



Cybersecurity for Industry 4.0

Garrick Ng

Cyber Security Professionals Awards – Gold Winner

Smart City Consortium Security SIG Chairman

Chief Technology Officer

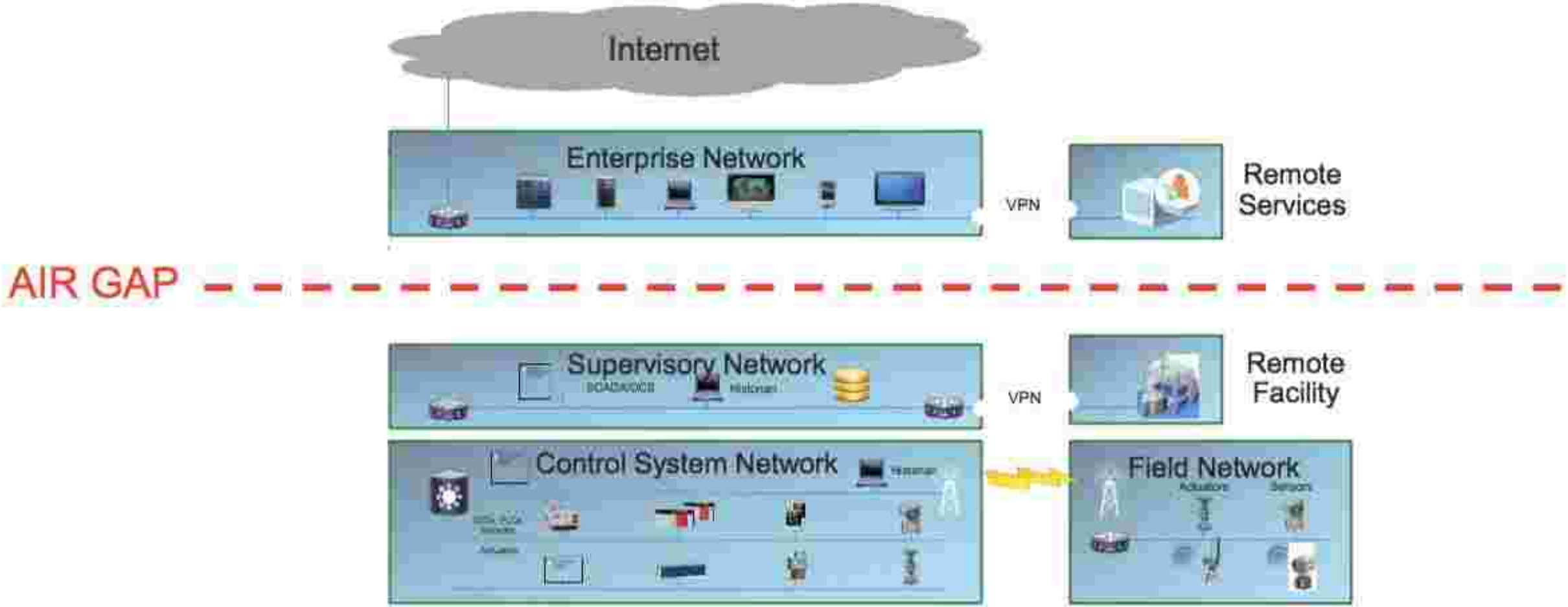
Cisco Hong Kong, Macau, Taiwan

Nov 2017

Hacker's view



Industrial Network Security





Iran Natanz Nuclear Facility ... Stuxnet

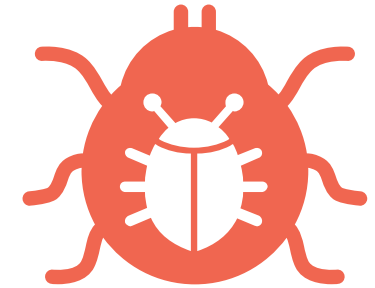
Industrial Systems as **Attack Surface**

Automation vendors still ship updates on **EOL Windows platforms**

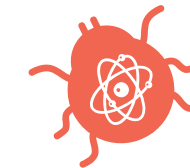
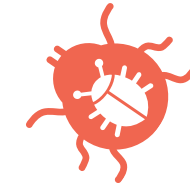
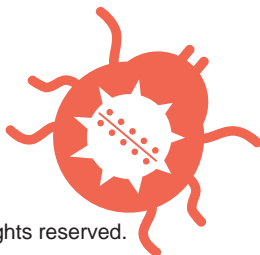
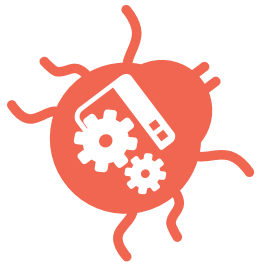


Vulnerabilities found in industrial systems rose **2400%** from 2009 to 2015

The most common ethernet based OT protocol **lacked authentication until Fall of 2015**



Yet ethernet in manufacturing grew **96%** the three years before





Welcome to C-Office



C-Service

C-Service online version on C-Office

C-Service contains electronic spare part catalogues, drawings and electronic service handbooks for Hlab company products. To get access to Hlab C-Service please contact you nearest Hlab company service representative.

C-Service online version requires .NET framework 1.1 to be installed. If you don't have .NET framework 1.1 installed, you can install it from [windows update](#) (recommended) or download it from [Microsoft](#).

You also need to install this setup [package](#), which set your .NET framework to fully trust the www.c-office.com site. Install this package after you have completely installed .NET framework 1.1.



ABB IRB140

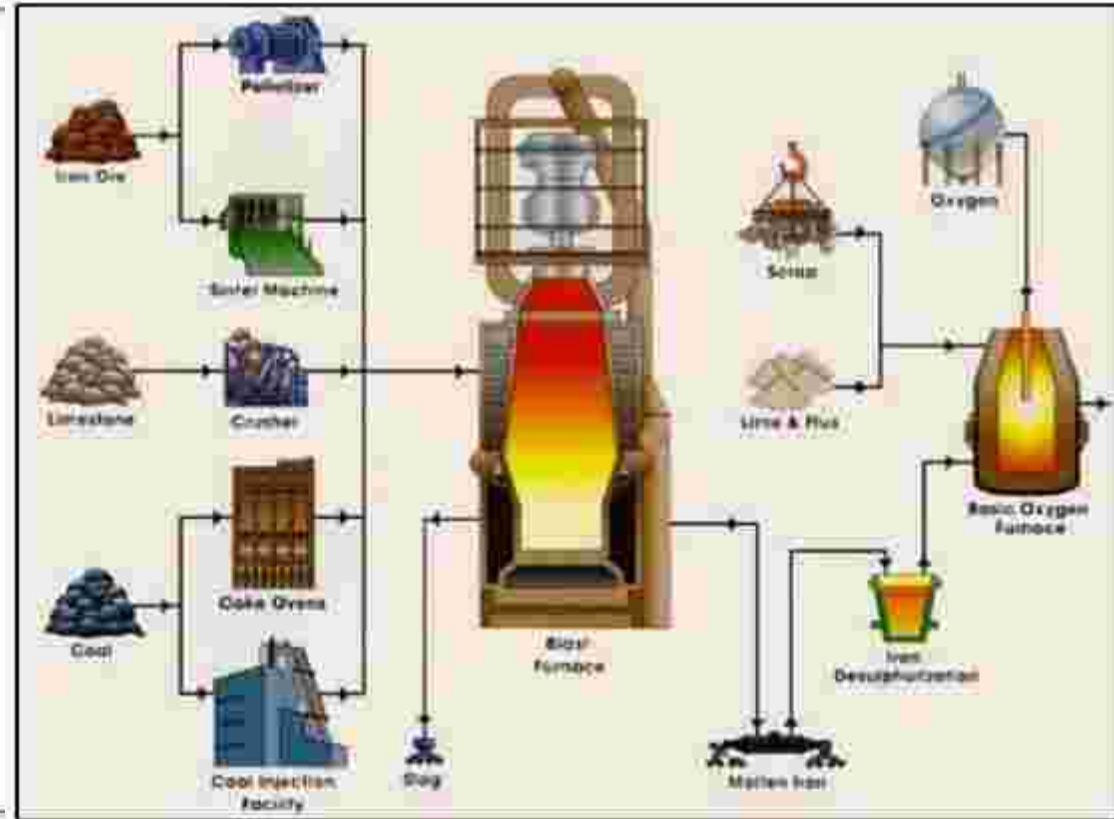
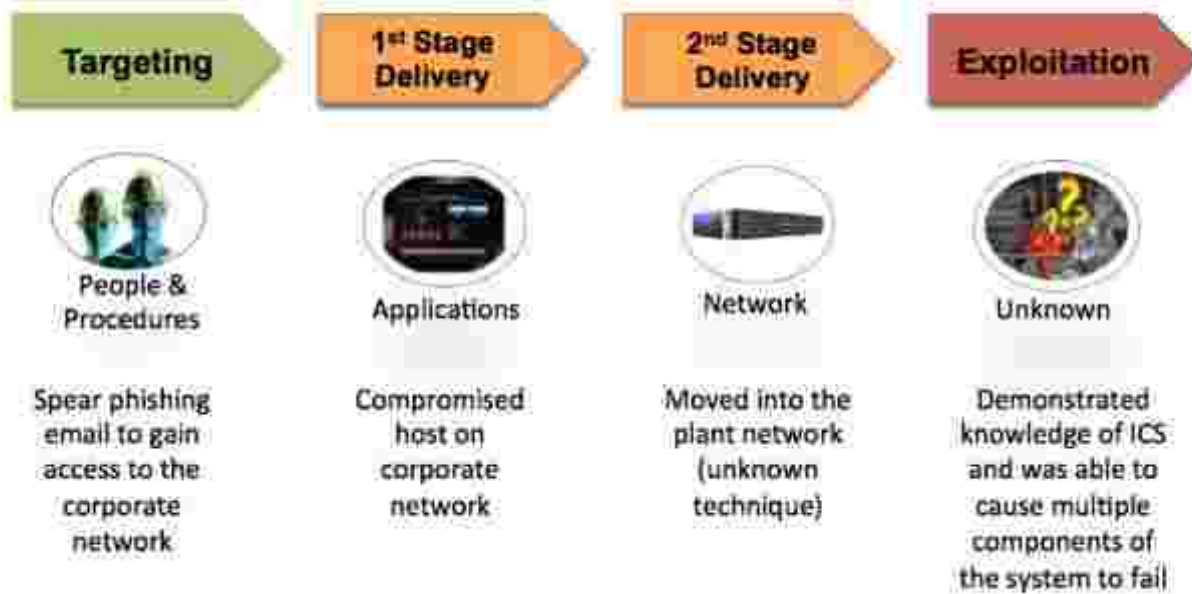


