ESG Lab Review

Dell EMC Digital Platform for Enterprise Assets and Internet of Things

Date: May 2017 **Author:** Mike Leone, Senior Analyst; and Tony Palmer, Senior Analyst

Abstract

This ESG Lab Review looks at how businesses drive outcomes with the use of Dell Technologies and Dell EMC assets. The Dell EMC assets include a turnkey platform consisting of Native Hybrid Cloud and Analytic Insights Module as part of Dell EMC Converged platforms and solutions. ESG Lab observed how Dell Technologies can empower organizations to:

- Define their approach to augmenting digital transformation with IoT (Internet of Things) and surveillance technologies with persona-driven use cases.
- Blend video-based, visual verification with IoT and enterprise data to move beyond traditional surveillance and security investigation and enhance customer experiences, identify overhead, respond to incidents, and collect evidence.
- Understand how to evaluate and extend an infrastructure for enterprise IoT—core, edge, and cloud—with data transparency and right-time intelligence.
- Accelerate maturity progression from proof of value to production, including multi-data center, mission-critical deployment.

Business Challenges

Business expectations are higher than ever before. In this age of digitization with the rise of the Internet of Things, organizations are increasingly turning to technology to compete effectively. Customers expect more precisely timed, personalized services and offerings in the context of previous interactions. Partners, suppliers, employees, and the larger community all share these higher expectations. This requires deeper predictive analytics, rapid and continuous software development, and the evolution of existing processes into more agile ones. Initially businesses adopted an approach that optimized processes to handle a single specific purpose where a limited set of data might be available. However, as digitization initiatives matured, these organizations realized that they lacked the architecture necessary to make the transition to more mission-critical and agile practices that can tap a wide variety of data sources across the time series.

New approaches are needed to fully integrate IT (information technology) and OT (operational technology), drive better outcomes through real-time event correlations, and provide capabilities for edge processing, advanced analytics, and data lifecycle management. Providing an immediate and optimal response to changing conditions may also benefit from predictive analytics models based on a longer historical view. This requires a multi-tier architecture that allows for agile application development and analytics that help change business behaviors and take advantage of broader insight.

Furthermore, many organizations are looking to build new businesses and expand beyond their traditional industry boundaries—think of an integrated retail and manufacturing company striving to become a service company with many new offerings, for instance—such an undertaking would require rethinking their technology investment strategy to make application development and analytics easier to deploy and more repeatable, while still managing ongoing business operations.

Based on an ESG research survey of over 500 IT professionals and executives, operational efficiency (45%), differentiated customer service (39%), product and service innovation (38%), and the creation of new business models (26%) were the most-cited impacts that organizations anticipated as a result of implementing IoT.[1]

[1] Source: ESG Brief, *IoT in the Context of Digital Industrial Transformation*, February 2016.

Accommodating each of these areas of impact will motivate organizations to pursue digital transformation as operations, processes, and business rules must be adjusted.

Therefore, a good place to start building a digital platform to take advantage of enterprise assets and IoT is with a robust platform that scales in edge, core, cloud, and multi-cloud environments. This is where most data integration and heavyweight analysis will take place but it can be also extensible for fog data centers and cloud. Begin with infrastructure choices that will meet the demands of IoT and enterprise applications and analytics at the core, including scalability, performance, reliability, and availability. Unless you feel strongly about a single vendor, this should be an open and flexible platform, as there isn't much to be gained from a narrow, vertical approach (except vendor lock-in). No one company offers everything in a technology stack spanning from machine sensors to machine learning. So, look to adopt an infrastructure provider with a fit for purpose-built components and that can provide a large, growing ecosystem instead.

The Solution: Dell EMC Digital Platform with the Internet of Things

While no single company can deliver all the hardware and software needed to build a complete IoT technology stack that drives a business outcome, it's still not desirable to source every component from a different vendor. The complexity of integrating and supporting everything would be daunting, to say the least. Organizations need to look at the environment as supporting the analytics and applications, then choose a vendor based on who can provide the most complete (and versatile) infrastructure platform.

Dell EMC has always offered a strong platform for core data centers and has a defined portfolio to accommodate customers with a preference for build versus buy choices. Dell EMC came to the enterprise market with components like Vblock Systems, VxRack Systems, VxRail Appliances, and other products (including specialized offerings like Dell EMC Isilon) available as Technology Extensions. These technologies were widely utilized in big data and video management software (VMS) solutions for central data analysis, model building, underlying custom/industry apps, business apps, analytics, and security/access apps. Similarly, Dell PowerEdge servers were widely used to support both applications and big data in data centers around the world. With the merger of Dell and EMC, the combined range of IoT solutions expands readily with Dell's Edge Gateways and PowerEdge servers tied locally to sensors and operational technology. Dell EMC's VxRail Appliances can also play an important role, acting as aggregation points with Dell Edge Gateways or with direct cloud connect from end devices. They provide additional processing and archival in many edge environments and can be integrated with larger data center implementations.

Dell EMC has also distinguished itself as an infrastructure provider for multi-data center, mission-critical environments where networking connections between the core and edge environments to collect and aggregate data are mandatory. Dell EMC fabric, with spine-leaf configurations, is designed to bring networking scalability without undue management complexity.

