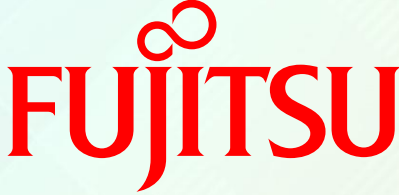


SILICON VALLEY

 In-Memory  
Computing | SUMMIT  
2017

 FUJITSU

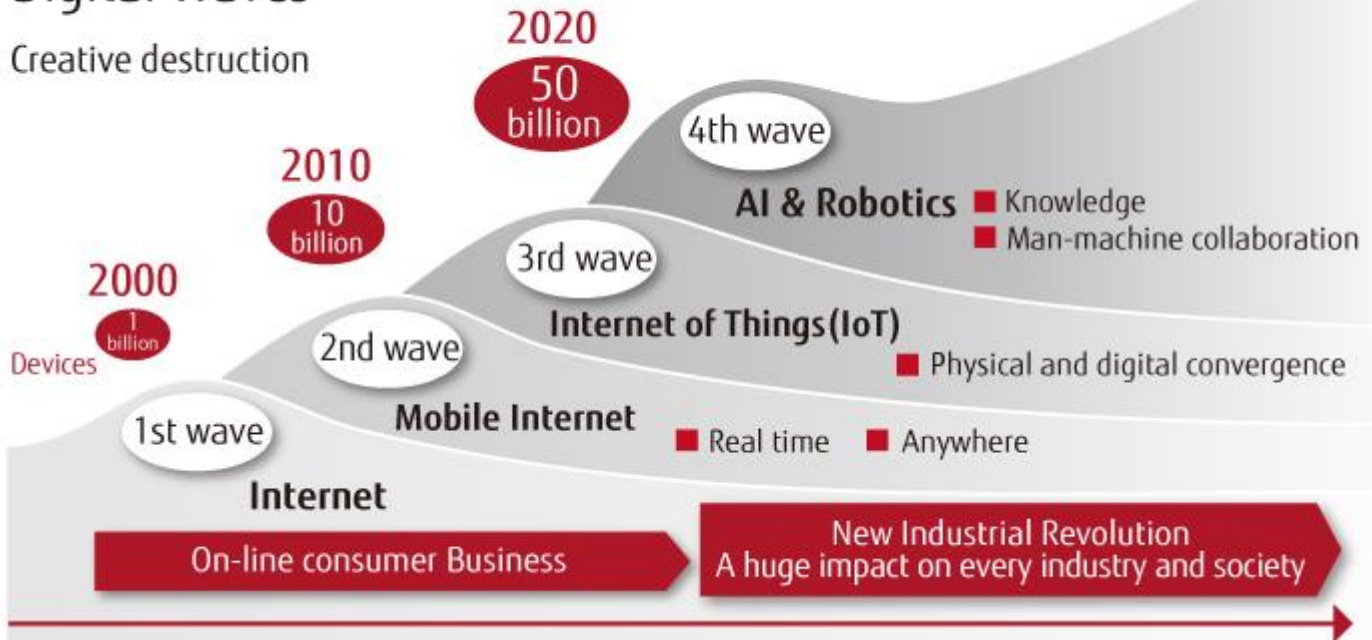
# Moving Forward Securely in Digital Factory

Ferhat Hatay  
Director of Strategy and Innovation  
Fujitsu Technology and Business of America

# The Business of the Future is Digital

## Digital Waves

Creative destruction

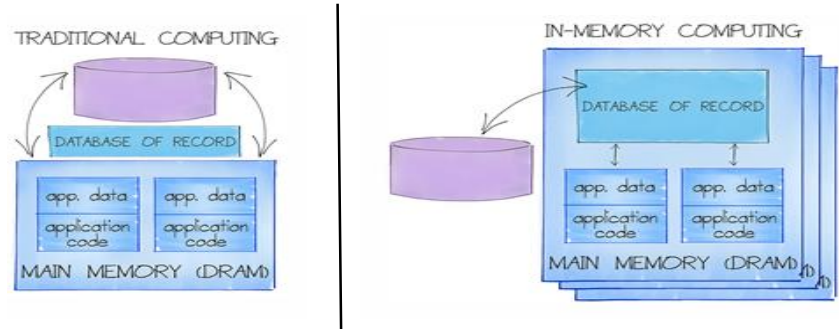


<http://journal.jp.fujitsu.com/en/2016/01/12/01/>

# Data and Analytics Forecast: Cloudy and Edge-y

- Internet of Things fueling the new 'Industrial Internet'
- Data stream through edge and cloud!
- Embedded analytics is the new BI
- Real-time interactions and analytics
  - Businesses need insights NOW!
- In-Memory Computing
  - Access data at memory speed
  - Accelerators: GPUs, FPGAs, CPUs too!

