machnation

MIT-E

Losant IoT
Vendor Excerpt

2018-09-10

Table of Contents

This report excerpt contains results for:

LOSANT

The full MIT-E report contains results for:

Altizon (Datonis)

Amazon (AWS IoT)

Bosch (Bosch IoT Suite)

ClearBlade (ClearBlade)

GE (Predix)

Google (Google IoT Core)

IBM (Watson IoT)

Litmus Automation (Loop Cloud and Loop Edge)

Microsoft (Microsoft IoT)

Sierra Wireless (AirVantage IoT Platform)

SIteWhere (SiteWhere CE)

Software AG (Cumulocity IoT)

ThingsBoard (ThingsBoard)

The full MIT-E report is available at machnation.com/mite

What is MIT-E?

MIT-E is an IoT platform test and benchmarking lab run by MachNation, the world's leading research firm for IoT platforms and middleware. In MIT-E, MachNation:

- performs a set of common hands-on tasks – operator and developer workflows
- scores these tasks based on the time-to-complete each task, ease-of-completion, completeness of task, and sophistication metrics
- compiles task scores in a MIT-E report

The results from MIT-E help enterprises compare IoT platform capabilities and usability. MachNation makes the results from MIT-E available to enterprises to help guide IoT platform purchase decisions. The results provide enterprises an apples-to-apples comparison of IoT platforms across relevant hands-on task metrics.

Using MIT-E, MachNation also provides additional services to enterprises including:

- Private testing of in-house built IoT platforms
- IoT platform RFx and vendor selection support
- IoT platform due diligence for acquisitions
- Co-development of use-case specific, enterprise, IoT solution architectures

Please contact MachNation for more information.

Legal Disclaimer

All contents of this report and all other MachNation IoT Test Environment (MIT-E) reports are and remain the intellectual property of MachNation. This report may not be reposted without the written permission of MachNation, such permission to be granted or denied at MachNation's sole discretion.

Methodology

C Completeness of Task

Measure of how completely the evaluated product executed the task requirements as defined in the task description.

SCORE RANGE	0 to 3
SCORE 0	Not completed or functionality not available in product (<50% completion)
SCORE 1	Partially completed task (50% to 74% completion)
SCORE 2	Mostly completed task (75% to 99% completion)
SCORE 3	Fully completed task (100% completion)

S Sophistication of Solution

Measure of how effectively and with what level of sophistication the evaluated product executed the requirements as defined in the task description.

SCORE RANGE	0 to 3
SCORE 0	Very unsophisticated solution with regard to task execution (e.g., unclear documentation, poor UI, bad design)
SCORE 1	Somewhat unsophisticated solution with regard to task execution (e.g., unclear documentation, UI, design)
SCORE 2	Somewhat sophisticated solution with regard to task execution (e.g., good documentation, UI, design)
SCORE 3	Very sophisticated solution with regard to task execution (e.g., excellent documentation, UI, design)

E Ease of Task Completion

Calculated statistic describing the relative percentile of a single Timing of Task measure for a single given task, relative to the aggregate Timing of Task measures for all tested products and vendors for the same given Task.

SCORE RANGE	0 to 3
SCORE 0	Bottom 25% (Slowest) of all Timing of Task measures for the given Task
SCORE 1	Bottom 50% (Slow) of all Timing of Task measure for the given Task
SCORE 2	Top 50% (Fast) of all Timing of Task measures for the given Task
SCORE 3	Top 25% (Fastest) of all Timing of Task measures for the given Task

T Timing of Task

Measure of how long the task execution took to complete in minutes. Timing values only assigned to tasks that were "fully completed" as per Completeness of Task criteria. Does not include timing of: initial familiarization with product, research of items/documentation/elements not directly related to the task description, preliminary configuration/ setup not directly related to task description, or or time spent waiting on vendor responses to inquiries.

SCORE RANGE	0 to infinite
TIMING	Total time to execute task in minutes
DNF	Did not finish (DNF), task could not be completed

