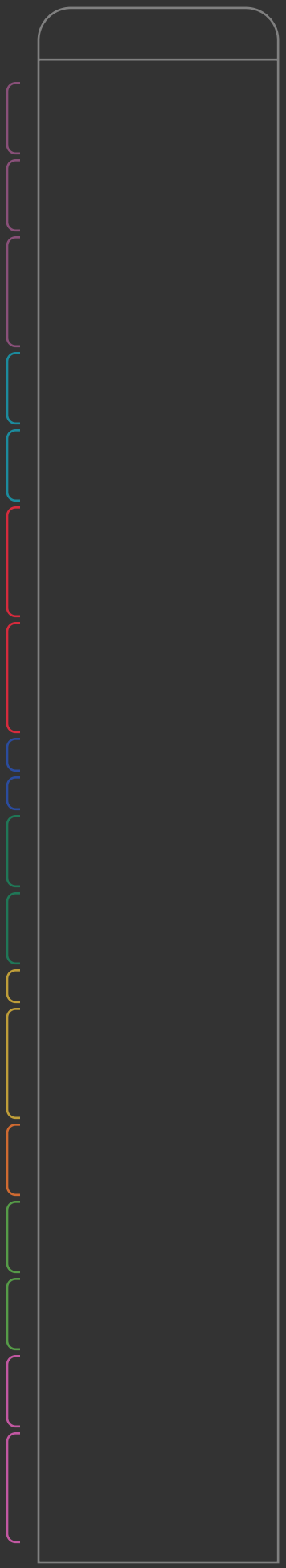
machnation



MIT-E Results

December 18, 2017

MachNation

What is MIT-E?

MIT-E is an IoT platform test lab run by MachNation, the world leading analyst firm researching IoT platforms and middleware. MIT-E's core product is a database to help enterprises compare IoT platform usage statistics. MIT-E analysts perform a set of common hands-on tasks – developer workflows – on IoT platforms. MIT-E analysts score these tasks and compile them in a database. MIT-E scores platform tasks based on the time-to-complete each task, ease-of-completion, completeness of tasks and sophistication metrics. MachNation makes the MIT-E database and detailed reports available to enterprises to help guide IoT platform purchase decisions. The database and detailed reports provide enterprises an apples-to-apples comparison of IoT platforms across relevant hands-on task metrics.

Legal Disclaimer

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 time spent waiting on "blocking" elements outside of core task description requirements.

SCORE RANGE	0 to infinite
TIMING	Total time to execute task in minutes
DNF	Task could not be completed