- In-Memory Analytics @ Scale
  - Terascale problems
  - Performance and scalability
  - SaaS and Cloud
  - Cognitive computing



# Silicon Challenge: Go High Performance Go Low Power

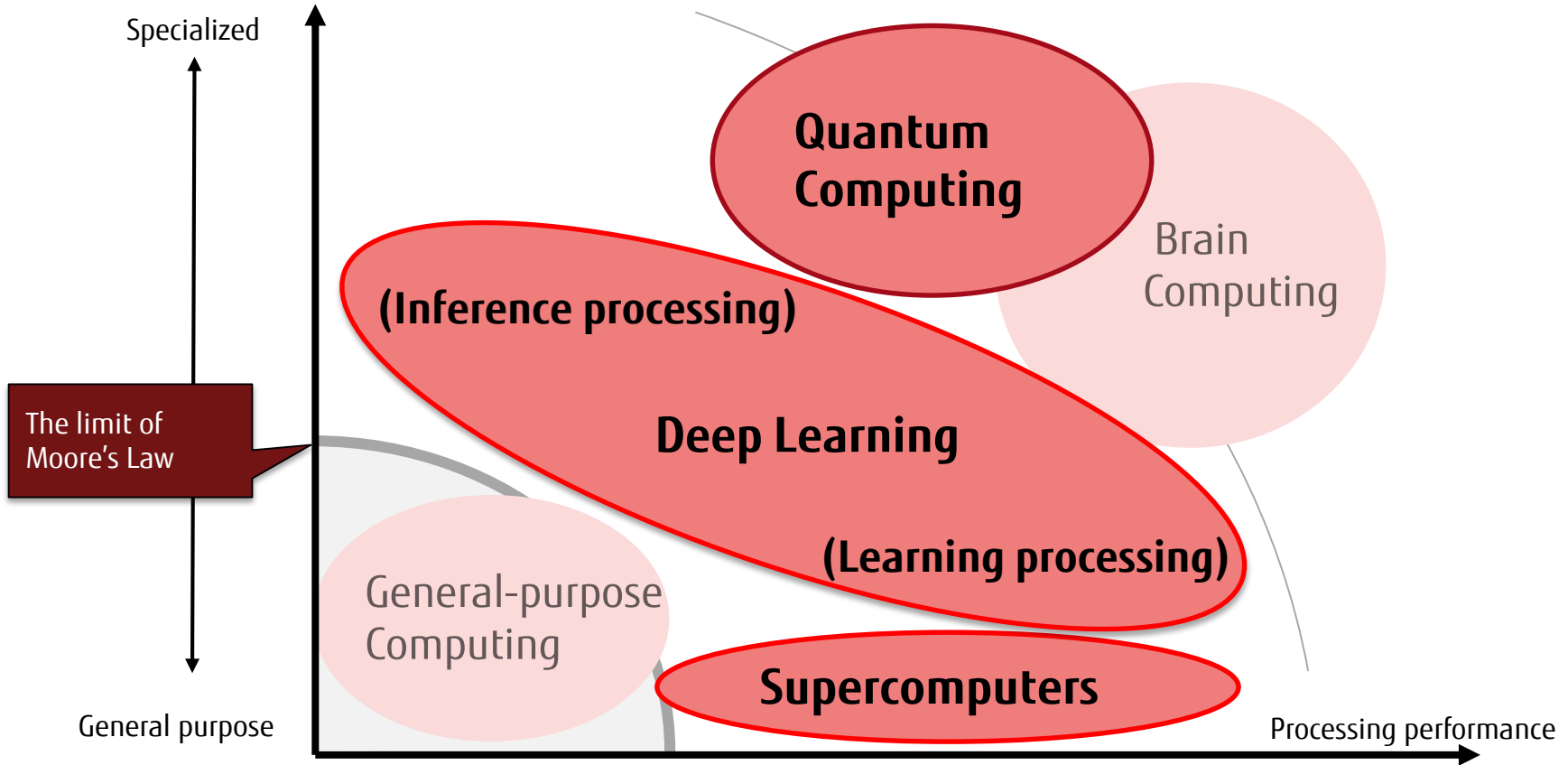
Orders! of magnitude improvements needed  
on **Performance/Watt** for Deep Learning



- More transistors
  - State of the art 0-0-0
  - Many Execution Units/\$
- Higher Frequency

- Less transistors
  - Less control logic
  - Fewer Execution Units/\$
- Lower Frequency

# New Computing Architecture for Deep Learning



# Three technologies accelerates

Solve combinational optimization problems

Quantum  
Computing

Three world-class cutting edge technologies will combine to contribute to business expansion for customers

