platform must be able to track every device and its relationships to build a complete end-to-end picture of activity on your IoT network. Comprehensive logging and reporting is required to make this information available to the people who need it. Some IoT platforms offer visual dashboards to allow you to instantly see the current status of network activities.

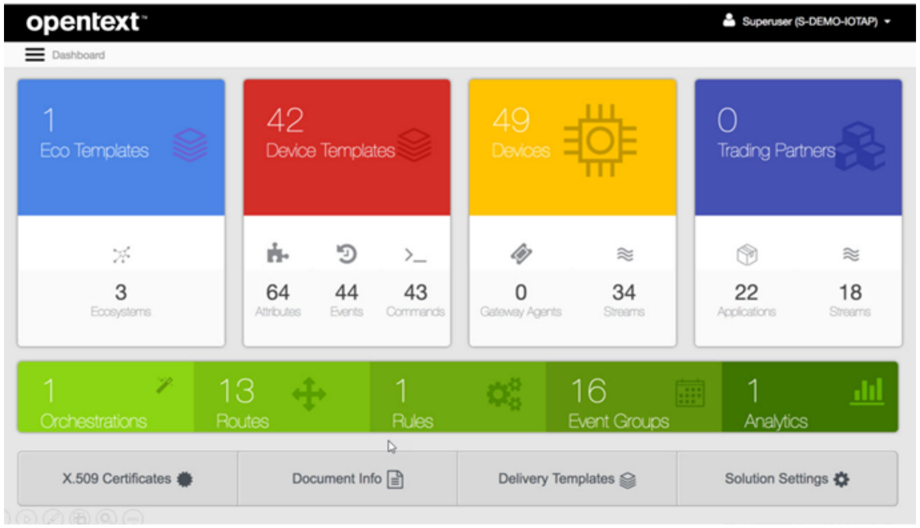


Figure 1-2: Easy to use dashboards allow you to see at a glance the status of your identity-driven IoT platform.

Chapter 2

The core capabilities of an identity-driven IoT platform

In this chapter

- Discover the key features of an identity-driven IoT platform
- Learn about its identity management and security capabilities
- Understand the available deployment models

As we have seen, every IoT network comprises a fragmented range of devices, software, communications protocols, people and systems. Achieving effective integration across this new digital ecosystem requires comprehensive identity management. Research shows that building this identity capability from scratch can consume as much as 40 percent of IoT development. The alternative is to deploy an identity-driven IoT platform from a leading provider.

Managing the digital ecosystem

The identity-driven IoT platform offers a foundation for organizations to create, secure and grow their digital ecosystems. It effectively manages the identities of the three key IoT network entities: connected people, connected systems and connected things.

Connected people: The platform creates a single digital identity for every person—employees, suppliers, partners, customers and contractors—who needs access to your IoT network and IoT-enabled products and services, such as the connected car. Identities are quickly—often automatically—provisioned, delivered, managed and governed securely and at scale.

Connected systems: The platform enables secure integration and information sharing between disparate systems over the IoT network. The data can be collected from a wide range of sources and presented in the right format to securely connect your IoT capabilities and enterprise systems, such as ERP or CRM systems.

Connected things: The platform supports and integrates any Industrial IoT device with which you need to connect and share information. It should be agnostic of device type, communications protocol or data standard. IoT devices and gateways can be seamlessly connected to people, enterprise applications and other things through standards-based, any-to-any integration in realtime.

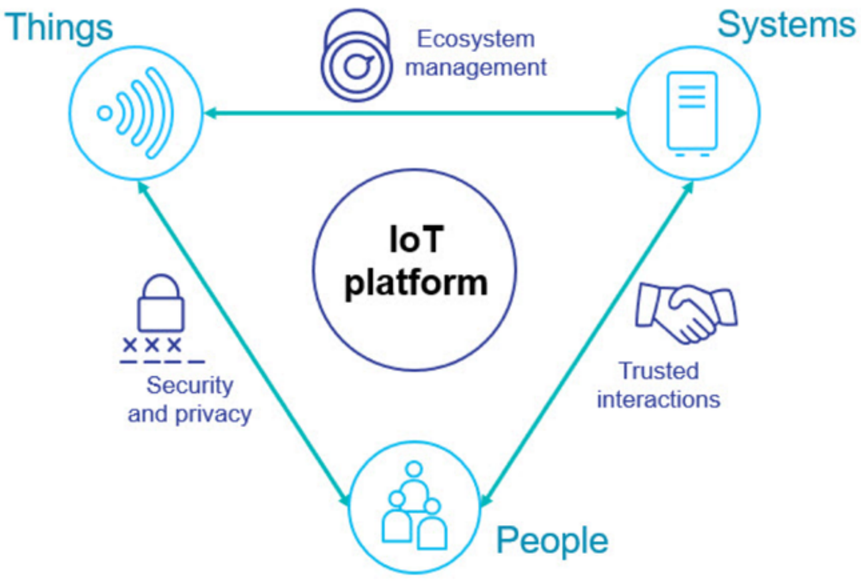


Figure 2-1: The identity-driven IoT platform helps create a digital ecosystem of connected people, connected systems and connected things.

The identity-driven IoT platform manages all identities and the complex set of relationships between the various entities. It establishes and enforces the access control and permissions necessary to govern network interactions and allow secure data flows.

The key features of an identity-driven IoT platform

It is important to note that security is not simply about letting the good guys in and keeping the bad guys out. In modern business, there are security implications involved in virtually everything you do. It is not enough to protect the endpoints on an IoT network.

The identity-driven IoT platform must include data management and relationship management functionality and easily adapt to the quickly changing IoT environment and evolving security threats.

There are six key features you should look for when selecting your platform:

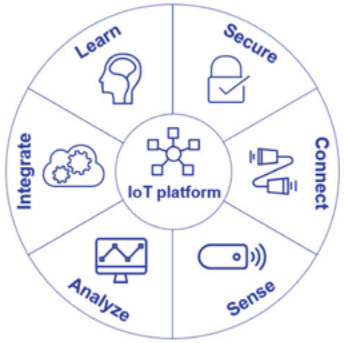


Figure 2-2: The six key features of an identity-driven IoT platform.

- **Secure:** The IoT platform must deliver comprehensive security to protect all IoT endpoints from external cyberattacks, as well as the potential for malicious activities from inside the organization. This requires scalable authentication, authorization and certificate management to guarantee the integrity and confidentiality of all interactions between entities on the IoT network.
- **Connect:** Each IoT device must be quickly and securely provisioned and managed throughout all lifecycle stages, including tracking and authorizing devices as they are provisioned, registered, activated, suspended, unsuspended, deleted and reset as required. The platform needs to provide a secure connection to IoT devices at both the physical layer, such as Wi-Fi or cellular communications, and the data layer, such as MQTT or HTTP.
- **Sense:** The platform should offer support for the widest range of industry-standard IoT devices, such as sensors, tags and beacons. It should automatically sense their presence on the network to establish a secure connection and quickly establish the device's credentials or automatically assign them where required.
- **Analyze:** The value of the IoT platform is in the ability to properly analyze the growing volume of information to uncover insight that improve data-driven decision-making. The sensor-based information from connected devices must be blended with other data sources to create a more rounded view of IoT network performance and the behaviors and activities of the entities attached to it.
- **Integrate:** Integration is one of the most important services within the IoT platform. Its API (applications program interface) functionality enables IoT devices to seamlessly and securely connect and share information with different enterprise applications, cloud services, mobile apps and legacy systems. In addition, the platform's messaging and orchestration capabilities provide the integration layer for transporting data and integrating across devices and systems, eliminating the complexity of creating and syndicating integrations for device-to-device, device-to-people or device-to-system.

