Transforming the World through the Power of Connectivity

New Relic | Electric Imp Workshop

August, 2016

Electric Imp

Padma Duvvuri, Head of BD & Ecosystem

Betsy Rhodes, Software Engineer

Terrence Barr, Senior Solution Architect

Jaron Abelsohn, BD Manager

New Relic

Clay Smith, Developer Advocate

Jackson De Oliveira, Field and Community Marketing Manager

Agenda

- Electric Imp Company Overview
- Collaboration Benefits of New Relic & Electric Imp
- Workshop and Demo Overview
- New Relic and Electric Imp integration:
  - Challenge 1: Tutorial
  - Challenge 2: Self-paced
- Conclusion and Next Steps
- Q&A

New Relic®

&imp

Introduction to Electric Imp

Our Mission: Transform the world through the power of connectivity

Hugo Fiennes, CEO & Co-Founder

A history of leading development of world class connected device innovations

Led the hardware team through first four generations of Apple iPhone

Designed and architected hardware for the Nest Thermostat

Founded 2011
HQ in Los Altos, CA
Product Development in the US and UK

Electric Imp Team: Experience across leading technology companies:

Google nest cisco Roku Microsoft ORACLE

100+ customers

105+ countries

14 Billion

Messages processed per month

600,000+

Devices in the market

IoT Market Focus

Intelligent Buildings
Light Industrial
Energy
Connected Home Infrastructure

The Challenge of Connectivity

To realize the value of data, companies must first securely connect their products

Connectivity

Edge to Cloud Security

Hardware and Firmware Design

Approvals and Certifications

Scalability and Availability

OTA Software & Security Updates

Support and Maintenance

Testing and Productization

HW/SW Infrastructure integration

Provisioning and Management

Edge Intelligence and Control

- Connectivity is complex; building it is expensive and time intensive
- Companies often lack the resources, expertise, and long-term support commitment
- Connectivity decisions today are critical; changing platforms is hard
- Ongoing security adds additional complexity and cost

IoT Data & Applications

Conclusion: To maximize ROI, companies should evaluate **Buy-vs-Build** for connectivity

Solution:

Electric Imp takes the Complexity out of Connectivity

Our leading IoT connectivity platform provides the core services to get any device online

Security Ongoing, managed security-as-a-service for connectivity

Reliability Less risk and reduced development costs with a proven platform

Flexibility Easily adapt to different use cases & customer requirements

Scalability Effortless scalability for large deployments

Seamlessness Faster time to market with complete out-of-the-box connectivity and drop-in integration

Customer Proof Points

Our single platform meets the business objectives of a wide range of customers

pitney bowes

Connected Postage Meters via "SmartLink"

- Update units in the field
- Meet stringent security requirements Accommodate users with a wide range of technical aptitude

CYBEX

Cybex "Care" Connected Treadmill

- Retrofit units in the field
- Provide predictive maintenance
- Expedite time to market

hiku

"The Shopping Button"

- Bridge between assets and the cloud
- Offer analytics for the real world
- Builds direct customer engagement

ABInBev

"Bud-e Fridge" Smart Home Beer Fridge

- Automated fulfillment
- Usage tracking
- Accessible user experience
- Innovate brand engagement

Petasense

Vibration "mote" for predictive maintenance

- Retrofit industrial vibration monitoring
- Provide real-time analytics and dashboarding
- Reduce unplanned downtime and repair costs

&imp

Customers in a variety of roles use New Relic to solve problems faster and improve visibility.

DEVELOPERS

- Extra visibility helps them solve problems faster and build better apps.

APPLICATION OWNERS

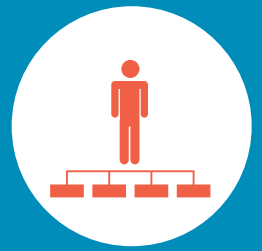
- Service-level responsibility to the business, understands monitoring from a transactional point of view.

OPERATIONS

- Important to keep apps and services up and running. Availability and app health drives their business.

MANAGERS & EXECS

- Direct visibility into how performance is affecting the bottom line.



SUPPORT

- Quickly diagnose performance issues affecting customers. Reduce time to resolve issues.

New Relic &imp

New Relic®

&imp

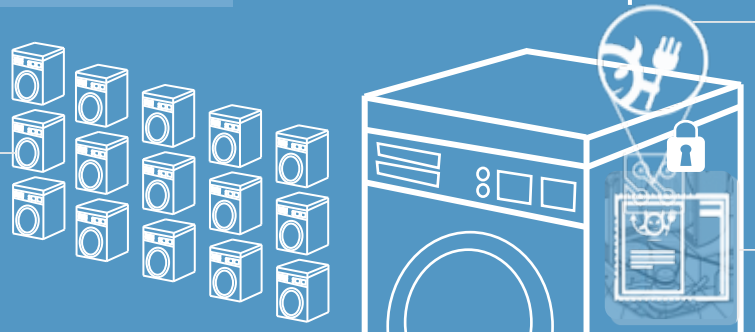
Collaboration Benefits

With Electric Imp's platform every device has a customizable, secure, powerful, and intelligent virtual presence

imp APIs
- Rest API, webhooks & partner integration libraries
- Seamless integration with mobile apps, web apps, data services, and enterprise systems

BlinkUp™
- Patented secure optical provisioning and authentication
- Enables production scale device enrollment

imp Scalability
- Full suite of tools from prototyping to deployment
- Scales across multiple product lines & product groups



impCloud Agent
- Small, powerful cloud virtual machine paired with device VM
- Container for programmable middleware
- Total resilience, always on, and near infinite scaling

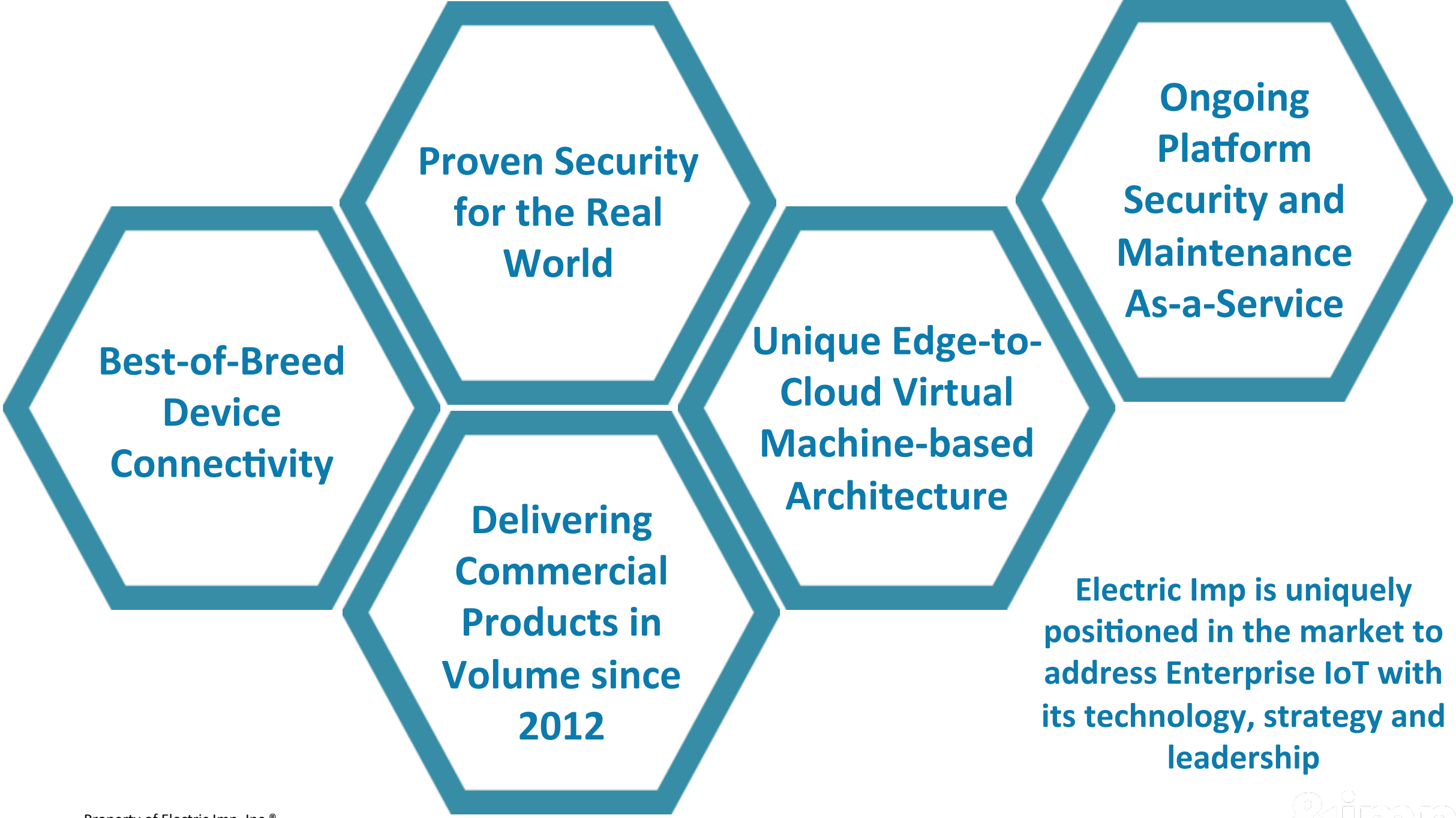
impSecure
- Edge to cloud security
- Lifetime managed by Electric Imp