Simulation and pre-processing

HPC

High-speed learning environment

Deep  
Learning

# What's the New Architecture for the DLU?

## ■ Domain Specific, Optimal Precision, and Massively Parallel

### Conventional Architecture

General Use

Complicated 0-0-0 cores

High Precision

Double/Single precision FP

Sequential + Parallel

Multiple strong cores



### New Architecture

Domain Specific

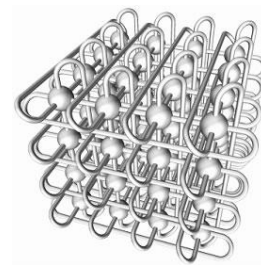
Domain specific cores

Optimal Precision

Deep Learning Integer

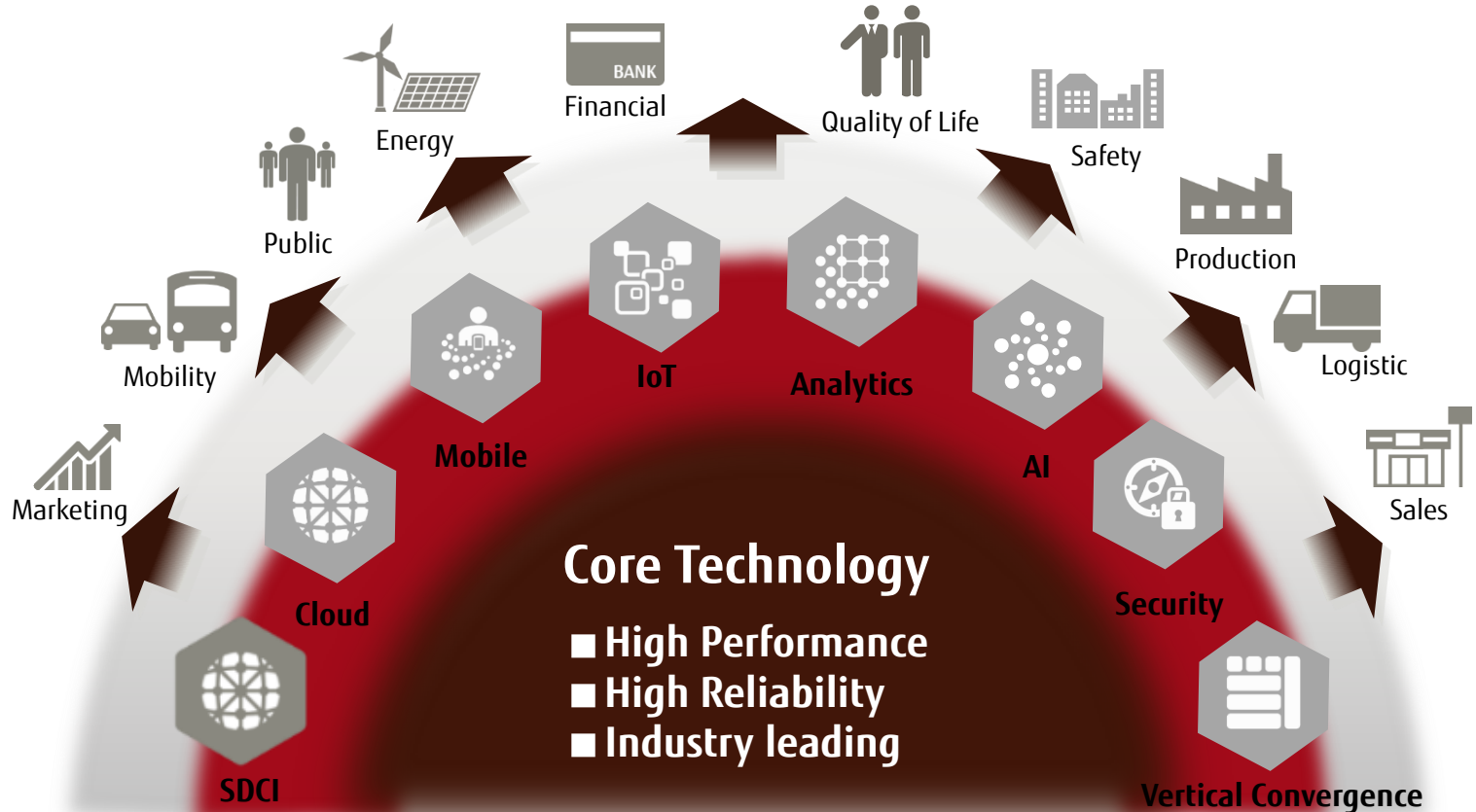
Massively Parallel

Many cores w/ on-chip network



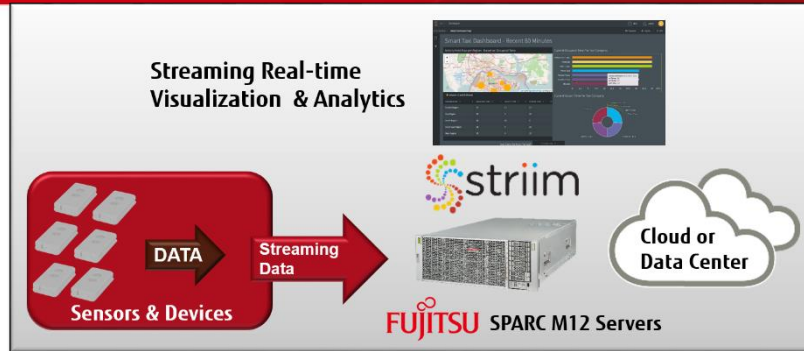
Large scale DLU interconnect through off-chip network

# Digital Co-Creation with Partners





# Moving Forward in A Hyperconnected World



# Hyperconnectivity Increases Vulnerability

A network diagram showing various icons (laptops, servers, and microchips) connected by dotted lines. A large white rectangular box with a red border is centered over the diagram, containing the text "INTRUSIONS SPREAD RAPIDLY IF EVERYTHING IS CONNECTED".

