Palantir

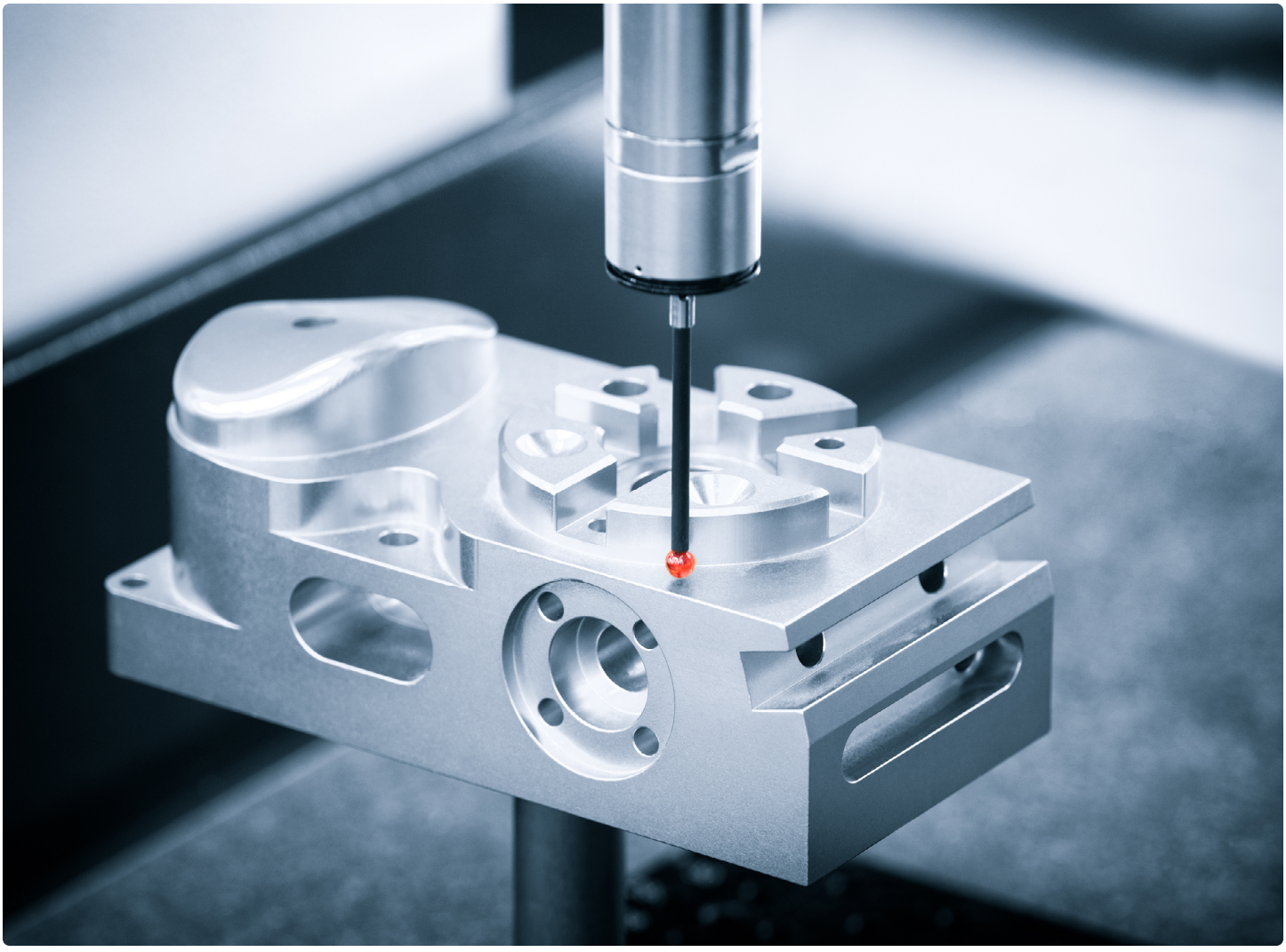
Palantir Foundry for Industry 4.0:

Scaling the Future of Enterprise Manufacturing Operations

Palantir Technologies UK
→ palantir.com

March 2022

→ palantir.com



Palantir

Palantir Foundry for Industry 4.0:

Whitepaper — March 2022

Introduction: The State of Industry 4.0

AT A GLANCE

Founded	2003
Locations	20+
Global Employees	3,300+

INTRODUCTION

—— We were founded in 2003 and started building software for use by the intelligence community in the United States to assist in counterterrorism investigations and operations, as well as by commercial enterprises. We have built two principal software platforms, Palantir Gotham and Palantir Foundry.

