Protecting Operational Technology (OT) using Fortinet's Security Fabric

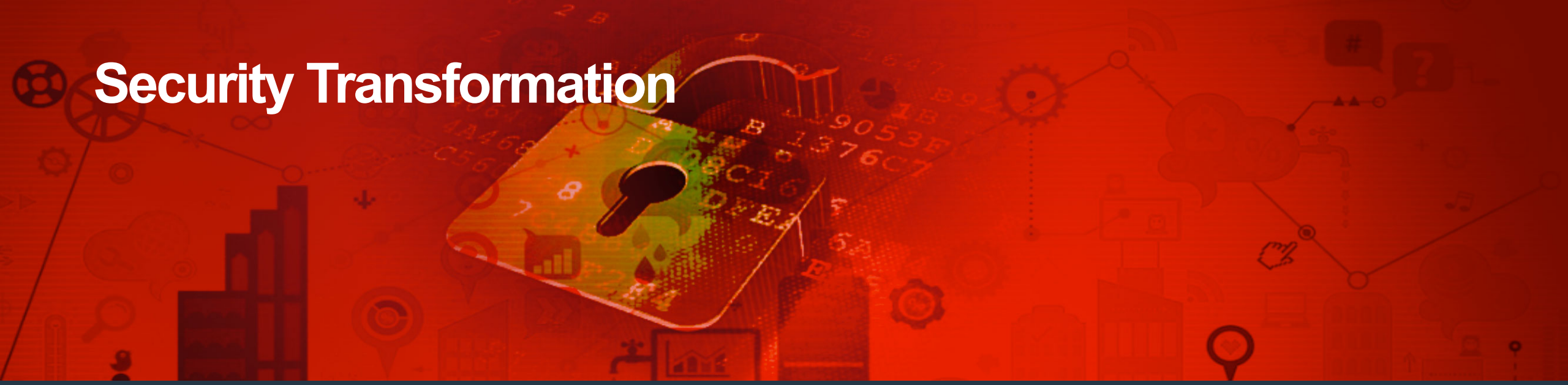
Q1 2019

Operational Technology & Critical Infrastructure Global Enablement Team

Digital Transformation

DX is the integration of digital technology into all areas of a business, resulting in fundamental changes to how businesses operate and how they deliver value to customers

Security Transformation

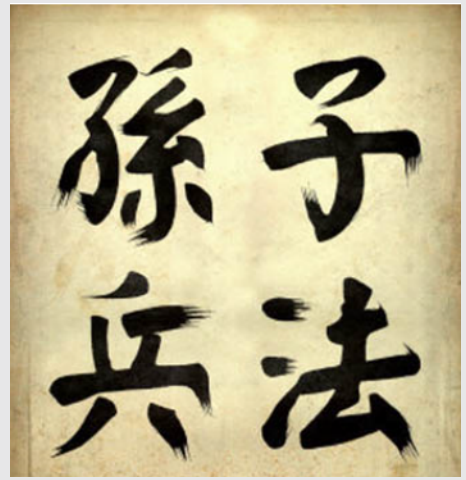


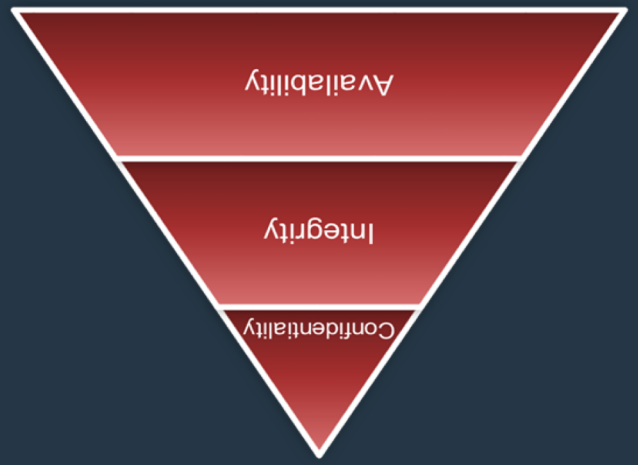
SX is the integration of security into all areas of digital technology, resulting in a Security Architecture that provides a Continuous Trust Assessment

