Why Most IoT Projects Fail And how to ensure success with OSIsoft and Cisco Kinetic

Presented by

Stephen Friedenthal, IoT Solutions Architect

About Cisco Systems, Inc.

San FranCISCO

Things you may know…

- Founded in **1984**
- **72,900** Employees worldwide
- **$48.0** Billion Annual Revenue 2% Y/Y growth

And, things you may not know…

- **6%** of Revenue comes from the cybersecurity unit, which grew by 14% year-over-year
- **51%** of Software Revenue is Subscription based
- Cisco spends **$3.5 million** per year on maintaining a dedicated disaster relief team – TacOPs for disaster response

Companies want to derive value from data

IoT exponentially increases the amount and types of data

Why IoT?

- A sense of scale….
  - 19 Billion IOT connected “things” in 2017
    - 31% YoY growth from 2016
  - 82 Billion connected “things” by 2025
- And, yet….
  - 60% of IoT projects never proceed beyond Proof-of-Concept
  - 74% of IoT projects fail to meet all of their objectives
  - 33% of IoT projects were viewed as a Failure

The Challenge – How to succeed with minimum risk?

Home

Cisco Survey Reveals Close to Three-Fourths of IoT Projects Are Failing

436 total shares

Released at marquee industry event IoT World Forum, the survey data also reveals keys to IoT success

MAY 23, 2017

LONDON - The Internet of Things World Forum (IoTWF), May 23, 2017 – IDC predicts that the worldwide installed base of Internet of Things (IoT) endpoints will grow from 14.9 billion at the end of 2016 to more than 82 billion in 2025[1]. At this rate, the Internet of Things may soon be as indispensable as the Internet itself.

Despite the forward momentum, a new study conducted by Cisco shows that 60 percent of IoT initiatives stall at the Proof of Concept (PoC) stage and only 26 percent of companies have had an IoT initiative that they considered a complete success. Even worse: a third of all completed projects were not considered a success.

"It's not for lack of trying," said Rowan Trollope, Senior Vice President and General Manager, IoT and Applications, Cisco. "But there are plenty of things we can do to get more projects out of pilot and to complete success, and that's what we're here in London to do."

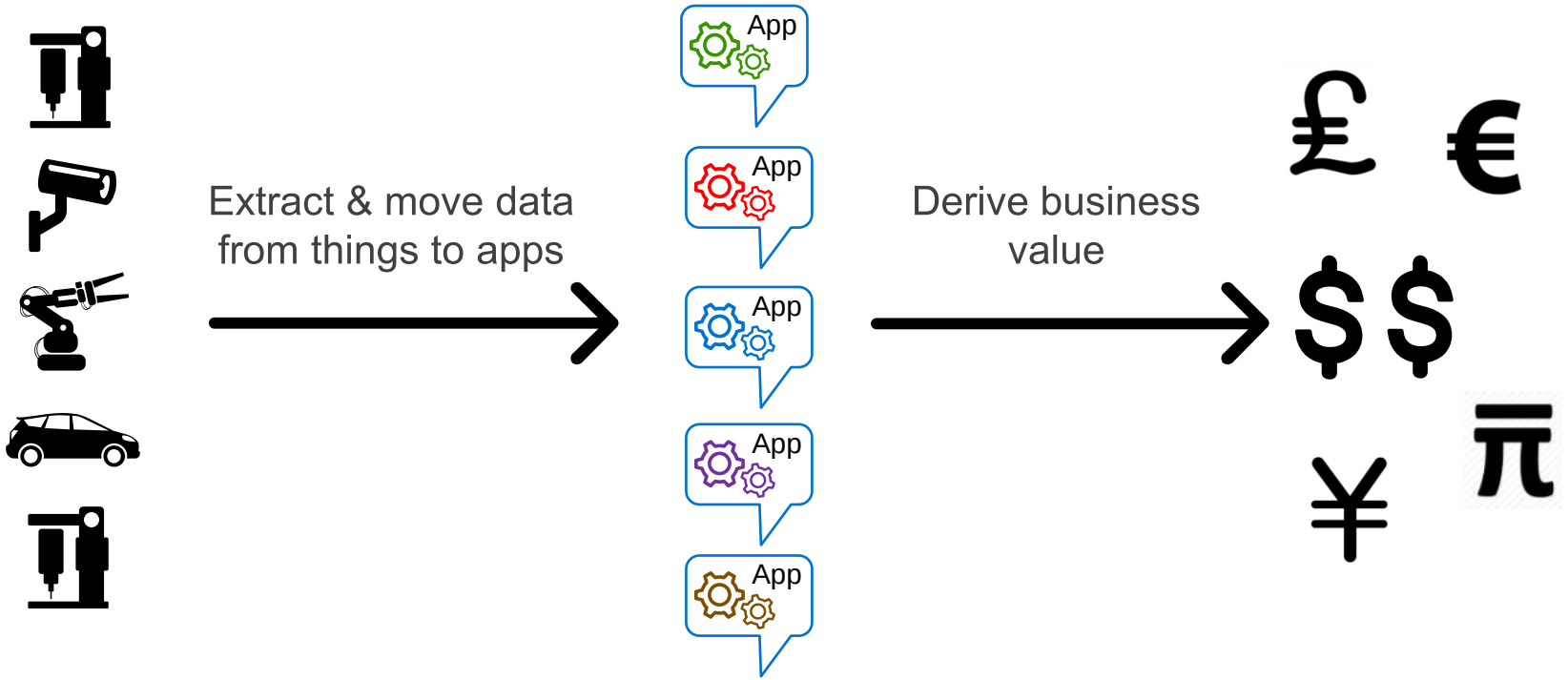
Why Most IoT Projects Fail

- People & Culture
  - Poor collaboration between IT, OT and the Business
  - Culture that focuses too much on technology
  - Lack of expertise
- Process – Going it Alone
  - What looks good on paper proves to be too difficult to implement
    - Time, expertise, data quality, Integration efforts, Budget
  - Successful projects engage the partner ecosystem throughout
- Tie Success with the Business
  - Customer satisfaction, Operational Efficiency, Improved product/service, Increased Profits

