TOMORROW
starts here.

The Internet of Things: A Double-Edged Sword. How Can You Embrace it Securely?

BRKSEC-2005

Gary Spiteri

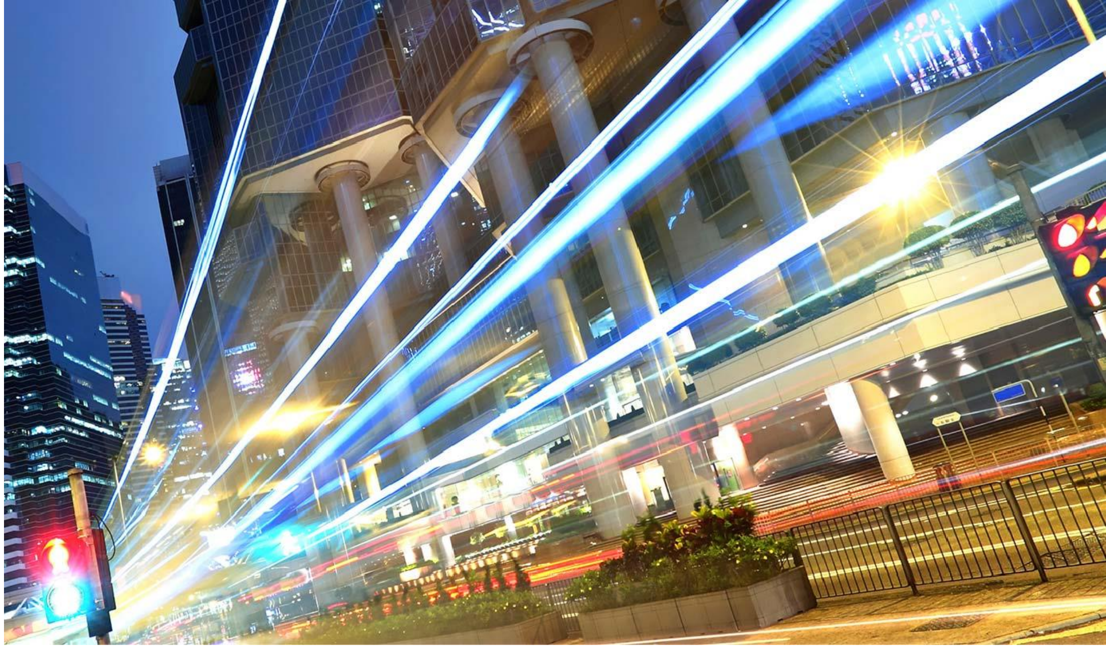
Consulting Security Engineer

#clmel

Cisco live!

Agenda

- Introduction
- Extraordinary Benefits
- Major Security Challenges
- Delivering Security Across the Extended Network
- The Best of Both Worlds
- Conclusion



What is the Internet of Things?

> “The Internet of Things is the intelligent connectivity of physical devices driving massive gains in efficiency, business growth, and quality of life”

Relationship to the Internet of Everything (IoE)

IoE
010101
11001
001

People

Connecting People in More Relevant, Valuable Ways

Process

Delivering the Right Information to the Right Person (or Machine) at the Right Time

Data

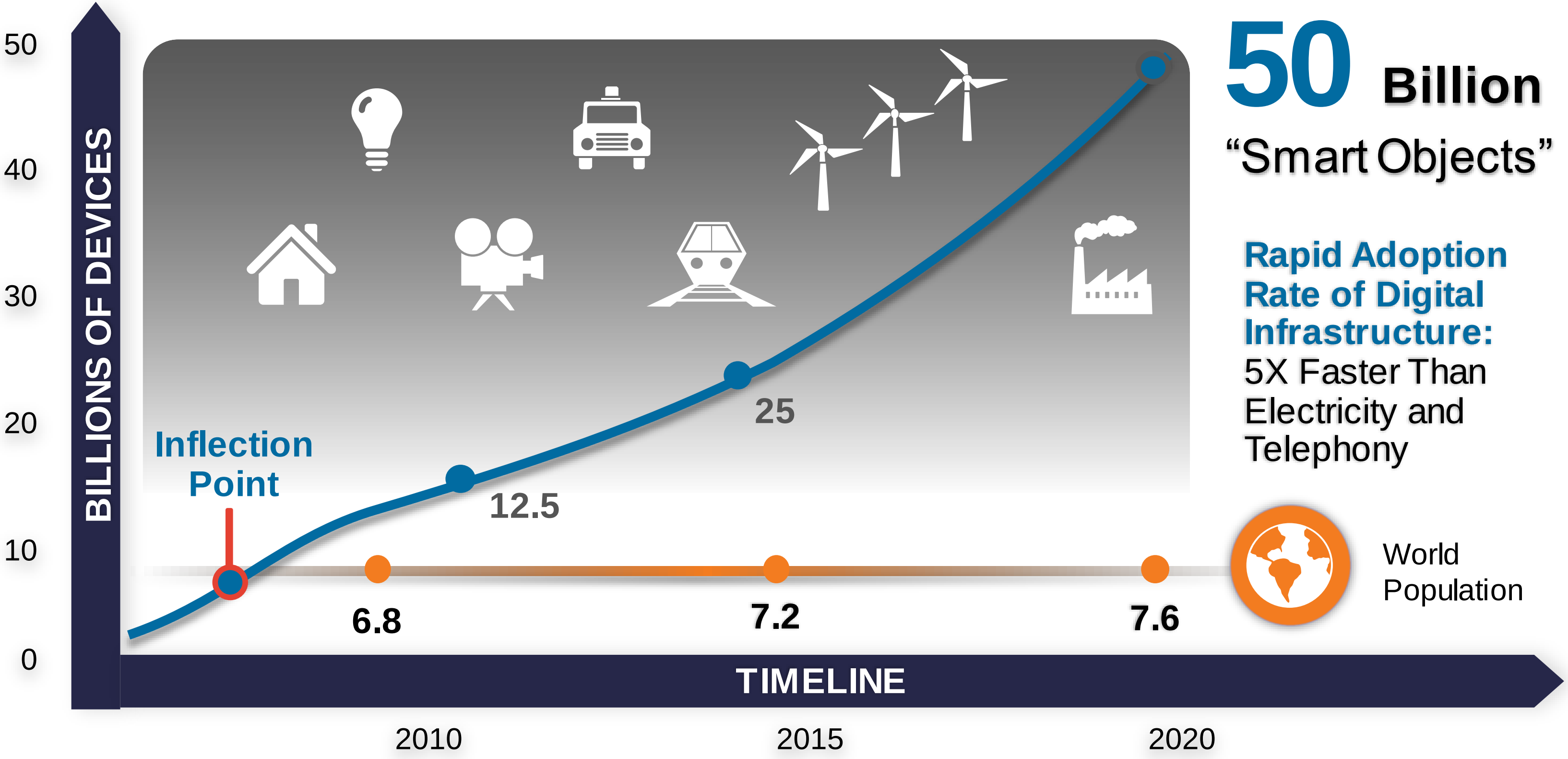
Leveraging Data into More Useful Information for Decision Making

Things

Physical Devices and Objects Connected to the Internet and Each Other for Intelligent Decision Making

Networked Connection of People, Process, Data, Things

IoT is Here Now – and Growing!