impOS
- Purpose built & optimized for IoT applications
- Hardware independent customer app in device VM
- OTA management and instant updates

imp Authorized Hardware
- Vetted hardware design and security
- Partner supplied commodity hardware
- Preloaded with impOS and security keys

Why Electric Imp & New Relic?

- **Proven** edge-to-cloud solution to address real-world challenges of delivering, securing, and managing connected products
- **Low complexity**, IP-based architecture enables customers to easily connect devices to New Relic Insights and other services
- **Secure and scalable solution** allows easy customization and reuse across different use cases and products
- **Full visibility** of performance from the edge to critical backend systems



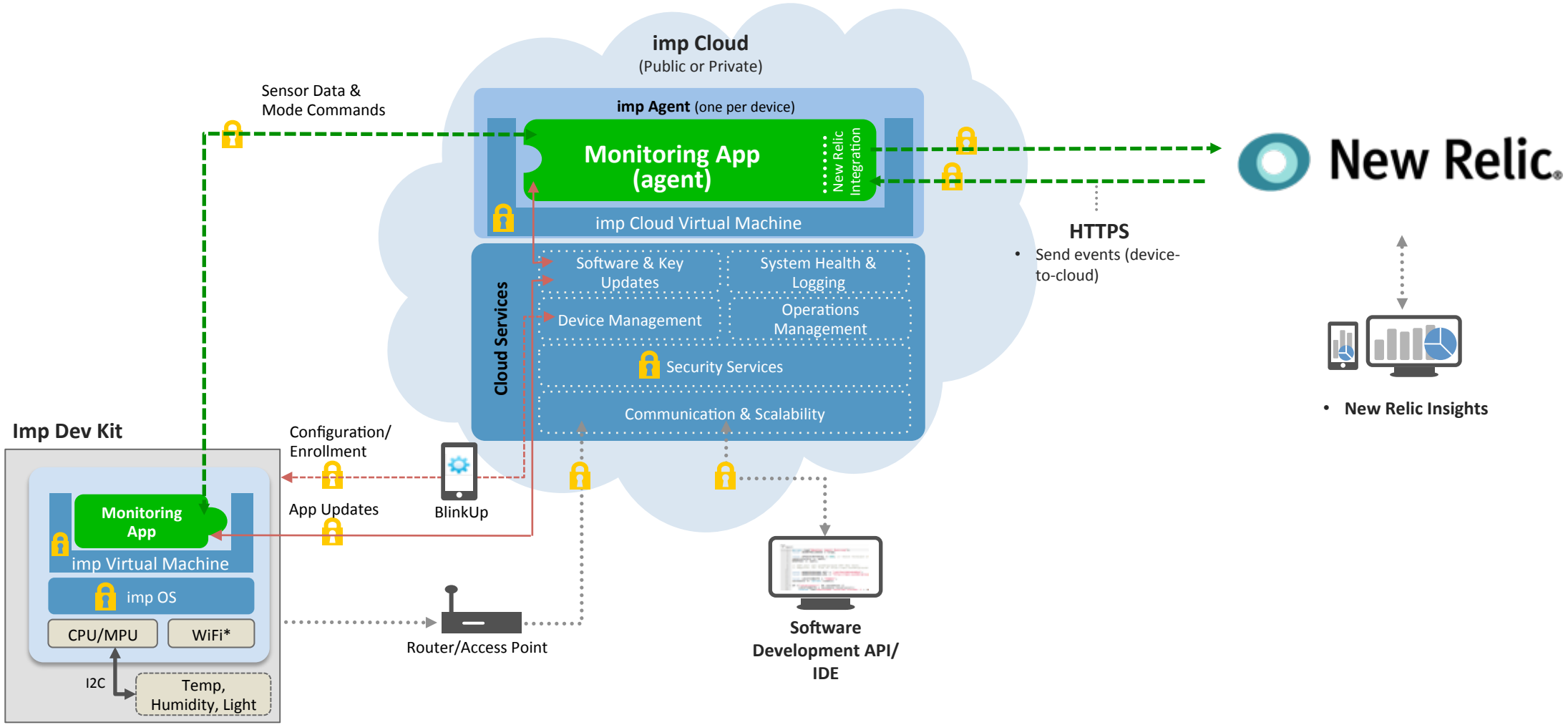
Electric Imp is uniquely positioned in the market to address Enterprise IoT with its technology, strategy and leadership

New Relic®

&imp

Workshop & Demo Overview

Demo Architecture: Environmental Monitoring



Demo Application Structure

Device-side application

- imp001 Developer Kit + 'Environmental Tail'
  - Single module Cortex-M3 MCU and WiFi
  - Temp + humidity sensors
- Monitor device and environmental conditions
  - WiFi strength, latency, free memory, and voltage
  - Temperature, humidity and light level
- Log readings
- Send readings to cloud agent

Cloud-side Agent application

- Endpoint for bidirectional device-agent communication
- Pass data between device and agent over secure, managed communication link
- Push data into New Relic
  - Temperature, humidity and light level
  - WiFi strength, free device memory, message round-trip time

Demo Overview and Steps

1

Create Electric Imp developer account & download BlinkUp app for iOS or Android

Create a New Relic account

2

Power up imp001, connect & enroll imp into cloud

- Use BlinkUp to provision WiFi credentials and enroll into imp Cloud

3

In Electric Imp Online IDE:

- Create application (model) with device and agent code
- Insert OAuth Settings
- Press "**Build**" button in IDE to build, deploy, and auto-run application on device and agent

4

Use Electric Imp development kit to collect readings

- Devices will send readings to the agent
- Agent forward data to New Relic:
  - Env Data
  - Device Data

