Hype Cycle for Managing Operational Technology, 2023

Published 31 July 2023 - ID G00789203 - 96 min read

By Analyst(s): Kristian Steenstrup, Jo-Ann Clynch

Initiatives: Manufacturing General IT Initiatives; Energy and Utilities Technology Optimization and Modernization

> The challenge of managing OT, and in some companies, ET, arises as organizations become integrated digital businesses. This means CIOs and other technology leaders need to understand the characteristics and maturity of the tools and methods at their disposal.

More on This Topic

This is part of an in-depth collection of research. See the collection:

- 2023 Hype Cycles: Deglobalization, AI at the Cusp and Operational Sustainability

Analysis

What You Need to Know

Operational technology (OT) is hardware and software that detects or causes a change in physical processes or events through the direct monitoring and/or control of physical devices (typically, industrial equipment) in the enterprise. OT increasingly interacts with IT and engineering technology (ET). Complicating this, Internet of Things (IoT) components and architectures are used to extend and augment OT. CIOs and other technology leaders are reacting to increased demands for efficiency and responsiveness to changing business requirements, leading to the situation where increasing similarity of IT, OT and ET solutions offers opportunities for combined deployment, support and life cycle management:

- ET is used to define, design, build, simulate, analyze, visualize and validate.
- OT is used to operate and monitor equipment in real time.
- IT is used to record and report transactions and deliver business processes.

Use this Hype Cycle to assess the hype and maturity of the innovations described and the implied risks in order to inform decision making.

The Hype Cycle

The alignment and integration of IT, OT and ET is progressing in many companies due to the increasing overlap in technologies, systems, and processes and, hence, the overlap of skills to manage them and the opportunities for better technology exploitation. In the 2021 Gartner IT/OT Alignment and Integration Survey, 84% of the IT and business leaders surveyed stated that CIOs had significant or complete responsibility for Level 2 OT systems such as SCADA. [1] For many CIOs, there is still much progress to make, as evidenced in the 2023 Gartner CIO and Technology Executive Survey. Sixty percent of CIOs from asset-intensive manufacturing companies indicated they would be investing in IT/OT integration within the next three years. [2]

We have noted new areas of inquiry as clients broaden their inclusion and the scope of IT/OT alignment. These are now included on this Hype Cycle:

- Software-defined assets
- IoT-enabled equipment as a service

There are three clusters of innovations evident (see Figure 1). In the early stages, there are a few items related to managing an OT environment. These are less developed, thus requiring careful evaluation before inclusion into strategy and delivery roadmaps. These include the items listed above plus:

- Cyber-physical systems
- Smart and sustainable building
- Smart robots
- IT/OT/ET alignment

In the middle stages we find:

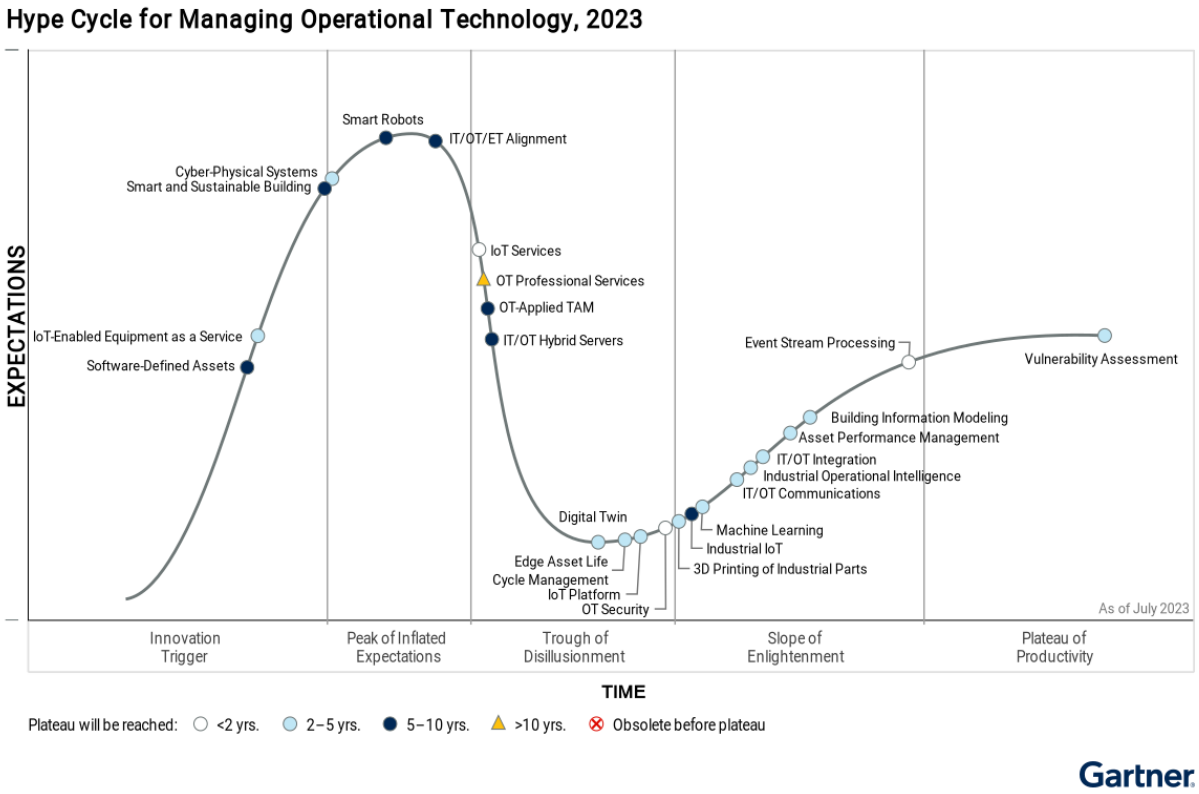
- OT professional services
- IoT services
- OT-applied TAM (technology asset management)
- IT/OT hybrid servers

Toward the later stages, there is a further cluster of more mature technologies marching toward business as usual. These include:

- Building information modeling
- Industrial operational intelligence
- IT/OT integration
- Asset performance management
- IT/OT communications
- Machine learning
- Industrial IoT
- 3D printing of industrial parts
- Digital twins

What is evident from these three clusters (early, mid and late stages) is that clients need to consider the maturity of the technology being dealt with, as some are less developed and/or carry higher risk. Clients should tailor their investments to the maturity of the technology under investigation and their appetite for risk.

Figure 1: Hype Cycle for Managing Operational Technology, 2022



The Priority Matrix

CIOs need to immediately prepare for the impact of innovations critical to their organizations that are two years away from reaching mainstream adoption, specifically:

- Event stream processing — Event stream processing (ESP) is computing that is performed on streaming data (sequences of event objects). Normally, this will be OT data in an industrial environment.
- OT security — As threats and security solutions multiply, a generic category of OT security that was once dominated by network-centric tools is now evolving into multiple categories.

- IoT services — IoT and IoT services function within the broader digital optimization or transformation strategy, especially within asset-intensive industries. The key value of IoT services lies in creating the contribution value of data from non-IT assets and the resulting analytics for digital execution.

Additionally, the transformational innovations reaching near-term maturity (2-5 years) should be included in CIOs' plans for technology assessments in the coming years. Of highest priority should be those that are expected to have a transformational impact:

- Cyber-physical systems
- Digital twin
- IoT-enabled equipment as a service
- Machine learning

Table 1: Priority Matrix for Managing Operational Technology, 2023

(Enlarged table in Appendix)

Benefit	Years to Mainstream Adoption			
↓	Less Than 2 Years ↓	2 - 5 Years ↓	5 - 10 Years ↓	More Than 10 Years ↓
Transformational	Event Stream Processing	Cyber-Physical Systems Digital Twin IoT-Enabled Equipment as a Service Machine Learning	Smart and Sustainable Building	
High	IoT Services OT Security	Asset Performance Management Building Information Modeling Edge Asset Life Cycle Management Industrial Operational Intelligence IoT Platform IT/OT Integration Vulnerability Assessment	Industrial IoT IT/OT/ET Alignment IT/OT Hybrid Servers Smart Robots Software-Defined Assets	OT Professional Services
Moderate		3D Printing of Industrial Parts IT/OT Communications	OT-Applied TAM	
Low				

Source: Gartner (July 2023)

Off the Hype Cycle

- Network access control — This has moved beyond the Plateau of Productivity and is considered normal, unhyped technology.
- Machine learning — This is covered in other Hype Cycles and is not considered OT-specific
- Edge asset life cycle management — This is covered as a concept in the Hype Cycle for Edge Computing.
- Light-cargo delivery drones — This is considered an outcome of OT utilization.
- Lights-out manufacturing — This is considered an outcome of OT utilization.
- IoT-enabled product as a service — This has been replaced by the more descriptive and specific industrial topic of equipment as a service.

On the Rise

Software-Defined Assets

Analysis By: Lloyd Jones

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

A software-defined asset (SDA) encapsulates and virtualizes its hardware capabilities to manage its unique local constraints, by optimizing and modifying its capabilities, behaviors and/or states across control, automation, function and topology to meet global optimization goals. SDAs may orchestrate with other assets and/or systems to meet their assigned goals within a delegated decision envelope.

Why This Is Important

SDAs operationalize reactive and predictive analytics to control and operate cyber-physical systems (CPS). SDAs enable adaptive and orchestrated operations. SDAs dynamically change their control and automation patterns to achieve physical process goals with global optimizations such as lower production costs, and reduced defects or operator errors. SDAs are the building block that will open up machine-to-machine ecosystems across business boundaries.

Business Impact

CPSs need global and local optimizations. SDAs deliver the capabilities to meet a wide range of scheduling outcomes by coordinating CPS outcomes across asset classes and ecosystem participants. Intelligent operational practices across business boundaries will become common as SDAs optimize and orchestrate operations (and production), across operational and contractual envelopes. Orchestrated SDAs may optimize physical flow by changing topology and/or control and automation configurations.

Drivers

- Digital twin capabilities are maturing and have expanded beyond siloed use cases and are becoming truly composite, able to support a wide range of use cases across operations, asset management and performance optimizations.

- R&D developments are positioning distributed digital twins as edge capabilities.
- Intelligent operational practices are evolving away from setpoint optimization of a fixed process toward a dynamic reoptimization and even reconfiguration of an asset control loop.
- Distributed digital twins hosted on the edge with compute capabilities either at gateway and/or asset level, will become a critical lever — able to optimize exposed automation and control variables through software as operational contexts shift.
- Organizations are moving toward adopting intelligent operational practices by exploring AI and machine learning, to systematically orchestrate production (or operations) resources. Examples include distributed energy resources such as electric vehicles (EVs) and rooftop solar systems, and oil well control and coordination.

Representative industry applications:

- The energy transition is pushing utilities to become orchestrators of distributed resources (which are SDAs) owned by multiple participants. Utilities are stabilizing the grid by asking SDAs to orchestrate their operational envelopes to meet multiple and/or conflicting objectives. Use cases include smart chargers, smart thermostats, and solar PV.
- Oil and gas companies need to optimize vast collector networks assembled from discrete assets in remote locations that are hard to reach. These assets can become SDAs able to parallel and serialize their topologies to protect physical flows while enduring disruption, through local coordination and reconfiguration, to return to a preferred operating state, or seamlessly coordinate to align product delivery to market opportunity.

Obstacles

- Legal concerns around decision responsibility have so far constrained AI and edge AI deployment, leaving a person in the loop.
- The standards that will bring together the capabilities of industrial control systems, Industrial Internet of Things (IIoT) and digital twins to enable autonomous intelligent operations by the SDA are still in development.

- Examples of constraints that need to be resolved before operationalizing SDAs and their AI include authorizations, control, bounding, defining, testing, deploying, retiring, retesting and retraining.
- SDAs may not be delivered on a unified platform. In fact, we can expect that the design, deployment and even operation of SDAs will be composable, particularly for industry-specific use cases.
- Horizontal scale-out in some industry applications come with cyber-physical system security concerns.
- SDAs could be perceived as replacing field technicians, requiring human change management to resolve job displacement fears.

User Recommendations

- Invest in advanced analytics and digital twin competencies to help enable this transition.
- Accept that SDA capabilities will not be rolled out across all assets, but will be an essential precursor to intelligent assets. Over time SDAs will evolve into intelligent assets with no central supervision.
- Transition incrementally by investing in discrete digital twins for individual equipment classes one by one and invest in composite digital twins for individual operations one by one. Over time, this will expand your portfolio of capabilities to increasingly build out more resilient grid capabilities.
- Raise your demands of OEM suppliers by specifying digital services that encapsulate asset capabilities in a structured manner to support SDAs.
- Leverage the lessons learned in your own and other asset-intensive industries.

Gartner Recommended Reading

Research Roundup: Top 10 Trends Shaping the Utility Sector in 2023

Quick Answer: What Are Intelligent Assets and Why Are They Important?

Quick Answer: What Are the Digital Checkpoints to Achieve Intelligent Operations?

IoT-Enabled Equipment as a Service

Analysis By: Eric Goodness, Scot Kim

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

Internet of Things (IoT)-enabled equipment as a service is a commercial model where businesses acquire “servitized” operational assets as recurring operating charges. Agreements define fitness for purpose and guaranteed outcomes based on asset performance, availability and output quality. Embedded IoT, AI and connectivity provide stakeholders with asset data required to audit asset health, usage and effectiveness, and to effect remedies to avoid or address nonperformance.

Why This Is Important

Leasing contracts are well established in select industries. However, selling multiple pieces of equipment as a service, based on usage fees without terms and revenue commitments, is nascent. Redefining non-IT assets as flexible operating expenses with conditions for performance, scale and availability is a transformational promise for enterprises. This business model reduces impediments to purchasing equipment including where margins from consumables offset selling equipment at cost or near cost.