- **Learn:** IoT is heavily event driven and the platform must be able to learn from events that occur on the network. This involves event processing and data aggregation from IoT devices and other information sources that feed its rules engine and decision processing capabilities to identify a recommended course of action. For example, an IoT device connects to the network once a day to transfer data to a maintenance system. If that device suddenly requests multiple connections, it can raise alarms around its unusual behavior.
- To achieve the six features outlined above, the IoT platform requires a range of components in two core areas: identity and security.

The core capabilities: Identity

An IoT platform should deliver the following identity capabilities:

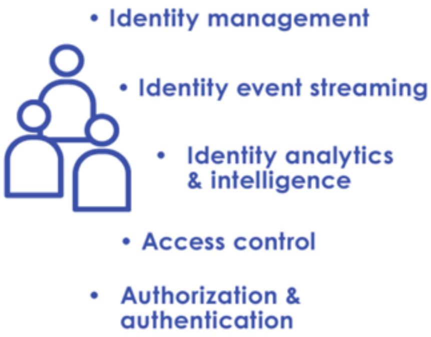

• Identity management
• Identity event streaming
• Identity analytics & intelligence
• Access control
• Authorization & authentication

Figure 2-3: The identity components of an identity-driven IoT platform.

- **Identity management:** The IoT platform establishes unique identities for every entity on the network to ensure each is who it claims to be. It defines the profile of each entity, including elements such as access rights, period of access and access levels. This combination of unique identifiers and metadata provides high levels of security on the IoT network.
- **Authorization and authentication management:** The IoT platform delivers authorization management to make sure that entities only access resources which they should. It establishes an authorization and policy management framework that validates and verifies all identities, ensuring the safety of corporate assets, and enables multi-level authentication for secure access. The IoT platform can feature attribute-based authorization to personalize authorization for every person, system or thing on the network.
- **Access control:** The IoT platform allows you to manage all the credentials of every person, system and thing in their varying states within the identity lifecycle. It enables you to quickly alter, re-assign or deny rights. It is possible to set up rules and workflows to automatically transition resources, such as IoT devices, from one state to another. In addition, policy-based governance is essential to manage data access across people, systems and things. Data access must be granted or revoked based on centralized governance policies that are executed across multiple channels and endpoint connections.
- **Identity event streaming:** The IoT platform synchronizes identity-related data and directories to simplify the management of vast quantities of IoT identities by accelerating identity and action checks against the relevant directories. Every requested interaction between elements on the network generates an event message that is streamed to the directory, such as an LDAP-based user directory, to enable fast authentication and access provisioning. This provides the basis to track all behaviors of all entities on the network to help establish authentication and allow for early triggers when unusual behaviors occur.
- **Identity analytics and intelligence:** Advanced IoT platforms deliver identity analytics and intelligence that collect, cleanse and correlate data about administration, authentication and authorization events. It then applies advanced analytics to transform the data into actionable intelligence with respect to identity management performance, compliance regulations and corporate security and risk policies.

The core capabilities: Security

An IoT platform should deliver the following security capabilities:

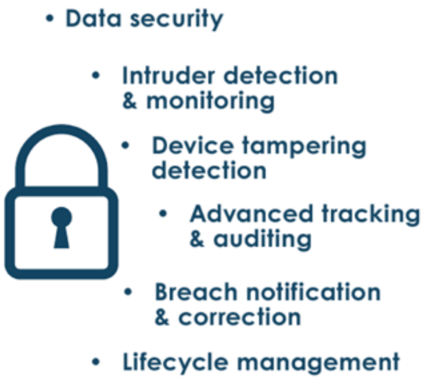

• Data security
• Intruder detection & monitoring
• Device tampering detection
• Advanced tracking & auditing
• Breach notification & correction
• Lifecycle management

Figure 2-4: The identity components of an identity-driven IoT platform.

- **Data security:** All data on the IoT network must be secure in transit and at rest. Many older IoT devices use encryption levels that are no longer considered secure. The IoT platform provides the latest security features and the leading cloud-based platforms benefit from constant updates to the latest web security and encryption standards (see below).

- **Advanced tracking and auditing:** The advanced tracking capabilities of the IoT platform allow for close monitoring of activities, such as messages being sent and received, and behaviors, such as how often someone accesses a device and from where, across the network. This offers insight into the flow of data between all connected people, systems and things over the platform, enabling it to immediately spot and address unusual behavior. Capturing all activity data allows an organization to audit its security performance.
- **Intruder detection and monitoring:** Built on comprehensive authentication, the IoT platform should provide intruder detection and monitoring. With so many IoT devices connected to the network, it is possible for an attacker to launch multiple credentials-based attacks on a device without anyone knowing. The IoT platform can detect when suspicious activity occurs, immediately alert the appropriate people and, where required, quarantine the specific device.
- **Device tampering detection:** Newer generations of IoT devices have built-in tamper detection. They can send immediate alerts to the IoT platform if parts of the casing have been broken, potentially indicating that someone has attempted to tamper with the device.
- **Breach notification and correction:** Analysts agree that most companies will fall victim to a cyberattack and IoT devices are the weak link. The question is not so much whether your devices will be attacked but how quickly and effectively you can identify and recover from it. If an organization does suffer a breach to its IoT network, the platform should be able to offer forensic security capabilities to enhance endpoint detection, report the incident and efficiently remediate the breach.
- **Lifecycle management:** IoT devices can be deployed for either very short or very long periods. For example, sensors attached to pipeline may be installed and are expected to operate for many years. The IoT platform must be able to manage every device through its lifecycle and de-provision it immediately when it outlives its purpose. This is particularly true when dealing with updates and patches to installed devices. The IoT platform must also be able, where possible, to manage remote software upgrades to ensure they don't create new security vulnerabilities.

These identity and security capabilities combine to provide a complete, end-to-end solution that helps establish and grow an Industrial-grade IoT environment.

Deployment models for identity-driven IoT platforms

An identity-driven IoT platform can be deployed in a variety of formats: on-premises, cloud-based and hybrid cloud. Most IoT platforms are cloud-based, as this offers smooth scalability, cost-effective data storage and internet-based performance and security.

However, the IoT platform must be able to integrate seamlessly with on-premises applications because master data, such as customer, order or product data, is often held in on-premises systems, such as ERP and MES, for information confidentiality and governance reasons.