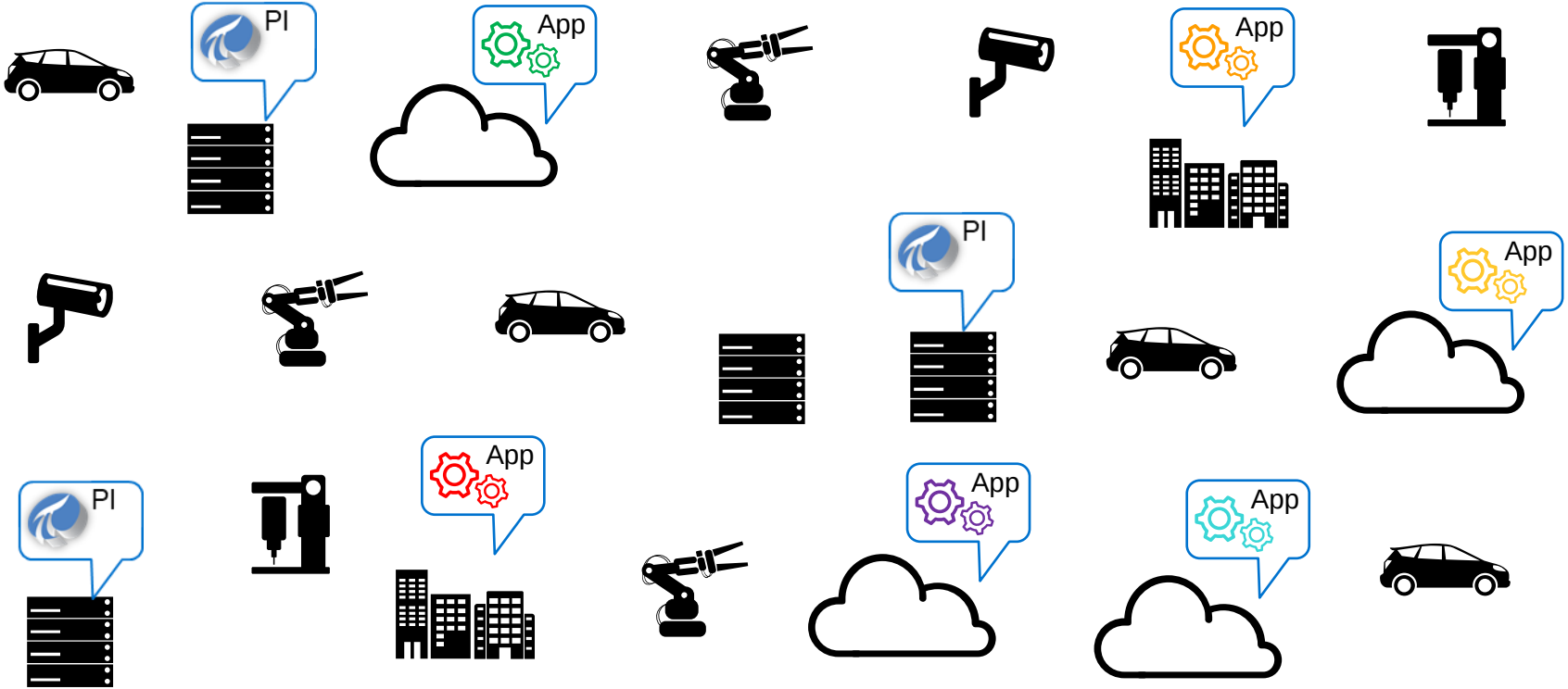
A Successful IoT Framework… From a Technology Perspective

- Provide tools and systems that are Easy, “Operational-Centric” not IT-Centric
- Don’t go it alone – develop an ecosystem and data layer that is cross-platform and cross-industry
- Industry standards and Open standards – make it easy to integrate
- Make it easy to extract real value from the solution
- Keep it simple

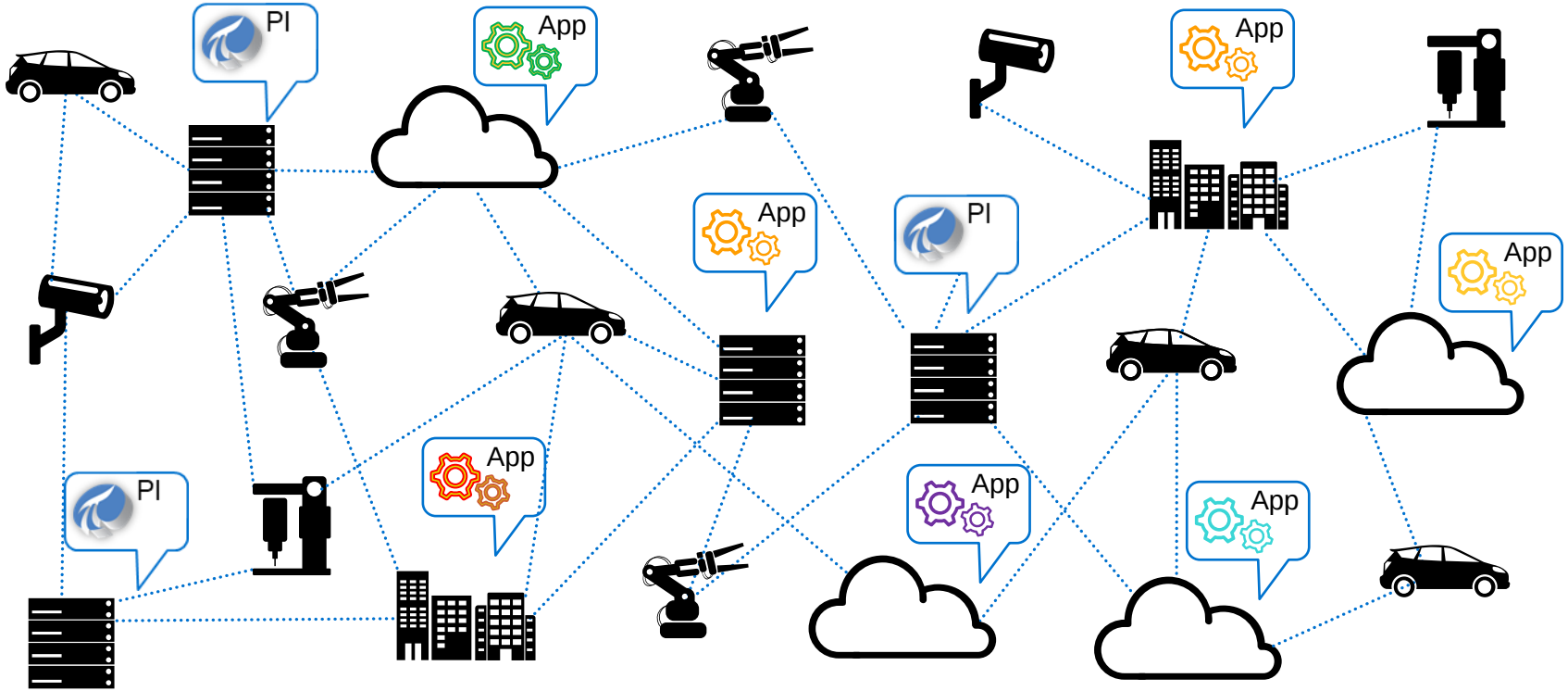
To get value from data



Customer are challenged!



Cisco Intent-Based Network is needed



But customer challenges remain…

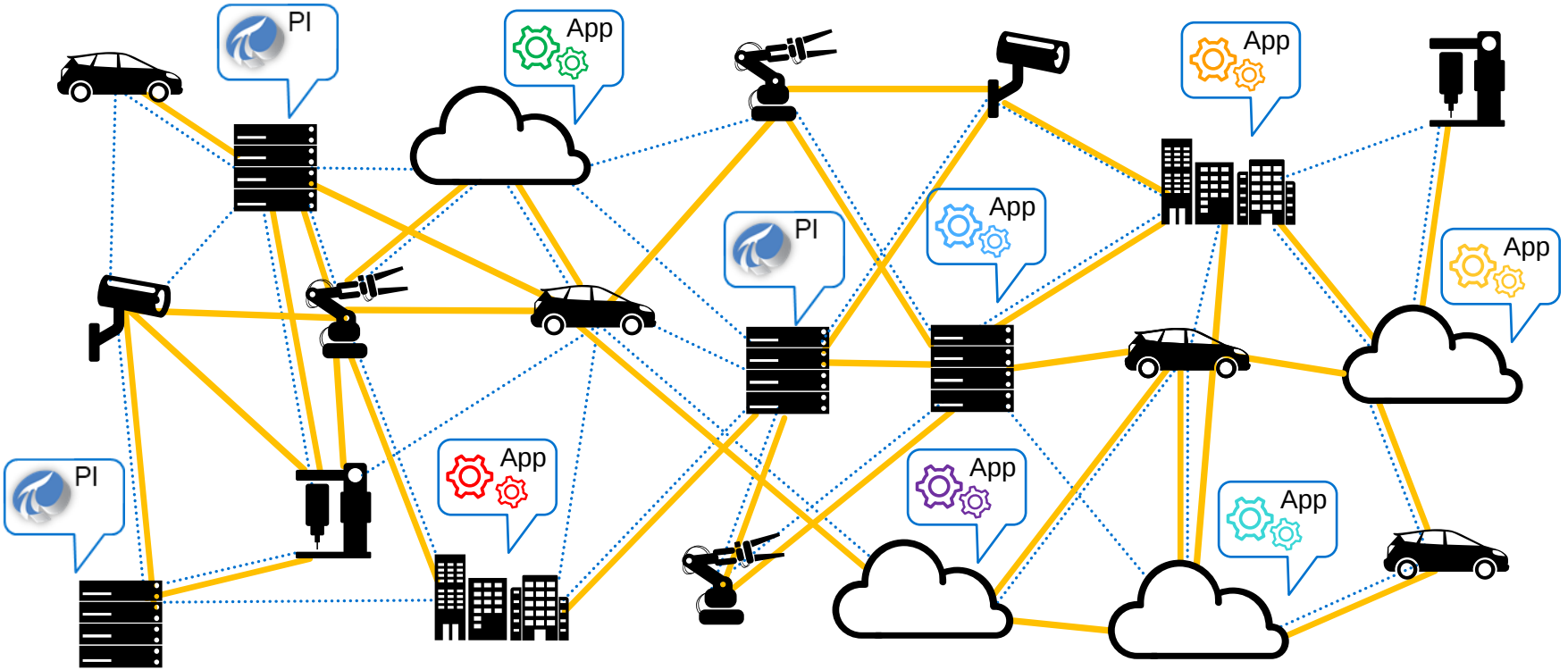
- ✓ Complexity of connecting, securing and managing a set of diverse devices
- ✗ A lot of data remains locked inside its sources
- ✗ No programmatic way to move the *right data* to the *right apps* at the *right time*
- ✗ No programmatic way to enforce ownership, privacy, and security policies