Cultural Conflict IT vs OT

Information Technology
CIA Rule
Confidentiality, Integrity, Availablity
IT doesn't have a Systemic Safety Culture
Security isn't Systemic, it's bolt on
Protection of Data
Manipulate Data
Data is Backed up, and recoverable
Standardization
Information Technology has it's own Language
Lack of Executive Engagement and Communication

Operational Technology
SAIC Rule
Safety, Availability, Integrity, Confidentiality
Systemic Corporate Wide Safety Culture
Security isn't Systemic, it's bolt on.
Protection of Physical Processes
Manipulate Physical Things
Safety of Human Life is Paramount
Specialization
Operational Technology has it's own Language
Lack of Executive Engagement and Communication





Cultural conflict is a type of conflict that occurs when different cultural values and beliefs clash. It has been used to explain violence and crime. Jonathan H. Turner defines it as a conflict caused by "differences in cultural values and beliefs that place people at odds with one another".

Cultural conflict - Wikipedia
https://en.wikipedia.org/wiki/Cultural_conflict

FORTINET

Cyber Security Challenges to Address for a Successful Digital Transformation

Protecting Data

No matter where it is in the Network Or what State it's In

Securing OT

Extending IT security to Operation Technology Networks

Flexible Security Comsumption

To cover hybrid in a multi-cloud environment

Addressing Compliance

As part of a broader Risk Management Strategy

Expanding Threat Landscape

Requires Innovation and automation

Architecture & Technologies: Increasingly Similar

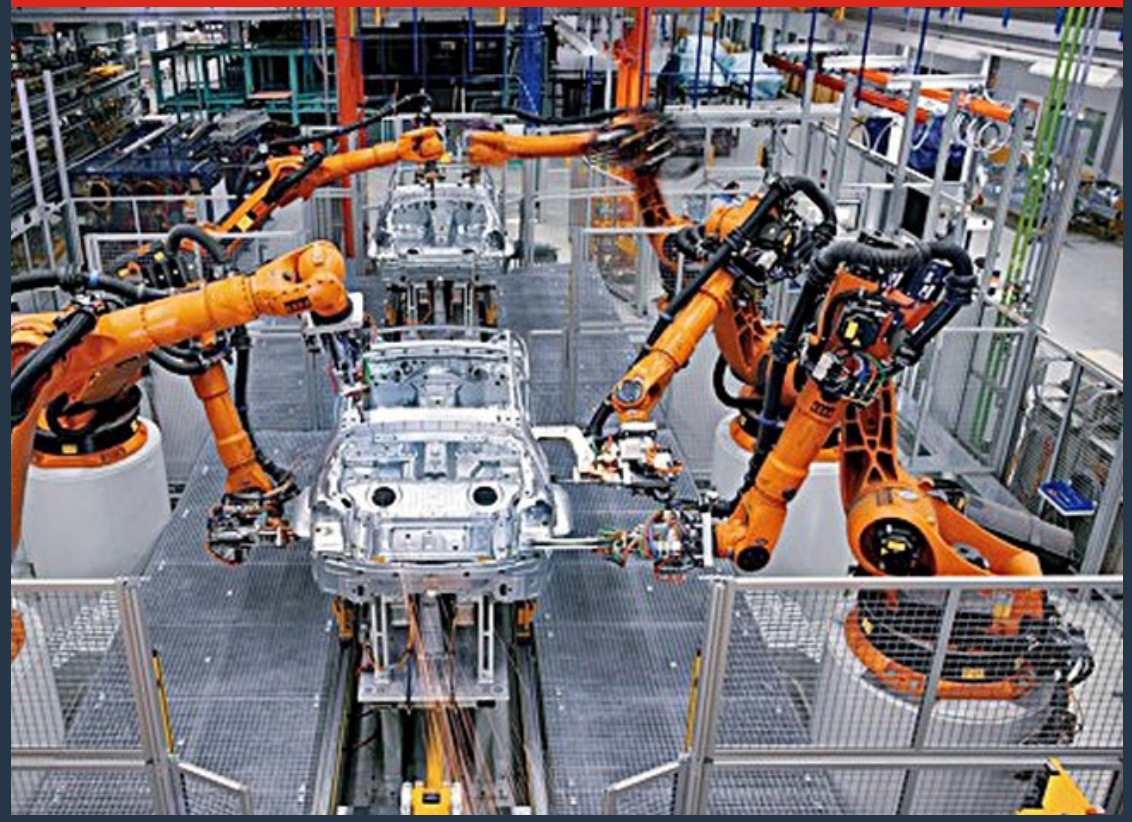
In the past, OT was …	Now OT is …	Recommended Controls…
▪ Disconnected from IT ▪ Run on proprietary bridged control protocols ▪ Connected by private fiber runs and copper ▪ Run on specialized hardware, proprietary embedded OS ▪ Out of sight, out of mind [except to long-time OT experts]	▪ Transited\Tunneled over corporate networks ▪ Riding common internet protocols ▪ Increasingly connected via wireless technologies ▪ Run on general purpose hardware, mainstream OSes ▪ Increasingly targeted by cybercriminals	▪ Segmentation and Encrypted Communication ▪ Access Control (Device, User, Application, Protocol) ▪ Secure Wireless Access ▪ Vulnerability and Patch Management ▪ Behavioral Analytics and tracking (UEBA)