Chapter 3

Challenges involved in the Identity of Things

In this chapter

- Learn about the key challenges associated with IDoT
- Understand the importance of an identity framework
- Learn about the role of identity governance

Research has shown that as few as a third of companies believe their IoT projects have been a complete success.[1] Security is a major barrier. A survey from mobile company, Vodafone, found that three quarters of respondents saw security as the key concern when selecting connectivity for IoT.[2] So, what are the key challenges of applying IDoT?

Different devices

IoT has created a wide, and growing, range of devices designed for different purposes and environments. These include:

- **Smart tag:** Based on RFID (radio frequency identification), the most basic form of tag simply transmits a unique ID number to any scanner that comes within close proximity. Tags become IoT devices when they are used to generate data for analysis in real time.
- **Smart sensor:** A smart sensor is the most common form of IoT device. It monitors its immediate environment and transmits information to other systems for analysis. Sensors contain an analog chip for reading real world information, such as temperature, pressure or movement. The analog signal is converted to digital data by a microcontroller chip.
- **Smart camera:** The latest advances in technology involve cameras with built-in intelligence, which are increasingly being used as IoT sensors. The applications for smart cameras include recording the license plates of cars using toll roads, performing quality checks on manufactured goods and assisting security staff with remote monitoring.
- **IoT beacon:** Like smart tags, IoT beacons generate information via their interactions with other devices in the system. A beacon repeatedly broadcasts a small piece of information and, if a compatible device moves close enough to the beacon to receive the message, an automated action occurs.

- **IoT receiver:** Many IoT systems include devices that are controlled by the system, such as smart street lights that dim or brighten based on traffic conditions. These use IoT receivers. A receiver is similar to a beacon, as they only comprise basic connectivity. The difference is that the IoT receiver uses long-range radio.
- **IoT gateway:** IoT devices that communicate using an unlicensed radio spectrum connect to the internet via gateway devices. An IoT gateway operates two or more communication protocols, enabling data to flow from one network to another.

Each device needs its own unique identifier. However, there is no specific approach to identifiers for IoT and it is highly likely that there never will be. Manufacturers and users have developed various types of identifiers with different characteristics based on the application for which that IoT device is being used.

IPv6 (Internet Protocol Version 6) was introduced in 2012 to address the shortfall of available IP addresses. It provided an almost limitless number of URLs—more than all the planets in the universe. Some people have suggested that this could act as the identifier for IoT, but this will not work. Not all IoT devices connect directly to the internet. When a device, such as a sensor, breaks it may be given a new IP address or the company's system may dynamically award IP addresses upon connection. In this case, any other system that has a relationship with the device would fail, as it would try to identify it with a now outdated IP address.

Different standards

Standards lie at the heart of the development and adoption of IoT. A large IoT network is likely to have a range of IoT devices and use a range of software standards and communications protocols.

Today, IoT is a technology with many standards but little standardization. For example, IoT devices use a variety of methods to connect and share data, such as:

- Infrastructure, including 6LowPAN, IPv4/IPv6 and RPL.
- Data protocols, including MQTT, CoAP, AMQP, Websocket and Node.
- Device management, including TR-069 and OMA-DM.
- Authentication, including Auth0, TPM and X.509 certificates.
- Semantic, including JSON-LD and Web Thing Model.

There are no universal standards. In 2016, there were at least 55 influential associations and standards bodies in the IoT space and tech giants, such as Microsoft®, Apple® and Google™, promoted their own IoT ecosystems based on proprietary standards and protocols. Without a huge number of options available and no consistent standards, the focus must be to deliver effective interoperability between devices and systems.

Different communications protocols

Just like IoT standards, there is a huge range of connectivity options when designing an IoT network. Each has its own variations and different standards and protocols.

In terms of communication protocol, you can use an unlicensed radio spectrum via an IoT gateway, using Wi-Fi, Bluetooth® or Zigbee™, or link directly to mobile networks, such as 5G, LTE-M or LP-WAN.

Protocols, such as Physical Web, mDNS and DNS-SD are required for network discovery services. Device identification requires EPC, uCode, IP6 or URIs. A large IoT network will include a range of devices using a variety of standards and protocols that have to be managed as a single, end-to-end solution.

Different relationships

IoT introduces new relationships into your digital ecosystem. These include:

- Device-to-device
- Device-to-person
- Device-to-system
- Person-to-person
- Person-to-system
- System-to-system

Relationships will often be multi-layered. For example, an IoT device is usually assigned an ownership relationship with a person. However, the device can have more than one owner and each owner can have different access rights to that device. Ownership often changes from manufacturer to administrator to user, and many of these relationships are temporary or time limited.

In addition, the IoT network will have thousands or more concurrent relationships taking place. You must be able to manage and secure all these relationship, prioritize the most important and manage all change processes at scale. A person should only have ownership or access rights to a device for as long as they need it.

Different data formats

Handling the volume and velocity of data being created by IoT devices is a significant challenge for every organization. In addition, IoT creates new data types and formats that users have not had to handle before. All this IoT data must be collected, stored and analyzed before it can be turned into actionable insight.

Data integrity is paramount, as you must be able trust the IoT device and the data that it is creating and transmitting. Where analytics is applied, that data has to be prepared, cleansed, formatted and indexed. You need to deliver a ‘single source of the truth’ for your IoT data.

As your organization starts to blend different types of IoT data with data from other sources to create central data lakes, you need to be able to normalize the data into a single format and validate it for use with applications, such as advanced analytics.

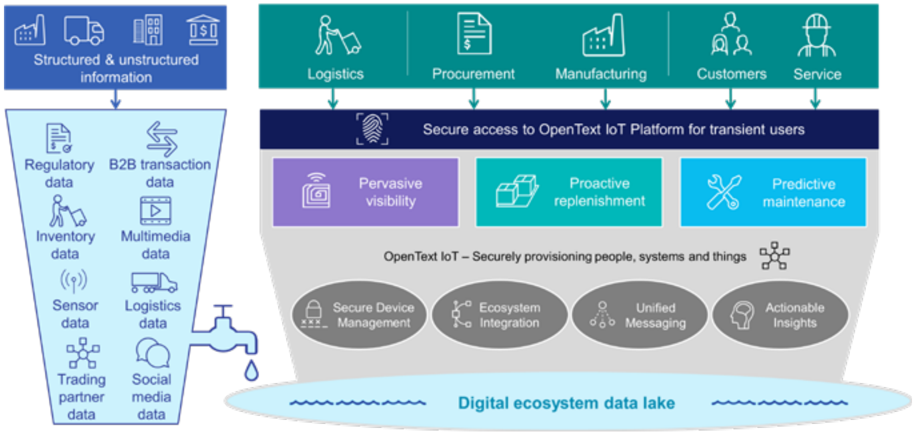


Figure 3-1: Blending data from different sources to build a data lake to create a single source of the truth for IoT data.

The need for a consistent IoT identity framework

With so many devices, identifiers, standards and protocols, you need a standard approach for recognizing and managing all the different identities across your IoT network.

