White Paper

Securing IT/OT Convergence for Industry 4.0 Success

Sponsored by: Tenable

Christopher Kissel Jonathan Lang Kevin Prouty
April 2021

IDC OPINION

Industry 4.0 technologies and use cases are presenting significant opportunity for industrial enterprises in manufacturing, oil and gas, utilities, mining, and others to digitally transform their operations and achieve competitive advantage. Remote accessibility of operational data and systems offers new business capabilities for data-driven decision making, greater operational resiliency, more predictive and prescriptive asset management strategies, flexible and remote working and customer servicing models, and much more. In pursuit of these new capabilities and working models, companies are connecting their historically air-gapped operational technology (OT) systems to enterprise and outside information technology (IT) systems to enable a host of new use cases. Yet as they create these remote connections to operational data and systems, they simultaneously open the operations environment to new risks including unauthorized data access, corporate espionage, and risks concerning the potential for harmful impact to health, safety, and critical infrastructure. Balancing the benefits of integrating IT and OT systems against the risks they expose has become tantamount to Industry 4.0 success.

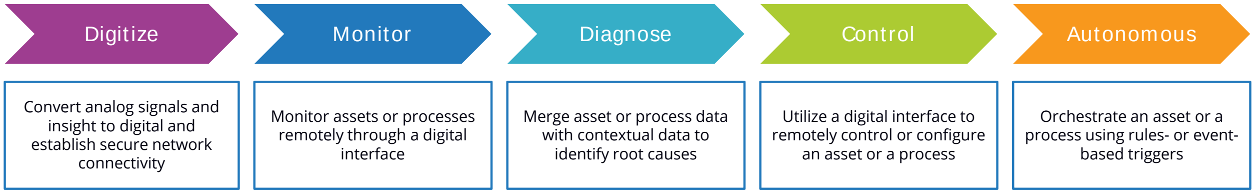
SITUATION OVERVIEW

The State of Industry 4.0

Industrial operations are inherently heterogeneous brownfield environments. Legacy OT systems have been implemented without any of the kind of architecture that is typical of IT environments. Site by site on a functionality "as-needed basis," a variety of purpose-built control systems and operational software and networking have been deployed to meet the changing needs of an operation. To advance up the Industry 4.0 continuum and pursue new use cases, companies must work within this challenging legacy environment to digitize, monitor, diagnose, control and, ultimately, develop autonomous capabilities (see Figure 1).

FIGURE 1

Industry 4.0 Continuum



Digitize: Convert analog signals and insight to digital and establish secure network connectivity

Monitor: Monitor assets or processes remotely through a digital interface

Diagnose: Merge asset or process data with contextual data to identify root causes

Control: Utilize a digital interface to remotely control or configure an asset or a process

Autonomous: Orchestrate an asset or a process using rules- or event-based triggers

Source: IDC, 2021

In the rush to capitalize on Industry 4.0 use cases, which garner a lot of business interest, the convergence of these legacy systems with enterprise IT systems is often taking place today in an ad hoc manner as part of a particular use case or technology initiative. IDC has observed companies pursuing Industry 4.0 use cases without a holistic Industry 4.0 security strategy and approach in place, introducing significant pitfalls that companies fall victim to. One such pitfall is failing to place the data and connectivity of an individual asset or process into the broader context of future work to be done. This lack of strategic approach creates challenges downstream when companies look to advance monitoring, diagnostic, and control capabilities and utilize the data for use cases:

- Blind spots in terms of visibility into a given process or asset, limiting the ability to contextualize the data for meaningful insights across all salient applications and use cases
- Introduction of additional complexity and heterogeneity by deploying technologies in silos, creating challenges in managing them at scale, and introducing greater complexity in managing and securing the overall environment
- Organizational challenges by reinforcing siloed responsibilities around physical versus digital asset management, physical security versus cybersecurity, and physical versus digital process management (e.g., data management versus process execution)
- Demonstrating regulatory compliance to auditors problematic without a systemic (and continuous) approach to monitoring all devices, applications, and OSs that are within the company's IT/OT network

According to IDC's 2020 *Worldwide IT/OT Convergence Survey* of over 1,000 industrial IT and operations professionals, security concerns about integrating IT and OT systems are top barriers at over 50% of companies surveyed. Yet companies are forging ahead with developing Industry 4.0 capabilities and treating security as an afterthought. As we look to the challenges that current approaches to Industry 4.0 are creating downstream, each of them exacerbates these security concerns, and IT/OT convergence can quickly become fraught with peril. For example, creation of blind spots in terms of asset visibility only compounds the challenge of securing that asset. Isolated technology deployments make it even more challenging to create a security program that addresses all of the paths a threat could take into operations. Organizational separation of data and network management from process execution makes it more difficult to identify meaningful anomalous changes to data and applications. All this while, the very nature of IT and OT convergence increases the overall threat surface area for an organization in some of its highest risk environments: those where human health and safety are on the line.