Many organizations are deploying their own custom applications in conjunction with enterprise applications and analytics on the Dell EMC portfolio of products, with an extensive variety of third-party software solutions. These solutions allow them to extend the ecosystem with Dell Edge Gateways available from a large community of more than 70 partners. Dell Edge Gateways can also be used as scale points with a variety of Dell EMC products and services as the number of devices and data attributes grow in core, edge, and cloud architectures.

To enable PaaS and IaaS clouds, the Dell EMC Native Hybrid Cloud Platform can be a fast and flexible path forward for analytics and application development. This turnkey platform is designed to provide a path to digital transformation, accelerate time to market, and enhance customer experiences. Included in this portfolio is the Analytic Insights Module, a fully engineered solution providing self-service data analytics with cloud-native application development in a single hybrid cloud platform, eliminating the months it takes to build your own. Complementing that approach, the Virtustream managed service offers smooth portability of applications to the optimal environment for the workload and enables organizations to manage and optimize their IT assets.

In consideration of the growing interest from customers who want to build a multi-industry solution, Dell EMC leveraged the cross-industry nature of the Dell EMC platform and created what it calls the "Use Case Factory," where organizations can build new use cases out of others by adding different modules based on use case orientation and business needs. The use cases and modules serve as building blocks in a way that is like a factory. This also serves as a foundation for developing entirely new business models for organizations who may seek to expand their vertical coverage or transform from a product company into a services company.

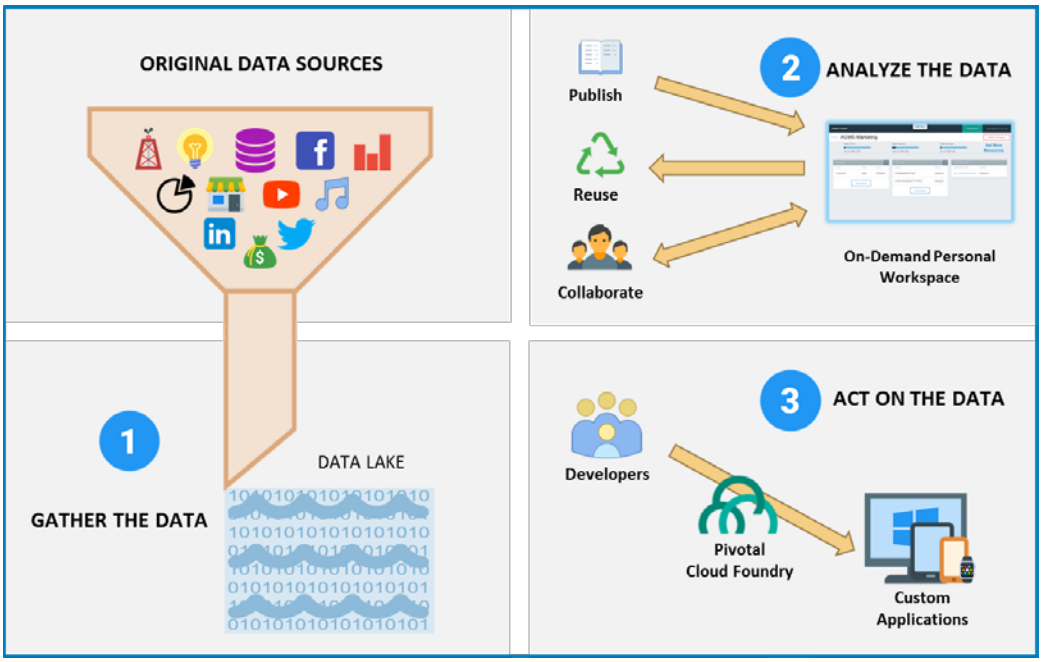
Dell EMC Analytic Insights Module

Dell EMC Analytic Insights Module is a solution that combines self-service data analytics with cloud-native application development into a single cloud platform, engineered to enable organizations to transform data into actionable insights. The Analytic Insights Module workflow consists of three primary components, as shown in Figure 1:

1. Gathering the data.
2. Analyzing the data.
3. Acting on the data.

For an organization to be competitive, the gathered data needs to include traditional, legacy, enterprise, and IoT data and the solution needs to be able to combine them easily. When incorporating the Analytic Insights Module into one of the aggregation tiers in the edge, core, and cloud architectural approach, organizations can manage IoT and non-IoT data assets alike and readily extract value from the data assets that were formerly hard to access, integrate, or draw insights from. The Analytic Insights Module works in conjunction with the complement of Dell Technologies assets from the fit-for-purpose infrastructure portfolio to enable organizations to start small and expand as their project demands grow. This access to an increased variety of data can help businesses discover patterns and generate insights rooted in the enterprise architectural foundation, which is becoming a prerequisite for a new generation of competitive organizations—data-driven enterprises that adapt quickly for increased operational efficiency, improved customer engagement, product innovation, and innovative new business models that keep pace with rising business expectations.

