LITMUS

WHITE PAPER

# WHAT ENTERPRISES ARE LOOKING FOR IN IOT

PROJECTIONS FOR THE SIZE OF THE BURGEONING INTERNET OF THINGS (IOT) VARY GREATLY—BILLIONS OF CONNECTED DEVICES REPRESENTING A MULTI-TRILLION-DOLLAR MARKET—SPARKING DEBATES OVER THE ACCURACY OF THE NUMBERS AND HOW MUCH OF THE REPORTING IS MERE HYPE. AFTER ALL, THE IOT HAS BEEN THE NEXT BIG THING FOR A WHILE.

There is, however, growing consensus over which part of the IoT will have the biggest impact. Consider the candidates:

Home: This emerging sector has been garnering more media coverage during the last few years. We recognize its connected services and products with a consumer orientation, from fitness monitors to smart thermostats.

Government: Public-sector initiatives, from smart cities to digital government in the form of re-engineered service delivery have started to take shape. Given the generally cautious nature of the public sector, these initiatives are more ad hoc, though actors like the UK have started to develop comprehensive implementation strategies. Government activities will likely centre on setting policies and performing the role of public reassurance over issues such as universal access and security.

Enterprise: This will likely be the dominant IoT sector given the prevalence of existing projects and a longer engagement with IoT technology—products and services—in addressing business-related problems. Moreover, the enterprise sector has the ability to scale owing to its ability to deploy capital in different markets, particularly in industrial and manufacturing sectors such as automotive.

Questions remain over how significant enterprise IoT can be, whether it represents welcome though incremental improvements in business practices or something truly strategic. For enterprise to move beyond the connectivity of peripheral devices such as smartphones and performance-monitoring sensors to integrating truly transformative business processes requires overcoming certain obstacles:

- High costs of installation or of actually building systems and maintaining the associated infrastructure.
- Vulnerability to security breaches, and widespread concern over these.
- Inflexibility and a lack of future-proofing in systems.

Enterprise systems require architecting and implementation in ways that enable them to adapt to innovations in devices, software, or technologies. Moreover, they require the ability to assimilate data they gather and share them with applications that can generate insights. This is complicated not just by the multiplicity of devices but also different types of devices from different vendors, using disparate protocols and outputting data in different formats. These data assimilation capabilities will enable enterprises to keep adjusting their processes more intelligently and to enrich their relationships with customers.

Strategic enterprise stakeholders face a complex problem when planning IoT initiatives: How do you eschew high implementation costs while simultaneously benefiting from connectedness and minimizing the security risks brought by that desired connectedness? Business planners must address this issue in the context of gaining competitive advantage for their firms without negatively affecting financial performance. Focus usually turns to overcoming the security concerns and price barriers characteristic of implementations.

**Producing a Compelling Business Case for Large-scale Deployments**

Before enterprises can undertake large-scale deployments they need to develop a convincing business case, and the absence of a compelling business case represents another obstacle to overcome if enterprise are to achieve growth. This offers business leaders opportunities to discover and articulate those business cases, and to attempt the difficult task of quantifying the results. One source of inspiration is the concept of network effects: Greater value accrues to, and inheres in, a network the more popular and intertwined it becomes, particularly when connectedness yields greater benefits to network members by virtue of their participation. This not only accounts for the importance of growth to start-ups but also established enterprises.

The problem is that this is all new territory. A lot depends on how enterprises can manage and interpret data given that the proliferation of connectedness might strain existing human capacity to make sense of it all. The problem for the enterprise sector is the novelty of the situation. The most effective business cases will depend on the use that enterprises can make of the data that connectedness enables, especially since the proliferation of data might tax the institutional capacity to manage and interpret it all. The IoT creates an added dimension of complexity that puts a premium on the following competencies and resources:

- Monitoring and managing connected devices
- Data center storage and bandwidth to handle increased traffic resulting from increased connectedness

**Enterprise-ready?**

Whether the IoT is enterprise-ready depends on organizations developing new policies regarding traffic management to allow for information to get through instead of falling instead of being blocked by network congestion. Where organizations with networks at capacity contemplating enhancements to infrastructure, the challenge will be changing the mind-set of employees to consider security in novel ways, and to give IT personnel the tools, training, and outlook to implement and manage device automation. As connected products function like nodes for data collection in an enormous worldwide network, one cannot overlook the significance of the cloud in managing and operating connected devices.