What was Air Gapped and Proprietary is Increasingly Connected and General Purpose

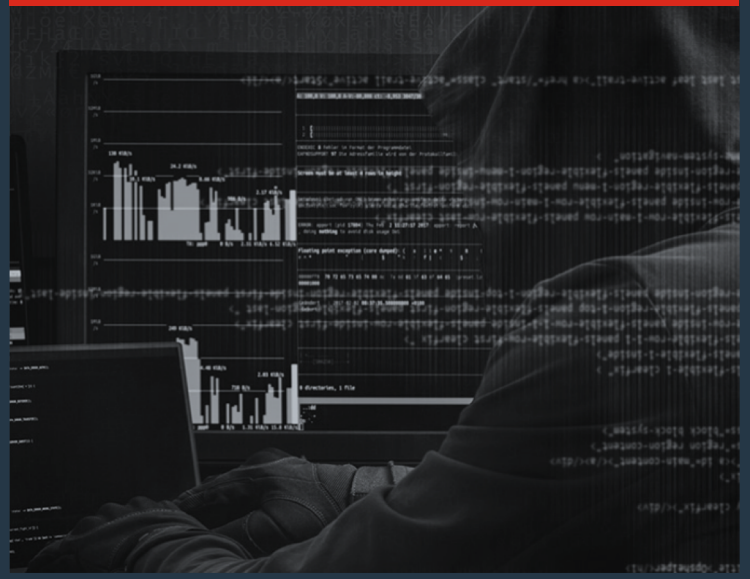
Operational Technology (OT): Used For

Monitor, Control, Operate

Industrial Automation

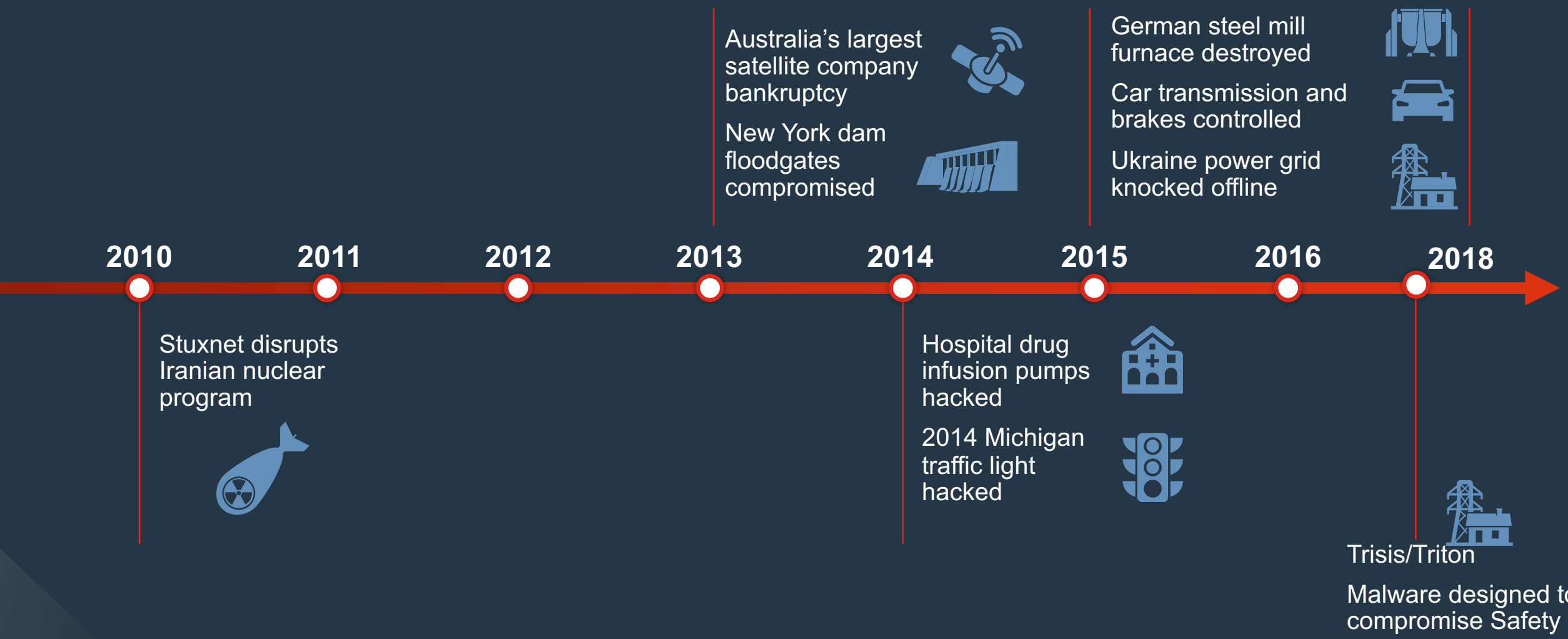


Motivations for ICS Attacks

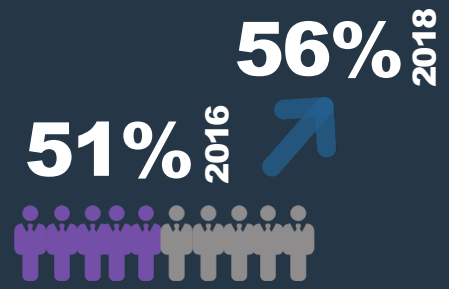
Extortion & Economical Damage	Industrial Fraud	Industrial Sabotage
		

CRITICAL INFRASTRUCTURE ATTACKS

THE RISK IS REAL



Industrial Controls Survey Trends



Surveyed reported an ICS security breach in the past year*

17%

Surveyed noted an increase in 6 or more security breaches in 2015**

15%

Surveyed required more than a month to detect a breach

44%

Surveyed were unable to identify the source of the breach

25%

By 2020, IT security vulnerabilities will be responsible for 25% of physical incidents in ICS environments

* Fortinet& Forrester – 2016 & 2018 Industrial Control Systems Security Trends: Challenges and Strategies For Securing Critical Infrastructure