An overarching IoT identity framework can establish how your organization will define the identities of all the people, systems and things on your network, as well as help set out the policies and procedures you need to put in place.

It can also facilitate the process of identifying the identity components you need to manage a quickly growing digital ecosystem. This gives you the foundation on which to select the correct identity-driven IoT platform (see Chapter 6) for your business.

Establishing identity governance

IoT creates more data and gives more people access to it. The result is an extra strain on your information governance and compliance capabilities. As regulations, such as the EU’s GDPR, strengthen data protection, all organizations must be acutely aware of the data liability and privacy issues involved in implementing an IoT environment.

The new governance and compliance responsibilities of IoT require that organizations take a top-down and bottom-up approach to risk capabilities that reaches across all users and business departments.

Applying IDoT solutions can help enable the proactive security, risk identification and mitigation that can help you meet your compliance obligations. It can identify and address policy violations, ensure the correct authentication and access rights are applied and, importantly, enable you to confirm and demonstrate that the proper security measures and compliance procedures are in place.

[1] Cisco, The Journey to IoT Value: Challenges, Breakthroughs, and Best Practices https://www.slideshare.net/CiscoBusinessInsights/journey-to-iot-value-76163389

[2] Vodafone, Vodafone IoT Barometer 2017/18 (2017) https://syswinsolutions.com/wp-content/uploads/2017/10/Vodafone-IoT-Barometer1718,0.pdf

Chapter 4

Applying Identity to the Industrial IoT

In this chapter

- Examine the use cases driving the Industrial IoT
- Learn about the identity challenge for each use case
- Discover how IDoT can address these challenges

Industrial IoT use cases fall into two related categories, applications of IoT that enable organizations to improve their complex production and operational processes and applications that allow companies to create new revenue opportunities, product and service differentiators and business models. This chapter looks at some of the key use cases and the role IDoT plays in their successful implementation.

Product quality

Based on a survey it conducted, the consulting firm, Bain & Co, believes that manufacturing quality control is the most promising application of Industrial IoT.[1] It provides manufacturers with unprecedented levels of realtime visibility into their operations, enabling them to quickly root out process inefficiencies and reduce waste.

Companies have used technology solutions for many years to achieve 'lean' goals, such as increased uptime or improved output, but these have mostly been siloed, point solutions. IoT allows you to integrate these systems to provide operational visibility across assets, product lines, factories and your entire business.

More than this, IoT sensors attached to a product can allow you to track and analyze how customers actually use it. This information can be fed back into the design and production process to improve the product and add functionality for which you already know there's customer demand.

The identity challenge

There can be hundreds or thousands of IoT devices within a single production asset, which means that asset is creating a large amount of data every day. To gain visibility over your entire production process, you must be able to accept data from every asset in every production facility anywhere in the world.

If you are also tracking customer behaviors and usage patterns, you need to be able to capture this data and blend it with IoT data from your production assets. This data must be available to users across departments, such as design, production, operations and marketing, as well as integrated with your enterprise systems, such as ERP, MES and CRM.

How IDoT helps

An Identity of Things solution can:

- Rapidly provision new IoT devices.
- Manage the lifecycle of all IoT devices, whether attached to your production assets or your products.
- Ensure secure data flows, both internally and externally.
- Bring together data from different sources and make it available to the users and systems that need it.
- Authorize and authenticate all people, systems and things on the IoT network.
- De-provision all IoT devices, including those attached to customer products, as soon as they are no longer required.

Predictive maintenance

Predictive maintenance has become one of the most popular applications for IoT technology. Keeping production assets up and running significantly decreases operational expenditure and can save you millions of dollars. It has the potential to virtually eliminate unplanned downtime and significantly reduce the need for scheduled maintenance.

This use case is built on the integration of IoT with AI and machine learning. With the help of machine learning algorithms, the IoT network takes realtime and historical data from sensors, as well as data from other relevant sources, to determine the likely failure of a component or sub-system.

By creating a comprehensive picture of the component sources, including elements such as weather conditions or service history, you can predict outcomes and decide whether the part should be repaired or replaced. Production assets will operate at optimum capacity for a longer time.

The identity challenge

Predictive maintenance has been considered one of the major drivers for Industrial IoT. However, the Bain & Co. survey found that the area is yet to fully take off as expected. Companies that have begun to implement predictive maintenance have found it more challenging than expected.

The consulting firm points to three main reasons for this: Security remains a key concern, but organizations are experiencing difficulty when integrating their operational technology and IT systems, as well as handling data from many sources in multiple formats. Uncertain returns on investment round out the surveyed concerns around IoT and reflect how challenging it is to integrate a new, disruptive technology.

How IDoT helps

An Identity of Things solution can:

- Facilitate secure connectivity between IT and OT systems.
- Create and manage temporary access to devices for personnel, such as engineers and maintenance crews, to undertake repair or replacement activities.
- Leverage historical sensor information to determine the likely failure of a component.
- Ensure data integrity from all connected devices.
- Bring together data from different sources and make it available to analytics capabilities to drive decision-making.

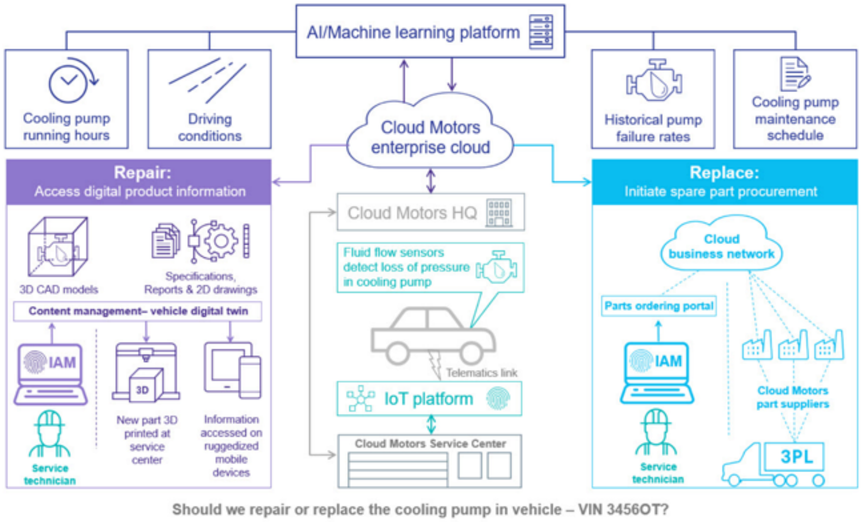

AI/Machine learning platform
Cooling pump running hours
Driving conditions
Cloud Motors enterprise cloud
Historical pump failure rates
Cooling pump maintenance schedule
Repair:
Access digital product information
3D CAD models
Specifications, Reports & 2D drawings
Content management– vehicle digital twin
IAM
3D
Service technician
New part 3D printed at service center
Information accessed on ruggedized mobile devices
Cloud Motors HQ
Fluid flow sensors detect loss of pressure in cooling pump
Telematics link
IoT platform
Cloud Motors Service Center
Replace:
Initiate spare part procurement
Cloud business network
Parts ordering portal
IAM
Cloud Motors part suppliers
Service technician
3PL
Should we repair or replace the cooling pump in vehicle – VIN 3456OT?