Dealing effectively with data is crucial if enterprises expect to derive value processing and analyzing it, if they are to leverage it to improve operations, fine-tune digital marketing, or reap the benefits of connectedness across different functional areas. Yet resources and existing approaches to information management are at risk of being swamped by data. Effective enterprise management of data requires the following:

- Predictive workflows based on models and analytics.
- Analytics along two dimensions: 1) enterprise modeling of workflows, process es, and user behavior so that the enterprise can processes based on insights

into emergent patterns, and 2) visualization to enable data-driven decision.

- For consumer enterprises, the ability to comprehend the context of user environments and activities users engage in, in order to 1) build more accurate user profiles, and 2) determine the best sources of data for shedding light on contributors to consumers finding, adopting, and regularly using their products.
- An approach to instrumentation that facilitates data generation and collection.
- A data stack that allows the enterprise to scale as necessary to handle high-speed, device driven data generation, which implies 1) capabilities for assimilating external data sets that, via combination, yield actionable insights, and 2) the ability to deal with heterogeneous systems—especially mission-criti cal ones—and devices.

In confronting the difficulties of IoT connectivity, enterprises in the manufacturing sphere must contend with competing against disruptive models made possible by data-driven approaches and the likelihood of having to re-engineer business processes. Consumer-focused organizations, meanwhile face the challenge of incorporating new modes of customer engagement that provide more fine-tuned data through dramatically increased device connectedness. Yet what makes facing these challenges worthwhile is prospect of creating network effects: value creation inheres to participation in a vibrant network. The potential for achieving competitive advantage through data acquisition and interpretation explains why enterprises in the consumer products sphere (such as automakers, GE, Google, and Philips) are intent on maximizing network effects. We've all become aware of the rise of the term "ecosystem" in business and the benefits of not only belonging to the best ecosystem but also, if possible, owning it.

### Adaptive Products and Product Development

The desire to generate IoT network effects via disruptive products and services puts a premium on adaptive products and, more importantly, product development processes that can adapt.

Mainstream reporting has made us aware of instances where enterprise IoT implementations have succeeded, but the failures are more interesting and compelling. The story could be a Ukrainian power outage caused by hackers disabling the power grid or hackers gaining control over a Jeep Cherokee on the highway (both incidents occurring in 2015). It's clear that enterprise has a way to go before allying fears over whether IoT implementations are connection-ready. In many instances, the issue is not that individual devices or implementations lack security but that human behaviour and organizational dynamics enabled vulnerabilities. In the case of the power grid hack, attackers gained access via compromised login credential. In the case of the hijacked Jeep, the automobile represented the end point of a wireless communications system connected to it, which offered the same degree of access as a third-party device connected through a vehicle diagnostic port. This situation is typical in environments where organizations prioritize establishing market presence over security.

### Lessons Learned

Successes and failures in enterprise IoT implementations allow us to draw the following conclusions:

- Thinking of the IoT implementation from the end user’s standpoint enables the enterprise to design products that address the business requirement to gain insight from data sources. Enterprises can attain that by providing their users with simple ways of doing something useful they could not do with an uncon nected device.
- Enterprises can achieve more efficient implementations by designing IoT solutions that don’t increase the physical technology footprint or add inconve nient complexity via the need for more intermediary devices. Having ore inter mediary devices increases electrical power requirements and the employee learning curve.