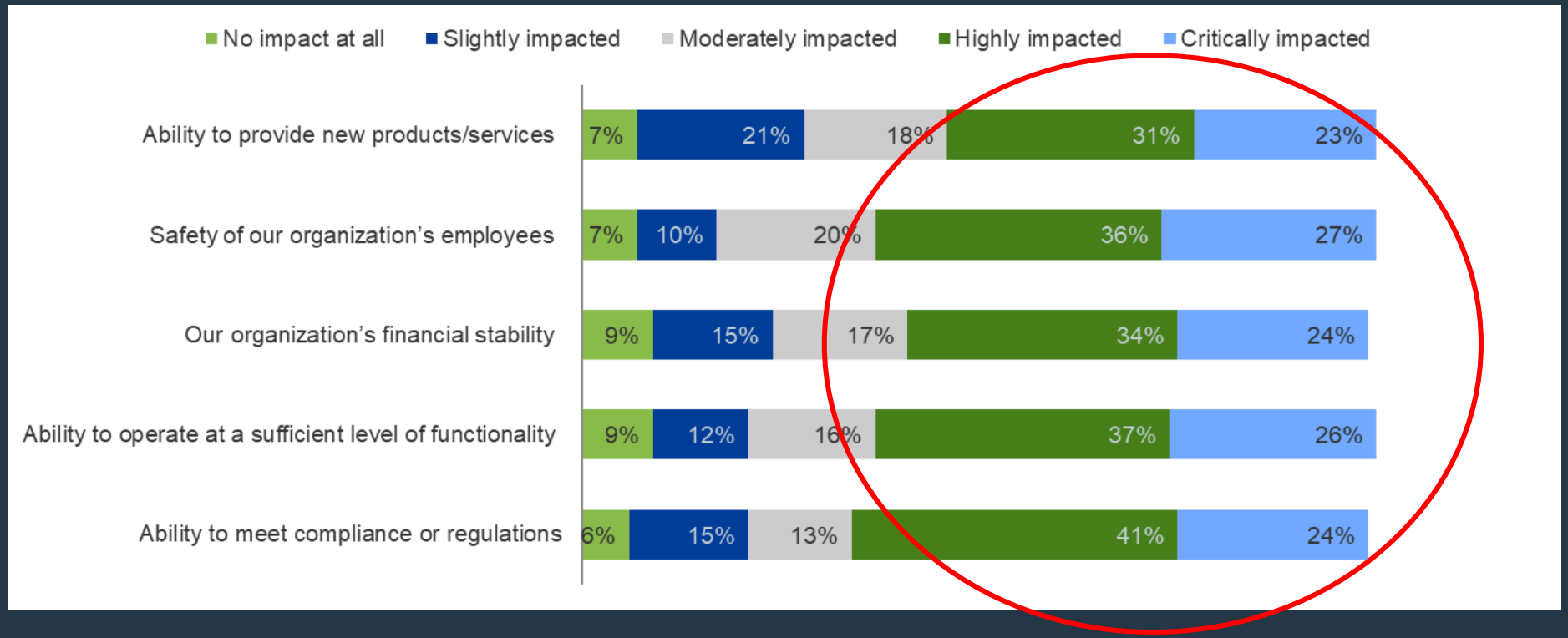
**Sans Institute Survey – The State of Security in Control Systems Today (June 2015

Sans Institute Survey – The State of Security in Control Systems Today (June 2015)

Tripwire – The State of Security- ICS Next-frontier-for-cyber-attacks (June 2016)

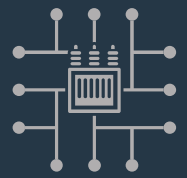
Market Situation for OT/ICS/SCADA Cybersecurity

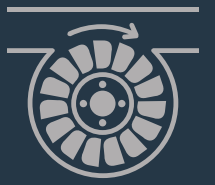
>50% of breaches had high/critical impact

