Recent Threats and Security Solution for a Smart Factory

Laksana Budiwiyono, Country Manager

DIGITECH INDONESIA 2018

Conference, Exhibition, Award

Jakarta Convention Center, 28 Oct 2018

Trend Micro

- 30 years focused on making **“A World Safe for Exchanging Digital Information”**
- Headquartered in Japan, Tokyo Exchange Nikkei Index
- Annual sales of approximately $1.3B US, consistently profitable
- Customers include 45 of top 50 global corporations
- 6000+ employees in over 50 countries

500k commercial customers &
250M+ endpoints protected

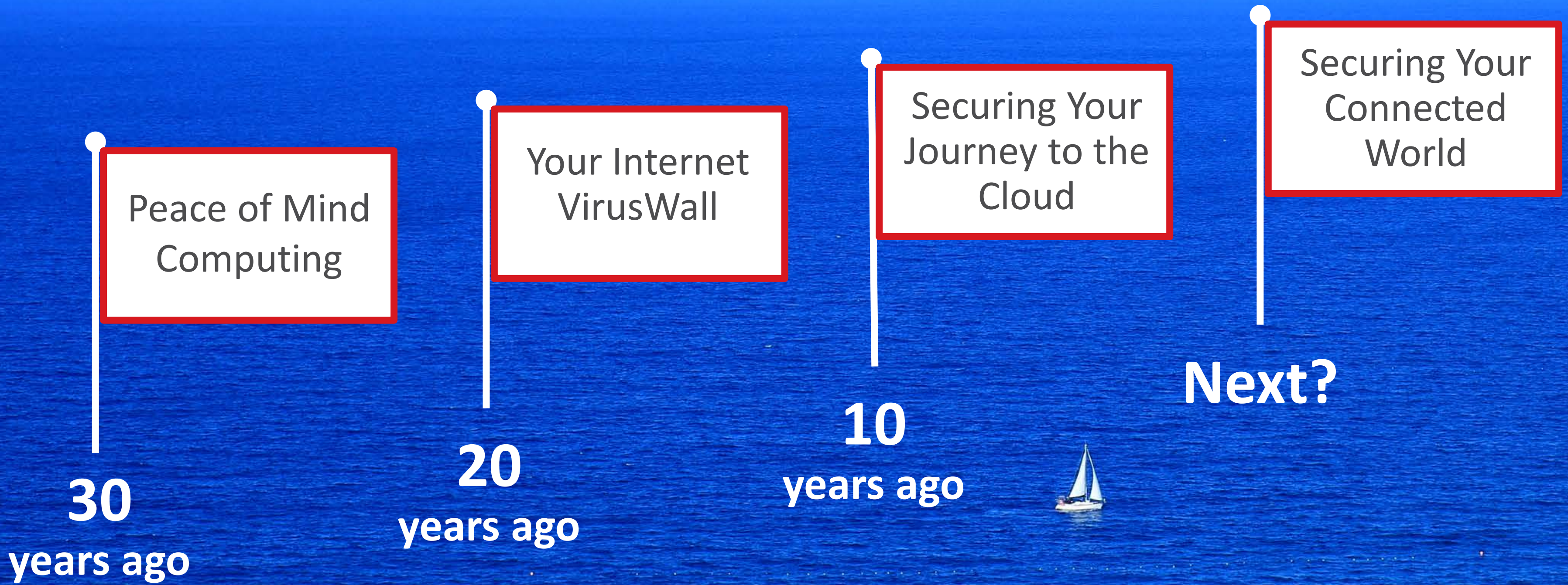
Enterprise

Midsize Business

Small Business

Consumers

VISION: A world safe for exchanging digital information



30 years ago

Peace of Mind Computing

20 years ago

Your Internet VirusWall

10 years ago

Securing Your Journey to the Cloud

Next?

Securing Your Connected World

So what’s next?

This image cannot currently be displayed.

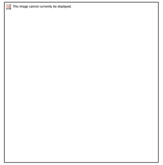
20 Billion ‘Things’ Connected by 2020

Greater reliance on cloud

IOT / 5G

Massive data & network traffic

Increasingly Stealthy Threats



Cybercriminals will further exploit server, browser and SCADA **vulnerabilities**

Your ‘network’ will extend beyond enterprise systems to include all smart devices

IT Meets OT!

mage cannot currently be displayed.