This is the current state of Industry 4.0 and IT/OT convergence initiatives. Many companies are deploying technologies and use cases in silos and discovering down the line that they created blind spots and further challenges in the process. It is IDC's firm and primary guidance to industrial enterprises that a holistic Industry 4.0 strategy be developed and executed, and that security be a leading feature of that strategy from the beginning of the journey. For those companies that have put the cart before the horse, it is imperative to develop and execute a holistic strategy that incorporates past and future efforts.

THE CONCERNS ABOUT A BLENDED IT/OT SECURITY PRACTICE

Until the focus on Industry 4.0 in recent years, the practice of companies hosting separate IT and OT environments was neither unusual nor necessarily unwelcomed. In the most basic generalization, IT environments are designed to monitor servers, IT infrastructure, data, and authorized/unauthorized users. In general, OT environments are designed to maintain asset uptime, operate in a safe and sustainable manner, and maximize productivity. OT assets can be varied from drill presses to chemical titration machines to the electrical grid. Operational performance is the priority and, until recently, there has been an inherent value in restricting remote access to machines through the internet. The differences between IT and OT environments are notable. Table 1 explains what the challenges for creating a unified defense may be.

TABLE 1

Comparing IT and OT Environments

Dynamic	IT Environments	OT Environments
Networking and architecture	In the great majority of IT environments, the network is designed to allow secure but agile access to and from the internet. IT environments have to account for security of straight-to-user applications.	OT environments are often air gapped. And often an OT team may live with some vulnerabilities if the cost of implementing a patch takes a machine out of production.
Types of devices	The types of IT devices secured in a network are changing. However, traditionally machines use either Windows, iOS, or Linux OS. In Windows, devices could be monitored through the Windows Machine Instrumentation (WMI) protocols.	OT environments are very specialized as many of the machines will have proprietary devices and protocols. As opposed to a persistent IT environment, a PLC (for example) may make a one-time handshake to associate itself to a network and then wait 20 days to reassociate to the central network.
Telemetry and detection	Telemetry and detection in an IT environment include packets/signatures for detection and policy violation.	OT environments include flow data (if available)/ user behavioral analytics and policy violation.
Remediation	Older devices can be lost and become "exploitable." However, IT environments are designed for patching (which present their own challenges) and software upgrades for new versions of OS, IT tools, and security appliances upgrades.	As opposed to an IT environment, often OT devices are designed to work either standalone or in isolated multiunit cells. Many machines are using instruction sets based on proprietary execution code like ladder logic or deprecated systems like 12-year-old Java or Windows OS 7. Patching has to be incorporated in workflow because production downtime is difficult to coordinate.

Source: IDC, 2021

An important shift is also seen in what is happening in both the tactics and the motivation of the adversary. Let's discuss three cybersecurity breaches of note:

- **Stuxnet.** This breach occurred 11 years ago. Many consider this to be a watershed moment in that it was the first high-profile incident where an air-gapped environment was breached. Specifically, this malware was designed to change the oscillation rate of centrifuges, ruining the enrichment of uranium. The malware effectively ruined the enrichment process but was also designed to register as a non-incident on the dashboards of the technicians monitoring the process. Naturally, the centrifuges were air gapped, and it is believed that part of the malware was installed by USB drives.
- **Oldsmar water treatment plant.** In February 2021, a remote access breach attempted to add lye to the water flowing to the city's water distribution system. Lye is typically used in small quantities to adjust water pH and in corrosion chemistry. The previous year, a remote management and access app was installed on the distribution system's Windows 7–based SCADA system so that engineers could check system status when offsite. The lack of a firewall and poor IT security policies made the system vulnerable. But a plant operator noticed the lye's set point change through the SCADA system display panel and immediately corrected it. While the security policy failed, the process for maintaining the safe operation of the plant did not.
- **German steel mill.** A phishing email attack on an IT system led to the exposure of a German steel mill's control system for a blast furnace through its connection to the local corporate LAN. The resulting incident locked out the control system from shutting down the blast furnace in a controlled manner. This led to the furnace and surrounding equipment being severely damaged. The unusual nature of this attack was that the attackers not only had knowledge of IT vulnerabilities but also detailed knowledge of the control systems and a detailed understanding of the precise operating processes for this furnace.