Cisco Intent-Based Network

PI System + Cisco Kinetic + Cisco IOx

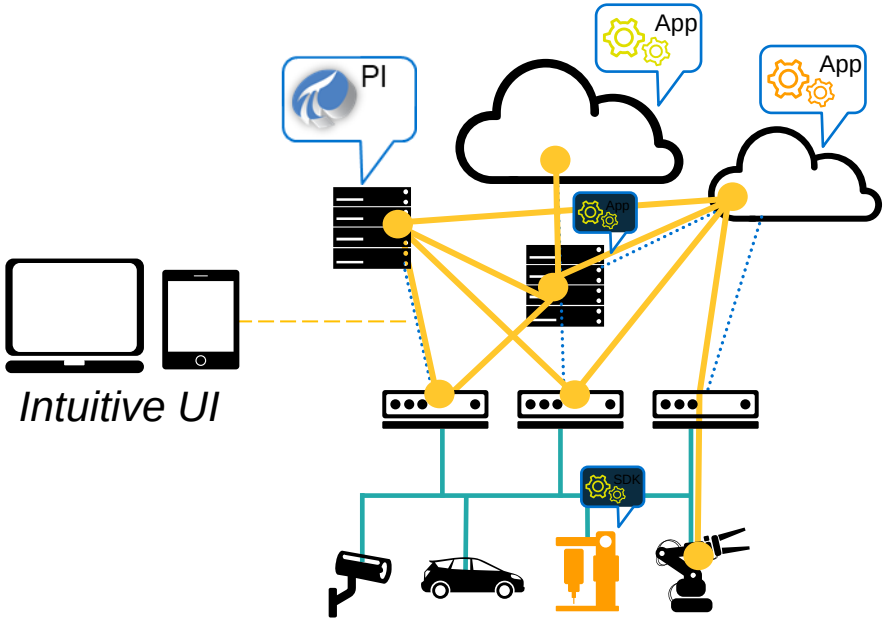
An IoT data fabric is needed

extract data, compute data, move data



Cisco Kinetic

A system of software that runs across distributed nodes of end points, network, edge, data centers, and clouds



Extracts data

Programmatically moves data

Enforces ownership, privacy, security

Computes data in optimal location

Provides ‘data API’ for App developers

Architecture

Cisco End-to-End Integrated Framework

Connectivity Extended to Devices

Cisco IR829 router
Cisco IOx (Linux)

Cisco IR809 router
Cisco IOx (Linux)

PI Connector (Linux)

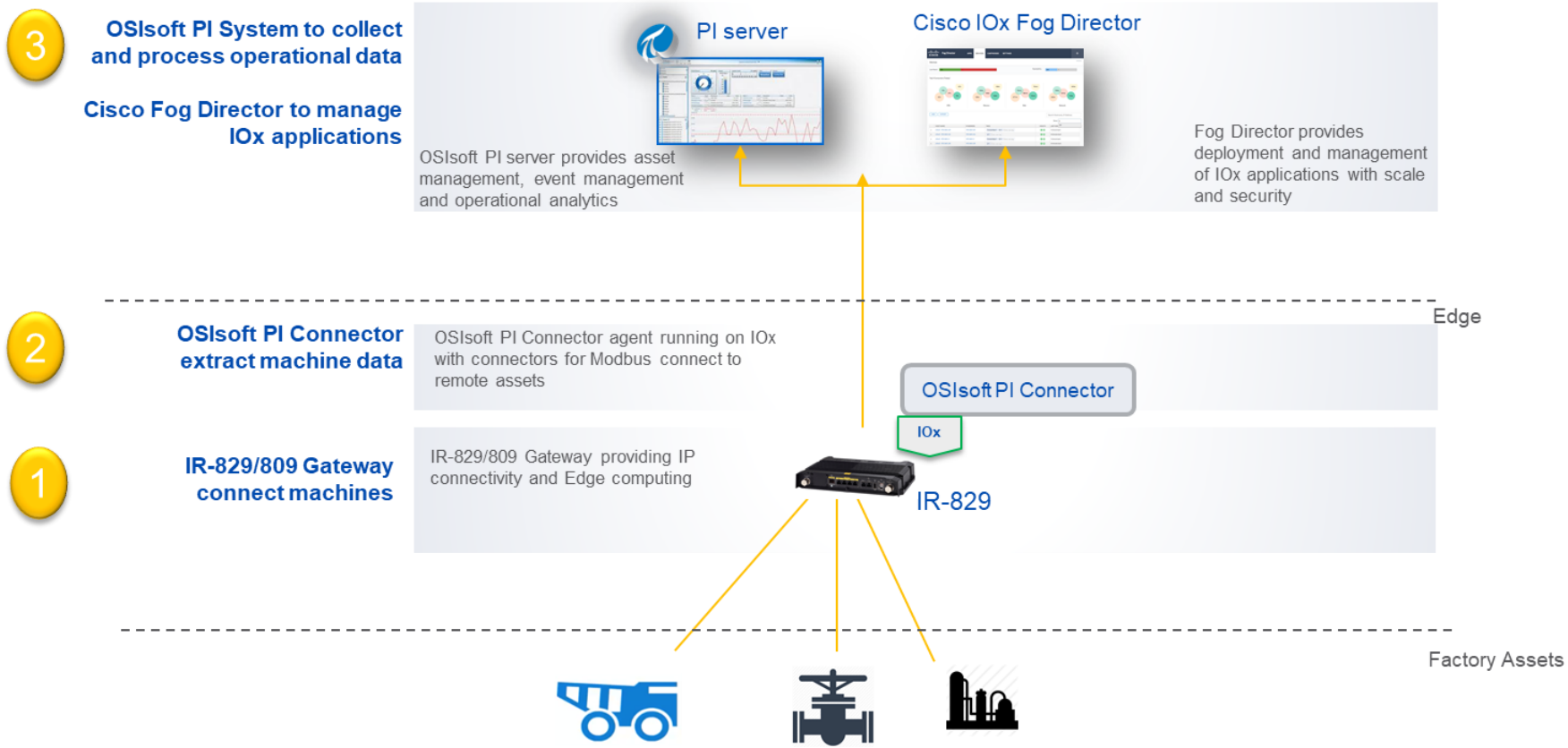
PI Connector (Linux)

PI Connector (Linux)