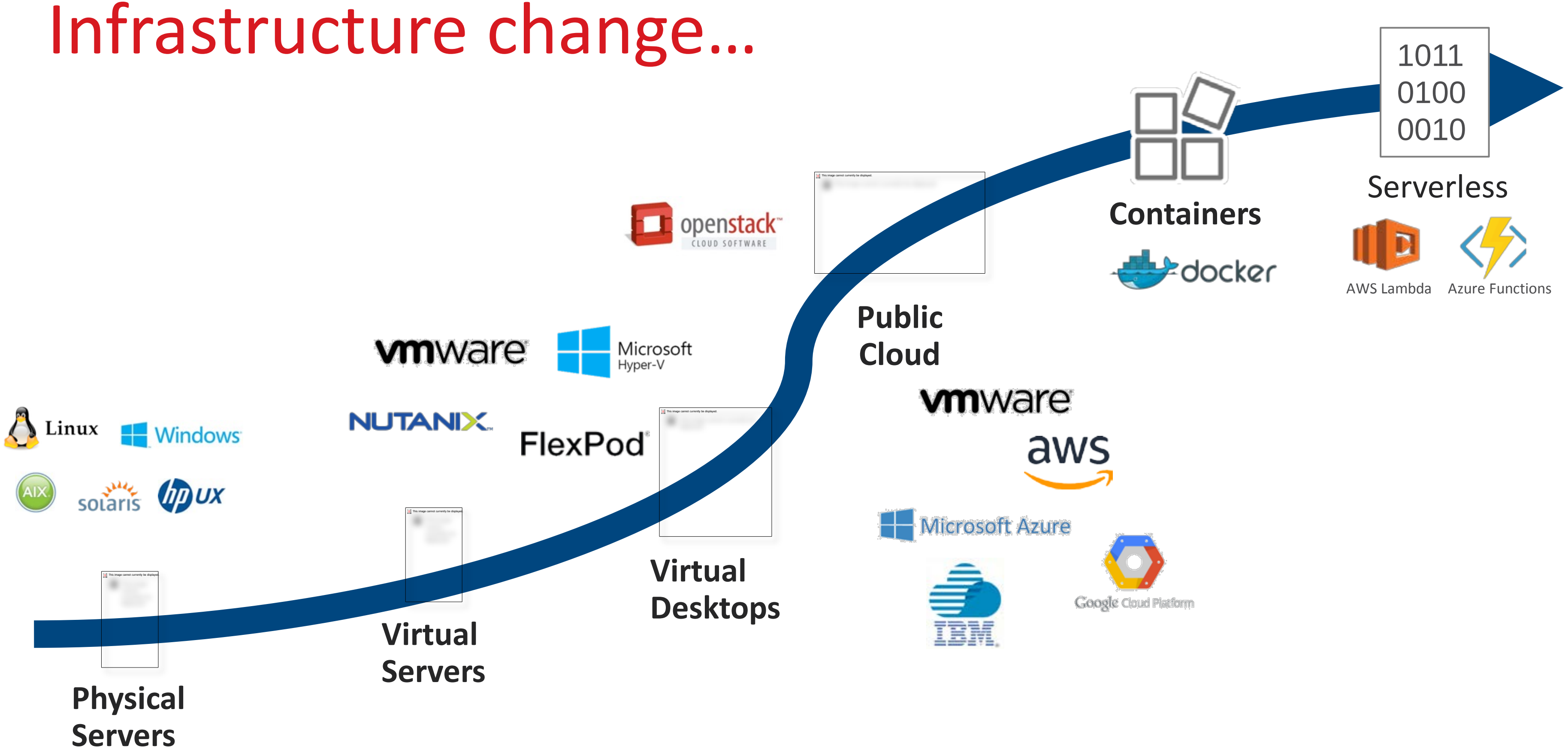
More Difficult Given Skills Shortage

1.8M

open cyber security jobs by 2022

2017 Global Information Security Workforce Study “Benchmarking Workforce Capacity and Response to Cyber Risk”, June, 2017

Infrastructure change…



Physical Servers

Virtual Servers

Virtual Desktops

Public Cloud

Containers

Serverless

Data breaches a global phenomenon

84 countries with confirmed data breaches

69% of breaches were in Finance, Information, Public, Retail, Accommodation, & Healthcare

1935 confirmed data breaches

88% of breaches align with 9 known patterns from 2014

verizon✓
2017 Data Breach Investigations Report

GDPR DEADLINE LOOMING!