Business Impact

IoT-enabled equipment as a service transforms how manufacturers sell equipment and services, and how enterprises consume them in terms of flexibility for usage and ability to ramp up or scale down usage. A good model for IoT-enabled equipment as a service requires an end-to-end IoT distributed architecture that supports a usage-based business asset with contracted guarantees for reliable business outcomes that span asset performance and effectiveness. Such a model reduces the risk of asset investment and performance, and provides clarity to the cost of operations.

Drivers

Drivers that lead enterprises to consider IoT-enabled equipment as a service include the following:

- Increasingly, the technologies needed to implement the IoT-enabled equipment-as-a-service business model are readily available at costs that continue to decrease year over year. Key to the reduction in costs is the use of open-source technologies, and the increasing presence of off-the-shelf capabilities to integrate into various IT and OT systems reduces the costs of development and integration.
- IoT-enabled equipment as a service speaks to a strong overall business trend to shift business costs from asset ownership and capital expenditure (capex) to asset subscription and operating expenditure (opex).
- There are an increasing number of financial intermediaries willing to finance large, expensive assets in the IoT-enabled equipment-as-a-service model. This relieves OEMs of owning the very assets they manufacture. That said, the financial intermediaries could also be separate business units within the same corporate structure of the equipment manufacturer.
- Additionally, a growing class of IT and OT systems integrators have embraced IoT-enabled equipment as a service as a new revenue stream. These vendors bundle assets with life cycle services that price assets as a service; the model also eliminates the user need to staff for the maintenance and support of the asset.
- IoT and “connectedness” provide an improved approach to ongoing over-the-air (OTA) software release and change management for software updates, patches and fixes.

Obstacles

- The adoption of IoT-enabled equipment as a service requires due diligence as the service concept is not well known by many sourcing and vendor management professionals. Users must take a host of business considerations into account ahead of procurement, such as hours or coverage for service and support, SLAs and time to cure for business-impacting events, determinants for penalties and termination for nonperformance.
- IoT-enabled equipment as a service requires input from IT and OT executives and operations management. Operations managers must support the performance management approaches and practices of the provider offering revenue-generating assets as a service. The IT organization is key to ensuring the support systems that enable the “servitization” of assets conform with the architecture, systems and security of the buying organization.

User Recommendations

- Perform your own multiyear total-cost-of-ownership analysis to validate the benefits of an IoT-enabled equipment-as-a-service offering.
- Work to determine if the manufacturer engages with financial intermediaries to operationalize the as-a-service offerings. Determine if P&C coverage is available to mitigate the risks of engaging in such a model.
- Negotiate agreements that clearly establish mutually agreed SLAs and operating-level agreements (OLAs) for IoT-enabled equipment-as-a-service performance and reliability.
- Factor in all nonrecurring and recurring charges, terms of agreement and penalties into your IoT-enabled equipment-as-a-service business model.
- Secure the rights to IoT-enabled equipment-as-a-service data, including mutual agreements on exactly which data and the methods are required for accessing it.
- Determine which other entities will have access to your data and how your data is monetized by the supporting ecosystem.

Sample Vendors

Atlas Copco; Caterpillar; Cy.Pag.; Danfoss; Michelin; Philips; Toshiba; Xylem

Gartner Recommended Reading

3 Successful Best Practices in Servitizing Products for Manufacturers

Evolving Network-as-a-Service Pricing Strategy Is Necessary to Accelerate Business Transitions

Now Is the Time to Deliver IoT-Enabled Product Servitization to Manufacturers

At the Peak

Cyber-Physical Systems

Analysis By: Katell Thielemann

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Cyber-physical systems (CPS) are engineered systems that orchestrate sensing, computation, control, networking and analytics to interact with the physical world (including humans). They control production and mission-critical assets, and underpin all critical infrastructure-related industries.

Why This Is Important

Whether deployed in smart grids, smart buildings or autonomous vehicles, CPS are core to manufacturing, industrial control systems (ICS)/supervisory control and data acquisition (SCADA), operational technology (OT), Internet of Things (IoT), and industrial IoT deployments. They represent the confluence of physical and digital systems to connect people, products, data and processes. Deployments can use sensors, robotics, cloud services, analytics, machine learning and high-speed networks, to orchestrate data and physical processes in real time.

Business Impact

CPS orchestrate data flows and physical processes between previously disconnected systems, automate unstructured processes, shorten cycle times, and improve product and service quality. In industrial environments, CPS replace stand-alone production process control and automation, materials handling systems, and transactional workflow systems to process real-time information. They improve productivity, reduce costs, and enable value creation for all asset-intensive industries.

Drivers

- Customer or citizen demand for faster, cheaper, better and more products/services.
- New digital business models.
- Productivity and maintenance improvements.

- Labor cost reduction made possible by automation provided by robotic CPS.
- CPS-enabled operational excellence and enhanced operational data gathering.
- Improved situational awareness in operations or mission-critical environments.
- The need to keep up with the competitive landscape by automating as many processes as possible.

Obstacles

- Concerns over physical perimeter breaches, jamming, hacking, spoofing, tampering, or command intrusion must be addressed above and beyond cybersecurity considerations.
- Deployment-related obstacles include scale (potentially billions of devices are in scope), complex architectural requirements and design approaches from many disciplines involved, sense and control loops that must be designed to evolve with business needs, the need for significant computational resources, and a variety of sensory input/output devices.
- Many organizations increasingly have a mix of legacy and new systems with proprietary protocols, which creates interoperability challenges. While end users have been seeking better interoperability, common standards are still under development in many industries.
- Many devices lack storage and compute power to facilitate security mechanisms.
- Because CPS are usually highly automated, new skills are needed for operations, security and maintenance.

User Recommendations

- Determine the business value of CPS deployment by weighing benefits against cost, complexity and security.
- Promote the use of standards and interoperability recommendations to manage complexity, enable scalability and extensibility, and ensure focus on security and safety imperatives.
- Make sure that any deployment is negotiated with CPS OEMs to ensure upgrades can be easily incorporated. Emerging technologies, such as cloud computing and 5G, will greatly impact these systems.

Sample Vendors

Honeywell International; Johnson Controls; Medtronic; Siemens; Yokogawa

Gartner Recommended Reading

Predicts 2023: Cyber-Physical Systems Security — Beyond Asset Discovery

CPS Security Governance — Best Practices From the Front Lines

Innovation Insight for Cyber-Physical Systems Protection Platforms

Smart and Sustainable Building

Analysis By: Gavin Tay, Tori Paulman

Benefit Rating: Transformational

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

A smart and sustainable building is a facility where multiple functions cooperate to achieve work-life ambiance and broader sustainability outcomes. Such outcomes encompass automation, efficiency, experience, wellness, safety, sustainability and security through the analysis of contextual and real-time information, shared among Internet of Things (IoT), information and communication technology (ICT), and operational technology (OT) systems.

Why This Is Important

Smart and sustainable buildings advance with a heavy reliance on smart technologies although a common data environment is at the core. Building management system (BMS) adoption rates are fairly slow due to its legacy nature. Hardware for HVAC and lighting implemented with new construction has a lifetime of 10 to 20 years. System failure retrofits have heightened with stringent standards of safe management accelerating the importance of experience, well-being, safety and sustainability.

Business Impact

- Increasing people centricity and a growing focus on sustainability will demand not only decarbonization, but also a shift from energy efficiency to incorporating renewable energy.
- Building performance can be optimized and predictive and preventive maintenance can be improved by responding to real-time human preferences based on activities, emotions and reactions.
- Formulating holistic solutions will stretch alignment of cross-functional teams to address work-life ambience and sustainability.

Drivers

- Today, the operating elements of a smart building typically include space, environment and maintenance management, along with wellness, safety, energy management, sustainability and workplace experience. Such rapid evolution of smart buildings means that facilities and real estate professionals will want to leverage the CIO portfolio.
- Energy efficiency such as use of solar panels has long been a key area of investment for smart building technologies. However, incorporating or reselling surplus renewable energy is emerging at an exponential rate.
- As the pent-up delay of new building construction gets underway, demand for a reinvigorated experience particularly in commercial buildings and coworking spaces will rally a surge for an orchestrated AI-augmented infrastructure alongside expertise to bring it to reality.
- The demands and expectations of workers from workplaces are shifting from merely good air, temperature and hygiene to work-life ambience. As a result, a smart building experience requires the exploitation of an ever-growing number of IoT business solutions that are intelligently cohesive.
- IoT and AI have the potential to speed up the implementation of more IT into a common data environment by extending and augmenting existing equipment. Cost savings can be achieved by integrating the sensors with BMS software in older buildings. Sometimes, it is more economical to upgrade rather than adapt to an older system.
- Various nations and organizations have a strong commitment to sustainability, driving the focus of management from pure energy to broader environmental parameters such as water, air quality and waste.

Obstacles

- CIOs assembling smart and sustainable buildings lack a clear vision of the architectural building blocks comprising a common data environment and an understanding of the privacy and data security implications increasingly.
- Delivering total experience is diverse and complex, when managing a multivendor IoT landscape and technology architecture with limited exposure to governing moving parts and the flow of activities in buildings.

- Gartner estimates that by 2028, there will be over four billion intelligently connected IoT devices in commercial smart buildings, making it hard for CIOs to provision, manage, connect and analyze their data.
- Coordinating varied expectations, use cases and budgets from different stakeholders such as facilities management, HR, and CISO (security, privacy and data sovereignty) adds to existing complexity.

User Recommendations

- Broaden corporate priorities in construction and building management by focusing on decarbonization and other sustainability initiatives.
- Address energy inefficiencies by using real-time data from the IoT and IT infrastructure to enable communication between the different BMSs or energy management systems (EMSs) in a building. According to ENERGY STAR, average buildings waste 30% of their energy in lighting, heating and cooling areas that are not occupied.
- Leverage the advantages of IoT to build holistic, engaging experiences while increasing building efficiency and competitiveness. Alleviate the potential business and technical challenges of creating a piecemeal smart building.
- Opt for flexible payment methods, and don't treat such investments as a capital liability. Channel the savings obtained from building efficiencies to the repayment of these solutions or services, making it an operating expense instead (e.g., energy management contracts).

Sample Vendors

Eutech Engineering; General Electric (GE); Honeywell Forge; Intel; Johnson Controls; Schneider Electric; Siemens; Signify; Spacewell; Terminus

Gartner Recommended Reading

Tech CEO Insight: Align the Smart Building Value Communication With the Shift Toward Well-Being and Sustainability

Creating Sustainable and Innovative Smart Buildings Through Data

How Technology and Data Can Be Used to Develop Smart Building Solutions

Emerging Technologies: The Future of Sensing

Smart Robots

Analysis By: Annette Jump

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

A smart robot is an AI-powered, often-mobile machine designed to autonomously execute one or more physical tasks. These tasks may rely on, or generate, machine learning, which can be incorporated into future activities or support unprecedented conditions. Smart robots can be split into different types based on the tasks/use cases, such as personal, logistics and industrial.

Why This Is Important

Smart robotics is an AI use case, while robotics in general does not imply AI. Smart (physical) robots had less adoption compared with industrial counterparts but received great hype in the marketplace; therefore, smart robots are still climbing the Peak of Inflated Expectations. There has been an increased interest in smart robots in the last 12 months, as companies are looking to further improve logistic operations, support automation and augment humans in various jobs.

Business Impact

Smart robots will make their initial business impact across a wide spectrum of asset-, product- and service-centric industries. Their ability to reduce physical risk to humans, as well as do work with greater reliability, lower costs and higher productivity, is common across these industries. Smart robots are already being deployed among humans to work in logistics, warehousing, police as well as safety applications.

Drivers

- The market is becoming more dynamic with technical developments of the last two years, enabling a host of new use cases that have changed how smart robots are perceived and how they can deliver value.
- The physical building blocks of smart robots (motors, actuators, chassis and wheels) have incrementally improved over time. However, areas such as Internet of Things (IoT) integration, edge AI and conversational capabilities have seen fundamental breakthroughs. This changes the paradigm for robot deployments.
- Vendor specialization has increased, leading to solutions that have higher business value, since an all-purpose/multipurpose device is either not possible or is less valuable.
- Growing interest in smart robots across a broad number of industries and use cases like: medical/healthcare (patient care, medical materials handling, interdepartment deliveries and sanitization); manufacturing (product assembly, stock replenishment, support of remote operations and quality control [QC] check); last-mile delivery; inspection of industrial objects or equipment; agriculture (harvesting and processing crops); and workplace and concierge robots in workplaces, hospitality, hospitals and so forth.

Obstacles

- **Companies are still struggling to identify valuable business use cases and assess ROI** for robots, especially outside of manufacturing and transportation. Therefore, the position of “smart robots” is still climbing to the Peak of Inflated Expectations.
- **Hype and expectations will continue to build around smart robots during the next few years**, as providers expand their offerings and explore new technologies, like reinforcement learning to drive a continuous loop of learning for robots and swarm management.
- **Lack of ubiquitous wireless connectivity solutions outside of smart spaces and immaturity of edge AI technologies** can inhibit the pace at which smart robots become semiautomated and mobile.
- **The need to offload computation to the cloud** will decrease from 2024, as robots will make more autonomous decisions.
- **The continuous evolution of pricing models**, like buy, monthly lease or hourly charge versus robot as a service for robotic solutions can create some uncertainty for organizations.