German Steel Mill Massive damage

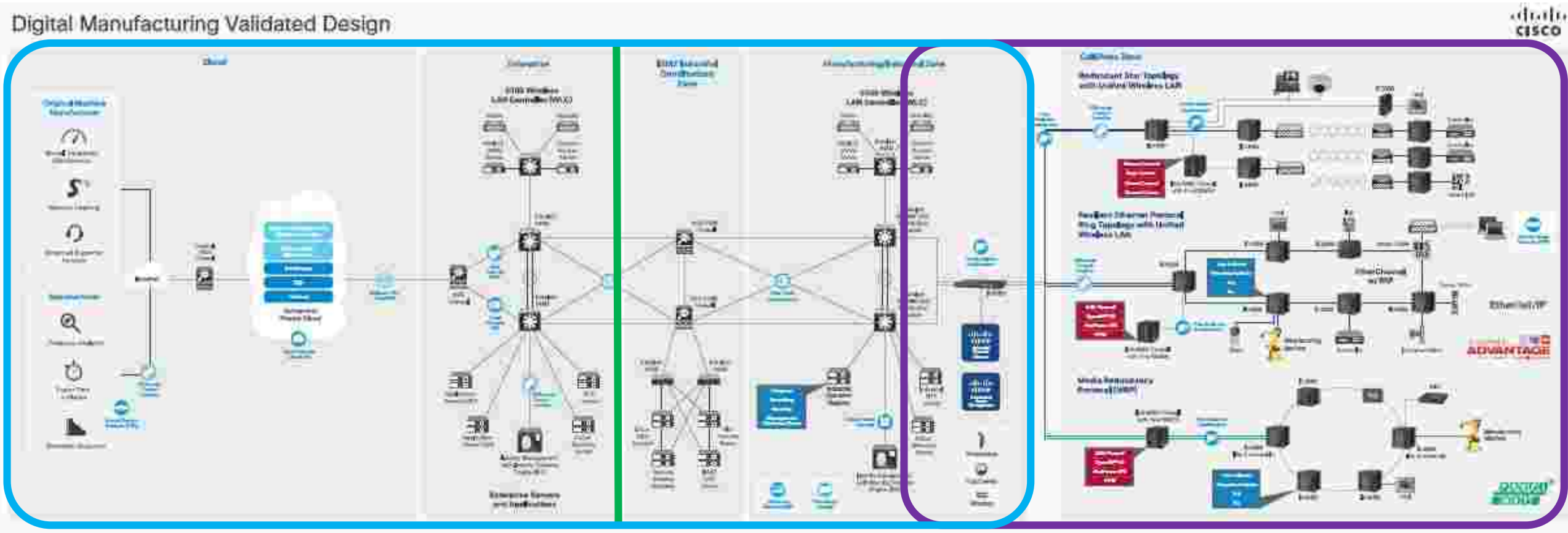
Attack on German Smelter

Exploited Vulnerabilities by ICS Component

German Steel Mill Incident



Cisco Validated Designs – Digital Manufacturing



IT/OT Alignment





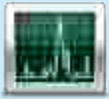




Source: <http://www.sensationalquotes.com/Dating.html>

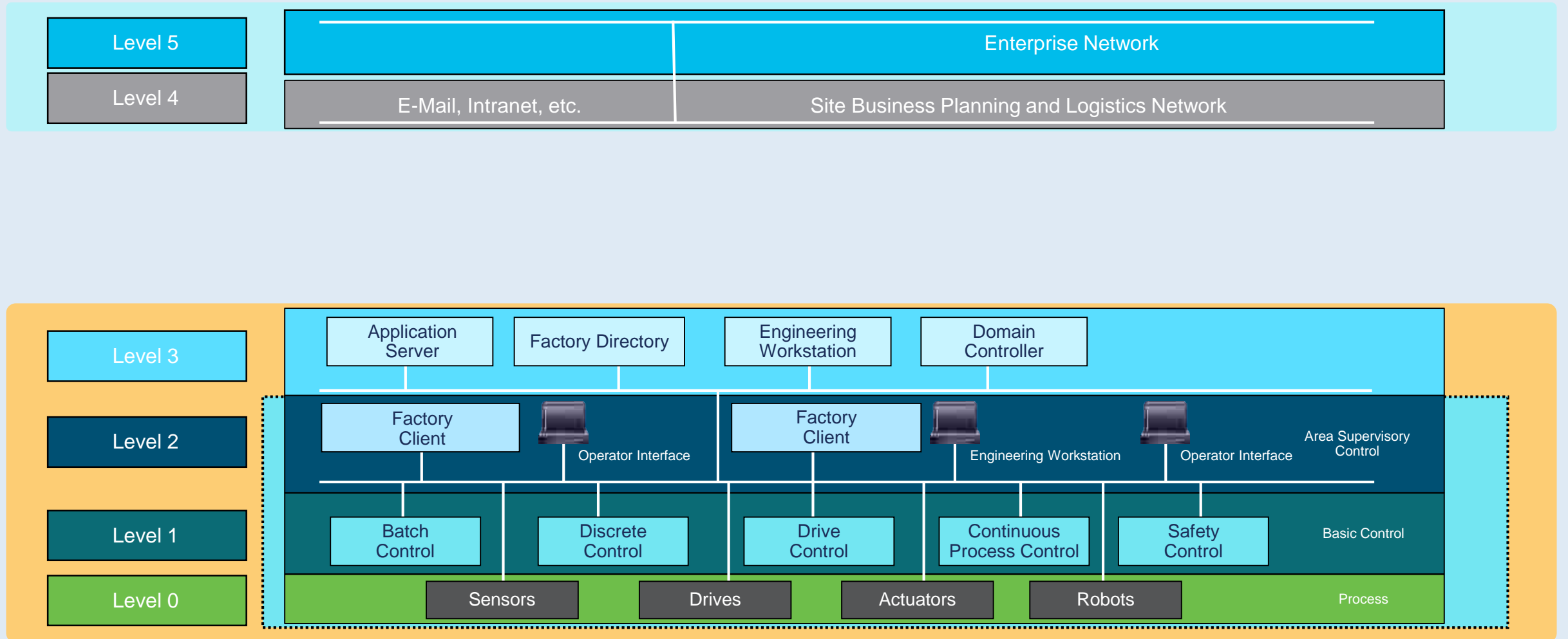
IT (Information Technology) Vs OT (Operation Technology)