On 25 May 2018, **less than 50%** will fully comply[1]

Must have: “State of the Art” security, Detect and Notify process, Security Best Practices

Fine: Up to **€20 million**, or up to **4%** of annual sales, whichever is higher

2018: Many will take actions **only when** first high-profile incident or lawsuit is filed

[1] *Gartner, “GDPR Clarity: 19 Frequently Asked Questions Answered”, August 29, 2017*

RANSOMWARE REIGNS

27 new families/month on average

94% blocked at email layer, but also can spread via **vulnerabilities** (i.e. WannaCry)

Only **60 seconds** to encrypt endpoints

Ransomware-as-a-service makes it easy, and **Bitcoin** makes it secure for cybercriminals

2018: **Higher impact targets (IIoT, GDPR)**

BUSINESS EMAIL COMPROMISE = BIG LOSSES

This image cannot currently be displayed.

Cumulative losses to exceed **$9B**

According to FBI, scams have been reported in **over 100** countries

2018: Cybercriminals seeking bigger payouts will use **Business Process Compromise**

VULNERABILITIES CONTINUE TO BE EXPLOITED

Over 1000 vulnerabilities found in 2017, including:

118 zero days

138 SCADA-related

45 browser-based

ZERO DAY INITIATIVE

2018: Cybercriminals will further leverage **SMB** and **JavaScript-based** browser vulnerabilities

Agenda

- Recent Threats and Incidents
  - Incidents
  - Increasing risks by IIoT and Industry 4.0
- Trend of Security for a Factory
  - 3 Directions of security measures
  - Customer cases

Threats and Incidents

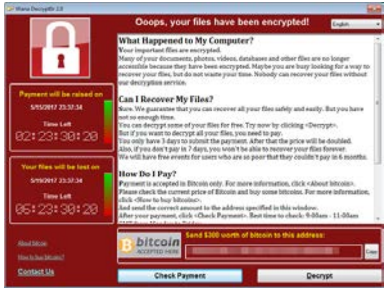
Recent Incidents and News

- RANSOMWARE disrupted factories
- COINMINER is seeking next target
- Malware infection in a factory is NOT minority

RANSOMWARE disrupted Factories

Date	Ransomware	Impact
May, ’17	WannaCry	Japanese and French major car manufacturer’s factories shutdown in Europe and German train related systems compromised.
Jun, ’17		Japanese major car manufacture’s factory shutdown a whole day in Japan.
Jun, ’17	Petya variant	American pharmaceutical company’s factory shutdown, and it brought late shipment and drop of stock price.
Aug, ’18	WannaCry Variant	Taiwanese semiconductor manufacturer‘s factories shutdown in Taiwan and caused about $200M loss.

WannaCry



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

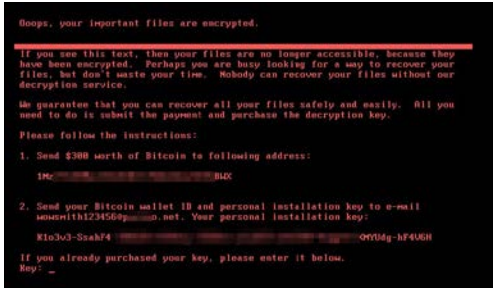
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/15/2017 23:37:34
Time Left
02:23:30:20

Your files will be lost on
5/19/2017 23:37:34
Time Left
06:23:30:20

Send $300 worth of bitcoin to this address:
[redacted]

Petya Variant



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz[redacted]BWX

2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@p[redacted]o.net. Your personal installation key:

   K1o3v3-SsahF4[redacted]<MYUdg-hF4VGH

If you already purchased your key, please enter it below.
Key: _
```

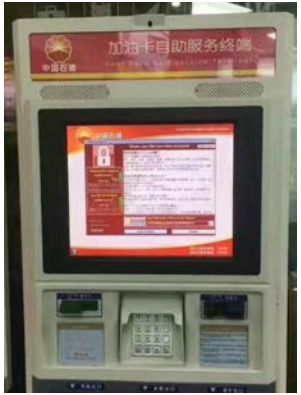
Ref: WannaCry cases

Production line

HMI in a factory

Railway control center

ATM



Payment terminal
in a gas station

Train Information Display

Ref: http://b0n1.blogspot.jp/2017/05/wannacry-ransomware-picture-collection_17.html

Ref: Another incidents in Industrial Control Systems

	Industrial Facility	Water Treating Plant	Railway Traffic Control System
Impact	Centrifugal separator crash	Loss of control for 3 months (1ML of polluted water emission)	Shutdown of train service
Cause	Stuxnet malware	Unauthorized access	Blaster malware
Path	USB flash drive or office network	Wireless link	Unknown

	Car Factory	Steel Plant	Chemical Plant
Impact	13 production line stopped/ $14M loss	Steam turbine control system stopped	8 hours of monitoring incapability
Cause	Zotob malware	DOWNAD/Conficker malware	PE_SALITY malware
Path	Carry-on PC or Office network	Unknown	Unknown

Source: http://www.ipa.go.jp/security/fy20/reports/ics-sec/rep_main_fy20.pdf, http://www.ipa.go.jp/security/fy21/reports/scada/documents/scada_report.pdf, http://www.securityincidents.org, http://www.jpcert.or.jp/ics/2011/20110210-oguma.pdf

Business Impacts of Incidents in a Factory

Not only financial damage but also company reputation and safety are affected. It is about corporate management issue.

Delay of delivery of goods

← Factory shutdown

Low physical safety

← Malfunction

Recall

← Defectives shipping

Recovery costs

← Infection

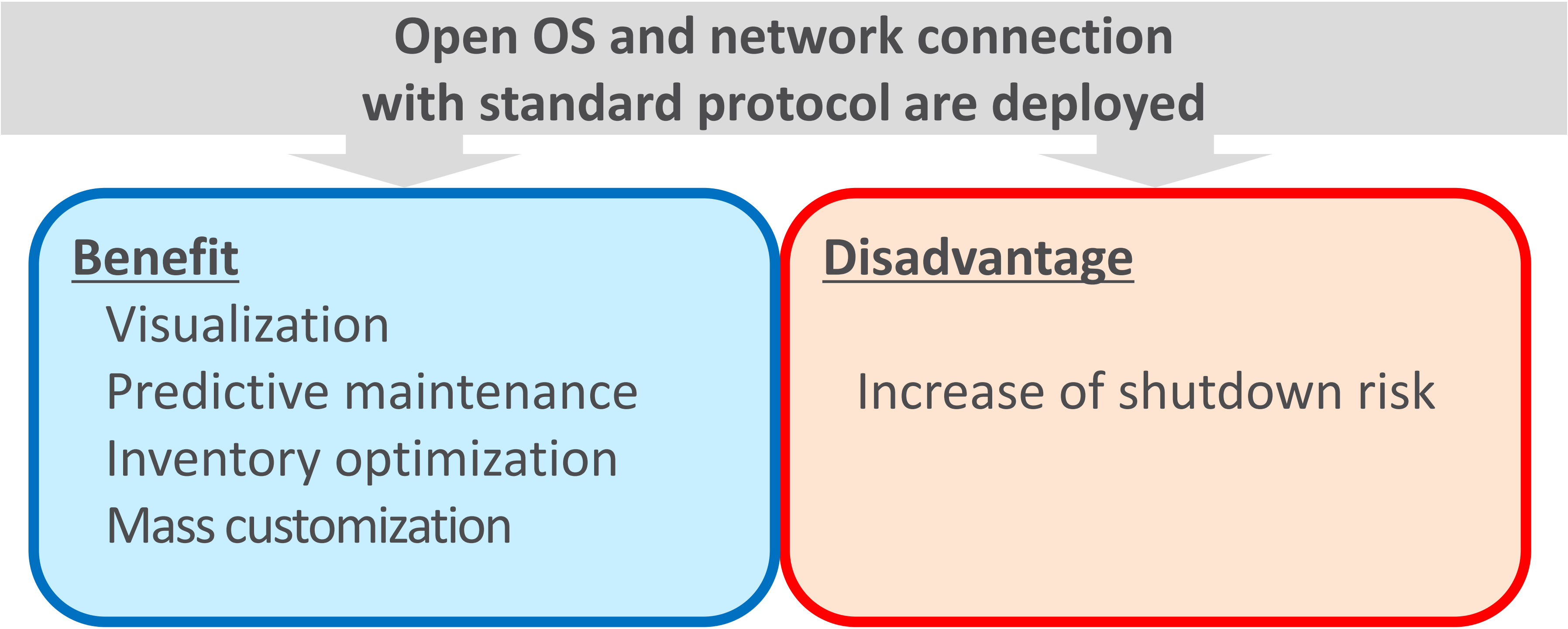
Why they couldn’t protect a factory?

- **No security or Not enough security**
  - Common concept: device vendor should have security responsibility
    - But actual damages come to asset owners and customers
  - Myth: closed environment is safe