Losant IoT

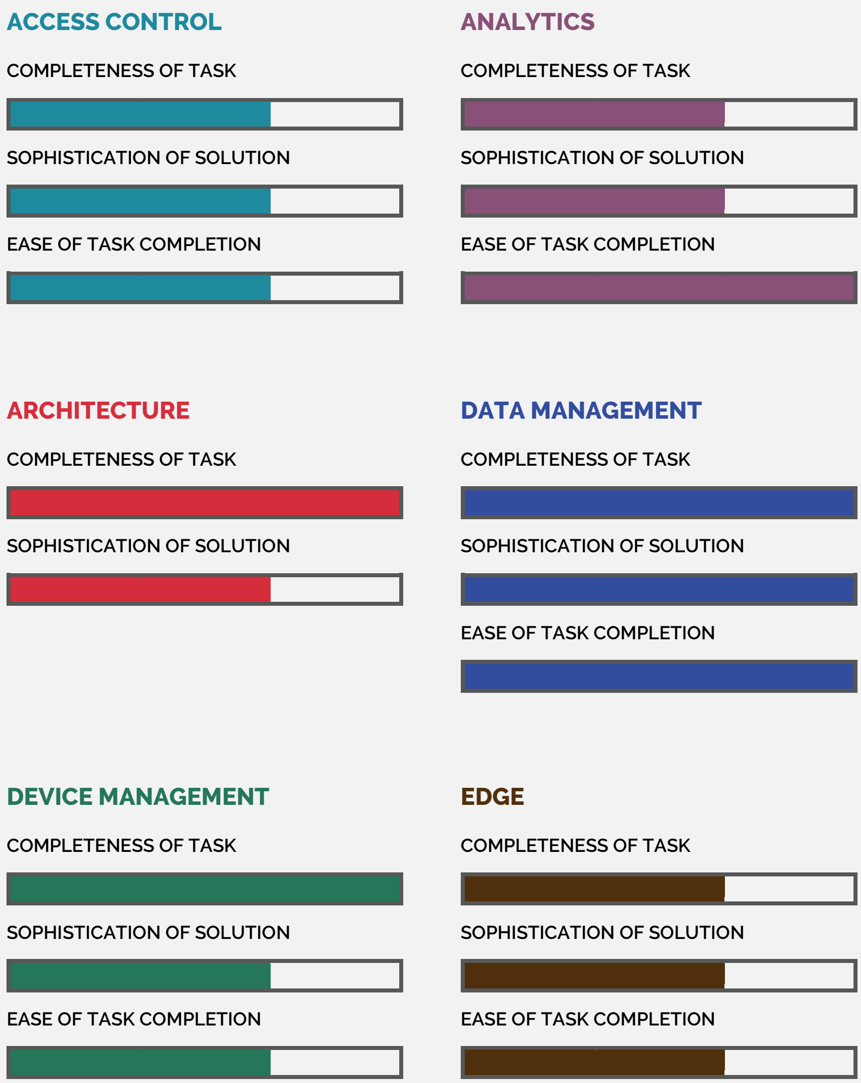
Product Name

Losant IoT

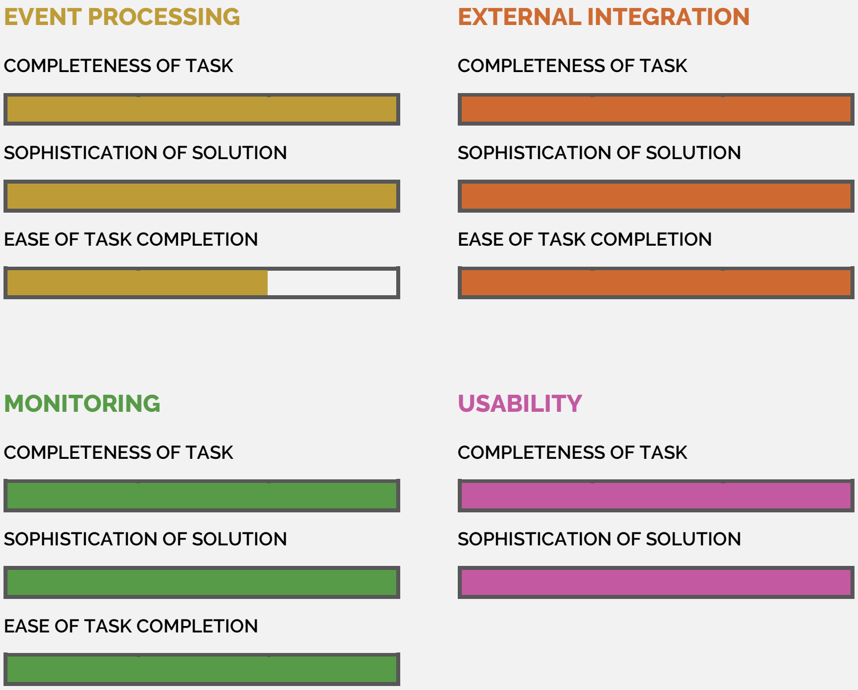
Product Version

2018.08.13

Losant IoT Summary



Losant IoT Summary



Access Control

Losant IoT

SUMMARY

Access control is an area of mixed strengths and weaknesses for the Losant IoT platform. Many of the access control aspects of the platform exhibit strong usability, good API and UI integration, and easy UI-driven flows for user, device, and external service authorization management. While these workflows enable efficient operator control over basic asset authentication and authorization (including many wizard-driven interfaces), Losant IoT lacks advanced features such as per-resource and per-user granular access control, supporting only limited user roles such as "administrator" or "editor". Also lacking from the platform is support for certificate-based device authentication. Multi-factor authentication (MFA) is supported out-of-the-box for users, requiring only minimal configuration effort, however, support for external federated authentication providers is not currently supported. While some shortcomings such as PKI-only device authentication can be overlooked due to the strength of implementation offered, the lack of more granular access control mechanisms, including the inability to flexibly apply multi-tenant and customer-of-customer access control policies does detract from an otherwise highly usable solution.

Access Control

Losant IoT

RESULTS

C = COMPLETENESS **S = SOPHISTICATION** **E = EASE OF TASK COMPLETION** **T= TIMING OF TASK**

	ACCESS CONTROL	C	S	E	T
C-01-01	Authorize device credentials	3	3	3	1
C-01-02	Authorize bulk device credentials	3	2	2	3
C-01-03	Configure certificate-based device credentials	0	0	DnF	DnF
C-01-04	Create subordinate user or organization in hierarchy	2	1	DnF	DnF
C-01-05	Restrict permissions of subordinate user or organization	2	1	DnF	DnF
C-01-06	Create a new user	3	2	3	1
C-01-07	Create bulk new users	3	2	2	4
C-01-08	Configure user multi-factor authentication (MFA)	3	3	3	1
C-01-09	Configure federated authentication service	0	0	DnF	DnF

Analytics

Losant IoT

SUMMARY

Analytics is an area of overall strength for the Losant IoT platform, however, this competency is limited to the domain of descriptive or operational analytics. More advanced analytic methods, such as predictive model creation, model optimization, and machine learning are not currently provided through Losant's platform. The descriptive analytic methods available, however, are highly effective and enable seamless integration between platform-ingested IoT data and the on-platform dashboarding and data explorer components. Both the dashboarding components and the data explorer provide filtered views which support multiple devices and multiple observed metrics as well as support for a variety of aggregation types. This enables platform operators to quickly assess the real-time and historical state of devices and collected observations through graphical views. In addition, Losant provides an effective method for quickly exporting aggregated data views into downloadable CSV files, useful for external analytics tools. Finally, the external integrations provided by the Losant IoT platform enable easy integration of external data analytics tools with the platform, enabling customers to leverage their own chosen off-platform analytic solutions.