Palantir Gotham is utilized by analysts at defense and intelligence agencies and it enables users to identify patterns hidden deep within datasets, ranging from signals intelligence sources to reports from confidential informants. Palantir Foundry transforms the ways in which organizations interact with information by creating a central operating system for their data.

OUR CLIENTS

Introduction: The State of Industry 4.0

The Data Foundation

Petabytes of data are created daily in every industry and context imaginable. Machines in factories hold troves of sensor and operational data. Vehicles and airplanes generate a wealth of telemetry data. Video and audio data fly across networks every second. Structured data — like shift schedules, lab data, and the information contained in ERP platforms — augments unstructured data, generating an endless trails of intel for companies to harness.

The goal of Industry 4.0 is to operationalize all this data. Companies that are able to logically create and organize workflows using data can maximize production output, save time and resources they would otherwise spend on maintenance, and build manufacturing scenario simulations before implementing expensive changes in the field.

Although the promises of Industry 4.0 are exciting, organizations often encounter challenges implementing their Industry 4.0 ambitions.

Challenges with Industry 4.0 Projects

DATA INTEGRATION HEADACHES

The large, compounding volume ** of data that companies can access is both a blessing and a curse. Data is only an asset when it's accessible. Too often, analysts find themselves wading through endless sensor, video, telemetry, ERP, lab, and other potentially useful data without knowing the right ways to bring it all together. Flooding databases and analytical applications with unstructured data makes it difficult to separate the signal from the noise, preventing you from making effective use of the data you have at hand.

DISPARATE SOLUTIONS LEAD TO CRIPPLING COSTS AT SCALE

Because so many kinds of projects fall under the Industry 4.0 umbrella, most vendors have an overwhelming number of solutions and applications for IT and business staff to sort through. For example, vendors often expect firms to cobble together a machine learning solution, a cloud warehouse, and a sensor management solution — and that's just to start.

This lack of consolidation doesn't just result in more complicated projects. It also means that the more opportunities to leverage your data, the greater the spend on different connectors, services, and solutions, resulting in a runaway budget. Suddenly, a project originally scoped for two connectors and two applications now requires six connectors, six applications, and higher costs than anticipated.

Introduction: The State of Industry 4.0

Challenges with Industry 4.0 Projects ↳ Continued

LONG TIMELINES AND AND COMPLEX CONFIGURATIONS

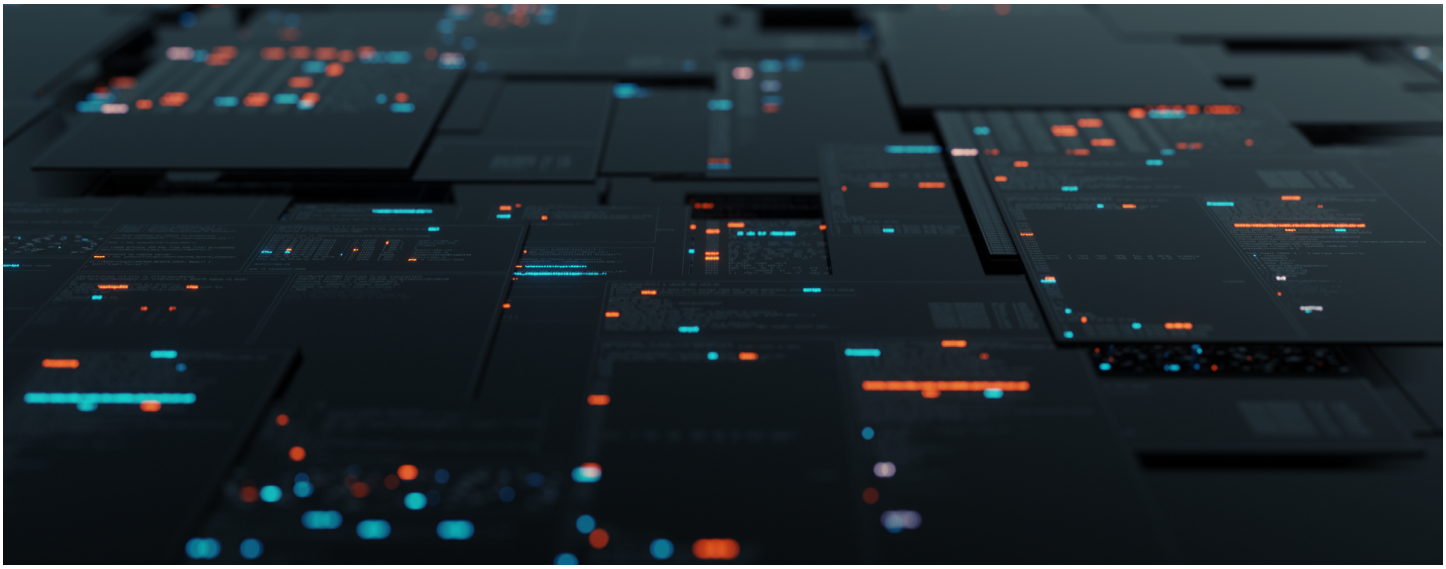
When it comes to Industry 4.0 projects, many companies make ambitious goals, create a reasonable roadmap, and marvel at their pre-work. But while these roadmaps look great on paper, they don't account for the difficulty of integrating structured and unstructured data and the subsequent creation of useful workflows. Companies struggle to sift through numerous cloud storage warehouses, build custom operational tools, and allocate the required internal resources, resulting in much longer timelines (and more complicated roadmaps) than originally anticipated.