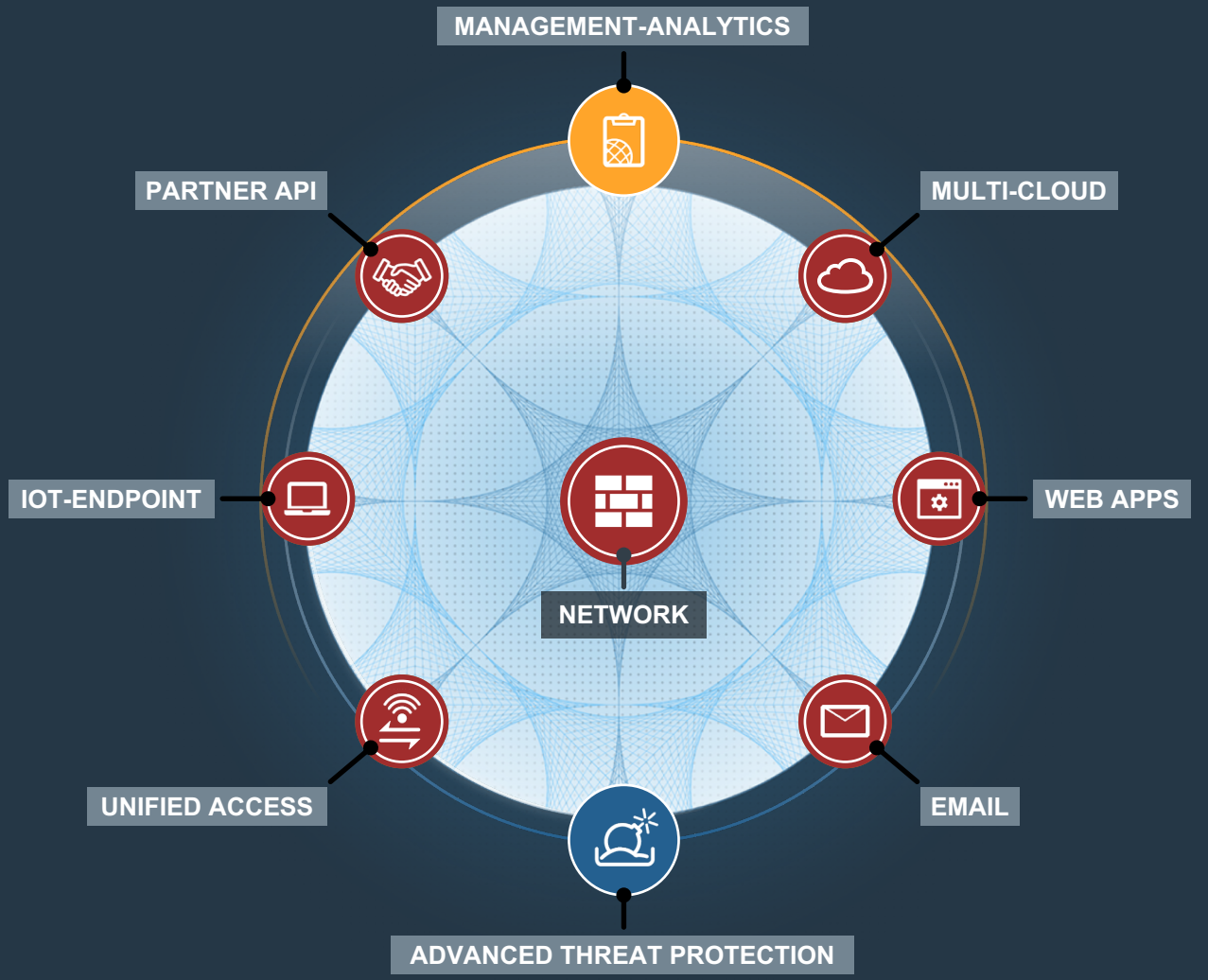


Source: A commissioned study conducted by Forrester Consulting on behalf of Fortinet, January 2018

Fortinet Security Fabric for Protecting ICS/SCADA







Use Cases with Fortinet / Nozomi Networks

Blocking Reconnaissance Activity

- New unknown node joins trusted control network (or process network)
- SCADAguardian detects it and triggers alert to FortiGate
- FortiGate enforces policy and blocks node from all access