Security Policies	IT Network	OT Network
Focus	Protecting Intellectual Property and Company Assets	24/7 Operations, High OEE, Safety, and Ease of Use
Priorities	<ol style="list-style-type: none"> 1. Confidentiality 2. Integrity 3. Availability 	<ol style="list-style-type: none"> 1. Availability 2. Integrity 3. Confidentiality
Types of Data Traffic	Converged Network of Data, Voice and Video (Hierarchical)	Converged Network of Data, Control Protocols, Information, Safety and Motion (P2P & Hierarchical)
Implications of a Device Failure	Continues to Operate	Could Stop Processes, Impact Markets, Physical Harm
Threat Protection	Shut Down Access to Detected Threat and Remediate	Potentially Keep Operating with a Detected Threat
Upgrades and Patch Mgmt	ASAP During Uptime	Scheduled During Downtime (months, years)
Infrastructure Life Cycle	Equipment upgrades and refresh <5yr	Avoid Equipment upgrades (lifespan 15+ yrs)
Deployment conditions	Controlled physical environments	Harsh environments (temp, vibration, etc)

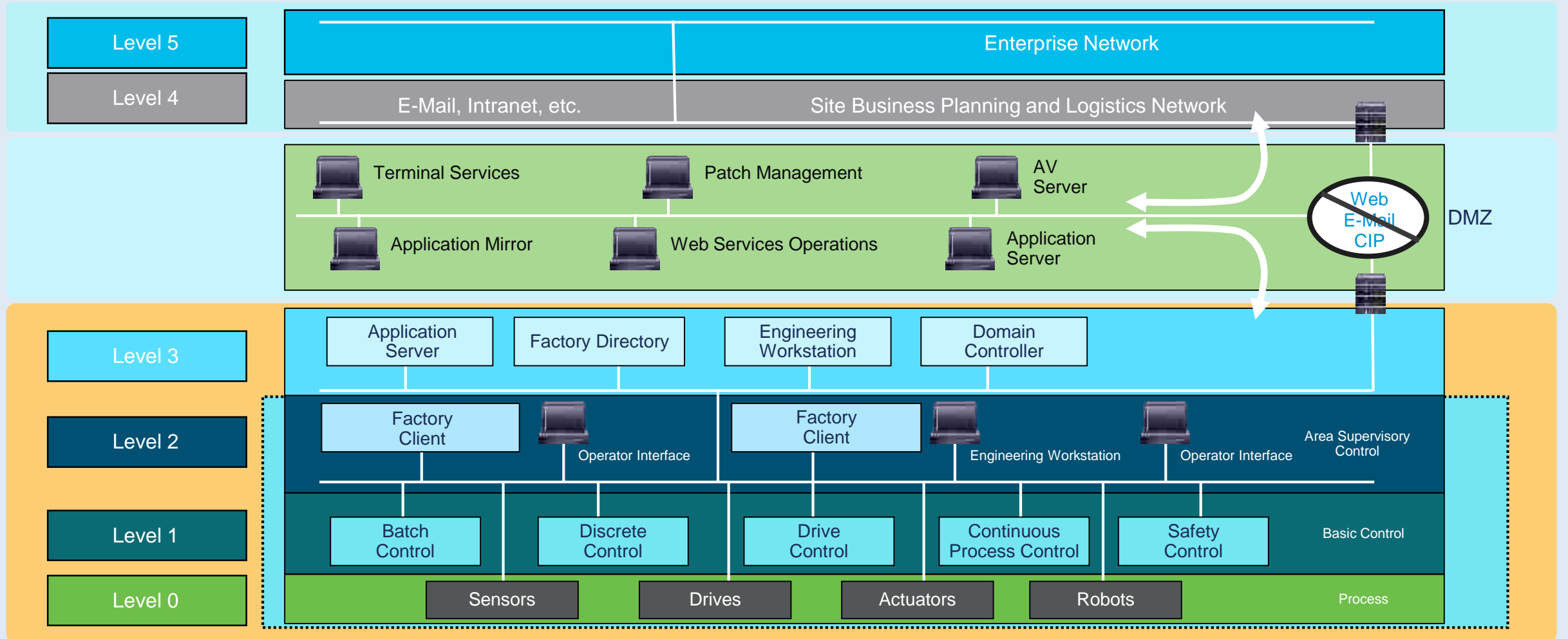
Assets we need to protect

	Asset	Description	Examples and Notes
	IEDs	Intelligent Electronic Device – Commonly used within a control system, and is equipped with a small microprocessor to communicate digitally.	Sensor, actuator, motor, transformer, circuit breaker, pump
	RTUs	Remote Terminal Unit – Typically used in a substation or remote location. It monitors field parameters and transmit data back to central station.	Overlap with PLC in terms of capability and functionality
	PLCs	Programmable Logic Controller – A specialized computer used to automate control functions within industrial network.	Most PLCs do not use commercial OS, and use “ladder logic” for control functions
	HMIs	Human Machine Interfaces – Operator’s dashboard or control panel to monitor and control PLCs, RTUs, and IEDs.	HMIs are typically modern control software running on modern operating systems (e.g. Windows).
	Supervisory Workstations	Collect information from industrial assets and present the information for supervisory purposes.	A supervisory workstation usually windows
	Data Historians	Software system that collects point values and other information from industrial devices and store them in specialized database.	Typically with built-in high availability and replicated across the industrial network.
	Other Assets	Many other devices may be connected to an industrial network.	For example, printers can be connected directly to a control loop.

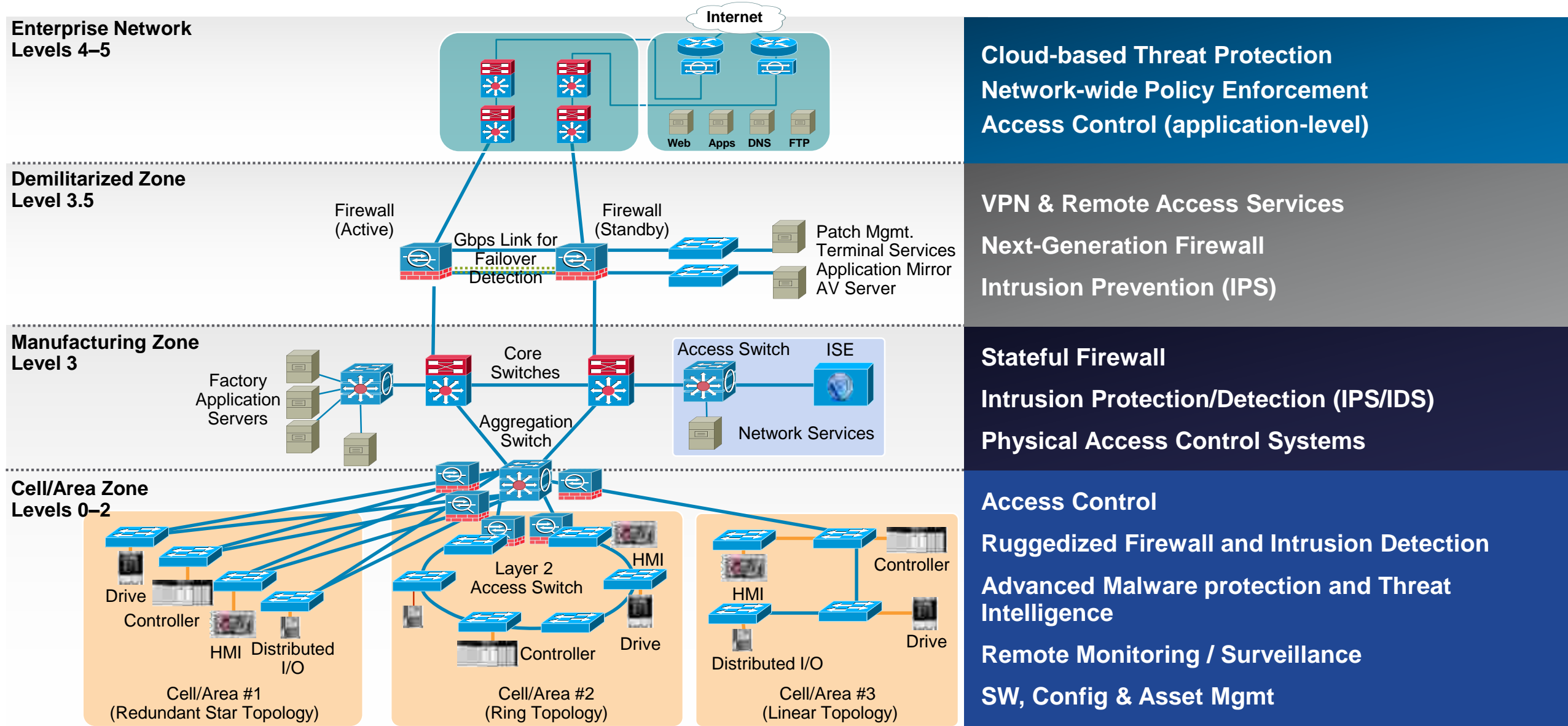
ISA 99 / IEC 62443 / Purdue Model for Manufacturing