Midsize firms face the challenge of scale and resourcing. These organizations need a solution that can scale without requiring them to hire tons of engineers.

Enterprise firms, on the other hand, certainly could scale headcount, but doing so would be a tremendous waste of time and resources. Enterprises need to focus on innovation. This requires access to tools that remove the minutiae of managing workflows from engineers' plates. Enterprise resources are better served building and delivering new capabilities, not optimizing Excel reports.

THE BOTTOM LINE: DATA IS ONLY USEFUL IF YOU CAN USE IT TO BUILD OPERATIONAL WORKFLOWS

With all of the data coming from machines, devices, vehicles, and more, your enterprise has no shortage of data. But are your integrations adept enough to allow for operational decision making? Can you simulate changes to your operations before implementing them? And can you build workflows spanning the IT team, business strategists, and machine operators?

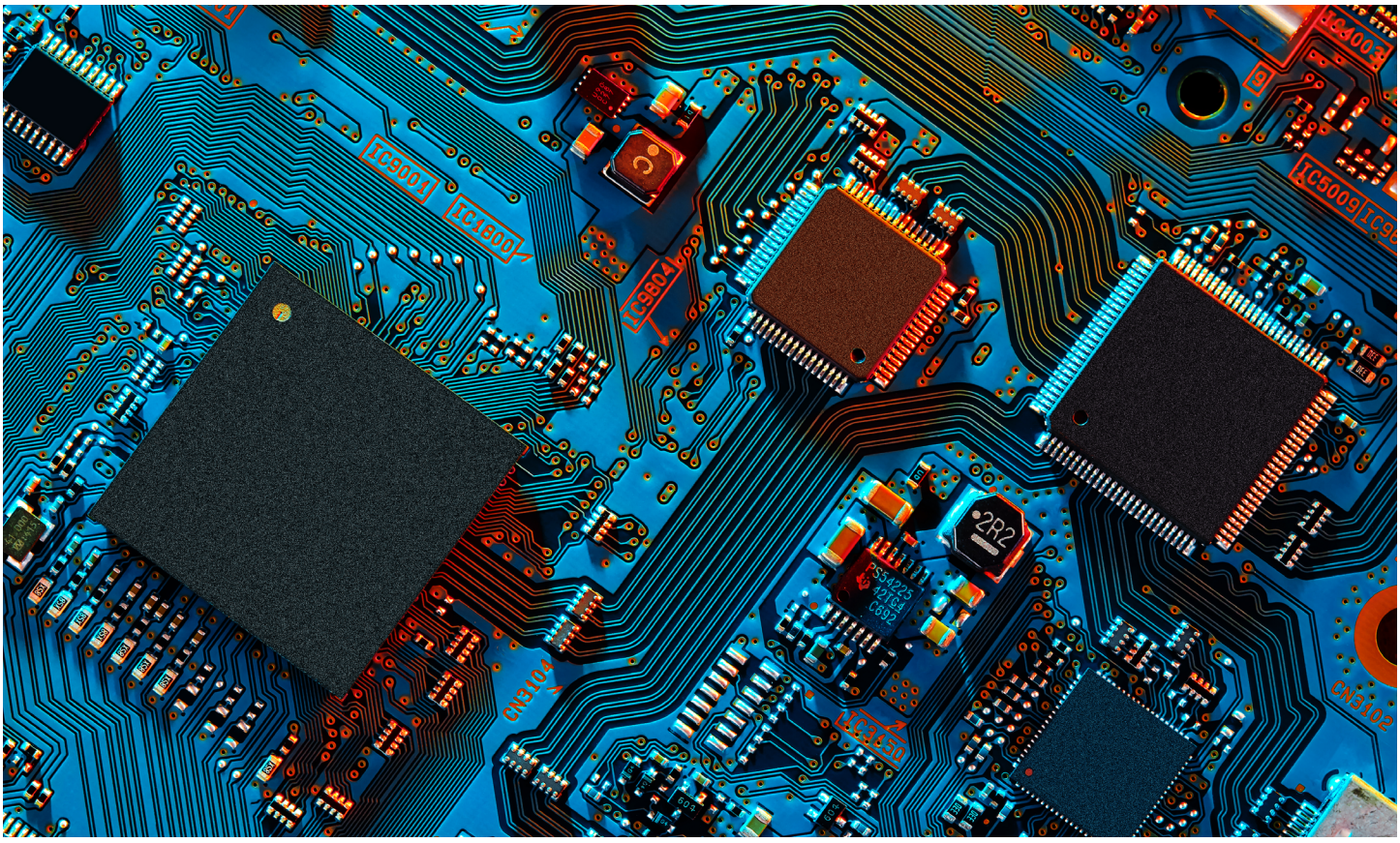


The Nine Pillars of Industry 4.0

—— The nine pillars of Industry 4.0, originally outlined by Boston Consulting Group (BCG) in 2015[1] and summarized below, are the technological advancements that make the Fourth Industrial Revolution possible. They bring together the physical and digital — human and machine. Many of these technologies have been used in manufacturing for some time, but it's their convergence that makes Industry 4.0 a reality.

01	Big Data and Analytics	In an Industry 4.0 context, the collection and comprehensive evaluation of data from many different sources — production equipment and systems as well as enterprise and customer management systems — has become table stakes.
02	The Cloud	The more production-related initiatives a company undertakes, the more it needs to share data across sites. Meanwhile, cloud technologies continue to get faster and more powerful. Companies are increasingly deploying machine data and analytics in the cloud, thus enabling more data-driven services for production systems.
