Splunk as a Platform for Operational Intelligence In SCADA and other Industrial Systems

Brian Gilmore

Solution Expert, IoT and Industrial Data

Splunk

splunk>

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not, be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

Big Data Comes From Machines …

Volume | Velocity | Variety | Variability

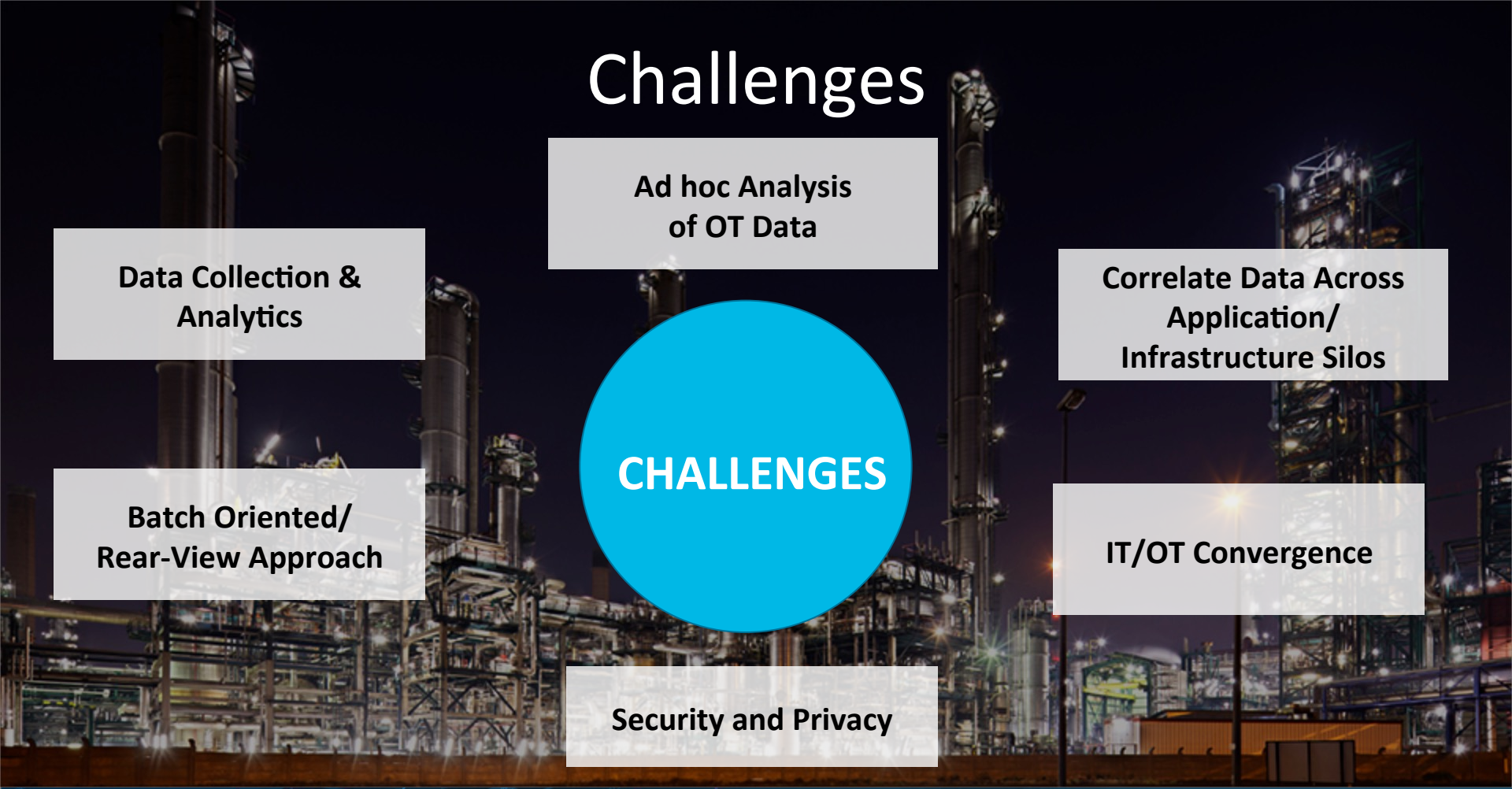
GPS,
RFID,
Hypervisor,
Web Servers,
Email, Messaging,
Clickstreams, Mobile,
Telephony, IVR, Databases,
Sensors, Telematics, Storage,
Servers, Security Devices, Desktops

… Including From Operational Technology (OT)