Figure 1. The Dell EMC Analytic Insights Module Architecture



Source: Enterprise Strategy Group, 2017

In addition, the Analytic Insights Module was engineered to make it easier for organizations to get real business value out of their data by promoting better collaboration across analysts and data scientists supporting various lines of business. Data

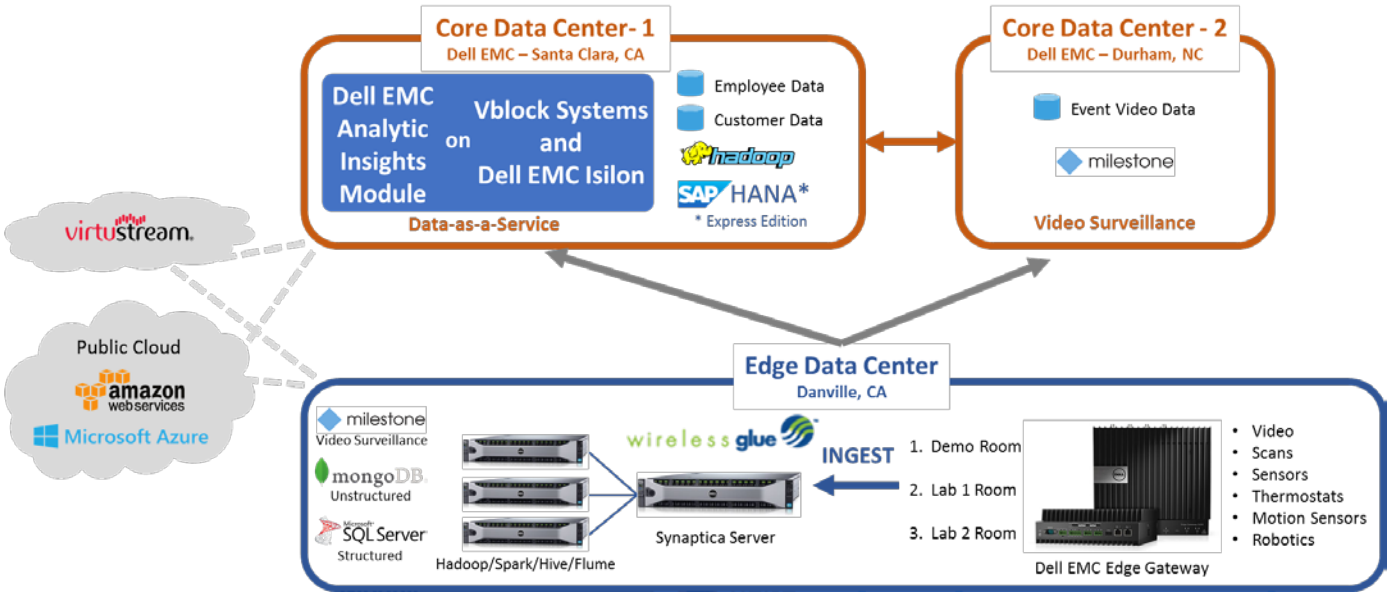
analytics has traditionally required dedicated IT resources and personnel to perform data acquisition and analysis, application development to operationalize insights, and many other manual, time-consuming activities before value can be extracted. Analytic Insights Module is designed to enable organizations to rapidly transform data into actionable insights with high business value in the fastest time possible. Data analyst teams can rapidly find valuable insights on a self-service cloud platform where IT teams can apply policies to the environment for ensuring corporate governance.

Demonstrating the Value of Blending Edge Analytics with Enterprise Data at the Core Data Center

ESG leveraged a prebuilt IoT environment (see Figure 2) consisting of multiple geographic locations, each of which represents a key element of edge analytics for IoT. The edge data center was in Danville, CA, representing a location where frontline workers might complete near-real-time analytics. The environment consisted of four Dell EMC PowerEdge servers, running Wireless Glue—data translation middleware chosen for this environment. The environment also leveraged core big data software components, such as Hadoop/Map Reduce, Spark, Hive, and Flume to handle the ingest of structured and unstructured data from Dell Edge Gateways. The simulated edge devices were in three lab environments in Colorado Springs, CO, where the Dell Edge Gateways were used to connect the various wired and wireless devices and systems, aggregate and analyze the data, and send it to the data center edge for processing.

The edge data center was connected to the core data center in Santa Clara, CA, which consisted of the Vblock System with Dell EMC Isilon and Hadoop running Dell EMC Analytic Insights Module, while a second data center was co-located in Durham, NC, focused primarily on video surveillance with Milestone, a video surveillance management platform. Both core data centers were used for deeper data exploration and historic data analysis. ESG focused on Dell EMC's ability to leverage and integrate with common cloud platforms for additional data storage, management, and analysis.