- Effective enterprise-based IoT initiatives benefit from taking a holistic view of the employee’s situation and use context relative to long-term strategic objectives rather than concentrating on incremental process enhancements.
- Network connectivity has to present a clear advantage to the enterprise or, at the very least, not saddle it with an experience that suffers from data overload and significant lag time that prevent stakeholders from deriving fresh insights.
- Addressing security is costly, and enterprises benefit from taking a cross-disciplinary approach that aligns security priorities with market penetration ones. The former tend to lag during the "land-grab" phase of business development, but mature enterprises have shown a willingness to give them due attention.
- Enterprise implementations with significant potential for success are those that bridge divides, grappling with the problems of incompatibility between devices and protocols.
- Enterprises in industrial environments have tremendous opportunities to derive benefits—such as increased efficiency via re-engineered processes and data insights—because of the ability to scale effects in ways not possible with consumer applications.

Much like IoT technologies themselves, enterprise IoT business models are becoming mature—and need to be, otherwise enterprises risk being left behind by their more innovative competitors. Indeed, the ability for enterprises to leverage IoT shows wide variance by industry sector. For example, by being able to track user’s driving habits via on-board sensors, insurance firms are able to offer better rates to better drivers while reducing portfolio risk. Utilities, meanwhile, can pursue cost reduction strategies through connected infrastructure and smart meter deployments. The challenge, for enterprises, is to combine their own data with that of their industries—or even different industries—to create unanticipated business opportunities. It’s not enough, from a competition standpoint, to simply connect devices and collect data. Given that consumers will be immersed in these increasingly inter-connected networks, enterprise can expect to struggle with interoperability issues and conflicts pertaining to data. Who controls the data will be as important as who controls the network, and concerns over privacy on the network will only increase. Continually exchanging information derived from accumulated data in the quest for new value represents the new norm for the connected business environment.

### Learning via Pilot Projects

Two effective tactics enterprises can use to learn about effecting IoT-driven transformation in their business or industry-wide include:

- Assessing benefits derived from experimentation with projects on a small scale.
- Getting ideas from deployments in different industries.

One can be forgiven for thinking that most IoT innovation occurs in the consumer world of small connected devices such as wearables and smart appliances, judging from the attention these implementations garner in the media but very sophisticated deployments in industry and municipalities have already yielded tangible benefits en route to transforming how the various organizations operate.

| Sector | Utilities and smart metering | Logistics and product ordering | Energy, smart pipeline | Municipalities, connected cities | Municipalities, connected cities |
|---|---|---|---|---|---|
| Enterprise or Organization | BC Hydro, British Columbia | Coca-Cola, Atlanta, Georgia | Kenya Pipeline Company, Kenya | Rio Operations Center, Rio de Janeiro | Copenhagen |
| Key Players | *Cisco, Itron, Cap Gemini, Accenture* | *Cisco, SAP, Datria* | *Schneider Electric* | *Cisco, IBM, Samsung* | Private companies such as Rambøll and the University of Copenhagen, the University of Aalborg, the Technical University of Denmark (DTU), and the IT University of Copenhagen. |

