

# DELL—TAKING PART OF THE MYSTERY OUT OF THE INDUSTRIAL INTERNET OF THINGS

DELL'S PRAGMATIC, REALISTIC, AND FLEXIBLE APPROACH ENABLES INDUSTRIAL IIOT RESULTS, TODAY

## EXECUTIVE SUMMARY

Internet of Things (IoT) applications are real, today. Some organizations around the world are deploying IoT systems and reaping the benefits of smarter data gathering, analysis, and usage to optimize and adjust their operations. Most organizations, however, are not there yet. Specifically, in the Industrial Internet of Things (IIoT), corporations are just beginning to understand the power of sensor-driven data gathering and edge and cloud analytics. Many of these organizations are looking now for vendors and partners that have the experience and skills to help them implement IoT solutions.

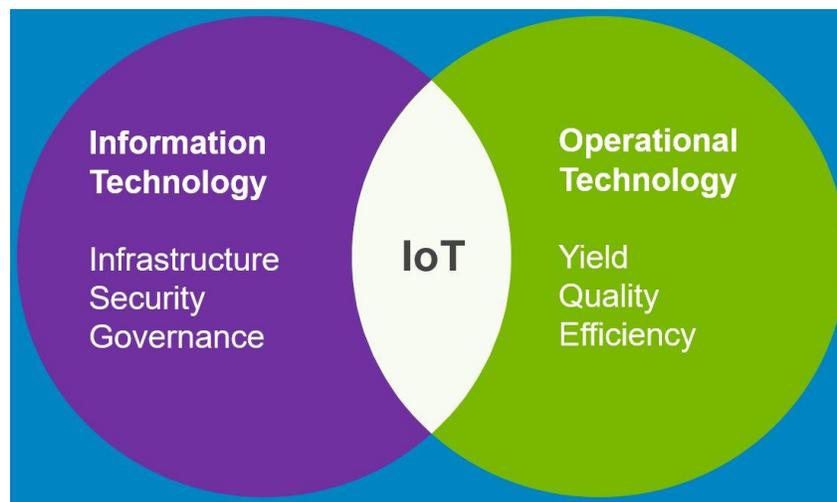
Moor Insights & Strategy (MI&S) believes the vendors that are having success and generating revenues in the IIoT are **pragmatic**, **realistic**, and **flexible** in their approaches. They understand that innovation in the IIoT does not mean developing new systems from scratch; instead, it's often about taking existing processes and capital investments and adapting them to today's new environment. It's about understanding that value is created when Operational Technology (OT) and Information Technology (IT) collaborate to develop new processes and solutions that integrate data, analytics, and control. MI&S believes Dell is one of those companies that understands this dynamic. Dell is a tier 1, global end-to-end technology provider in the commercial space, working not only directly with enterprise and manufacturing customers but also with partner experts in industrial vertical markets, making Dell an obvious choice to consider when seeking out solutions to real-world IIoT problems.

## IIOT IS NOT NEW

Though the discussion of IoT is fairly new, the concept itself is not. Industrial IoT has its roots in Machine-to-Machine (M2M) applications that have been around for more than 50 years. Today, M2M has transitioned to the IIoT, moving from "black box" closed applications to systems that are all about standards which ensure connections, sharing, and interactions. These systems—and the trillions of endpoints they will monitor and

control—are driving innovation in devices, gateways, the cloud, and all the software that collects, monitors, analyzes, and controls these fit-for-purpose applications. M2M has always been about localization using little data and little control. Today, we take that little data and little control, and we combine it into Big Data, add analytics, and bring an incredible amount of power and flexibility to solve real-world problems that could not have been imagined years ago.