Figure 2. Proof of Concept - Edge to Core IoT Environment



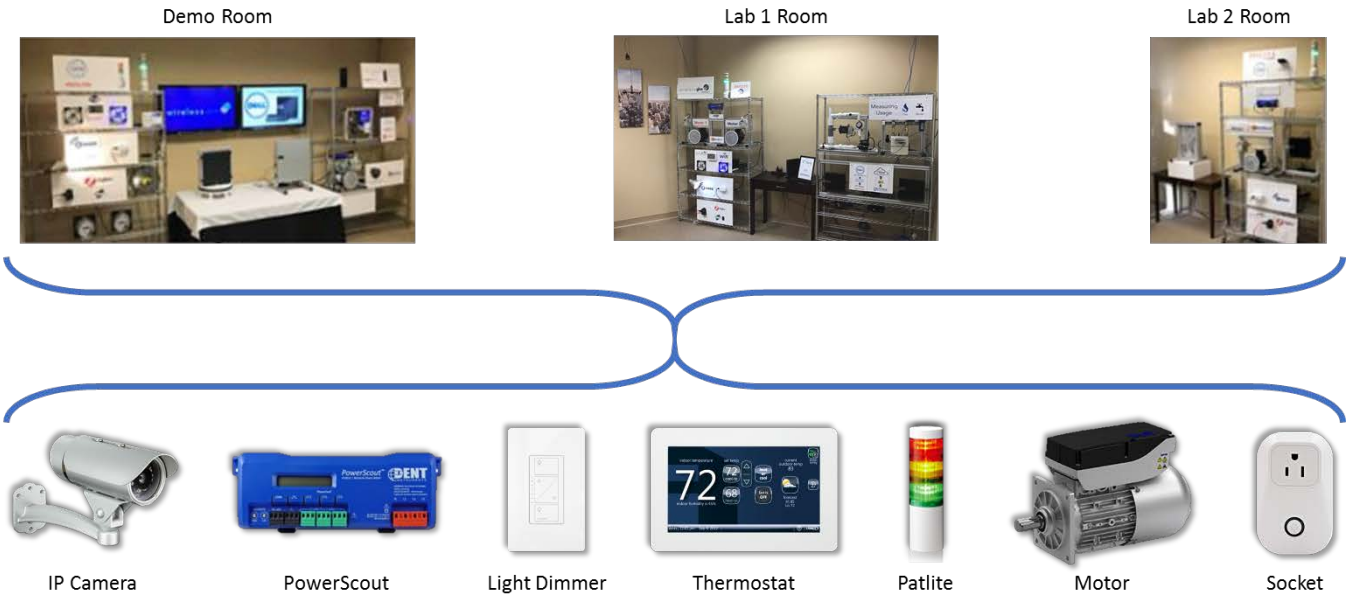
Source: Enterprise Strategy Group, 2017

Use cases and personas were created that leverage the complete environment, including how the edge data centers and core data centers may be used to complete different, though connected, tasks. As shown in Figure 3, a collection of different endpoints was configured and connected to the edge gateway of each room—Demo, Lab 1, and Lab 2—at the edge. Each room contained both off-the-shelf and industrial Internet-connected devices, including IP cameras, PowerScouts, light dimmers, thermostats, Patlites, motors, and sockets. The devices communicate simultaneously across several protocols, including TCP/IP, WiFi, Zigbee, Z-Wave, BACnet, and Modbus. A few important extra notes: The IP cameras were leveraged to not only view each room, but also to record 24 x 7 footage, which then was managed and archived with Milestone; the Patlites, common in the industrial IoT space, help to signal events in a building, with green

meaning everything is fine, while flashing red means something is wrong, often accompanied by sound; and a current transformer (CT) sensor was attached to the motor to monitor data related to metrics such as RPM.

Three use cases were tested, one for each room, with a goal of highlighting the ability to receive and analyze data in real time as an event occurs and from that analysis, generate an alert to act.

Figure 3. Edge Test Rooms and Endpoints



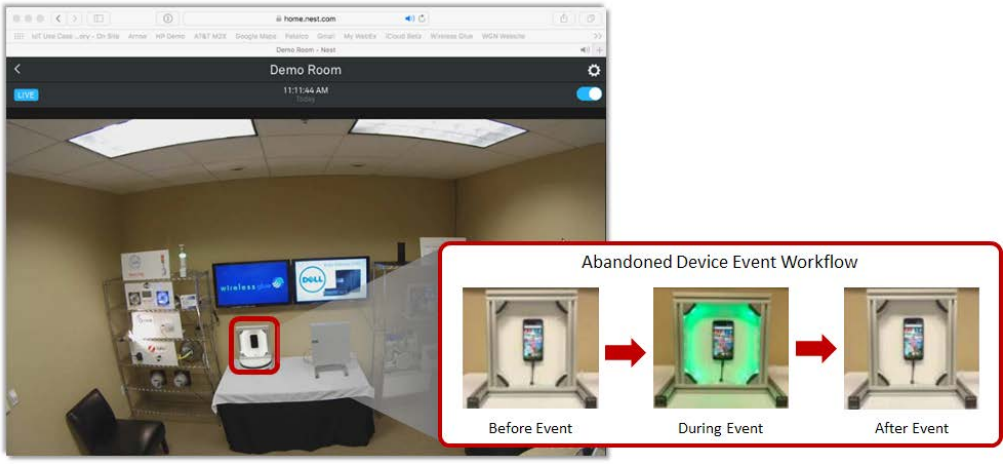
Source: Enterprise Strategy Group, 2017

Use Case 1 – Incident Management—Abandoned Electronic Device

The first use case focused on investigating an abandoned electronic device in a crowded area, such as an airport, and locating it. This represents a scenario where real-time analysis is required to take appropriate action and determine if there is a threat to people and property, or if the item has been lost and can be delivered back to the owner. Once detected, several actions can be taken, like finding the passenger who is the owner of the device before the flight takes off, as a means of ensuring customer satisfaction, sounding an alarm to let everyone know to evacuate the airport, or disabling all equipment around the abandoned device. To accomplish this, actions like notifying security personnel to secure the area and determine if the device is a threat can be taken. The event can also be used to activate crowd control devices to limit foot traffic near where the device was detected. A video management system could also be used for visual verification of the individual who left the device and/or whether security personnel are on the scene to accelerate retrieval of the device.