Blocking Unauthorized Activity

- Node in trusted networks issues a command to reprogram a PLC
- SCADA guardian detects anomaly and triggers alert to FortiGate
- FortiGate enforces policy and blocks communication

Blocking Advanced Malware or Zero Day Attack

- SCADA Master changes process in subtle way towards a critical state
- SCADAguardian detects anomaly and triggers alert for FortiGate
- FortiGate enforces policy and blocks SCADA Master from all access

OT Specific Solutions

Specialized Hardware

FortiGate Rugged 60D

FortiGate Rugged 90D

- Line of Rugged Firewalls
- Line of Rugged Switches
- Line of IPS-rated wireless access points

Specialized Threat Info

- Industrial Control Services
- OT-specific protocols
- OT-specific vulnerabilities
- More signatures than any other cybersecurity vendor

Specialized Team

- Experienced professionals
- Decades in Industry
- Decades of customers

Industrial Standard and Compliance Ready

EMI

Unprotected devices can fail or be destroyed when exposed to high levels of electromagnetic interference

- A strong electromagnetic compatibility **(EMC) design is required**

Thermal

A wide (-20 to +75C) operating temp can be expected in a hash environment.

- Requires efficient heat dissipation system and self warming

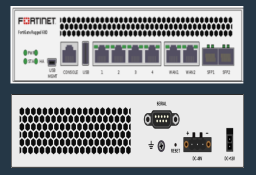
Vibration

- Devices must survive being dropped from a cabinet rack mount
- 50G anti-shock & 5-500 Mhz anti-vibration requirement is present
- Protective components are used to cushion the device

IEC-61850 describes a unified communications system design for use in electrical sub-stations. **IEC-61850-3** provides guidance on the hardware requirements of equipment deployed in this demanding environment.

Purpose-Built Rugged Devices for Industrial Solutions

	FGR-30D	FGR-35D	FGR-60D	FGR-90D
Firewall (1518/512/64 byte UDP)	900 Mbps	550 Mbps	1.5 Gbps	2 Gbps
Concurrent Sessions	750,000	750,000	500,000	2,500,000
New Sessions/Sec	5,000	5,000	4,000	20,000
IPSec VPN	45 Mbps	45 Mbps	1 Gbps	84 Mbps
IPS (Ent. Mix)	230 Mbps	230 Mbps	200 Mbps	1,100 Mbps
Interfaces (LAN, WAN & DMZ)	4 x GE RJ45 2 x SFP 2 x DB9 Serial	3 x GE RJ45	4 x GE RJ45 2 x Shared Media Pairs 1 x DB9 Serial	3 x GE RJ45 2x SFP 1 x RJ45 Bypass Pair 2 x DB9 Serial