Citing these specific breaches leads to a larger purpose. IT security is hard enough to implement against known malware, but it is not built to gain the visibility, security, and control of OT/IoT or converged environment threats. The Stuxnet threat was deployed, but for nearly three years, the dashboards that Iranian technicians looked at showed no anomalies. Open source machines and software often fill in gaps in networks, and third-party applications are simply a reality in enterprise networks. Certainly, the ingenuity of attackers is noted, but the means to create nefarious activities come through explainable and simple vulnerabilities, but we realize our naivete always in hindsight.

Last, it is not so much that an IT/OT convergence is a matter of preference; rather it is becoming an ongoing reality. The COVID-19 pandemic accelerated the digital transformation that was already in motion. Security teams that gathered on premises were scattered to branch or home offices. The explosion in IoT devices is not being met proportionally with the hiring of new IT/OT/IoT personnel. And while newer concerns about OT security are problematic, companies are finding integration through public cloud adds savings in storage, advantages in cloud compute, and an easier path to push one-to-many software upgrades to local machines.

INCORPORATING SECURITY INTO A HOLISTIC INDUSTRY 4.0 STRATEGY

Although many past Industry 4.0 pilots and initiatives have taken a piecemeal approach to various technology and use case implementations, many organizations have realized that to reach scale, they must develop a strategic architecture and management team to orchestrate these initiatives from key areas. IDC has observed that digitally mature enterprises have a common organizational feature. What has started out as working groups focused on a single use case — typically remote monitoring and diagnostics of assets — have formalized into teams that IDC refers to as "digital engineering" organizations. These groups are staffed by a combination of IT and operations subject matter experts. While they started out as remote asset diagnostic groups, for leading organizations, they are quickly taking on key responsibilities such as data model life-cycle management, OT strategic architecture, application development in low-code environments, advanced analytics and machine learning, and operations cybersecurity. While the creation of a *digital engineering* organization is not an imperative, particularly for smaller enterprises, it offers key insight into successful methods of developing and executing holistic Industry 4.0 strategies. It is from these groups that IDC has witnessed three best practices emerging that carry significant value in advancing Industry 4.0 capabilities while bolstering operations' cybersecurity. If executed correctly, organizations will incorporate cybersecurity as inherent to operations processes and ensure long-term viability of the cybersecurity strategy.

Practice 1 — Asset Inventory

For many operations today, there is a gap in the knowledge of what IT and OT assets exist within operations at a given time. For example, in IDC's 2020 *Worldwide IT/OT Convergence Survey,* when asked what percentage of operational equipment is instrumented with a PLC, DCS, sensor, meter, or other digital capability, responses from IT versus operations were nearly 10% separate on any given percentage range. This creates business challenges when Industry 4.0 capabilities advance to more comprehensive and cross-operations analytics use cases by limiting the ability of predictive asset management models to accurately understand and measure a process or the relationship between a series of assets. This lack of awareness can render predictive asset management models ineffective at reducing unplanned downtime or predicting other events. They can create a false sense of confidence and trust in asset model that does not see the full picture. But they also create security challenges like being unable to identify when changes are made to a PLC, unable to identify whether vulnerable OT hardware is on the network and requiring patching, unable to identify data policy violations, and others. In summary, you cannot transform or secure what you are unaware of.

That is why in the first step of the Industry 4.0 continuum, Digitize; digital leaders are first developing a comprehensive and persistent asset inventory capability. This baseline inventory of both IT and OT assets in operations provides the visibility necessary to develop advanced predictive modeling capabilities for the business while ensuring that OT asset management and cybersecurity capabilities are comprehensive. By continuously monitoring the industrial network for assets, companies can understand brands, models, and firmware versions of these assets to more easily identify known vulnerabilities as well as recognize when new assets are deployed outside of the purview of governance processes, ensuring that those new assets are properly onboarded holistically across necessary systems. This holistic onboarding process is another important best practice for the line of business as well as cybersecurity programs. With operational data as the backbone of nearly all Industry 4.0 use cases, it is critical that a newly acquired asset has data access and network policies defined, has the data tagging practices aligned to overall analytics models, ensures that there is a management strategy in place that accounts for the physical and digital condition of the asset, and has that new data source made available to the host of applications and roles requiring it to improve their overall decision-making capability.