ISA 99 / IEC 62443 / Purdue Model for Manufacturing



IT/OT Converged Security Model (CPwE Reference Architecture)



Cloud-based Threat Protection
 Network-wide Policy Enforcement
 Access Control (application-level)

VPN & Remote Access Services
 Next-Generation Firewall
 Intrusion Prevention (IPS)

Stateful Firewall
 Intrusion Protection/Detection (IPS/IDS)
 Physical Access Control Systems

Access Control
 Ruggedized Firewall and Intrusion Detection
 Advanced Malware protection and Threat Intelligence
 Remote Monitoring / Surveillance
 SW, Config & Asset Mgmt

Secured Connectivity

Key Security features:

FIPS 140-2

Port Security

802.1X

dACL's

*Multi-domain authentication

Cisco Trustsec

*SGACL

*SGT Inline Tagging

*MACSEC

Dynamic ARP inspection

DHCP Snooping


TACACS & Radius


Vlan assignment




Industrial Firewall ISA 3000



 Manufacturing

 Transportation

 Energy

Stateful inspection industrial firewall (IPS, AVC, Anti-malware)

Industrial protocol (DNP3, Modbus, IEC 60870, CIP)
visibility and rules for known vulnerabilities

Vulnerability protections for ICS, Windows, MES
components, OT applications, NW infrastructure

High-performance VPN, DNS, DHCP, NAT Netflow

Hardware bypass, alarm I/O, dual-DC power, rapid set
up via SD card, PTP support in HW

Industrial protocol specific parsing, protocol abuse
control, detect set-point level changes

High Availability and latency controls

Certified for power substations, industrial, and railway
and helps meet NERC-CIP, ISA99, IEC 62443