5

Integrate with New Relic

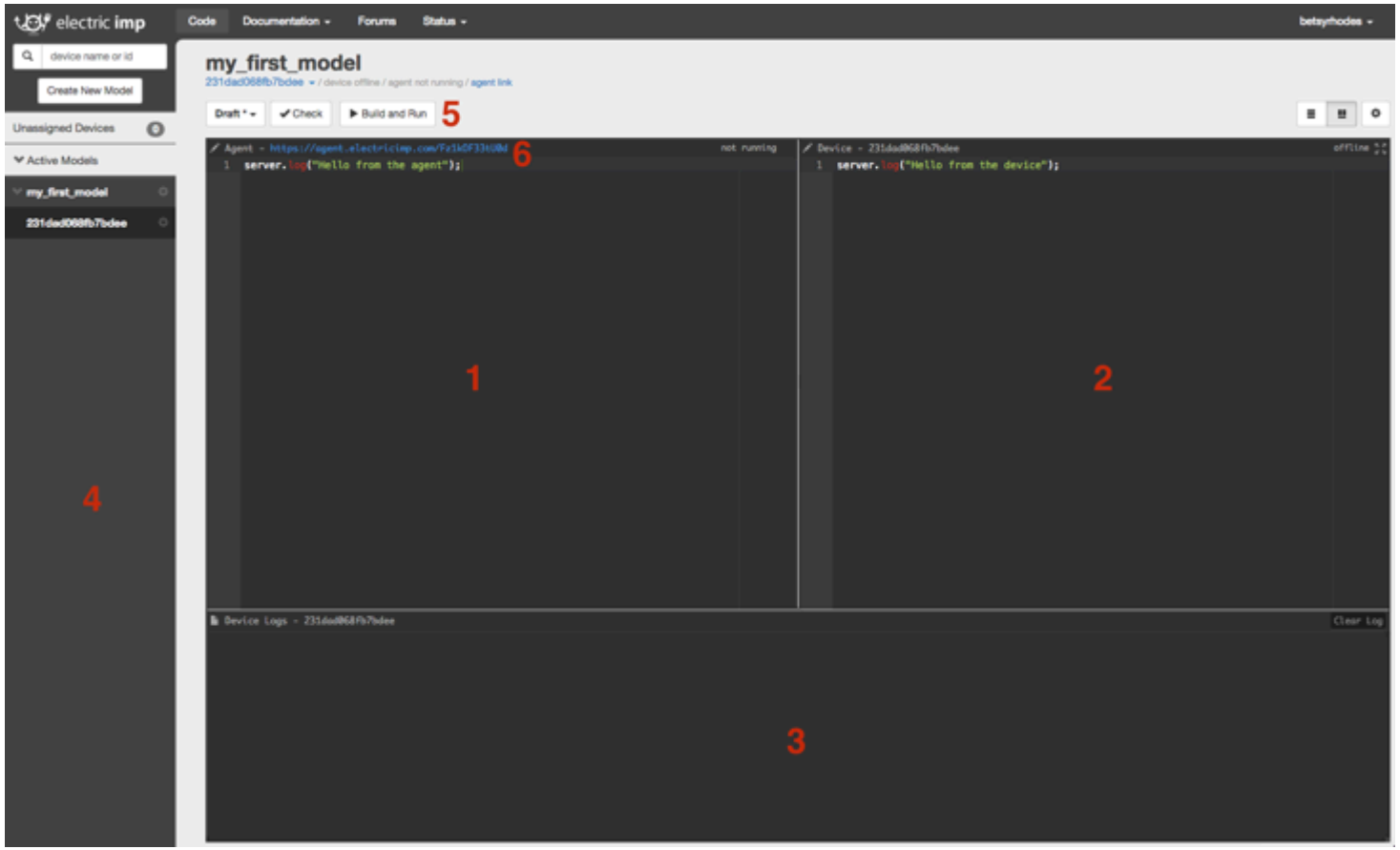
- Use Insights to create custom visualizations of data sent from devices.
- Create dashboards to share with your team and integrate with other monitored applications.

Electric Imp App/BlinkUp™: Simple and secure method of provisioning a device to end user Wi-Fi network

- Mobile app uses light pulses to pass information (SSID & password) to the device
- Device is automatically authenticated, enrolled into the Electric Imp cloud, and provisioned (e.g. Wi-Fi network)
- Now you can program your device in the online IDE

IDE Overview

ide.electricimp.com



1 – Agent Code Window

2 – Device Code Window

3 – Log Window

4 – Sidebar
- Models
- Devices

5 – Build and Run

6 – Agent URL

Electric Imp IDE Demo

New Relic &imp

Challenge 1 (tutorial)

Challenge 1: Environmental Monitoring

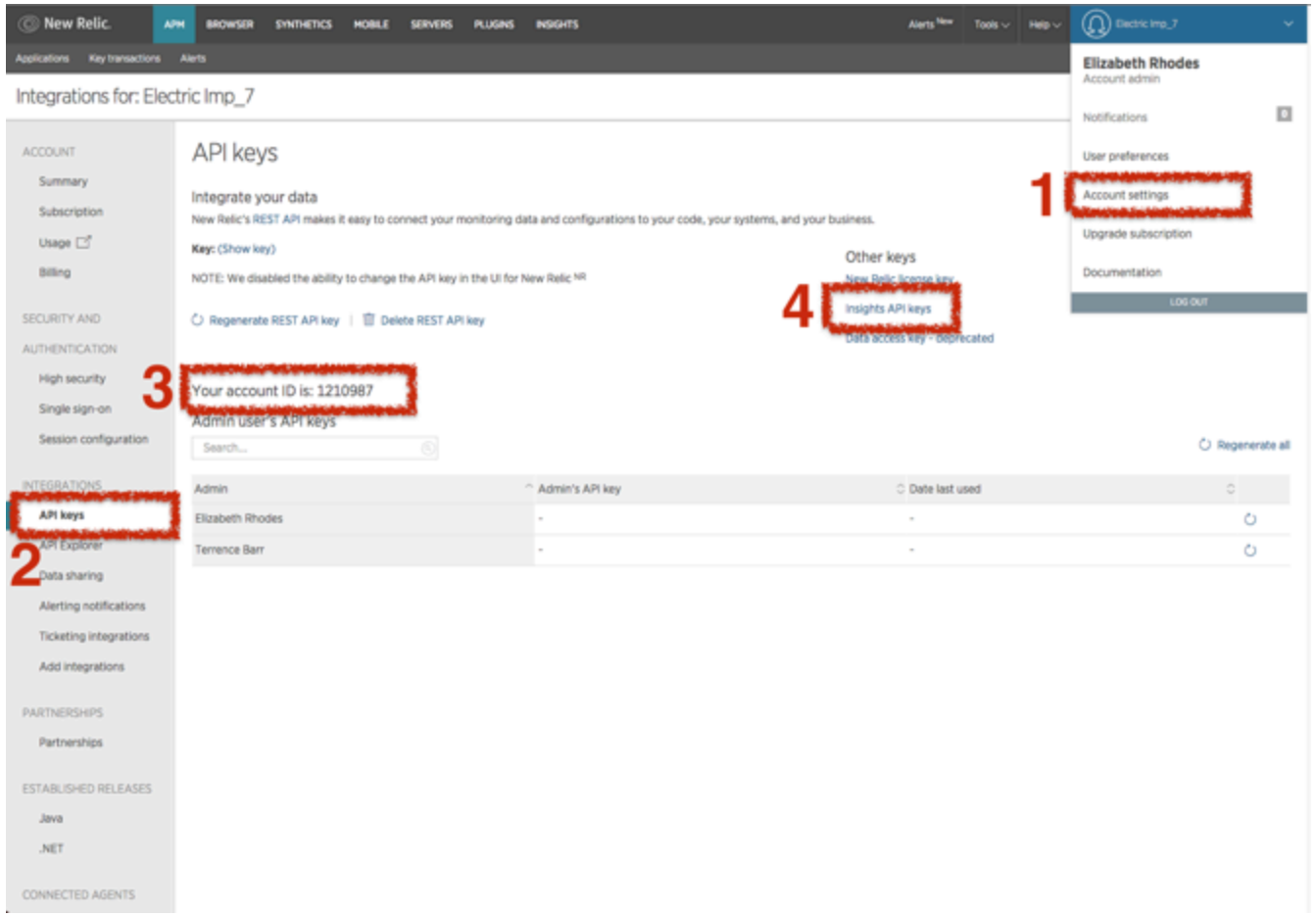
- Monitor environmental parameters
- Push Data to New Relic Insights
- Query/visualize data in New Relic Insights