50 Billion

“Smart Objects”

Rapid Adoption Rate of Digital Infrastructure:
5X Faster Than Electricity and Telephony

Source: Cisco IBSG, 2011

Connected Objects Generate Big Data

46 million in the U.S alone
1.1 billion data points (.5TB) per day

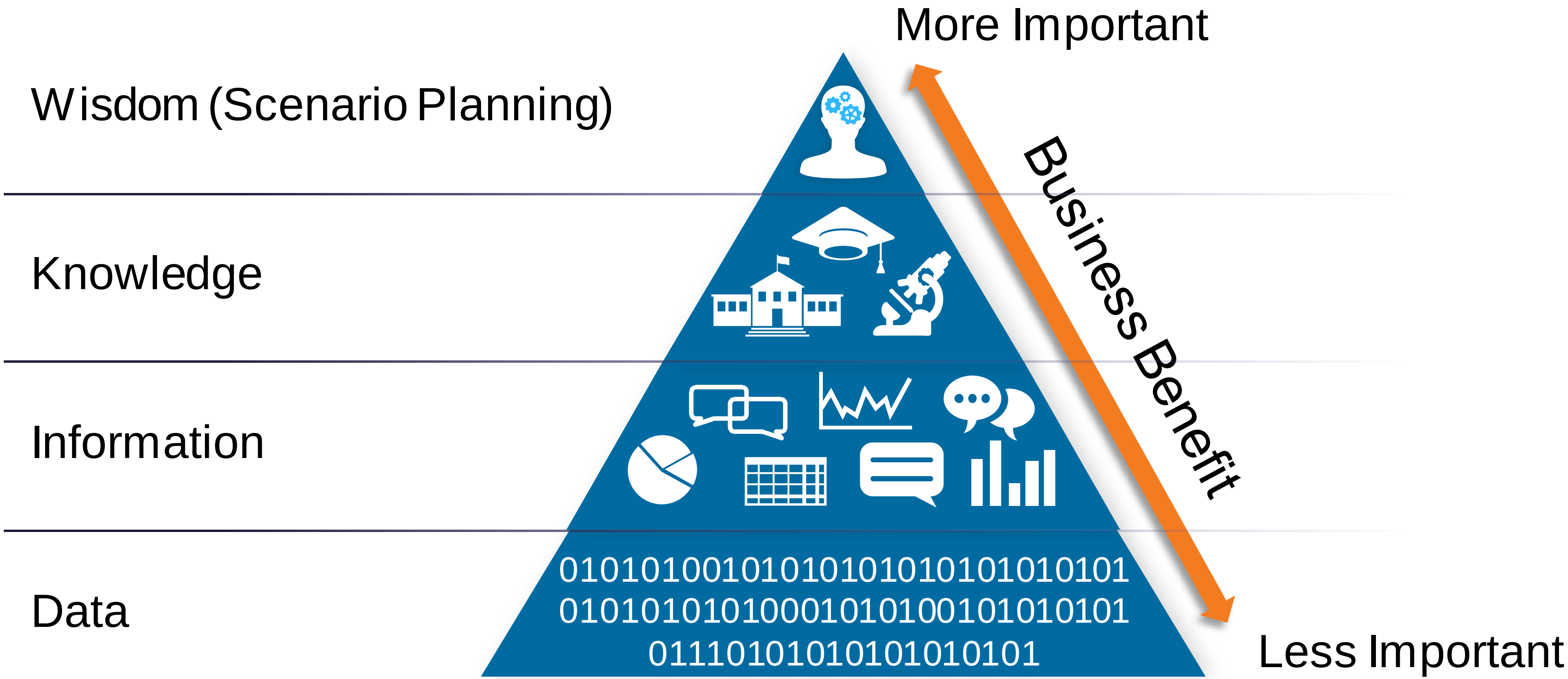
A single consumer packaged good manufacturing machine generates 13B data samples per day

A large offshore field produces 0.75TB of data weekly
A large refinery generates 1TB of raw data per day

10TB of data for every 30 minutes of flight
With >25,000 flights per day, petabytes daily

The World Generates More Than 2 Exabytes of Data Every Day

IoT Transforms Data into Wisdom



More Important

Wisdom (Scenario Planning)

Knowledge

Information

Data

Business Benefit

Less Important

Big Data Becomes Open Data for Customers, Consumers to Use

Sizing the Opportunity

$19.0* Trillion

VALUE AT STAKE

14.4 Trillion PRIVATE SECTOR

Includes Both Industry-specific and Horizontal Use Cases:

- Customer experience
- Innovation
- Employee productivity
- Supply chain
- Asset utilisation

4.6 Trillion PUBLIC SECTOR

Includes Cities, Agencies, and Verticals Such as Healthcare, Education, Defence:

- Increased revenue
- Reduced cost
- Employee productivity
- Connected militarised defence
- Citizen experience

Estimate Is Based on Bottom-up Analysis of **61 Use Cases**, Including 21 for Private Sector and 40 in Public Sector (*2013-2022)

IoT Delivers Extraordinary Benefits

Connected Rail Operations

PASSENGER SECURITY

- In-station and onboard safety
- Visibility into key events

ROUTE OPTIMISATION

- Enhanced Customer Service
- Increased efficiency
- Collision avoidance
- Fuel savings

CRITICAL SENSING

- Transform “data” to “actionable intelligence”
- Proactive maintenance
- Accident avoidance

Cost savings, improved safety, superior service

Smart City

CONNECTED TRAFFIC SIGNALS

- Reduced congestion
- Improved emergency services response times
- Lower fuel usage

PARKING AND LIGHTING

- Increased efficiency
- Power and cost savings
- New revenue opportunities

CITY SERVICES

- Efficient service delivery
- Increased revenues
- Enhanced environmental monitoring capabilities