User Recommendations

- Evaluate smart robots as both substitutes and complements to their human workforce in manufacturing, distribution, logistics, retail, healthcare or defense.
- Begin pilots designed to assess product capability and quantify benefits, especially as ROI is possible even with small-scale deployments.
- Examine current business processes for current deployment of smart robots and also for large-scale deployment over the next three to five years.
- Consider different purchase models for smart robots.
- Dissolve the reluctance from staff by developing training resources to introduce robots alongside humans as an assistant.
- Ensure there are sufficient cloud computing resources to support high-speed and low-latency connectivity in the next two years.
- Evaluate multiple global and regional providers due to fragmentation within the robot landscape.

Sample Vendors

Ava Robotics; Geek+; GreyOrange; iRobot; Locus Robotics; Rethink Robotics; SoftBank Robotics; Symbotic; Temi; UBTECH

Gartner Recommended Reading

Emerging Technologies: Top Use Cases for Smart Robots to Lead the Way in Human Augmentation

Emerging Technologies: Top Use Cases Where Robots Interact Directly With Humans

Emerging Technologies: Venture Capital Growth Insights for Robots, 2021

Emerging Technologies: Smart Robot Adoption Generates Diverse Business Value

IT/OT/ET Alignment

Analysis By: Kristian Steenstrup, Marc Halpern

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Emerging

Definition:

IT/OT/ET alignment is the coordination of information technology (IT), operational technology (OT), and engineering technology (ET) through shared standards and governance. Each plays a complementary role to the other two technologies. While IT records transactions and business processes, OT operates and monitors industrial assets, and ET is used to define, design, simulate, analyze, visualize and validate those assets (e.g., GIS, computer-aided design and manufacturing [CAD]/CAM]).

Why This Is Important

For asset-intensive industries, system interoperability is improved when OT, ET and IT systems and processes share infrastructure and planning. This also enhances the agility to change configurations to adapt to market demands, improve product quality and optimize productivity. As a result, organizations seek common architecture plans and standards for the technology acquired, and increasingly look for vendors that support this direction. Most companies are at least beginning this exercise.

Business Impact

The impact of IT/OT/ET alignment is mainly focused on four aspects:

- More efficient use of technology and support resources across IT, OT and ET investments.
- Easier sharing of data from design documents (ET) to operational systems (OT) and business administration, supporting digital threads and digital twins.
- Easier sharing of performance data from OT into the ET process for design and improvement.
- Consistent security and risk management across all technology.

Drivers

- Cost reduction by not duplicating licensing, maintenance and support for common software components.
- Cost optimization by consolidating via cloud, virtualization or colocating servers and back-end hardware in a common data center.
- Agility by being able to start new hybrid IT/OT/ET projects quicker and reacting to changes in a consistent way.
- Risk avoidance by aligning security, patching, disaster recovery and upgrading processes.
- Benefits of using the same support and configuration tools, support contracts, and purchase processes.
- Process and information sharing between domains driving collaboration and cross-pollination of practices and approaches, leading to effective management of digital threads.
- Easier access to ET and OT data for IT analysis such as digital twins, predictive maintenance and production optimization.
- Leveraging OT performance data in product development using ET systems.
- Designing of systems via ET that better cater to OT effectiveness, and future OT system support and data acquisition.

Obstacles

- Coordination between three domains is complex technically and politically. Different cultures and approaches of IT departments, manufacturing/operations and design/engineering need to be reconciled.
- There may be a possible temporary increase in cost on the OT or ET side initially, as technology investments are made to bring software up to the required IT standard/version and to deal with any license compliance gaps.
- The lack of common tools for software asset management (SAM) that caters for IT and OT technology makes centralized control difficult.
- The absence of short-term benefits in terms of cost avoidance make project approval more challenging.
- The entrenched separate positions and practices associated with OT and ET systems, and their criticality, safety and stability, means that realignment takes time.
- Aligning risk appetite and security requirements across three domains with different pedigrees increases the effort needed to identify and manage risk and security.

User Recommendations

- Get agreement on a change imperative, so you have a mandate for change.
- Establish a common governance model across the three domains.
- Evaluate technology management processes to determine how much IT process is applicable to OT and ET, how the unique needs of OT and ET must be recognized and supported, and how to get them aligned and secured by design.
- Incorporate OT and ET requirements in enterprise risk management by adopting an integrated security strategy across IT, OT, ET, physical security and cyber-physical systems (CPS) for greater visibility.
- Create combined hardware platform and architecture policies to ensure compatibility between IT, OT and ET systems by formulating compatible governance for software, communications, and infrastructure.
- Use a responsible, accountable, consulted and informed (RACI) analysis to help manage this transition, and to map out organizational responsibilities for different parts of the technology environment.

Sample Vendors

Bentley Systems; Dassault Systèmes; PTC; Siemens

Gartner Recommended Reading

2022 Strategic Roadmap for IT/OT Alignment

What Should I Know About OT Security?

How IT Standards Can Be Applied to OT

Survey Analysis: IT/OT Alignment and Integration

When Does a CIO Need to Be Involved in OT?

Sliding into the Trough

IoT Services

Analysis By: Eric Goodness, Emil Berthelsen, Kristian Steenstrup

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Legacy

Definition:

Internet of Things (IoT) services provide foundational business and technical expertise to developments that require data used by IoT-enabled software or analytics systems. IoT services function within the broader digital optimization and transformation strategy, especially within asset-intensive industries. IoT services contribute to acknowledging the data value from non-IT assets and the resulting analytics for digital execution.

Why This Is Important

Organizations' lack of internal resources in IoT technologies and knowledge about operationalizing the integration of IT, operational technology (OT) and IoT drives the demand for IoT services. Also, solutions where IoT is integral to developments, such as manufacturing and building management optimizations, are key drivers of IoT services. The availability of a broad pool of providers that can balance technical expertise with sector-specific insights is crucial for successful IoT adoption and further digital business impact.

Business Impact

Sourcing, procurement and vendor management (SPVM) leaders should use IoT services to:

- Improve the processes related to strategy development and vendor due diligence.
- Accelerate time to solution in recognizing internal benefits to operations.
- Accelerate time to solution of market-facing solutions that impact customer experience (CX).
- Reduce the need for noncore resources and mitigate the risks of deployment, integration and support.

Drivers

- External service providers (ESPs) can provide the skills and expertise not found in most enterprises. As the most common IoT service providers for hardware and software are OEMs and independent software vendors (ISVs), the emerging market for IoT solutions has created a unique market landscape for IoT services. ISVs are responsible for integrating a great number of IoT platforms in the market.
- ESPs offer enterprises a way to derisk the deployment, integration and implementation of IoT-centric products in the enterprise. ESPs may bring in added capabilities and expertise in change management processes. Users can hold providers to various SLAs to ensure proper functionality and outcomes from the IoT solutions they use. Risk mitigation is also extended to cost control for project deployment.
- A fast-growing market of IoT service suppliers, ranging from industrial equipment, OEMs, traditional IT ISVs, and IT and OT systems integrator to niche IoT providers — hardware and software — offer a catalog of IoT services that span design, build and run services. The growing pool of providers can address technology challenges and factor in business insights relating to sector-specific and regulatory requirements of customers, thus ensuring specific business outcomes.

Obstacles

- Determining the suitability of service providers is challenging for many users. The market for providers is fragmented, and expertise is distributed unevenly — usually by technology segments, IoT devices, middleware and applications.
- The market for IoT platforms and devices is huge but fragmented, thus forcing ESPs to focus on a limited set of products. This has led users to purchase IoT development and integration services from existing IoT platform vendors.
- IoT's early maturity level is reflected in the service catalogs, delivery frameworks and architectural patterns IoT service providers bring to the market. Very few companies — if any — have pursued standardized, cross-enterprise solutions because they are usually hindered by costs, security and privacy concerns.
- The market has not seen a broad pool of third-party maintainers for IoT products. This means maintenance and support services are mostly awarded to OEM devices and middleware vendors.

User Recommendations

- Engage service providers early to accelerate successful IoT adoption. Do so by clearly defining the activities and success metrics that support the transition of IoT proofs of concept (POCs) to production systems and services. Service fees charged before the acceptance of production systems and services may be returned or credited to the user or the organization.
- Create a plan to identify where you provide services that augment internal resources with partnered services. Alternatively, source services entirely from external providers by aligning internal resources with IoT project phases and success requirements.
- Ensure access to the best resources for the service life cycle by abandoning legacy vendor management choices. Vendor size and legacy have little to do with the success of IoT solutions. The IoT market is fueled by smaller, nontraditional service providers and business models — such as build-operate-manage (BOM) and build-operate-transfer (BOT) models — and revenue sharing.

Sample Vendors

Accenture; Atos; Cognizant; Insight; KORE; LTIMindtree; NTT DATA; Orange; Vodafone; Wipro

Gartner Recommended Reading

Tech Providers 2025: MSPs Must Lead the Adoption of Emerging Tech Services for Digital Businesses

Forecast: IT Services for IoT, Worldwide, 2019-2025

3 Areas to Drive IoT Differentiation Beyond Functions and Features

Important and Compelling Innovations for Commercial IoT Use Cases

Magic Quadrant for Global Industrial IoT Platforms

OT Professional Services

Analysis By: Kristian Steenstrup

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Operational technology (OT) professional services encompass professional services delivered by consulting companies with engineering capabilities, OT systems integrators and OT system OEMs. The services focus on data collection (IT integration) and management of equipment, such as heavy machinery as well as OT cybersecurity, technology management tools and processes. Providers supporting these services typically offer industry-specific or product-specific OT system knowledge.

Why This Is Important

Asset-intensive companies may need help integrating IT and OT domains, so they should consider OT professional services. The market is split between OT OEMs offering professional services, OT-focused service providers and IoT-focused companies that are organically growing OT capability. The rise of the Internet of Things (IoT) means that IT-centric service providers may disrupt the OT professional services market. The conservative and risk-averse nature of the OT market creates slower growth.

Business Impact

Businesses are impacted in three ways:

- Accelerate transformation by utilizing OT professional services in coordination with internal IT resources.
- Organizations can be protected from dependence on just the OEM.
- OT professional services can support industries to deploy digital solutions for business initiatives that drive key outcomes — such as cybersecurity, asset optimization and operational efficiency — and provide operational cost reductions and savings.

Drivers

- While IT is increasingly responsible for OT in many companies, their lack of experience will require outside expertise.
- Business initiatives driven by the proliferation of digital business and Industrie 4.0 continue to increase enterprise spending on OT professional services.
- There is interest in integrating industrial IoT and edge gateways into OT platforms which can have a shorter time to benefit from professional services help.
- Many organizations (24% from our last survey) will look to their OT vendors to provide these services because they are most familiar with the equipment and OT systems deployed.
- OT professional services providers bring deep vertical knowledge, equipment knowledge and updated strategies to manage and leverage OT environments.
- Shortage of time and required skills in end-user organizations lead organizations to source externally.
- Increased government regulation requires organizations to deploy security capabilities for which they lack skills and/or knowledge.

Obstacles

- Overestimation of an organization's internal capabilities slows professional services adoption.
- Providers struggle with marketing their value and contribution to tip the balance.
- OT services are more industry- and equipment-specific than we see in IT services, and therefore are more specialized and fragmented.
- OEMs providing services have revenue dependence on their customer base potentially driving vendor lock-in.
- Risks exist if the OT service provider does not have sufficient experience in a client's specific technology platforms and industry.
- Diverse heterogeneous portfolio of OT systems creates complexity.
- Overall scarcity of experienced resources in the OT service providers' organization.
- In short-staffed organizations, knowledge transfer to internal staff is impossible meaning the organization will remain dependent on the service provider.

User Recommendations

Industrial companies with OT requirements are moving forward in the deployment of digital solutions, increasing the need for OT expertise. OT professional services knowledge is an inherently verticalized function.

- Seek providers that support your industry locally with domain-specific operations knowledge. These providers should have an understanding of the equipment and OT systems, data processing and analytics methods, operational data flows, the level of integration required between IT and OT, and the opportunity to leverage OT data for business gain.
- Create a capability assessment that defines your internal OT expertise, as well as evaluation criteria to identify and select the best-fit OT professional services provider.
- Partner with OT professional services providers that are aware of the more prevalent IoT-industry-focused standards, regulations and consortia not only within your industry but your geography.

Sample Vendors

Accenture; Atos; Black & Veatch; Hitachi; NTT DATA; Rockwell Automation; Schneider Electric; Wipro

Gartner Recommended Reading

Quick Answer: What Are IT/OT Alignment and IT/OT Integration?

Manufacturing Insight: How to Position Hybrid IT/OT Offerings

Alternative Organizational Models for IT/OT Alignment

Survey Analysis: IT/OT Alignment and Integration

When Does a CIO Need to Be Involved in OT?

OT-Applied TAM

Analysis By: Roger Williams

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Emerging

Definition:

Operational technology (OT) applied technology asset management (TAM) expands the scope of IT asset management concepts beyond traditional technology environments. The goal is to provide information about OT assets, which enables effective life cycle management decisions. Technology assets may include software, hardware and cloud services that generate, receive or process digital information to support business activity, regardless of environment.

Why This Is Important

Increasing IT/OT convergence, such as industrial Internet of Things (IoT), and blurred lines between IT, OT and line-of-business (LOB) systems are driving higher demand for TAM to be extended to OT systems. Within OT environments, TAM includes the management of software and hardware assets such as servers, applications supporting manufacturing systems, sensors and operating systems, and the management of OT-specific systems such as industrial control systems that include digital elements.

