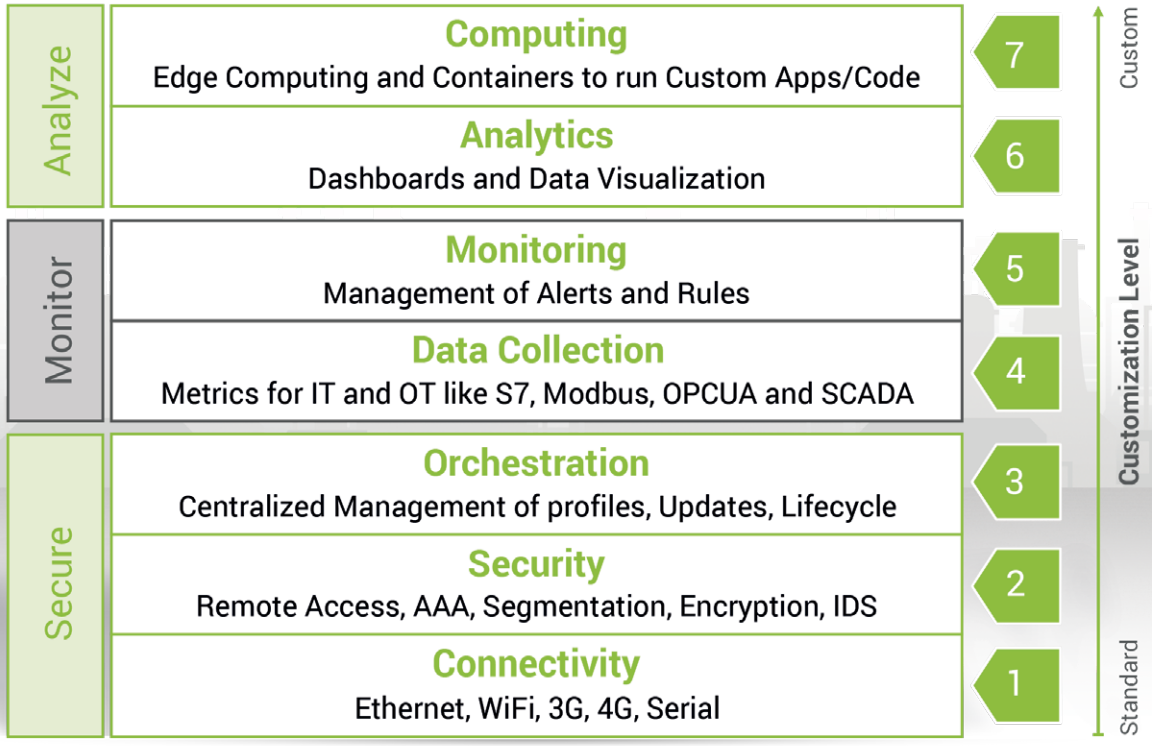
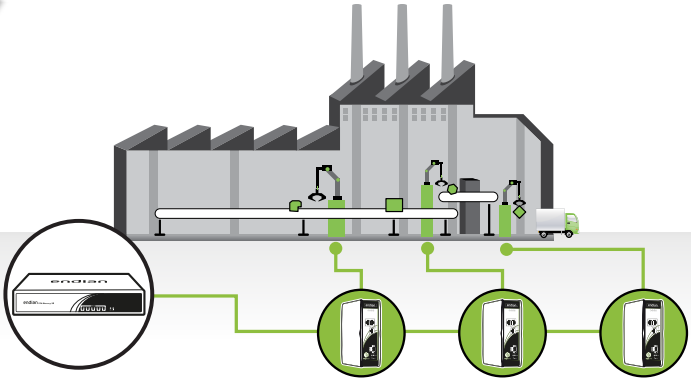
# Anatomy of a Secure Digital Platform (for Industry 4.0)




The structure of a secure digital platform in Industry 4.0 is composed of many parts all working together to form a complete solution. This guide explains the most important seven parts of the platform.

While there is a huge number of individual products in the Industry 4.0 category, there is not a single solution on the market that turns an analog industrial company into a digital one. Rather, a multi-product and multi-stage process is required before data from machines and plants can be converted into innovative business models. A central aspect of this process is security, because with the increasing degree of networking and exposure to the Internet, the attack surface for malware and hackers becomes larger. With the principle of “Secure - Monitor - Analyze”, digitization succeeds while simultaneously securing data and machines. The platform is divided into seven individual components, which are explained in this guide:

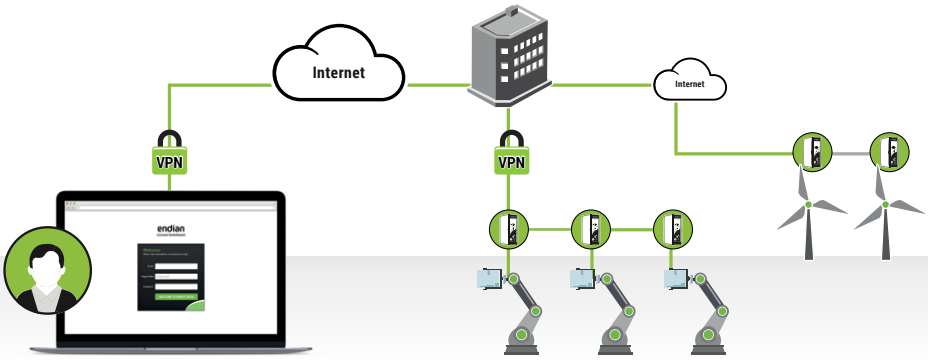
# Secure



## Step 1

## Connectivity - Connecting and linking machines

Due to the long service life of industrial machinery and equipment, heterogeneous machine parks are widespread in industrial companies. In addition, the plants are often located in environments that do not offer a continuous internet connection. In such situations Industrial IoT gateways (IIoT) are best suited to securely connect machines and plants to the Internet. In order to cope with a wide range of application environments, IIoT gateways must be equipped with a variety of connectivity options, such as Ethernet, Wifi, 3G or 4G.



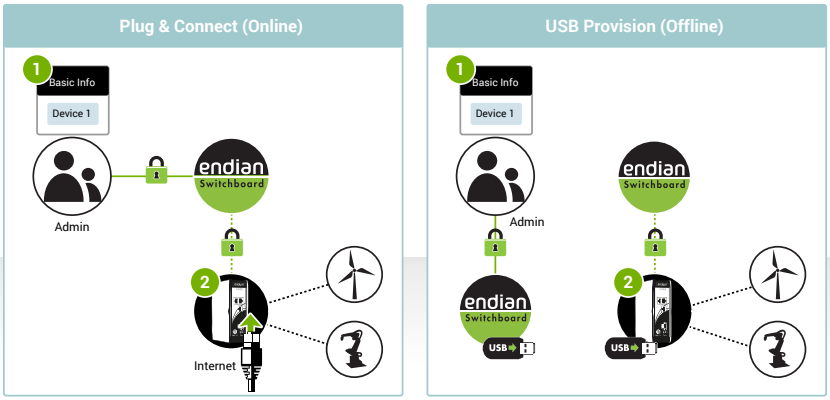

## Step 2

## Security - Remote access, segmentation and encryption

To secure infrastructure and data, only IIoT gateways should be used that have several coordinated security functions, so that comprehensive protection against cyberattacks is possible. This includes features such as firewall and malware / intrusion prevention systems (IPS).

With the help of IIoT gateways, corporate networks can also be segmented, which represents a very important step towards greater IT and OT security. Network segmentation prevents intruders and/or malware from spreading easily from one machine to the next. The basis for efficient network segmentation is the holistic view of a network and its contact points inside and outside the company. The next step is to define network areas with comparable protection requirements and to separate them from each other using IIoT gateways.

The IIoT gateways should simultaneously allow remote access to the machines. This would give users the opportunity to manage and monitor the entire infrastructure. If a defect occurs on a machine, a technician can assess and, if necessary, correct it remotely.

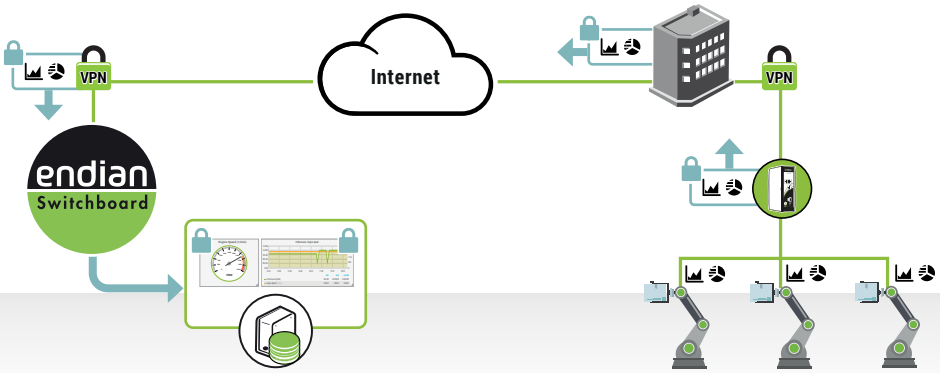



## Step 3

## Orchestration - Central management of user profiles, updates and lifecycles

As IIoT gateways are being deployed to connect and protect all the company networks and machinery, it's important to consider central management. Using central management ensures a valid security configuration is applied consistently to all gateways and makes updating the configuration of all devices simple to centrally administer. In addition the application of regular updates ensures that the security functions in the IIoT gateways remain up-to-date at all times, providing effective long-term protection against cyberattacks and malware.