Safety, financial, and environmental benefits

The Connected Car

WIRELESS ROUTER

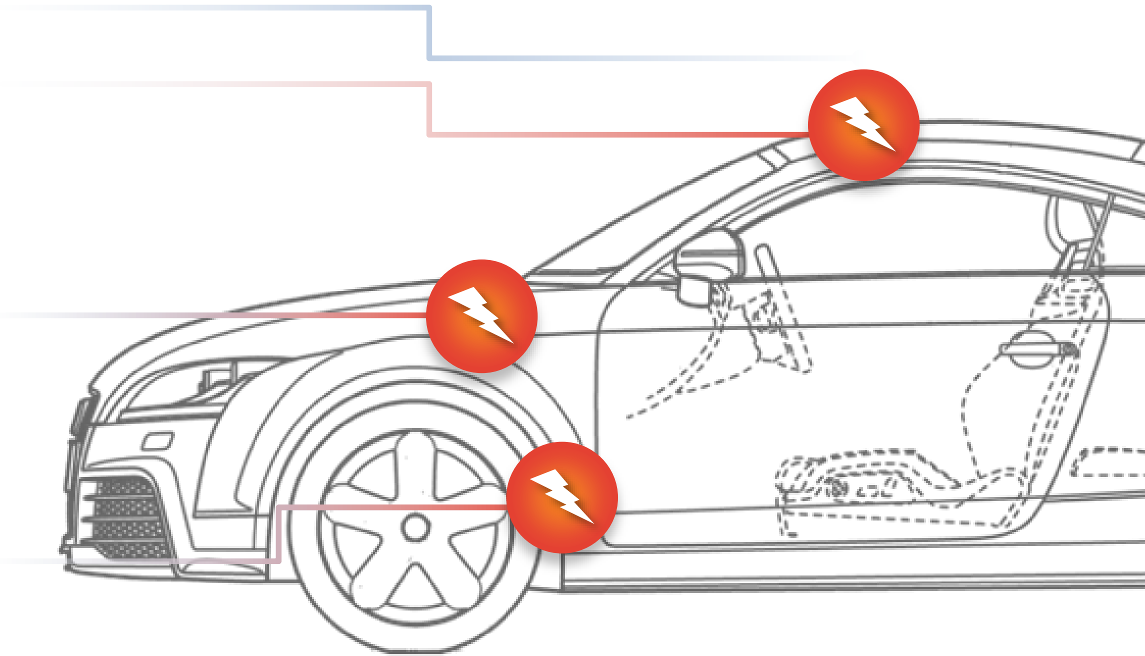
- Online entertainment
- Mapping, dynamic re-routing, safety and security

CONNECTED SENSORS

- Transform “data” to “actionable intelligence”
- Enable proactive maintenance
- Collision avoidance
- Fuel efficiency

URBAN CONNECTIVITY

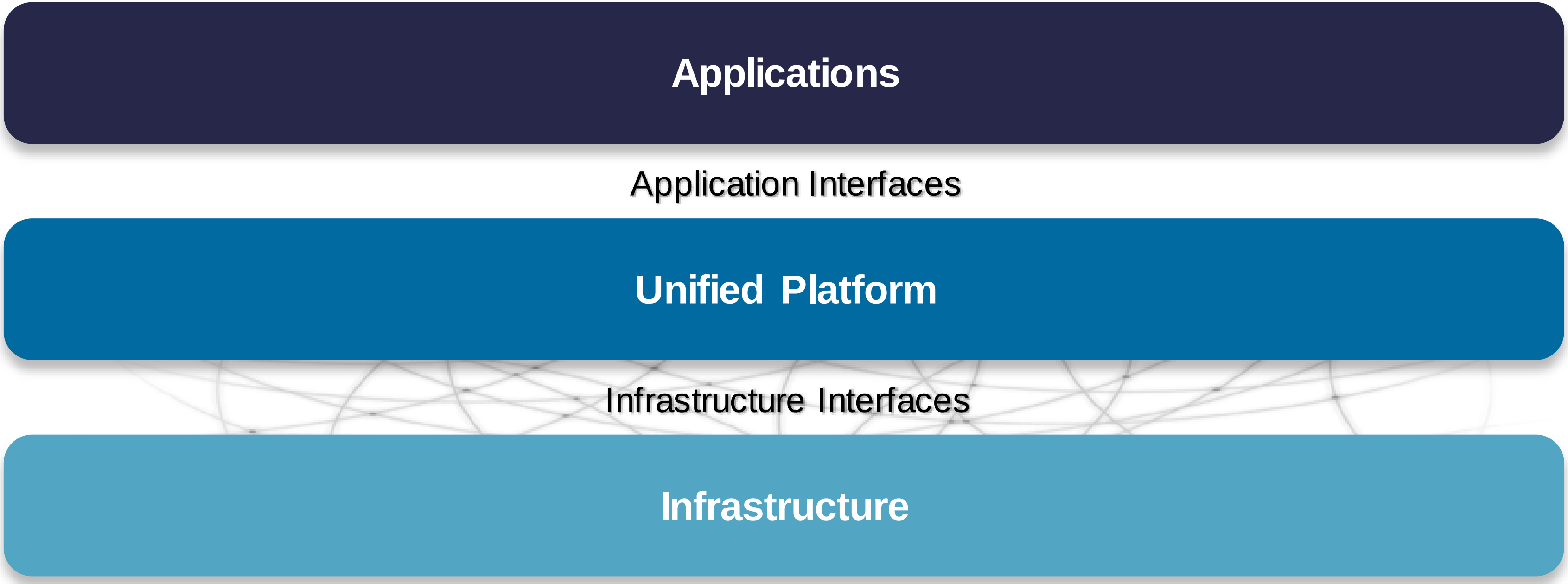
- Reduced congestion
- Increased efficiency
- Safety (hazard avoidance)



Actionable intelligence, enhanced comfort, unprecedented convenience

… but it also adds complexity.