The test scenario began with the device under control of its owner, the device being activated after being abandoned, the abandoned device being detected, and the device being deactivated once found. Inside the Demo Room, a device was mounted within a casing and surrounded by lights. Before the abandoned device event occurred, the light remained off. During the event, a green light came on, which signified abandonment and was detected by one of the IP surveillance cameras. Once the event completed, the light went off. This process is shown in Figure 5. It should be noted that when the event occurred, all metadata from each of the IoT devices within the room was collected and sent to a centralized surveillance and security system for evaluation to help understand if another device was affected or influenced the abandoned device.

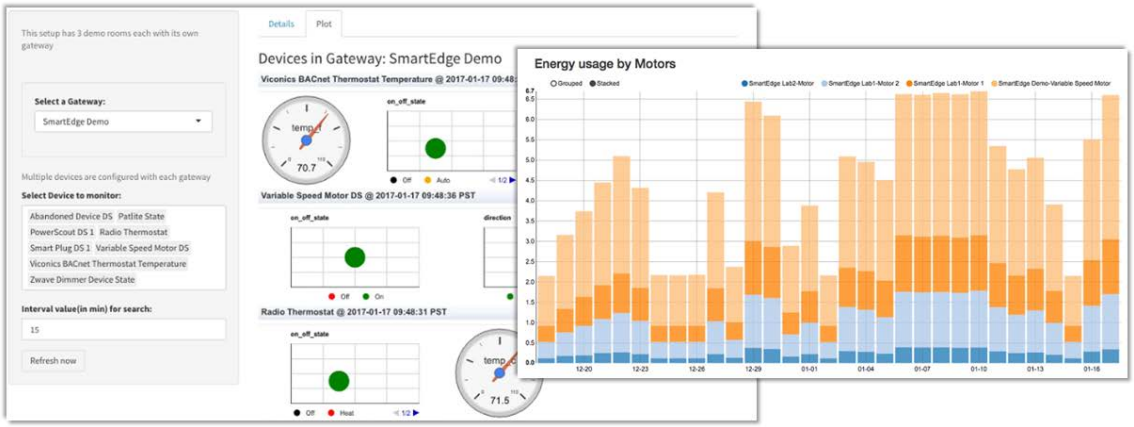
Figure 4. Abandoned Device Event Workflow



Source: Enterprise Strategy Group, 2017

Real-time event data from each device was monitored through a custom user interface. As shown in Figure 5, a dashboard view presented key metrics from custom-selected IoT devices. By selecting a specific device, even more granular details can be seen in an interactive histogram chart. The chart shown in Figure 5 displays energy usage of all the motors when the abandoned device event occurred.

Figure 5. Dashboard and Granular IoT Device Metrics in Real Time



Source: Enterprise Strategy Group, 2017

It is important to follow the flow of data from the device to the edge data center to the core data center and cloud. For the abandoned electronic device scenario, different technologies were leveraged to store and handle event data. Milestone was leveraged to manage all recorded video, MongoDB was leveraged to store unstructured event data from the lost device, while Hadoop received data to eventually process for deeper insights. After the real-time insights were achieved in the edge data center, all data was sent to the two core data centers where Milestone and Hadoop, along with Dell EMC hardware and software, were used to store the data and eventually complete deeper analysis with less sensitivity to an immediate response.

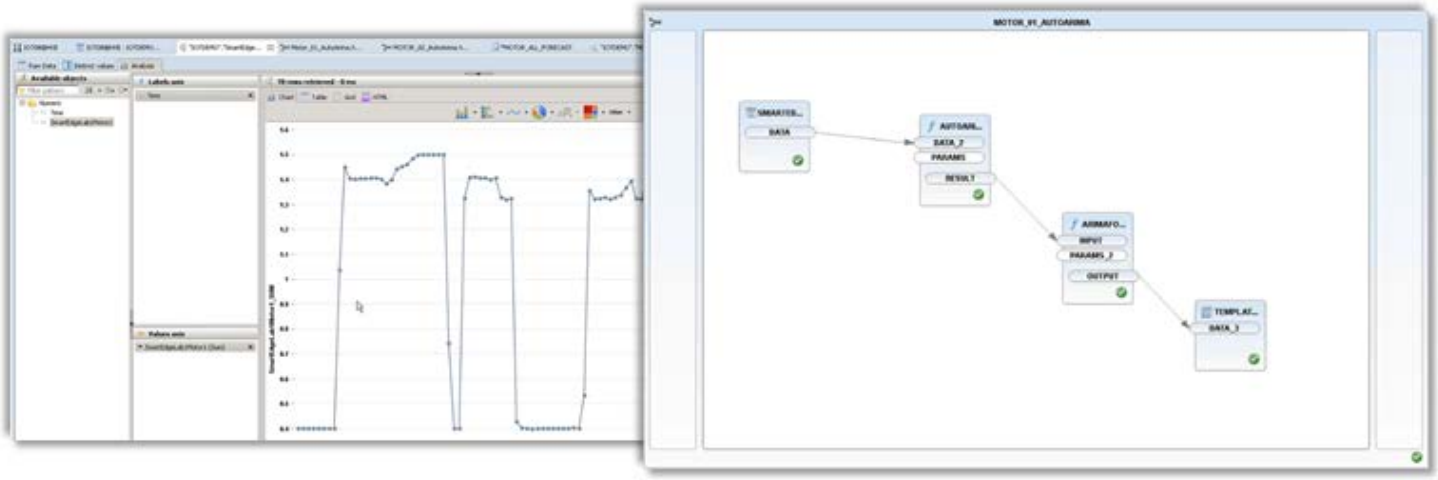
ESG walked through a detailed data workflow demonstration where data was taken from the edge devices and eventually placed into SAP HANA Express Edition,[2] an in-memory data management and application computing platform. The complete