Reminder: You need these things to continue…

- You should already have set up your Electric Imp Account and blinked up your Imp
- A New Relic account with Insights enabled
  - New account sign-up
    - newrelic.com/electricimp
  - Existing account
    - Account > Upgrade subscription > Dedicated > Add a promo code: ELCEVT14APM
- Code at
  - github.com/electricimp/NewRelicWorkshop_2016

New Relic Account Settings

rpm.newrelic.com/accounts



1 – Account Settings

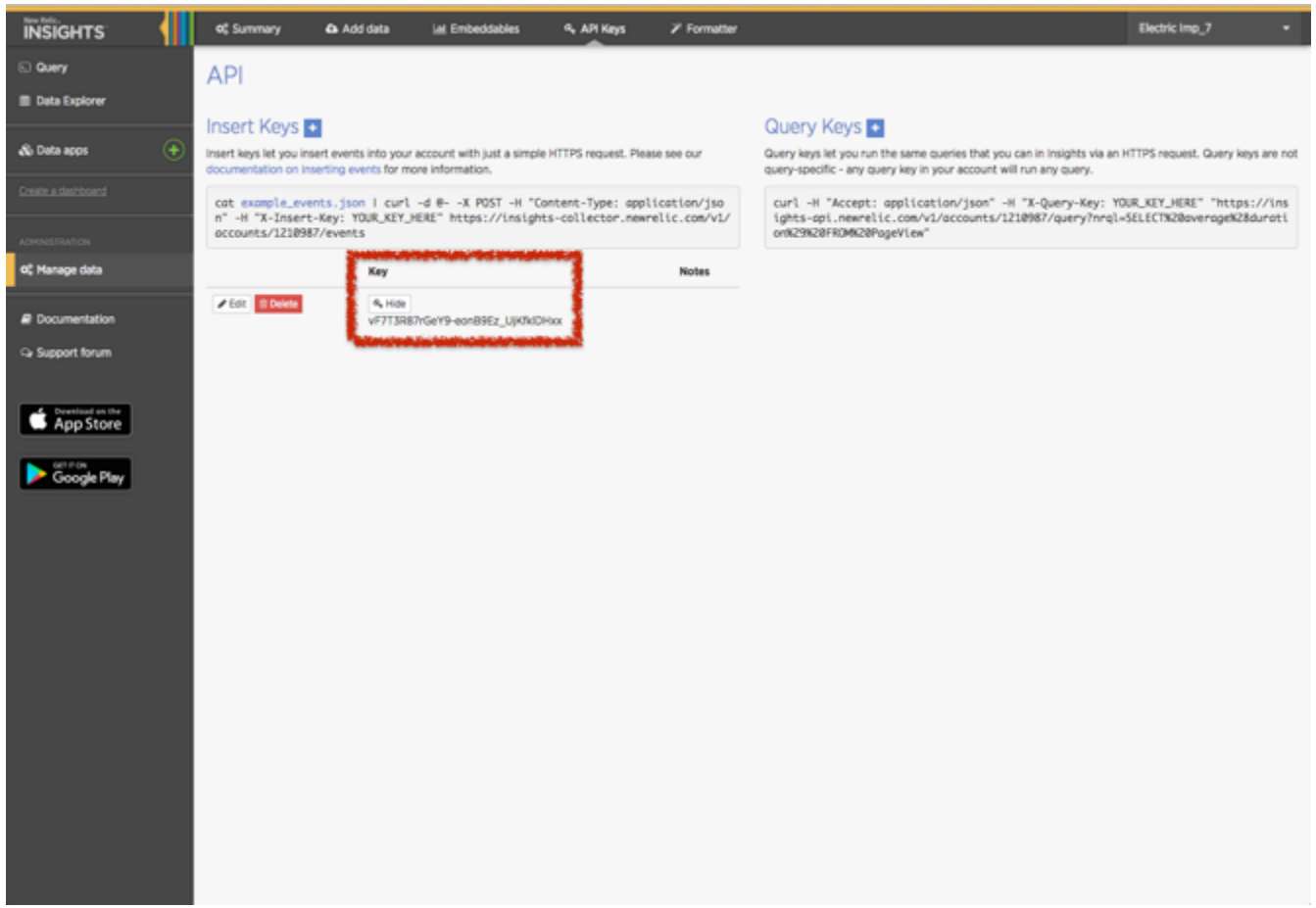
2 – Integrations -> API keys

3 – Note Your Account ID

4 – Click Insights API keys

New Relic API Key

insights.newrelic.com/accounts



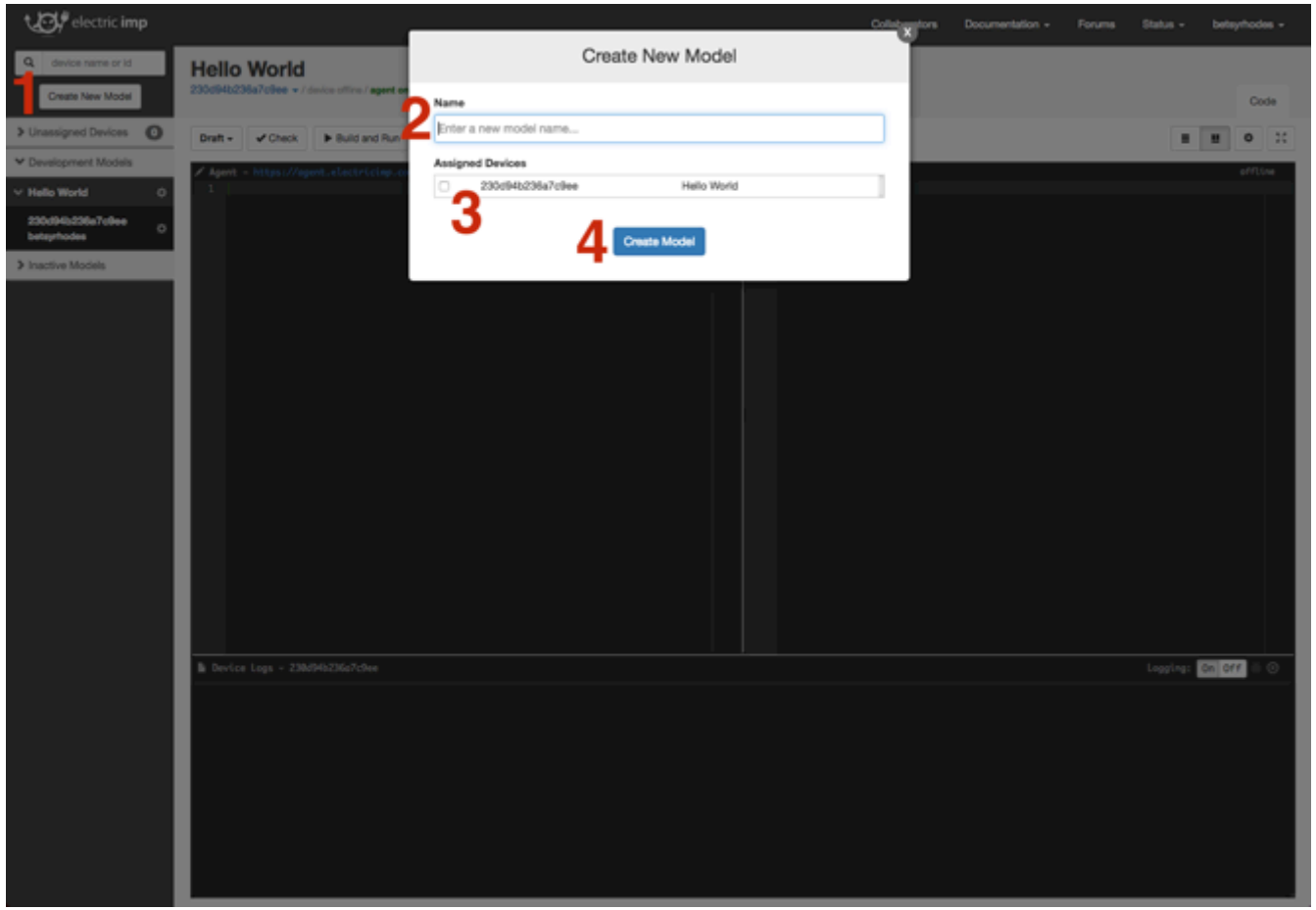
1 – Click Show

2 – Note Your API Key

Note: this is an Insights key, not the REST API Key.