New Business Models **Partner Ecosystem**



Applications

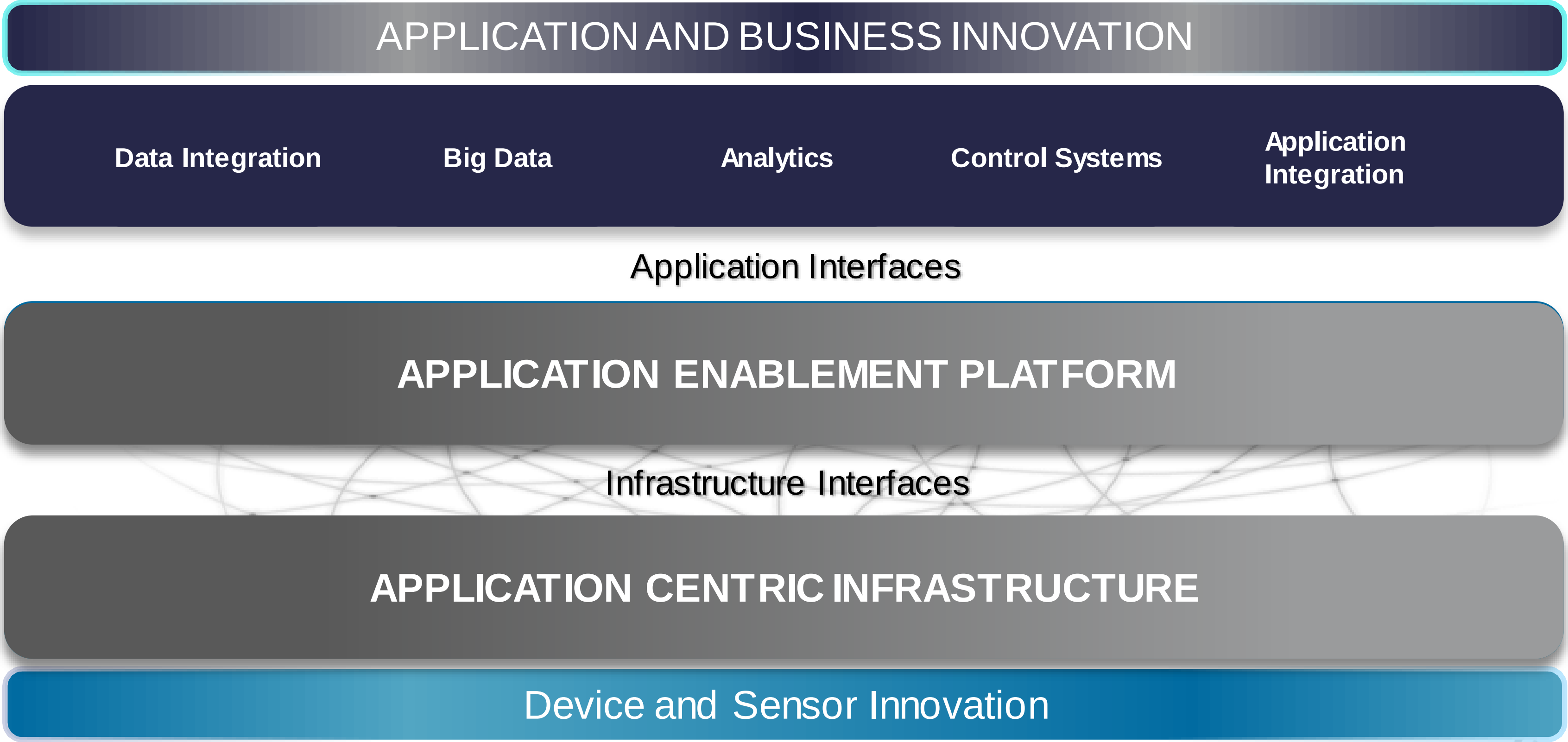
Application Interfaces

Unified Platform

Infrastructure Interfaces

Infrastructure

… but it also adds complexity.



APPLICATION AND BUSINESS INNOVATION

Data Integration

Big Data

Analytics

Control Systems

Application Integration

Application Interfaces

APPLICATION ENABLEMENT PLATFORM

Infrastructure Interfaces

APPLICATION CENTRIC INFRASTRUCTURE

Device and Sensor Innovation

What Comprises IoT Networks?

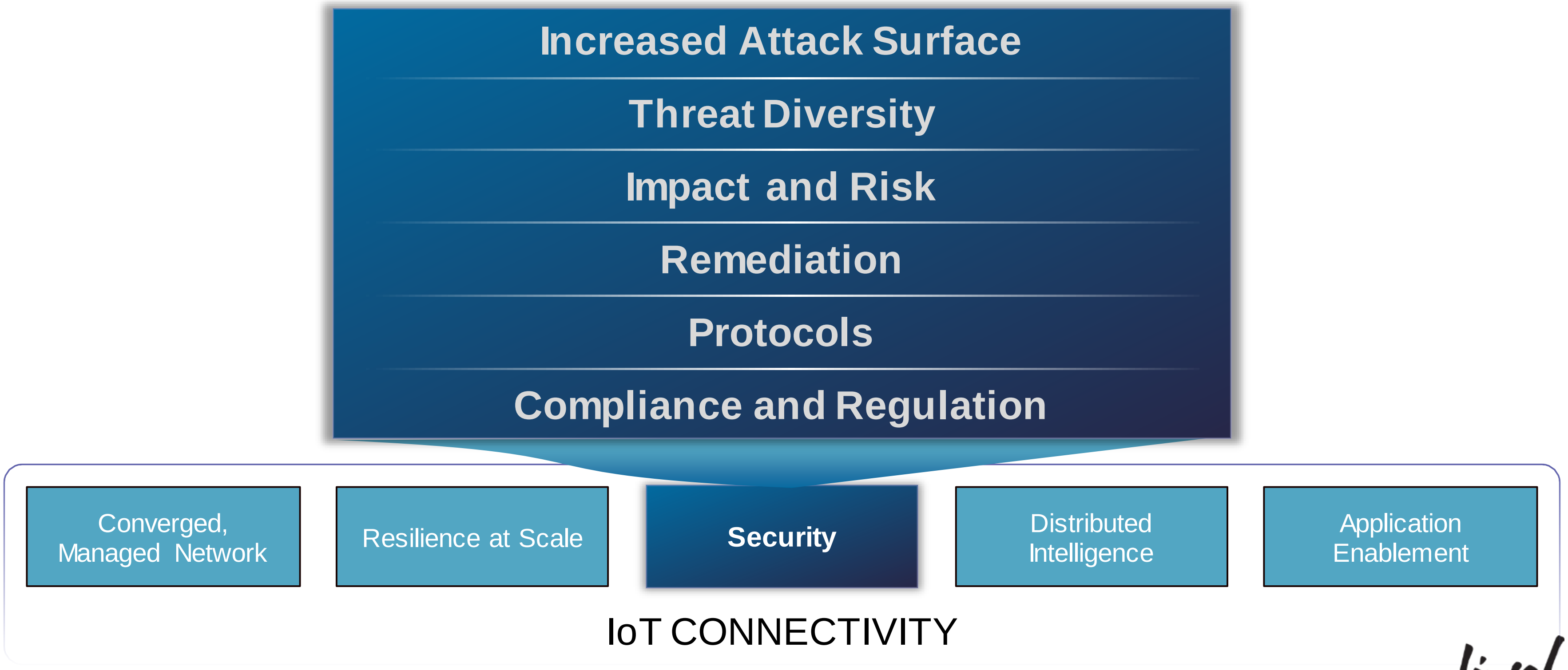
Information Technology (IT)

Operational Technology (OT)

Smart Objects

The Flip Side: Major Security Challenges

IoT Expands Security Needs



Increased Attack Surface

Threat Diversity

Impact and Risk

Remediation

Protocols

Compliance and Regulation

Converged, Managed Network

Resilience at Scale

Security

Distributed Intelligence

Application Enablement

IoT CONNECTIVITY

What Can Breach IoT Networks?