IoT Threat Defense



Remote Access

Secure third-party access with control and visibility



Segmentation & Access Control

Extensible, scalable segmentation to protect IoT devices



Visibility & Analysis

Detect anomalies, block threats, identify compromised hosts

Secure remote access



Remote vendor
support

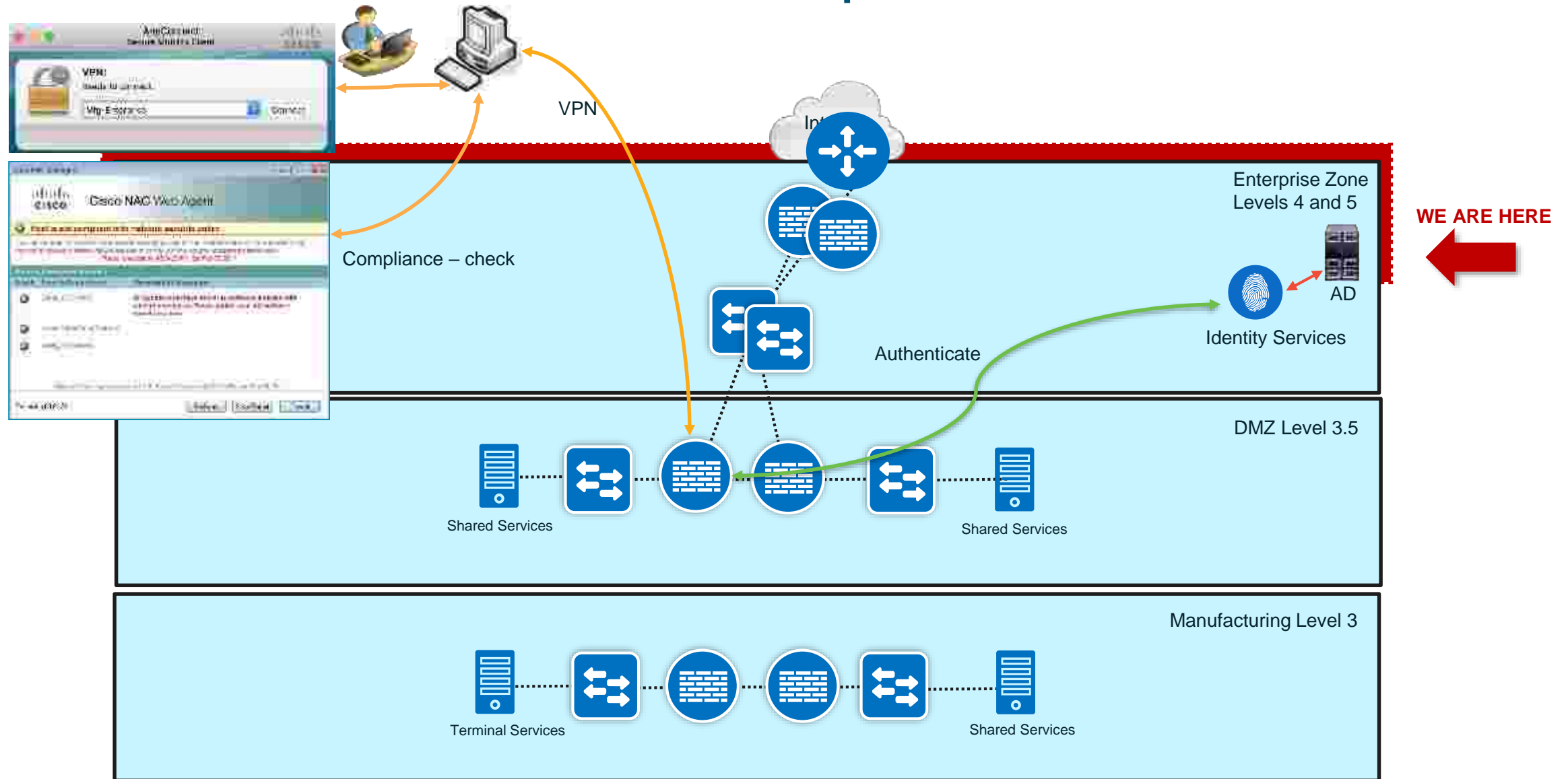


Defense vulnerabilities

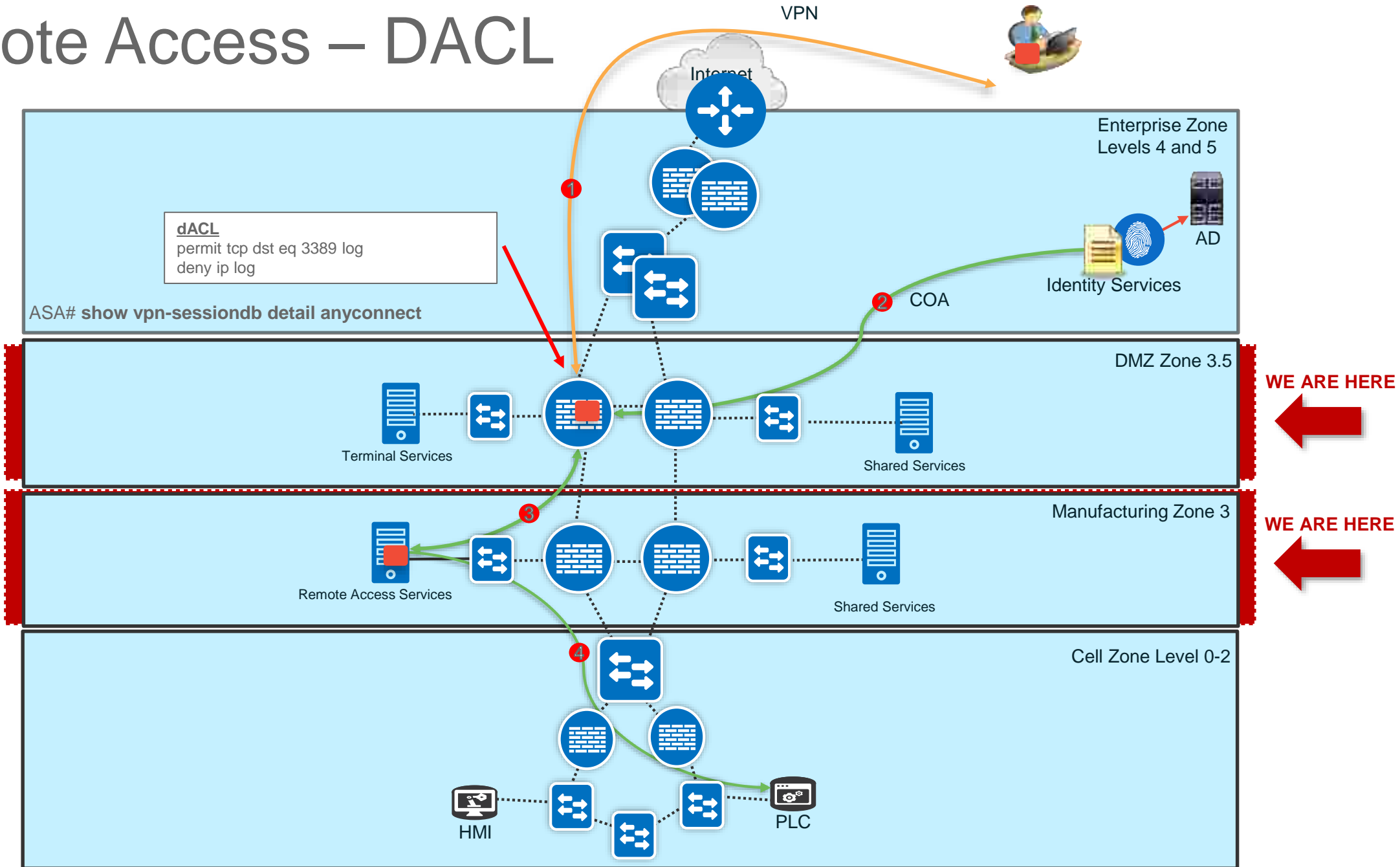


Visibility at risk

Vendor Access – VPN & Compliance



Remote Access – DACL





Segmentation & Access Control

IoT Threat Defense also helps with segmentation by:



Protect inbound and
outbound
communications and
from each other



Management



Segment
Infrastructure
based on role and
policy



Compliance
and best
practice

Introducing Cisco TrustSec



Traditional Security Policy - ACL



Business Policy

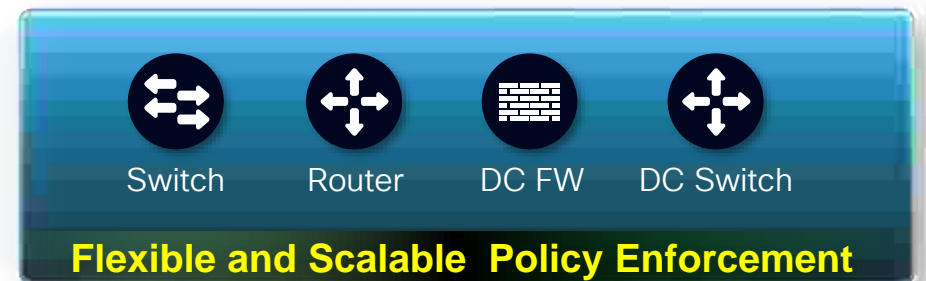


Protected Assets

	Production Servers	Development Servers	Internet Access
Employee (managed asset)	PERMIT	DENY	PERMIT
Employee (Registered BYOD)	PERMIT	DENY	PERMIT
Employee (Unknown BYOD)	DENY	DENY	PERMIT
ENG VDI System	DENY	PERMIT	PERMIT

Source

software defined
segmentation



Visibility and Analysis



IoT Threat Defense also analyzes network traffic entering and exiting your organization to:



Detect anomalies



Block attacks



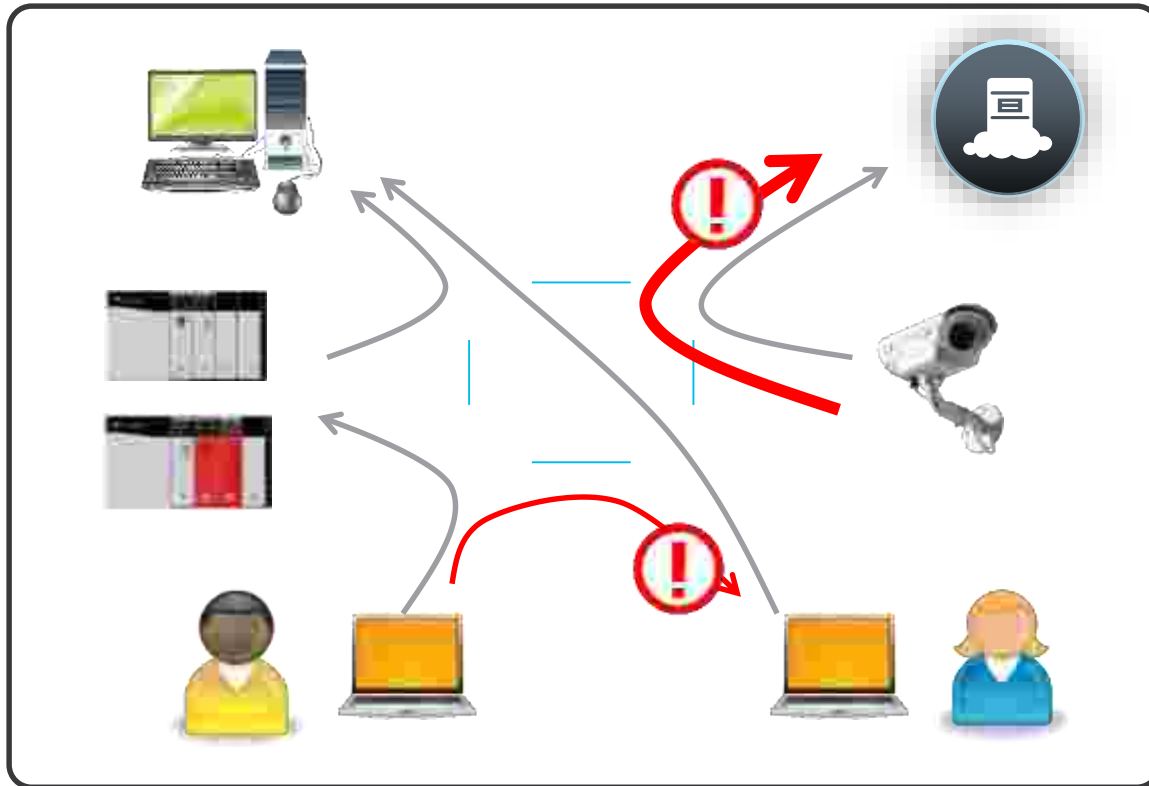
Identify
compromised hosts



Help prevent
user error

Visibility in Manufacturing

Anomaly Detection & Analysis



- Monitor normal traffic flow
- Detect anomaly traffic volume
- Detect anomaly communication

Communication pattern on plant floor is predetermined in general

>> Easy to detect anomalies

Sample:

Sudden communication between end-nodes
Sudden increase of traffic volume

NetFlow - The Network Phone Bill

NetFlow = shows you the **who, what, where and when**. It's a phone bill, which we use to look for out of the ordinary behaviour.