**FIGURE 1: THE IT / OT COLLISION**



*Source: Dell*

For years, M2M and operations solutions have been driven by business needs to solve a limited subset of problems: run a manufacturing line, operate a robot, or monitor temperature or pressure. These Operational Technology (OT) problems and priorities are focused on improving safety, production, yield, quality, efficiency, and self-sufficiency and enabling automation. OT teams designed, installed, and maintained these functions as separate, locally controlled systems with no need, capability, or thoughts to connect them together, and certainly no need to bring the data out of the building to a corporate or centralized system. With the reduction in cost and expanded availability of sensors—combined with the advancement in computation, storage, networking, and applications—IIoT was “born”.

Suddenly the possibilities of not only **monitoring** systems, but **analyzing** the data in real-time to provide intelligence for local control and then **combining** it with other systems became possible. Complexity significantly increased; a robot may have a few things to monitor and react to, but a car can have millions of variables if you include

time and locations. Given the huge increase in complexity and connectivity issues, the collision of OT and IT was inevitable.

IT and OT have traditionally served very different purposes based on their goals and those involved in designing the solutions.

**TABLE 1: OPERATIONAL TECHNOLOGY AND INFORMATION TECHNOLOGY COMPARISON**

	<b>Operational Technology</b>	<b>Information Technology</b>
<b>Endpoints</b>	<ul style="list-style-type: none"> <li>• Generally a “thing”, be it a pump, gauge, valve, or sensor</li> <li>• Not normally held or managed closely by humans</li> <li>• Equipment age can span decades or longer</li> <li>• Control is often automated</li> </ul>	<ul style="list-style-type: none"> <li>• Typically computing devices used by humans such as laptops, tablets, &amp; cell phones</li> <li>• Normally under control by a person most of the time.</li> <li>• The age of much of the equipment is new (relative to OT) endpoints</li> <li>• Control normally is not automated &amp; is under direction of a person</li> </ul>
<b>Architectures</b>	<ul style="list-style-type: none"> <li>• Mish-mash of mostly closed systems focused on safety, resiliency, redundancy, risk mitigation, <i>etc.</i></li> <li>• Proprietary systems driven</li> <li>• Proprietary communications standards abound</li> <li>• Slow to adapt &amp; adopt newer technologies</li> </ul>	<ul style="list-style-type: none"> <li>• More standardized &amp; homogeneous than OT architectures connected using servers, routers, &amp; gateways</li> <li>• Proprietary systems exist but quicker to take advantage of standardization &amp; innovation</li> <li>• Uses communications standards when possible</li> <li>• Much quicker to adapt &amp; adopt newer technologies</li> </ul>
<b>Applications</b>	<ul style="list-style-type: none"> <li>• More “thing-centric” software providing data &amp; control for the production or movement of goods &amp; control of systems</li> <li>• Humans sometimes interact but provide supervisory roles</li> </ul>	<ul style="list-style-type: none"> <li>• More “people-centric” software providing data to individuals to make business decisions</li> <li>• Humans generally involved in the decision making</li> </ul>
<b>Owners</b>	<ul style="list-style-type: none"> <li>• Purpose-built systems designed, developed, &amp; supported by business units for narrow purposes</li> <li>• Drives the use of technology for improvements in task specific applications</li> </ul>	<ul style="list-style-type: none"> <li>• Supports corporate functions such as HR, finance, order management, sales, CRM, <i>etc.</i></li> <li>• Drives the use of technology for improvements in corporate business processes</li> </ul>

For over 50 years, IT and OT have existed in two very separate and different worlds. In the new IoT world they are not only going to have to get along but work together to solve real world problems.

## WE CAN ALL JUST GET ALONG—SERVING IT / OT NEEDS

In the new world of the Industrial Internet of Things, neither IT nor OT can follow their traditional methods and processes to serve corporate needs for the future. OT business problems are no longer isolated, and current pinpoint solutions are expensive, proprietary, inefficient, and no longer serve the needs of the business. OT problems are all about increasing efficiency, resiliency, self-sufficiency, and automation, and today's solutions need to allow for localized, datacenter, and cloud-based analytics and control. OT solutions need to reduce cost of ownership, improve their asset utilization, and mitigate risk, and IT is here to help. Making OT systems more interoperable with corporate IT systems will drive new innovations in both in corporate and in narrower business applications.

