# Data management in digital manufacturing:

## Achieving end-to-end visibility in the era of IoT



cisco

# Data management in digital manufacturing:

## Achieving end-to-end visibility in the era of IoT

No one can say that manufacturers aren't innovating. In fact, manufacturers have made great process improvements over the last several decades (such as Six Sigma and lean manufacturing).

In today's world, the digital manufacturing revolution is changing everything. However, on factory floors across the country, there is still a considerable amount of unconnected devices and data silos.

As a manufacturer, you could harness that untapped potential to drive even more efficiency and productivity. But, in the current state, those silos and unconnected devices quickly become operational bottlenecks.

The emergence of Industrial Ethernet as a standard on the plant floor is a game changer, however.

In combination with other digital manufacturing technologies, Industrial Ethernet is:

- Eliminating network silos
- Driving a convergence of industrial and enterprise networks
- Bridging gaps between operations technology (OT) and information technology (IT)

Amid their many benefits, these advancements also introduce potential challenges to the factory floor, including:

- Security risks
- Database management challenges
- Network management issues

Adapting to this new world of "always on" data means embracing the possibilities wisely. The goal is to collect and leverage all relevant data, without introducing new risks to your company.

### Cisco Digital Network Architecture (Cisco DNA) for Manufacturing

Today, **nearly 4 out of 5 manufacturers expect moderate to major effects from digital disruption[1].** This relentless pressure on manufacturers leads them to find new ways to innovate and squeeze more productivity from production facilities.

Cisco DNA revolutionizes how manufacturers design, build and manage enterprise and production facilities. It means faster deployment and simpler, centralized management of your network, getting multiple network locations up and running in days rather than months. It also offers actionable network-wide insights for smarter operations on the production line. **With Cisco DNA for manufacturing solutions, manufacturers can deliver key digital capabilities with a digital-ready foundation - securely, simply, and intelligently.**

Learn more about Cisco DNA for Manufacturing.

1. http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/digital-network-architecture/at-a-glance-c45-739029.pdf

# Section I. Embracing the possibilities of a fully connected factory

We see two major possibilities as you work to connect previously unconnected devices: improved plant visibility and advanced analytics.

## Improved plant visibility

**According to U.S. Bureau of Economic Analysis figures, the average age of all fixed assets stood at 22.8 years in 2015, the oldest in records going back to 1925[2].** As a result, most of the machinery in these manufacturing operations aren't connected to the network.

However, times are changing. Today, Industrial Ethernet is the standard for plant networks. And advances in industrial networking continue to progress. Standards like Time Sensitive Networking (TSN, IEEE 802.1) allow even deterministic applications that need extremely tight control loops to run over Industrial Ethernet. Ultimately, this drives more interoperability across the plant floor.

With all these innovations, manufacturers are now uniting "data islands." In fact, **manufacturing produces more data than any other sector in the US economy[3]**.

By strategically tapping into that data, you can:

- Gain full visibility into the performance and working conditions of machinery and assets, which:
  - Improves overall equipment effectiveness (OEE)
  - Reduces downtime
  - Drives faster new product introduction (NPI)
  - Improves inventory turns
- Increase coordination of maintenance schedules. This helps avoid unplanned downtime and optimizes plant cells through predictive maintenance.
- Get insights into energy usage, then optimize workflows and operations to reduce costs.

*"Manufacturing produces more data than any other sector in the US economy."*

Tweet this thought

## Cisco Kinetic – Unlock the Value of your IOT Data

Get real business value from all of your IoT data. Use the power of the Cisco® Kinetic platform to extract, compute, and move data from your connected things to various applications.

With Cisco® Kinetic, you can:

- **Extract data from disparate sources, regardless of protocol**
- **Compute data anywhere from edge to destination to provide processing where it's needed**
- **Move data programmatically to get the right data to the right applications at the right time**

Learn more about Cisco Kinetic.