Analytics

Losant IoT

RESULTS

C = COMPLETENESS **S = SOPHISTICATION** **E = EASE OF TASK COMPLETION** **T= TIMING OF TASK**

ANALYTICS		C	S	E	T
A-01-01	Configure on-platform analytics service for live streaming data	3	3	3	1
A-01-02	Configure on-platform analytics service for stored/historical data	3	3	3	1
A-01-03	Configure platform for live/streaming external analytics service integration	3	3	3	9
A-01-04	Export on-platform data for external/off-platform analytics service	3	3	3	2
A-02-01	Build a single observation, on-platform analytics report	3	3	3	3
A-02-02	Build a multi-observation, on-platform analytics report	3	3	3	4
A-03-01	Evaluate on-platform descriptive analytics capabilities	3	3	N/A	N/A
A-03-02	Evaluate on-platform data lake / big-data storage capabilities	3	2	N/A	N/A
A-04-01	Evaluate on-platform predictive analytic model building	0	0	N/A	N/A
A-04-02	Evaluate on-platform predictive analytic model operation	0	0	N/A	N/A
A-05-01	Evaluate on-platform prescriptive analytic model capabilities	0	0	N/A	N/A
A-06-01	Evaluate on-platform machine learning (ML) model creation and training process	0	0	N/A	N/A
A-06-02	Evaluate on-platform machine learning (ML) model evaluation and execution capabilities	0	0	N/A	N/A
A-06-03	Evaluate on-platform machine learning (ML) automated model creation capabilities	0	0	N/A	N/A
A-06-04	Evaluate platform support for machine learning (ML) hardware acceleration	0	0	N/A	N/A
C-04-01	Configure rule/alert associated with device status	3	3	2	8
C-04-02	Configure rule/alert associated with sensor data configured range exceeded	3	3	2	4
C-04-03	Configure time/schedule based rule	3	3	3	3
C-04-04	Configure device action based on device state change	3	3	2	9
C-04-05	Configure data action based on data configured range exceeded	3	3	3	6
C-04-06	Configure rule/alert associated with sensor data based on a real-time, group-based, moving average	3	3	2	6
C-04-07	Configure rule/alert associated with sensor data based on anomaly detection	3	1	3	8

Architecture

Losant IoT

SUMMARY

Platform architecture is well-designed and well-implemented within the Losant IoT platform. The platform is provided as a PaaS hosted within the Google Cloud. Although on-premises deployments are available for enterprises, there is no immediately available on-premises distribution of the platform available. Taken comprehensively, Losant IoT is a developer-centric platform that also addresses many of the needs of larger enterprises, and as such, it is well-suited to trial, proof-of-concept, and larger at-scale IoT deployments. While the lack of productized support for legacy industrial devices and lack of connectivity management integration will give pause to some, overall it is a well-designed platform with extremely well-executed northbound external integration and complex event processing capabilities. When combined with off-platform services for analytics and after initial implementation of the device management components, Losant IoT provides a very strong horizontal IoT solution that can cater to large and small customers.

Architecture

Losant IoT

RESULTS

C = COMPLETENESS **S = SOPHISTICATION** **E = EASE OF TASK COMPLETION** **T= TIMING OF TASK**

ARCHITECTURE		C	S	E	T
C-06-01	Evaluate overall cogency and quality	3	3	N/A	N/A
C-06-02	Evaluate overall security model and implementation	2	2	N/A	N/A
C-06-03	Evaluate platform scaling methodology	3	2	N/A	N/A
C-06-04	Evaluate platform deployment model	3	1	N/A	N/A
C-06-05	Evaluate overall productization	3	3	N/A	N/A

Data Management

Losant IoT

SUMMARY

Data management is overall an area of strength for the Losant IoT platform, with only limited shortcomings. As with many other purpose-built IoT solutions, an on-platform time-series data historian is provided out-of-the-box, enabling immediate storage of ingested IoT observations without the need to separately configure and manage a data storage layer. In addition, Losant provides a Data Table service that allows table-based storage of any IoT-related data while also exposing this stored data natively to Losant's complex event processing service called Workflows. Both UI and API methods are well developed, providing create, read, update, and delete (CRUD) access to both ingested IoT data and the Data Table service via API, and read-only access to both services via UIs. In conjunction with Workflows, Losant IoT enables a variety of data normalization, extract-transform-load (ETL), and other common data management tasks. Perhaps the biggest weakness of the Losant platform is the lack of flexibility for customers to leverage their own preferred underlying database engine for on-platform data, however, productized connectors to support ingest/egress for both MongoDB and Redis are provided, as well as native on-platform support for Google's Pub/Sub service.

Data Management

Losant IoT

RESULTS

C = COMPLETENESS S = SOPHISTICATION E = EASE OF TASK COMPLETION T= TIMING OF TASK

DATA MANAGEMENT		C	S	E	T
C-02-01	Forward live sensor data to external endpoint	3	3	2	6
C-02-02	Configure persistent on-platform data storage	3	2	3	1
C-02-03	Compute aggregate stats for single data point	3	3	3	1
C-02-04	Compute aggregate statistics for multiple data points	3	3	3	2
C-02-05	Delete a single historical sensor data point	3	3	3	1
C-02-06	View historical sensor data for a single device	3	3	3	1
C-02-07	View historical sensor data for a group of devices	3	3	3	1

Device Management

Losant IoT

SUMMARY

Device management is an area of relative strength for the Losant IoT platform, however, like many large public cloud or developer-centric IoT vendors, the device management capabilities are not well-productized, requiring significant customer development efforts to fully implement. However, once fully implemented, Losant IoT offers a mostly complete device management solution, providing support for edge computing devices, gateways (aggregation devices), and unmanaged assets connected through MQTT or the RESTful API. While the platform does not support firmware or software management out-of-the-box without customer- and device-specific implementations, Losant does provide an on-platform repository that can be used to help facilitate firmware over-the-air (FOTA) updates. Managed device status and device monitoring all well-provided within the platform UI. In addition, the API supports all provided device management functionality. Losant IoT does not currently support the LWM2M industry-standard device management protocol nor does it provide a programmatic system for staged software or firmware deployments. In addition, Losant does not provide out-of-the-box integration or support for connectivity management solutions. Such oversights are particularly important for cellular and LPWAN integrations, adding additional cost and complexity for customers. Although the platform requires customer development efforts to implement all offered capabilities, Losant IoT provides an overall strong framework for device management.