Volume | Velocity | Variety | Variability

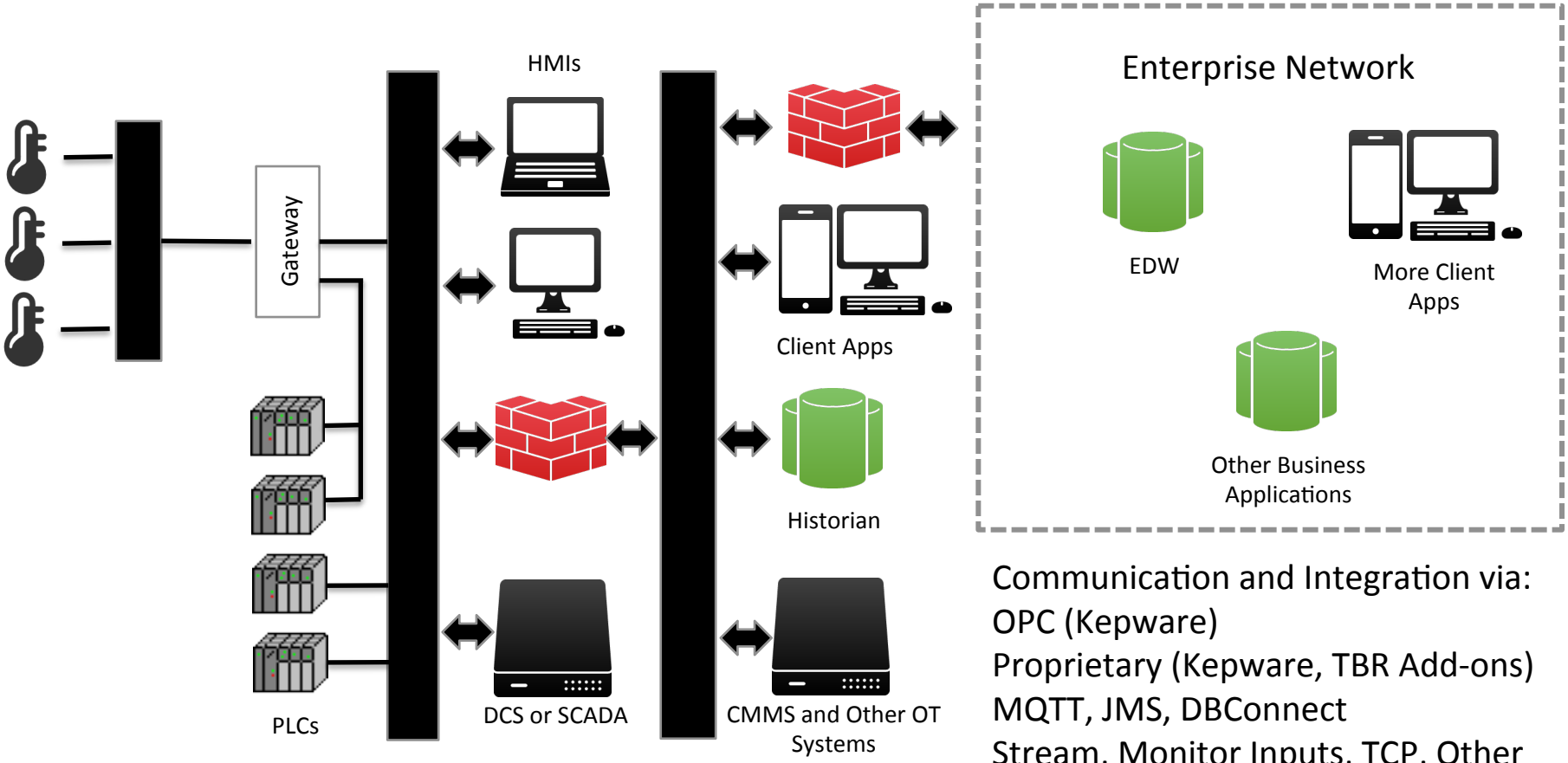
Sensors, Pumps,
GPS, Valves, Vats,
Conveyors, Pipelines, Drills,
Transformers, RTUs, PLCs, HMIs,
Lighting, HVAC, Traffic Management,
Turbines, Windmills, Generators, Fuel Cells, UPS