Telephone Bill



#	Time	Number	Label	Min	Amount/Charge	ISDN/Service	Number
1	01080213	4220PM	576-906-2077	1	0.00	0.00	024
2	01080213	4210PM	435-235-6371	1	0.00	0.00	024
3	01080213	4214PM	576-217-7763	1	0.00	0.00	024
4	01080213	4219PM	576-217-7763	1	0.00	0.00	024
5	01080213	4253PM	478-077-4303	2	0.00	0.00	024
6	01080213	4222PM	576-217-4303	2	0.00	0.00	024
7	01080213	4430PM	478-937-4301	18	0.00	0.00	024
8	01080213	4540PM	576-217-4301	36	0.00	0.00	024
9	01080213	4627PM	576-961-9300	3	0.00	0.00	024
10	01080213	4740PM	576-217-4301	8	0.00	0.00	024
11	01080213	4747PM	576-217-7763	4	0.00	0.00	024

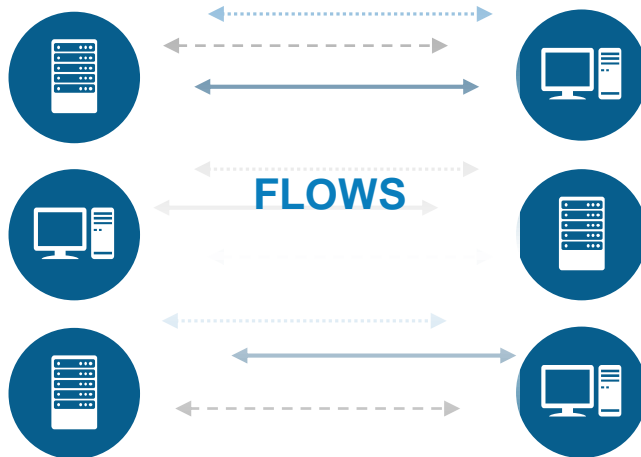
Flow ID	Source IP	Destination IP	Source Port	Destination Port	Protocol	Bytes	Packets	Start Time	End Time	Duration	Interface	Outgoing Interface
1	10.1.1.1	10.1.1.2	80	80	TCP	1024	1	01/08/2013 10:00:00	01/08/2013 10:00:01	00:00:01	Ethernet0/0	Ethernet0/0
2	10.1.1.1	10.1.1.3	80	80	TCP	2048	2	01/08/2013 10:00:02	01/08/2013 10:00:03	00:00:01	Ethernet0/0	Ethernet0/0
3	10.1.1.1	10.1.1.4	80	80	TCP	3072	3	01/08/2013 10:00:04	01/08/2013 10:00:05	00:00:01	Ethernet0/0	Ethernet0/0
4	10.1.1.1	10.1.1.5	80	80	TCP	4096	4	01/08/2013 10:00:06	01/08/2013 10:00:07	00:00:01	Ethernet0/0	Ethernet0/0
5	10.1.1.1	10.1.1.6	80	80	TCP	5120	5	01/08/2013 10:00:08	01/08/2013 10:00:09	00:00:01	Ethernet0/0	Ethernet0/0
6	10.1.1.1	10.1.1.7	80	80	TCP	6144	6	01/08/2013 10:00:10	01/08/2013 10:00:11	00:00:01	Ethernet0/0	Ethernet0/0
7	10.1.1.1	10.1.1.8	80	80	TCP	7168	7	01/08/2013 10:00:12	01/08/2013 10:00:13	00:00:01	Ethernet0/0	Ethernet0/0
8	10.1.1.1	10.1.1.9	80	80	TCP	8192	8	01/08/2013 10:00:14	01/08/2013 10:00:15	00:00:01	Ethernet0/0	Ethernet0/0
9	10.1.1.1	10.1.1.10	80	80	TCP	9216	9	01/08/2013 10:00:16	01/08/2013 10:00:17	00:00:01	Ethernet0/0	Ethernet0/0
10	10.1.1.1	10.1.1.11	80	80	TCP	10240	10	01/08/2013 10:00:18	01/08/2013 10:00:19	00:00:01	Ethernet0/0	Ethernet0/0

Flow Record

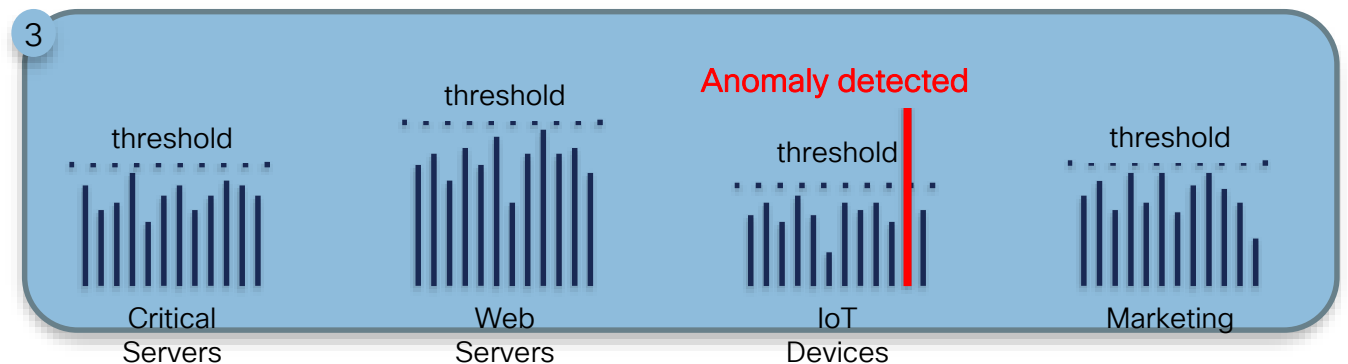


Network as a Sensor: Behavioral Detection and Anomaly Detection

ANALYZE
TRAFFIC FLOWS



Network Scanning TCP, UDP, Port Scanning Across Multiple Hosts	Denial of Service SYN Flood, Open, ICMP, UDP/Port Flood	Host Reputation Change Inside Host Potentially Compromised	Botnet Detection When Inside Host Talks to Outside C&C Server
Fragmentation Attack Host Sending Abnormal # Malformed Fragments	Worm Propagation Worm Infected Host Scans, etc.	Data Exfiltration Large Outbound File Transfer VS Baseline	Policy Violation Flag unusual transactions between network segments



Visibility Case Study

Case Study 1

- Korea manufacturing customer was facing factory network down issue because of excessive traffic from infected terminal

Case Study 2

- Japan manufacturing Customer need to connect the OT network to the IT network

Ransomware in 2016: \$1 billion

Locky, Cerber, CryptXXX, Cryptowall, ...



Swansea Police, Massachusetts \$750

Dickson County Police, Tennessee \$572

Tewksbury Police, Massachusetts \$500

Midlothian Police, Chicago \$500

Melrose Police, Massachusetts \$450

Melrose Police Dept, MA. \$500

Ransomware 2.0

Targeted Ransomware (APT)

Cryptoworm



Hollywood Presbyterian Medical Center
Methodist Hospital in Henderson, Kentucky
Chino Valley Medical Center in Chino, Ontario, California
Desert Valley Hospital in Victorville, Ontario, California
Ottawa Hospital, Canada
MedStar managed hospitals in Baltimore, Washington, Maryland
King's Daughter's Health, Indiana
Alvarado Hospital Medical Center, San Diego
Chino Valley Medical Center, California
Desert Valley Hospital, California

LA Hollywood Presbyterian Medical Center, \$17000



메인 사이트의 트래픽 과부하로 인해 임시 사이트를 운영하고 있습니다.

랜섬웨어 서버복구 과정에 대한 공지,

사이트 복원을 비롯한 문의 사항에 대한 응대를 진행하고 있습니다.

이용에 불편을 드려 죄송합니다.

[임시 사이트 바로가기 >](#)

[기존 사이트 바로가기 >](#)



Due to heavy traffic on the main site, we run temporary sites.

Notice of Ransomware server recovery process.

We are responding to inquiries, including site restoration.

We apologize for the inconvenience.