Device Management

Losant IoT

RESULTS

C = COMPLETENESS S = SOPHISTICATION E = EASE OF TASK COMPLETION T= TIMING OF TASK

DEVICE MANAGEMENT		C	S	E	T
C-03-01	Monitor historical network status	3	0	3	1
C-03-02	Monitor current network status	3	0	3	1
C-03-03	Configure/compile device agent for a device	3	3	3	2
C-03-04	Add new unmanaged logical device to platform	3	3	3	2
C-03-05	Deploy device and establish uni-directional communication	3	2	3	2
C-03-06	Add new managed logical device to platform	3	3	3	2
C-03-07	Deploy device agent and establish bi-directional communication	3	3	3	6
C-03-08	Configure customer-defined metadata parameter	3	3	3	1
C-03-09	Assign single device to a group	3	1	3	2
C-03-10	Obtain diagnostic log for a single device	3	3	2	2
C-03-11	Obtain diagnostic log for multiple devices	3	3	2	5
C-03-12	Obtain audit and/or config logs for the platform	3	3	2	4
C-03-13	Reboot remote device	2	3	DnF	DnF
C-03-14	Push firmware to a single device	1	2	DnF	DnF
C-03-15	Push software to a single device	2	2	DnF	DnF
C-03-16	Update/create firmware image on the platform repository	3	2	3	1
C-03-17	Remotely update device parameter for a single device	3	3	3	1
C-03-18	Remotely trigger command for a single device	3	3	3	2
C-03-19	Remove a single device from the platform	3	2	3	1

Edge

Losant IoT

SUMMARY

Edge capabilities are an area of mixed strengths for the Losant IoT platform. the edge and gateway agent is well designed and packaged as a Docker container, enabling easy distribution and providing support for both x86 and ARM platforms. However, it lacks many of the on-edge features found in more-developed platforms. On-edge workflows, which support nearly all of the excellent on-platform workflow capabilities, are well managed from within the platform interfaces, including workflow versioning and workflow deployment to edge devices. However, as of the current release, Losant's workflow service is the only method for deploying application logic from the cloud to the edge. Management of additional Docker containers or other packaged applications is not currently supported out-of-the-box. In addition, Losant IoT expects customers to implement their own protocol adapters: other than Modbus, no other industrial or legacy asset communication protocols are supported including lack of productized support for BLE. This deficiency, combined with a lack of support for connectivity management solutions and on-edge UI elements, forces customers to develop many of their own components to deploy a fully functioning edge solution. Furthermore, Losant's IoT Edge Compute agent lacks support for on-edge or on-premises SQL databases, one of the more common integration requirements in brownfield edge deployments. Management of deployed edge devices from within the platform is efficient and logically implemented, supporting both gateway device and full edge-computing devices. One last feature that is lacking is the ability to leverage a deployed edge or gateway device as an MQTT broker for other on-premises IoT devices. Devices can report upstream to the cloud/platform through the gateway, but this must be developed and implemented by the customers themselves as a productized method is currently absent. Overall, Losant IoT provides an excellent solution for extending workflows and complex event processing capabilities to edge devices, but many other critical features are left to customers to implement at their own expense and complication. Unfortunately, this task is made more difficult by the lack of an openly available SDK for the on-edge or on-gateway containerized agent.

Edge

Losant IoT

RESULTS **C = COMPLETENESS** **S = SOPHISTICATION** **E = EASE OF TASK COMPLETION** **T= TIMING OF TASK**

EDGE		C	S	E	T
E-01-01	Evaluate southbound protocol support	2	1	N/A	N/A
E-01-02	Evaluate edge-to-cloud connectivity support	2	1	N/A	N/A
E-01-03	Evaluate edge autonomous capabilities (store/forward)	3	1	N/A	N/A
E-01-04	Evaluate edge autonomous capabilities (edge event processing)	3	2	N/A	N/A
E-01-05	Evaluate on-edge security model	2	2	N/A	N/A
E-02-01	Configure edge for observation collection from a downstream sensor	3	1	2	11
E-02-02	Configure edge for northbound data flow of collected observations	3	3	3	3
E-02-03	Configure on-edge ephemeral data storage for observations	3	3	3	1
E-02-04	Configure on-edge persistent data storage for collected observations	3	3	3	2
E-02-05	Configure on-edge connectivity to on-premises data store	3	2	3	5
E-03-01	Configure edge agent	3	3	3	2
E-03-02	Deploy edge agent and establish bi-directional platform connectivity	3	3	3	6
E-04-01	Configure on-platform rule/alert for edge device status	3	3	3	6
E-04-02	Configure on-edge rule/alert for edge-connected device status	3	2	3	9
E-04-03	Configure on-edge rule/alert for edge-connected sensor data range exceeded	3	2	3	8
E-04-04	Configure on-edge data normalization/transformation capability	3	3	2	9
E-05-01	Evaluate on-edge analytics software capabilities and integration	1	1	N/A	N/A
E-05-02	Evaluate on-edge analytics hardware acceleration capabilities	0	0	N/A	N/A
E-06-01	Push configuration from platform to edge device	3	3	3	2
E-06-02	Deploy firmware package to edge	1	1	DnF	DnF
E-06-03	Prepare firmware package for edge deployment	1	0	DnF	DnF
E-06-04	Deploy application to edge	3	3	3	2
E-06-05	Prepare an application for edge deployment	3	2	3	3
E-07-01	Create an on-edge dashboard with edge-connected device data	0	0	DnF	DnF
E-07-02	Create an on-edge dashboard with edge-connected device status	0	0	DnF	DnF
E-07-03	View sensor data on-edge for an edge-connected device	2	1	DnF	DnF
E-07-04	View sensor data on-edge for multiple edge-connected devices	2	1	DnF	DnF
E-08-01	View edge health/status from on-platform monitoring solution	3	3	3	1
E-08-02	View data observations from on-platform monitoring solution	2	1	N/A	N/A