So where is the value in getting IT involved in OT problems? IT has years of experience developing processes and systems that can reduce costs, increase efficiency, and improve reliability, structure, and security. IT organizations have unlocked great value from data to improve business performance, and IoT is all about doing the same for OT processes. Combining IT and OT expertise will bring standardization, state-of-the-art technologies, processes, and innovation to outmoded industrial systems. IT's experience in lifecycle management, device management, and data management will provide much-needed value to current OT processes. MI&S believes IT's influence will:

- **Connect the cloud.** Current OT systems don't connect "up". New IIoT systems will use standards-based networking equipment (generally gateways) to connect endpoints / devices to localized resources and to the cloud. Data can be analyzed in real-time using lightweight models for localized control. It can be aggregated and analyzed at intermediate points in the network. And it can be integrated into cloud-based or enterprise systems for longer-term analytics and integration with a wide range of internal and external data sources via corporate systems, both inside and outside a company's organization.
- **Provide standards-based communications interfaces.** Current OT systems are often standalone and use outdated communications standards at best. Industry standards provide more cost-effective solutions both from an implementation and a maintenance standpoint, as well as increased security and

a long term upgrade path. In addition, current OT systems use a variety of legacy protocols (e.g., BACNet, Modbus, DNP3, CAN Bus). The ability for gateways with more computing horsepower to be able to “process” older OT protocols into new more modern and standard communications methods will drive the rapid adoption of IIoT solutions.

- **Make the data secure.** In the past, OT systems did not need to be overly concerned about security, because the data never left the building, and they were closed-loop systems rarely tied into the more susceptible IT systems. Isolated systems, however, severely limited opportunities for new efficiencies and innovations. With cloud-connected systems, security must be built in from the beginning at every point in the chain from the device, to the aggregation points, and finally to the cloud. End systems that were not designed with security from day 1 need to be re-examined and brought up to today’s security standards.

By integrating IT best practices with current OT systems, MI&S expects to see:

- Faster time-to-market for IIoT systems
- A lower total cost of ownership
- Improved asset utilization
- Enterprise level risk management
- Greater interoperability that will lead to more innovation

## IT’S ALL IN THE DATA

IoT is all about the data. True, without the “things” there would be no data, but really IoT is all about obtaining data from sources not previously available and converting that data into insights which drive actions. Unless the data is accurate, secure, and actionable, it’s not worth gathering.

## *MEASURE THE RIGHT THINGS*

As enterprises move from M2M to IoT, a change in measurement approach is required. OT systems were more about simple real-time control of critical operations, or they were based on “after-the-fact” lagging or outcome-based indicators. IoT is all about using current data for outcomes and control. In today’s environment we require measurements that can predict, determine, and influence outcomes. The most advanced systems will enable data to be not only collected but analyzed and acted upon from the edge of the network to intermediate nodes and up to cloud and enterprise

systems. For whatever systems and for whatever period being measured, systems must be able to monitor and control the endpoints.

Not only do we need to measure the right things, but we need to do it accurately. Just because we gather the data and feed it into a control loop does not guarantee the accuracy. Systems and sensors must be combined with some sort of business knowledge to ensure that we receive information that makes logical and business sense before providing actions.

IoT analytics should not be limited to control data collected by sensors and operational feeds. Organizations benefit from bringing models and contextual data into the mix as well. IoT analytics can be about small, fast predictions, and predictions based on Big Data assembled from an ensemble of systems to provide a complete picture.