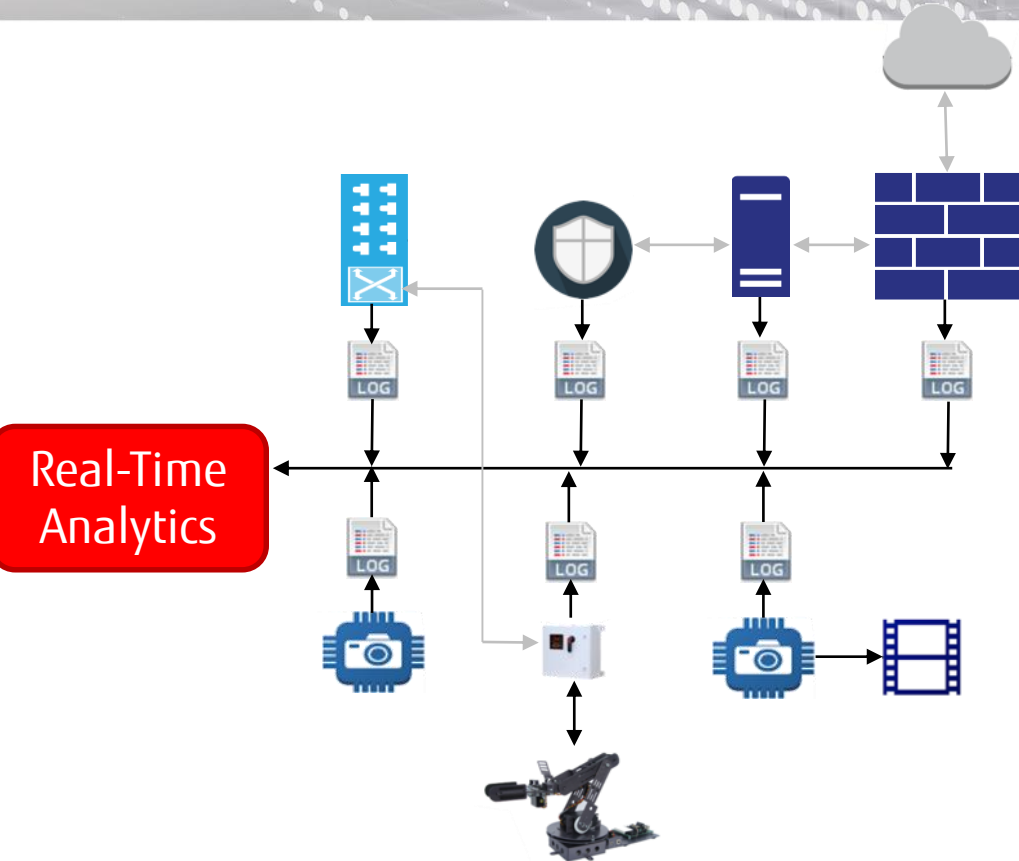
**INTRUSIONS SPREAD RAPIDLY  
IF EVERYTHING IS CONNECTED**

# Hackers Will Try to Cover Their Tracks



**DON'T PANIC!**  
**EVERYTHING IS NORMAL!**





- Device Data
- Controller Data
- Network Routers
- Malware Detection
- VPN Logs
- Firewall Logs
- Monitoring Equipment
- Cameras

Over-Instrument

Collect All Available Data

Use Real-Time Analytics

Utilize Machine Learning

Use The Best Technology

**EVERYTHING IS NORMAL!**

- Example Stuxnet
- Gas Centrifuges
- Lying About Spin Speed
- If You Also Measure
  - Vibration Levels
  - Power Draw
  - Temperature
  - Noise
  - Add Video Imaging
- More Data = More Confidence