| Project | *Smart Meter and Clean Energy Program*<br>$900 million smart grid, smart meter investment for improvements to grid stability and meter efficiency | *Supply Chain and Logistics Improvements to Streamline Order Processing*<br>VoIP-based picking system used by 3,000 employees across 100+ facilities handling inventory, shipping, and service support<br>Partial replacement of manual, keyboard-driven operations with voice recognition | *Pipeline Automation*<br>Modernization of 900 KM pipeline network comprised of three lines<br>Implementation of supervisory control and data acquisition (SCADA) by Schneider Electric to address processes from transmission to operations to invoicing | *Smart City Implementation*<br>Data collection from city-wide sensors to assist decision-making<br>Centralized operations via technology integration<br>Objectives:<br>Improve traffic control<br>Improve safety<br>Cut emergency response times<br>Increase inter-agency collaboration | *Smart City Implementation*<br>Taking the city in a greener *direction*<br>34 million Euro investment in new streetlights<br>13 million Euro investment in intelligent traffic management, new traffic lights |
|---|---|---|---|---|---|
| Payoff | 1.8 million meters replaced across Canada enable remote monitoring, s over-the-air firmware<br>75% theft reduction<br>$330 million savings in meter reading costs<br>$224 million operations cost reduction because of self-service features | $2 million capital cost reduction<br>10% worker productivity increase<br>99.8% outbound order accuracy in more than 7.5 million yearly orders (historical accuracy was only 90%) | Elimination of oil theft via automatic leak detection<br>Safety improvements through energy shutdown capabilities<br>Increased operation uptime<br>Centralized control system addresses technology challenges and policy changes | 20% reduction in emergency response time<br>Improved quality of life for city residents and visitors<br>Improved public event security | Projected 10% reduction in travel time for  cyclists and bus passengers by 2018<br>Commitment to keep travel time for motorists the same |

### Limiting Security Risks

As with consumer implementations, industrial and enterprise implementations share the concern of limiting the effects of connectedness on security. Lacking the necessary precautions, even harmless consumer devices—such as appliances—can pose dangers to enterprises, if not through the damaged caused by network hacks then through damage to an organization's reputation by a data breach—which can have serious follow-on financial consequences. Issues management staff probably never anticipated having to explain an Internet-connected fridge sending spam to tens of thousands of users after being made into a botnet. The difficulty for enterprises is to understand the security implications of Internet connectivity featuring different types of devices and protocols when this is not their core businesses. This challenge applies to industries as diverse as auto manufacturing and home appliance production. Addressing security must also go hand in hand with figuring out scalability, for enterprises need ways to get data into their enterprise systems in order to transform their business processes.

As with consumer implementations, industrial and enterprise implementations share the concern of limiting the effects of connectedness on security. Lacking the necessary precautions, even harmless consumer devices—such as appliances—can pose dangers to enterprises, if not through the damaged caused by network hacks then through damage to an organization's reputation by a data breach—which can have serious follow-on financial consequences. Issues management staff probably never anticipated having to explain an Internet-connected fridge sending spam to tens of thousands of users after being made into a botnet.

Given the projections for IoT explosion, a very large number of IP-enabled devices will be absorbed into enterprise networks, vastly increasing the number of insecure end-points. Consider:

- Consumer devices such as fitness monitoring applications, smart glasses, and smart watches.

- Asset-tracking systems.
- Industrial robots.
- Plant control systems.
- Sensors for monitoring and maintaining industrial equipment.
- Smart heating and lighting systems.
- Smart meters.
- Smart retail shelving.

Whether these devices have sensor-enabled Internet connectivity added, or whether they are single-purpose devices originating in the consumer market, perhaps most of them will remain vulnerable to common online attacks. Unless IT policies and behaviours change, IT departments are unlikely to monitor them or send them patches to remedy current security issues. This marks a divergence from standard firmware, OS, and patch support that enterprises count on to maintain a network infrastructure protected by anti-virus, anti-malware, and anti-spam measures.

The reality of widespread connectedness means changing one's ideas about what it means to protect the network. It might mean adopting the mind-set, as a starting point for crafting a defence, that the perimeter is permeable and has already been breached. It can be destabilizing to hold that the enterprise can no longer control access to a network, but that is not an argument for having no perimeter defence. As Amit Yoran, general manager at RSA and former director of the National Cyber Security Division at the U.S. Department of Homeland Security maintains, we won't be able to characterize enterprise networks as inherently stand-alone. Rather, there will be interconnected networks, areas of overlap between enterprise networks and the wider IoT. These nexuses of vulnerability offer the greatest opportunity for thinking about and implementing IoT security.