03	Cybersecurity	It's no surprise that Industry 4.0 boosts increased connectivity and the use of standard communications protocols. As a result, the need to protect critical industrial systems and manufacturing lines from cybersecurity threats rises dramatically. For this reason, secure, reliable communications, together with asset & vulnerability management for machines and identity verification of users, are essential.
04	Horizontal and Vertical System Integration	Industry 4.0 allows companies, departments, functions, and capabilities to become much more cohesive. Cross-company, universal data integration evolves and enables truly automated value chains.
05	The Industrial Internet of Things	Industry 4.0 means that more devices are enriched with embedded computing. This process allows devices to communicate and interact both with one another and with more centralized controllers. It also decentralizes analytics and decision-making, thus enabling responses in real time.
06	Simulation	Simulations are a cornerstone of Industry 4.0. They're used extensively in plant operations by leveraging real-time data to mirror the physical world. Done right, these models allow operators to test and optimize settings in numerous variations, thereby driving down machine setup times and increasing quality.

06	Simulation	Simulations are a cornerstone of Industry 4.0. They're used extensively in plant operations by leveraging real-time data to mirror the physical world. Done right, these models allow operators to test and optimize settings in numerous variations, thereby driving down machine setup times and increasing quality.
07	Additive Manufacturing	The classic example of additive manufacturing is 3D printing. Instead of prototyping individual components, companies can now produce small batches of customized products. The resulting advantages include the speedy manufacturing of complex, lightweight designs.
08	Augmented Reality	Augmented reality (AR) systems support a variety of services, such as selecting parts in a warehouse and sending repair instructions over mobile devices. With AR, companies can provide workers with real-time information that improves decision-making and work procedures.
09	Autonomous Robots	Autonomous robots can interact with each another and work safely side by side with humans. Over time, these robots will cost less and gain an increasing range of capabilities.