[2] SAP HANA Express Edition was used for this ESG Lab Review to demonstrate functionality. To use SAP HANA for production, please use a certified and supported Dell EMC hardware listed on the SAP Hardware directory.
Certified and Supported SAP HANA Hardware Directory
Dell/Dell EMC Certified Enterprise Storage for SAP HANA

process consists of taking data inputs from the edge locations, preparing the data, building a model, building consumable views, and then presenting them via SAP Lumira. Data scientists work at the data preparation, model building, and calculation view building phases, while analysts leverage SAP Lumira to complete tasks such as reviewing the dashboards or generating requests based on analysis.

From within SAP HANA Studio, a view of the motor data from Lab 1 was shown. Once the data resided in the system, data preparation was completed. Using a prebuilt analytic algorithm, the motor data was converted to a time series. This formatting of the data made it easier for the model to consume it. Next, a model was built using SAP HANA's drag and drop data modeler. Using the ARIMA time series analysis, predictive analysis of the received motor data was carried out. The data preparation and modeling phases from within SAP HANA Studio are shown in Figure 6.

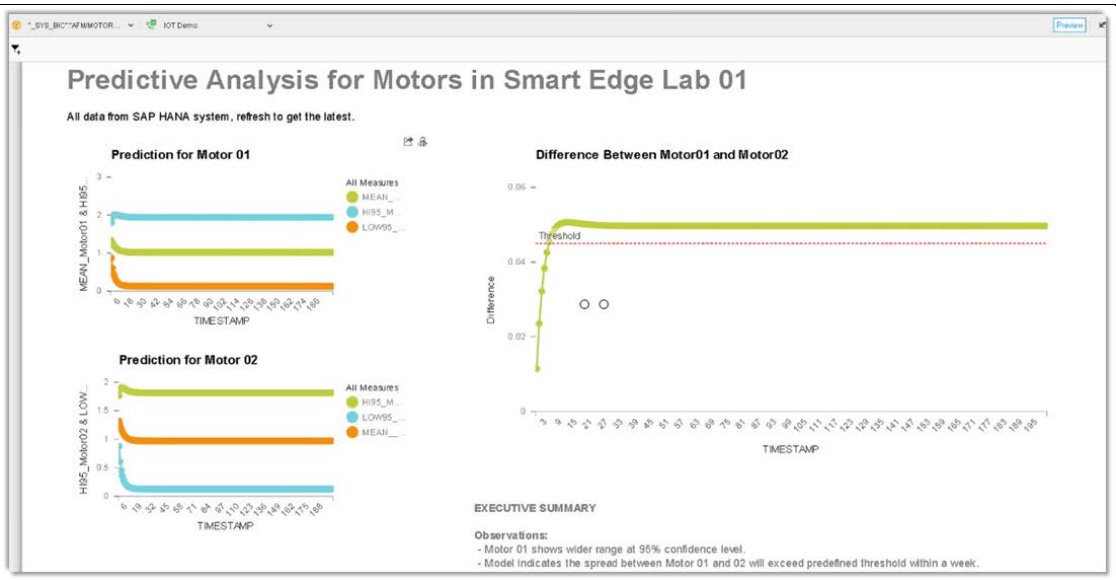
Figure 6. Data Preparation and Modeling with SAP HANA



Source: Enterprise Strategy Group, 2017

To consume the results from the analytical model in SAP Lumira, a calculation view was created. The results from both motors were linked together by timestamp and ESG quickly viewed the resulting data, which showed 200 iterations of combined results. Next, the role shifted from the data scientist to the business analyst. As shown in Figure 7, ESG viewed an SAP Lumira dashboard with the results. Individual and combined results are both displayed. The first motor showed a wider range at a 95% confidence interval and when the data was combined, the predictive model showed that the difference between the motors exceeded a predefined threshold. With both motors being in the same exact environment, the difference between motors indicates there is a problem. This analysis could then trigger an investigation or the creation of a service ticket to complete maintenance on the potentially faulty motor or possibly even deploy a new motor as a preventive measure. ESG also sees the potential for organizations to better manage supplier performance based on the quality and reliability of parts collected directly from where they are deployed. For example, enterprise data, including supplier master data and transaction data for pricing, timestamps, specific locations, etc., can be combined with IoT data to provide higher visibility and granularity to manage partner business and internal processes.