FortiGuard for Operational Technology

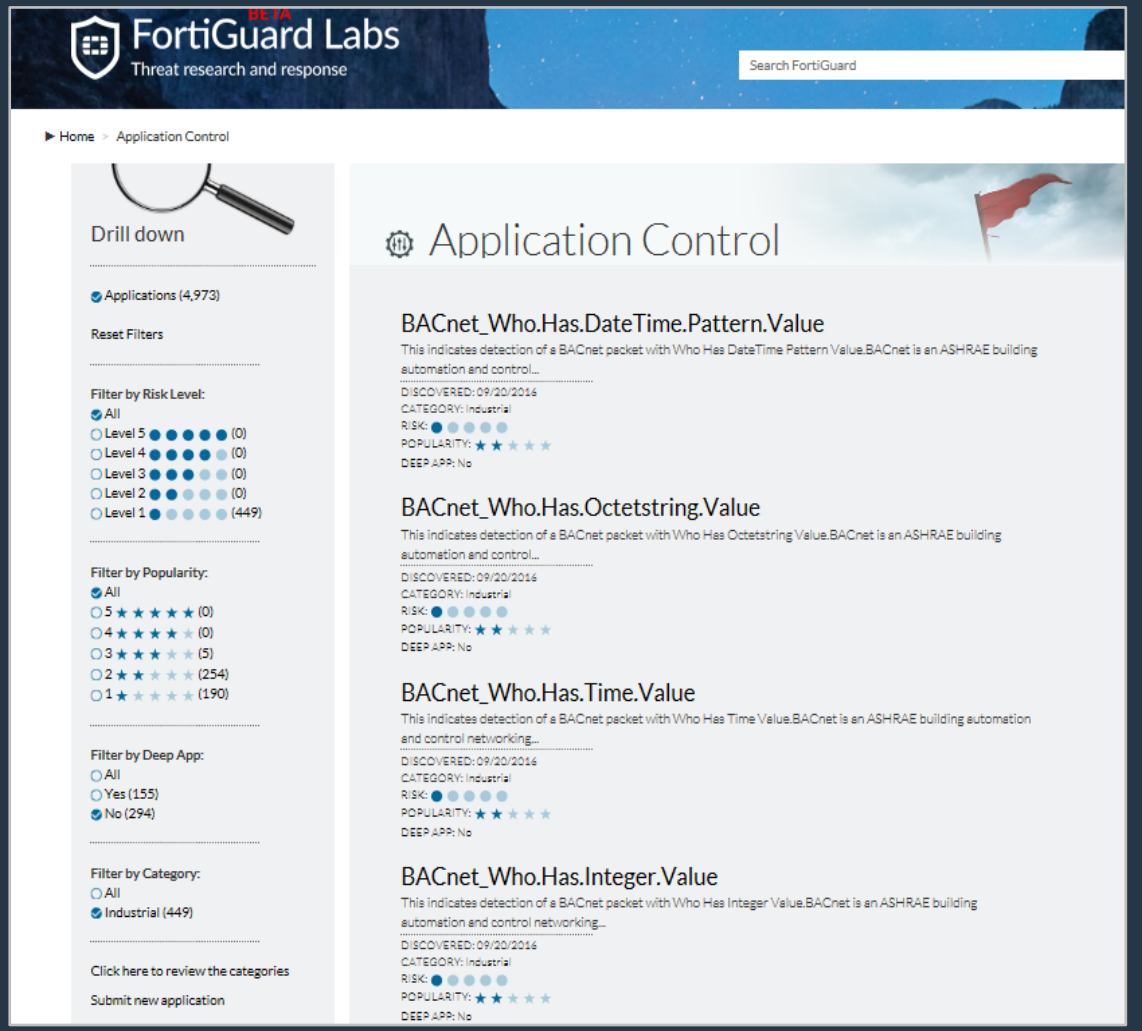
Specialized Security for OT

- Industrial Control Systems (ICS)
- Protects special type of applications
  – not generally used in an Enterprise environment
- Over 1,100 industrial app signatures

Recognized Protocols Unique to OT

Available Starting FOS 5.6

- Dedicated services offering for Operational Technology
- Fortinet adding more resources and attention for special application feeds



IPS/ Application Control for Industrial Systems

Some of the Supported Protocols

- BACnet
- DNP3
- Elcom
- EtherCAT
- EtherNet/IP
- HART
- IEC 60870-6 (TASE 2) /ICCP
- IEC 60870-5-104
- IEC 61850
- LONTalk
- MMS
- Modbus
- OPC
- Profinet
- S7
- SafetyNET
- Synchrophasor

Supported Applications & Vendors

- 7 Technologies/ Schneider Electric
- ABB
- Advantech
- Broadwin
- CitectSCADA
- CoDeSys
- Cogent
- DATAC
- Eaton
- GE
- Iconics
- InduSoft
- IntelliCom
- Measuresoft
- Microsys
- MOXA
- PcVue
- Progea
- QNX
- RealFlex
- Rockwell Automation
- RSLogix
- Siemens
- Sunway
- TeeChart
- VxWorks
- WellinTech
- Yokogawa


FORTINET