2. https://www.bloomberg.com/news/articles/2016-10-06/america-is-aging-in-more-ways-than-one
3. http://www.mckinsey.com/business-functions/operations/our-insights/digital-manufacturing-the-revolution-will-be-virtualized

# Section I. Embracing the possibilities of a fully connected factory

Connectivity is only part of the story. Once your devices are connected, you need actionable analytics to integrate the data into business processes. This influx of new data from the plant floor creates new opportunities, including:

1. **Increasing profitability.** Analyzing data from machinery can help you identify production and policy improvements. For instance, maintenance, repair, and operations (MRO) can take a lot of time and resources. Implementing condition monitoring with predictive analysis can help you:
   - Avoid downtime
   - Reduce human intervention
   - Improve maintenance scheduling
   - Diagnose issues with considerable accuracy
2. **Identifying efficiencies.** Real-time data analysis can help you improve quality, yield, and OEE. Many manufacturers are integrating data from enterprise resource planning (ERP) and manufacturing execution systems (MES). This allows you to compare real-time inputs and historical data to:
   - Drive better utilization
   - Eliminate poor visibility
   - Identify potential events before major disruptions
   - Ensure quality control early across production runs
3. **Improving business operations.** Through analytics, you can view, understand, and track the flow of materials as they travel around plant floor. This drives better efficiency and helps avoid production interruptions. This information also improves supply chain process planning, scheduling, and inventory management–improving margins and driving a better customer experience.

## Cisco and SAS edge-to-edge enterprise IoT analytics

In the connected world of the Internet of Things (IoT), petabyte-scale data is generated in real time. The capability to capture, monitor, and rapidly process information is essential for the modern enterprise.

**Cisco and SAS have partnered to create Edge-to-Enterprise IoT Analytics Platform which allows enterprises to quickly collect, process, and analyze massive amounts of data in real time, both at the network edge and in the enterprise data center.** The goal of IoT is valuable outcomes. The only way to achieve this value is through the timely application of analytics.

Learn more about Cisco and SAS' approach to IoT analytics.

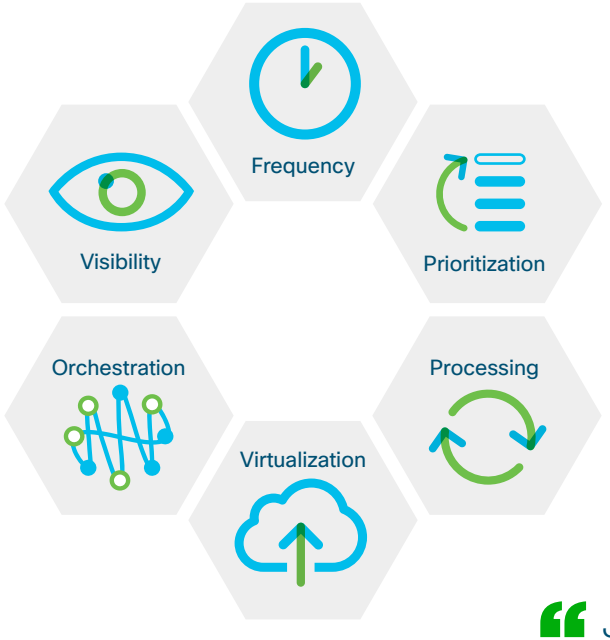
# Section II: Avoiding the pitfalls

By 2020, the International Data Corporation estimates that connected IoT will see around 30 billion endpoints. That number could exceed 80 billion by 2025. And, by 2019, 43 percent of IoT data will be processed at the edge[4].

While there are tremendous benefits from these connected devices, there are also potential risks. Two common pitfalls manufacturers often encounter are data overload and security threats.

## Avoiding data overload

All these new connected devices will create a tidal wave of data. That means your organization needs to decide where that data should go, how often to send it, and how to use it. You must assess your data flows and consider six key factors.




1. **Frequency:** Industrial operations often generate a high frequency of relatively small amounts of data. **But just because you can pull data every 10 milliseconds, doesn't mean that's a good idea.** It's important to understand how often the data adds value to the business, and pull it only that often. This avoids unnecessary data pulls that can cause data overload, network latency, or even take the network down.

   Network analytics can also help spot these anomalies–identifying issues or unknown changes outside of normal traffic specifications. One strategy that savvy analysts follow is to vary the data-density based on time. In other words, keep higher density data for a short period of time, then lower density data after that. So you might keep data every 100ms for two weeks, then dispose some of that data and store data from every second for two months, then every second for a year, etc.