Event Processing

Losant IoT

SUMMARY

Complex event processing, both in-cloud and on-edge, is an area of distinct strength for the Losant IoT platform. With support for a wide variety of input and output data sources, a deep library of data manipulation tools, strong integration with on-platform data stores, and a highly intuitive yet very powerful visual workflow builder, Losant's event processing framework is both usable enough to appeal to platform operators, but powerful enough to support nearly any IoT event processing requirement. While the platform lacks a more traditional condition/action rules-builder interface, the addition of workflow elements like the "gauge query" block enable easy creation of complex rules, supporting fixed or rolling time windows and providing easy access to both single- and multi-device data aggregation capabilities. Custom Javascript code is also supported, enabling even more extensibility for complex actions, while a debugger provided in the interface helps to resolve issues during development. Finally, flexible deployment of workflows to edge computing devices enables event processing to occur on-edge without requiring constant northbound platform connectivity. Taken together, these workflow capabilities enable customers to implement nearly any real-time or historical IoT event processing requirements in a well-managed and logically consistent manner.

Event Processing

Losant IoT

RESULTS

C = COMPLETENESS **S = SOPHISTICATION** **E = EASE OF TASK COMPLETION** **T= TIMING OF TASK**

EVENT PROCESSING		C	S	E	T
C-04-01	Configure rule/alert associated with device status	3	3	2	8
C-04-02	Configure rule/alert associated with sensor data configured range exceeded	3	3	2	4
C-04-03	Configure time/schedule based rule	3	3	3	3
C-04-04	Configure device action based on device state change	3	3	2	9
C-04-05	Configure data action based on data configured range exceeded	3	3	3	6

External Integration

Losant IoT

SUMMARY

In conjunction with workflows, the Losant IoT platform offers a very strong solution for northbound external integration, although southbound gateway-to-asset support is lacking. Losant enables productized, northbound integrations with support for a variety of Google Cloud services including Pub/Sub, BigQuery, and Cloud ML; Particle and Meridian; and a clever MQTT-compatible broker. In addition, through the workflows service, integration can be easily completed with limited development effort for most services that offer a RESTful API. In addition, Losant offers a highly customizable external-facing webhook service that enables workflows to either expose or collect data via specific publicly accessible URLs. This feature further reduces complexity when integrating existing enterprise applications or services. Unlike the copious offerings for northbound integration, southbound integration is distinctly lacking in the Losant IoT platform. With industrial asset compatibility limited to Modbus and no support for emerging standards such as LWM2M(for either data ingestion or device management, customers will likely be required to develop their own on-gateway or on-edge protocol adapters to support legacy systems and assets, which detracts from overall platform proficiency in terms of external integration.

External Integration

Losant IoT

RESULTS

C = COMPLETENESS **S = SOPHISTICATION** **E = EASE OF TASK COMPLETION** **T= TIMING OF TASK**

EXTERNAL INTEGRATION		C	S	E	T
C-05-01	Configure rule/platform for outbound external app action	3	3	2	5
C-05-02	Configure credentials for external application	3	2	3	1
C-05-03	Trigger device command from externally accessible API	3	3	3	3
C-05-04	Configure rule/platform for outbound pre-integrated app action	3	3	3	5
C-05-05	Configure rule/platform for outbound cloud data-plane integration	3	3	3	6
C-05-06	Locate and evaluate quality of device SDKs	2	3	N/A	N/A
C-05-07	Locate and evaluate quality of industry-standard protocols	2	1	N/A	N/A

Monitoring

Losant IoT

SUMMARY

Monitoring is an area of distinct strength for the Losant IoT platform. Losant makes it easy for both operators and administrators to monitor connected assets, ingested IoT data, and the state of platform configuration with a variety of easy-to-use wizard-driven interfaces, a dedicated and multi-tiered alerting and notification system, and highly customizable dashboarding capabilities. While some interfaces seem better suited to support small numbers of deployed devices and while device groups are implemented through metadata tags rather than proper hierarchical groups, the operation of platform tasks is still intuitive and remains highly functional. The platform's dashboarding service is of particular note. The easy-to-use and very responsive interface is complemented by a highly extensible list of component widgets including maps, graphs, and table views. Therefore, customers don't need to choose between aesthetically pleasing or technically capable solutions. Single device views are also noteworthy in that they provide direct debugging and diagnostic tools that greatly aid in device operation and configuration. The platform provides responsive and utilitarian real-time monitoring views enabling easy visibility into incoming and outgoing device messages. The only significant monitoring feature Losant's solution lacks is certain aggregated device views for administrators, which instead typically require the use of dashboards to gain visibility into the state of many connected assets simultaneously.