[Temporary site shortcut>](#)

153 Linux servers, 3400 websites encrypted. **\$1 million US** paid

[Existing site shortcut>](#)



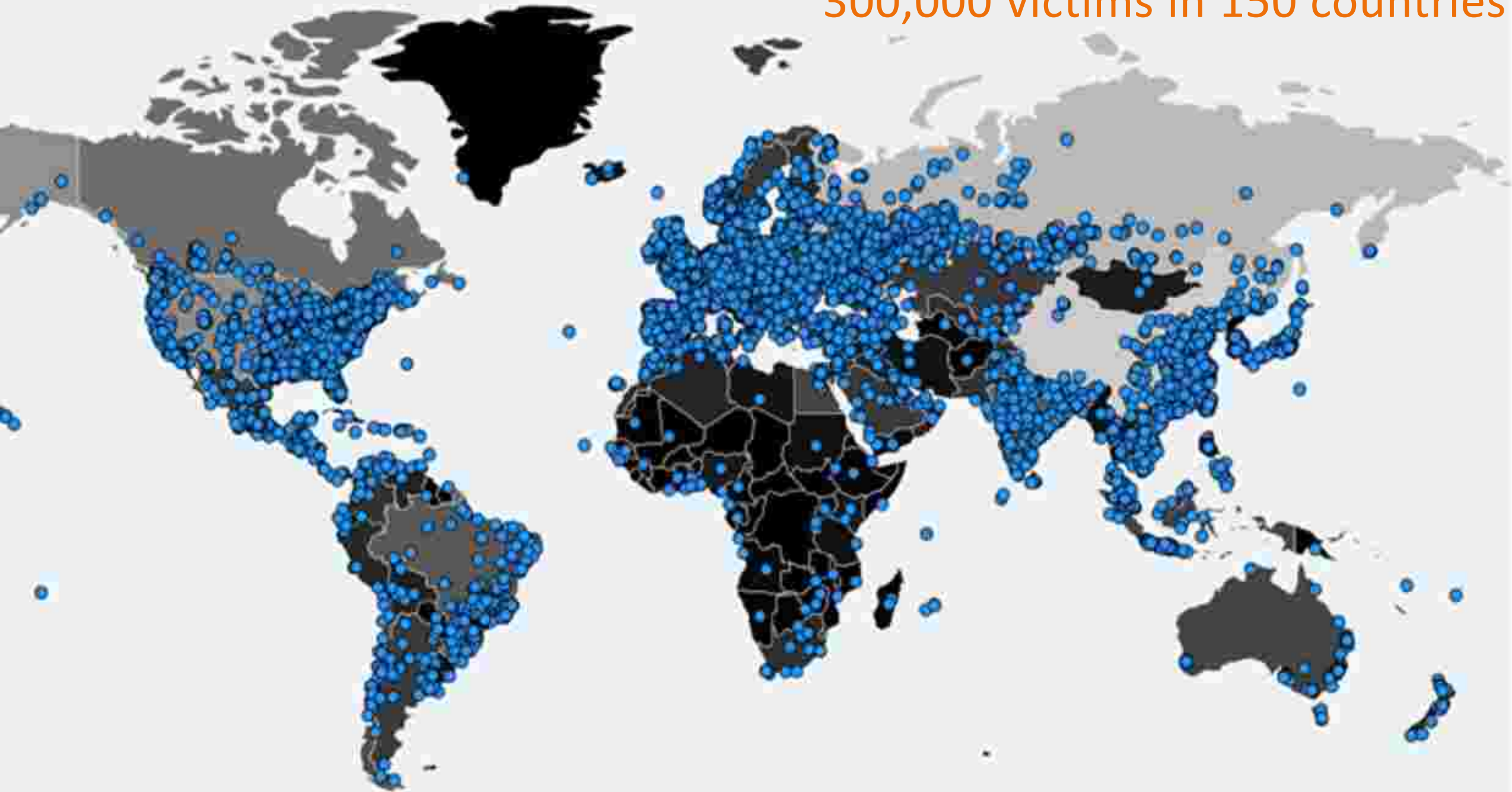
TALOS

WANNACRY?

12/5/2017



300,000 victims in 150 countries



Cyber-attack that crippled NHS systems hits Nissan car factory in Sunderland and Renault in France

Japanese car giant latest to be affected by ransomware sweeping the globe

By [Andrew Lister](#) | [@andrewlister](#) | [Twitter](#) | [Facebook](#) | [LinkedIn](#) | [Google+](#)

388



Renault shut down several French factories after cyberattack

The attack also affected one of Nissan's UK factories

By [Andrew Lister](#) | [@andrewlister](#) | May 18, 2017, 10:05am BST

Twitter Facebook LinkedIn



Dacia production in Romania, partially crippled by cyber-attack | WannaCry infection suspected

By [Declan Peat](#) | [@DeclanPeat](#) | May 21, 2017 13:58 | 0 comments



Car maker Dacia said that the production at its plant in Mioveni was partially stopped due to a cyber-attack, which might be linked to the WannaCry ransomware infection that hit computers in 99 countries.

UPDATE: Dacia announced on Monday that the production was restarted and the cyber threat was removed.

Dacia's site in Mioveni is currently the largest vehicle plant of French

Honda forced to halt car production after being infected by WannaCry ransomware

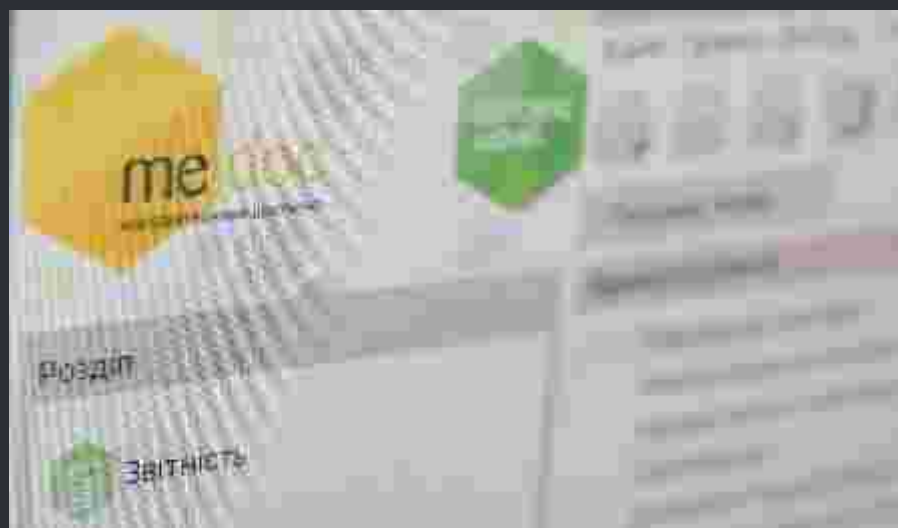
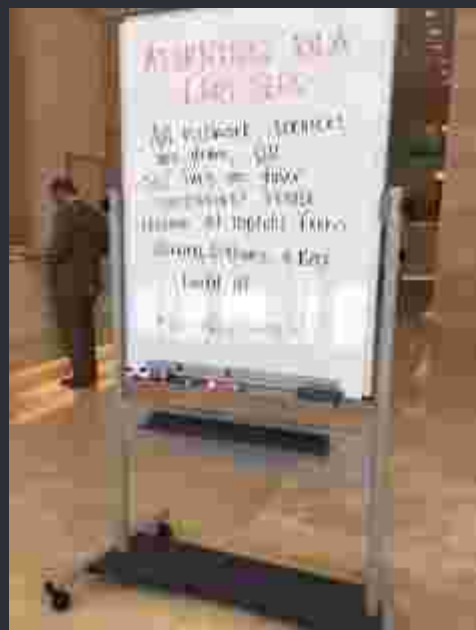
WannaCry caused a global incident last month after infecting machines in 150 countries.

By [Jason Murdoch](#) | [@jmurdoch](#) | June 21, 2017 10:35 BST

Twitter Facebook LinkedIn



Petya / NotPetya / Petrwrap / Nyetya



27/6/2017



Reckitt Benckiser - \$117 million



Maersk - \$200-\$300 million



Fedex and TNT: \$300 million



Merck: \$310 million



Typical Ransomware Infection



Infection
Vector
(Email
attachment,
Clicks a link,
Malvertising)



C2 Comms &
Asymmetric Key
Exchange



Encryption
of Files



Request
of Ransom

Encryption C&C

Payment MSG

NAME	DNS	IP	NO C&C	TOR	PAYMENT
Locky					DNS
SamSam					DNS (TOR)
TeslaCrypt					DNS
CryptoWall					DNS
TorrentLocker					DNS
PadCrypt					DNS (TOR)
CTB-Locker					DNS
FAKBEN					DNS (TOR)
PayCrypt					DNS
KeyRanger					DNS





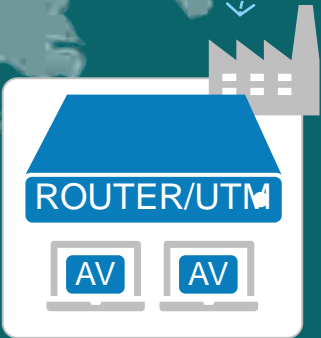
MALWARE
C2/BOTNETS
PHISHING

DNS

First Line



HQ



Branch



Roaming user

BENEFITS

Simple. Deploy in mins!