Palantir

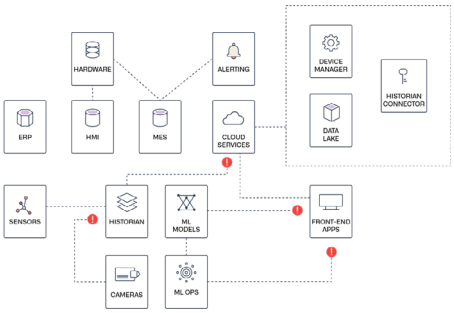
Palantir Foundry for Industry 4.0:

Whitepaper — March 2022

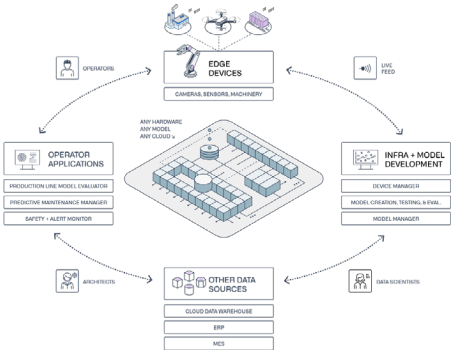
Palantir Smart Manufacturing Solution

—— Palantir's approach to Industry 4.0 focuses on enabling converged IT/OT workflows derived from data across the horizontal and vertical levels of the Purdue model for ICS security.[2]

EXISTING EDGE ARCHITECTURES



PALANTIR FOR INDUSTRY 4.0



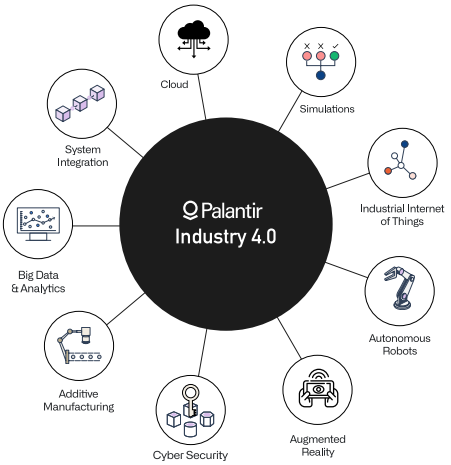
The Palantir Foundry platform can help address:

→ [Connectivity & Models for] Autonomous Robots

→ [Connectivity & Models for] Additive Manufacturing

Big Data and Analytics

Big Data and Analytics is the core capability of Palantir Foundry. Foundry is adept at managing large, complex data sets from a varied set of data sources that traditional data processing software struggles to manage. It has fifty times faster compression ratios on machine-generated data compared to other common storage formats. This includes hard-to-manage volumes of data, both structured and unstructured.



Cloud

Cloud integration is a key requirement for Industry 4.0. The use cases are varied and include the integration of field-level sensor data with cloud applications, including but not limited to condition monitoring systems, BI/BA apps, enterprise dashboards, and more. With Foundry, you get out-of-the-box connectors for various cloud service providers. Foundry also enables ingestion of data from systems across different layers of the Purdue model.

OT/ICS Cybersecurity

Before the advent of Industry 4.0, cybersecurity goals involved defending organizational parameters, such as private computer networks. The methods used to prevent breaches were limited to firewalls, anti-malware software, and intrusion detection systems. In the ever-evolving manufacturing industry, the integrated and distributed nature of Industry 4.0 makes it difficult to completely secure a business from cyber threats due to a number of factors:

→ Data sharing: With an Industry 4.0 approach to manufacturing, data is shared across supply chains and various stakeholders. Systems are being integrated between consumers and suppliers. Data is distributed all through these systems, which means a greater security scope.

→ Points of attack (attack vectors): Since these systems involve a number of stakeholders in the value chain as well as consumers, the number of user access points drastically increases. These access points are all possible points of attack. The more attack vectors to cover, the harder (and more expensive) it becomes to secure the entire system.

→ Convergence of information technology and operational technology: With so much sensor, telemetry, video, and other hardware data being ingested and analyzed, the lines between software and hardware get blurred. To secure Industry 4.0 systems from end to end, companies must consider both the digital and physical components. The methods used previously, such as anti-malware, intrusion detection systems, and firewalls, may fall short of the mark when the Industry 4.0 systems involve a wide variety of software and hardware systems.

→ Playing catch-up: Even prior to Industry 4.0, cybersecurity threats tended to be one step ahead of potential solutions or preventive measures. Commonly, organizations set up firewalls or intrusion detection systems in an attempt to react to these new and novel threats. However, the threatscape only increases with Industry 4.0, given that systems cut across industries and have possibly thousands of different devices and networks interacting with each other. The possibility of new threats increases exponentially.