Monitoring

Losant IoT

RESULTS

C = COMPLETENESS **S = SOPHISTICATION** **E = EASE OF TASK COMPLETION** **T= TIMING OF TASK**

MONITORING		C	S	E	T
C-07-01	Trigger email on event	3	3	2	4
C-07-02	Trigger SMS on event	3	3	2	5
C-07-03	View sensor data for bulk devices	3	2	2	3
C-07-04	View device alert status for bulk devices	3	2	3	3
C-07-05	Create a dashboard for multiple-device status	3	3	3	4
C-07-06	View historical device status of a single device	3	3	3	1
C-07-07	View device status for a single device	3	3	3	1
C-07-08	View device status for multiple devices	3	3	3	2
C-07-09	View sensor data for a single device	3	3	3	1
C-07-10	View device alert status for a single device	3	2	3	1

Usability

Losant IoT

SUMMARY

Usability is an area of particularly noteworthy strength for the Losant IoT platform. With a complete and effective developer portal, publicly accessible community forums, and message board topics embedded within the platform documentation, all developer resources are easily located and utilized. Extensive platform documentation provides details on virtually every single platform feature, although, at times, the depth of examples and use-cases is limited within the main documentation. However, Losant does provide an extensive list of tutorials and projects to help customers prototype solutions and understand how best to utilize the offered platform capabilities. Of additional note, the platform interfaces and developer portal are both extremely responsive, providing real-time updates to data fields and tables nearly instantaneously, quick movement between platform elements, and an overall clean and modern UI aesthetic. Losant does lack some support in terms of productized device agents and device SDKs, although sufficient framework is provided to allow customers to quickly develop their own implementations.

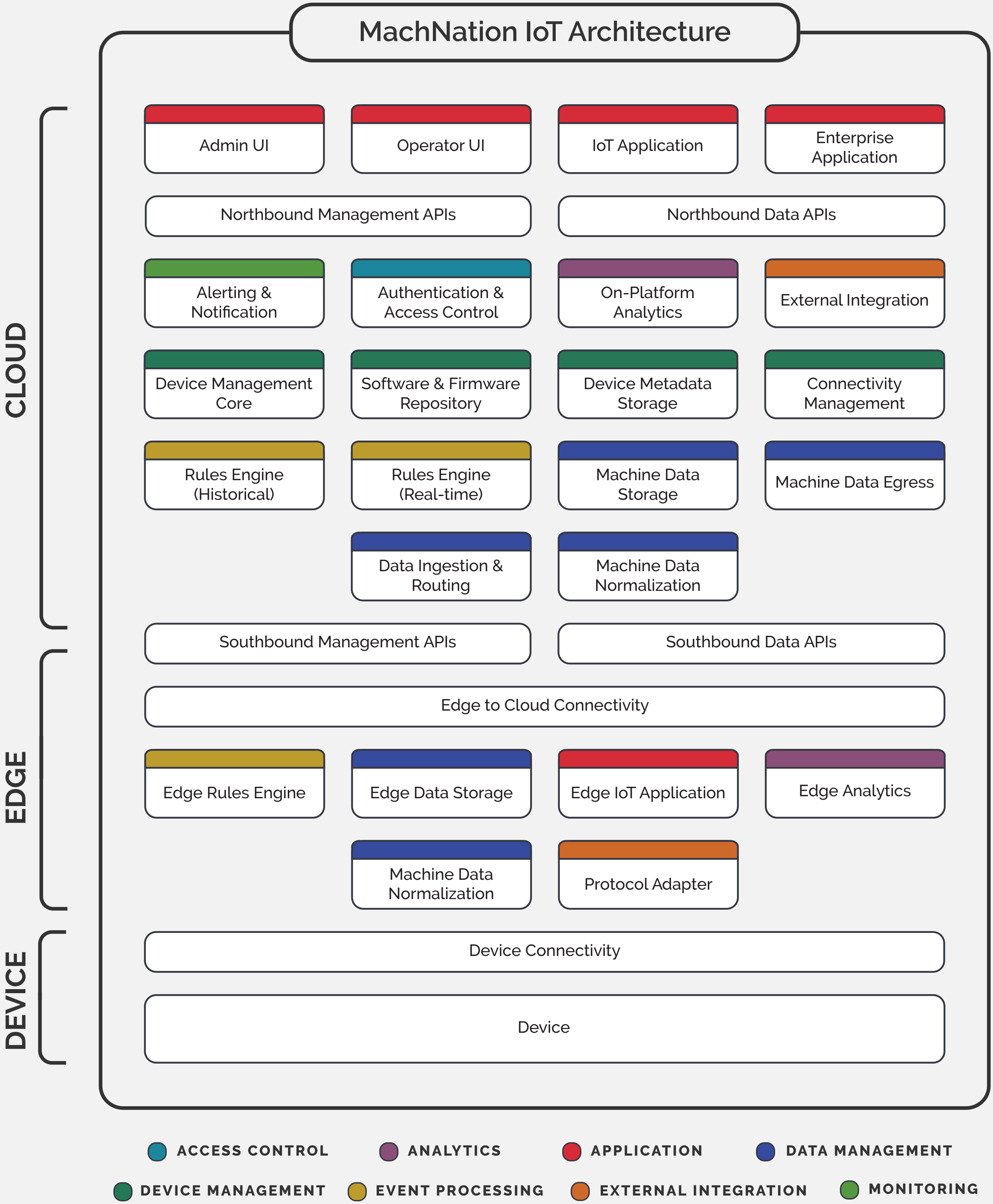
Usability

Losant IoT

RESULTS

C = COMPLETENESS **S = SOPHISTICATION** **E = EASE OF TASK COMPLETION** **T= TIMING OF TASK**

USABILITY		C	S	E	T
C-08-01	Locate and evaluate quality of developer portal	3	3	N/A	N/A
C-08-02	Locate and evaluate quality of platform-level documentation	3	2	N/A	N/A
C-08-03	Locate and evaluate quality of northbound APIs	3	3	N/A	N/A
C-08-04	Locate and evaluate quality of southbound APIs	3	2	N/A	N/A
C-08-05	Locate and evaluate quality of platform management APIs	3	3	N/A	N/A
C-08-06	Evaluate overall cogency/quality of admin user interface (UI)	3	3	N/A	N/A
C-08-07	Evaluate overall cogency/quality of operator user interface (UI)	2	3	N/A	N/A