    - Infection from USB memory stick or maintenance PC
    - Unmanaged network connection and devices
  - IS department: factory is out of scope
  - Long-term lifecycle
    - Legacy OS, non-patched systems
    - No program update due to the importance on Availability
  - Device vendor prohibits to install other software
  - Security product: signature file is never up-to-date
- **Not enough operational rules**
  - Rules are hard to thoroughly uphold and complex

Why did damage expand in a factory?

- Infection through Network and/or USB flash drive
- One-off device and difficult to replace it
- No Incident response rule and organization
- Fail to notice a malicious behavior
- Fake UI (i.e., STUXNET)

Increasing Risks by IIoT and Industry 4.0



Open OS and network connection with standard protocol are deployed

Benefit

- Visualization
- Predictive maintenance
- Inventory optimization
- Mass customization

Disadvantage

- Increase of shutdown risk

Trend of security for a factory

Background of security deployments

- **Risk management by executives**
  - Factory shutdown damages in company reputation
    - Shutdown 1 hour = Loss of USD few million
  - Risk of lawsuits
  - Government’s enforcement

- **Mind-set change in OT admin**
  - Cyber incident causes an identical result, *a factory shutdown*, as physical incident

3 Direction of Security Measures

1. Establish Security Standard

2. Defense in Depth

3. Develop Organization and Human Resources

1. Establish Security Standard

Preparation of Security Standard for the entire system life-cycle

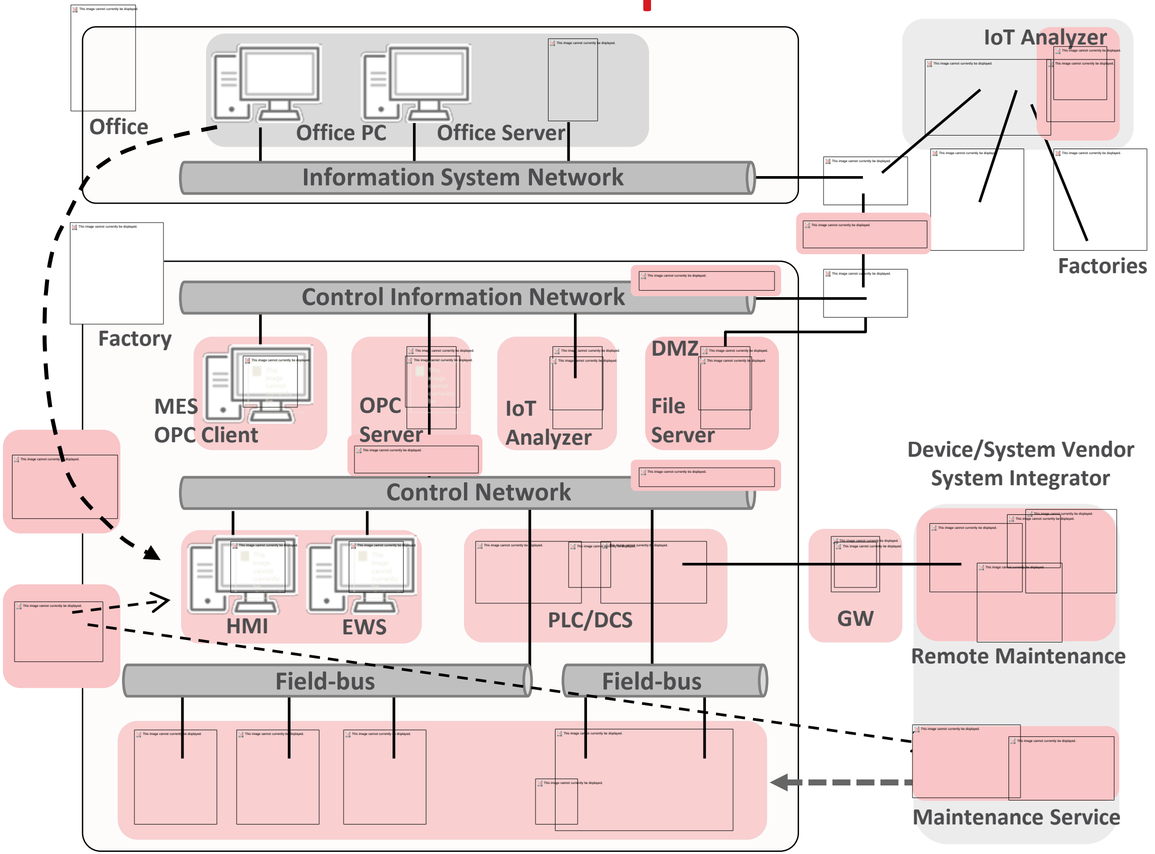
Basic Concept	Requirement Definition	Design / Development	Deployment / Operation