The efficiency, security, and operational gains from an automated asset inventory capability are significant across roles. "Roles" in this case is a double entendre. In both IT and OT security, roles include individual access and the enforcement of policy. However, visibility, much less context, is a constant battle. Previously, it was noted that OT machines often handshake once and then deliberately disassociate from the network. In IT, software upgrades and patches require that a machine be online. Automated asset inventory truncates many of these disparate processes. From this shared value proposition, alignment and integration between the line of business and IT can be developed, improving overall digital maturity.

Practice 2 — Operational Subject Matter Context

One of the biggest challenges that IDC has observed for enterprises looking to capitalize on their operational data is the lack of context. In operations today, for process improvement there is a heavy reliance on subject matter experts in operations. It can be said that in operations, every engineer is a silo of one. A considerable opportunity for Industry 4.0 initiatives is codifying operational context into data and analytics models. Yet that context is frequently changing and is increasingly reliant on and integrated with IT systems. This lack of context can impact production quality, create unplanned downtime, and introduce regulatory and safety risks as well as security vulnerabilities. It reduces the overall impact of any given Industry 4.0 use case by reinforcing silos and creating inefficiencies and room for error. It is to the benefit of both operations and IT professionals to collaborate on capturing and codifying operational context, inclusive of IT and OT systems.

When considering the security impact, IT and OT environments are different enough that advanced threat detection is problematic without situation awareness of both environments. In IDC's December 2020 *XDR and EDR Survey,* findings show that half of all adversarial attacks used more than one malware signature. Malware is designed to be stealthy; without an established record of behavior detection common tactics, an SQL injection or buffering error could be incorrectly described as a (temporary) network performance issue. On the other end of the spectrum, IT environments are everchanging. When new configuration or software is uploaded, if not properly accounted for, alerts could be generated against old parameters. Without comprehensive understanding of either an IT or an OT environment, it is difficult to separate what is meaningful and requires action. This lack of awareness creates significant false positives in many of today's operations cybersecurity programs, which frustrates operations professionals and lacks significance to security professionals.

A second best practice shared among leading industrial enterprises is to develop comprehensive data governance and access capabilities that are managed holistically in an effort to ensure salient context is available for all of the roles and systems that require operational data. For lines of business, access to operational data provides the fuel for advanced use cases such as digital twins. For IT and security professionals, access to operational data enables them to support the technology needs of the business more effectively. As discussed in the Asset Inventory practice, complete visibility into OT data and insights reduces blind spots and ensures that known vulnerabilities and intrusion detection capabilities can be acted on effectively. But for unknown or behavior-based threats, this broader context is essential to identifying the most common and evasive security threats — insiders. In discussions with enterprises and examining past incidents, the most frequent security threats for industrial operations come from ignorance of employees making changes to systems outside of policies or from disgruntled current or ex-employees and contractors. This is because a successful cyberattack on an industrial operation requires subject matter expertise to understand the industrial network, processes, data tagging methodologies, and OT vulnerabilities to execute.

To defend against these more nuanced insider threats requires hybrid threat detection capabilities and proactive threat hunting on an ongoing basis. It also requires that these systems have subject matter expertise and context baked in — through their inherent capabilities from the vendor and through their access to operational data — to be effective. Processes change in operations frequently, sometimes on the fly, and these process changes must be documented and available for these models to adapt accordingly.

Device vulnerability assessment scanners and other security professionals submit vulnerabilities to MITRE for verification. MITRE assigns a Common Vulnerability Scoring System (CVSS) score to quantify the vulnerability (on a scale of 1-10, with 10 being the most exploitable). The CVSS system is good, but the problem is that it too lacks contextual awareness. For example, security professionals may find an exploit path, but there is no known malware that is "weaponized" against the vulnerability. Second, not all 10s are created equal. An exploit to a DNS resolver or email server is a catastrophic event; however, a vulnerability to a local print server may only have limited consequences. If a security operations center (SOC) is tracking down and mitigating incidents based on risk, it will be in a never-ending chase. However, the better and smarter strategy is to understand risk that requires the contextual awareness of the asset, the vulnerability, the likelihood of an exploit, and the chance that an exploit cannot be contained.