MachNation IoT Architecture

CLOUD

Admin UI | Operator UI | IoT Application | Enterprise Application

Northbound Management APIs | Northbound Data APIs

Alerting & Notification | Authentication & Access Control | On-Platform Analytics | External Integration

Device Management Core | Software & Firmware Repository | Device Metadata Storage | Connectivity Management

Rules Engine (Historical) | Rules Engine (Real-time) | Machine Data Storage | Machine Data Egress

Data Ingestion & Routing | Machine Data Normalization

Southbound Management APIs | Southbound Data APIs

EDGE

Edge to Cloud Connectivity

Edge Rules Engine | Edge Data Storage | Edge IoT Application | Edge Analytics

Machine Data Normalization | Protocol Adapter

DEVICE

Device Connectivity

Device

● ACCESS CONTROL ● ANALYTICS ● APPLICATION ● DATA MANAGEMENT

● DEVICE MANAGEMENT ● EVENT PROCESSING ● EXTERNAL INTEGRATION ● MONITORING

Definitions of Categories

Access Control

Access control is the system of identity verification and permission management for all platform-connected elements including APIs, administrator or operator interfaces, devices, users, organizations, stored or in-transit data, or any other platform service.

Analytics

Analytics refers to the ability of an administrator or operator to monitor both historical and real-time observations collected from platform-connected IoT devices. Analytics can include descriptive, predictive, and prescriptive components.

Application

An application is any piece of contained logic either running on or directly integrated to an IoT platform. On-cloud and on-premises applications enable code-based control over IoT platform components, enriching the raw assets or data with customer-specific logic. An application can contain customer-, operator-, or administrator-facing user interfaces (UIs), or could function as a self-contained service, providing any type of relevant data or device manipulation.

Data Management

Data management is defined as the capabilities within an IoT platform to ingest, store, manage, and forward data received from platform-connected IoT devices.

Device Management

Device management refers to the ability of a platform to provide lifecycle management functionality for connected devices, including device onboarding, deployment of software and firmware updates, and configuration of managed devices.

Event Processing

Event processing refers to the ability of an IoT platform to execute actions or provide notifications based on administrator or operator configured rules or triggers.

External Integration

Integration is defined as the ability of an IoT platform to interface and share data with off-platform or third-party applications, services, or systems.

Monitoring

Monitoring is defined as the ability of a platform to trigger events, evaluate device status, and follow ingested data streams. Platform capabilities for monitoring should include both aggregated and drill-down views, and typically include operator- or administrator-facing dashboards and other graphical interfaces.

Definitions of Functional Blocks

Administrator User Interface (UI)

The administrator UI provides configuration management capabilities including access control and platform configuration. This administrator interface is also typically responsible for configuration of vendor-provided on-platform services, such as device and data management configuration.

Alerting and Notification

Alerting and notification is any system of pushing data, metadata, and messages to operators, administrators, or external systems for purposes of generating logged events. Alerting and notifications may include user-configurable notifications provided through UI and user experience (UX) elements in a dashboard or list views. Alerting and notifications might also use push-based or pull-based API/M2M elements to complete their message delivery purposes.

Authentication and Access Control

Authentication and access control is a system of identity verification and identity management for all platform-connected elements including APIs, admin UI, operator UI, devices, and platform-provided services. Authentication and access control should support multi-factor authentication for both users and devices and support multi-tenant and customer-of-customer models. Authentication and access control may also include encryption and data protection though not required in all IoT cases.

Connectivity Management

Connectivity management is a service which manages the device-to-cloud or edge-to-cloud communications layer. Connectivity management may include, SIM management (e.g., provisioning, billing metric collection, etc), LPWAN management (e.g., a LoRa server or SigFox integration), or WiFi/BTLE/LAN management (e.g., 802.1X, mesh routing, etc). While many connectivity management services such as SIM management for 3G/4G connectivity may be protocol-specific, connectivity management integration should be protocol agnostic and enable a variety of device-to-cloud or edge-to-cloud communication technologies.

Data Ingestion and Routing

Data ingestion and routing is a service that allows platforms to ingest machine data from connected IoT devices, aggregation points, and gateways and then forward ingested data to other on-platform or off-platform services. Data ingestion and routing is often an MQTT/HTTP endpoint, but is logically protocol agnostic. Data ingestion and routing acts as a message hub, enabling an individual ingested message to pass through the variety of on-platform or off-platform services.

Device

A device is a combination of hardware and software assembled to perform some IoT function. The hardware component is often comprised of an integrated circuit or system on chip (SoC), sensor, actuator, communication module, and a security module. The software component is often comprised of firmware, bootloader, operating system, and device agent.

Device Connectivity

Device connectivity is the communication path allowing data to travel from an individual device to an IoT edge gateway using Bluetooth low-energy, Zigbee/Z-Wave, or other LAN-based technologies. In addition, some devices may connect directly to the platform without transiting an IoT gateway by using LPWAN, cellular, satellite, or fixed-line services.

Device Management Core

Device management core is a service that provides a central repository and inventory of information for all connected or managed IoT devices, aggregation points, and gateways. In addition, the device management core exposes services that enable lifecycle management of devices.

Device Metadata Storage

Device metadata storage is an asset database that provides a collection point for all IoT device metadata including device current state and historical state. Very often device metadata storage is implemented as a SQL-type datastore. Device metadata storage can be exposed directly to the IoT platform or enterprise application (e.g., asset tracking or inventory management systems), or can only be exposed internally to the IoT device management services.