Challenges

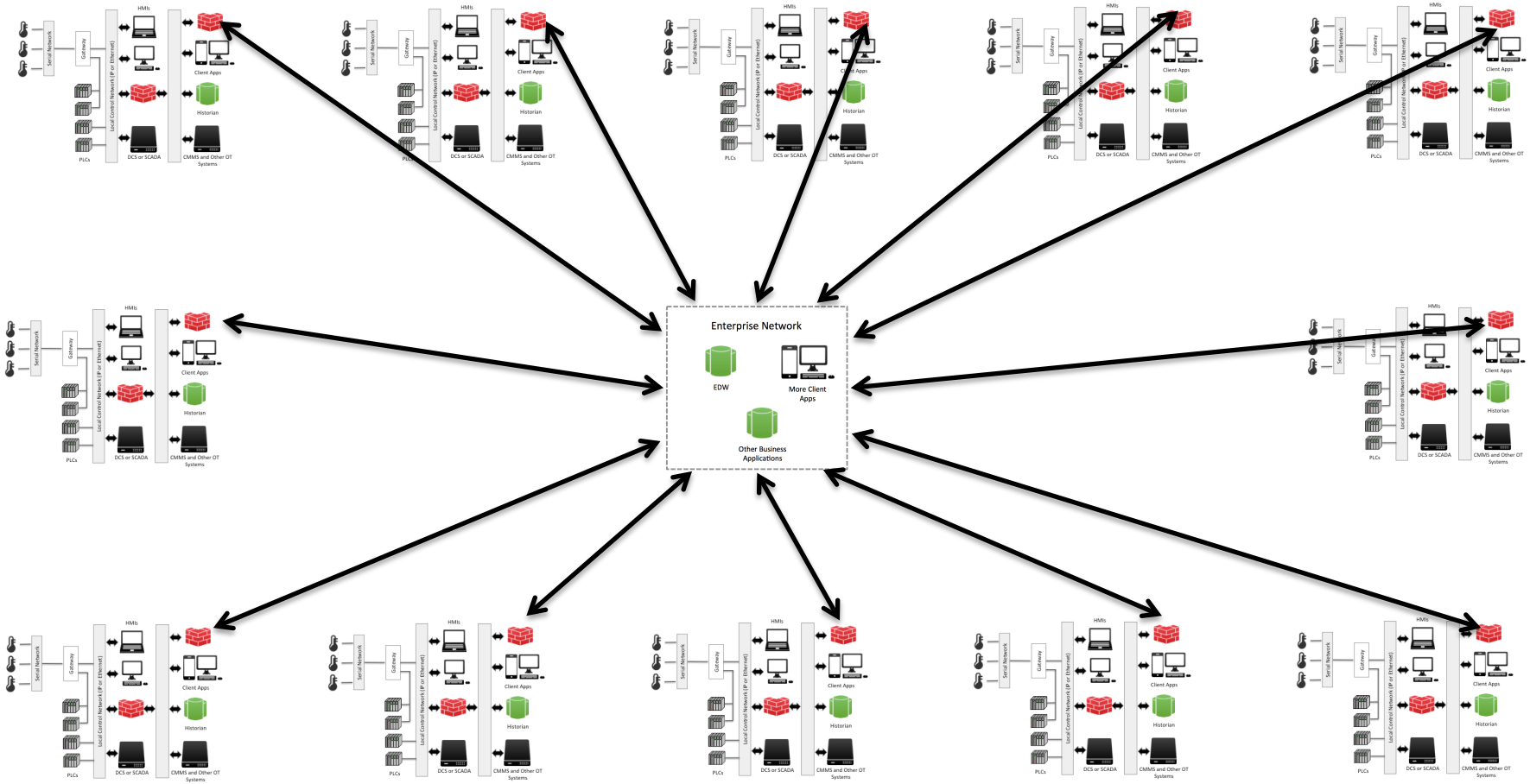

Ad hoc Analysis of OT Data
Data Collection & Analytics
Correlate Data Across Application/ Infrastructure Silos
CHALLENGES
Batch Oriented/ Rear-View Approach
IT/OT Convergence
Security and Privacy

OT Overview

splunk>



Communication and Integration via:
OPC (Kepware)
Proprietary (Kepware, TBR Add-ons)
MQTT, JMS, DBConnect
Stream, Monitor Inputs, TCP, Other


Enterprise Network
EDW
More Client Apps
Other Business Applications
HMIs
Client Apps
Historian
PLCs
DCS or SCADA
CMMS and Other OT Systems
Gateway
Serial Network
Local Control Network (IP or Ethernet)

Why Is OT Different Than IT?