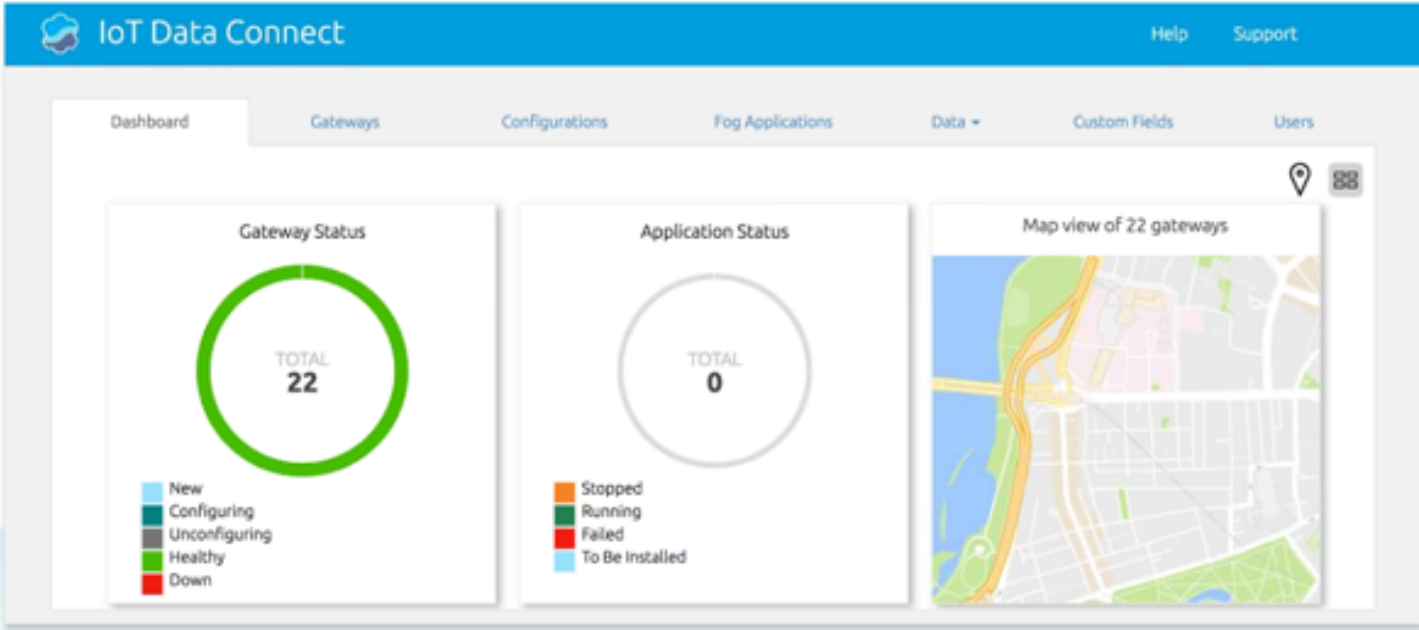
PI Connector Relay

Enterprise PI Server

Connect and Monitor: Cisco and OSIsoft Solution



Cloud Managed Cisco Industrial Routers 8x9



- Cloud-based Gateway Management
- Zero Touch Deployment
- Intuitive User Interface
- Gateway Monitoring
- Policy based configurations
- Application Lifecycle Management

Customer Use Cases

Pipeline Monitoring

COMPANY and GOAL

Natural Gas Pipeline and Storage Company

Goal: Improving system reliability with real-time predictive analytics

TransCanada

CHALLENGE

Large geographical footprint with diverse communication architecture

- Maintain 15,341 miles of pipeline covering 17 states
- Eliminate data gaps
- Require scalable solution for over 3,000 potential sites

SOLUTION

Deploying PI Connector on Cisco IR-829 with Iox using Fog Director

- Locate data buffering at the edge
- Common configuration for scalable solution
- Hardened device for harsh environments

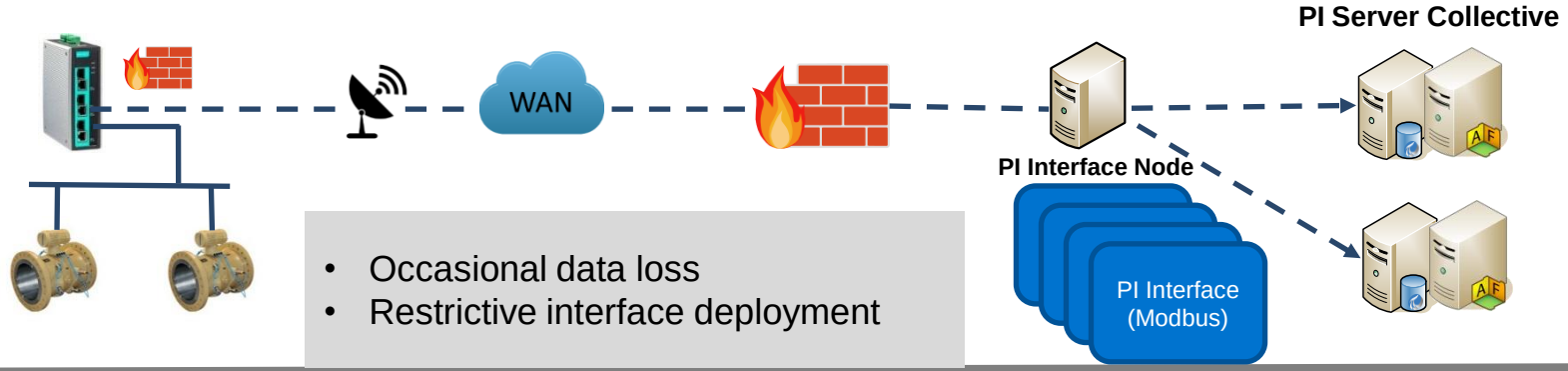
RESULTS

Early detection of potential meter and gas quality issues

- Reduced data loss
- Improved bandwidth utilization
- Cellular backup connectivity

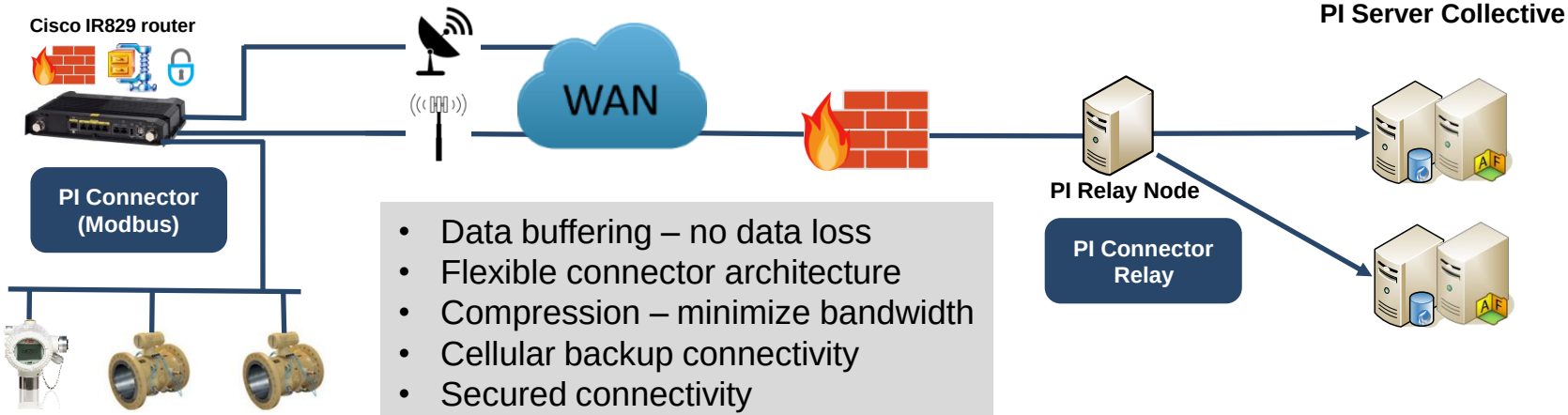
TransCanada Extends PI System Connectivity to the Edge