As employees make their IP-enabled devices part of the enterprise network, the trend places greater demands on IT and IT security departments to provide support and ensure that information is secure. This represents an opportunity for vendors adept at performing complex technology integrations if they can negotiate the interplay between enterprise

networks and the new world of heterogeneity.
The hardware and software environment of the IoT will present IT security people with something unlike the layered software model of traditional networks. Hardware plus applications embedded in the operating systems of devices and appliances will render the environment more heterogeneous, and IT departments will have to expand their capabilities to handle new communications protocols such as IoT6, WebHooks, and Zigbee which will join 802.11, HTML5, and TCP/IP. John Pescatore, research director at the SANS Institute in Bethesda, Md. sees that IT departments will also need to expand their view of a normal life cycle lasting two or three years to something that can be mere months to a couple of decades.

Surveyed IT managers listed consumer devices, control systems for industry, medical devices, and smart building applications as major concerns with Internet connectivity. Configuration errors in IP addresses for IP-enabled devices such as webcams, printers, and photocopiers will pose challenges in networks where they have been put online without having their default IP settings changed.

To get a flavour of the challenges of the heterogeneous network, it's worth examining use patterns and behaviour related to DNS lookups revealed in research conducted by OpenDNS Security Labs. OpenDNS Security Labs conducted a series of tests on FQDN queries related to network traffic for Samsung's smart TVs and the Nest thermostat. Without user input, smart TVs actively call out to external addresses (beacon). This enables frequent, regular, updates to installed applications in order to obtain current content. OpenDNS Security Labs found that many FQDNs directed at xpu.samsungelectronics.com originated from a range of industries: apparel, energy, health care, restaurants, and retail—locations where one might expect to find televisions. Furthermore, the server queried was using an untrusted certificate.

OpenDNS Security Labs expressed concern that smart TVs beacon almost every minute they're in use. In the corporate world, this increases the risk of sources outside the corporate network being able to figure out the purposes for which the devices are used and to capture input from voice recognition software. The implications become more apparent when one considers that enterprises place smart TVs in places where employees congregate and increasingly use them in place of boardroom projectors.

The research by OpenDNS Security Labs highlights the complexity of the issues faced by IT departments when managing the interaction between enterprise networks and the IoT. For instance, it would be simple for a firewall administrator or upstream Internet service provider to block access to an IP address or subnet—because of bad neighbourhood associations—rather than block a list of specific, malicious domains. This might have unintended consequences, such as preventing legitimate communications between IoT devices their cloud-based or hosted services.

Both the enterprise IT establishment and their user communities are struggling to keep up. IoT devices embedded in enterprise networks enable new paths for remote exploitation, yet most IoT devices skirt IT professionals' control by virtue of their reliance on network infrastructure that is cloud-based or hosted. In a recent survey, almost 75% responding IT professionals indicated that their enterprises had defined policies for connecting Internet-connected and employee-owned IoT devices, but 65% of employees either did not believe such policies existed or were unaware of any IoT policy their companies had enacted. That blocks to untrustworthy cloud subnets or hosting could inhibit the functioning of IoT devices on enterprise networks undermines the employee attitude that their IoT devices are their own personal gadgets or just toys, for these devices co-exist in an environment with enterprise IT equipment.

The IoT, while enabling, or compelling, enterprise to change its processes is bringing change to the relationship between enterprise and its employee stakeholders. Enterprise is increasingly in the role of enabling employees to perform functions in order to meet business objectives by adapting their wok styles and bringing their own devices. Enterprise leaders are thinking seriously about security, and must assess the security implications of their policies even as they try to create more nimble and insightful organizations made possible by IoT implementations.

### Achieving Results

While there is no template for IoT success, there are apparent trends enterprises can look to for planning inspiration.

- Control technologies and data are making the workplace smart and connected via sensors and wearable devices.
- Field operations and office processes are increasingly measurable and amena ble to improvement via quantification because of greater instrumentation use.
- Managing the information created by connectedness and deriving insights from it will be the task addressed by tools developed for big data.
- Enterprises will evolve to designing their products and services around IoT from an earlier stage of simply enabling IoT connectivity.
- Staying relevant with customers round-the-clock will become essential to maintaining marketplace presence.