2. **Prioritization:** As more devices connect online, you need to determine which services get priority within the network. Some devices are more sensitive to delay, jitter, and packet losses. Therefore, it's important that noncritical traffic doesn't affect network reliability. By using TSN and automating quality of service (QoS) parameters, your organization can prioritize critical traffic over noncritical traffic, ensuring network integrity. Even under heavy congestion, QoS features can help make sure that important traffic reaches its destination.
3. **Processing:** Traditional computing models send the data to the core data center for analysis. However, this is impractical in many manufacturing scenarios. Often, manufacturing data requires real-time analysis and response times measured in milliseconds. You need to see mission critical data in real-time. In some at the edge of the network, reducing latency

> *"Just because you can pull data every 10 milliseconds doesn't mean that's a good idea."*

Tweet this thought

4. Source: IDC Dawn of the DX Economy and the New Tech Industry, doc #DR2017_GS1_FG, February 2017

# Section II: Avoiding the pitfalls

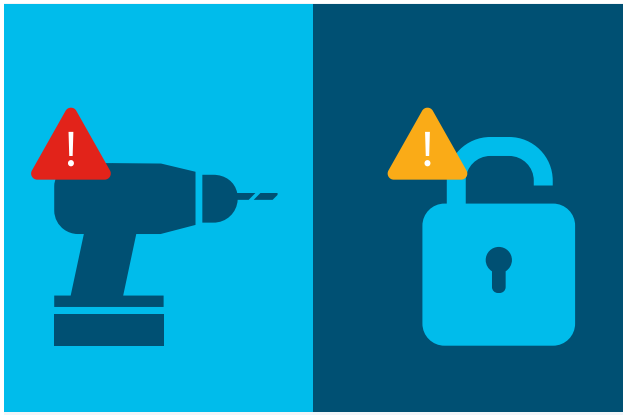
and ensuring data is properly delivered to end users. Network architects should consider a hybrid solution of edge computing and centralized data computing within the data center.

4. **Virtualization:** Many manufacturers are decoupling hardware from operating systems to support standardization, centralized management, pooling of resources for servers and applications, and disaster recovery. While virtualization can help support more business flexibility, it can also impact data center design, data consumption storage, security, and network performance. Predictable application performance and availability is critical for these services.
5. **Orchestration:** The influx of data from IoT increases the importance of mapping out who receives that data and how they consume it. Operations teams may gain new insights from the connectivity of the machinery, but it only benefits them if that data is applicable to their daily tasks and outputs. Sharing too much data can create paralysis within teams. For instance, you might want to share certain data with a machine builder to help optimize that machine operation–but you may not want that machine builder to see enough data to know exactly how many parts you produce.

   In addition, without proper orchestration, sensitive information can unintentionally become available to wrong parties. It's important to implement consistent control and awareness of who receives the data, when they receive it, how it's delivered, and why they receive it. Automation is key in managing and reducing the complexity of orchestration processes.
6. **Visibility:** Modern network infrastructures are no longer isolated areas of information at the device. Dashboard reporting tools can now collect data from the network as it operates, providing context that helps OT and IT teams better understand the operation of the network and support learning that drives network adaption and automation.

# Reducing the risk

Manufacturers typically want the business benefits of connecting new devices, but not at the cost of security.



Security breaches on the plant floor can create safety risks and cause major downtime such as loss of IP (recipes, program code).

Security breaches on the enterprise side can create data and privacy risks that can threaten a company's reputation and customer trust.

Protecting production integrity is mission critical, but connecting previously unconnected devices can introduce new security vulnerabilities.

It's important to have security solutions that are fully tested for compatibility. This ensures efficient operation and protection.

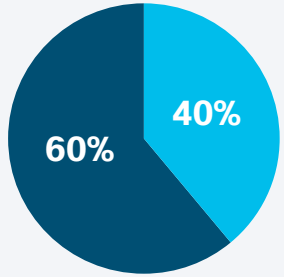
In many cases, legacy factory devices were never designed with security in mind and cannot protect themselves from vulnerabilities. And it's not just the legacy equipment that's at risk–new devices can have issues as well. Yes, many device vendors have made large strides in the security of their offerings, but many are still behind the curve. Often, they must continually upgrade devices already deployed in the field. These resulting vulnerabilities create ample opportunities for attackers to exploit devices and gain network access.

Gaps in visibility can also create security risks. In many cases, devices are added to the network ad hoc, either through OT/IT misalignment or from a "shadow IT" project. This is no longer acceptable.

Now more than ever, it's important to have full visibility. You must be able to discover, onboard, and automatically segment device traffic to ensure security.