Practice 3 — Leverage Existing Investments and Capabilities

Industry 4.0 pilots are often pursued in isolation. IDC has frequently identified industrial companies that fail to scale these initiatives into production. This occurs for a variety of reasons — the architecture chosen for the pilot is not applicable in multiple operations, the data is nonconforming and too difficult to cleanse at scale, or a security issue they were unaware of is identified during a pilot that must be addressed before bringing a use case or technology to production. Indeed, the heterogeneous nature of OT environments today makes for considerable challenges for bringing new technologies and use cases to value at scale. It also makes security challenging — from endpoints to access, industrial networks to enterprise networks, remote connectivity, OT and IT asset management, and physical security monitoring and access; the list of considerations and capabilities required is significant.

That is why digitally mature industrial enterprises approach Industry 4.0 holistically, starting with the inventory of assets and resources outlined in Practice 1. They move up the maturity scale from the *digitize* capability to *monitor* and *diagnose* capabilities by developing the shared data and contextual models outlined in Practice 2 and to develop *control* capabilities, or the ability to direct action back into operations to realize the benefits of these use cases and initiatives. This requires an approach to Industry 4.0 that unifies the systems of engagement or action that are deployed today. It is about working within existing technologies and capabilities to orchestrate action. Under the guise of broader digital twin efforts, companies are unifying these applications to better orchestrate the actions to be taken based on new analytics capabilities. There is no initiative where this is more critical to apply than in cybersecurity.

Operations professionals must be the ones to take action and intervene in a process if there is a security threat. To do this requires security systems that inform the applications in place. Whether those systems be asset monitoring applications and platforms, IT ticketing systems, physical security systems, or others, cybersecurity practices must be integrated and inherent to business processes. In security, we see this manifesting across all of these systems of engagement including a broad portfolio of existing security applications themselves. There is also increasing interest in merging physical and cybersecurity systems and staff to gain efficiency and to better contextualize physical access and behaviors into the digital activities taking place at a given time. Leading companies are combining security alerts and recommendations into broader operational awareness and engagement activities, in addition to the specialized security dashboards and tools for their security teams.

CONSIDERING TENABLE

Tenable is a cyber exposure management company with over 30,000 customers globally. Tenable focuses on risk reduction across the enterprise.

In December 2019, Tenable acquired the OT security vendor Indegy. The strength Indegy offered was a comprehensive understanding of the many different customized PLC controllers (e.g., Honeywell, Siemens, and Schneider Electric among many) as well as offering visibility, security, and control. Indegy integrated into Tenable.sc and Tenable.io to create a unified OT framework with the intelligence needed to better reach to overall risk and threats across the environment.

In January 2020, Tenable introduced the Tenable.ot platform. For Tenable, the platform was the fruition of years of strategic development. Tenable's scan technology has been evolving for 25 years. Tenable was founded as a commercial version of the open source Nessus project. In IT environments, Tenable was one of the first companies to introduce a comprehensive methodology for providing full asset inventory down to a granular level and security, which includes the ability to perform device and network monitoring and control of changes to PLCs and other industrial assets.

Tenable.ot is a converged IT/OT platform. One way to describe Tenable.ot is through the surfaces and environments Tenable.ot has visibility and coverage over:

- **Industrial infrastructure.** Tenable.ot can create inventories of all devices and applications on the network. The detailed inventory is used as a basis to find risky behavior, vulnerabilities, and threats that can impact OT environments.
- **Site operations.** Tenable Core (the unified telemetry and analytics engine of Tenable.ot) creates user behavioral analytics and monitors TCP/IP and Fieldbus protocols for anomalies.
- **Enterprise network.** Tenable Nessus scanner offers both credentialed and uncredentialed scanning in the protection of servers, infrastructure, and PC-centric endpoints. In addition, Tenable offers extended visibility of containers and cloud.
- **Site supervisory.** Observation of various workflows includes SCADA, human-machine interfaces, and engineering workstations.
- **Direct network controls.** The Tenable.ot has visibility and preestablished filters monitoring anomalistic activity and vulnerabilities that may impact PLC and remote terminal units.
- **Physical processes.** Monitoring PLCs is well and good, but the motors, pumps, sensors, and robotics also provide data. Tenable.ot can find problems in OT that may not be related to the PLC.