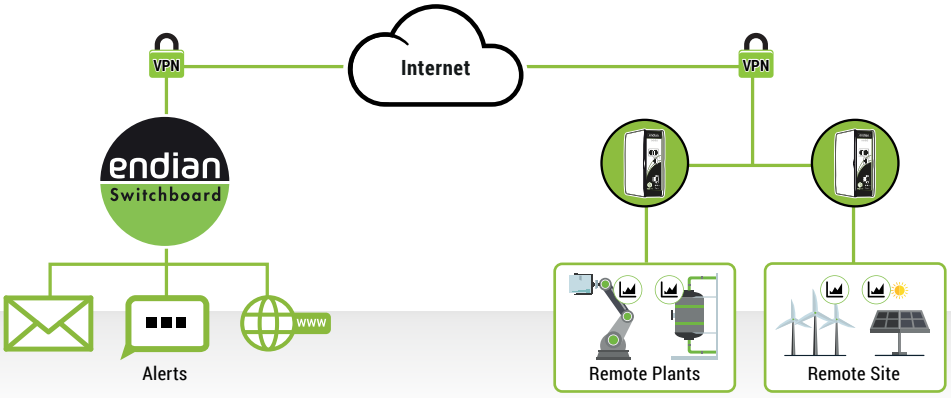
# Monitor




## Step 4

## Data collection - Mastering different machine languages

In the next step, data can now be collected from the machines. The IIoT gateways act as collectors of SCADA data. Since the machine parks are often heterogeneous, the gateways have to cope with a wide variety of machine languages, such as Siemens S7, Modbus and OPCUA. The machine data is then transferred to a central platform for storage and analysis.




## Step 5

### Monitoring - Monitoring machine states

The industrial infrastructure is of critical importance for companies and therefore it requires the highest levels of availability. A central platform should therefore be equipped with integrated monitoring functions and have a variety of options for alerting appropriate staff in the case of faults. This enables companies to react immediately to potential problems.

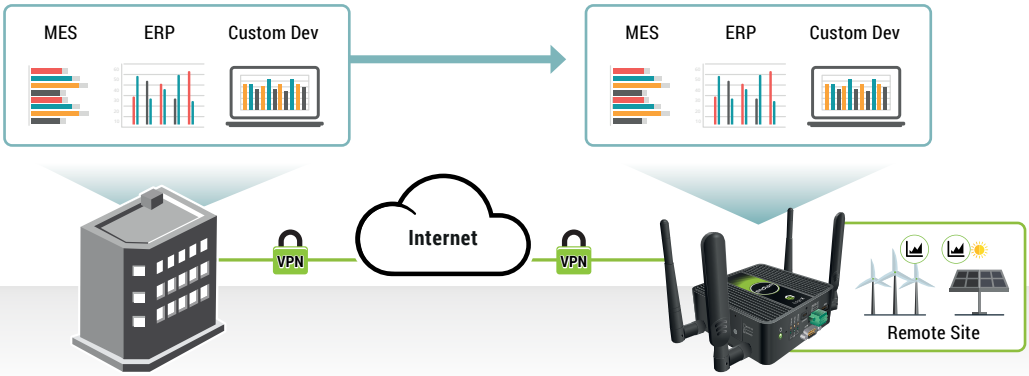
# Analyse


Endian Connect Platform

## Step 6

### Analytics - Predictive Maintenance

As soon as all data is aggregated at a central point, the phase of analyzing the data begins. With the support of dashboards, the data can be easily visualized. Patterns and anomalies become visible and can help to predict errors and solve product problems before they lead to major disruptions. This is what we call predictive maintenance and it offers decisive advantages: Downtime can be minimized and overall productivity and efficiency increased.




Step 7

## Computing - Advantages of the edge

The networked infrastructure and data analysis now form the basis for a solution which can benefit from the advantages of Industry 4.0. In particular, Edge computing, can offer huge benefits in IIoT. Edge computing references technology that enables data processing at the edge of the network, reducing bandwidth congestion and centralized data processing. At the same time, they improve the real-time capability in data evaluation and analysis by reducing or eliminating the network latency during data transmission to a central infrastructure. Using Edge technology, companies can move applications and critical services to run at the network edge thereby positioning them closer to the actual machine data and the users who need to utilize them.

# Are you ready for the Digital Transformation?

## Endian Proof of Concept Kit

The Endian PoC platform makes it easy to (a) collect and (b) analyze your IoT data from your field devices. The majority of the platform is securely hosted by Endian in our safe, secure, reliable cloud infrastructure. On your side, all you need to do is plug in and connect one of our client machines and devices to securely "translate" your IoT data from the field to our analyze platform where you can monitor and build visualizations (dashboards) for that data in real-time. We support a wide variety of IoT protocols including OPC UA, Modbus, Siemens S7 and more. We can also custom implement almost any protocol as well.

## How It Works

**It's extremely simple and for most customers can be done in a just a few weeks.**

### 1 - Define PoC

We'll work with you to define the parameters of your project based on your goals and requirements. Together we'll define which machine or device should be connected, how the network will be configured, which data should be collected and how to design your dashboard.

### 2 - Setup & Test

Next we will setup your private test account and send your pre-configured test device(s) to connect to your IoT. In addition we will help do any post-installation configuration to get your IoT data securely collected and build your first dashboard. From here you can easily build custom dashboards and test our platform.

### 3 - Next Steps

Once you're done evaluating the PoC, we will work with you on a taking the next steps to move forward with the Connect & Analyze platform to figure out the perfect solution for your customers and your business. Together we'll plan how to build a scalable solution and implement a roll out strategy.