Electric Imp Create New Model

ide.electricimp.com



1 – Click Create New Model

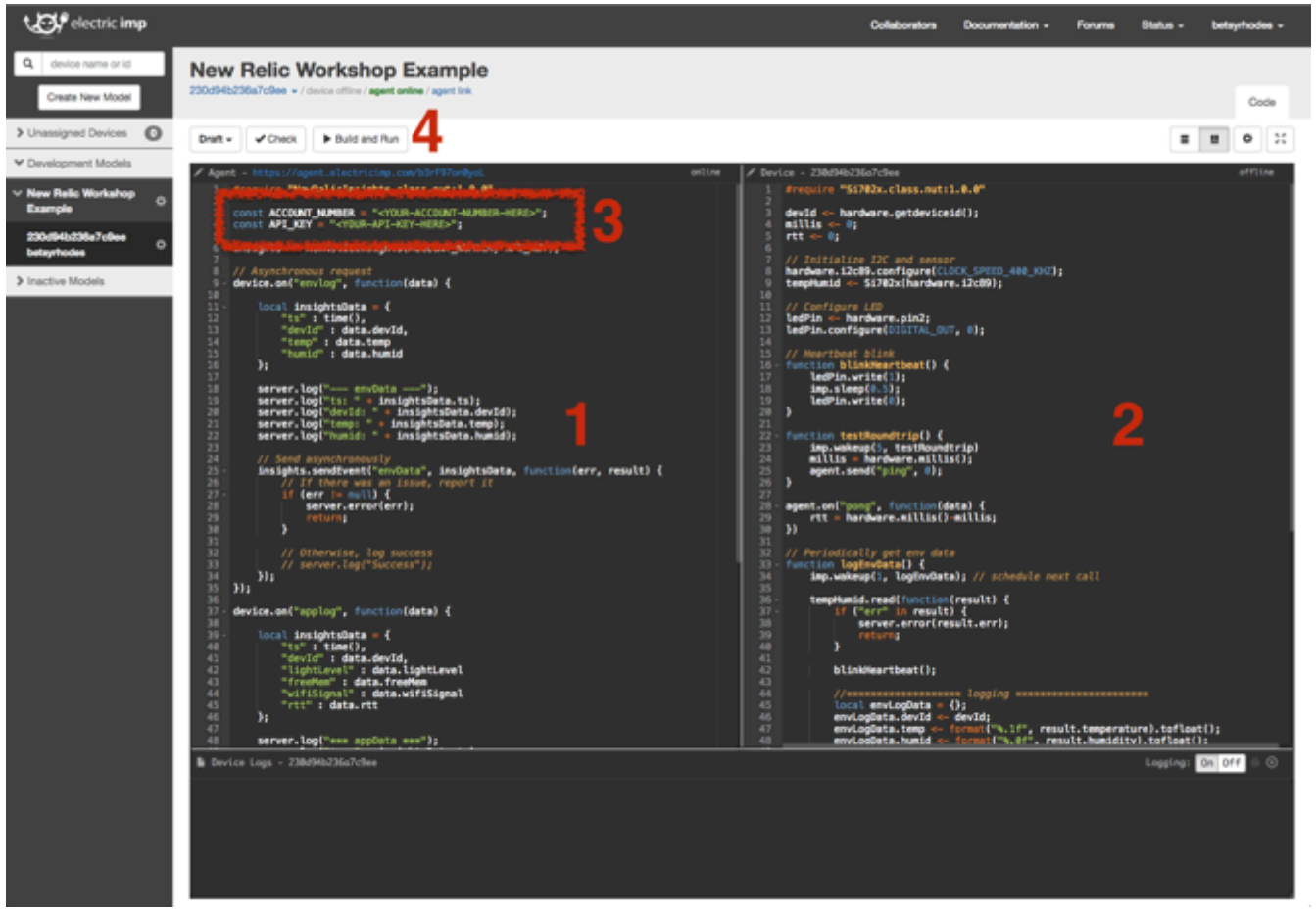
2 – Enter Name for your Model

3 – Assign your Device to the Model

4 – Click Create Model

Electric Imp Run Example Code

ide.electricimp.com



1 – Copy and Paste Agent Code

EnvironmentalMonitoringExample.agent.nut

2 – Copy and Paste Device Code

EnvironmentalMonitoringExample.device.nut

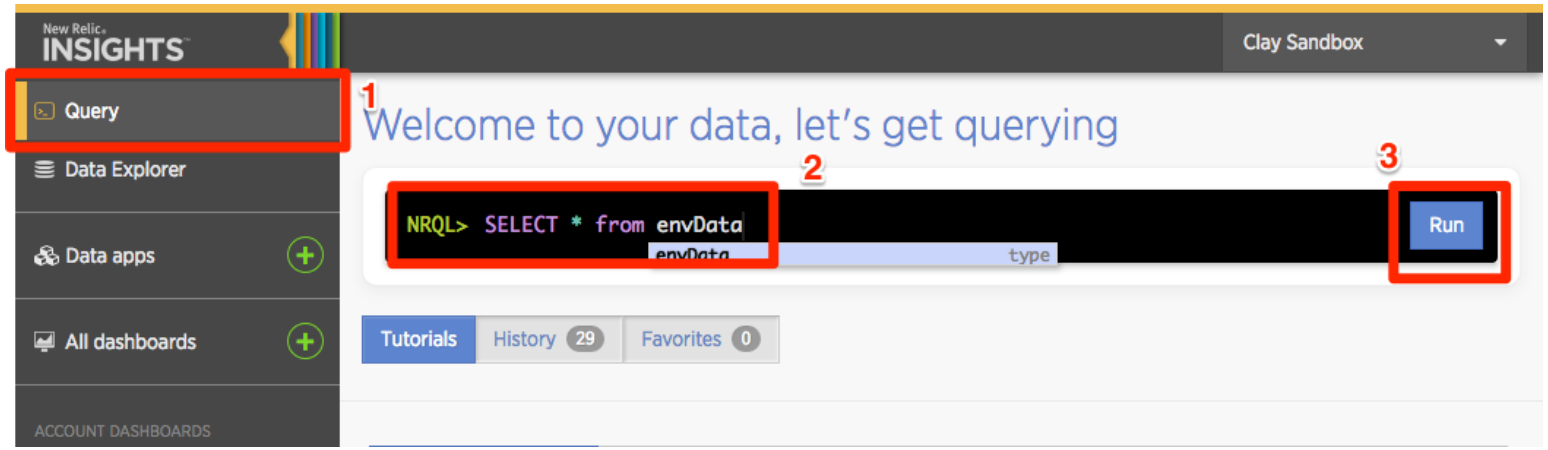
3 – Enter Your New Relic Info

- Account Number
- API Key

4 – Click Build and Run