Before



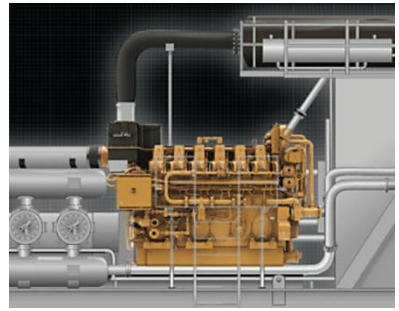
- Occasional data loss
- Restrictive interface deployment

After



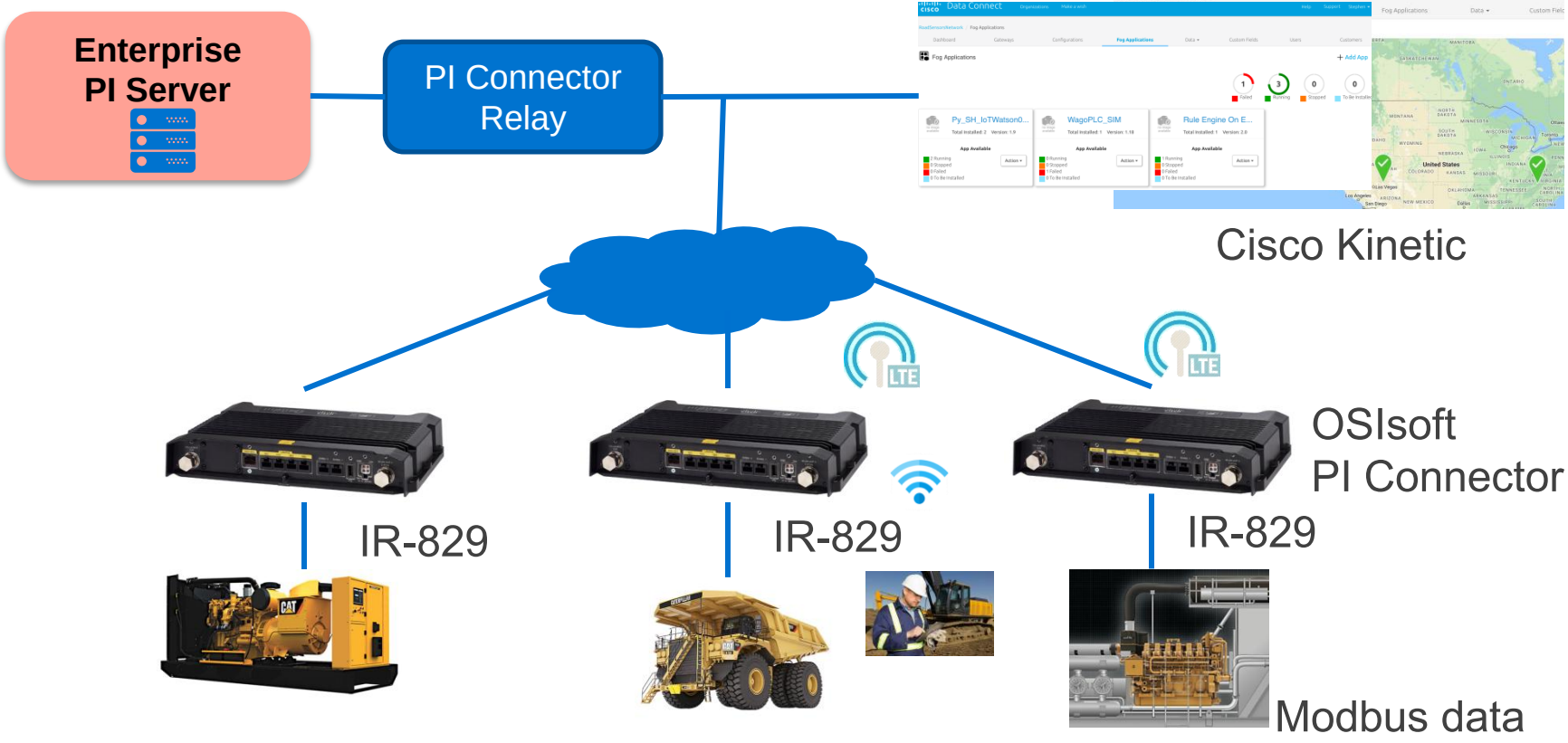
- Data buffering – no data loss
- Flexible connector architecture
- Compression – minimize bandwidth
- Cellular backup connectivity
- Secured connectivity

Cat Power Systems



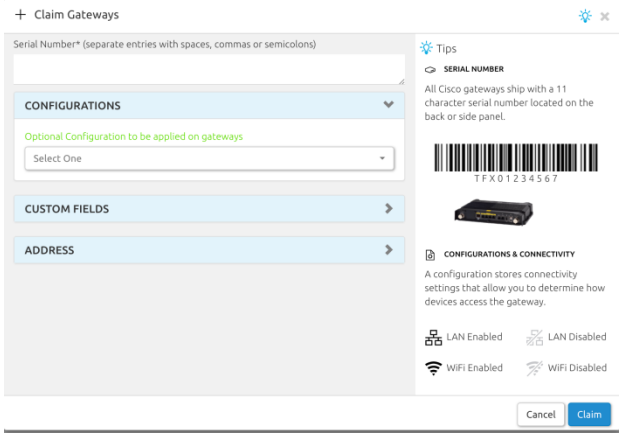
- Engine Natural Gas Compressor data via Modbus protocol
- Replace industrial PC with Cisco IR-829 LTE/WiFi Router & Cisco IOx
- OSIsoft PI Modbus interface runs within IOx to send data to PI analytics server

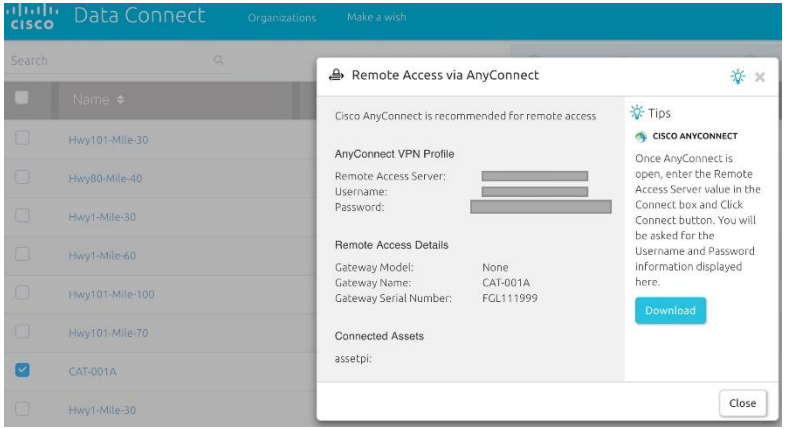
System Architecture



Solution Benefits

- Less Hardware-> Greater Uptime
- Integrates with OSIsoft ecosystem
- Fast onboarding & management of installations via Cisco Kinetic
- Secure VPN remote access to connected devices and PI Connector





Vehicle Reliability Monitoring

COMPANY and GOAL

- Public transportation system in Davis
- Fleet of 50 Natural Gas Buses
- All drivers/supervisors are students

UCDAVIS

CHALLENGE

- 142 road service calls over on ~50 buses last year
- Disruption of service
- Potential safety incidents

- Many unplanned stoppages
- Customer inconvenience
- Stranded riders could potentially get in to dangerous traffic situations

SOLUTION

- Install on board monitoring infrastructure to feed a PI System
- Create a dashboard that shows the real-time location/attributes of the bus