Developing insights from an approach to handling data that scales and allows the enterprise to incorporate new types of information makes sense because where enterprises use a flexible platform that can adapt to the future. Without such platform adaptability, application development means a lot of headaches. Companies risk being stuck with a static system, which forces them to constantly invest resources—significantly, time—in developing their next generation IoT products and services.

Beyond changing the ways that enterprise develops products and services, IoT-connectable products transform customer relations by changing the end user experience in ways that allow for more nuanced forms of marketing, which, in turn, generate insights for incorporation into processes, design, and service delivery. Enterprises that achieve success with IoT will be skilled at re-thinking their approaches and developing products that adapt to the user by applying the context of the user's intent based on a sophisticated profile and an awareness of the user environment.

There is a strategic dimension to developing adaptive IoT products. Applying good IoT techniques and design principles will probably generate revenue value-added services that will likely generate revenue, but for enterprises to have the biggest impact they will have to leverage the network effects of a big-data ecosystem, either pre-existing or self-created. The risks of not doing so, and the rewards of achieving this, should be apparent.

## The Litmus Approach

The overriding enterprise need is for an IoT approach flexible enough to accommodate their application infrastructure and existing hardware, and work with their hardware partners. Such an approach should be adaptable enough to incorporate new protocols, hardware, and systems. The Litmus approach meets these requirements, allowing enterprises to build out pilots and production level deployments while eliminating concerns about, connectivity, device management, data integration, security, and scalability.
Many companies struggle with the complexity of developing applications to connect devices to the Internet and derive useful insights. The process can take months, or years. The Litmus approach reduces the time it takes to build your proof of concept to weeks or even days. We make it easy to get started by offering ready-to-go client libraries for gateways, embedded systems, mobile, and desktop. A few clicks enable smart devices to start sending data to the applications of your choice. This is true rapid development--days or weeks instead of months or years.
With Litmus, connecting devices to the Internet cannot get any simpler, for it provides a complete Internet of Things connectivity package. Litmus simplifies the connection of devices to application with a secure, scalable, cloud platform, enabling faster time to market for IoT initiatives. Features include:

- Integration with existing enterprise systems
- Hardware-agnostic platform compatible with major embedded systems including legacy industrial and other protocol standards
- Real-time device management
- Industry’s first enterprise application marketplace

- Cloud presence enabling expanded interconnectivity to other solutions.

We know that enterprise won’t make money just by connecting things to the Internet; value comes from generating business insights from those devices. So, Litmus provides cost certainty through pricing that lets enterprises scale economically. Paying $1-$5 per month per device for IoT connectivity is not a sustainable business model, for that limits the enterprise's ability to scale. Instead, the Litmus business model focuses on every application connected. Connect one device, 100 devices, or 10,000 devices; it really doesn’t matter to Litmus. Since there's no charge per device, there's no tax your scalability.

Making the most of IoT deployment becomes less of a challenge with the Litmus one-click connectors and zero-config approach to get devices communicating with applications. Enterprises can send data in any format, any structure, and Litmus will re-format it on the fly to speak to the end application. Litmus eases integration by providing a one-of-a-kind IoT marketplace of ready solutions. Litmus’ flexibility at working with all protocols lets enterprises future-proof their solutions in a world of fluid, competing, or non-existent standards. Litmus provides integration, end-to-end connectivity, and future-proofing built in.

Litmus also provides data security, for safeguarding business-critical information is a serious concern. The Litmus approach to security is multi-dimensional, encompassing the transport layer, authentication, and encryption. Litmus does not store a single byte of your data. Instead we collect data from sensors and transmit that data to applications employing fine-grained authentication and authorization policies. Data transmission occurs over an encrypted pipe, which uses SSL and TLS.