Figure 3-1: Blending data from different sources to build a data lake to create a single source of the truth for IoT data.

Asset monitoring

As supply chains become more complex, many companies require greater visibility into the status of their shipped goods. Customers expect to know where their products are during transit and when they will be delivered. Asset monitoring, or pervasive visibility, delivers continuous insight as products pass through your supply chain.

It provides accurate, realtime information on all aspects of your shipments through highly connected supply chain assets, such as products, pallets or trucks. Products and supplies are much easier to track, identifying slowdowns and inefficiencies. You can retrieve information from a range of IoT sensors, including GPS, temperature and humidity.

Logistics carrier performance can be monitored in real time so that if issues arise, for example damaged goods, you can act quickly while the IoT data delivers audit capabilities for future compensation or penalties.

The identity challenge

Asset monitoring is of little use unless you can quickly act on the IoT data you are receiving. First, you must be able to guarantee that the information you are receiving is accurate and from a trusted source. Then, you must be able to quickly inform all the people involved as soon as a potential issue arises to take remedial actions.

For example, a truck carrying perishable goods is traveling across the U.S. A variety of different IoT sensors, using different standards and protocols, are monitoring many aspects, such as location, temperature, humidity, etc. When an issue arises, the driver must be informed so they can determine whether they can fix the problem. The distribution center must be informed to determine if new stock needs to be dispatched. And, the customer must be told if there are delays or problems with their order.

How IDoT helps

An Identity of Things solution can:

- Provide secure, realtime monitoring of products, pallets and containers and multi-modal transportation methods, ie. trucks, ships and rail and flight.
- Retrieve information from a variety of IoT devices and make it available to the correct people and systems.
- Enable two-way communication with IoT devices to facilitate remote access and remediation where appropriate.
- Rapidly provision secure IoT devices, preventing unauthorized access to sensor information.
- Connect all IoT devices, regardless of the standards and communications protocols used.
- Authorize and authenticate all people, systems and things on the IoT network.
- De-provision all IoT devices, including those attached to customer products, as soon as they are no longer required.

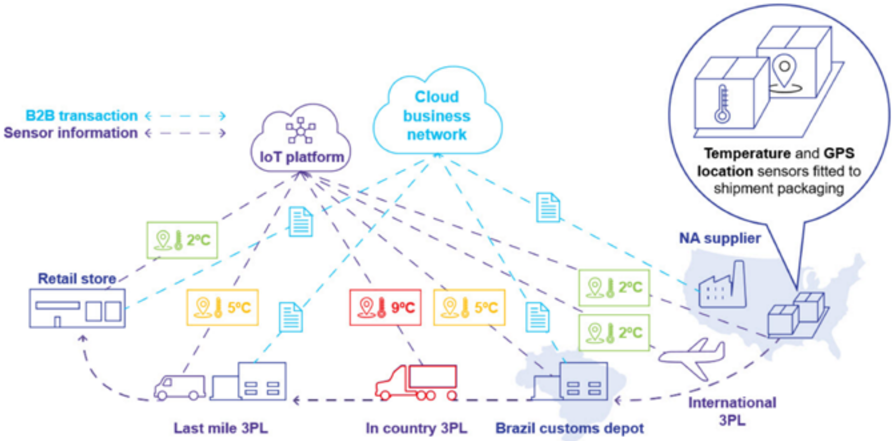


Figure 4-2: IoT sensors being used to provide pervasive visibility of a shipment moving through the supply chain.

Proactive replenishment

IoT is increasingly being used within supply chains to provide realtime monitoring of inventory levels and to initiate automated replenishment processes with suppliers.

Events are effortless to monitor across the supply chain, providing a comprehensive view of inventory. IoT devices are combined with AI and analytics to monitor product and material consumption patterns with pre-defined triggers that determine when to activate the replenishment process.

With integration between the IoT network and enterprise systems, such as ERP or warehouse management systems (WMS), inventory across the supply chain can be monitored and aligned more closely with consumer demand to reduce the amount of inventory required while ensuring continuous product availability.

The identity challenge

You need to be able to accommodate a wide range of connected devices attached to both your supply chain assets and your products and securely manage the different data formats from these devices.

As a good proportion of your inventory will be in transit, you need secure, realtime tracking across a range of communications protocols, such as Wi-Fi, 5G or LP-WAN¬, that connect different parts of your supply chain.

How IDoT helps

An Identity of Things solution can:

- Provide end-to-end visibility into the status of all inventory within your supply chain.
- Rapidly provision a wide variety of IoT devices.
- Manage the lifecycle of all IoT devices, whether attached to your production assets or your products.
- Ensure secure data flows from multiple data sources.
- Bring together data in different data formats and make it available to your analytics capabilities for improved decision-making.
- Rapidly authorize and authenticate all people, systems and things on the IoT network—at scale.

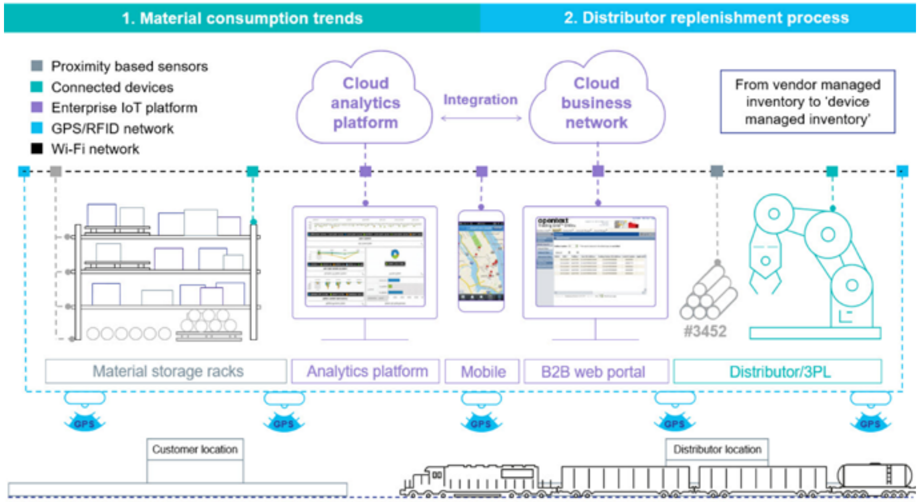


Figure 4-3: IoT and analytics combine to deliver proactive replenishment from the distribution center to a customer's door.

Digital twins

A digital twin is the digital representation of the physical and functional characteristics of a physical object. Built around a model, commonly the CAD model established during initial design, the twin acts as a shared knowledge resource for the object by including all relevant information on the object.

The digital twin also takes data from IoT devices connected to the physical object and combines that sensor data with information from other sources, such as your CAD and ERP systems. In this way, it helps manage the physical object throughout its entire lifecycle from inception to disposal.