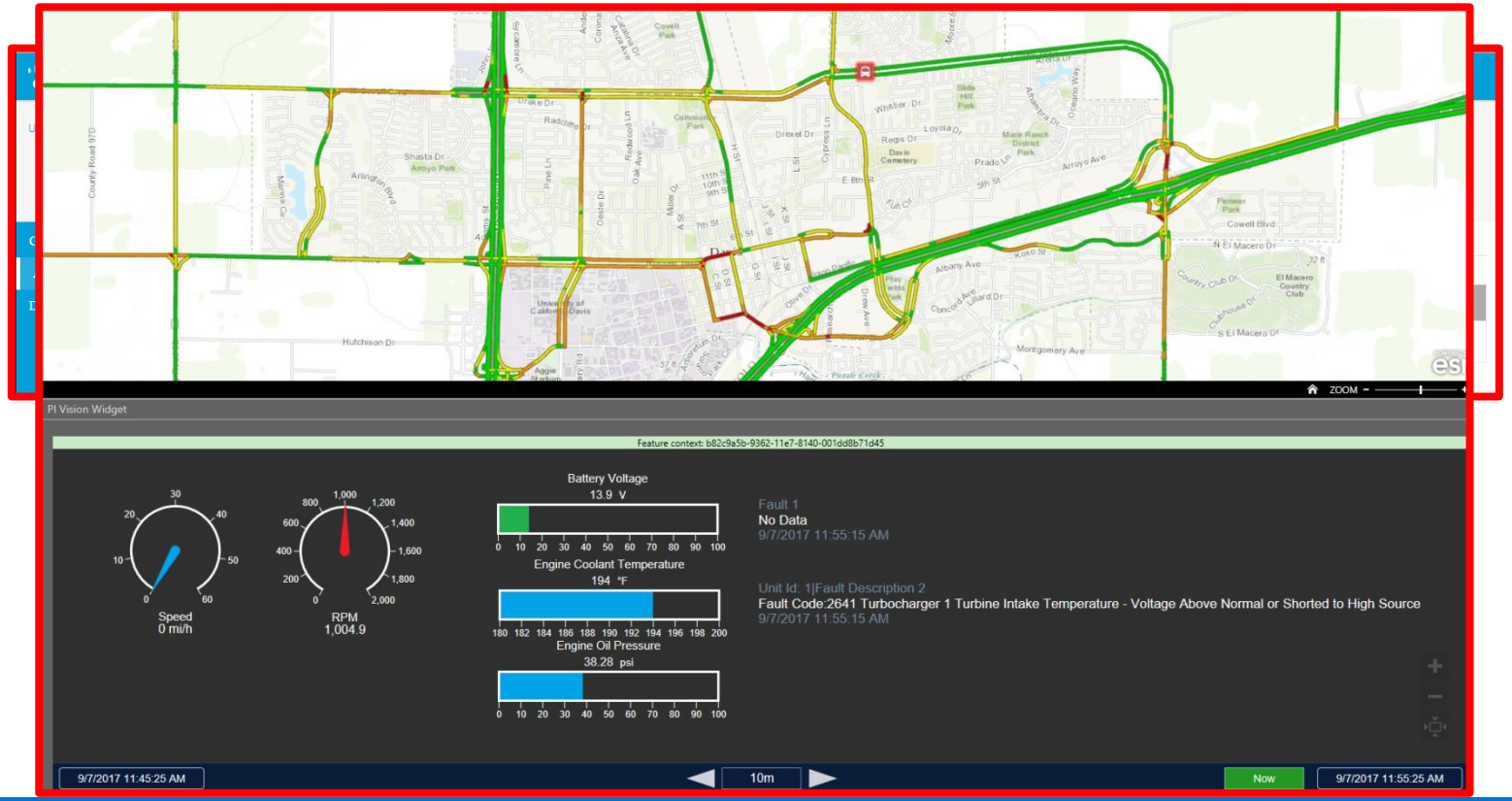
- Cisco IR-829 Router with 4G-LTE
- PI Connector for Modbus
- PI Vision Display
- Esri ArcGIS Integration

RESULTS

- Monitor buses in real time
- Collect attributes that can help maintain the buses
- Engine data, fault codes, GPS
- Visualize the data to help the maintenance team

- Near real-time feedback
- Identified several “false positives”
- Reduction in non-required service

Simple Configuration with Cisco IoT Data Connect
- Dashboards integrate real-time data and Geospatial context

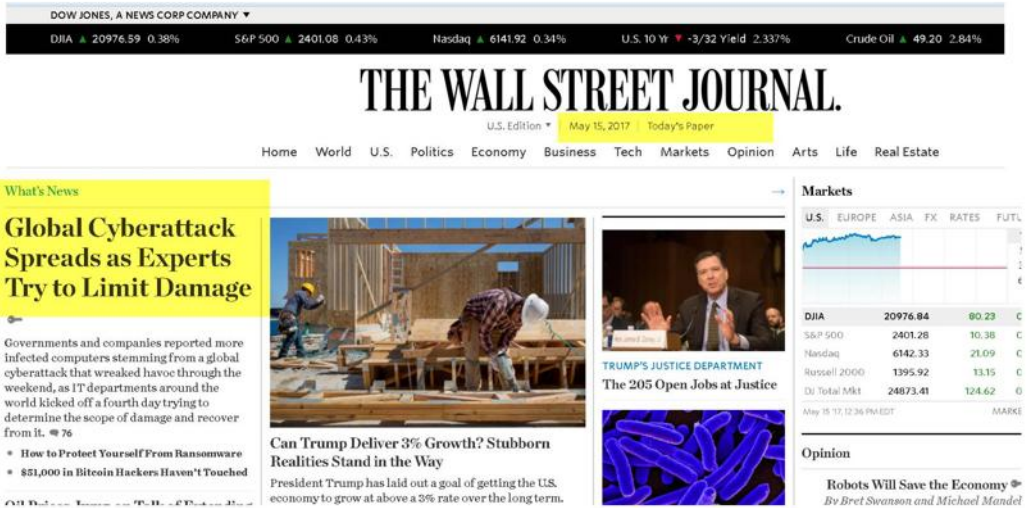


IoT and Security

Anatomy of an Attack [video removed]

Recent Events: Friday May 10, 2017

While much is known, the situation is still active and tenuous, affecting many organizations the world over, reportedly including **major telco's**, **hospital systems** and **transportation providers** such as FedEx. The attack has purportedly spread to **230,000 computers across 150** countries around the world.


DOW JONES, A NEWS CORP COMPANY

DJIA 20976.59 0.38% | S&P 500 2401.08 0.43% | Nasdaq 6141.92 0.34% | U.S. 10 Yr -3/32 Yield 2.337% | Crude Oil 49.20 2.84%

THE WALL STREET JOURNAL.

U.S. Edition | May 15, 2017 | Today's Paper

Home World U.S. Politics Economy Business Tech Markets Opinion Arts Life Real Estate

What's News

Global Cyberattack Spreads as Experts Try to Limit Damage

Governments and companies reported more infected computers stemming from a global cyberattack that wreaked havoc through the weekend, as IT departments around the world kicked off a fourth day trying to determine the scope of damage and recover from it.

- How to Protect Yourself From Ransomware
- $51,000 in Bitcoin Hackers Haven't Touched

Can Trump Deliver 3% Growth? Stubborn Realities Stand in the Way

President Trump has laid out a goal of getting the U.S. economy to grow at above a 3% rate over the long term.

TRUMP'S JUSTICE DEPARTMENT

The 205 Open Jobs at Justice

Markets

U.S. EUROPE ASIA FX RATES

DJIA	20976.84	80.23
S&P 500	2401.28	10.38
Nasdaq	6142.33	21.09
Russell 2000	1395.92	13.15
DJ Total Mkt	24873.41	124.62

Opinion

Robots Will Save the Economy

By Bret Swanson and Michael Mandel

WannaCry virus forces Honda car plant to ha delaying production of 1,000 vehicles

Why Most IoT Projects Fail

- PIT-Focused Attack: Target / Home Depot…
  - No stores were shut down
  - No customers were refused
  - No sales were impacted
  - Yet the cost of the Target breach is now beyond $300 Million

- OT-Focused Attack: German Steel Plant…
  - Factory damaged – automation destroyed
  - No personal injuries reported
  - $20-30 Million in direct damage to plant process equipment
  - Plant still shut down – ultimate cost ???