- What can't?
  - Billions of connected devices
  - Secure and insecure locations
  - Security may or may not be built in
  - Not owned or controlled by IT … but data flows through the network

- Any node on your network can potentially provide access to the core

Connected Rail Operations

REMOTE CONTROL

- Passenger, train and station monitoring
- PTZ control to avoid detection

SYSTEM CONTROL

- Schedule manipulation
- System shutdown

MECHANICAL CONTROL

- Sensor manipulation
- Creation of unsafe conditions

Individual components or the system as a whole can be targeted

Smart City

REMOTE ACCESS

- Increased traffic congestion
- Creation of unsafe conditions

SYSTEM CONTROL

- Device manipulation
- Remote monitoring
- Creation of unsafe conditions

SERVICE MANIPULATION

- Environmental degradation
- System shutdown
- Lost revenue

Potential impact to services and public safety

The Connected Car

INDIRECT PHYSICAL ACCESS

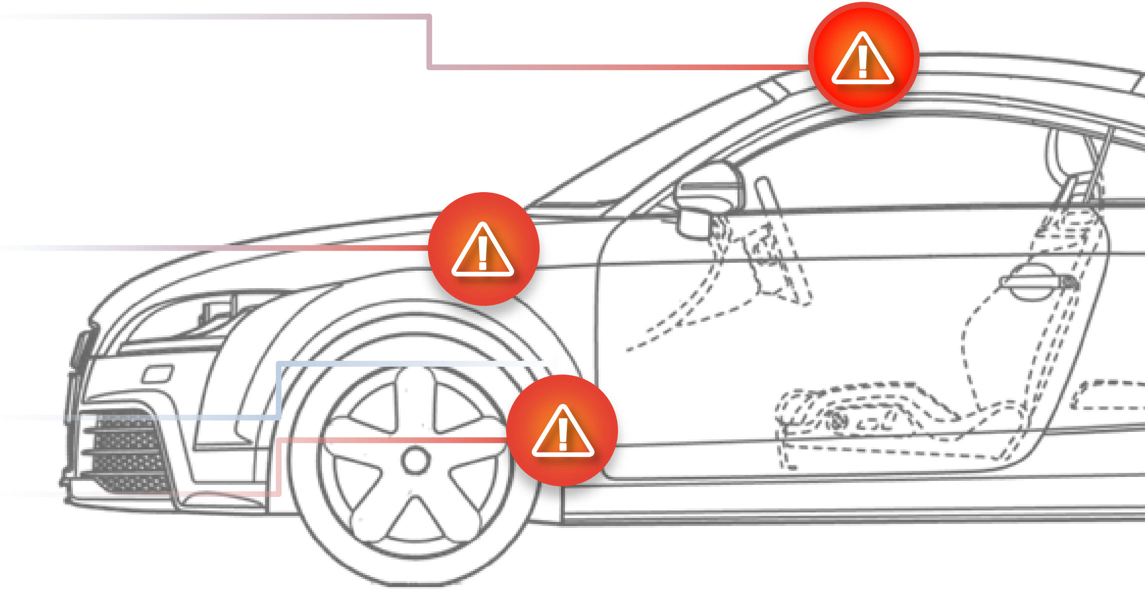
- OBD-II (PassThru)
- Disc/USB/Phones

SHORT-RANGE WIRELESS

- Bluetooth
- Remote Keyless Entry
- SDRC

LONG-RANGE WIRELESS

- Broadcast Channels (RDS)
- Wi-Fi / WiMax
- Cellular (LTE)



Each new connection or device adds a potential target

Attack on Energy Infrastructure

- Targeted Energy Firm in Middle East
  - 30,000 workstations were rendered unusable
  - No impact on production operations
- Objective was not stealing data or financial profit but Denial of Service and total destruction of data
  - Attributed to skilled “amateurs”!

Shamoon

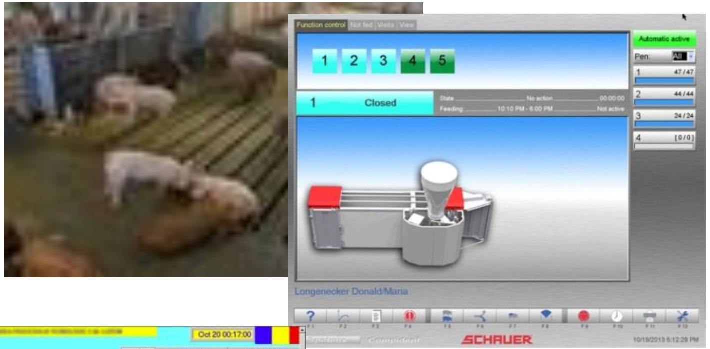
IT Breach via OT Network

- Breached via Stolen Credentials from HVAC Vendor
- 40 Million Credit And Debit Cards Stolen
- PII Stolen From 70 Million Customers
- Reputation Damage*
  - 46% drop in year-over-year profit
  - 5.3% drop in year-over-year revenue
  - 2.5% drop in stock price
- CEO Fired

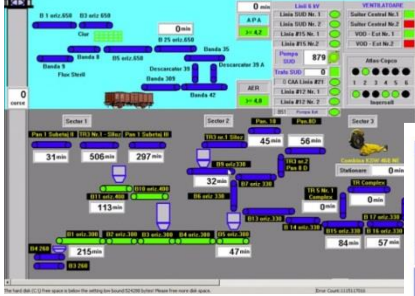
* Source: KrebsonSecurity, May 2014

Other Unintended Security Exposures*

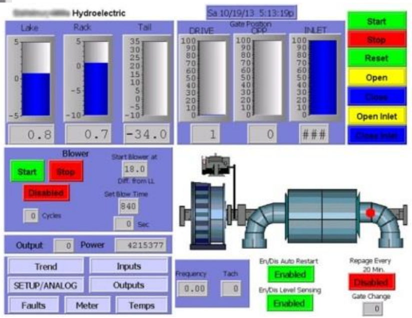
- Farm Feeding System in the U.S.



- Mine Ventilation System in Romania



- Hydroelectric Plant in the U.S.