Business Impact

Evolving TAM to support OT environments:

- Lowers hardware and software costs by leveraging existing contracts and technology procurement expertise.
- Reduces risks from software license compliance audits which can lead to potential fines and penalties, and suboptimal hardware tracking which can lead to lost or missing devices.
- Provides data to a range of stakeholders to assist with decision making and planning, such as for vulnerability remediation and provisioning.

Drivers

- Many CIOs express interest in being able to use a single approach to manage both IT and OT systems. For instance, patching systems across IT-OT boundaries can introduce risks if vulnerabilities are not addressed in a timely manner due to different IT and OT approaches to this work.
- Strengthening skills, clarifying responsibilities and adopting consistent TAM approaches provide the context needed to improve the benefits delivered by technology assets within the OT environment, while optimizing costs and risks, such as with OT security and improved service delivery.
- Software audits can trigger TAM engagement with OT. As traditional IT software, including standard OSs such as Windows and Linux, is introduced into OT environments, software vendors are increasingly extending license compliance audits into this space and demanding consumption data about use of their software by OT systems.
- OT software vendors, such as CAD tool providers, have largely shifted to subscription models and auditing for compliance with software license terms and conditions, increasing the risk of significant unbudgeted costs. When TAM practices, such as software asset management (SAM), are initially applied, both overlicensing and underlicensing are often identified, along with significant opportunities to improve processes, leverage existing contracts and consolidate volume purchases.
- Poor hardware asset management practices lead to increased costs on account of adoption of industrial IoT systems and continued challenges with tracking IT hardware in OT environments.

Obstacles

- IT teams lack familiarity with OT systems, licensing models and vendors, as management of technology assets within the OT space often does not fall within IT's purview.
- IT and OT vendors tend to work differently with their customers. OT vendors don't always adhere to IT standards, and OT system development, delivery and support have evolved quite differently due to their different characteristics. IoT in many cases is increasing this divergence.
- Difficulties in discovering OT systems arise due to different communication protocols in use. The patching of OT systems is less timely than IT systems due to more frequent gaps in OT vendor software support and less frequent maintenance windows for continuously operating systems.
- The standardization of OT management practices is hindered by highly diverse and fragmented OT environments and constrained resources. Very long OT replacement cycles inhibit the ability to use system refreshes to address security and other nonfunctional requirements.

User Recommendations

- Extend and adapt the existing TAM best practices to OT if maturity and capability levels are high. If maturity and capability levels are low, create a shared business case and charter to address TAM concerns across both IT and OT environments.
- Baseline the OT environment to identify IT hardware and software assets, and OT-specific digital technology assets that would benefit from TAM. Include industry-specific systems that have network connections and software. Use existing tooling to create the baseline and supplement with OT-specific technologies as needed.
- Work with IT and OT procurement leaders, software asset management staff and sourcing teams to rectify any license compliance issues before attempting to focus on consolidation and cost reduction.
- Use TAM to enhance, instead of replacing, existing OT practices and emerging IoT practices. Leverage lessons from both TAM (particularly for software licensing) and OT practices for physical assets.

Sample Vendors

Auvesy; Axonius; Cyberbit; Flexera; Open iT; OpenLM; RAY ALLEN (RAI); Raynet; ServiceNow; Verve Industrial Protection

Gartner Recommended Reading

How IT Standards Can Be Applied to OT

The CIO's Role in Supporting Industrial Assets

As IT and OT Converge, IT and Engineers Should Learn From Each Other

2022 Strategic Roadmap for IT/OT Alignment

IT/OT Hybrid Servers

Analysis By: Tony Harvey

Benefit Rating: High

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

Information/operational technology (IT/OT) hybrid servers are edge devices that interface, collect and process data from OT systems that provide real-time control of physical systems and industrial processes. They are designed to operate with a higher resilience to shock, vibration, humidity and temperature than typical data center servers. Industrial communications interfaces — such as CAN bus, Modbus or Profinet protocols, as well as wireless or 5G technology — may also be included.

Why This Is Important

IT/OT hybrid servers allow the data created by OT systems to be processed in real time to optimize the process under control. Connections to IT networks allow hybrid IT/OT servers to collect and transmit data. This data can then be used for training AI/ML models to deliver further efficiencies and provide insight into manufacturing and production capacity and scheduling.

Business Impact

IT/OT hybrid servers help enterprises realize the potential of the large data pool that is generated by OT systems. The ability to use this data will generate new cost efficiencies and innovations in manufacturing and industrial control processes. Enterprises that successfully integrate IT/OT hybrid servers into their digital transformation strategy will lower their costs and deliver new services to market faster. Enterprises that do not adopt them, however, may find themselves left behind.

Drivers

- Businesses need real-time analysis and decision making based on capturing data that allows the optimization of industrial processes and assets to reduce costs and increase quality.
- By using near-real-time reporting of manufacturing, operations and production data, businesses will be able to provide more predictability in order cycles and a better usage of components.
- Equipment breakdowns can cause line stoppages, which drive manufacturing costs up. By enabling the collection and analysis of device monitoring, IT/OT servers enable predictive maintenance to prevent these issues.
- Regulatory and compliance requirements mandate that certain datasets should be processed and stored at edge locations, which requires the deployment of appropriate systems on-site. Further, latency and bandwidth limitations at these sites further stress the need for on-site systems.
- Organizations are collecting OT data to enable AI/ML training and digital-twin-model building.
- There is a need for specialized servers that can meet the environmental requirements for industrial sites.

Obstacles

- Industrial enterprises are cautious about the security risk of using IT and network connectivity systems in industrial process control, where failure could result in loss of life or significant property damage.
- IT and OT are separate groups with different cultures and different risk perceptions. The differences between these groups must be managed for any successful implementation.
- Businesses grapple with the complexity of defining what data must stay at the edge versus what data should be transmitted to and subsequently processed in the cloud.
- Budgeting for IT/OT hybrid servers can be difficult because there is an overlap between OT and IT systems.
- Management solutions designed to operate at large scale across a wide geographic range with highly variable connectivity characteristics are very immature.
- Standard IT equipment will not meet the harsh environmental requirements of industrial locations. Further, there could also be issues with electronic noise and interference.

User Recommendations

- Create an integrated IT/OT group that has full responsibility for these solutions, reducing the disconnects related to technology, management and budgeting.
- Reduce the risk of conflicts between the teams by aligning the IT & OT groups across architecture, governance, security and software management, and infrastructure, support and software acquisition.
- Develop a blended IT/OT culture that mixes the rigor and risk awareness of the OT engineering mindset with the flexibility and tolerance for change that is inherent in an IT mindset.
- Embed safety, security and risk training, foster awareness and include talent in hybrid IT/OT teams to ensure that systems are designed with safety and security in mind.
- Remove budget conflicts by defining upfront the budget sources for ongoing support, maintenance and dependencies across the entire combined IT/OT environment.

Sample Vendors

Dell Technologies; Hewlett Packard Enterprise; Lenovo; Schneider Electric

Gartner Recommended Reading

As IT and OT Converge, IT and Engineers Should Learn From Each Other

Survey Analysis: IT/OT Alignment and Integration

When Does a CIO Need to Be Involved in OT?

2022 Strategic Roadmap for IT/OT Alignment

How IT Standards Can Be Applied to OT

Digital Twin

Analysis By: Alfonso Velosa, Marc Halpern, Scot Kim

Benefit Rating: Transformational

Market Penetration: 1% to 5% of target audience

Maturity: Adolescent

Definition:

A digital twin is a software-enabled proxy that mirrors the state of a thing, such as an asset, person, organization or process to meet business outcomes. There are three types of digital twins: discrete, composite and organizational. Digital twin elements include a model, data, a one-to-one association and monitorability. Digital twins are built into a range of software: analytics, 3D models, CRM and IoT. Data on the state of the thing must be sourced via telemetry or application state changes.

Why This Is Important

Enterprises are using digital twins to create virtual representations of previously opaque or time-lagged things. Digital twins can help meet business outcomes such as process optimization, improved visibility or new business models. Specific examples include improving supply chain decisions via better supply and demand visibility, and reducing downtime by monitoring equipment state. Tech providers are increasing value by building domain-specific templates and integration to data sources.

Business Impact

Enterprises are implementing digital twins to:

- Gain visibility into things such as equipment or customer state that enable people to make better maintenance or marketing decisions.
- Assess, simulate and reduce the complexities of designing and developing innovative products and new service models.
- Improve patient outcomes, employee safety and customer transactions by using digital twins of people.
- Drive new data monetization models and contribute to product-as-a-service business approaches.

Drivers

- Enterprises are accelerating their adoption of digital twins to support a broad variety of business outcomes. These business outcomes include reducing the cost structure through improved monitoring of assets and optimizing equipment and processes by aligning asset digital twins into a range of solutions, such as predictive analytics and field service management. They also include product differentiation by engaging consumers and controlling assets, and integrating data silos into one central visualization.
- Asset-intensive sectors — for example, oil and gas, transportation, manufacturing and buildings — are leading in using digital twins to optimize business processes such as product development, supply chain and operations.
- Leading OEMs are exploring how digital twins can help add long-term annuity streams to their regular revenue.
- Leading-edge enterprises are implementing digital twins to model book-to-bill status, foreign exchange risk and supply chain processes. They do so to optimize costs and improve processes.
- Technology providers — from large cloud vendors to startups — are identifying potential ways to serve and charge customers using digital-twin-enabling product portfolios. In particular, they are developing template libraries to demonstrate domain knowledge and to shorten time to value for enterprise customers.
- Standards organizations such as IEEE, Eclipse, ITU and consortia (including the Digital Twin Consortium) contribute to establishing digital twin standards, architectures, ontologies and improving visibility.

Obstacles

- Few enterprises understand what they are trying to achieve, let alone the metrics for digital-twin-based projects. This lack of vision limits project scope and investment into new business processes that can take advantage of digital twins.
- Few enterprises have the cross-functional fusion teams — across business, finance, operations and IT — that are required to achieve business outcomes powered by digital twins.
- Digital twins present a technical challenge for most enterprises due to the blend of operational and information technologies required to develop and maintain them.
- Pricing remains an art, and most vendors focus on their technology differentiation, even though customer organizations are looking for business value outcomes when purchasing digital twin offerings.
- Standards bodies remain emergent. Most vendors use proprietary formats. There is a lack of standards for a broad range of digital twin technical areas such as data source and model integration and metadata management.

User Recommendations

- Co-create the digital twin strategy with the enterprise business unit to identify opportunities and challenges and establish clear success metrics. Further, the business must select sponsors and super users, create a budget and build a roadmap that starts small and scales up.
- Avoid digital twin projects that lack a business sponsor as this is key to success. Lack of internal sponsorship will waste IT resources.
- Identify IT organization technology, governance and skills gaps and build a plan to resolve them.
- Protect intellectual property by working with procurement to ensure that digital twin data and custom models belong to the enterprise.
- Develop an architectural, security and governance framework to manage large numbers of discrete digital twins, as well as composite and organizational digital twins.
- Select vendors not just for their technology portfolio, but more importantly, for the intellectual property (IP) they have in your vertical market. The IP should be demonstrated in libraries of prebuilt digital twin precursor models.

Sample Vendors

Akselos; Esri; GBTEC Group; Mavim; Nstream; Sight Machine; Toshiba; TwinThread; Vanti; visCo

Gartner Recommended Reading

Quick Answer: What Is a Digital Twin?

Emerging Tech: Tool — Digital Twin Business Value Calculator

Life Cycle Management of Software-Defined Vehicles: Step 3 — Vehicle Digital Twin 2.0

Quick Answer: Privacy Basics for a Digital Twin of a Customer

Emerging Tech: Tech Innovators for Digital Twins — Digital Business Units

Edge Asset Life Cycle Management

Analysis By: Thomas Bittman

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Adolescent

Definition:

Edge asset life cycle management includes onboarding, monitoring, change management and decommissioning of edge computing systems. Edge computing systems can be intelligent gateways, edge servers and workstations deployed in remote offices or sites, or Internet of Things (IoT) systems, such as embedded devices or IoT servers. They may also be part of an operational technology (OT) vendor system.

Why This Is Important

Edge asset life cycle management software provides better control and visibility to the edge infrastructure. This can include edge servers, intelligent gateways or embedded devices. Edge asset life cycle management software ensures that infrastructure life cycle management policies that are applied in the data center or the cloud can be similarly applied to edge environments.

Business Impact

As enterprises build distributed IT architectures, infrastructure and operations (I&O) leaders must ensure they can centrally manage or support the business unit in managing the health and life cycle of these systems, regardless of location. System management software is crucial and when organizations begin to scale their edge projects and deploy large numbers of endpoints, gateways and edge servers, centralized management of these distributed systems is imperative. This ensures better visibility and control of the environment.

Drivers

- Edge environments, such as remote offices, are often managed by data center system management software, which is less capable of handling the scale and distribution of edge assets.
- Gateways provided by OT vendors typically lack consistent life cycle management capabilities.
- System management for IoT-centric edge environments is still nascent. In this case, IoT asset management software is usually provided by the hardware vendors as software as a service (SaaS) offerings.
- Cloud vendors and emerging asset management vendors now offer IoT platforms that support remote management of IoT gateways and embedded devices.

Obstacles

- Edge life cycle management requires agreement between the responsible operations teams (IT and OT) on how asset health is to be managed, and the types of asset updates that will be allowed.
- Although it is relatively easy to update remote assets through wired networks, over-the-air (OTA) updates via cellular networks are often challenging and may result in inconsistent results.
- Updating is subject to device availability, which may be restricted to production shutdown periods for OT systems.
- Updating low-power-constrained devices operating on low-power wide-area networks (LPWANs) is a challenge. In some cases, the cost of OTA updates on constrained devices may be higher than the cost of replacing the asset.
- Vendor-led asset management tools become untenable as heterogeneous edge assets grow in scale and volume.

