A HURWITZ WHITE PAPER

The Value of Bringing Analytics to the Edge

Daniel Kirsch
Principal Analyst
and Vice President

HURWITZ
& ASSOCIATES
Insight to Action

Sponsored by Dell

Introduction

The Internet of Things (IoT) has quickly gained traction and captured the attention of organizations because of the profound insights that it can provide. Massive amounts of data from sensors can be analyzed to make our world more efficient and safer. Companies are also beginning to understand that the IoT can drastically change the way offerings are developed, sold and consumed. Technology advancements in areas such as communications, power and compute efficiencies, as well as cloud, big data and analytics capabilities have made the IoT accessible to more organizations. Many organizations are investing in new IoT initiatives in a variety of use cases including retail, hospitality, energy, and fleet management.

While connected devices stream massive amounts of data, the complexities of managing all of that data and producing meaningful insights are difficult. There are many different approaches to managing IoT data based on your business objectives and the technical challenges. Organizations are using centralized cloud and data center environments in certain situations to support IoT based analytics. This centralized data integration approach is especially important in analyzing disparate data sources and when real time and speed are not priorities. However, there are other situations where IoT data needs to be analyzed in near real time in order to ensure rapid execution and effect change. For example, real-time analysis of sensor data on a manufacturing system can detect too much moisture or too high a temperature. This situation will require immediate action to prevent failure. Achieving this type of rapid response creates a new set of requirements in areas such as storage, security, data management and bandwidth. Without an infrastructure that supports this type of real-time action, many companies are not realizing the full potential of IoT data.

One of the ways organizations are beginning to gain more insight and value from IoT data is by architecting for analytics at the "edges" of their environments. This architecture requires that analytics be embedded both directly within endpoints such as sensors, controllers, equipment, and machines, and in nearby aggregation locations such as basements, control rooms, data closets and ceilings. Collecting and analyzing data close to the endpoints means that action can take place locally in real or near-real time. In this way, only meaningful information needs to be backhauled to the datacenter or cloud for storage, benchmarking or advanced statistical analysis.

Collecting and analyzing data close to the endpoints means that action can take place locally in real or near-real time.

The Challenges of Managing and Executing Analytics on Sensor Data from a Centralized Location

There are many complexities involved in gaining the type of insights that businesses increasingly require from their IoT data. To be successful, organizations need to have the right foundation in place. These organizations need to make it a priority to evaluate the potential challenges of executing analytics on IoT data from a centralized environment. Some of the challenges are

HURWITZ & ASSOCIATES
Insight to Action

caused by the nature of the data itself and the physical environment where the data resides. Other challenges are related to how to protect highly sensitive data. In addition, companies need to be mindful of issues related to latency, and the overall complexity of the environment. In this next section we will focus on the approaches that will help you begin your journey to a well-executed IoT strategy. The challenges can be understood based on four imperatives:

IoT infrastructure is highly fragmented
An IoT environment is typically comprised of a myriad of sensors and devices communicating over non-standard protocols that are difficult to integrate and manage. This is especially the case in commercial and industrial environments where organizations need to integrate legacy equipment. Additionally, wireless mesh sensors are often capable of running for years on a single battery by requiring small amounts of power and not connecting directly to the Internet.

Latency and inconsistent connectivity can be inhibitors
IoT solutions often require rapid data insights and control responses. Typically you can't achieve the required speed if latency is introduced from sending data and application calls between remote devices and centralized systems. For example, there are many uses cases where inconsistent wide area connectivity can make centralized analytics impractical. Depending on the use case, a large organization could have hundreds to millions of sensors constantly going on and offline.

Data movement and storage can be costly
Billions of devices, sensors and networks are connected to the Internet and create and receive data around the clock. This generates tremendous amounts of data that must be transferred to a location for storage and analysis. As the number of devices expands and the volume of data increases, the costs of data transport and data storage can quickly become prohibitive.