Your first NRQL query

https://insights.newrelic.com



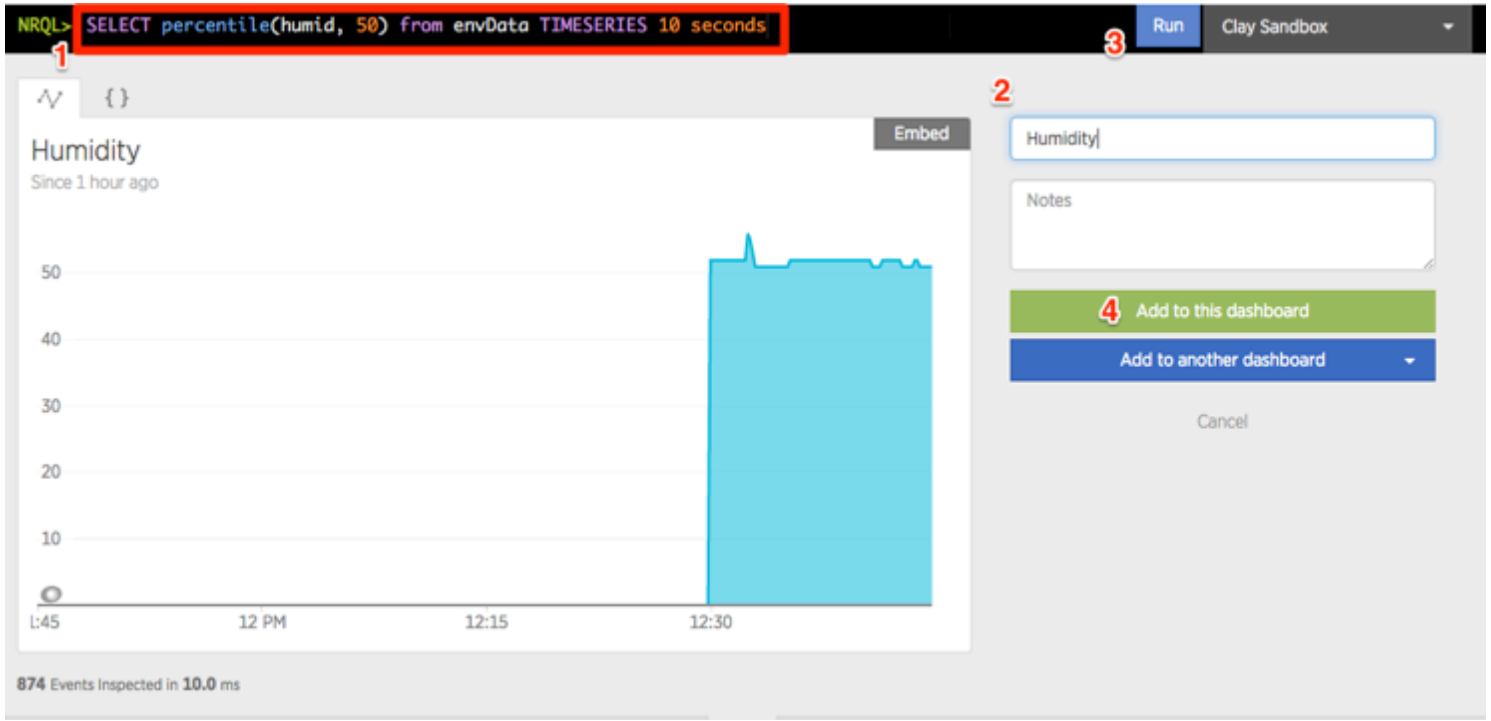
1 – Click “Query”

2 – Enter “SELECT * from envData” (just like SQL!)

3 – Click “Run” to execute query and see results being sent to Insights.

Visualizing Humidity Readings

https://insights.newrelic.com



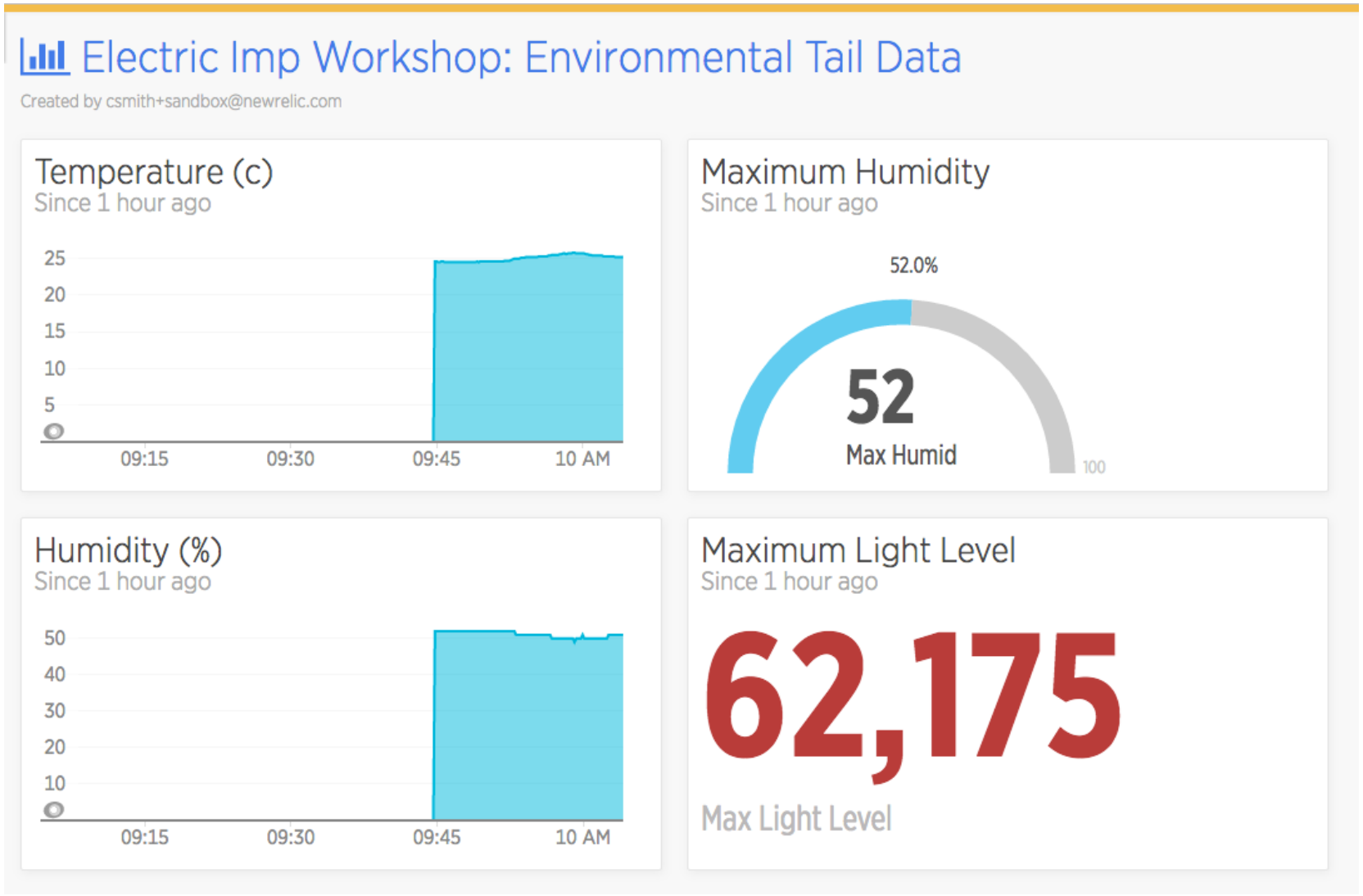
1 – Write a query to visualize data

2 – Give the chart a title

3 – Click “Run” to execute query

4 – Add to your dashboard

Experiment with Queries and Add New Widgets



Status Check

Questions?

Comments?