Edge Analytics

Edge analytics is any type of data- and metadata-related quantitative exploration executed locally at the edge. Edge analytics often include limited anomaly detection or other essential security-related analytic services, though more complete analytic implementations are also possible.

Edge Data Normalization

Edge data normalization is a service that enables the conversion and standardization of machine data at the IoT edge from unstructured, streaming sources to compressed, structured data formats for northbound transmission or storage. Additionally, data normalization may aggregate high refresh-rate sensor data into moving averages or other windowed metrics.

Edge Data Storage

Edge data storage is a service that provides either ephemeral or persistent storage of machine data at the IoT edge. Edge data storage can be used as a short-term storage engine during periods of intermittent platform connectivity or as a longer-term storage engine for edge-based analytics or monitoring.

Edge IoT Application

An edge IoT application is an IoT application deployed to and executed from the edge of an IoT solution. It typically interfaces with locally available resources and devices, but may also connect to southbound or northbound (data and management) APIs.

Edge Event Processing

Edge event processing is the ability to execute actions including external callouts, notifications, and alerts executed on the edge of the IoT network. Edge event processing is often a feature-limited version of the on-platform, cloud-based event processing, though it may also be implemented as fully-featured complex event processing (CEP).

Edge to Cloud Connectivity

Edge-to-cloud connectivity is the communication service allowing data to travel from IoT devices, aggregation points, and gateways to cloud IoT platform and other cloud services. Connectivity options include low-power wide-area networks (LPWAN), cellular, satellite, proprietary networks, and fixed-line services. Typically, this component is monitored and controlled via the Connectivity Management service.

Enterprise Application

An enterprise application is any external service including a third-party analytics service, data-storage service, and others, that interfaces with northbound (data and management) APIs to provide functionality to platform operators.

Event Processing (Historical)

Event processing (historical) is the ability to execute actions including external callouts, notifications, and alerts based on stored machine data. The actions performed are based on machine data that have been stored. Event processing (historical) can either be based on anomaly-detection rules, moving averages, or other operator- or administrator-defined parameters.

Event Processing (Real-time)

Event processing (real-time) is the ability to execute actions including external callouts, notifications, and alerts based on live or streaming machine data. Event processing (real-time) can also provide anomaly-detection and value limits, but these must be provided near real-time with event processing occurring within a few minutes after initial data ingestion.

External Integration

An external integration is a solution using an API or other connector allowing the bidirectional flow of data between an IoT platform and external systems or platforms including ERP, CRM/SFA, inventory management, trouble ticketing, and others. External integrations, unlike generic machine data egress topologies, are productized offerings providing pre-built connectors to selected external systems or platforms. These external integrations allow the selective push of data based on business rules.

IoT Application

An IoT application is any piece of contained logic running on the IoT platform or directly integrated to the IoT platform. An application could contain customer-, operator-, or administrator-facing UIs, or function as a self-contained service, providing any type of relevant data manipulation or device manipulation. IoT applications running on-cloud or on-premises enable code-based control over the IoT platform components, enriching the raw assets or data with customer-specific logic.

Machine Data Egress

Machine data egress is a service to programmatically provide data retrieval from on-platform data stores. Machine data egress usually allows users to create time series filters and queries against underlying data stores that are then typically exposed to either on-platform or off-platform applications.

Machine Data Normalization

Machine data normalization is a service that enables the conversion and standardization of machine data from unstructured, streaming sources to compressed, structured data formats for northbound transmission or storage. Additionally, data normalization may aggregate high refresh-rate sensor data into moving averages or other windowed metrics.

Machine Data Storage

Machine data storage is a service that allows the persistent storage of IoT device data typically in time-series formats. Machine data storage provides services to allow querying of machine data based on IoT device or time period. It usually consists of a NoSQL data store, although relational data stores are also possible. Some IoT platforms provide no storage capabilities, some require usage of an external-to-platform data store, and some provide limited periods of data retention.

Northbound Data APIs

Northbound data application programming interfaces (APIs) are either a single API or collection of APIs facilitating management of data storage. The northbound data APIs provide programmatic access to data stored within the IoT platform as well as live data received from IoT devices.

Northbound Management APIs

Northbound management APIs are either a single API or collection of APIs facilitating management of the configuration and operations of an IoT platform. The northbound management APIs may be separated into a device management API, operation API, administrator API, and others.

On-Platform Analytics

On-platform analytics is any type of data- and metadata-related quantitative exploration executed in the cloud platform. On-platform analytics can include discrete analytics services, fully-integrated analytics services, or vendor-provided applications.

Operator UI

The operator UI provides the day-to-day interface for platform operators for functions including device management, data management, reporting, and analytics. All capabilities are provided for the platform and associated services.

Protocol Adapter

Protocol adapter is a service deployed at the IoT edge that enables compatibility between industrial or other SCADA-type hardware and the device management and data management platform components. This service typically serves as a bridge between proprietary protocols and standardized protocols such as MQTT or LWM2M and can be deployed either within the platform or directly on edge devices or gateways.

Software and Firmware Repository

Software and firmware repository is a service that provides a centralized collection point for software and firmware to be pushed to or accessed directly from IoT devices, aggregation points, or gateways.

Southbound Data APIs

Southbound data APIs enable communication on the data layer between connected IoT devices, aggregation points, and gateways and data ingestion and routing service components. Southbound data APIs are typically MQTT/HTTP endpoints, but many different protocols are used in different platforms.

Southbound Management APIs

Southbound management APIs enable bidirectional management-layer communication between a device management service and managed IoT devices, aggregation points, and gateways. Southbound management APIs are often provided as an HTTP endpoint or via a standard such as LWM2M, but proprietary protocols are also common. These APIs are distinct from the machine data ingestion endpoint in that no actual machine data is provided over this channel, only data associated with device management including lifecycle management data, firmware, and other.