Connecting infrastructure and devices can introduce security risks
Security is paramount to any data-driven solution. Traditionally, IoT solutions have been designed to be closed-loop networks that have no exposure to the Internet. While isolation is certainly a way to avoid risk, it also prevents the system from taking advantage of the value of external data feeds and tapping into even more powerful remote processing to supplement local analytics capabilities. In addition, many connected devices that collect and transfer data to a centralized repository lack the capability to deploy sophisticated security controls and safeguards. Further, if every single IoT device were linked across the Internet to a centralized cloud, it would expose an incredibly large attack surface for hackers to gain access to critical data and applications. Even more troubling, this centralized approach can potentially send malicious control commands back to the devices. One effective solution is to consolidate multiple sensor connections into a secure aggregation point behind a firewall. Centralizing data behind the firewall helps reduce the overall attack surface.

While isolation is certainly a way to avoid risk, it also prevents the system from taking advantage of the value of external data feeds and tapping into even more powerful remote processing to supplement local analytics capabilities.

The Role of an Intelligent Edge Gateway

A new generation of devices – intelligent edge gateways – are providing enterprises with the option to address some of these challenges by performing critical data analytics close to endpoints at the edge of the network. These

HURWITZ & ASSOCIATES
Insight to Action

small gateways aggregate the fragmented wired and wireless sensor protocols common in operations environments and normalize them into standard IP traffic that is well-understood by IT.

In addition to unifying fragmented sensor data, an intelligent edge gateway has the processing capacity to perform additional analytics in real or near-real time to make data-driven decisions as close to the data generation as possible. Performing analytics on the gateways helps reduce network bandwidth cost because only meaningful information needs to be sent to the next tier, whether it is another gateway, the datacenter, or cloud. In contrast, analytics in the datacenter or cloud is often focused on larger data sets and performed in batches. Distributed IoT architectures that include intelligent gateways help balance the overall system and reduce the big data burden on the datacenter and cloud.

Distributed IoT architectures that include intelligent gateways help balance the overall system and reduce the big data burden on the datacenter and cloud.

As Figure 1 shows, an IoT analytic system can be broken up into four key elements:

1. **Data sources:** The system can consist of a variety of endpoints that gather and transmit data. The data sources can be discrete endpoints such as sensors, machines, energy producers, medical devices or even security cameras. In addition, the data sources can be entities that aggregate many endpoints, for example a building, factory, or vehicle. The data coming from these endpoints is often transmitted in a variety of protocals including DNP3, LAN, ZigBee and SCADA.

2. **Edge aggregation and analytics:** Depending on the use case, the data sources may be set up to feed data directly into an edge aggregation and analytics device or directly to the cloud. In the case of an intelligent gateway, some data can be processed with local analytic software in real or near-real time to generate data-driven actions and insights. Additionally, data may simply be passed through to the next tier such as another gateway, datacenter or cloud. In the framework presented in Figure 1, several gateways have been deployed. Some of the gateways have a single endpoint feeding it data while one of the gateways has several endpoints streaming data to it in a variety of protocols.

   Consider an intelligent gateway inside of a rooftop HVAC unit that collects hundreds of data points a second. The organization's central monitoring station may require only a few key points be sent every day. Meanwhile, the gateway can be used to analyze every piece of collected data in real time in order to optimize performance or sense an impending failure. The gateway can then trigger events to alert repair crews or safely shut itself down. Once in the centralized system, the subset of data from the HVAC unit can be used for batch analytics and longer-term energy efficiency planning. Transferring only the most important information greatly reduces the amount of data sent across the network while still providing insights and business value to the end user.

3. **Storage and analytics:** Sensor data sent to the datacenter or cloud can be stored and further analyzed for benchmarking, predictive analytics, and other long-term planning. In Figure 1 some of the data is transmitted from the gateways to the cloud via a wireless wide area network while other