• Making security guideline • Continuous budget for security • Organization for security • etc…	• Considering security in requirements • Designing system based on security standard like IEC62443 • Building Incident Response process • etc…	• Secure coding • Redundant system • Fuzz testing, Penetration testing • Utilizing a test-bed • etc…	• Operation scheme based on CSMS • Review of normal operation, i.e., use of external medias • Clarifying Incident Response process • Regular assets inventories • etc…

2. Defense in Depth

- **Direction**
  - Existing Factory: Minimizing downtime
    - Early anomaly detection and rapid recovery from damages without changing existing facilities
  - New Factory: Prevention
    - Protection without impacting on availability and performance

- **3 Steps approach**
  1. Prevent incoming threats and attacks
  2. Existing Factory: Anomaly detection without system changes.
     New Factory: Prevent facilities and devices from threats
  3. Quick recovery

Solution Example: New Factory



TippingPoint™ Threat Protection System

Next generation IPS
against vulnerability attack

Deep Discovery™ Inspector

Early anomaly detection
Threats’ visibility

Trend Micro Safe Lock™

Lockdown AV software
without using pattern file

Trend Micro Portable Security 2™

USB shaped AV scanning tool
without software installation

Trend Micro USB Security™

Secure USB flash drive

** Available in specific regions only*

Trend Micro Deep Security™

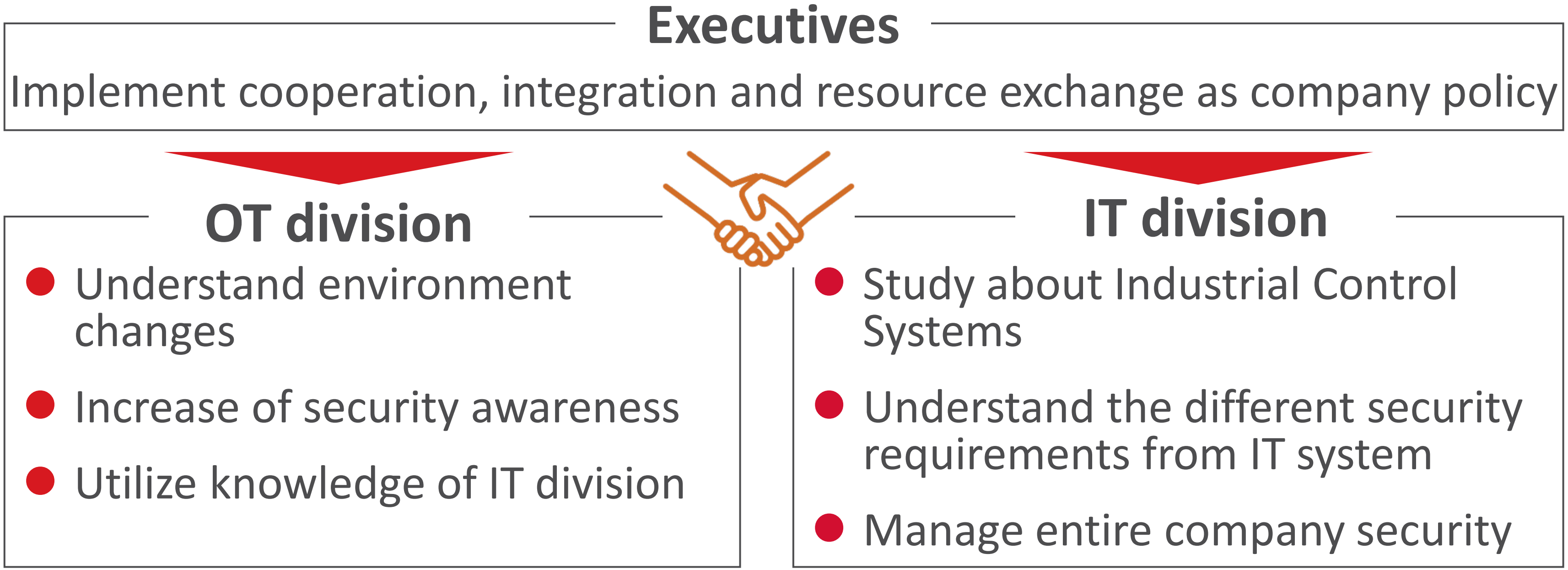
Next generation server security solution

Trend Micro IoT Security

Security software for
IoT devices

3. Develop Organization and Human Resources

Utilize knowledge and experiences of IT security for factory security
Establish a cooperative structure of resource development and central management



Executives

Implement cooperation, integration and resource exchange as company policy

OT division

- Understand environment changes
- Increase of security awareness
- Utilize knowledge of IT division

IT division

- Study about Industrial Control Systems