### *SECURE THE DATA*

For many M2M applications, security was hardly considered because many of these systems were never connected. If the data is collected and used only “on premise” then why worry about it? Today, IIoT is all about integrating either new or existing data with something bigger than just a local system. Often the data is moved from a sensor or device (often outside the corporate firewall) to a local gateway or computation point and then aggregated into the cloud. Security is of particular concern when data is turned into valuable information through analytics, and security is paramount when paths for automated control decisions are opened back up to the network edge. To many, the control aspects are more worrisome. A hacker taking control of a gas production facility has much greater implications than credit card theft, which is in turn more serious than someone getting control of a lighting system. Whether in a retrofit scenario or built from scratch, data has to be both secured and manageable through the entire communication chain. Additional security also must not be a “burden” to the applications, as sacrificing performance, speed, usability, or general operations is not an option. Best practices can lead to a security system protected end-to-end with the appropriate amount of security to not hinder system performance and usability—and remain adjustable based on the characteristics of the data.

### *TAKE ACTION*

IoT is all about action, whether it be at the “edge” or in the datacenter or cloud. Collecting data without acting on it is inefficient and a waste of money. Current M2M systems collect data and may do a modicum of analytics and control, but M2M systems

are not good at dealing with or discovering anomalies or making predictions *i.e.*, seeing the bigger picture in advance. Moving forward, IIoT systems will enable the usage of data in real-time to improve efficiency and reduce downtime and to predict anomalies and optimize processes that can not only directly affect the bottom line but also bring new insights that can spark innovation. Local data will be used for real-time monitoring, control, and predictions. Beyond the very edge, data can be aggregated in intermediate network nodes for “regional” monitoring, control, and predictions and then in cloud-based applications to give both bigger pictures as well as integrate into larger enterprise-level systems. The resulting Big Data can then be combined with other internal and external data sources and analyzed and used for longer-term predictions, decisions, and actions. In general, analytics performed closest to the edge will be in real-time or nearly-real-time, whereas analytics in the datacenter or cloud will trend more towards offline.

## MAKING IT REAL

Industrial IoT is not about hype. The media buzz continuously focuses on consumer products...watches, wearables, light bulbs, just to name a few. MI&S believes that Industrial IoT applications are not a thing of the future. They are real today. Vertical markets such as manufacturing, building automation, transportation, logistics, agriculture, and healthcare are all using IIoT implementations to increase efficiency, reduce costs, and improve the bottom line.

To attack real world challenges, MI&S believes that hardware and software manufacturers have to get “real” with what’s out there and take a practical approach to the IIoT. Installing IIoT systems when building from scratch with all new equipment and installations is **not** the norm. Most potential IIoT installations have to work with existing equipment, software, and conditions, and vendors need to be flexible to allow current installations to maximize already invested costs.

## REAL APPLICATIONS

As examples we can look at a number of verticals and some very real applications that are running today using IIoT systems.

- **Building Automation, Energy, and Utilities:** Smart buildings provide one of the more accessible and near-term applications of IIoT. Simple installations consist of endpoints in heating, ventilation, and air conditioning systems (HVAC) with data aggregated by often more than one gateway through a legacy RS-485