Figure 7. SAP Lumira Dashboard



Source: Enterprise Strategy Group, 2017

Why This Matters

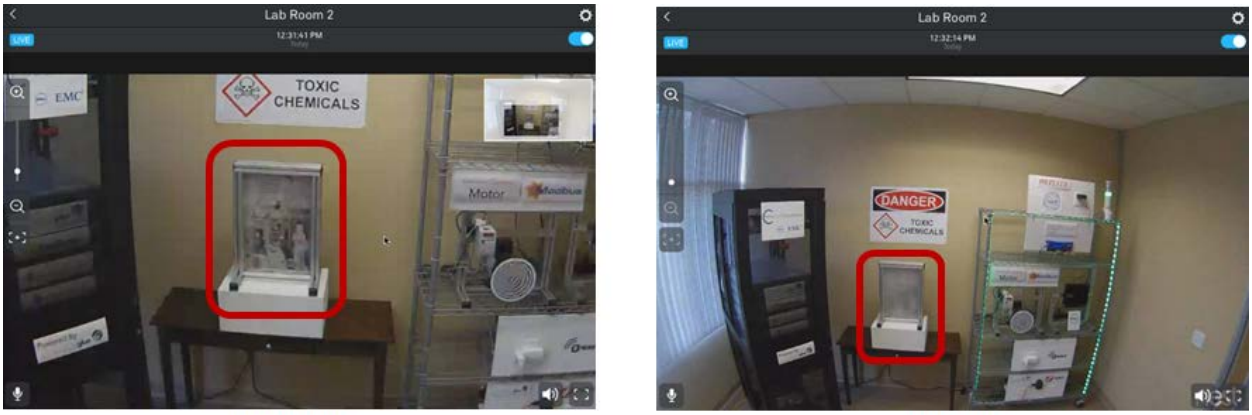
Incident management surrounding the abandoned electronic device scenario represents a way to leverage real-time and historic IoT analytics on Dell EMC hardware with Dell IoT Edge Gateways to rapidly respond to an event, and move data offsite for deeper analysis using SAP HANA. Business benefits for this approach are wide—from enhancing customer experiences, through responding to potential criminal incidents, to initiating deeper investigation with a complete audit trail for regulatory compliance and governance needs. Aside from the obvious benefits of creating a safer work environment through constant surveillance, event detection, alerting, and remediation, additional return-on-investment benefits are achieved throughout the audit process. Faster initial reporting for compliance and ongoing data retrieval during potential litigation enable organizations to rapidly respond to requests efficiently and effectively. And with SAP HANA, ESG witnessed the ability to apply predictive analytics to IoT device data and visualized the data with SAP Lumira to alert organizations to the need for proactive maintenance to help avoid issues.

Use Case 2 – Managing Safety, Productivity, and Health

The second use case focused on the safety of a work environment. This IoT scenario highlights a way to leverage Wireless Glue and Dell EMC to constantly monitor air quality and detect when a contaminant is present. Again, the scenario consisted of four steps: an IP camera is viewing a factory floor; an air quality event occurs; once detected, a light begins flashing; and finally, the air quality event is deactivated. Milestone was leveraged in this test for video monitoring and management in the edge data center, which notifies Wireless Glue when the event begins and ends. At the start of the event, Wireless Glue gathers all metadata from each device in the room and, based on real-time analysis, notifies the devices that an air quality event has occurred. Wireless Glue then turned on an emergency signal light signifying that people should evacuate the building. Once the event ended, Wireless Glue packages everything (IoT device metadata, video management system metadata, and video clip of the duration of the event), and sends the package to the core data centers for deeper analysis.

As shown in Figure 8, ESG viewed the event workflow in the Lab 2 Room through an IP camera. Before the event occurred, an image can clearly be seen. Once the event is initiated, the picture is frosted. The event was immediately detected by Wireless Glue in the edge data center and an alert was sent to one of the IoT devices, causing the green lights to come on around the shelf.

Figure 8. Safety, Productivity, and Health Event



Before Event During Event

Source: Enterprise Strategy Group, 2017

For a scenario like this, it is important to understand how different personas within an organization would leverage the environment and the device data as it is collected and dispersed. Four personas were identified: a facility manager, a data scientist, a security manager, and a digital transformation officer tasked with modernizing the organization and its processes and workflows.

The *facility manager* is responsible for maintaining the safety and efficiency of the facility. Therefore access to real-time data is essential. In this case, based on analysis done at the edge data center, the facility manager can quickly assess the severity of an event and order an evacuation, if necessary. Shortly after the event, that data would then be leveraged by the facility manager from the core data center to try and understand what caused the event to occur and what improvements should be made to eliminate such an event in the future.

The *data scientist* would be responsible for using the collected device data to understand patterns that may have caused the event to occur. Did a flaw exist in a current process? Did a different device cause the problem? How could a potential change affect the outcome in the future? Real-time data analysis is not a requirement, but historical data is essential to understand how the data is connected and what the data means.

The *security manager's* responsibility is to investigate, identify, and mitigate the threat. Did a cyber-attack cause the air quality event to occur? Was faulty equipment to blame? This persona requires both real-time and historic data analysis. When the action occurs, the security manager is notified immediately that an event occurred. Upon the event ending, she must investigate what caused it and how to mitigate a future incident.