Enterprise Network Security Trends

63M

new devices

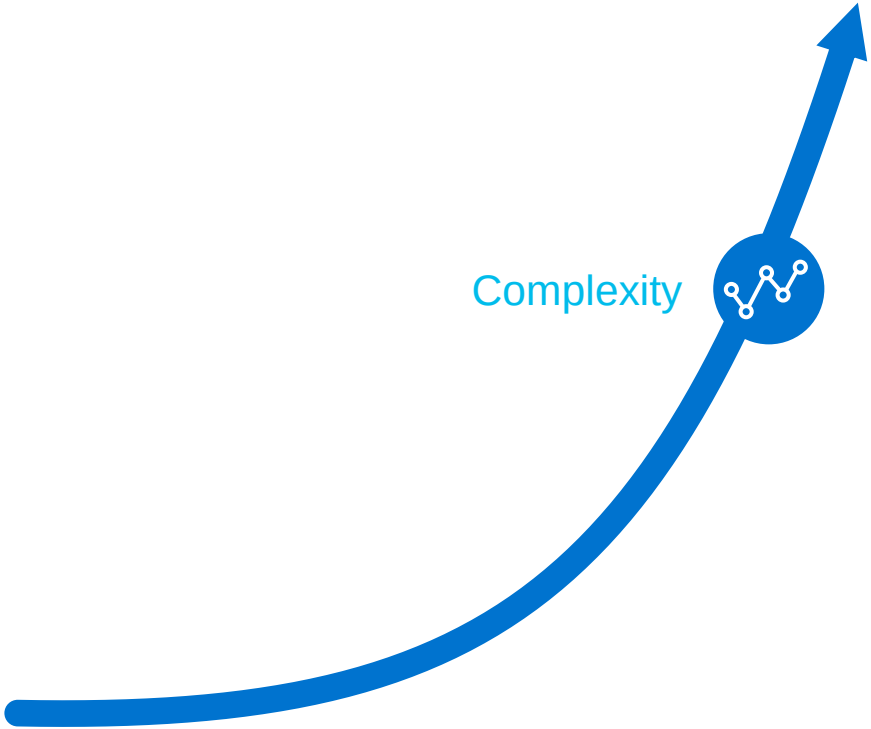
attaching to enterprise networks **per second** in 2020