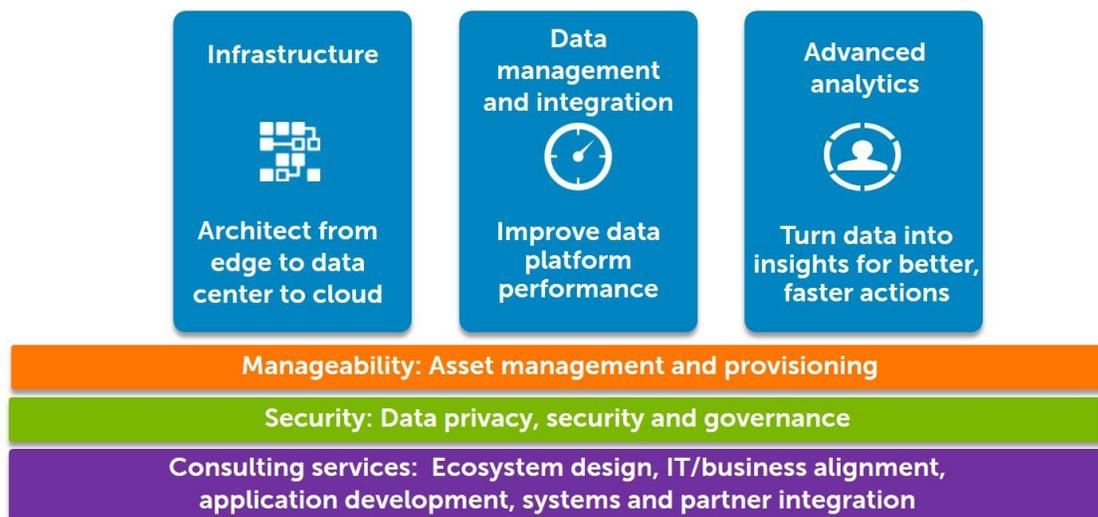
connection and then aggregated again in a cloud-based and / or datacenter platform. Analytics platforms provide simple analysis of the data and provide it to operations managers through an easily-interpreted UI to be acted on. Using this system reduces costs by tailoring energy usage in real-time, but it also reduces maintenance costs by allowing staff and systems to proactively make adjustments and repairs—and in many cases for the system to predict its own impending failure. Existing systems also go a step further, adding smart LED lighting that uses proximity to turn on and off bulbs when rooms are empty, or motion detectors that reduce heating / AC, saving significant energy usage. While small buildings or retail spaces may only have one gateway to aggregate various subsystems, larger buildings will often have many gateways (e.g., one per floor) aggregating diverse subsystems, which in turn are controlled by a master gateway that communicates with the backend.

- **Industrial Automation and Manufacturing:** There are a never-ending number of examples in manufacturing using IIoT systems. A simple example consists of a robotic manufacturing arm that attaches nuts to a bolt automatically. The arm has a laser scanner to identify the parts, picks up the proper nut, screws the nut on the bolt, checks and adjusts the torque, and then moves on. A variety of sensors are at work here, and they are communicating data back to a centralized location (confirms the correct pieces, removes the pieces from inventory, orients the pieces properly, screws the nut on with the correct torque, etc.). These procedures are continuously monitored, but they also can be adjusted to different size pieces, different torques, etc. remotely and automatically to maximize production efficiency. In addition, the analysis of the arm on a continuous basis will provide new insights such as predictive maintenance, preventing inefficiency and downtime. While certain industries may not be ready to replace their longstanding proprietary control systems with IoT technology, MI&S believes there is broad opportunity today to overlay existing mission-critical systems with IoT gateways and sensors to provide new insights for predictive equipment maintenance and quality control.
- **Transportation and Fleet Logistics:** Connecting vehicles to the internet, along with embedded sensors and telematics, enables IoT systems for transportation and fleet management as well as control and oversight on driver behavior. Logistics managers deploy IoT by chipping shipping pallets with RFID technology to control and track products before, during, and after they are loaded on / off vehicles. Harnessing the power of the internet, organizations can improve security, efficiency, customer satisfaction, regulatory compliance, and more.

- **Agriculture:** Systems monitoring production and health of both plants and animals in farm settings can contribute directly to the bottom line. Current installations integrate sensors on animals or embedded in the ground with gateways and cloud applications that continuously monitor temperature, pressure, production, geo-location, and other facets of animal and plant health. Gathering and centralizing review of this data enables production managers to make instantaneous decisions that will maintain or increase output of fields or herds.
- **Healthcare:** Healthcare is one of the largest applications for IIoT solutions and one of the biggest challenges. Even with regulatory, liability, and privacy issues a major concern, wearable and home healthcare devices are already available in many categories including measuring stations and scales, blood pressure cuffs, and even toothbrushes. The home healthcare industry itself will be revolutionized by telemedicine with remote monitoring. There are examples of real-time information from surgeries being used to predict the probability of a patient developing a surgical site infection while the operation is in process. The ability to monitor patients, as well as a wide variety of medical equipment from a distance, is already having a direct effect on the quality of life for many individuals.