Modern networks need to operate as a security extension. They need to provide context into the network and identify traffic patterns and the flow of data. By capturing and analyzing data, you can establish a network's baseline traffic. Then, you can set up alerts to notify you when traffic anomalies occur.

According to the 2017 Cisco Mid-Year Security Report, 40 percent of the manufacturing security professionals said they do not have a formal security strategy[5].

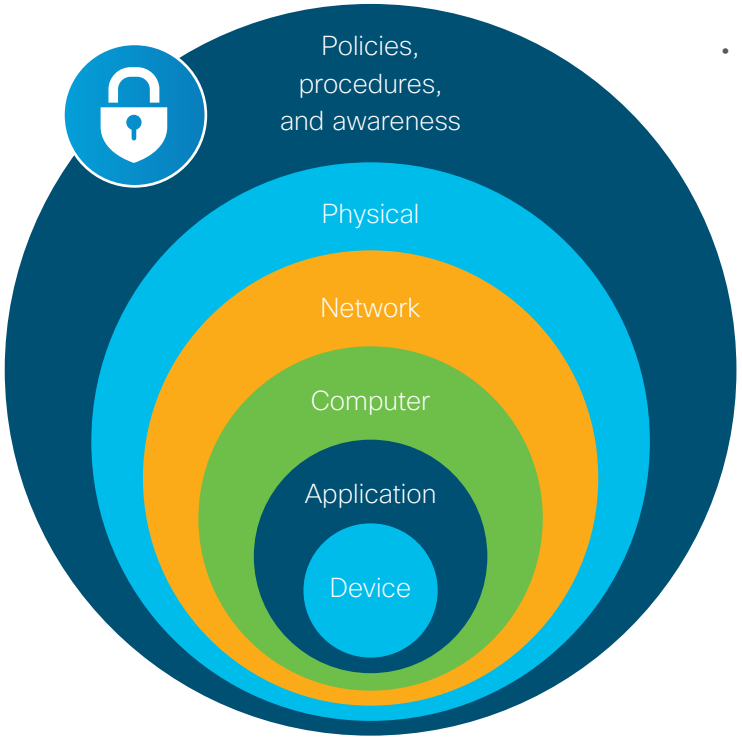



5. http://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/1456403/Cisco_2017_Midyear_Cybersecurity_Report.pdf?elqTrackId=f6ccd8439e9945639096a9846044695a&elqaid=5897&elqat=2

# 3 ways to protect your data

So, how can you mitigate these security risks? Deploy a combination of trusted best practices, new technologies, and strategies.

1. **Defense in depth:** Modern, advanced threats require a holistic security strategy. That's why manufacturers turn to a defense-in-depth approach. "Defense-in-depth" strategies incorporate layers of independent security controls (physical, procedural, and electronic).




2. **Trusted best practices:** In the modern landscape of IoT, some old best practices still apply. For instance:
   - Device segmentation remains an important first step
   - It's still important to create specific policies that define device access
   - Strong firewalls are critical

3. **New technologies:** At the same time, newer technologies also play an important role:
   - Network visibility analytics: New offerings provide constant reporting and monitoring.
   - Access control: Today, you can define permissions at the user and device level, with a profile that notes where they are entering and exiting the enterprise, as well as what they are trusted to access.
   - Threat intelligence: Attackers are developing new attacks at an increasing rate, and manufacturing is becoming a highly targeted sector. Intelligence from third-party feeds can help correlate and detect incidents before they become widespread.

## How strong is your defense-in-depth security strategy?

A strong defense-in-depth strategy covers procedural, physical, and electronic security.

Want to learn more? The best first step is understanding where you are today.

Get started.

# What's next?

The manufacturing industry is modernizing at a faster rate than any time in history. Organizations are breaking down silos and connecting previously unconnected devices.

This means you'll soon have access to more data than ever before, driving productivity, reducing downtime, and improving OEE.

At the foundation, a strong network architecture is critical for enabling you to drive these efficiencies and the business forward. This requires bold steps and a modern approach in thinking through network architecture, connectivity, visibility, and security and bridging the gap between IT and OT.

Cisco is a true partner in these efforts–helping you unlock the potential of connectivity while avoiding the pitfalls.

## Ready to take the next step? Learn more about:

- Cisco Connected Asset Manager for IoT Intelligence
- Cisco DNA for Manufacturing
- Cisco Connected Factory
- IoT Threat Defense

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.