Attacks take

100 days

to resolve

on average



Enterprise Network Security Trends

Advanced attacks take

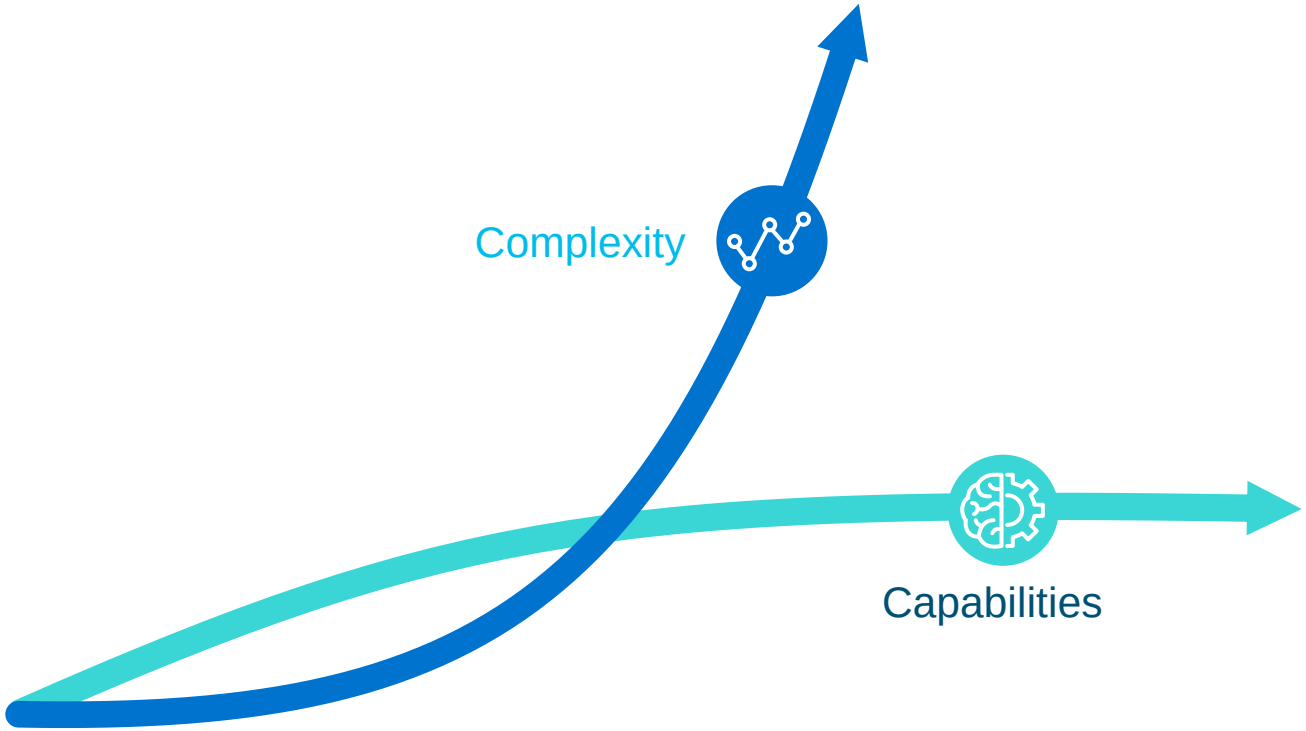
170 days

to detect

76%

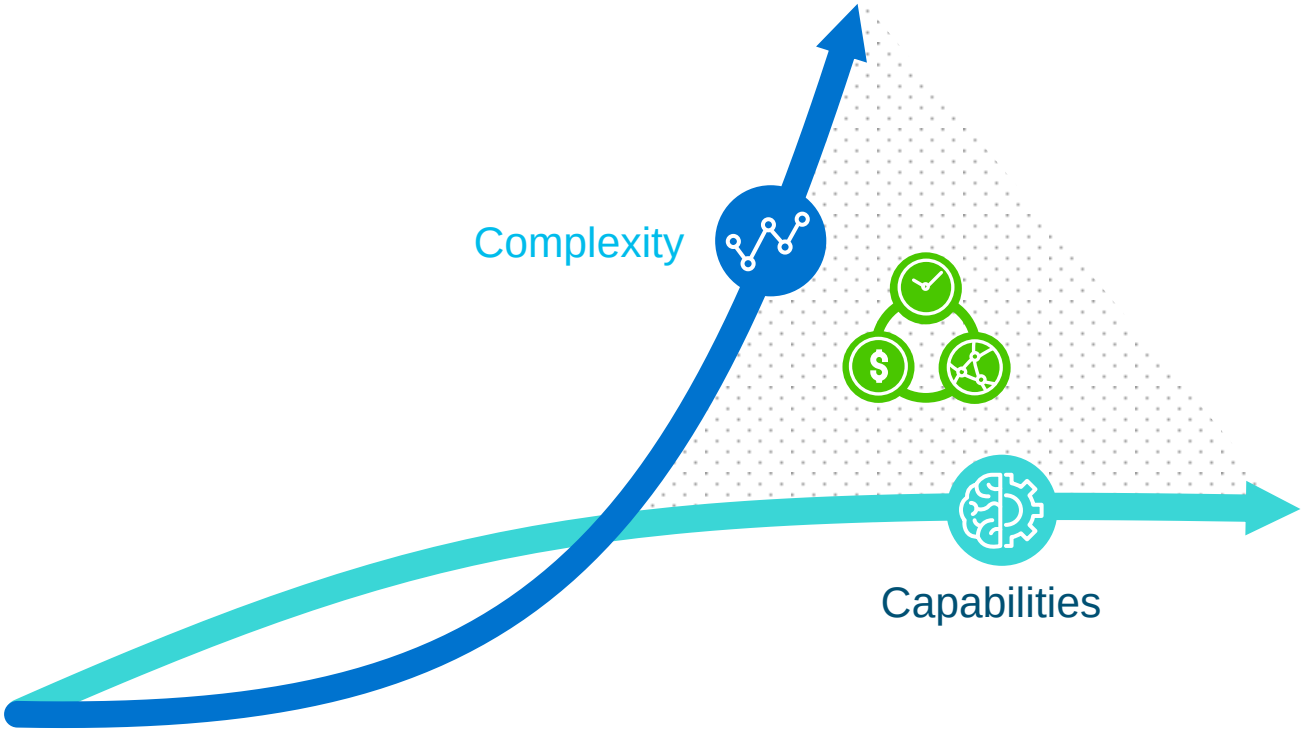
of IT professionals

say a **lack of visibility** is their **biggest challenge** in addressing network threats



Enterprise Network Security Trends

The average total cost of a single data breach is $4M



Cisco Enterprise Network Security

Trustworthy Systems

Security embedded into hardware and software by design

Network as a Sensor

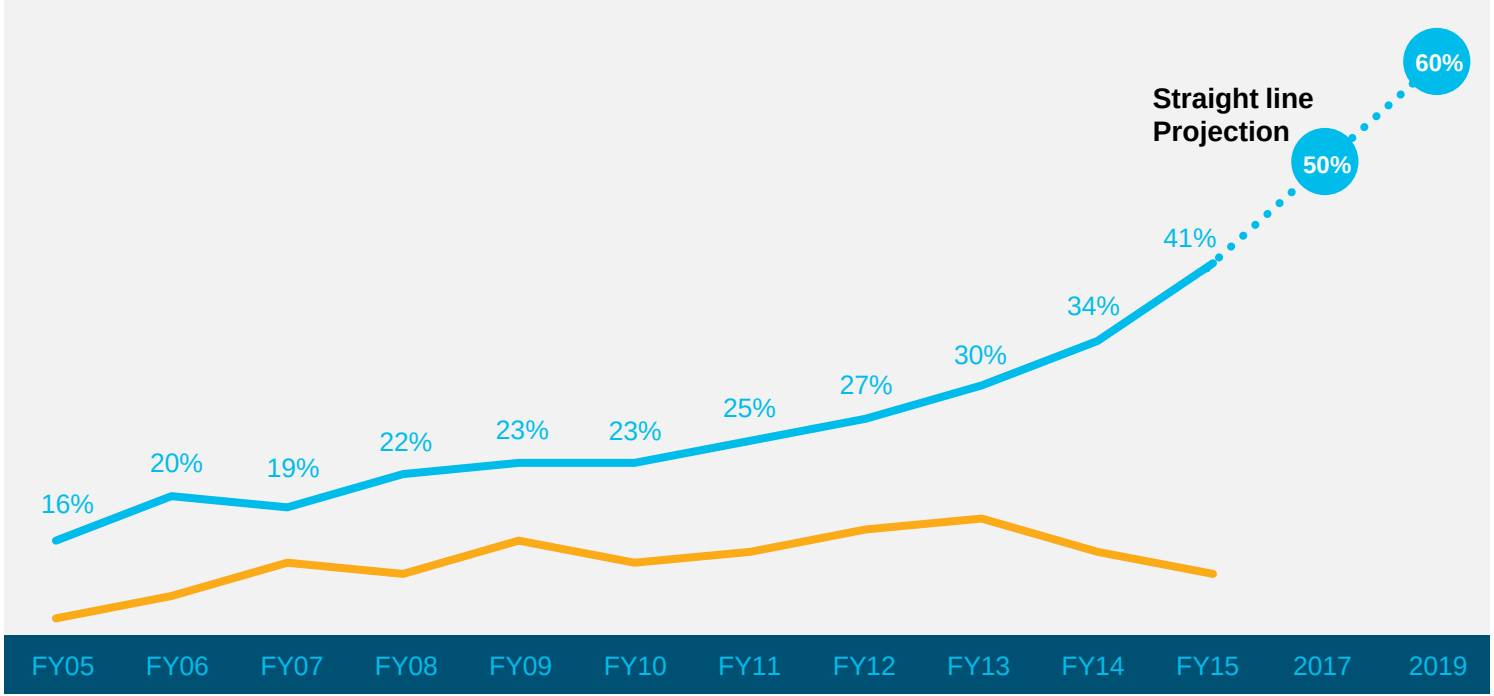
Visibility and analytics across the extended enterprise, industry-leading threat intelligence

Network as an Enforcer

Consistent threat protection and remediation across the network

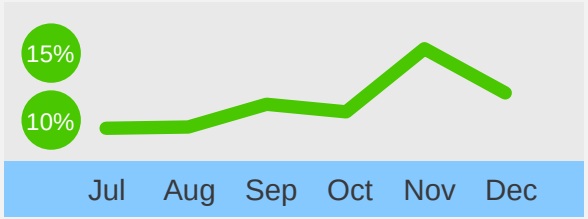
Secure your digital network in real-time, all the time, everywhere

Encryption Is Changing The Threat Landscape



Source: Thales and Vormetric

Network Threats Are Getting Smarter … And Finding Ways To Stay Hidden



Based on Cisco ThreatGrid Analysis

81% Organizations have been victims of a cyber attack

41% Attackers used encryption to evade detection

64% Cannot detect malicious content in encrypted traffic

200days Industry Average Detection Time for a Breach

60days Industry Average Time To Contain a Breach

$3.8M Average cost of a data breach

New Attack Vectors:

Employees browsing over HTTPS: Malware Infection, Covert channel with C&C server, Data exfiltration

Employees on internal network connecting to DMZ servers: Lateral propagation of encrypted threats

Enhanced Network as a Sensor

Industry’s first network with ability to find threats in encrypted traffic **without decryption**

Avoid, stop or mitigate threats faster then ever before | Real-time flow analysis for better visibility

IoT Security Best Practices

- Educate & Enforce Security Policies
- Defense in depth: A firewall, airgap, etc., isn't enough
- Identify & profile all network devices – wired & wireless
- Segment & Isolate: VLAN & DMZ. North-South, East-West
- Secure the edge: VPN, Remote Access, industrial Firewalls
- Multi-faceted approach: Secure DNS, Identity Services, Secure assets on and off the corporate network, Treat corporate and industrial equally.
- Obscurity is not a defense: Industrial protocols are a target
- Secure older SCADA systems: Older systems very "hackable"

Take Aways

- Projects have a high degree of success
- Relatively short time get lab and field trials completed
- Use Cases build upon capabilities that you already understand
- Build security into the solution from the beginning.
- Don’t try to boil the ocean.
  - Quick wins
  - Clear ROI
  - Don’t go it alone

Stephen Friedenthal
stfried@cisco.com
IoT Solution Architect
Cisco Systems, Inc.

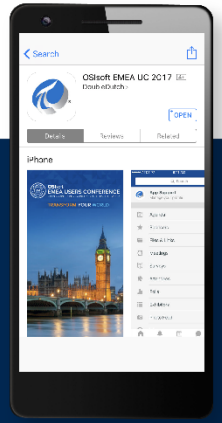
Questions

Please wait for the **microphone** before asking your questions

State your **name & company**

Please remember to…

Complete the Online Survey for this session



Download the Conference App

- View the latest agenda and create your own
- Meet and connect with other attendees

Search **OSIsoft** in the app store

Download on the App Store

GET IT ON Google Play

HTML