Overall, Litmus is highly customizable and works well with existing infrastructure—which enables tailor-made solutions. If the enterprise requires modifications, Litmus can design and build a custom solution for the specified platform.

### Supported Clients

Designing a solution with Litmus takes just a few lines of code. Enterprises can deploy Litmus out of the box for prototyping platforms such as:

- Arduino
- Arduino
- BeagleBone Black
- Chipkit Max32
- Chipkit Wifire
- Compex WPJ344
- Cubieboard
- EA LPC4088
- Electric Imp
- Flyport
- Freescale Kinetis K64/KL25Z
- Intel Edison
- Libelium Wasmote
- Mbed
- MSP430
- Netduino Plus 2
- Raspberry Pi
- Spark
- TI Stellaris
- TI's CC2540 SensorTAG
- TM4C1294
- WeIO
- Wiznet (IP compatible )

Support for mobile platform such as:

- Android
- iOS
- Windows

### Scalability

Litmus has been built from the ground-up with scalability and high availability in mind:

- Handles a large numbers of concurrent connections.
- Smart orchestration architecture automatically allocates resources to ensure optimum device performance.

### Fast, Secure Communications

Embedded systems have limited processing power. Litmus uses the MQTT communications protocol which works well with constrained devices.

- Higher throughput for the same amount of power.
- Less network overhead compared to existing HTTP or HTTPS protocols.

## A Note on Sources

The following sources of information contributed to this Litmus white paper.

- 6 ways the Internet of Things will transform enterprise security, Computerworld, http://www.computerworld.com/article/2489549/security0/6-ways-the-internet-of-things-will-transform-enterprise-security.html, http://bit.ly/1HDQ85q
- 10 enterprise Internet of Things deployments with actual results, Network World, http://www.networkworld.com/article/2848714/cisco-subnet/10-enterprise-internet-of-things-deployments-with-actual-results.html, http://bit.ly/1vl0oem
- IoT Revolution: Is The Enterprise Ready?, InformationWeek, http://www.informationweek.com/strategic-cio/it-strategy/iot-revolution-is-the-enterprise-ready/a/d-id/1319636, http://ubm.io/1bDcjMO
- Is the Internet of Things strategic to the enterprise?, ZDNet, http://www.zdnet.com/article/is-the-internet-of-things-strategic-to-the-enterprise/, http://zd.net/1EYGTrB
- The 2015 Internet of Things in the Enterprise Report, Open DNS, https://www.opendns.com/enterprise-security/resources/research-reports/2015-internet-of-things-in-the-enterprise-report/, http://bit.ly/1VMGG8o
- The corporate 'Internet of Things' will encompass more devices than the smartphone and tablet markets combined, Business Insider, http://www.businessinsider.com/the-enterprise-internet-of-things-market-2014-12, http://read.bi/1usaNje
- The Internet of Things and the Enterprise Opportunity, Forbes, http://www.forbes.com/sites/gartnergroup/2015/07/16/the-internet-of-things-and-the-enterprise-opportunity/#2e1d0f4e2c28, http://onforb.es/1VMHES1
- The Internet of Things is a necessary choice for the enterprise, CIO, http://www.cio.com/article/2908958/internet-of-things/internet-of-things-is-not-a-choice.html, http://bit.ly/1JNopOY
- What's the Internet of Things' enterprise potential?, TechTarget, http://internetofthingsagenda.techtarget.com/feature/Whats-the-Internet-of-Things-enterprise-potential, http://bit.ly/1TrTwoy

LITMUS

Litmus enables out-of-the-box data collection, analytics, and management with an Intelligent Edge Computing Platform for IIoT. Litmus provides the solution to transform critical edge data into actionable intelligence that can power predictive maintenance, machine learning, and AI. Customers include 10+ Fortune 500 manufacturing companies, while partners like Siemens, HPE, Intel and SNC Lavalin expand the Company's path to market.

**LITMUS.IO**