User Recommendations

- Leverage separate edge life cycle platforms when the ownership of edge assets (e.g., the operations team versus IT infrastructure and operations teams) and policies for edge life cycle management are distinctly different.
- Choose platforms that support easier packaging and delivery of software updates (such as containers) to the edge system to manage IoT assets.
- Synchronize work with planned maintenance shutdowns to manage OT-related edge devices.
- Consolidate IoT functionality — analytics, visualization, application and device life cycle management — onto a common IoT platform.
- Ensure that updates are delivered in a secure manner and the base OS/firmware of the asset has a rollback option.
- Focus on the usability aspect of these platforms, which is equally important, particularly when the enterprise begins to scale from a small number of assets to thousands.

Sample Vendors

Amazon Web Services (AWS); CloudPlugs; Infiot; ioTium; Microsoft; SECO

Gartner Recommended Reading

Magic Quadrant for Global Industrial IoT Platform

Emerging Technologies and Trends Impact Radar: Internet of Things for Industrial Manufacturing

IoT Platform

Analysis By: Alfonso Velosa, Eric Goodness, Scot Kim

Benefit Rating: High

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

An Internet of Things (IoT) platform enables the connection and capture of data from IoT-enabled assets to develop, deploy, and manage business solutions that improve operations such as monitoring remote assets or optimizing maintenance. Capabilities include device management, integrated data management, analytics, application enablement and management, and security. It may be delivered as edge or on-premises software, or cloud IoT platform as a service, or a hybrid combination.

Why This Is Important

Enterprises continue adding IoT capabilities to assets and products, to achieve benefits such as cost optimization, process optimization, improved customer experience, sustainability and new opportunities such as product as a service. The complexity, scale and business value of these IoT solution requirements call for specialized technology resources, most often implemented as an IoT platform.

Business Impact

IoT platforms are required to implement IoT-enabled solutions to make better business decisions from the data generated by connected assets. Goals include:

- Differentiated smart products

- Cost optimization strategies centered on improved maintenance
- Optimizing output by coordinating asset health with process health
- Opportunities to sell new services and data products or adopt new business models such as product servitization
- Sustainability improvements and reporting

Drivers

- Asset-intensive (oil and gas, manufacturing) and asset-light industries (healthcare, insurance) are implementing IoT-enabled projects to meet business objectives.
- IoT platforms help enterprises accelerate time to market for smart products while consolidating and structuring the data.
- Enterprises are finding IoT platforms already incorporated in their equipment by their OEMs to help them lower operating costs, reduce waste, minimize carbon footprint, avoid unplanned downtime and enhance worker safety.
- Technology providers' are increasing their focus on business outcomes, encouraging enterprise customers to implement IoT projects. Tech provider investments in improved ecosystems and channel partners make it easier for clients to achieve business value.
- In parallel, technology providers continue to improve their technology, user experience and vertical market templates, to ensure they can deliver business solutions, such as reduced waste, for their customers.

Obstacles

- IoT platforms still require extensive customization to achieve business outcomes for large-scale deployments, driving up cost and schedule.
- Many enterprises approach IoT projects as technology projects, instead of business projects that use IoT platforms to achieve business outcomes.
- Many enterprises operate in siloed fashions, adopting different IoT platforms for each use case, limiting their ability to scale and adding complexity.
- Enterprise leaders often underinvest in culture change processes or in training key employees. This leads employees to underuse or reject the data produced by the IoT platform, leading the project to underperform against its objectives.
- Gaps in enterprise IT and operational skills to address IoT technical needs and complexity often create project delays.
- Technology providers have yet to clearly demonstrate they can deploy and support their platforms at a large scale on a global basis.

User Recommendations

- Start small. Treat initial IoT platform projects as IT and business capability programs to acquire implementation lessons, identify challenges and opportunities, and verify alignment with business KPIs and needs.
- Develop a scenario analysis for the probability IT will have to assume IoT platform budget and long-term management.
- Identify the differing enterprise needs for IoT platforms and establish an IT team to establish a multiplatform architecture. These include simple projects with new assets using new protocols versus complex projects in legacy plants that connect to heterogeneous assets and protocols.
- Use a skills gap for IoT platforms to build an improvement plan for IT team capabilities such as integration or digital twin development or security.
- Evaluate vendors across criteria such as vertical market expertise, proof of value projects, the ability to drive large-scale deployments, technology portfolio and partner ecosystem.

Sample Vendors

Alleantia; Alibaba; Arduino; AVEVA Group; Covacsis Technologies; Haier Group; Intelligent Plant; NEC; Panasonic; Vodafone Group

Gartner Recommended Reading

Magic Quadrant for Global Industrial IoT Platforms

Technology Opportunity Prism: Internet of Things

Competitive Landscape: IoT Service Providers

Infographic: IoT Use-Case Prism for Sustainability and ESG

OT Security

Analysis By: Katell Thielemann

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Operational technology (OT) includes hardware and software that detect or cause a change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events. OT security focuses on protecting them. As threats and security solutions multiply, a generic category of OT security that was once dominated by network-centric tools is now evolving into multiple categories.

Why This Is Important

Once disconnected from IT networks, the increased connectivity of OT and IT systems has created new security risks. As operational systems are the centers of value creation, OT security has major relevance to organizations in national critical infrastructure, and to any other industrial verticals with operations and asset-centric environments. Network-centric security, with a focus on segmentation and firewalls, traditionally anchored OT security approaches, but new categories have emerged.

Business Impact

Whether it be nation-states targeting critical infrastructure and intellectual property (manufacturing is often targeted for cyber espionage), or financially motivated hackers deploying ransomware, the number of attacks on systems in production or mission-critical environments has increased over the past five years. The impact of operational disruption can range from mere annoyance to hundreds of millions of dollars, along with reliability, life and safety impacts.

Drivers

- Digital transformation initiatives are multiplying in asset-intensive organizations, in turn creating new risks that security teams may have no visibility into.
- Due to a rapidly changing threat landscape, asset-centric organizations are increasingly focusing their attention on the security risks they face outside of enterprise IT. They realize they are surrounded by cyber-physical systems (CPS) that underpin all their production, distribution and value creation efforts.
- International standards, such as IEC 62443, NIS2 and NIST 800 series, are emerging to provide guidance. In some industry verticals, security mandates, such as NERC CIP or TSA directives, are already in place. Given the close relationship between critical infrastructure and national security, and the growing concerns of targeted attacks, government-led efforts are on the rise, adding to the growing list of existing national legislations.
- One of the initial focus areas was network-based security, which has underpinned most OT security efforts for the last decade. But, many specific categories have emerged to deal with the fast-evolving threat landscape and introduce innovation in security operations. As a result, a singular OT security market is evolving.
- Some of the emerging new categories for CPS include protection platforms, cyber risk quantification platforms, secure remote access solutions, security services, network-centric solutions, or onboard diagnostics solutions.

Obstacles

- Organizations face cultural, governance and security controls challenges that prevent a one-size-fits-all approach to security. For instance, production assets often run 24/7 and cannot be stopped at will.
- Manufacturers often connect remotely to production assets to maintain and update them. If not done securely with consistent policies, this creates additional risks. They also often control deployment of updates on the basis of contracts and warranties, which can hamper security efforts.
- Shortages of OT security skills remain acute and growing.
- The age of systems and devices (up to 20 years) means no security updates are available anymore.
- OT security is evolving into CPS asset-centric security, enabled by platforms that support not only OT, but also IoT, industrial IoT, or smart building assets. This is changing OT security from focusing on segmentation and firewalls to placing the assets at the center of security, and layering defense-in-depth approaches around them.

User Recommendations

- Initiate risk discussions between IT security and production/engineering teams, and determine the current extent of OT security efforts.
- Deploy CPS asset discovery, inventory and network mapping security platforms.
- Determine immediate gaps, such as flat networks and missing or misconfigured firewalls.
- Accelerate security awareness and skills training for converging IT and OT infrastructures.
- Focus on organizational and cultural trust challenges between IT and OT personnel.
- Collaborate with your procurement team to demand that OEMs of OT systems ensure that systems are secure by design.
- Prepare for the new reality of CPS security as a centralizing discipline for securing the ever-growing list of IT, OT, IoT and industrial IoT systems, and for bringing together an asset-centric cybersecurity discipline.

Sample Vendors

Blue Ridge Networks; Booz Allen Hamilton; Optiv Security; Waterfall Security Solutions

Gartner Recommended Reading

3 Initial Steps to Address Unsecure Cyber-Physical Systems

Predicts 2023: Cyber-Physical Systems Security — Beyond Asset Discovery

CPS Security Governance — Best Practices From the Front Lines

Innovation Insight for Cyber-Physical Systems Protection Platforms

Climbing the Slope

3D Printing of Industrial Parts

Analysis By: Ivar Berntz, Marc Halpern

Benefit Rating: Moderate

Market Penetration: 5% to 20% of target audience

Maturity: Adolescent

Definition:

3D printing (3DP) of industrial parts refers to the use of 3DP to produce a finished item, subassembly or intermediate product. It can also be used to print tools, jigs, fixtures, dies and molds that would be used during the production of finished goods. This applies to OEMs and their suppliers, which can produce items on an assembly line or in a machining, casting or forming line using 3DP.

Why This Is Important

Manufacturers continue to use 3DP, for its perceived cost and time advantages, to produce customized complex products just in time (JIT) and simplify supply chain logistics and manufacturing operations. CIOs must become familiar with 3DP because it is an operational technology (OT) enabled by engineering technology (ET), but depends on IT to operate efficiently and effectively.

Business Impact

3DP for industrial parts is being used to eliminate bottlenecks in manufacturing and supply chain operations and enhance business resiliency. It reduces the inventory required for spare parts and tools and can quickly produce customized products with new material combinations and complex geometries. It transforms manufacturing operations and service with its ability to produce industrial parts JIT instead of purchasing them or using a service bureau.

Drivers

- 3DP advances the popular goal of lean manufacturing for industrial, asset-intensive organizations and offers shorter lead times, since inventories of spare parts can be reduced and supply chain operations streamlined.

- 3DP helps in improved cost position, higher design reuse, faster product launch and introduction and better aftermarket services for industrial manufacturers, resulting in improved competitive value.
- 3DP directly uses 3D data from geometric design models, either created from scratch or scanned from existing products. 3DP eliminates the additional work needed to translate 3D data into execution instructions for mainstream manufacturing operations.
- 3DP offers design and structural freedom, leading to the development of in-house capabilities such as prototyping and design verification. Since it is an additive procedure, expensive raw material and resources are not wasted.
- The technology advances the ability to increase the energy efficiency and durability of products, especially across the aerospace, defense and automotive industries. It can produce products with complex shapes, and high strength and weight resistance, that cannot be produced with traditional manufacturing techniques.
- Consumers increasingly demand personalized products, which can be delivered more rapidly through 3DP. These individualized products are also more scalable and less costly than other manufacturing approaches, where the major cost arises from the molding process for low-volume products.
- 3DP is part of a technology convergence trend that stimulates innovation where there are advances in material science and the ability to embed technologies (e.g., sensors, actuators, computer chips) in larger 3D-printed industrial parts through nano 3DP.

Obstacles

- 3DP's investment cost and production time continue to be a major challenge for producing industrial parts. This can be overcome by planning the technology's adoption roadmap and leveraging service bureaus to scale production.
- The multiple parties involved in the 3DP process lead to siloed adoption. This results in poor integration between 3D printers and designing software (the OT and ET components), and workflow software such as manufacturing execution systems (MES), ERP and SCM (the IT component).

- Owing to limited materials available for industrial parts production, there are concerns around the reliability and performance of these products, especially under adverse environmental conditions of high temperature, resistance and chemical exposure.
- Insufficient training, education and awareness to use 3DP technologies and materials efficiently is decreasing the technology's uptake.
- IP related to industrial products' ideas and design must be safeguarded, or it will be subject to financial losses and lost growth opportunities.

User Recommendations

- Partner with the decision-making teams in the organization (finance, engineering and operations) to validate the viability of 3DP technologies by building an investment case.
- Align the involved parties to create a connected workflow to create an IT-ET-OT alignment.
- Audit and invest in IT components needed to connect 3D printers with workflow and design applications such as CAD, PDM, ERP and MES that capture content needed for 3DP operation.
- Augment the production of tools and fixtures by encouraging the use of 3DP. This will result in a shorter lead time and pay for the initial cost and time investment.
- Work with supply chain leaders to assess the potential impact of 3DP on your extended supply chain across activities such as sourcing of parts, maintenance, overhaul and repair.
- Monitor the advances in 3DP and materials technology and discuss with decision makers to evaluate the benefits to manufacturing and supply chain operations.

Sample Vendors

3D Systems; Desktop Metal; EOS; Fictiv; GE Additive; Markforged; Materialise; Protolabs; Stratasys; Xometry

Gartner Recommended Reading

IT/OT/ET Alignment With 3D Printing Enhances Scalability

3D Printing Will Accelerate Design and Product Innovation in Existing Manufacturing Setups

The Manufacturing CIO's Role in Adopting and Scaling 3D Printing

Market Guide for 3D Printer Manufacturers

Quick Answer: Mapping Design for Additive Manufacturing Tools to 3D Printing Use Cases

Industrial IoT

Analysis By: Simon Jacobson, Scot Kim

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

The industrial Internet of Things (IIoT) is a subsegment of the greater market of IoT. In manufacturing, it is used to improve asset management decision making and operational visibility, as well as control for plant infrastructure and equipment within asset-intensive industries and environments.