While modeling is not new, digital twins deliver richer, realtime data for greater and more precise analysis. More advanced digital twins offer bi-directional communications, so that the twin does not just monitor the object but can control and change it. This helps optimize your production operations and can inform product design and personalization.

The identity challenge

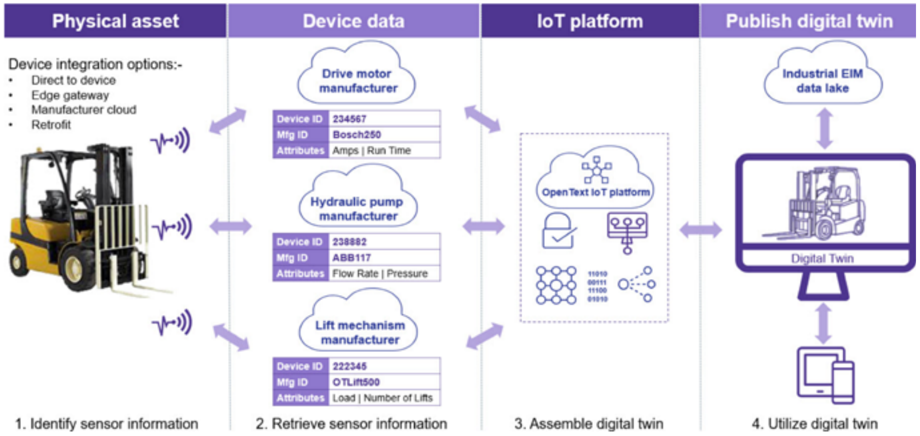
While the concept behind a digital twin is relatively simple, implementation can be extremely complex. Every physical object, in theory, can have a digital twin and every component and sub-component within a production asset can have its own twin, meaning there can be hundreds or thousands of connected devices within the digital twin for that asset.

Organizations are now scaling up to create digital twins of complete production facilities, such as a factory or even their entire global production operations. Manufacturers are increasingly delivering their products with its own digital twin. With limited standards, this rapidly creates a heterogeneous IoT environment based on different devices, standards, protocols and data formats.

How IDoT helps

An Identity of Things solution can:

- Ensure secure and managed integration between different levels of digital twins.
- Manage the messaging and orchestration so that all network entities can communicate effectively with each other.
- Rapidly provision new IoT devices.
- Manage the lifecycle of all IoT devices, whether permanently or temporarily connected.
- Ensure secure data flows between people, systems and things.
- Authorize and authenticate all people, systems and things on the IoT network.



Device ID	234567
Mfg ID	Bosch250
Attributes	Amps | Run Time

Device ID	238882
Mfg ID	ABB117
Attributes	Flow Rate | Pressure

Device ID	222345
Mfg ID	OTLift500
Attributes	Load | Number of Lifts

Figure 4-4: Leveraging IDoT to establish a digital twin of a physical piece of equipment

Connected vehicles

It is estimated that more than one billion connected cars are already on the roads, with 64 million new units shipped in 2019. Today, there is as much software engineering as mechanical engineering in a new vehicle. The connected car is an excellent example of where Industrial IoT blends with consumer IoT.

Automotive companies are using IoT to monitor and improve the performance of their vehicles and develop new revenue streams in areas, such as infotainment and service and maintenance. Fleet management is one area where IoT is being deployed to continually monitor aspects, such as driver performance and vehicle status, for enhanced safety and improved gas mileage.

IoT is also implemented to improve the vehicle owner's experience. In addition to infotainment services and predictive maintenance, connected vehicles offer entirely new driver assistance features. Self-parking cars are becoming more common, as are vehicles that help with speed regulation, overtaking and collision avoidance.

The identity challenge

The sheer scale of an IoT network designed to support connected vehicles is the main identity challenge. For global automotive companies, this easily runs into millions of customers and hundreds of millions of connected devices.

These devices are operating concurrently and often in transit. The importance of ensuring that all devices can operate seamlessly and in real time can't be overstated. This is also true of the security implications around the threat of a connected vehicle being hacked.

How IDoT helps

An Identity of Things solution can:

- Enable secure and effective data transmission of every IoT device at scale.
- Deliver the highest levels of device and data security both at rest and in transit.
- Provide complete data privacy to protect the personal information of drivers and customers.
- Provision and manage all IoT devices at scale.
- Authorize and authenticate all people, systems and things on the IoT network.
- Ensure consistent connectivity of devices to the IoT network, with failover options available.
- Ensure the integrity of all data flows.

[1] Bain & Company, Bain IoT Vendor Survey and Bain IoT Customer Survey (2018) https://www.bain.com/insights/which-applications-of-the-industrial-IoT-are-gaining-the-most-traction-snap-chart/

Chapter 5

The benefits of the Identity of Things

In this chapter

- Learn how IDoT can improve security
- Understand how IDoT increases productivity and reduces costs
- Learn how IDoT can help drive business and operational improvements

There may be several challenges but successfully implementing an IDoT strategy can also deliver a whole host of benefits to your business. These include:

Improved security

Cybercrime is on the rise and cybersecurity is front of mind for every CIO. When the cause of cyberattacks is analyzed, research has shown that the vast majority of attacks are credentials-based.[1] In other words, the hacker broke into the network by misusing credentials, such as a user name and password, or already had access to the network.

The cost of this type of breach can easily run into the millions of dollars. In addition, it can often take several months for the breach to be noticed, by which time the attacker may have wrought untold havoc. Even more worrisome, organizations are often unaware that a breach has occurred and are unable to determine the cause when they do find out.

IoT devices can dramatically increase the vulnerability of a corporate network for a number of reasons:

- **Creating a back door:** IoT devices can create a back door onto your network. Once the hackers gain access to the device, they use it to access and attack your entire company IT infrastructure and other resources. Once the device vulnerability has been exploited, it can be grouped with other hacked devices to create botnets to launch widespread denial-of-service attacks.
- **Simple password protection:** Many IoT devices are basic. Security is not a leading feature in their design and they are often protected by a simple password, which is hard-coded into the device. When deploying hundreds or thousands of similar devices, it is too easy to retain the factory setting for the password, which increases its vulnerability.
- **Lack of sophisticated OS:** The majority of IoT devices, such as sensors or actuators, are designed to conduct a specific discrete task, so the operating system (OS) is going to be limited and lacking in security features, especially authentication and cryptography.

- **Edge computing and IoT devices:** As the price of IoT devices decreases and their computing power grows, organizations are moving more of the computing and data processing to the 'edge' of their network. This means that the IoT device becomes responsible for many of the computing tasks previously conducted at the system level. These IoT devices require higher levels of security to protect both access and the data now held on them.

IDoT provides the platform required to deliver the secure and robust technologies needed to provision, authenticate, authorize and audit the identities of the wide and growing range of IoT devices.

Increased productivity

IDoT allows you to centralize and automate many of your identity and access management processes to encompass all people, systems and things on your network. Automated provisioning, rights assignment and de-provisioning allow you to rapidly onboard new entities to your network at scale.

You can quickly and effectively assign and alter rights, enabling new devices and people to get up and running faster.