New Relic

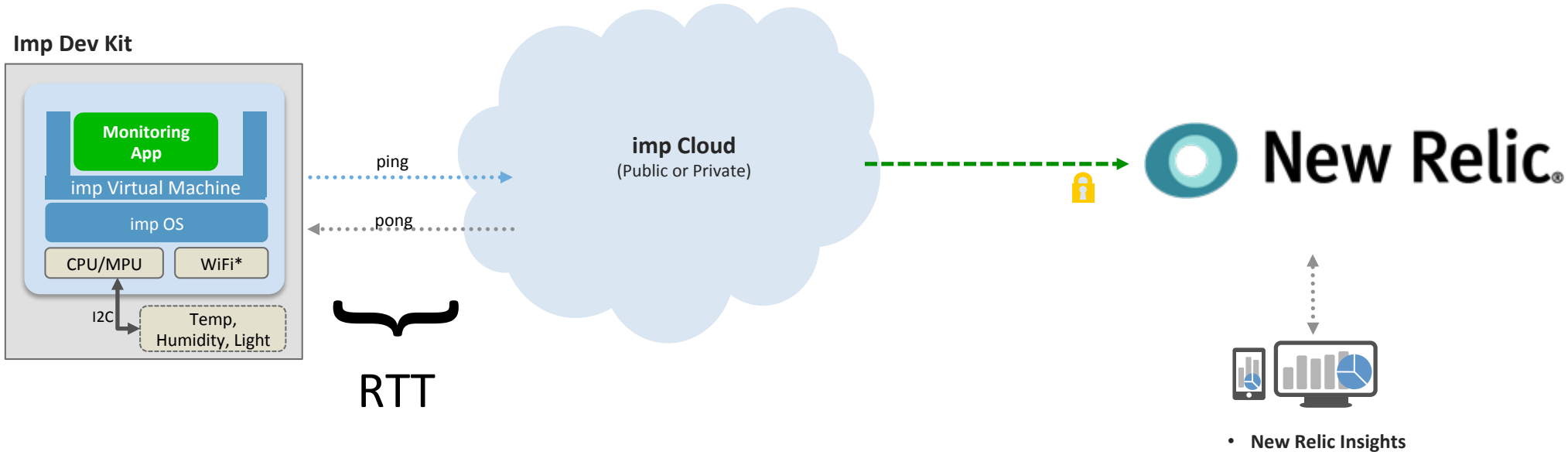
&imp

Challenge 2 (self-paced)
Background

Challenge 2: Monitoring Application Performance at the Edge

- Previous Challenge: Monitor environmental parameters
- This Challenge: Monitor the edge application itself
- How?
  - Capture key performance metrics indicative of application/device performance
  - Send to New Relic Insights
  - Analyze metrics, generate statistics, provide insights into application performance at the edge
- Suggested metrics to monitor
  - Device WiFi signal strength
  - Free application memory
  - Message communication round-trip time (RTT)

Measuring Round-Trip Time (RTT) for Better Network Visibility



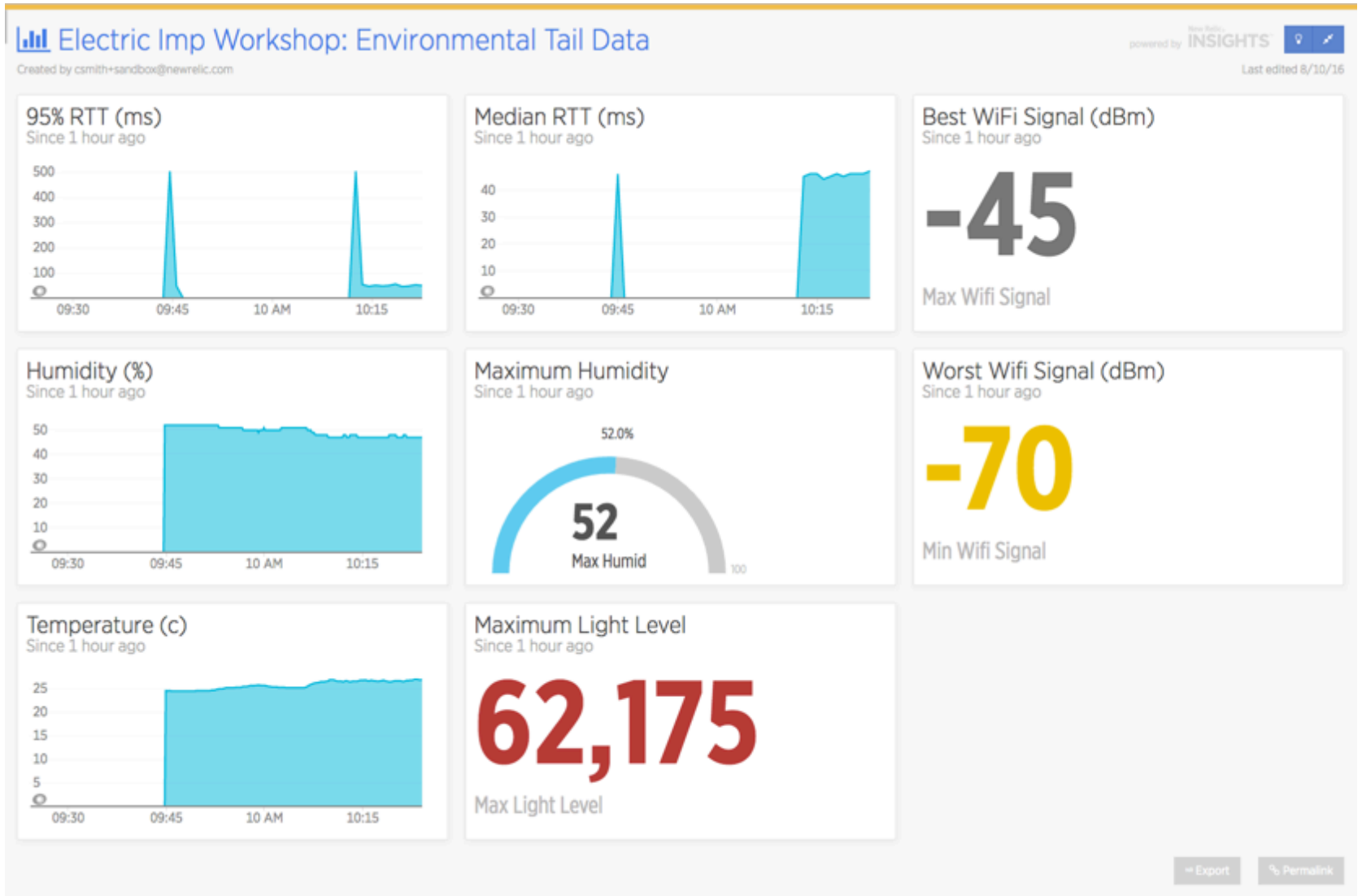
- Goal: understand the impact of network latency from the Imp to the cloud
- Implement simple “ping/pong” event that measures time elapsed, send to New Relic
- Don’t **blame the network**: understand how it impacts performance

Challenge 2: Hints

Hints

- See
  - electricimp.com/docs/api/hardware/ and electricimp.com/docs/api/imp/
- To measure round-trip time, use `agent.send()` <-> `agent.on()` ping-pong
- As data gets send to Insights, create new dashboards that display results
  - docs.newrelic.com/docs/insights/new-relic-insights/using-new-relic-query-language/using-nrql

Recap: Complete Dashboard Example



Conclusion and Next Steps

Conclusion and Next Steps

Electric Imp & New Relic: Extending Application Monitoring to the Edge

- ✓ Easy integration of device- and application data into New Relic Insights (and other New Relic services such as APM)
- ✓ Our integrated product offering can rapidly enable high value end-to-end IoT solutions
- ✓ Electric Imp focuses on the complexities of device connectivity and security so you can focus on your product- and application value-add

Next Steps

- Integrate Electric Imp device monitoring with existing backend software monitored by New Relic for full visibility from the edge to internal systems
- Use data to diagnose performance issues and discover connectivity issues or errors
- Know how your IoT devices are performing on different networks

New Relic®

&imp

Q&A

Transforming the World Through the Power of Connectivity

betsy@electricimp.com
padma@electricimp.com
terrence@electricimp.com
jaron@electricimp.com