Amazon

Product Name

AWS IoT

Product Version

2017.08.24

AWS IoT Summary

ACCESS CONTROL

COMPLETENESS OF TASK

SOPHISTICATION OF SOLUTION

EASE OF TASK COMPLETION

DEVICE MANAGEMENT

COMPLETENESS OF TASK

SOPHISTICATION OF SOLUTION

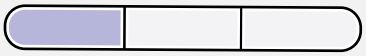
EASE OF TASK COMPLETION

DATA MANAGEMENT

COMPLETENESS OF TASK

SOPHISTICATION OF SOLUTION

EASE OF TASK COMPLETION

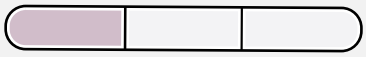


ANALTYICS

COMPLETENESS OF TASK

SOPHISTICATION OF SOLUTION

EASE OF TASK COMPLETION



EVENT PROCESSING

COMPLETENESS OF TASK

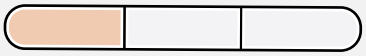
SOPHISTICATION OF SOLUTION

EASE OF TASK COMPLETION

EXTERNAL INTEGRATION

COMPLETENESS OF TASK

SOPHISTICATION OF SOLUTION



EASE OF TASK COMPLETION

MONITORING

COMPLETENESS OF TASK

SOPHISTICATION OF SOLUTION

EASE OF TASK COMPLETION

USABILITY

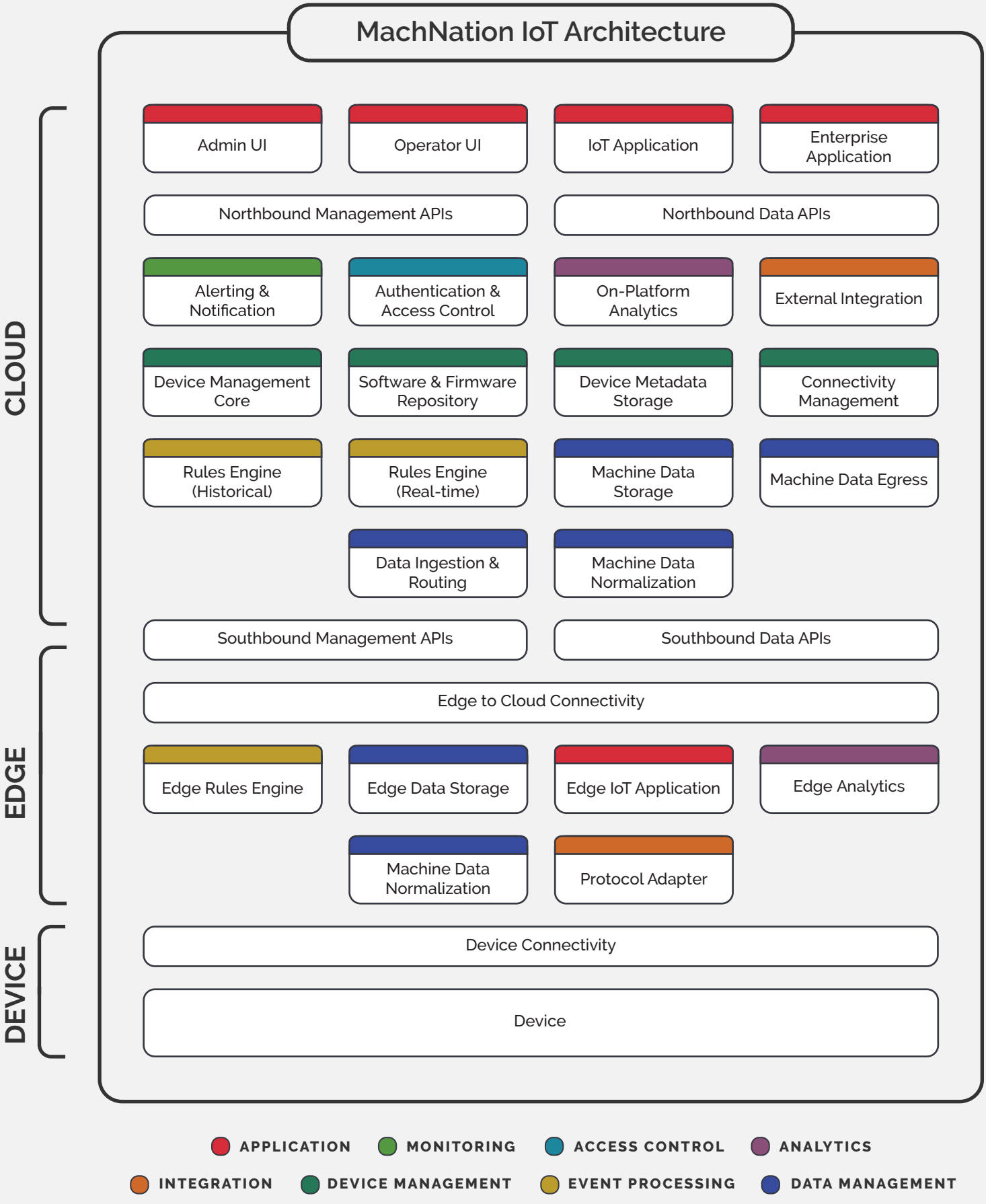
COMPLETENESS OF TASK

SOPHISTICATION OF SOLUTION

COMPREHENSIVE EVAL

COMPLETENESS OF TASK

SOPHISTICATION OF SOLUTION


MachNation IoT Architecture
CLOUD
EDGE
DEVICE
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 to Cloud Connectivity
Edge Rules Engine
Edge Data Storage
Edge IoT Application
Edge Analytics
Machine Data Normalization
Protocol Adapter
Device Connectivity
Device
APPLICATION
MONITORING
ACCESS CONTROL
ANALYTICS
INTEGRATION
DEVICE MANAGEMENT
EVENT PROCESSING
DATA MANAGEMENT

Categories of IoT Platform Functionality

Administrator User Interface (UI)

The administrator user interface (UI) provides configuration management capabilities including access control and platform configuration. All capabilities are provided for the IoT platform and associated services.

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 an action. Alerting and notifications may include UI and user experience (UX) elements in a dashboard, email or SMS message. 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, administrator UI, operator UI, devices and platform-provided services. Authentication and access control should support multi-factor authentication for both users and devices. Authentication and access control may also include encryption and data protection though not required in all IoT cases.

Connectivity Management

Connectivity management refers to any system that orchestrates, configures, or otherwise manages the device connectivity layer. Such systems may manage provisioning, billing, or utilization metrics of the relavant wireless or wired technologies utilized by IoT devices or IoT gateways.

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. Data ingestion and routing is often a MQTT/HTTP endpoint, but is logically protocol agnostic. Data ingestion and routing relays collected data to rules engines, storage engines or external 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 security module. The software component is often comprised of firmware and software packages, a boot loader, an operating system and a device agent.

Device Connectivity

Device connectivity is the communication service allowing data to travel from devices to an IoT edge gateway using Bluetooth low-energy, Zigbee/Z-Wave, LPWAN or other LAN/WAN technologies. Devices may also connect directly to the IoT platform without using an IoT gateway by using LPWAN, cellular, satellite, or fixed-line services. Typical communication protocols include MQTT or HTTP(S).

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, 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 basic 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.

Edge Data Storage

Edge data storage is a service that provides either transient or long-term amassment 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 network that typically interfaces with locally available resources and devices, but may also connect to southbound or northbound (data and management) APIs.

Edge Rules Engine

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

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.

External Integration

An external integration is a solution using an API or other connector allowing 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

The IoT application interfaces with the northbound (data and management) APIs to provide access to platform data, non-platform data and configurations on the platform.

Machine Data Egress

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

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.

Machine Data Storage

Machine data storage is a service that allows the amassment 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 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 application programming interfaces (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.

Rules Engine (Historical)

Rules engine (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. The rules engine (historical) can either be based on anomaly-detection rules, moving averages or other operator- or administrator-defined parameters.

Rules Engine (Real-time)

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

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 by 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(S) 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 HTTPS endpoint, 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 such as lifecycle management commands, firmware updates, and other device management functionality.