≠

Critical OT Endpoints

HMI
Historian
Controllers

Engineering
Workstations

Embedded
Devices

Control System
Communication

Splunk for OT

splunk>

Leading Platform for Industrial Data

Industrial Assets

- Sensors
- Pumps
- GPS
- Valves
- Vats
- Conveyors
- Pipelines
- Drills
- Transformers
- RTUs
- PLCs
- HMIs

Core OT

- Control Systems
- Asset Management
- Connected Assets
- Security Appliances
- Network Telemetry
- Work Order Systems
- Safety Applications

Core IT

- Web Services
- Telecoms
- Servers
- Storage
- Messaging

splunk>enterprise splunk>cloud

Partner Ecosystem

Predikto

splunk> R splunk>

RBS Red Balloon Security

Ultra Electronics

+ a b l e a u

DG LOGIK

prelert

falkonry smarter IoT applications

BAYSHORE Industrial-Strength Cybersecurity

paloalto Networks

CQ CQCloud

n3n

Advanced Analytics and ML

IoT and ICS Security

Custom User Interfaces

CISCO

splunk>

amazon web services™

kepware

bluvision

ThingWorx A PTC Business

B+B SmartWorx

carvoyant Your Car. Your Data. Your API.

octoblu

xively by LogMeIn

TATA TATA Consultancy Services

ALLIED SOLUTIONS

robotron

CQ CQCloud

mds technology

CONSIST Business Information Technology

Ingest and Platforms

Services and Delivery

Fully Integrated Enterprise Platform

splunk>

Collect and Index

Industrial Assets

Consumer and Mobile devices

OT

IT

Native Inputs

SDKs and APIs

Modular Inputs

Technology Partnerships

New HTTP Event Collector

TCP
UDP
Logs
Scripts
Wire
Mobile
Java
JS
C#
Python
Ruby
PHP

MQTT
AMQP
COAP
REST
JMS
HTTP

splunk>enterprise splunk>cloud

Kepware Technologies

ThingWorx A PTC Business

xively by LogMeIn

octoblu

Search, Alert, Report and Analyze

Industrial Assets

Consumer and Mobile devices

OT

IT

Native Inputs

SDKs and APIs

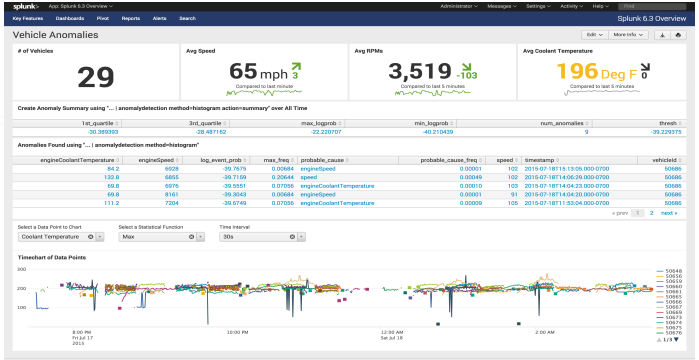
Modular Inputs

Technology Partnerships

New HTTP Event Collector

TCP
UDP
Logs
Scripts
Wire
Mobile
Java
JS
C#
Python
Ruby
PHP

MQTT
AMQP
COAP
REST
JMS
HTTP



splunk>enterprise splunk>cloud

Kepware Technologies

ThingWorx A PTC Business

xively by LogMeIn

octoblu

Enrich Industrial Data with Structured Data

ICS Tag Data

Asset ID

Tag

```
9/8/15 4:41:48.055 PM      2015-09-08 23:41:48.055 +0000 Tag="Windfarm 10.Turbine 10.Wind Direction"
Value="132.959152" AssetID="K23441gF4224" Quality="good" demo=Windfarm
host = 127.0.0.1 source = tcp:9997 sourcetype = opc 9/8/15 4:41:48.055 PM      2015-09-08
23:41:48.055 +0000 Tag="Windfarm_10.Turbine_10.Temperature" Value="19.3928394" Quality="good"
demo=Windfarm host = 10.7.102.1 source = tcp:9997 sourcetype = opc 9/8/15  4:41:48.055 PM
2015-09-08 23:41:48.055 +0000 Tag="Windfarm_10.Turbine_10.Statc" Val
Quality="good" demo
host = 127.0.0.1 source = tcp:9997 sourcetype = opc
9/8/15
```

Host

Tag Value

Tag Quality

Workorder, Asset Databases

Asset ID	Technician	Date Serviced	Part Number	Lot Number
✓	50446	9/7/15	1224-56-A	B00747

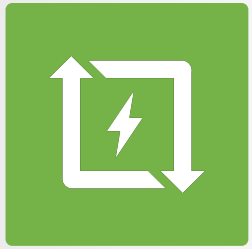
Asset ID	Location
✓	Site 7

Location	Latitude	Longitude	Site ID	Address Line 1
Site 7	39.11515	84.45651	A345	409 Park St.

Demo

Key Takeaways

Secure data collection across different formats, protocols and connectivity options



Scalable time-series storage of sensor, diagnostic and transactional data

Search, ad hoc correlations and powerful analytics across OT and IT data

Real-time dashboards and reporting

THANK YOU

splunk>