Aside from visibility, a key capability of Tenable.ot is that it produces a Vulnerability Priority Risk (VPR) score for each device and over the entire surface. Different categories of threat monitoring include configuration events, SCADA events, network events, and device-based threats.

The proactive protection aspects of Tenable.ot are arguably as important as the detection aspects. The platform lets admins simulate potential attack vectors to identify weak spots. "Attack vectoring" helps analysts monitor for unusual or high-risk scenarios (i.e., open ports, risky protocols, and connected assets that should not be talking to one another) and enables remediation prior to an attack.

Last, Tenable.ot integrates across its portfolio, enabling unified management across enterprise environments. Integration and ecosystem partnerships with a variety of common enterprise security suites extend this unified management for enterprises leveraging multiple vendors' tools.

CHALLENGES/OPPORTUNITIES

As mentioned previously, industrial enterprises today are at varying stages of Industry 4.0 and cybersecurity maturity. There are a host of tools and suites deployed today across enterprise and operations environments. According to IDC data, companies are also looking to single tools or integrated toolchains to manage security capabilities. Tenable will need to be able to meet customers where they are to integrate their capabilities and drive value, even for companies that may have progressed on a different path thus far. It will also need to rely on and further develop strong partnerships with incumbent or complementary products to create a broad and lasting footprint in the technology architecture.

In addition, there is an increasing set of hardware and software tools being introduced as part of Industry 4.0 progression. Tenable's ability to successfully contextualize OT data and systems relies on the company's ability to keep up with the lengthening list of assets deployed in operations. There is also the need for users to adopt configuration capabilities and successfully communicate value propositions internally to ensure adoption and acceptance from operations roles who are notoriously skeptical of security tools and initiatives. Yet the success of a tool such as Tenable.ot relies on this collaborative and broad adoption.

Tenable is creating a comprehensive unified IT/OT platform, but there are two practical types of competition. The first set of competitors come from the PLC controllers themselves — these companies may offer security and monitoring of their own PLCs. The second set of competitors include other OT security providers such as Claroty, Forescout, and Tripwire. Tripwire is a subsidiary of Belden, and Forescout acquired SecurityMatters in November 2018 to augment its OT technologies. Tenable will need to demonstrate efficacy and differentiation as well as compete with these companies' channels to succeed in the market.

SUMMARY OF RECOMMENDATIONS

To summarize and build upon the practices outlined previously, having a holistic Industry 4.0 strategy that is inclusive of both the physical and digital assets and processes in operations is essential to success at scale.

This holistic strategy must include stakeholders and subject matter experts from across IT and OT to ensure that it captures and delivers on the objectives of all parties. For operations, plant safety and uninterrupted operations are not negotiable. This is often a barrier to security undertakings in operations. While IT is focused on developing capabilities for identifying threats, tracking unpatched vulnerabilities, and documenting violations, these objectives historically bore little weight with operations. To what extent the benefits of security programs can be framed in operational terms will ensure adoption and buy-in.

Asset inventory capabilities are often executed within cybersecurity assessments, yet as outlined previously they carry significant value potential for broader Industry 4.0 assessment. By automating the asset inventory process early and ongoing and including this capability in the overall Industry 4.0 road map, security will become embedded into subsequent Industry 4.0 steps. This is the foundation of collaboration between IT and operations that is the missing link inhibiting value and introducing unnecessary risk in many Industry 4.0 initiatives today.

It is true that data is the new oil fueling transformation in operations, yet without context this oil is unrefined and will damage the decision-making engine. Companies that want to tap the value of this data resource must develop governance and access capabilities that not only serve the line-of-business stakeholders that apply the data but also shore up the risk introduced by the creation and sharing of all of this data.

And last, the journey of Industry 4.0 is a journey of IT and OT integration — across legacy OT systems and applications in place, new IT hardware and software capabilities, and in the staff and processes that execute on the combined capabilities. Collaboration and integration of processes are the best way to ensure that Industry 4.0 initiatives are transformative, and not incremental. This calls for the advent of new organizational structures and for an architecture in operations that allows for security to become an embedded responsibility in every role and application it applies to. IDC has seen digital leaders following these practices gain and widen their competitive advantage over laggards that discover these considerations and practices too late to gain full value from them.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com