Why This Is Important

IIoT is a core building block for smart manufacturing, improving its reliability and accessibility by extending, augmenting or replacing operational technology (OT). IIoT improves how data sources (historic and real-time across operations and systems) are accessed, analyzed, contextualized, and leveraged. Overlay IIoT platforms and solutions pave the way for how to leverage cloud, edge computing/devices, sensors, and AI/machine learning (ML) to optimize performance through enabled applications and a digital thread across operations.

Business Impact

IIoT provides access to a wider range and deeper set of data sources with the power of extracting insights and improving data-based decision making (and therefore operational performance), influences trade-offs across the network, and identifies future opportunities for automation and cost-efficiencies. The impact that IIoT delivers is bringing insights into industrial data that legacy OT systems have failed to provide.

Drivers

- Smart manufacturing, Industrie 4.0, proliferating industry consortia and nationally driven industrialization initiatives placing IIoT at the center of their initiatives. This highlights the importance of interoperable platforms as a nucleus to an organization's strategy, and not simply a nice-to-have technology.
- Better cost-efficiency in industrial operations by extending the functional life of capital assets.
- Improved productivity and operational excellence through improved quality and optimized asset performance.
- Improved data-driven decision making by frontline workers.
- Ambitious automation designs and the exploration of how certain processes can be managed remotely.
- Establishment of distributed manufacturing networks and servitization/"as a service" models.

Obstacles

- Organizational complexity, cultural impediments and process (re)engineering are required for success.
- IT and OT heterogeneity catalyze architectural debates and turf wars, impeding progress.
- Components for successful IIoT implementation are complex and of diverse maturity levels.
- Security concerns go beyond data confidentiality, integrity and availability to encompass the safety and reliability of physical operations.
- IIoT projects rely on interoperability which inherently introduces new integration challenges, making firms navigate a sea of standards, reference models and proprietary protocols.
- Resource requirements (skills, cost and integration) are often underestimated.
- Provider options continue to expand and create complications for manufacturing systems' strategies.
- Even with robust ROI, the funding models for scalability are elusive.
- The knowledge to build, partner or acquire IIoT expertise and technologies is lacking.
- IoT-enabling technologies without any business value or business buy-in are still preferred.

User Recommendations

- Develop a plan to map data, processes and use cases with site capabilities. Then segment use-case pursuits into those that will enhance the core of operations and those that will foster future innovation and process capabilities.
- Use a maturity-based continuum to develop the roadmap by aligning current and future use with both site and supply chain business objectives. Leverage a maturity-based continuum to holistically plan architecture, deployment models, standard work and interoperability.
- Ensure alignment between IT, OT, engineering technologies (ET), frontline workers and line-of-business stakeholders, so they can accurately budget resources, identify the role of standards and clarify expected benefits.
- Examine the trade-offs around buy/build/acquire/partner diligently based on in-house capabilities, time, budget and deployment environment.
- Determine the prerequisites prior to embarking on an IIoT journey by identifying the vision, architecture and associated data sources to ensure successful transformational implementations.

Sample Vendors

Amazon Web Services; Augury; Automation Intellect; Braincube; Litmus Automation; Microsoft; PTC; Software AG

Gartner Recommended Reading

Magic Quadrant for Global Industrial IoT Platforms

Innovation Insight for Smart Factory

Quick Answer: How to Communicate the Value of Industrial IoT Platforms to SCADA Solutions

Emerging Technologies and Trends Impact Radar: Internet of Things for Industrial Manufacturing

Machine Learning

Analysis By: Shubhangi Vashisth, Peter Krensky

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Mature mainstream

Definition:

Machine learning (ML) is an AI discipline that solves business problems by utilizing statistical models to extract knowledge and patterns from data. The three major approaches that relate to the types of observation provided are supervised learning, where observations contain input/output pairs (also known as “labeled data”); unsupervised learning (where labels are omitted); and reinforcement learning (where evaluations are given of how good or bad a situation is).

Why This Is Important

Over the last few years, ML has gained a lot of traction and is entering mainstream adoption because it helps organizations to make better decisions at scale with the data they have. ML aims to eliminate traditional trial-and-error approaches based on static analysis of data, which are often inaccurate and unreliable, by generalizing knowledge from data.

Business Impact

ML drives improvements and new solutions to business problems across a vast array of business, consumer and social scenarios, such as:

- Credit approval automation
- Price optimization
- Customer engagement
- Supply chain optimization
- Predictive maintenance
- Fraud detection

ML impacts can be explicit or implicit. Explicit impacts result from ML initiatives. Implicit impacts result from products and solutions that you use without realizing they incorporate ML.

Drivers

- Augmentation and automation (of parts) of the ML development process has improved productivity of data scientists and enabled citizen data scientists to make ML pervasive across the enterprise.
- Availability of quality, labeled data is driving ML adoption at enterprises.
- Pretrained ML models are increasingly available through cloud service APIs, often focused on specific domains or industries.
- ML education is becoming a standard at many academic institutions, fueling the supply of talent in this space.
- Active research in the area of ML in different industries and domains is driving applicability far and wide.
- Newer learning techniques — such as zero- or few-shot learning — are emerging, reducing the need to have high volumes of quality training data for ML initiatives, thus lowering the barrier to entry.
- New frontiers are being explored, including federated/collaborative, generative adversarial, transfer, adaptive and self-supervised learning — all aiming to broaden ML adoption.

Obstacles

- Conventional engineering approaches are unable to handle the growing volumes of data, advancements in compute infrastructure and associated complexities.
- ML is not the only popular AI initiative to emerge in the last few years. Organizations also rely on other AI techniques, such as rule-based engines, optimization techniques and physical models, to achieve decision augmentation or automation.
- Organizations still struggle to take their ML models into production. MLOps continues to be a hot trend and organizations look to specialized vendors and service providers for support in their journeys of better operationalizing ML models.
- Application of ML is often oversimplified as just model development. Several dependencies that are overlooked — such as data quality, security, legal compliance, ethical and fair use of data, and serving infrastructure — have to be considered in ML initiatives.

User Recommendations

- Assemble a (virtual) team that prioritizes ML use cases, and establish a governance process to progress the most valuable use cases through to production.
- Utilize packaged applications that fit your use-case requirements to derive superb cost-time-risk trade-offs and significantly lower the skills barrier.
- Explicitly manage MLOps and ModelOps for deploying, integrating, monitoring and scaling analytical, ML and AI models.
- Adjust your data management and information governance strategies to enable your ML team. Data is your unique competitive differentiator, and adequate data quality — such as the representativeness of historical data for current market conditions — is critical for the success of ML.

Sample Vendors

Amazon; ClearML; Databricks; Dataiku; Domino Data Lab; Google; H2O.ai; KNIME; Microsoft; MindsDB

Gartner Recommended Reading

Market Guide for Multipersona Data Science and Machine Learning Platforms

Market Guide for DSML Engineering Platforms

How to Improve the Performance of AI Projects

Infographic: Common Layers of Data Science and Machine Learning Activity

Use Gartner's MLOps Framework to Operationalize Machine Learning Projects

IT/OT Communications

Analysis By: Tim Zimmerman, Mike Leibovitz

Benefit Rating: Moderate

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Information or operational technology (IT/OT) communications continue to incorporate IT standards-based technology for line-of-business processes. IT/OT communications must be able to address deterministic performance, 100% availability and latency-sensitive application requirements. The move from proprietary communications protocols to IT standards — such as IEEE 802.3 and 802.11 — must be part of every OT to IT communications migration strategy.

Why This Is Important

Communications must be resilient, reliable and latency-sensitive to meet mission-critical demands in markets such as manufacturing. OT, specifically, supports activities in which downtime or failure can not only impact productivity, but also threaten worker safety and the environment. While OT infrastructure is often proprietary, industry-standard technologies continue to improve and can now be integrated into OT solutions. Historically, they would have required proprietary solutions and separate networks.

Business Impact

- IT/OT convergence enables organizations to integrate disparate networks.
- Security and connectivity requirements create more opportunities to integrate IT and OT systems.
- An IT strategy that includes OT may reduce the staff that had historically managed multiple proprietary networks, technologies and applications, reducing costs without affecting performance.
- IT/OT communications allow for OT applications to use cloud applications, architectures and skills in some instances, such as data storage for offline analysis.

Drivers

- Elimination of proprietary technology saves initial procurement and operational costs as well as service and maintenance costs.
- IoT platforms provide the middleware and integration that allows for disparate systems to be fused together.
- Different organizations and their disparate requirements (such as facility management, building automation, line of business and operational technology) are being aggregated into “edge computing” strategies. The implementation of edge computing strategies will likely provide a unifying foundation for connectivity, management and security.
- IT/OT communications will allow IT tools and personnel to address OT communications requirements such as security. Historically, these requirements have been addressed by an air-gapped network.
- IT networks have the ability to address latency with a time-sensitive networking functionality, and are isolated with virtual segmentation. This means that many operations can be upgraded.

Obstacles

- IT and OT teams often don’t speak the same language or address the same needs and constraints.
- Security risk continues to be the biggest obstacle. Devices on OT networks are often vulnerable to security issues when exposed to traditional IT environments, because they are on old OS releases or are unpatched. They may require specialized security approaches since they may not support 802.1X or other security policy requirements.
- OT networks have been designed to address specific issues that “best-effort” IT network architectures cannot address.
- OT monitoring may be remote or embedded into equipment, which can lead to issues regarding equipment access and responsibility.
- Long refresh cycles for OT equipment may prevent the evaluation of an IT-equivalent functionality.
- Organizations have a misguided belief that a shared network environment will degrade the OT performance because of uncontrolled IT bandwidth usage.

User Recommendations

- Align IT and OT organizationally and culturally to build relationships and trust. Then, establish open communication between the teams.
- Document and incorporate mandatory technical requirements into the associated business process. This will help enterprises that use proprietary OT communications solutions without a proper information management governance, such as security or communications policies.
- Review requirements and risks against the existing implementation by having IT and OT work together. Enterprises will then be able to know if switching to standards-based components is viable in terms of risk, performance, latency, migration, environment (such as temperature, humidity and vibration) and cybersecurity.
- Start with noncritical workflows and equipment. That may allow you to take advantage of networking IT solutions without compromising the business outcome while providing cost-optimization opportunities.
- Test all upgrades to ensure compliance with existing IT and OT requirements.

Sample Vendors

ABB; Cisco Systems; Emerson; Rockwell Automation; Schneider Electric; Siemens

Gartner Recommended Reading

Emerging Technology Analysis: Time-Sensitive Networking

Magic Quadrant for Industrial IoT Platforms

When Does a CIO Need to Be Involved in OT?

2022 Strategic Roadmap for IT/OT Alignment

How IT Standards Can Be Applied to OT

Industrial Operational Intelligence

Analysis By: Nicole Foust

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Industrial operational intelligence (OI) combines capabilities formerly found within other siloed operations systems. Capabilities include the ability to capture, store and visualize time series data (from historian software); model assets and processes for business user context; provide situational awareness and initiate field actions; provide operations-focused analytics; and offer support for asset management.

Why This Is Important

Industrial OI is a platform to monitor and add context to large volumes of sensor data and information from diverse OT sources into an Operational Data Lake that can host more tools and integrate IT data sources. OI manages operational performance within a broader business context than legacy siloed systems, such as SCADA or other plant and control center applications. Industrial OI combines capabilities from these more mature applications into one integrated decision support platform augmented by AI/ML.

Business Impact

Industrial OI supports operational decision making across plants and networked assets operations. A key capability is the ability to define and maintain persistent functional and operational models (or relationships) to create business context for users. Example benefits include:

- Dynamic grid stability
- More efficient and effective operations for quality and switching
- Better optimization of asset utilization and investments

Drivers

- The role of industrial OI in industries such as utilities has been elevated by edge technologies and AI, which dictates a new focus on analytics and managing big data. The development of industrial OI is occurring across multiple industrial sectors. The size of the market opportunity has attracted the interest of more-generic OI platform vendors.
- Industrial OI can suggest changes to operational performance in the context of multiple constraints and a changing business environment and can help mitigate operational risk.
- More timely management of data streams coming from historians and real-time production systems, combined with advanced and augmented analytics, will help organizations to uncover potential problems and develop better predictive capabilities.
- Industrial OI will support real-time situational awareness, predictive “what if” capabilities and event-driven collaboration.

Obstacles

- Broader adoption still faces a number of barriers, including the limitations of existing solutions; poor integration and alignment of IT and OT; and cultural resistance to work across silos in a cohesive way and technology limitations for information sharing.
- Stand-alone legacy systems have not moved as quickly regarding the requirement to create and manage multiple data models; use data mining and discovery tools; and leverage advanced analytics.

User Recommendations

- Establish a governance for deploying industrial OI to mitigate both OT and IT impacts. This should be undertaken as part of a broader initiative that converges and aligns IT and OT.
- Create more value from OT data by investing in industrial OI solutions. Sometimes, your existing vendors are building out the necessary capabilities. However, remember the limitations of legacy architectures, and don't rule out using more generic OI platforms. To justify your OI investments, focus on specific benefit opportunities and identify suitable use cases for your industry.
- Start small and expand over time to leverage both OT and IT data sources and to provide a closed loop that links operational and business performance to deliver operational improvements.
- Identify which users need what information and when to support advanced decision making.
- Ensure that your industrial OI supports information usage, value and dissemination that match the speed of operations and support just-in-time decision making.