In addition, comprehensive authentication capabilities allow you to automate the presentation of credentials, such as geo-location or user behavior, to make it easier and natural for users to gain secure access to network resources.

Reduced costs

As IoT adds complexity to the network, some organizations have introduced more identity management systems to address different access requirements, including separate systems for internal and external users. This adds to the cost and complexity of identity management.

IDoT reduces operating costs by leveraging a single cloud-based platform with extensive identity management, automation capabilities and a centralized identity database.

Automating much of the provisioning, authentication, management, revocation and de-provisioning processes increases the effectiveness of your security facilities, while reducing the need for direct involvement from administrators. This decreases the costs and risk of error associated with manual processes.

Guaranteed data integrity

IoT delivers more active network connections than you have had to manage before. According to global research firm IDC, predicts that by 2025 there will be 55.7 B connected devices worldwide, 75% of which will be connected to an IoT platform.[2] You must be able to trust your IoT devices and the integrity of the data they create. If data cannot be trusted or is inaccurate, you cannot take the risk of basing business decisions on it.

IDoT can address trust and facilitate the deployment of IoT devices in three areas within your organization:

- **Authentication across the IoT ecosystem:** Only authorized and legitimate devices must be allowed to connect to the IoT network. As the devices will operate with little or no human intervention, IDoT can enable mutual authentication between devices, systems and users.
- **End-to-end data integrity:** You must be able to ensure the integrity of all data flowing across your IoT network, from the source to the final destination. You need to know where the data came from, that the source had the rights to create and transmit the data and that the destination is correct and able to compliantly receive the data.
- **Device updating and patches:** As IoT devices become more intelligent, the need to deliver software upgrades and patches, often automatically, increases. Each upgrade offers the opportunity to attract viruses or malware. IDoT can ensure that the legitimacy and integrity of the code is preserved throughout the device's lifecycle.

Improved business and operational performance

IoT enables organizations to approach many of their business and operational processes in ways that were not possible before. The data from IoT devices provides new levels of insight, visibility and control over how you do things, how your supply chain functions and how your customers respond to your company and products.

Telecommunications giant, Vodafone, conducts an annual IoT barometer that has shown that as you deploy more IoT devices into your business, the benefits grow rapidly. These IoT devices are being used to develop new and innovative business and operational practices, including:

- Preventative maintenance
- Proactive replenishment
- Asset monitoring
- Digital twins

None of these new IoT-driven approaches to business would be possible without IDoT. This is especially true, as IoT deployment does not happen in isolation. It is usually part of larger digital transformation initiatives and involves integration with other key enterprise systems, such as ERP, CRM or accounting.

[1] Verizon, 2019 Data Breach Investigations Report https://enterprise.verizon.com/resources/reports/dbir/

[2] IoT Growth Demands Rethink of Long-Term Storage Strategies, 27 Jul 2020 https://www.idc.com/getdoc.jsp?containerId=prAP46737220

Chapter 6

Selecting the right IDoT provider

In this chapter

- Understand the key capabilities of an IDoT provider
- Discover top tips for selecting an IDoT provider
- Learn what questions to ask an IDoT provider

Successfully implementing an IDoT solution can be complex. The next step is selecting the ideal provider with which to partner. Working with an identity-driven IoT platform provider should be a long-term relationship, so take some time to get it right. This chapter will discuss what to look for in a provider.

Key capabilities for an identity-driven IoT platform provider

An IDoT solution has many parts, so your platform provider must be able to demonstrate a range of technical capabilities and skills. The following sections outline the minimum capabilities you should expect from your provider. These include:

- A powerful, scalable and global IDoT platform that supports the widest range of devices, standards, protocols and data formats. The platform's identity-centric approach must focus equally on securing and managing the connected people and connected systems on your IoT network as it does on the connected things.
- The ability to manage every type of relationship taking place on your IoT network—device-to-device, device-to-person, person-to-system, device-to-system, etc.—at scale. It should be able to handle any number of concurrent relationships and be able to prioritize the most important data passing over the network.
- The ability to automate as much of the provisioning, authentication, monitoring and management of all devices, people and systems connected to your IoT network.
- Advanced analytics and dashboarding that allows you to gather all the important data on all activities happening on the IoT network and make them available, in an easily accessible format, to everyone who needs it.
- A comprehensive combination of both identity and access management (IAM) and IoT skills. The provider should thoroughly understand the IoT environment and approach identity as a native feature for IoT, rather than looking to overlay traditional IAM solutions onto the new environment.
- Change management expertise to deal with the constant evolution of technology, business processes and workflows and commercial strategies.

- Full program management capabilities for your identity-driven IoT platform, where required, covering aspects, such as technical implementation, day-to-day management, incident handling and ongoing maintenance.
- Access to solution sets that are complementary to IDoT and IoT, especially advanced analytics and AI. The combination of AI, analytics and IoT is fundamental in delivering use cases, such as predictive maintenance and pervasive visibility. A single provider can make the integration of different technologies significantly easier and reduce the risk of failure.
- A global cloud-based infrastructure and applications that provide regulatory compliance and service levels for your identity-driven IoT platform. It needs to ensure that you have continuous operations and availability while you comply with data privacy, security and integrity regulations.

8 top tips when selecting a platform provider

Finding the right identity-driven IoT platform provider can be time-consuming and costly. The following are some brief tips to consider when you begin speaking with potential providers.

Select the specialists…

It is important that the provider is an identity management expert. But, this should not come at the expense of their understanding of, and experience with, the digital ecosystems involved in your IoT network. Look for a provider that can demonstrate both IoT and identity management capabilities.

… not just in one discipline

Reaping the full benefits of IoT relies on the data management and analytics capabilities your provider can offer. As more and more organizations struggle to integrate various data formats, they need a provider that understands how to bring together and blend IoT data with information from other sources and present it for analysis to deliver actionable insights.

Avoid fragmentation wherever possible

Select a provider that lets you manage every person, system and thing on a single, enterprise platform. This is not just about the many types of devices, it is equally about all the people who need access to the IoT network—employees, customers, suppliers, partners and contractors. Every entity, and the dynamic and changing relationship between entities, must be effectively controlled and managed.

Don’t let your IoT network become another silo

Early implementations of IoT have focused on delivering solutions to discrete problems, such as improving the performance of a production asset. This can easily result in creating another information silo for each IoT deployment. You need to ensure that, even where there seems little need, that the IoT data you create can be made available across the enterprise. For example, the data from monitoring a production asset in one factory can be used to identify why similar assets in other facilities are under-performing. Look for a provider that can demonstrate the ability to integrate IoT data flows into large enterprise systems and business processes. Can the provider offer integrated solutions in areas, such as customer experience management, business process automation or B2B integrations?

Think performance, scalability and availability

Scalability has become a major determining factor when considering IoT platforms. When you are dealing with an environment that can grow from hundreds to hundreds of thousands of devices remarkably quickly, you need the virtually limitless capacity of the cloud. However, performance and availability are also essential criteria. Given the variety of relationships within your IoT network, you are faced with many concurrent connections that cannot be allowed to slow or suspend the network. If a disaster does occur, how quickly can you recover?