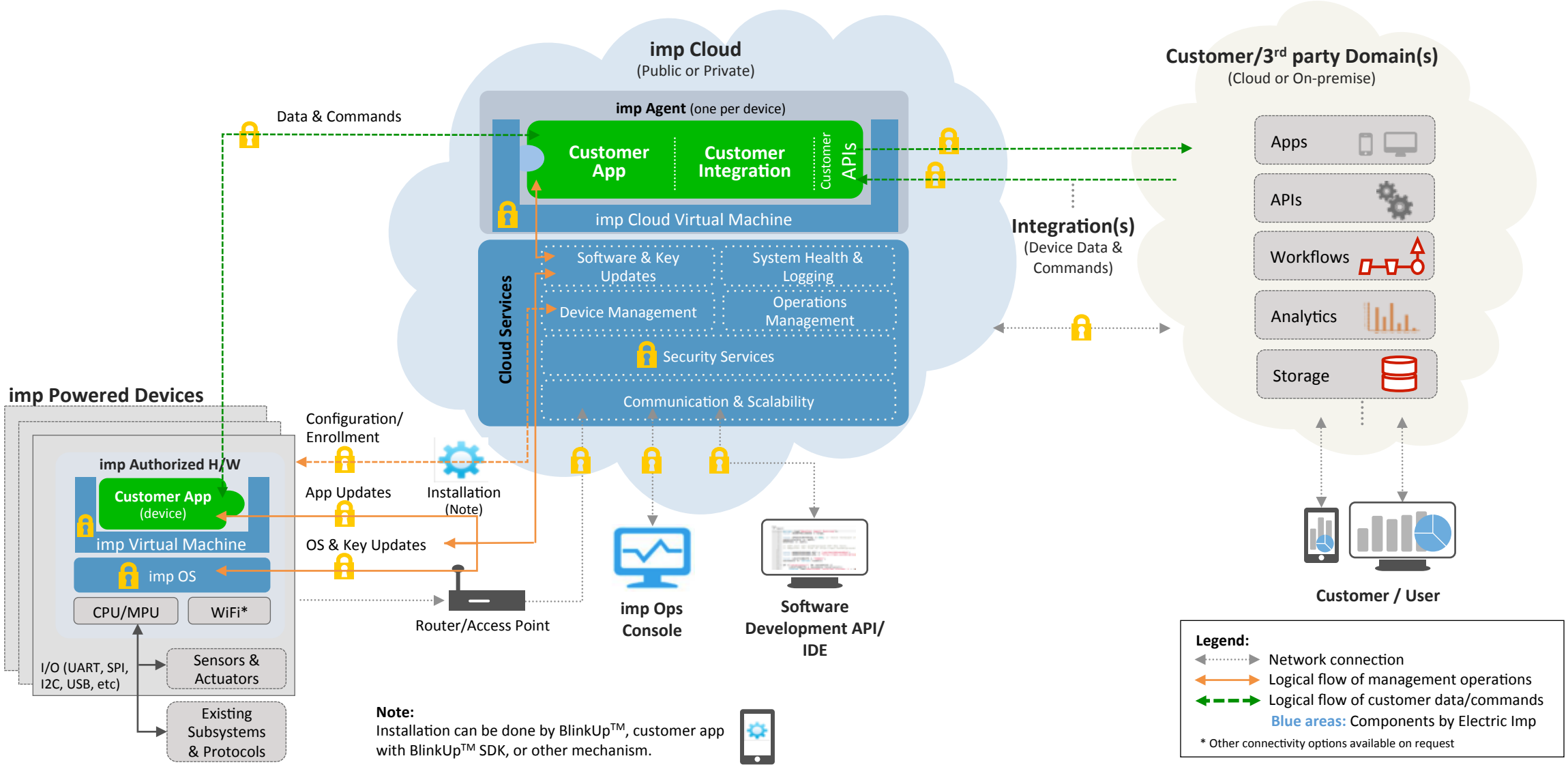
www.**electricimp**.com

New Relic

&imp

Appendix: Technical Deep Dive

Electric Imp Platform Architecture Overview



Electric Imp provides Worry-Free Security

Security is considered the number one inhibitor to IoT implementations

A security breach from just one device can cost a company millions of dollars in revenue loss, brand damage and expenses

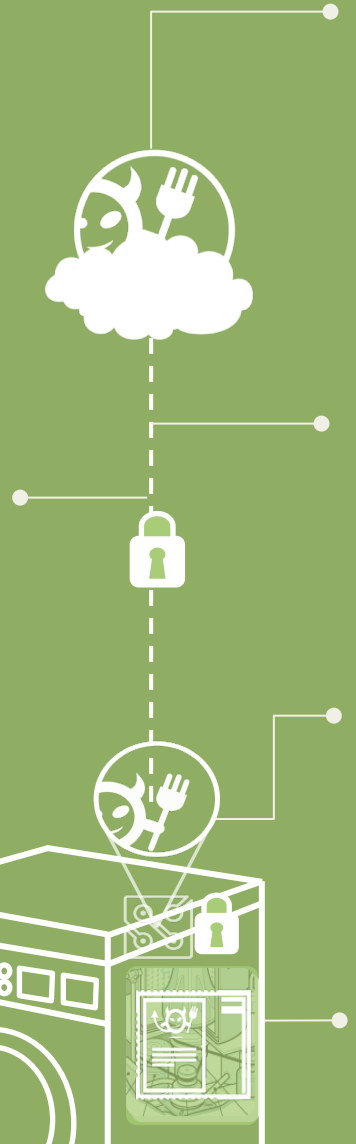
To safeguard the IoT, security must be designed in from the

The Electric Imp platform has an unparalleled security architecture from the hardware through the cloud

- **Device Security** - Hardware keys and code protected within the silicon
- **Communications Security** - Industry standard TLS link security and forward secrecy
- **Local Network Security** - Real activity is masked by random traffic
- **Device <> Server Monitoring** - Server and device identities are confirmed before any communication
- **Cloud Server Security** - Network servers firewalled and only accessed through a secure protocol
- **Secure Remote Updates** - Devices are updated automatically and seamlessly

Comprehensive Security Architecture

Addresses security at multiple levels, using industry standards and best practices, for the product lifetime



Servers

- Device link crypto terminated on home server (running agent), not load balancer
- Servers reside within VPC, minimal open ports
- Full PKI chain validation for outbound HTTPS connections from agent (vs on device which wouldn't have resources)
- Standard best practices including use of bastion host, minimal privileges, etc.
- Automated monitoring and configuration management of clusters

Link

- Minimal attack surface (no open ports except DHCP & DNS)
- Industry standard TLS 1.2 protected link, with forward secrecy (ephemeral DH)
- Parties validate each other with RSA certificates
- AES-128 or 256 encryption
- Outbound connection from device to cloud - no firewall holes
- Secondary non-impersonation protection using ECC challenge-response
- Random link maintenance traffic to hide application traffic patterns

Provisioning

- Replay-proof token-based optical provisioning system uniquely identifies user & device
- Simple: increases chances of being done correctly

Application

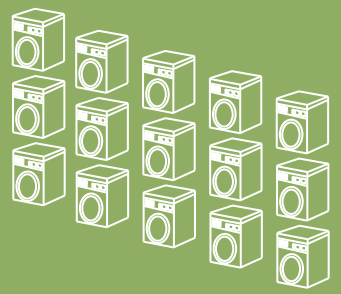
- Application storage either on-die or AES-GCM encrypted depending on model
- Secure OTA upgrades via TLS channel to server
- TOTP authorized deployments*

OS

- OS, network & security stack is maintained independently of application by Electric Imp for all devices
- OS updates do not require application or user involvement
- OTA OS upgrades/key management protected by RSA signing & AES-GCM encryption
- HSM-protected OS signing keys per cloud (each private cloud customer has their own set)

Hardware

- Secure boot, debug interfaces permanently disabled
- Unique per-device keys provisioned at time of module manufacture
- All off-die storage AES-GCM+AEAD encrypted with per-device keys
- Hardware no-execute protection on all writable RAM (violations reported to server over TLS)



Deploying on private cloud in 1H'16, public cloud in 2H'16