Palantir Smart Manufacturing Solution

CYBERSECURITY FROM THE FRONT LINES TO THE FACTORY FLOOR

The interconnectedness of Industry 4.0 makes airtight security non-negotiable. Foundry was built from the ground-up to power mission-critical workflows in the most secure environments. With accommodations for Department of Defense Controlled Unclassified Information (CUI) and National Security Systems (NSS), Foundry is an IL5 SaaS platform trusted and deployed both in factories and in active combat zones. Palantir is committed to ensuring security threats are kept at bay, so enterprises can focus on innovation rather than locking up the fort.

From a cybersecurity standpoint, Foundry's capabilities can be divided into six core work streams:

- → Asset management
- → Cyber threat intelligence
- → Incident management
- → Vulnerability management
- → Alert management
- → Threat hunting
- → Incident response

Foundry's capabilities are focused on creating integrated workflows that complement these various work streams, all with the goal of collaboratively achieving the cyber goals of the organization. For example, if an organization with a converged IT/OT environment deems "detecting cyber threats" a goal, Foundry enables workflows such as cyber threat intelligence, risk management, and incident management for seamless collaboration between various security teams, as shown below.

This workflow involves collaboration between the threat detection (cyber operations) and cyber threat intelligence teams to understand and analyze how current detection coverage compares to the threat landscape. Foundry enables analysts to unify the current threat detection data available within an organization (SIEM Tools, IPS/IDS etc.) with threat profiles in a single environment. From this centralized view, analysts across both cyber operations and cyber intelligence themes can work together securely to identify gaps and operationalize decision making.

Palantir Smart Manufacturing Solution

ASSET MANAGEMENT

Asset management (AM) is usually the biggest challenge and pain point in any industrial setup. To successfully build additional cybersecurity workflows on top of AM, it is vital that Foundry has visibility over all assets. The methodology is to start with rapid asset discovery and onboarding, and then take a deeper dive with precision onboarding for legacy data sources or whose accessibility is difficult due to their architectural placement.

CYBER THREAT INTELLIGENCE (CTI)

Palantir Foundry enables CTI professionals to manage their threat profile by integrating internal and external sources into a single environment. By ingesting and unifying this data, analysts can conduct their analysis from a single source of truth. Foundry also builds a digital representation of an institution's cyber environment based on industry-level standards and frameworks (STIX, ATT&CK etc.) by extracting entities and objects from traditional cybersecurity data sources and modeling establishing intuitive relationships between these objects and entities. Leveraging this data model, analysts can easily establish how various threats interact with parts of the environment, including commonly exploited vulnerabilities, systems running vulnerable software, or user groups who are commonly targeted, and prioritize their operations and defenses.

INCIDENT MANAGEMENT

The most reliable incident management solutions are highly flexible. They combine the automation and high-scale information processing of machines with the context and intuition of human analysts to ensure speed and precision in managing threats.

Foundry allows incident responders to rapidly add and link information that is being discovered in real time as they investigate and respond to incidents. This information is automatically captured in the platform for future analysts to benefit from as a form of internal threat intelligence. With its knowledge management capabilities, Foundry enables analysts to collaborate and share discoveries along with their observation and analysis techniques.

VULNERABILITY MANAGEMENT

Industrial networks contain thousands of OT and IoT devices from a variety of vendors. Unfortunately, most of those devices aren't designed for the level of security required in an Industry 4.0 world. Many ICS devices are, in fact, insecure by design — lacking authentication, encryption, and other security standards that typically apply to IT applications and systems. The challenge in this space is to identify which devices on the network are vulnerable and in need of special protection, as well as which ones require firmware updates or other actions to close the door on cyber risks.

Foundry can address this operational challenge by automatically identifying your system vulnerabilities. Foundry allows companies to identify devices at risk by integrating with the U.S. government's National Vulnerability Database (NVD), which provides standardized naming, description, and scoring. To help your security team prioritize high-level exposure points, the platform displays all vulnerabilities by vendor, severity level, and more in a dedicated view. Plus, it offers additional context on each vulnerability for deeper troubleshooting and remediation assistance.

ALERT MANAGEMENT

Most organizations have a variety of defensive measures already in place, such as firewalls, IDS/IPS, and AV/endpoint protection, which generate thousands of alerts. As a single pane of glass, Foundry enables analysts to prioritize and triage alerts through its case management offering. You can increase visibility, mobility, and scalability; expand the degree of contextual information; and group alerts into meaningful and actionable intrusions.