## DELL—CUTTING THROUGH THE HYPE AND PROVIDING REAL SOLUTIONS TODAY

FIGURE 2: DELL IOT TECHNOLOGIES



Source: Dell

Dell delivers flexible solutions that allow potential IIoT applications to take current technology investments and combine them with new technologies and analytics to drive actions to produce real business value. Dell does this through a combination of:

- **Real World Experience:** Dell has been integrating servers, PCs, analytical software, laptops, and tablets into large systems for many years through their OEM Division. With a world renowned supply chain from Healthcare to Manufacturing to Building Automation, Dell and its ecosystem partners have been working with companies that are leading implementers of IIoT systems and applications. By taking existing customers, partners, and relationships and extending their own offerings to IIoT-specific hardware and software, Dell has a distinct advantage to providing IIoT implementations.
- **Flexible Approach:** Dell focuses on solutions that allow customers to start with existing data and devices, clarify the business outcomes and ROI that match their business needs, and implement solutions that meet these goals. The modularity and flexibility of Dell IIoT solutions allows customers to start small and then grow as they prove they can build on current technology investments. Dell as a corporation is also committed to system openness and choice. They are flexible as to what sensors are used, how devices and data are managed, where analytics are performed, and what applications customers use and deploy. Providing customers with a current growth path that maximizes current investments while still providing a path forward as they evolve is critical to working with existing installations.
- **Comprehensive Portfolio:** Dell provides IIoT software and hardware solutions from gateway to cloud to datacenter. Dell software takes a modular approach to both local and centralized analytics that allows customers to move quickly from pilot to production, adding value quickly while allowing scalability for the future. Dell's infrastructure products put the data where it needs to be and when it needs to be there. Dell's initial purpose-built IoT gateway (Dell Edge Gateway 5000 Series) ingests myriad modern and legacy data protocols; it comprehends that all data does not have to go to the cloud and that many critical and time-sensitive decisions should be made as close to the edge as possible.
- **The Right Partners** Dell and Intel's long-standing partnership has worked to bring IoT from concept to reality by collaborating with numerous partners in the M2M space who have been delivering solutions to IIoT customers for years. As M2M moves to the IIoT, the ecosystem has not only followed but expanded into IIoT-specific partners providing key analytics, IoT platforms, and real-time

technologies. As part of their go-to-market, Dell is building a broad portfolio of partners. These include independent software vendors (ISVs) for applications development ranging from large players like SAP and OSISoft, to emerging providers such as ThingWorx and Lucid Design, and systems integrators such as Zones and ELM Energy that know how to deliver domain-specific solutions in IIoT verticals. Dell and Intel recognize the importance of enabling strong OT-focused partners to complement their long-standing IT expertise.

- **Built for Security and Manageability:** Dell is focused on providing security from the sensing devices to the datacenter...and every point in between. A gateway not only transports data from sensors to the backend, it can also help encrypt data from less capable endpoints to ensure data security and privacy throughout the solution. Sensors that are smart enough to be hacked but not capable enough to protect themselves by encrypting their outbound data are of real concern. A capable gateway not only transports data from sensors to the backend, it can also help encrypt data from less capable endpoints before it passes the firewall to ensure data security and privacy throughout the solution. Today, Dell's Edge Gateway 5000 Series, powered by the Intel Atom processor, provides a number of key security features, such as TPM for hardware authentication, secure boot, and BIOS-level lockdown of specific I/O ports. Dell understands not only the tools to enable data security but also best practices for deployment, including how to design in this security from day 1. Dell's security systems are architected to understand that "all data is not equal", maximizing ROI by adjusting security to meet and not exceed the needs of the data.
- **A Philosophy of Standardization.** Interoperability has also been widely recognized as one of the key challenges to the success of IoT deployments. Dell in conjunction with Intel have placed high importance on meeting this challenge and are providing strategic and technology leadership in key IoT standards and consortia to drive interoperability in IoT globally. Both companies are active members of the Industrial Internet Consortium (IIC) and the Open Interconnect Consortium (OIC). IIC aims to establish IoT end-to-end common reference architecture and frameworks and uses them as bases for identifying interoperability requirements and gaps over a broad spectrum, such as system components, analytics, data, connectivity, *etc.* It then works with and influences global and governmental Standard Development Organizations, such as OIC, ISO/IEC, JEC1, IEEE, NIST, *etc.* to develop the necessary standards. OIC takes

a mutually reinforcing multi-track approach in tackling interoperability with a keen focus on a fundamental IoT area—communication and connectivity.