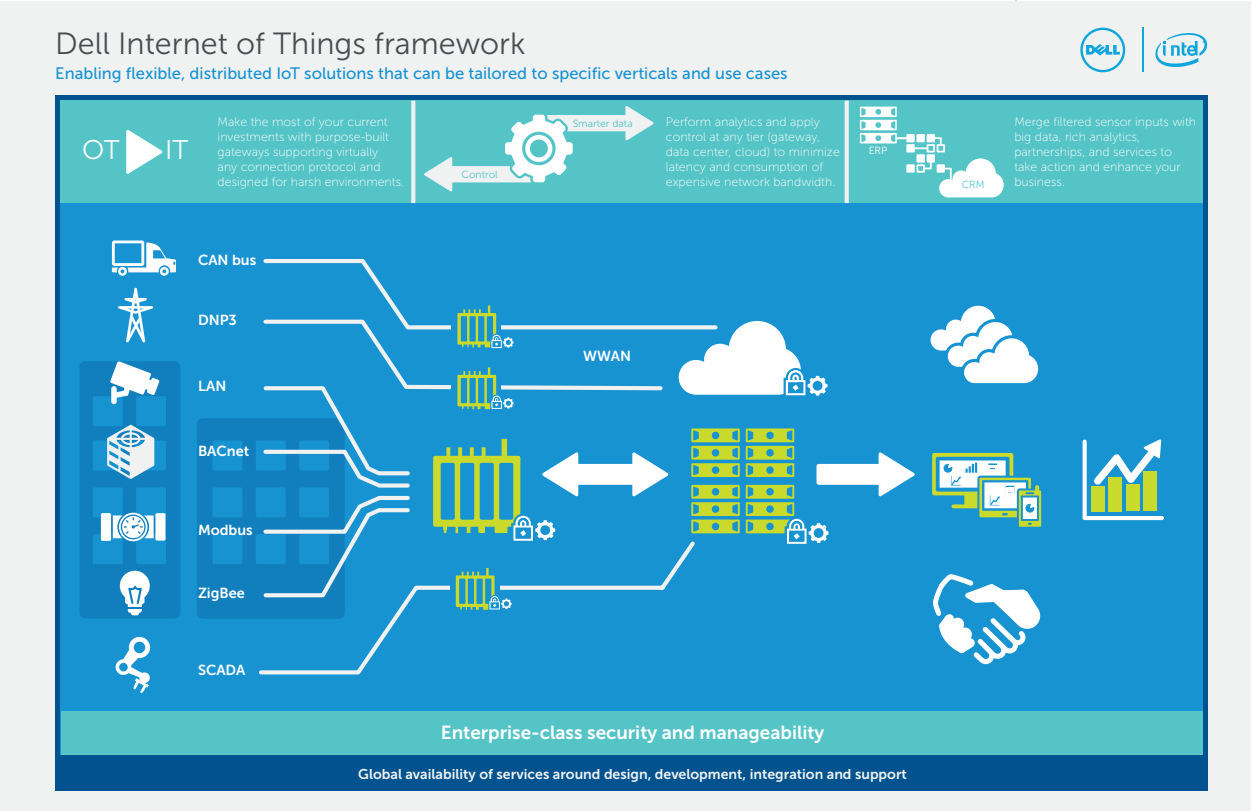
HURWITZ & ASSOCIATES
Insight to Action

gateways transmit data to a datacenter. Data scientists can run advanced analytic algorithms against the data to gain new insights and fine-tune the analytics performed on the edge device.

4. **Data insights:** The final element in an IoT system is the ability for customers and employees to gain insight from the data. To gain deeper contextual insight, IoT data can be blended with internal and third-party data sources. For example, IoT data can be integrated with CRM or ERP system data, as well as social media or weather data. In addition, organizations can provide rich analytic-based applications for customers to view and interact with their data.

To gain deeper contextual insight, IoT data can be blended with internal and third-party data sources.

Figure 1: Using Intelligent Edge Gateways to Solve Industry Specific Challenges



Source: Dell, 2015

Intelligent edge gateways provide a robust development platform for partners and customers to create industry and use-case-specific analytical solutions. We interviewed Aron Bowman, Vice President of Product Development at ELM Energy. ELM Energy is a solution provider that monitors and manages power to critical work sites such as mines and datacenters. Bowman's company often needs to quickly and automatically react to changes in customer power requirements.

One of ELM Energy's clients is a mining company that operates an off-the-grid mine. The mine has a number of electrical sources, including solar, battery and generator. The challenge for the mine was that it needed a way to manage the power sources in real time so that the most efficient source could be utilized while at the same time never losing power. The need for real-time analytics and

the fact that the mine is located in an off-the-grid location made an on-site solution mandatory. ELM Energy deployed its software solution called FieldSight that runs on a Dell intelligent gateway. The solution monitors the mine's energy requirements and the output from energy sources and then changes the energy source as needed in real time. For example, as solar power decreases the organization needs the system to be able to monitor and either pull energy from battery storage or increase generator output.