## CORRELATE BY IP/NAT & TIME ACROSS NETFLOW / FIREWALL/ ANTI-VIRUS LOGS

```

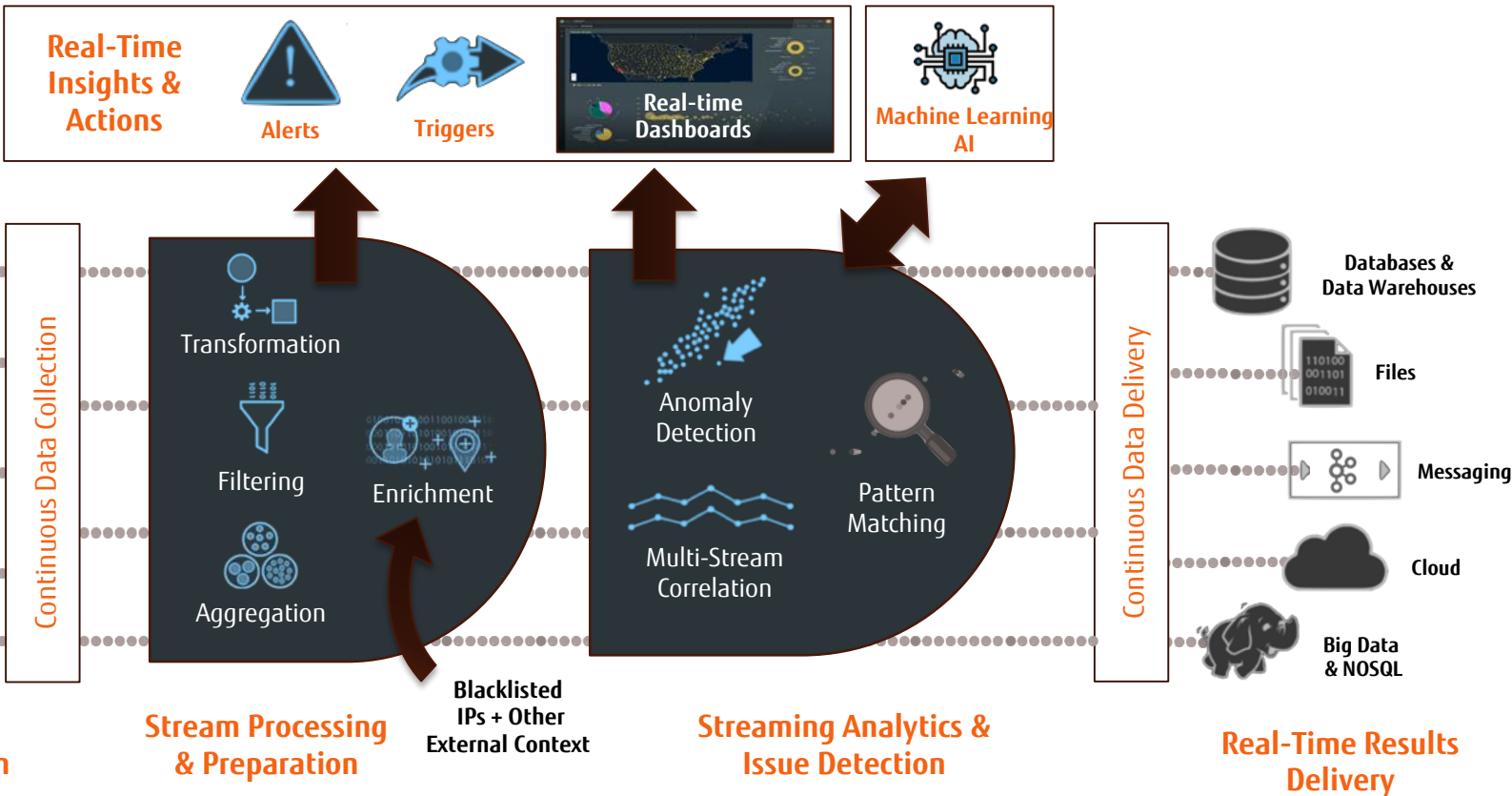
Fri Mar 24 18:21:46 UTC 2017,IDS,[121:2:1],Portscan detected from 192.168.20.2 to 192.168.0.0:10 sliding: 40) [**] 08/xx-14:29:14.676834
Fri Mar 24 18:21:48 UTC 2017,IDS,[121:2:1],Portscan detected from 192.168.20.2 to 192.168.0.0:10 sliding: 40) [**] 08/xx-14:29:14.676834
Fri Mar 24 18:21:52 UTC 2017,IDS,[121:2:1],Portscan detected from 192.168.20.2 to 192.168.0.0:10 sliding: 40) [**] 08/xx-14:29:14.676834
Fri Mar 24 18:21:52 UTC 2017,IDS,[121:2:1],Portscan detected from 192.168.20.2 to 192.168.0.0:10 sliding: 40) [**] 08/xx-14:29:14.676834
Fri Mar 24 18:22:00 UTC 2017,IDS,[121:2:1],Portscan detected from 192.168.20.2 to 192.168.0.0:10 sliding: 40) [**] 08/xx-14:29:14.676834
Fri Mar 24 18:22:00 UTC 2017,IDS,[121:2:1],Portscan detected from 192.168.20.2 to 192.168.0.0:10 sliding: 40) [**] 08/xx-14:29:14.676834
Fri Mar 24 18:22:00 UTC 2017,IDS,**ALARM** Malware Download Detected from www.badguy.com (123.45.6.7 ),IPNUKE-BLOODWINE
Fri Mar 24 18:22:00 UTC 2017,AV,Attended Vulnerability attack for MS-12345,192.168.20.2,12345,192.168.30.2,56789
Fri Mar 24 18:22:00 UTC 2017,AV,Attended Vulnerability attack for MS-12345,192.168.20.2,12345,192.168.30.3,56789
Fri Mar 24 18:22:00 UTC 2017,AV,Attended Vulnerability attack for MS-12345,192.168.20.2,12345,192.168.30.4,56789
Fri Mar 24 18:22:46 UTC 2017,AV,Attended Vulnerability attack for MS-123456,192.168.20.2,12345,192.168.30.5,56789
Fri Mar 24 18:22:48 UTC 2017,ARM** Malware "IPNUKE-BLOODWINE" detected on 192.168.20.2 - Removal initiated
Fri Mar 24 18:22:50 UTC 2017,ARM** Malware "WINNAIL-NTPSLAM" detected on 192.168.20.2 - Removal initiated
Fri Mar 24 18:22:50 UTC 2017,ARM** Malware "IPNUKE-BLOODWINE" detected on 192.168.30.2 - Removal initiated
Fri Mar 24 18:22:50 UTC 2017,ARM** Malware "IPNUKE-BLOODWINE" detected on 192.168.30.2 - Unable to remove!!
Fri Mar 24 18:22:50 UTC 2017,ARM** Malware "IPNUKE-BLOODWINE" detected on 192.168.20.2 - Unable to remove!!
Fri Mar 24 18:22:50 UTC 2017,WARNING** Excessive traffic from 192.168.20.2 to internal network ( 192.168.0.0 )
Fri Mar 24 18:22:50 UTC 2017,WARNING** Excessive traffic from 192.168.20.2 to internal network ( 192.168.0.0 )
Fri Mar 24 18:22:50 UTC 2017,WARNING** Excessive traffic from 192.168.20.2 to internal network ( 192.168.0.0 )
Fri Mar 24 18:22:50 UTC 2017,WARNING** Excessive traffic from 192.168.20.2 to internal network ( 192.168.0.0 )
Fri Mar 24 18:22:48 UTC 2017,FLOW,**ALARM** Extremely excessive traffic from 192.168.20.2 to internal network ( 192.168.0.0 )
  
```

PortScan

Anti-Virus Spots Updates, Not Original Malware

Download of Updates Spotted. Badguy.com Blacklisted

Maps to 192.168.20.2 Through NAT





# striim Visualization Streaming Dashboards



Set Visualization Query

Name: FTM.TxVolumeByNetworkEndPoint

```
1 SELECT *
2 FROM TxVolumeByNetworkEndPointAS [3 MINUTE AND PUSH]
3 ORDER BY LocalDtTm;
```