Sample Vendors

AVEVA; Bentley Systems; Dassault Systèmes; Hitachi Energy; PTC; SAP; Schneider Electric; Splunk

Gartner Recommended Reading

Implement a Design Authority Across Utility IT and OT to Drive Alignment

2022 Strategic Roadmap for IT/OT Alignment

Survey Analysis: IT/OT Alignment and Integration

How IT Standards Can Be Applied to OT

IT/OT Integration

Analysis By: Kristian Steenstrup

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Information technology/operational technology (IT/OT) integration is the end state sought by organizations (most commonly, asset-intensive organizations), where IT and OT are treated as a seamless entity with cohesive authority and responsibility. In this state, there is an integrated process and information flow. Integration includes infrastructure, software, processes and potential resources.

Why This Is Important

The IT content of OT has grown exponentially and their integration allows for unprecedented efficiency gains. Yet, for most organizations, IT and OT are managed by separate groups with different approaches to managing technology. Integration can be initiated by IT departments. However, operational business units may also seek integration when trying to solve other challenges, such as dealing with cybersecurity, rising support costs, safety concerns, disaster recovery or software administration.

Business Impact

Opportunities and benefits from transparency, and an integrated value chain based on data, come from integrating the systems. As IT and OT platforms and technologies converge through increasing the use of IT architecture within OT, a successful digital business manages both IT and OT together. There is a shared responsibility, even though direct reporting lines may not shift. Data can be shared, and process flows become continuous and coherent, with minimal interruptions.

Drivers

- With IT/OT integration for asset-intensive digital businesses, organizations will be much more capable of managing, securing and exploiting data, information, and processes.
- IT/OT integration results in integrated systems, processes and teams of people, as technology domains with different areas of authority and responsibility come together.
- A common driver is for better reliability and maintenance strategies through more direct access to condition, and the use of on-premises data and SaaS solutions for plants and equipment.
- Integrated operational intelligence will provide better production management, quality control and responses to events in the supply chain, and more efficient production processes. The result will be a more agile and responsive organization.
- Digital twins, digital threads, product as a service and equipment as a service require remote Internet of Things (IoT) and OT data collection, and hence integration of IT and OT domains.
- The data from OT systems will be the fuel for better decision making in areas such as operations (adjusting and responding to production events), energy consumption, environmental sustainability, material consumption, and product quality, safety and reliability.
- A single data ownership and governance can be set up, resulting in clear end-to-end accountability for data owners.

Obstacles

- A lack of common governance structures due to a siloed approach to managing technology in the past has to be overcome.
- Without incentives, this will not change because historically, IT and OT had little contact and have different reporting lines.
- Completely integrated approaches to IT and OT are difficult to achieve because of the deeply rooted tradition in many businesses, where engineers and operations staff have been the “exclusive owners and operators” of OT.
- Many companies have disparate standards of technology in IT and OT, and even different standards for documenting the technologies, making initial planning difficult.
- A common data model spanning IT and OT rarely exists.
- Risk appetite across IT and OT, which is currently diverse, may have to be aligned.
- With the increased number of attacks in OT that have originated in IT, most stakeholders in OT will be cautious about “opening the door to ransomware” when integrating IT and OT.

User Recommendations

- Evaluate the IT/OT integration challenges and benefits in your specific company, and individual business units within the company.
- Achieve consensus across groups and with senior management, and create an alignment activity first to manage governance and standards. Sustainable integration needs well-planned IT/OT alignment.
- Add a more integrated approach to technology progressively. This integration should extend at least to data exchange and platform maintenance, with particular attention paid to communications, cybersecurity, and enterprise architecture. In some companies, that commonality will lead to an organization no longer delineated between IT and OT.
- Balance increased complexity and risk on the one hand, versus the potential benefits from better production management and more efficient production processes.
- Initiate IT/OT alignment discussions to arrive at common standards for platforms, security and architecture.

Sample Vendors

Accenture; Cisco; Eurotech; NTT DATA; PTC; Rockwell Automation

Gartner Recommended Reading

Quick Answer: What Are IT/OT Alignment and IT/OT Integration?

Manufacturing Insight: How to Position Hybrid IT/OT Offerings

How IT Standards Can Be Applied to OT

Survey Analysis: IT/OT Alignment and Integration

When Does a CIO Need to Be Involved in OT?

Asset Performance Management

Analysis By: Nicole Foust, Kristian Steenstrup

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

APM systems are business applications for optimizing reliability and availability of operational assets (such as plant and infrastructure) essential to the operation of an enterprise. It uses data capture, integration, visualization and analytics to improve asset maintenance activities. APM includes capabilities and functionality to support asset strategy, risk management, predictive maintenance, reliability-centered maintenance and financially optimized maintenance activities.

Why This Is Important

APM is an important technology for asset-intensive organizations to enable business outcomes with strategic asset maintenance decision support. Organizations invest in APM tools and technologies to reduce unplanned repair work, improve asset availability and safety, minimize maintenance costs and reduce the risk of failure for critical assets. Realizing the business can move beyond the key use case of equipment reliability, organizations leverage APM to improve overall business operations.

Business Impact

APM is an important investment area for asset-intensive industries and can deliver measurable benefits:

- Asset availability (reducing maintenance and inventory carrying costs)
- Improved uptime and cost savings can be substantial (benefits measured in millions of dollars per year)
- Improved scheduling of maintenance and planned outages
- Reliable data quality
- Effective alarm management
- Reduced manual data entry hours per month
- Optimized resources to monitor spatially distributed assets

Drivers

- With the increased focus on the overall availability of their assets in asset-intensive industries (not just breakdowns and repair costs), organizations need better solutions to deliver enhanced asset insights. Innovation in enabling technologies such as cloud, IoT and AI/ML are widening the scope and decreasing the deployment cost, aiding more awareness and use of APM.
- As operations take advantage of newer sensors (e.g., acoustic), drones and bots, APM has access to increased data volumes of better quality and granularity (or reduced latency) and accuracy, yielding richer use cases and more robust capabilities.
- Business processes supported by APM software are becoming an important core business capability for asset-intensive organizations. CIOs are increasingly realizing benefits that aid the market transition beyond the use of APM focused on equipment reliability to increasingly leveraging APM to also help improve overall business operations.
- Most APM projects are executed on the premise that data-driven decisions will improve equipment reliability and, therefore, reduce operational risk.
- The potential of reduced maintenance cost and downtime, coupled with higher levels of operational reliability, is attracting other industries; however, all are progressing at a varied pace.

Obstacles

- Limited availability of good-quality, consistent and the right asset data to support a more advanced maintenance capability.
- Limited adoption of asset management standardization (such as ISO 55000) as well as digital business immaturity constrains organizational ability to support advanced asset maintenance capabilities.
- Whether the vendor and product have proven capabilities for your desired asset maintenance activities and classes of assets within your industry, and if they align with your asset management strategy.
- Integration to your EAM to be able to execute APM recommendations, which may be complicated if they are from two different vendors.

User Recommendations

- Assess the maturity of your EAM system and have an integration plan with your APM before investing in APM, as CIOs should not expect to get all APM capabilities from the EAM vendors themselves.
- Identify the combination of asset maintenance capabilities to support your asset types and situations across the business. Most vendors do not offer all levels of APM maintenance capabilities across all industries and asset types. Thus, organizations may need more than one APM product, depending on the complexity of their businesses, the types of assets and their asset maintenance goals.
- Ensure IoT and operational technology (OT) systems compatibility by getting involved in the planning of IoT monitoring of plants and equipment.
- Source good data — that is, historical service and operational data — organizations looking to invest in APM should also expect to make investments in information management infrastructure to capture operational data where it doesn't exist today.

Sample Vendors

ARMS Reliability (a Baker Hughes company); AVEVA; Bentley Systems; Cognite; Detechtion Technologies; GE Digital; Hitachi Energy; IBM; SAP; SAS

Gartner Recommended Reading

2022 Strategic Roadmap for Asset Management

Market Guide for Enterprise Asset Management Software

Market Guide for Asset Performance Management Software

Use a Step Program to Orchestrate Maintenance and Reliability Technology

Building Information Modeling

Analysis By: Marc Halpern, Bettina Tratz-Ryan

Benefit Rating: High

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Building information modeling (BIM) is the discipline supported by software to capture, organize and manage information needed to design, create, monitor, repair, evolve and operate facilities from earliest conception to demolition.

Why This Is Important

Increases in regulations governing design, construction, operations and maintenance of facilities compounded by the number of roles involved in these activities require better means of managing and accessing information. So, organizations in many industry sectors including construction, government, manufacturing and retail need better means of organizing and accessing content about their facilities to streamline facilities design, construction, management, operations, modernization and demolition.

Business Impact

BIM delivers the following benefits:

- Reduces lost time and unnecessary costs associated with using wrong or out-of-date content throughout the life cycles of facilities.
- Improves ability to find and access content to support any activity such as facilities design, construction, operation, upgrade, maintenance and demolition of facilities.
- Improves collaboration across many roles responsible for the life cycles of facilities.
- Enhances sustainability and circularity over the life cycles of facilities.

Drivers

- As the costs of constructing and operating facilities continue to rise, facility owners, construction firms and operators seek means to increase efficiency of life cycle activities by reducing cost and time.
- Product development team members working from remote locations, instead of at a central location, need a platform with rich collaboration capabilities that also includes requisite design and engineering functionality.
- Technology advances and growing experience with BIM encourages more companies to adopt it.
- Prevalence of SaaS for other business software encourages cloud-native BIM.
- Manufacturers, utilities and architectural engineering and construction firms seek better means of complying to a growing number of regulations (such as those here in Six construction regulatory issues looming in 2020 by Construction Management) that they believe BIM will support more efficiently.
- Stakeholders in facilities seek to reduce costly mistakes with BIM by enabling better access to more timely and accurate information.
- BIM enables improved collaboration across roles participating in life cycle activities from remote locations.

Obstacles

- Engineers and contractors are deeply invested in their current culture and processes, making it difficult to adapt to new ways of working that BIM requires.
- Reaching consensus on BIM priorities and architecture proves challenging given the number of involved roles both inside and outside an enterprise.
- There will be a need for a champion investor.
- The lack of digitized data, especially among constructors, poses challenges to BIM adoption.
- BIM champions struggle to make compelling business cases for the investment.
- Building BIM content in proprietary design software formats will decrease its utility over time, cause vendor lock-in and increase the cost to maintain BIM.
- BIM projects will fail if scope creep creates higher-than-expected costs and lower-than-expected ROI. Insufficient supplier, partner and customer participation in BIM initiatives can lead to gaps in key content.
- Inflexible or incorrect BIM model design undermines future usefulness or possibly makes it obsolete before the end of a facility's service life.

User Recommendations

- Reduce the risk of failed BIM implementations by phasing the implementations into smaller, focused projects that build upon each other.
- Structure BIM initiative using governance or maturity models. Use both the BSI Levels 0 through Level 4, and incorporate 2D BIM to 7D BIM (as explained by NBS in BIM Levels explained) categories of data as the company moves from one level of BIM maturity to the next.
- Address BIM data architecture challenges by assigning IT architects to work with key BIM stakeholders.
- Encourage BIM adoption by redefining job performance metrics that encourage potential users to adopt BIM.
- Assign a BIM lead to run a project defining corporate standards for creating and modifying BIM models, and establish a training program to educate the user community.

Sample Vendors

Asite; Autodesk; Bentley Systems; Hexagon; Nemetschek Group; RIB Software; Trimble

Gartner Recommended Reading

Innovation Insight for Building Information Modeling

Creating Sustainable and Innovative Smart Buildings Through Data

Event Stream Processing

Analysis By: W. Roy Schulte, Pieter den Hamer

Benefit Rating: Transformational

Market Penetration: 20% to 50% of target audience

Maturity: Early mainstream

Definition:

Event stream processing (ESP) is computing that is performed on streaming data (sequences of event objects) for the purpose of stream analytics or stream data integration. ESP is typically applied to data as it arrives (data “in motion”). It enables situation awareness and near-real-time responses to threats and opportunities as they emerge, or it stores data streams for use in subsequent applications.

Why This Is Important

ESP enables continuous intelligence and real-time aspects of digital business. ESP’s data-in-motion architecture is a radical alternative to the conventional data-at-rest approaches that have historically dominated computing. ESP platforms have progressed from niche innovation to proven technology, and now reach into the early majority of users. ESP will reach the Plateau of Productivity in less than two years and eventually be adopted by multiple departments within every large company.

Business Impact

ESP transformed financial markets and became essential to telecommunications networks, smart electrical grids, and some IoT, supply chain, fleet management and other transportation operations. However, most of the growth in ESP during the next 10 years will come from areas where it is already established, especially IoT and customer engagement. Stream analytics from ESP platforms provide situation awareness through dashboards and alerts, and detect anomalies and other significant patterns.

Drivers

Six factors are driving ESP growth:

- Organizations have access to ever-increasing amounts of low-cost streaming data from sensors, machines, smartphones, corporate websites, transactional applications, social computing platforms, news and weather feeds, and other data brokers. Many new AI and other analytical applications need this streaming data to satisfy business requirements for situation awareness and faster, more-accurate decisions.
- The wide use of Apache Kafka and similar streaming messaging systems is reducing the cost and complexity of ingesting, storing and using streaming data.
- Conventional data engineering pipelines take hours or days to prepare data for use in BI and analytics, causing delays that are unacceptable for some purposes. Therefore, an increasing number of data engineering pipelines are being reimplemented as real-time data flows (continuous ETL) in ESP platform products or stream data integration tools with embedded ESP. These real-time data flows filter, aggregate, enrich, and perform pattern detection and other transformations on streaming data as it arrives.
- ESP products have become widely available, in part because open-source ESP technology has made it less expensive for more vendors to offer ESP. More than 30 ESP platforms or cloud ESP services are available. All software megavendors offer at least one ESP product, and numerous small-to-midsize specialists also compete in this market. Cloud ESP platforms have lowered the cost of entry.
- Vendors are embedding ESP platforms into a wide variety of other software products, including industrial IoT platforms, stream data integration tools, unified real-time platforms (aka continuous intelligence platforms), insider threat detection tools and AI operations platforms.