In addition to performing local analytics on the gateway, the gateway transfers pre-processed data to a cloud-hosted version of its FieldSight software. Once the data is transferred to the cloud, further benchmarking and advanced analytics can take place. In addition, the maintenance of the gateway can be performed remotely. This is especially important for ELM Energy because the company often works with clients that have isolated sites. With its solution, customers are able to run reports, perform further analytics, and view the data via ELM's Software as a Service (SaaS) application.

By implementing Dell's intelligent edge gateway in its IoT strategy, ELM Energy is able to make automated, real-time energy decisions on client sites while at the same time, transfer the most meaningful data to its cloud for even deeper analytics.

Dell's Edge Gateway 5000 Series are purpose-built to provide the power of analytics at the edge of the network.

Dell Enables Secure Edge Analytics with an Intelligent Gateway

Dell has launched a new line of intelligent edge gateways designed to enable scalable IoT solutions. Dell's Edge Gateway 5000 Series are purpose-built to provide the power of analytics at the edge of the network. Dell's gateways are powered by dual-core Intel Atom processors and are capable of driving a wide range of IoT solutions. The Intel Atom dual-core processors provide the performance to bring intelligence to the edge. Figure 2 shows a Dell intelligent edge gateway mounted to a wall.

Figure 2: Dell Intelligent Edge Gateway

Source: Dell, 2015

Continued next page

A key attribute of Dell's Edge Gateway 5000 Series is its expanded I/O to connect to both modern and legacy endpoints. These endpoints could range from an Ethernet-based security camera to a Zigbee sensor to an HVAC unit communicating over the BACNet protocol. Both Dell and Intel support data normalization through protocol abstraction to improve interoperability. The goal is to normalize fragmented, non-standard protocols.

Dell gateways have an industrial-grade form factor and extended environmental specs, which allow them to be deployed in challenging environments in the middle of the action at the edge of the network, while performing 24/7 with long life. Examples where this is critical include predictive maintenance analytics inside a piece of outdoor equipment where temperatures can hit extremes, or quality control in a hot factory where contaminants would challenge less industrial-grade devices. Along with the right physical I/O, these capabilities qualify Dell gateways for edge analytics jobs that traditional PCs, routers, and servers simply can't address. In addition, both Dell and Intel place a high amount of emphasis on automated discovery and provisions of edge devices to ease deployment.

Both Dell and Intel view security as a critical element in IoT solutions, and advocate the use of embedded hardware and software level protection. The right mix of security features are needed to address the potential security risks that come from connecting sensors and other devices to the Internet. At the hardware level, Dell gateways feature TPM (Trusted Platform Module) chips that create a root of trust regarding the integrity of the device. In turn, this root of trust enables a secure boot, which loads and verifies local firmware and software. Dell gateways are also built with processing power to encrypt sensor data and can be programmed to run local stream analytics to trigger security alerts if abnormal network activity is detected. Furthermore, Dell's management tools further help ensure security and compliance levels are met. Combined, these capabilities help ensure data security and privacy starting from the foundation of an IoT solution stack.

Complimenting Dell's new line of edge gateways is its Statistica software platform, which enables advanced analytics of both structured (sensors, form input) and unstructured (documents, social media) data. Dell has recently announced a new distributed analytics offering that leverages Dell Boomi as the shuttle to move Statistica analytics jobs between gateways at the edge, the datacenter and the cloud to provide maximum flexibility. These enhancements are consistent with the Dell and Intel IoT strategy of providing a broad analytics infrastructure from edge to cloud. Dell is also certifying a wide variety of Independent Software Vendors (ISVs) that have purpose-built analytics software and industry domain knowledge.

Continued next page

Dell gateways have an industrial-grade form factor and extended environmental specs, which allow them to be deployed in challenging environments in the middle of the action at the edge of the network, while performing 24/7 with long life.

HURWITZ & ASSOCIATES
Insight to Action

Dell is participating in a variety of industry working groups and consortiums to bring IoT solutions to the market. Dell is a Premier member of the Intel Internet of Things Solutions Alliance. The Intel IoT Solutions Alliance has more than 400 global member companies. The alliance is focused providing scalable, interoperable solutions that accelerate the deployment of intelligent devices and end-to-end analytics. In Addition, Dell is a member of the Open Interconnect Consortium, and the Industrial Internet Consortium.