## CALL TO ACTION

Industrial IoT is not about hype. It is about implementing systems that increase efficiency, resiliency, and self-sufficiency. M2M applications have been around for more than 50 years under the control of businesses and Operational Technology staff. There are many of these systems in action today, monitoring data and providing some amount of insight for the organizations that use them.

Things have changed—sensors are cheap, and networking, storage, and computation continue to evolve and grow—and these changes are driving everything to be connected, either now or in the future. However, just because things are connected, and just because data is being gathered, does not mean the data is being used or used to its full advantage.

To really derive the benefits from the IIoT, OT systems and processes must move with the times to provide more value to their organizations. Combining the business knowledge of OT systems and staff with the experience of IT systems and staff will allow businesses to maximize the true advantages that IIoT has to offer.

Moor Insights & Strategy recommends that companies looking for IIoT solutions...

- Target **applications** that can provide a true return on new investment.
- Look for **flexible solutions** that allow you to begin small and grow as you succeed, leveraging your current technology investment wherever possible.
- Focus on **analytics** and what new insights can do for your business when enabled at the edge, intermediate levels / nodes of the network, and at the enterprise datacenter or the cloud.
- Think **security** before you start your IoT process, during the process, and after you think you are done. Security should exist from “beginning” to “end” and all points in between as you advance and grow your systems.

Dell is a vendor that MI&S believes companies should look at for developing IIoT applications from scratch **or** for upgrading current installations to add additional IIoT features and functions while leveraging their current investment in technology. Dell has a comprehensive, flexible solution that comprehends existing technologies, allows

companies to work with existing and new partners and fit-for-purpose applications, and provides security and manageability tools and expertise throughout the IIoT stack.

## IMPORTANT INFORMATION ABOUT THIS PAPER

### *AUTHOR*

Mike Krell, Analyst at [Moor Insights & Strategy](#)

### *PUBLISHER AND REVIEWER*

Patrick Moorhead, Founder, President, & Principal Analyst at [Moor Insights & Strategy](#)

### *EDITOR*

Scott McCutcheon, Director of Research at [Moor Insights & Strategy](#)

### *INQUIRIES*

[Contact us](#) if you would like to discuss this report, and Moor Insights & Strategy will promptly respond.

### *CITATIONS*

This note or paper can be cited by accredited press and analysts, but must be cited in-context, displaying author's name, author's title, and "Moor Insights & Strategy". Non-press and non-analysts must receive prior written permission by Moor Insights & Strategy for any citations.

### *LICENSING*

This document, including any supporting materials, is owned by Moor Insights & Strategy. This publication may not be reproduced, distributed, or shared in any form without Moor Insights & Strategy's prior written permission.

### *DISCLOSURES*

Moor Insights & Strategy provides research, analysis, advising, and consulting to many high-tech companies mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document. This paper was commissioned by Dell.

### *DISCLAIMER*

The information presented in this document is for informational purposes only and may contain technical inaccuracies, omissions, and typographical errors. Moor Insights & Strategy disclaims all warranties as to the accuracy, completeness, or adequacy of such information and shall have no liability for errors, omissions, or inadequacies in such information. This document consists of the opinions of Moor Insights & Strategy and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice.

Moor Insights & Strategy provides forecasts and forward-looking statements as directional indicators and not as precise predictions of future events. While our forecasts and forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forecasts and forward-looking statements, which reflect our opinions only as of the date of publication for this document. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forecasts and forward-looking statements in light of new information or future events.

© 2015 Moor Insights & Strategy.

Company and product names are used for informational purposes only and may be trademarks of their respective owners.