- Vendors are adding highly productive development tools that enable faster ESP application development. Power users can build some kinds of ESP applications via low-code techniques and off-the-shelf templates.

Obstacles

- ESP platforms are overkill for many applications that process low volumes of streaming data (i.e., under 1,000 events per second), or that do not require fast response times (i.e., less than a minute). Conventional BI and analytics tools with data-at-rest architectures are appropriate for most stream analytics with these less-demanding requirements.
- Many architects and software engineers are still unfamiliar with the design techniques that enable ESP on data in motion. They are more familiar with processing data at rest in databases and other data stores, so they use those techniques by default unless business requirements force them to use ESP.
- Some streaming applications are better-implemented on unified real-time platforms that process both data in motion and data at rest. Some unified platforms use embedded open-source ESP platform products, while others get their ESP capabilities from custom internal code.

User Recommendations

- Use ESP platforms when conventional data-at-rest architectures cannot process high-volume streams fast enough to meet business requirements.
- Acquire ESP functionality through a SaaS offering, an IoT platform or an off-the-shelf application that has embedded ESP logic if a product that targets specific business requirements is available.
- Use vendor-supported closed-source platforms or open-core ESP products that mix open-source with closed-source extensions for applications that need enterprise-level support. Use free, community-supported, open-source ESP products if developers are familiar with open-source software, and license fees are more important than staff costs.
- Use ESP platforms or stream data integration tools to ingest, filter, enrich, transform and store event streams in a file or database for later use.
- Choose a unified real-time platform with embedded ESP capabilities over a plain ESP platform if the application uses both data at rest and data in motion.

Sample Vendors

Confluent; EsperTech; Google; Hazelcast; IBM; Microsoft; Oracle; SAS; Software AG; TIBCO Software

Gartner Recommended Reading

Market Guide for Event Stream Processing

5 Essential Practices for Real-Time Analytics

Create an Optimal IoT Architecture Using 5 Common Design Patterns

Adopt Stream Data Integration to Meet Your Real-Time Data Integration and Analytics Requirements

Entering the Plateau

Vulnerability Assessment

Analysis By: Mitchell Schneider, Jonathan Nunez

Benefit Rating: High

Market Penetration: More than 50% of target audience

Maturity: Mature mainstream

Definition:

Vulnerability assessment (VA) tools operate across on-premises, cloud and/or virtual environments to help reduce exposure. They discover, identify and report on vulnerabilities of IT, cloud, IoT and/or OT devices OSs and software. They also establish a baseline of connected assets and vulnerabilities; identify and report on security configuration of assets; and support compliance reporting and control frameworks, risk assessment and remediation prioritization, and remediation activities.

Why This Is Important

VA is a foundational component of the vulnerability management (VM) process, supporting infrastructure hardening, security posture management, proactive prevention of threats, and conformity with regulations and compliance regimes. VA is a fundamental process for the discovery and enumeration of digital assets and their associated security weaknesses, helping to reduce the risk to IT.

Business Impact

Security exposures in infrastructure, apps and other assets can be abused by attackers for malicious purposes. When used in conjunction with a well implemented VM program, VA solutions can be used to effectively reduce the risks associated with security breaches, such as malware infections and ransomware. Also, many regulatory bodies and standards require organizations to perform VM for compliance mandates.

Drivers

The VA market is mature; however, advancement and innovation continues to be applied to VA tools and services in the areas of discovery, prioritization and remediation/mitigation (such as tracking vulnerability remediation progress and workflow automation) to meet buyers' evolving requirements and needs — including newer capabilities such as external attack surface management (EASM).

Although compliance use cases are still strong drivers for leveraging VA tools, many organizations are implementing these solutions to help understand, prioritize and reduce the risk of exposure from threats (see How to Implement a Risk-Based Vulnerability Management Methodology).

Depending on their maturity level, organizations typically pick one of three delivery models for VA:

- Buying, deploying and operating the product with internal staff. VA application and network scanners are both deployed on-premises or increasingly delivered as SaaS. SaaS (cloud)-delivered VA products have components on-premises, but are managed from the cloud.
- Buying and deploying the tool, then having it operated by a third party, such as a managed security service provider (MSSP) or managed detection and response (MDR) service provider.
- Outsourcing to a third party that provides managed VM services and uses its own proprietary technology or licensed commercial tools.

Obstacles

- Although VA solutions are relatively easy to deploy, if extensive agent deployment is not required, organizations will need resources and expertise that they may not have. Therefore, outsourcing VM to a security service provider is a credible option that many pursue.
- Risk-based prioritization of vulnerabilities is still not the norm for many VM programs, as the tools are still evolving this capability.
- The VA market is fragmented and characterized by a small number of large, pure-play vendors — along with startups and other vendors from various security markets offering VA as part of their overall product portfolio.
- VA used to be simple, with a big scanner deployment covering the entire environment, but factors are different now. Organizations may have multiple tools for cloud, another for containers, traditional vulnerability scanners, a solution to assess OT assets and one for endpoint detection and response (EDR), which can sometimes provide VA capabilities for the end-user systems.

User Recommendations

- Evaluate vendors offering a combined solution if your organization is resource-constrained or wants to consolidate vendors. Most VA vendors have added prioritization and EASM capabilities to their products.
- Evaluate and distinguish between the various deployment options available in the VA market, and understand how the technology fits your requirements.
- Network scanning involves remote scans of network-connected devices, but will not work when devices are off the network; give preference to authenticated scanning.
- Agent-based scanning assists with getting vulnerability data from assets that are not connected to the enterprise LAN. Agent-based scanning is best for remote workers or a DMZ.
- API-based scanning is often delivered from the cloud, but does not preclude scanning from on-premises appliances or software.
- Evaluate VA vendors that have strong built-in integrations with patch management and IT service management tools, which are aimed at streamlining the overall VM process.

Sample Vendors

Balbix; CrowdStrike; Intruder Systems; Microsoft; Outpost24; Qualys; Rapid7; Secureworks; Tenable; WithSecure

Gartner Recommended Reading

Market Guide for Vulnerability Assessment

Decoding Vulnerability Management: A Stand-Alone Tool vs. a Technique in Endpoint Protection

The Top 5 Elements of Effective Vulnerability Management

A Guidance Framework for Developing and Implementing Vulnerability Management

Appendixes

See the previous Hype Cycle: Hype Cycle for Managing Operational Technology, 2022

Hype Cycle Phases, Benefit Ratings and Maturity Levels

Table 2: Hype Cycle Phases

(Enlarged table in Appendix)

Phase	Definition
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Source: Gartner (July 2023)

Table 3: Benefit Ratings

Benefit Rating ↓	*Definition* ↓
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2023)

Table 4: Maturity Levels

(Enlarged table in Appendix)

Maturity Levels	*Status*	*Products/Vendors*
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constraints replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2023)

Evidence

[1] **2021 Gartner IT/OT Alignment and Integration Survey:** The 2021 Gartner IT/OT Alignment and Integration Survey was conducted to understand the degree to which CIOs and IT leaders are involved in operational technology (OT) management (varying by industry and country). The survey explored the IT/OT alignment and integration plans and the resulting benefits across different industries. It also covered a few areas of OT security (such as tools used, past security incidents, investment and accountability for risks). The research was conducted online from April through May 2021 among 401 respondents from North America, Western Europe and Asia/Pacific, and across different industries, such as resources, utilities, transportation, process manufacturing and discrete manufacturing. Respondents were screened for their involvement in OT-related activities (should be at least knowledgeable about the decisions of organization's OT-related activities). The survey was developed collaboratively by a team of Gartner analysts and Gartner's Research Data, Analytics and Tools team. *Disclaimer: Results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.*

[2] **2023 Gartner CIO and Technology Executives Survey:** This survey was conducted to help CIOs and technology executives overcome digital execution gaps by empowering and enabling an ecosystem of internal and external digital technology producers. It was conducted online from 2 May 2022 through 25 June 2022 among Gartner Executive Programs members and other CIOs. Qualified respondents are each the most senior IT leader (e.g., CIO) for their overall organization or some part of their organization (for example, a business unit or region). The total sample is 2,203 respondents, with representation from all geographies and industry sectors (public and private), including 211 from asset-intensive industries. *Disclaimer: Results of this survey do not represent global findings or the market as a whole, but reflect the sentiments of the respondents and companies surveyed.*

Document Revision History

Hype Cycle for Managing Operational Technology, 2022 - 18 July 2022

Hype Cycle for Managing Operational Technology, 2021 - 29 July 2021

Hype Cycle for Managing Operational Technology, 2020 - 13 August 2020

Hype Cycle for Managing Operational Technology, 2019 - 31 July 2019

Hype Cycle for Managing Operational Technology, 2018 - 26 July 2018

Hype Cycle for Managing Operational Technology, 2017 - 25 July 2017

Hype Cycle for Managing Operational Technology, 2016 - 20 July 2016

Hype Cycle for Managing Operational Technology, 2015 - 3 August 2015

Hype Cycle for Operational Technology, 2014 - 23 July 2014

Hype Cycle for Operational Technology, 2013 - 31 July 2013

Hype Cycle for Operational Technology, 2012 - 30 July 2012

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Understanding Gartner's Hype Cycles

Tool: Create Your Own Hype Cycle With Gartner's Hype Cycle Builder

Quick Answer: What Are IT/OT Alignment and IT/OT Integration?

2022 Strategic Roadmap for IT/OT Alignment

Alternative Organizational Models for IT/OT Alignment

Manufacturing Insight: How to Position Hybrid IT/OT Offerings

How IT Standards Can Be Applied to OT

When Does a CIO Need to Be Involved in OT?

Survey Analysis: IT/OT Alignment and Integration

2022 CIO and Technology Executive Agenda: An Asset-Intensive Manufacturing Perspective

---

Table 1: Priority Matrix for Managing Operational Technology, 2023

Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓
Transformational	Event Stream Processing	Cyber-Physical Systems Digital Twin IoT-Enabled Equipment as a Service Machine Learning	Smart and Sustainable Building	
High	IoT Services OT Security	Asset Performance Management Building Information Modeling Edge Asset Life Cycle Management Industrial Operational Intelligence IoT Platform IT/OT Integration Vulnerability Assessment	Industrial IoT IT/OT/ET Alignment IT/OT Hybrid Servers Smart Robots Software-Defined Assets	OT Professional Services
Moderate		3D Printing of Industrial Parts IT/OT Communications	OT-Applied TAM	
Low				

Benefit	*Years to Mainstream Adoption*			
↓	***Less Than 2 Years*** ↓	***2 - 5 Years*** ↓	***5 - 10 Years*** ↓	***More Than 10 Years*** ↓

Source: Gartner (July 2023)

Table 2: Hype Cycle Phases

Phase	*Definition*
Innovation Trigger	A breakthrough, public demonstration, product launch or other event generates significant media and industry interest.
Peak of Inflated Expectations	During this phase of overenthusiasm and unrealistic projections, a flurry of well-publicized activity by technology leaders results in some successes, but more failures, as the innovation is pushed to its limits. The only enterprises making money are conference organizers and content publishers.
Trough of Disillusionment	Because the innovation does not live up to its overinflated expectations, it rapidly becomes unfashionable. Media interest wanes, except for a few cautionary tales.
Slope of Enlightenment	Focused experimentation and solid hard work by an increasingly diverse range of organizations lead to a true understanding of the innovation's applicability, risks and benefits. Commercial off-the-shelf methodologies and tools ease the development process.
Plateau of Productivity	The real-world benefits of the innovation are demonstrated and accepted. Tools and methodologies are increasingly stable as they enter their second and third generations. Growing numbers of organizations feel comfortable with the reduced level of risk; the rapid growth phase of adoption begins. Approximately 20% of the technology's target audience has adopted or is adopting the technology as it enters this phase.
Years to Mainstream Adoption	The time required for the innovation to reach the Plateau of Productivity.

Phase ↓	Definition ↓

Source: Gartner (July 2023)

Table 3: Benefit Ratings

Benefit Rating ↓	Definition ↓
Transformational	Enables new ways of doing business across industries that will result in major shifts in industry dynamics
High	Enables new ways of performing horizontal or vertical processes that will result in significantly increased revenue or cost savings for an enterprise
Moderate	Provides incremental improvements to established processes that will result in increased revenue or cost savings for an enterprise
Low	Slightly improves processes (for example, improved user experience) that will be difficult to translate into increased revenue or cost savings

Source: Gartner (July 2023)

Table 4: Maturity Levels

Maturity Levels ↓	*Status* ↓	*Products/Vendors* ↓
Embryonic	In labs	None
Emerging	Commercialization by vendors Pilots and deployments by industry leaders	First generation High price Much customization
Adolescent	Maturing technology capabilities and process understanding Uptake beyond early adopters	Second generation Less customization
Early mainstream	Proven technology Vendors, technology and adoption rapidly evolving	Third generation More out-of-box methodologies
Mature mainstream	Robust technology Not much evolution in vendors or technology	Several dominant vendors
Legacy	Not appropriate for new developments Cost of migration constraints replacement	Maintenance revenue focus
Obsolete	Rarely used	Used/resale market only

Source: Gartner (July 2023)