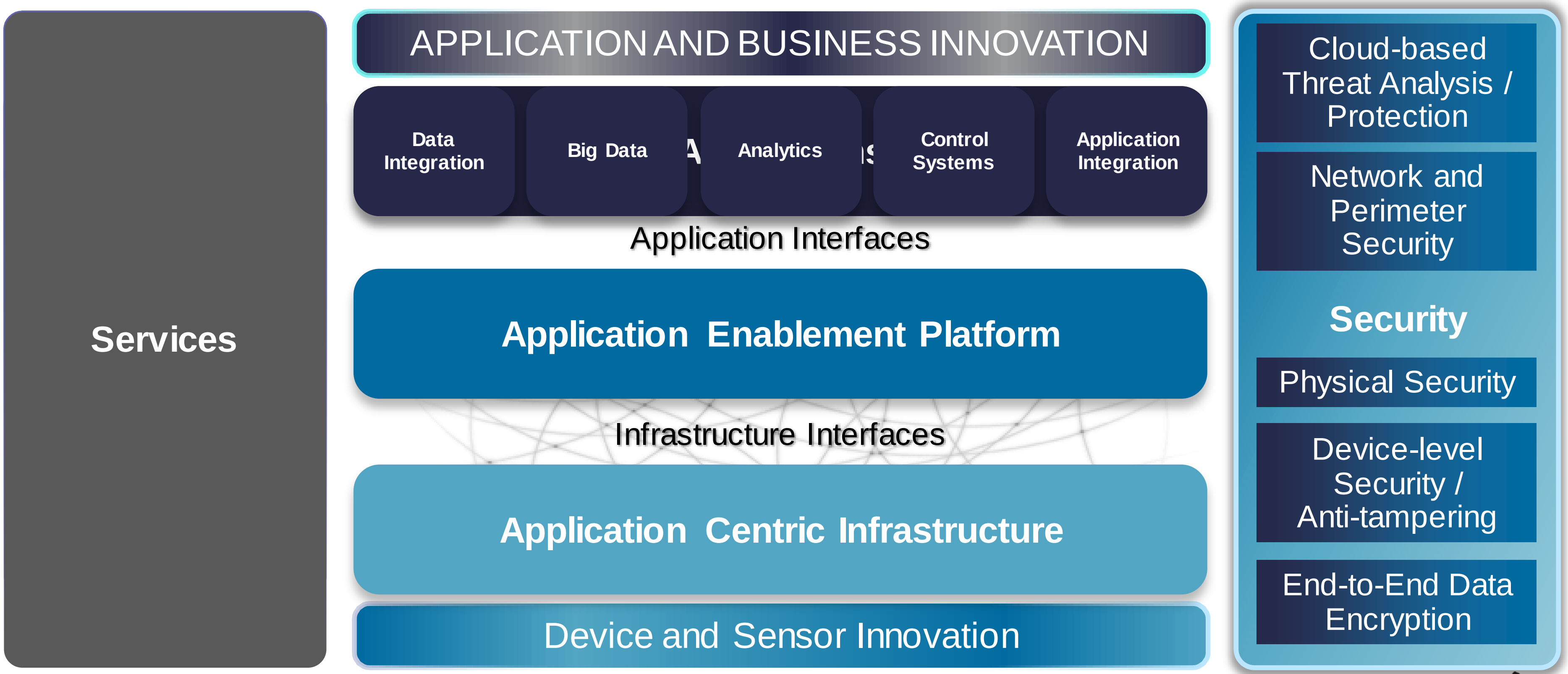
* Source: Wired, November 2013

And the Potential Risks

- BMW patches firmware of 2 Million cars to prevent remote door opening
- Proof of Concept malware for Man-in-the-middle ownage of Drones
- Progressive Insurance Dongle OBDII research concept
- Ghost In the Shell Arise (science fiction) – an attacker takes over the AIs of 20 million cars and uses them to attack a government server
  - Make believe for now…
  - But this is just another Botnet…
  - And collective compute is being used by Botnets, SETI, Electric Sheep

Delivering Security Across the Extended Network

The Secure IoT Architecture – IT Plus OT!



Services

APPLICATION AND BUSINESS INNOVATION

Data Integration

Big Data

Analytics

Control Systems

Application Integration

Application Interfaces

Application Enablement Platform

Infrastructure Interfaces

Application Centric Infrastructure

Device and Sensor Innovation

Cloud-based Threat Analysis / Protection

Network and Perimeter Security

Security

Physical Security

Device-level Security / Anti-tampering

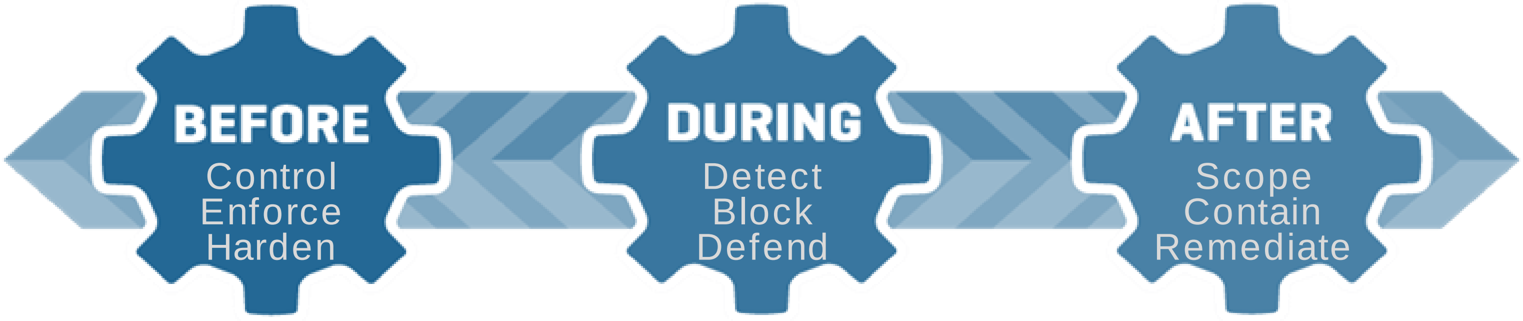
End-to-End Data Encryption

IT and OT are Inherently Different

- IT
  - Connectivity: “Any-to-Any”
  - Network Posture: Confidentiality, Integrity, Availability (CIA)
  - Security Solutions: Cybersecurity; Data Protection
  - Response to Attacks: Quarantine/Shutdown to Mitigate

- OT
  - Connectivity: Hierarchical
  - Network Posture: Availability, Integrity, Confidentiality (AIC)
  - Security Solutions: Physical Access Control; Safety
  - Response to Attacks: Non-stop Operations/Mission Critical – Never Stop, Even if Breached