Remember not all clouds are created equal

Most IoT platforms are cloud-based, but there are different types of cloud infrastructures. For most organizations, the IoT network will be mission-critical. This raises data management and confidentiality issues about using the public cloud. Most companies will wish to retain at least some of their data management and compliance capabilities on-premises and the provider must be able to integrate this seamlessly into the IoT platform. In addition, many organizations prefer to implement an entirely private network for all aspects of their IoT environment. Look for a provider that can deliver an IoT platform that exactly meets your security, confidentiality and compliance requirements.

A platform for today—and tomorrow

Your platform provider should be able to customize its service offering to your requirements today, while being flexible enough to change over time. Your contract and SLAs should set out how you will benefit as the provider introduces software upgrades and enhancements. Be sure that the services give you the future proofing you require.

A partner—not a provider

There is little point in entering into a contract with your provider unless you see it as a long-term relationship. You will find that value accrues over time. You cannot work with your provider in the traditional client and supplier model. This has to be a partnership. Take the time to ensure that the provider you select is a good cultural fit—will the organization work with you in the way you want?

Key questions to ask the service provider

Key questions to ask when selecting an identity-driven IoT platform provider include:

- Does it have the right mix of identity management and IoT skills?
- Does it offer a proven and mature IoT platform?
- Does it have clients who are willing to discuss their experiences with you?
- Does it operate its own global cloud infrastructure that lets you select the security and privacy you require?
- Does it have a global infrastructure to meet the scalability, performance and availability needs of your business?
- Does it offer complementary solutions, such as AI and analytics, to deliver a single platform for IoT environment?
- Does it offer integration services to other enterprise solutions, such as customer experience management or ERP, that allow you to build your IoT solutions into wider business processes?
- Does it have the program and technical capabilities, from initial IoT implementation to change management and ongoing support, in all the regions that you operate?
- Can it deliver 99.9 percent or more uptime for all components within your identity-driven IoT platform and will it build this into a service level agreement?

Chapter 7

Top 10 tips to consider when deploying IDoT

This chapter presents 10 handy tips to help you deploy an IDoT solution.

Think beyond IAM…

Traditional IAM was designed to manage the identities of your employees safely behind the firewall on your corporate network. Even more recent developments, such as consumer IAM and identity relationship management (IRM), are still primarily focused on the people connecting to your network, both internally and externally. IDoT has to be seen in a wider context of the relationships between people, systems and things. It is better to select a native IDoT solution rather that trying to adapt traditional IAM approaches for your IoT environment.

…but look to integrate

Moving beyond traditional IAM does not mean you have to rip and replace. Organization have undertaken great work in terms of IAM and governance. These are still appropriate today. You should look to integrate your IDoT solution with your existing IAM and governance frameworks. This provides a smoother path towards effective identity management for your IoT network, allowing you to keep your current best practices and integrate the new IDoT capabilities.

Authentication and authorization must meet your security needs

This may sound obvious, however, many IoT devices and gateways come with their own security features. You have to decide which work for you or whether you can implement and enforce standard authentication and authorization processes across all entities on your network. There are many competing IoT standards and you must decide which best suits your security and risk profiles or introduce an identity-driven IoT platform that can handle all standards, allowing you to enforce your own authentication and authorization techniques.

The access balancing act…

In the end, the levels of security and access control you set will be based on your business requirements. Often, too little access is as bad as too much access. Too much opens you up to security vulnerabilities, while too little will hamper your ability to conduct business effectively. Finding the right access levels will always be a balancing act and you need an IoT platform that will ensure you can enforce your security and credentials policies.

…means err on the side of caution

The rule of thumb should be that any user has access to the device only for the purpose and length of time that you specify. You must be able to dynamically assign, change and revoke rights as necessary. You can consider implementing solid restrictive practices into your identity management workflows to allow you to proactively restrict access for any entity on the network based on pre-defined procedures set out in your access governance framework.

Draw on your asset management capabilities

While you are likely to use a combination of a global unique identifier and associated metadata to identify and build trust for every device on the network, it is also good practice to draw upon your existing asset management capabilities to create an up-to-date and accurate inventory of all IoT devices within your organization. You can then categorize them by type of device and assign asset records based on ownership, deployment, de-provisioning and a range of other asset lifecycle activities.

IoT isn't plug-and-play

Factory settings—treat this phrase with caution, especially in an IoT environment. Many IoT devices are delivered with simple password authentication. Some organizations have implemented these devices without altering the factory settings. This is a major risk as once a hacker knows the default credentials, it is easy for them to gain access to your IoT systems and back door onto your corporate network. It is best practice to ensure that you centrally create and manage all default credentials.

A focus on certificates

Certificates, or tokens, are the preferred method for device authentication and confidentiality. They can be combined with other identity capabilities to build trust and security around any specific device. Certificates are now appearing that have been optimized for IoT environments, such as the IEEE 1609.2 credential format, that improve security while reducing the burden on the IoT network and devices.

Check your channels

Mobile and telecoms networks are a major part of an IoT ecosystem. As the smartphone becomes many people's primary device for computing and communications, an IoT platform's mobile capabilities grow in importance. For example, smartphones can be used as a means of authentication, such as SIM information or geo-location. In addition, mobile devices provide a platform for next-generation authentication for elements, such as facial recognition, voice recognition and gesture dynamics.

User education is essential

IoT security is not solely the province of the network administrator or CSO. IoT, such as cloud, AI and mobile, is part of the process to democratize technology, involving many more direct connections between people, systems and things than ever possible before. Users are now redefining their relationships with the IT and OT systems around them to change the way they work. This means that users also have to accept a level of responsibility to ensure the safety and security of your IoT environment. Users must be properly educated about your IoT ecosystem and its security features and must fully understand—and embrace—their role in device security and data privacy on the IoT network.

opentext™

The Internet of Things (IoT) is rapidly transforming almost every aspect of modern life, from monitoring our health to automating complex industrial production lines. As IoT deployments move from simple monitoring to alerting system failures and establishing digital twins of physical ecosystems, companies must adopt a zero-trust, identity-driven approach to securing devices and associated information flows. Identity of Things Explained introduces how an identity centric approach to IoT projects will help secure your connected devices and reduce the threat posed by cyber security threats.

Inside:

- An introduction to the Identity of Things (IDoT)
- The core capabilities of an IDoT platform
- The challenges involved in IDoT
- How to apply identity to Industrial IoT
- The benefits of IDoT
- How to select the right IDoT provider
- The top 10 tips to consider when deploying an IDoT platform

Bob Slevin is the Director of Product Marketing for IoT at OpenText. Bob is an Internet of Things (IoT) architect and evangelist with more than 25 years of experience in telecommunications spanning military and private sectors. He has collaborated with partners to deploy millions of connected devices across business and consumer markets. An IoT thought leader with an MBA in Technology Management, Bob is focused on identifying business challenges and building innovative solutions to improve operational efficiencies, drive growth and mitigate risks.