Finally, the *digital transformation officer* is tasked with vetting and proposing new business ideas, models, processes, and workflows. He works entirely out of the core data centers and leverages all historical data to evaluate the impact of new technologies on existing technologies and their feasibility within the existing business.

Use Case 3 – Investigation and Evidence Management with Video Surveillance

With hundreds of thousands of drones deployed on a regular basis, the third use case represented a video surveillance scenario where a drone enters a no-fly zone and a rapid response is required to act. The four steps of this test were:

- Step 1—No event.
- Step 2—Drone activated.
- Step 3—Drone detected by camera.
- Step 4—Drone deactivated.

Again, Milestone was leveraged for video surveillance, which requires detecting the drone and notifying Wireless Glue. Wireless Glue then collects all metadata from the IoT devices and notifies the devices a drone detection has occurred. In this scenario, edge rules are applied to two devices once the drone is detected: the smart switch turns on a spotlight on the drone, while the Patlite changes colors from green to red. The environment before the event and during the event are shown in Figure 9. Note that during the event, ESG witnessed the light come on over the drone, while the Patlite changed to red.

Figure 9. Surveillance Event

Before Event During Event

Source: Enterprise Strategy Group, 2017

Multiple requirements must be met throughout this test: The drone's flight path must be detected, police must be alerted, the pilot must be found, and video evidence of the drone intrusion must be recorded and presented to the proper authorities. This requires additional personas to leverage various components across the IoT infrastructure to properly complete their specific tasks. As an example, an *investigations manager* who may be responsible for speeding up investigations would quickly get involved in incident response based on real-time analysis completed at the edge data center, while a *law enforcement relations manager* would partner with local and federal agencies to help resolve the incident not only while it is occurring, but also post mortem to help with mitigation.

Why This Matters

ESG confirmed that combining the flexibility of deploying Dell Technologies hardware from edge to core with Wireless Glue or other software solutions, organizations can build a comprehensive infrastructure to handle real-time and historical analytics for IoT. Whether monitoring air quality on a factory floor or surveilling no-fly zones for drone intrusions, ESG witnessed rapid responses in real time to alerts and resulting actions based on occurring events. In this case, Wireless Glue not only received data from Milestone and sent appropriate data back to affected IoT devices, but information was also packaged and sent to the core data center for analysis with the Dell EMC Analytic Insights Module on a Vblock System with Dell EMC Isilon. Analytic Insight Module is also available on other hardware such as VxRail and Dell EMC Isilon systems. ESG recommends that customers look at the growing variety of partner solutions that run on Dell EMC products and Dell IoT Gateways based on their needs.

The Bigger Truth

Bringing IoT into an organization's digital transformation can be a significant multiplier for the business, monetizing the existing ecosystem to drive new revenue streams, and creating a sustainable competitive advantage that exploits core strengths—whether they are related to technology, brand, ecosystem, or geographical reach. What is needed to succeed in an IoT-enabled digital transformation initiative is a robust, versatile, and open infrastructure with fit-for-purpose solutions to choose from.

This approach serves as a foundation to deliver against digital transformation or IoT initiative requirements, from starting a new project to layering a variety of business use cases that can scale across the enterprise, while breaking down silos. Edge processing capabilities are important for local and low-latency response in seconds and minutes. Edge on-premises computing empowers organizations to choose the specific data to analyze locally, save, and send to the core via cloud, internal networks or gateways, especially video files. Systems in the core data centers can perform big data and analytics, powered by AI and deep learning, with an enterprise-wide repository of data spanning from weeks to years of record. Organizations can also create cross-industry modules with which to build new use cases based on existing modules as business priorities evolve. This can also empower businesses to move beyond the traditional boundaries of the current industries they are playing in.

ESG Lab validated the ability of Dell EMC to create a smarter environment through constant surveillance, event detection, alerting, and remediation; and provide a complete audit trail for regulatory compliance. Additional benefits are realized throughout the audit process, with fast initial reporting for compliance and ongoing data retrieval during potential litigation, which enables organizations to rapidly respond to requests efficiently and effectively. ESG Lab also witnessed the ability to apply predictive analytics to IoT device data using SAP HANA and visualize the data with SAP Lumira to alert organizations to the need for proactive maintenance to help avoid issues.

ESG confirmed that, by combining the speed of Dell EMC hardware with a target set of partner solutions, organizations can achieve a comprehensive infrastructure to handle real-time edge analytics for IoT. ESG observed rapid responses in real time to alerts and resulting actions based on events occurring in real time. Wireless Glue not only received data from Milestone and sent appropriate data back to affected IoT devices, but also packaged up data and sent it to the core data center for analysis with the Dell EMC Analytic Insights Module on a Vblock System with Dell EMC Isilon.

Dell EMC has a broad infrastructure portfolio that can enable organizations to create a scalable environment and build applications with confidence to transform business in the networked economy. Dell Technologies and its partner ecosystem significantly extend the reach of Dell EMC from the data center core to the operational edge across private and public clouds for a true hybrid multi-cloud implementation. Thanks to cloud deployment, application development, and crowd-sourced business models, the technological effort for transforming business that used to take years and months is now taking weeks and days. If your organization is working toward rapidly turning new ideas into solutions and business results, or even inventing new business models through digital transformation exploiting IoT, ESG Lab recommends taking a serious look at Dell EMC's outcome-driven solutions.