THREAT HUNTING

Palantir Foundry can enable threat hunting, which cybersecurity professionals Chris Peiris, Binil Pillai, and Abbas Kudrati define as "the proactive, analyst-driven process to search for attacker tactics, techniques, and procedures (TTP) within an environment."3 Attacker TTP must be researched and understood to know what to search for in collected data. Information about attacker TTP is mostly derived from signatures, indicators, and behaviors observed from threat intelligence sources. A prime example of threat hunting capabilities would be configuration-based detection, which identifies deviations from a known architecture or design like the known form of an internet protocol (IP) packet header or devices designed to communicate in a static pattern.

INCIDENT RESPONSE

Developing incident response capabilities enables organizations to prepare against evolving threats within their operational framework. By controlling and directing how security events and incidents are handled, companies have the essential tools to proactively respond to cyber threats:

- → Track security incidents and active threats
- → Track and analyze evidence from digital forensics
- → Collaborate through seamless tasking and reporting capabilities
- → Translate lessons learned into context and options for strategic decisions

Additional capabilities related to cybersecurity include:

- → Generation of baseline topology and behavior model, including all devices, ports and connections
- → Track and analyze evidence from digital forensics
- → Anomaly detection capability, which creates a behavioral network model using multiple parameters, including device sequence sampling time, frequency of operational values and more, toward detecting behavioral anomalies and compliance assessment
- → Real-time, KPI-backed visualizations and custom dashboards as part of business intelligence

Palantir

Palantir Foundry for Industry 4.0:

Whitepaper — March 2022

Horizontal and vertical system integration

Horizontal and vertical integration is the backbone of Industry 4.0. In pursuit of the concept of the "smart factory," horizontal and vertical integration center around technologies, processes, and systems that enable the collection, collation, communication and use of data. Horizontal and vertical integration offers substantial benefits by achieving heightened levels of alignment across entire organizational ecosystems, from the factory floor to enterprise-level systems across the supply chain and in all processes, business units, and partners alike.

WHAT IS VERTICAL INTEGRATION?

Industry 4.0 vertical integration involves connecting all business units and processes within your organization. In other words, it's all about converging operational technology (OT) at the production level with information technology (IT) at the enterprise level.

WHAT IS HORIZONTAL INTEGRATION?

Industry 4.0 envisions connected networks of cyber-physical and enterprise systems that introduce unprecedented levels of automation, flexibility, and operational efficiency into production processes. This horizontal integration takes place at several levels:

→ On the production floor: Always-connected machines and production units each become an object with well-defined properties within the production network. They constantly communicate their performance status and, together, respond autonomously to dynamic production requirements. The ultimate goal: to make smart production floors that can cost-effectively produce lot sizes of one, as well as reduce costly downtime through preventive maintenance.

→ Across multiple production facilities: If an enterprise has distributed production facilities, Industry 4.0 could promote horizontal integration across plant-level Manufacturing Execution Systems (MES). In this scenario, production facility data (inventory levels, unexpected delays, and so on) are shared seamlessly across the entire enterprise and, where possible, production tasks are shifted automatically among facilities in order to respond quickly and efficiently to production variables.

→ Across the entire supply chain: Industry 4.0 proposes data transparency and high levels of automated collaboration across the upstream supply and logistics chain — which provisions the production processes themselves — as well as the downstream chain, which brings the finished products to market. Third-party suppliers and service providers must be securely but tightly incorporated horizontally into the enterprise's production and logistics control systems.

Horizontal and vertical system integration

HOW FOUNDRY ENABLES HORIZONTAL AND VERTICAL INTEGRATION

From its inception, Foundry was designed to help organizations integrate all of their systems, business units, and processes enabling them to effectively operationalize their data. With Foundry, you're able to not only bring all of your structured and unstructured data together and organize it logically, but also analyze it and write decisions back to the relevant systems. This is what makes Foundry a comprehensive platform for data ingestion, data modeling, decision-making, simulation, AI/ML model building, and more.

Vertical Integration with Foundry:

→ Vertical integration creates connections between production and other parts of a manufacturing organization. Essentially, it networks beyond traditional production hierarchy levels — from the sensor to the business level of the company. Foundry helps you achieve tighter integration with assets at various levels, such as:

→ ERP interface (SAP ERP, Microsoft Dynamics, etc.)