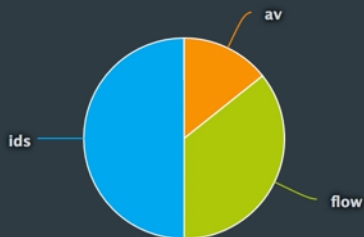
Press Ctrl-space for a pop-up menu of functions and cache, stream, and WActionStore names

SAVE QUERY



Multiple IDS(snort) alerts (7) indicating excessive portscans from 192.168.20.2

Alerts By Log Type

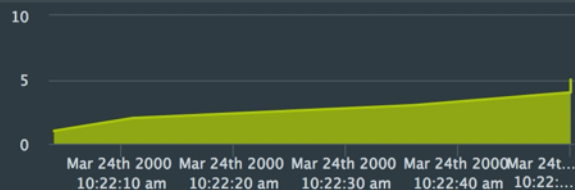


Alerts by Priority

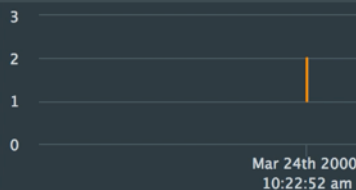
TIMESTAMP	SOURCE IP	MSG	PRIORITY
Mar 24th 2000, 10:21:52 am	192.168.20.2	Portscan detected from 192.168.20.2 Talke	90.8
Mar 24th 2000, 10:22:50 am	192.168.20.2	ALARM - ONGOING EXCESSIVE FLOW	80.2
Mar 24th 2000, 10:22:52 am	192.168.20.2	[AV-Service] - **ALARM** Malware ""IPNUK	96.3