Attack/Security Continuum – IT

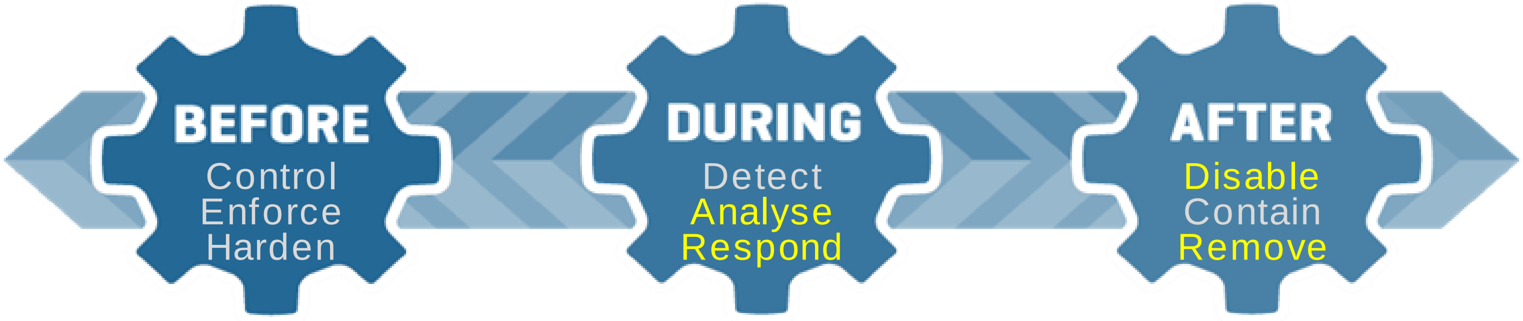


Cloud-based threat detection and prevention; policy enforcement via firewall, VPN and identity services

Quarantine based on real-time analysis and actionable security Intelligence from IPS and Web services appliance

Remediate using advanced malware protection and network behavioural analysis

Attack/Security Continuum – OT



BEFORE
Control
Enforce
Harden

DURING
Detect
Analyse
Respond

AFTER
Disable
Contain
Remove

Networked cyber and physical security solutions with OT-specific policies

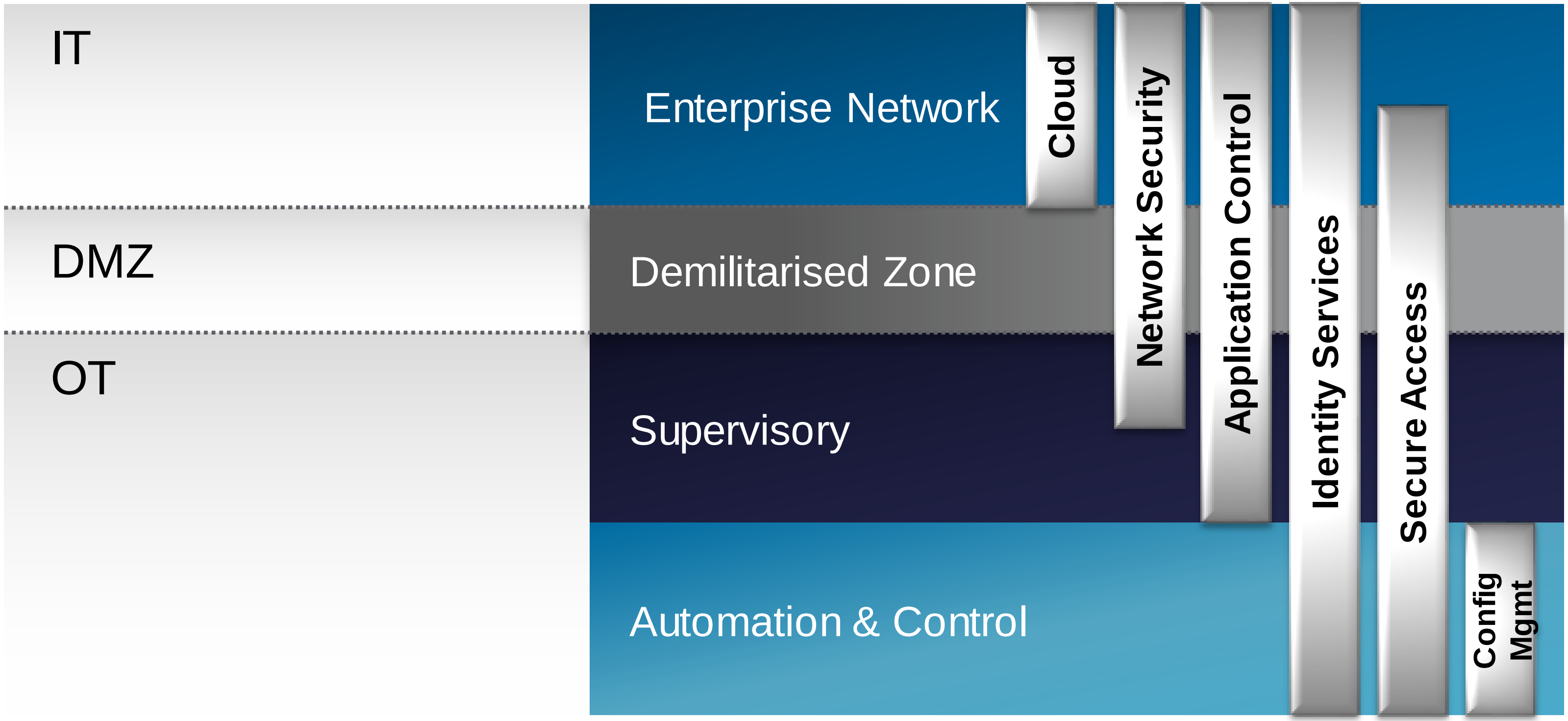
Response based on real-time analysis and actionable security Intelligence

Lockdown physical spaces or disable access to critical infrastructure

Network-Wide Security with Differential Applications

	Security Activity	IT	OT
Before	**Secure Access**	- Role-based access for individuals and groups - VPN/remote access for most systems throughout the network - Complex passwords with lockout policies - Application control	- Role-based access to few individuals - VPN to few systems and users - Badge readers/integrated sensors - IP cameras with video analytics - Simplified passwords (except for the most critical systems)
During	**Intrusion Prevention/Detection**	IPS – enforces policies	IDS – sends security alert only
	Threat Mitigation	Quarantine affected system	Analysis of the threat to determine appropriate action
	Data Integrity and Confidentiality	Data Loss Prevention (DLP)	Combined physical and cybersecurity access controls
	Network-wide Policy Enforcement	Differentiated actions based on value, function, and location of the device	
After	**Retrospective Security Policies**	Centralised remediation and adaptation	