The Benefits of Bringing Analytics to the Edge

Intelligent, purpose-built gateways are valuable tools to offset many of the cost and performance issues associated with running all analytics in a centralized location. For system integrators and OEMs, these gateways provide a flexible platform to develop analytics solutions that make big data more manageable, increase efficiency, maintain operations, and improve scalability. In this section we highlight some of the reasons why organizations are considering intelligent gateways as part of a distributed IoT architecture.

Better efficiency and 'less-big' data
Intelligent gateways can help organizations filter data close to the point of inception through real or near-real time analytics such as stream or Complex Event Processing (CEP). Only the most meaningful and pre-processed data and events are sent to a centralized data-hub. The ability to filter out non-critical data and only transfer the most important data to centralized data centers is a key capability of gateways and reduces the consumption of network bandwidth. The pre-filtering of data is especially critical in use cases such as smart city, fleet and remote applications where cellular is a common communication choice.

Self-sufficiency
Intelligent gateways are capable of bi-directional data flow in terms of aggregating new sensor data and pushing back control to connected actuators and equipment. With local intelligence, an edge gateway can execute either pre-programmed or dynamic control instructions based on analytics, autonomously from the backend. The ability to store data locally avoids the potentially catastrophic problems caused if an Internet connection is lost.

Improved security
The processing power of an intelligent gateway can help secure IoT solution because the gateways has the processing capacity to encrypt data from less capable connected devices and sensors. The increased processing power allows the gateway to run local stream analytics that can search for behavioral anomalies. Security measures can be built into the gateway solution to ensure that only trustworthy devices are allowed to connect. Gateways also aggregate data streams from otherwise cloud-connected devices, thus reducing the overall attack surface between the enterprise firewall and the cloud for hackers to exploit.

Gateways … aggregate data streams from otherwise cloud-connected devices, thus reducing the overall attack surface between the enterprise firewall and the cloud for hackers to exploit.

HURWITZ & ASSOCIATES
Insight to Action

Highly adaptable to vertical use cases and industries
Compared to legacy controllers and appliance-like routers, intelligent gateways can run modern operating systems and are designed to be highly extensible through new applications. The gateway's operating system and flexibility allows partners and customers to develop and deploy purpose-built applications that meet specific industry and use-case requirements. Examples of edge analytics solutions that have been implemented or are currently underway include energy management within buildings, predictive maintenance for industrial equipment, video analytics for quality control, tracking for critical shipments using wireless mesh sensors and intelligence within vehicles for reducing fuel consumption and breakdowns.

Conclusion

The need for more analytics, control and greater insight on IoT systems cannot be met by just connecting more sensors, endpoints and other devices to the Internet. It is imperative to take a holistic approach to creating an environment that provides a scalable, predictable, secure, and manageable solution. This engineered approach to IoT allows customers to be able to control costs by leveraging the most effective way to manage data movement, compute and storage. By creating a platform that supports change and growth, IoT environments can become a way to protect company assets and enable new business opportunities.

As enterprises increase their investments in the Internet of Things, intelligent gateways can play a significant role in keeping the balance between expansion and security. Intelligent gateways enable organizations to securely connect and process data at the place where it makes the most sense. Many of these IoT gateways must operate in harsh conditions where traditional devices such as PCs, routers and servers would be ineffective. Pushing analytics to the edge of the network with intelligent gateways for IoT data is also helping organizations make real-time decisions close to the data and reduce data storage and transfer challenges by focusing on the most meaningful data.

By creating a platform that supports change and growth, IoT environments can become a way to protect company assets and enable new business opportunities.

HURWITZ & ASSOCIATES
Insight to Action

About Hurwitz & Associates

Hurwitz & Associates is a strategy consulting, market research and analyst firm that focuses on how technology solutions solve real world customer problems. Hurwitz research concentrates on disruptive technologies, such as Big Data and Analytics, Cognitive Computing, Security, Cloud Computing, Service Management, Information Management, Application Development and Deployment, and Collaborative Computing. Their experienced team merges deep technical and business expertise to deliver the actionable, strategic advice clients demand. Additional information on Hurwitz & Associates can be found at www.hurwitz.com.

35 Highland Circle • Needham, MA 02494 • Tel: 617-597-1724
www.hurwitz.com