- Understand the different security requirements from IT system
- Manage entire company security

Market Leadership Position

HYBRID CLOUD SECURITY

IDC

The **market leader**
in server security
for **7 straight years**

Gartner

Trend Micro delivers **the most cloud security controls (16 of 21)** of all evaluated vendors.

- IDC, Securing the Server Compute Evolution: Hybrid Cloud Has Transformed the Datacenter, January 2017 #US41867116
- Gartner "Market Guide for Cloud Workload Protection Platforms", Neil MacDonald, March 22, 2017

NETWORK DEFENSE

NSS LABS

Recommended Breach Detection System
for **4 straight years**, and
Recommended Next-generation IPS

Gartner

Leader in Gartner Magic Quadrant for Intrusion Detection and Prevention Systems, January 2018

- NSS Labs Breach Detection Test Results (2014-2017);
  NSS NGIPS Test Results, 2017
- *http://www.trendmicro.com/us/business/cyber-security/gartner-idps-report/*

USER PROTECTION

Gartner

Named a Leader Once Again in the Gartner Magic Quadrant for Endpoint Protection Platforms, Jan 2018

AV TEST

#1 in protection and performance

- *https://resources.trendmicro.com/Gartner-Magic-Quadrant-Endpoints.html*
- av-test.org (Jan 2014 to Dec 2017)

TREND MICRO™

Enables your business and reduces risk

Automates security & streamlines incident response

Simplifies compliance and enables tool consolidation

FREE! Phishing Awareness Service

Send users a realistic phishing campaign

Login Alert

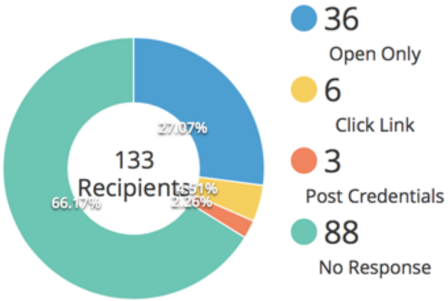
Hi Matthew

Your account was recently logged into from a new browser or device. Was this you?

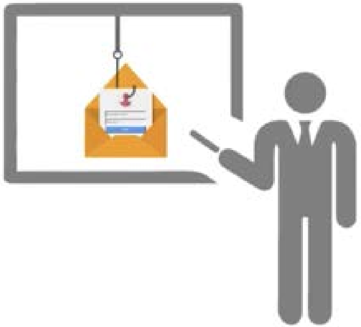
New Login

- February 9, 2018 at 5:30pm
- Near Panchiaochen, Taiwan
- Chome on Windows

Analyze the results



Raise user awareness with training



https://phishinsight.trendmicro.com

PHISH INSIGHT

TREND MICRO

Thank you!