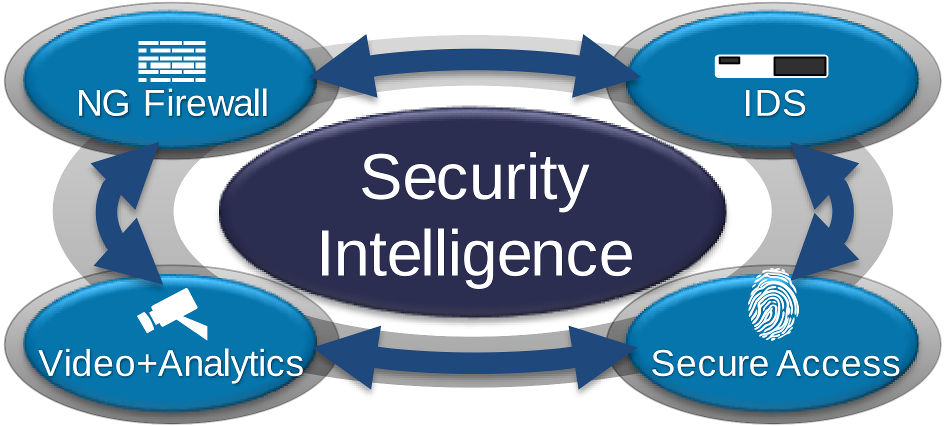
IT/OT Converged Security Model



The Best of Both Worlds

IoT Can Actually **Increase** Security Posture

- Network of Security Devices
  - Cyber Security
    - Firewall, IDS
  - Physical Security
    - IP cameras, badge readers, analytics
- Actionable Security Intelligence
  - Automated / M2M
  - Human Response
- Remote Capabilities
  - Configuration and Management
  - Collaboration Between Groups



Keeping Passengers Safe: Airport Security

- Profile
  - Large facilities with diverse human population
  - Significant security exposures
  - Need for real-time, actionable intelligence
- Existing Security Systems
  - Badge readers
  - IP cameras
  - Sensors
  - Network/perimeter security (firewall/IPS)
- Challenge
  - Limited visibility
  - Sluggish response times
  - High OpEx

IoT Enhances Security: The Connected Airport

- Video Analytics & Sensors
  - Multi-factor employee badge authentication
  - Facial recognition
  - Event correlation across multiple facilities
  - Rapid response
- Integration of Cameras & Sensors
  - Automatically zoom to potential problems
- Integration with Cyber Security
  - Employee/asset location monitoring
  - Critical system lockdown

Making Plant Operations Safe: Manufacturing Security

- Profile
  - Large facilities with dozens of independent systems
  - Complex robotics and other dangerous moving parts
  - Need for physical security and personnel safety
  - System availability is absolutely essential
- Existing Security Systems
  - IP cameras
  - Badge readers
- Challenge
  - Limited visibility
  - Data silos

IoT Enhances Security: The Connected Plant

- Integrate physical and cyber security
  - Device- and user-level authentication
  - Automated access lockout with breach detection
  - Removable media detection

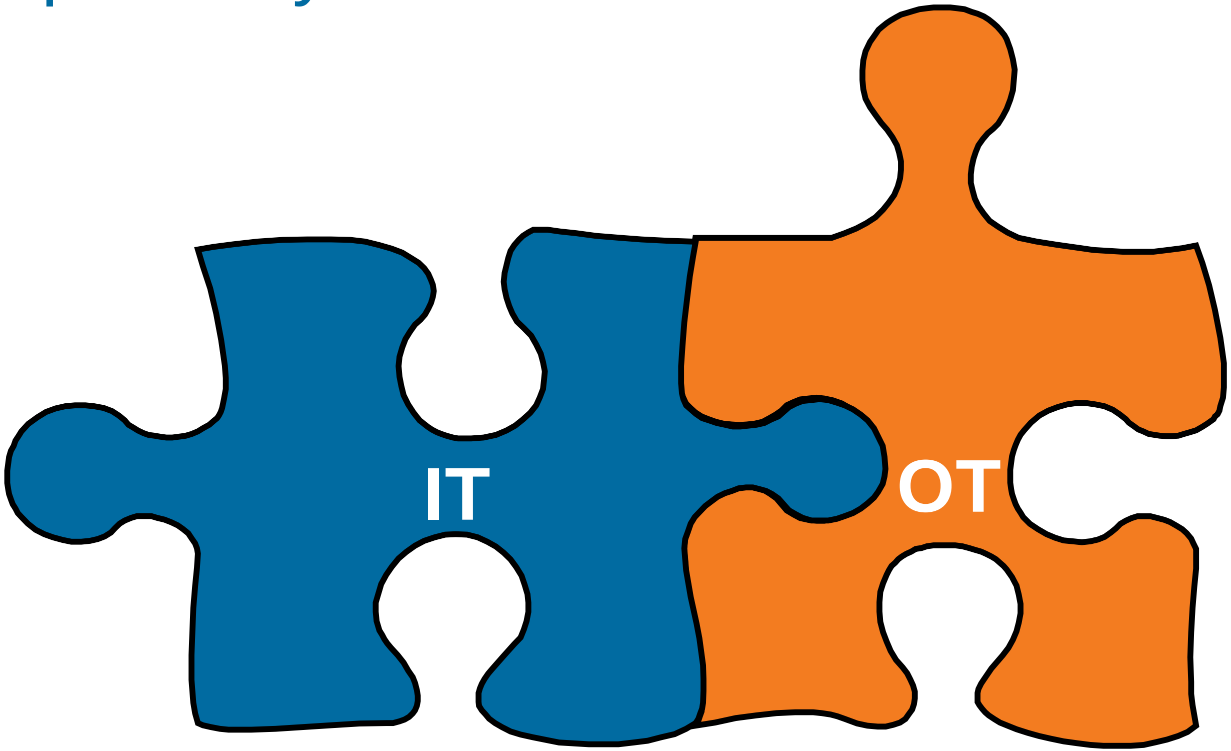
- Video Analytics & Sensors
  - Multi-factor employee authentication
  - Event correlation to avoid accidents

- Integration of Cameras & Sensors
  - Gain immediate visibility into potential breaches

Conclusion: Securely Embrace IoT!

- New challenges require new thinking!
  - avoid operational siloes
  - networking and convergence are key
  - a sound security solution is integrated throughout
  - build for the future
- Security must be pervasive
  - inside and outside the network
  - device- and data-agnostic
  - proactive and intelligent
- Intelligence, not data
  - convergence, plus analytics
  - speed is essential for real-time decisions

Most Importantly: Teamwork!



Continue Your Education

- Demos in the Cisco Campus
- Walk-in Self-Paced Labs
- Table Topics
- Meet the Engineer 1:1 meetings

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a Cisco Live 2015 T-Shirt!

Complete your Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site http://showcase.genie-connect.com/clmelbourne2015
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected in the World of Solutions on Friday 20 March 12:00pm - 2:00pm

Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations. www.CiscoLiveAPAC.com

Thank you.

cisco