Waiting for data

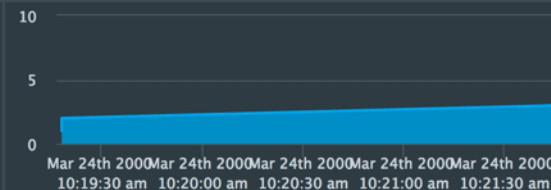
Flow Alerts

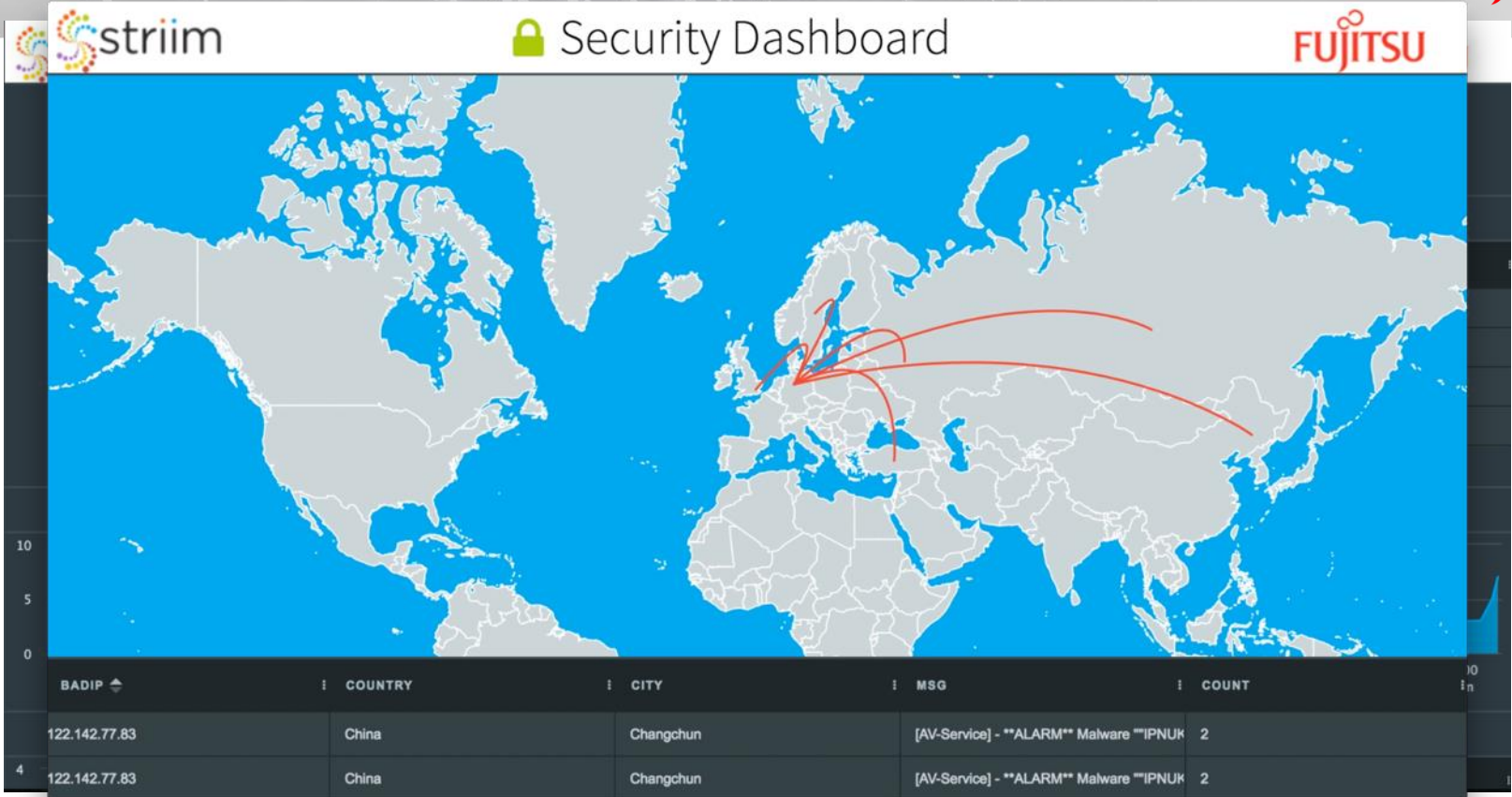


AV Alerts



IDS Alerts





## ■ Core component

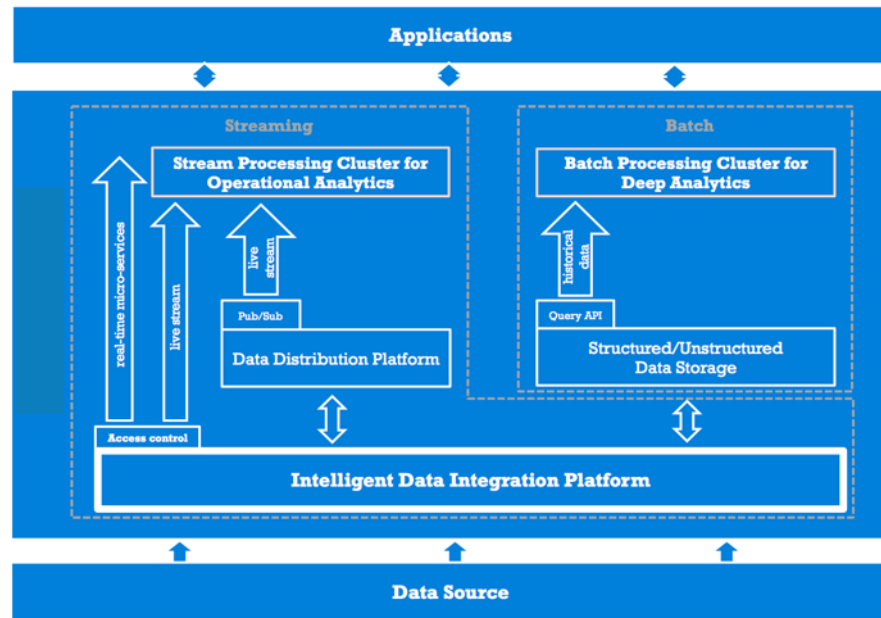
- Intelligent data integration platform

## ■ Streaming and Deep Learning

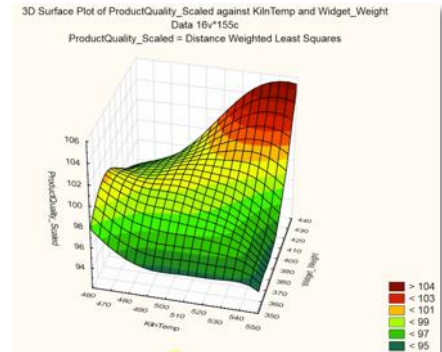
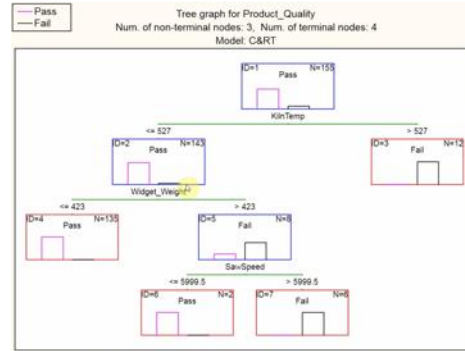
- End-to-end Digital Factory solution

## ■ Value propositions

- Real-time micro-service deployment
- Dynamic depth & breadth calibration of data collection
- Edge processing
- Flexible real-time analytics framework

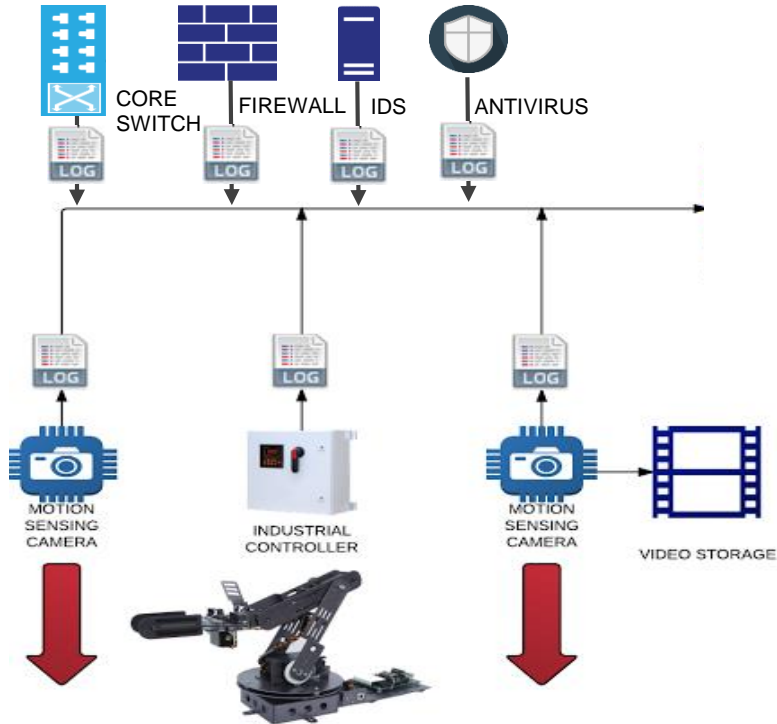


- Send Data to the Cloud
- Build Model In Cloud
- Export Model To Edge
- Do Real-Time Scoring
- Model = Normal
- Also Train for Problems
- Spots Anything Unusual