→ MES

→ SQL Server Interface (Data Historians)

→ Web Server or HTML5 Web Engine (Application Servers)

→ Cloud Integration

Horizontal Integration with Foundry:

→ In the typical manufacturing environment, horizontal integration must connect many types of equipment. Foundry connects with any system via these methods and more:

→ API

→ Agent-based (Magritte)

→ Log dump

→ Syslog

→ Third-party tool integration (Partners)

→ Custom connectors

→ Third-party sensors

With Foundry, you can build custom workflows across the value chain to achieve greater visibility and operational efficiency. The goal? To make your organization data-driven at the core and help you maximize the value of your data through globally optimized operations.

Simulation (Digital Twin)

A digital twin of your factory, manufacturing processes, or another relevant scenario could enable you to predict how a product or process will perform, while still retaining enterprise-wide data integrity. Foundry applications can integrate the Internet of Things (Industry 4.0 tech pillars), artificial intelligence, and software analytics to enhance the output.

Other capabilities of Palantir Foundry

PREVENTIVE MAINTENANCE

One of the most sought-after use cases of Industry 4.0 is preventive maintenance, especially in the manufacturing sector. The idea is to go beyond simple problem analysis and prevent problems before they occur. The objectives that relate to this kind of use case are:

→ Prevent process anomalies
→ Prevent machine breakdowns
→ Prevent product non-conformities

Preventive maintenance is comprised of data from:

→ Time-series data
→ Real-time analytics
→ Artificial intelligence

Foundry works on normal and large data sets and is scalable, modular and portable. It extracts relevant features from the time series generated by production machines and uses these features to feed into any artificial intelligence algorithm.

FULL WRITE-BACK CAPABILITIES

Knowing the right optimizations to put into place is only half the battle. Implementing changes automatically is crucial if you actually want to make processes more efficient, less costly, and more powerful. With Foundry, you can not only capture the data you need to make the right decisions, but also use native frameworks to feed these decisions to the underlying systems.

For example, an airplane manufacturer can not only use Foundry to understand where defects might be occurring on the assembly line, but also determine a next course of action (say, sourcing part #258 from a British supplier instead of a French supplier) and implement it quickly.

Since Foundry natively includes two-way (bidirectional) sync, new operational data constantly gets fed back into the platform, ensuring a steady state of optimization.

Conclusion

Sources:

1 Rüßmann, Michael, et al. “Industry 4.0: The Future of Productivity and Growth in Manufacturing Industries.” Boston Consulting Group, 9 Apr. 2015, https://www.bcg.com/publications/2015/engineered_products_project_business_industry_4_future_productivity_growth_manufacturing_industries.

2 What is the Purdue Model for ICS Security? Zscaler. (n.d.). Retrieved February 9, 2022, from https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security

3 Peiris, C., Pillai, B., & Kudrati, A. (2021). Threat Hunting in the Cloud: Defending AWS, Azure and Other Cloud Platforms Against Cyberattacks (1st ed.). John Wiley & Sons, Inc.

—— Industry 4.0 starts with data, but data alone isn’t enough. Companies looking to harness the full promise of Industry 4.0 need to integrate all of their data and create operational workflows to improve processes and drive efficiencies.

To really see success, organizations should start by identifying a high-priority, well-defined, yet relatively manageable opportunity to take advantage of their data. For instance, start by creating a monitoring and alerting infrastructure for a single step in the manufacturing process, and then build a workflow that will fix a single error in that step whenever it gets caught. Even a small project like this will require lots of collaboration between IT and OT, but laying that foundation is critical. Only once this project is perfected will you feel confident enough to expand the scope of your work and scale your efforts to more units, more processes, more plants.

Having the right platform in place for ingesting, integrating, analyzing, and acting on your data is also crucial. Palantir Foundry provides a secure and centralized platform for optimizing complex operations, from monitoring raw sensor data to constructing a full digital twin, making it ideal for Industry 4.0 applications. Foundry enables organizations like Scuderia Ferrari (https://www.palantir.com/scuderia-ferrari/), Wejo (https://www.palantir.com/impact/wejo/), and SOMPO (https://www.palantir.com/impact/sompo/) to build operational workflows; realize benefits in weeks, not years; and focus on innovation, helping them become leaders in their respective industries.

Learn more about how Palantir Foundry can make your Industry 4.0 dreams a reality. Reach out to business@palantir.com to schedule a demo and see the platform in action.