**INTRUSIONS CAN BE STOPPED  
THROUGH CORRELATED STREAM ANALYTICS**



## STRIIM AND FUJITSU CYBERSECURITY APPLIANCE

### REAL-TIME DASHBOARDS



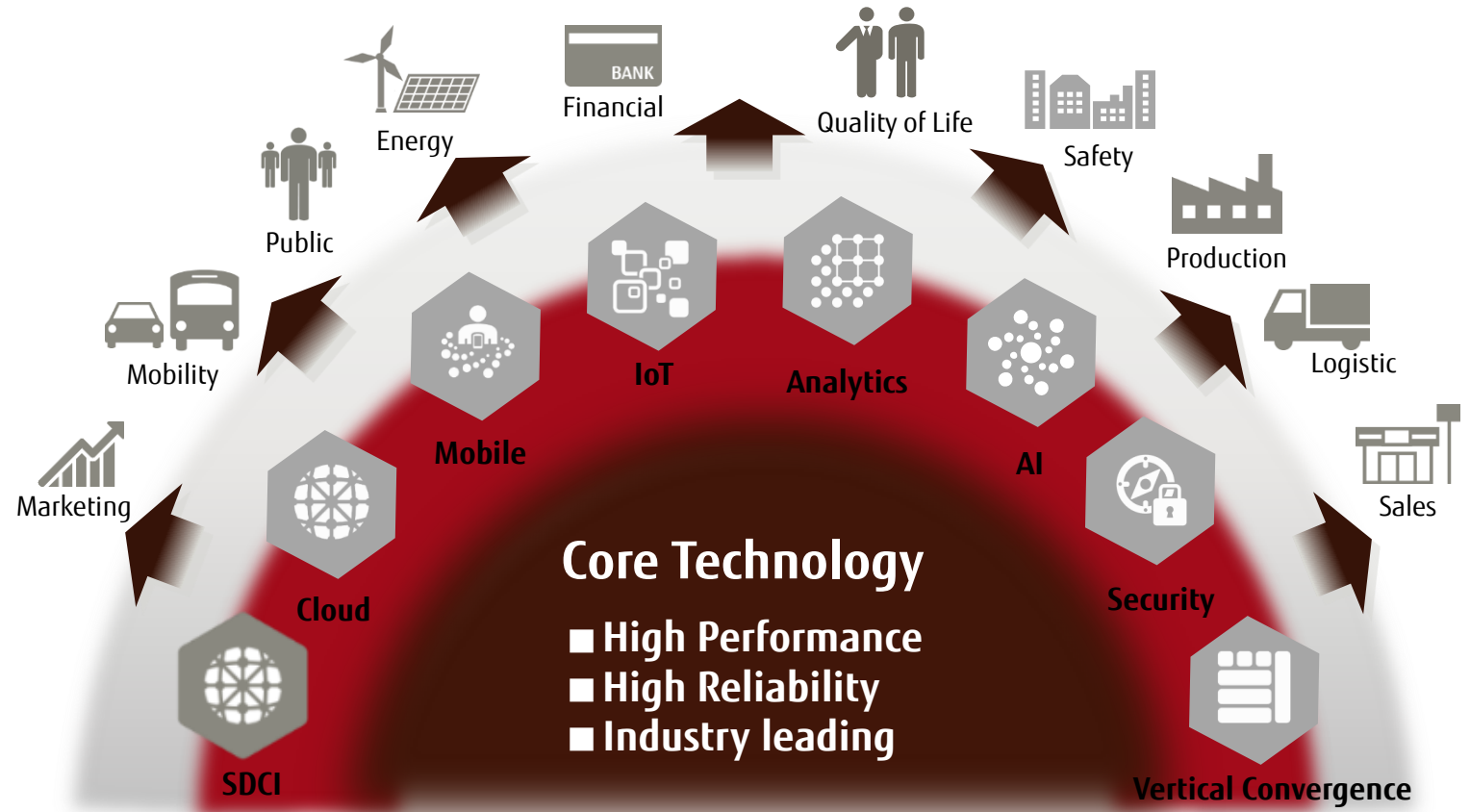
+



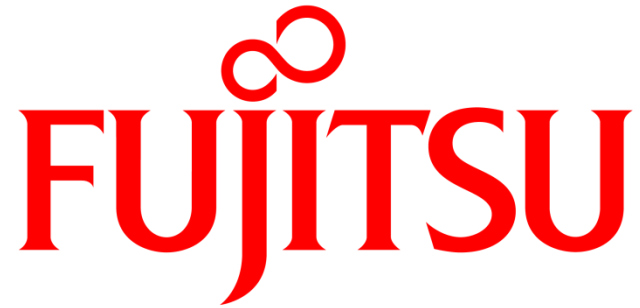
**Fujitsu SPARC M12**

STREAMING DATA INTEGRATION  
AND REAL-TIME SECURITY ANALYTICS

# Digital Co-Creation with Partners





The logo features a red infinity symbol positioned above the word "FUJITSU". The word "FUJITSU" is rendered in a bold, red, serif typeface. The letter "J" is notably stylized with a long, sweeping tail that extends downwards and to the left.

**FUJITSU**

shaping tomorrow with you