Alerts Reduced 2-10x

Protects ON & OFF network

Threat prevention, not just detection

Reactive

Predictive

100B

requests
per day

85M

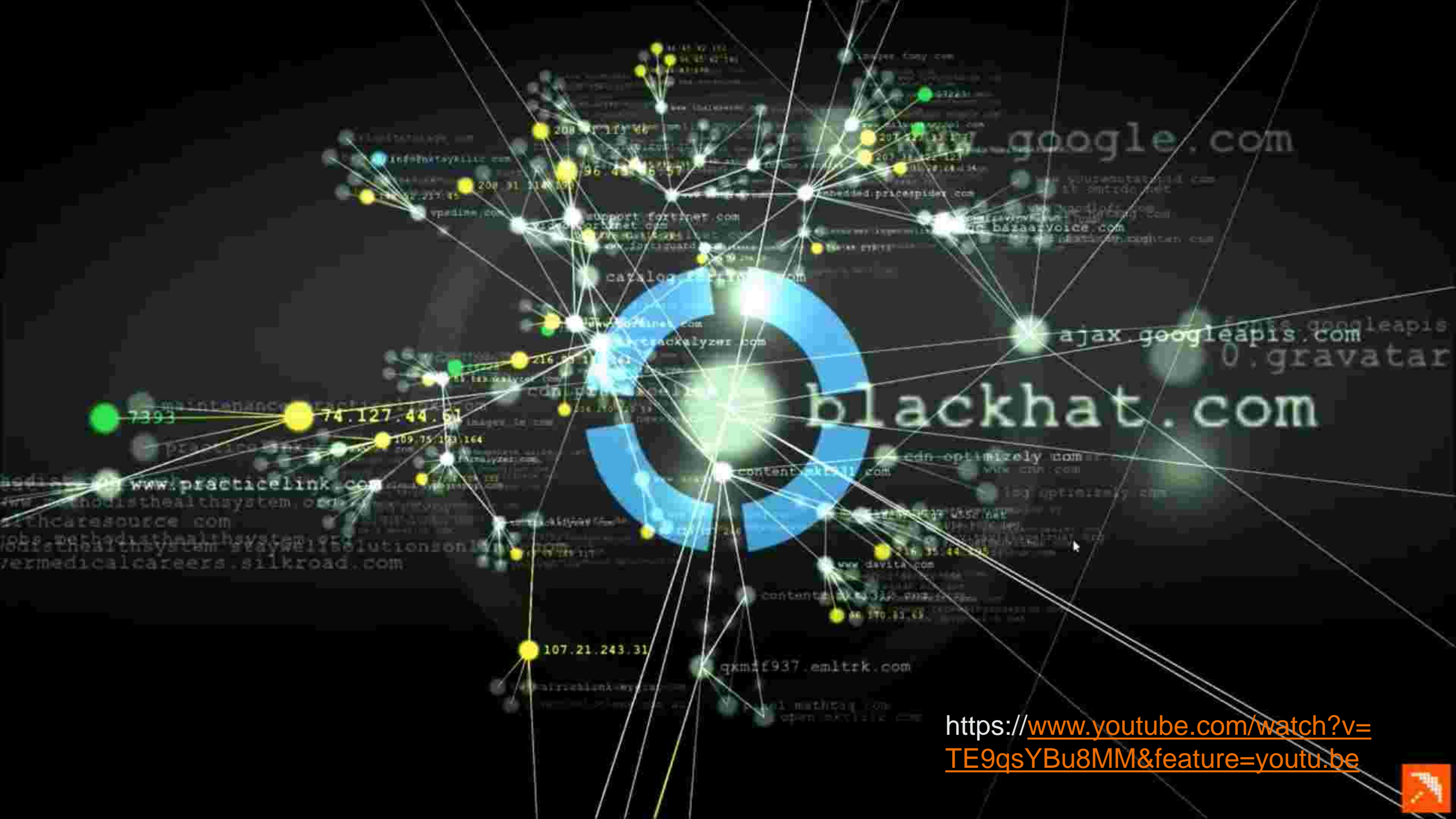
daily active
users

12K

enterprise
customers

160+

countries
worldwide



<https://www.youtube.com/watch?v=TE9qsYBu8MM&feature=youtu.be>



CRYPTOLOCKER

The "Ripple Effect" by OpenDNS Research

https://youtu.be/acwD_OA3QZ4

Why so powerful?

WannaCry = Ransomware + Exploit + Worm

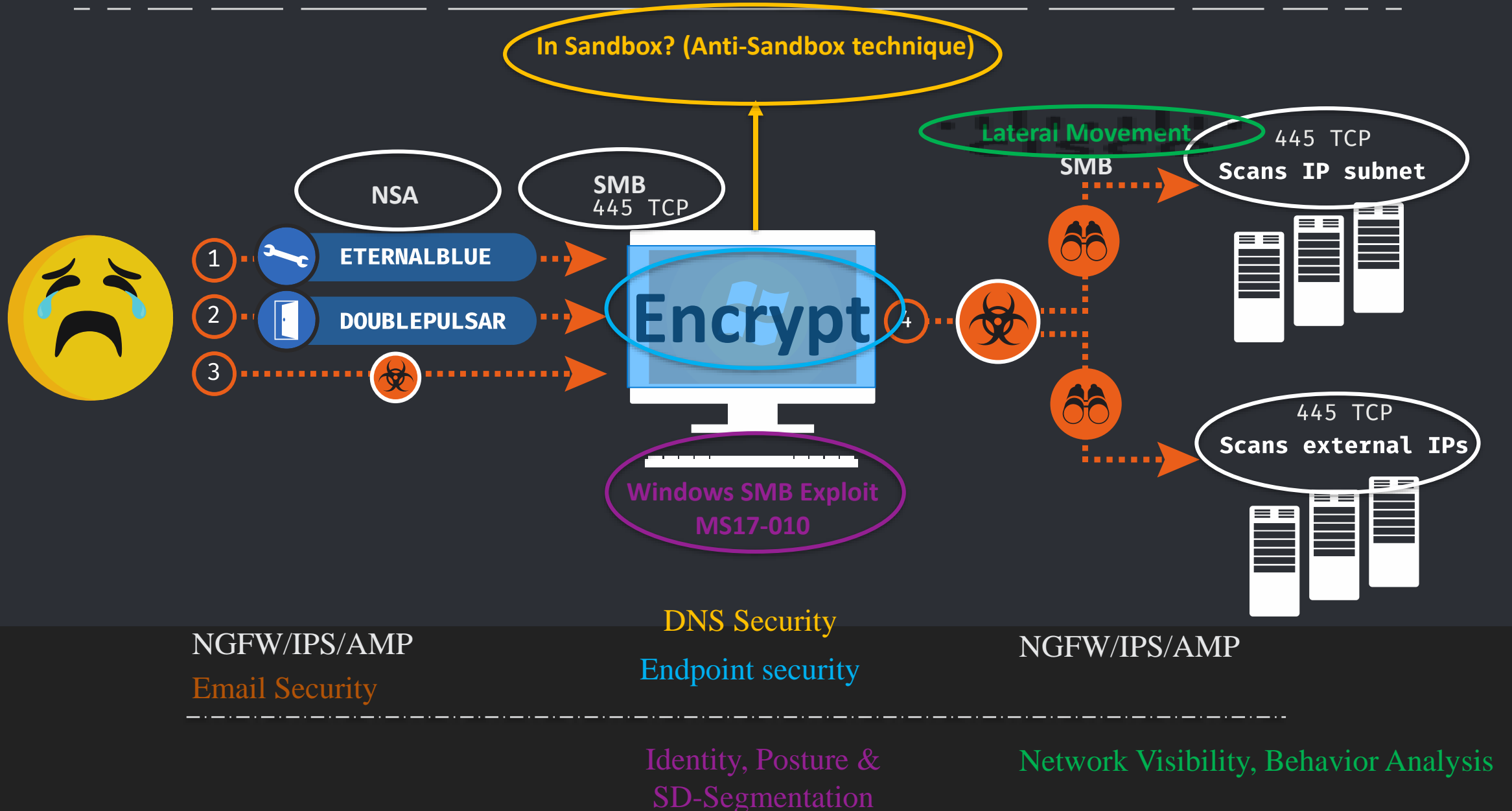
WannaCry

In Sandbox? (Anti-Sandbox technique)
Check domain (Kill Switch)



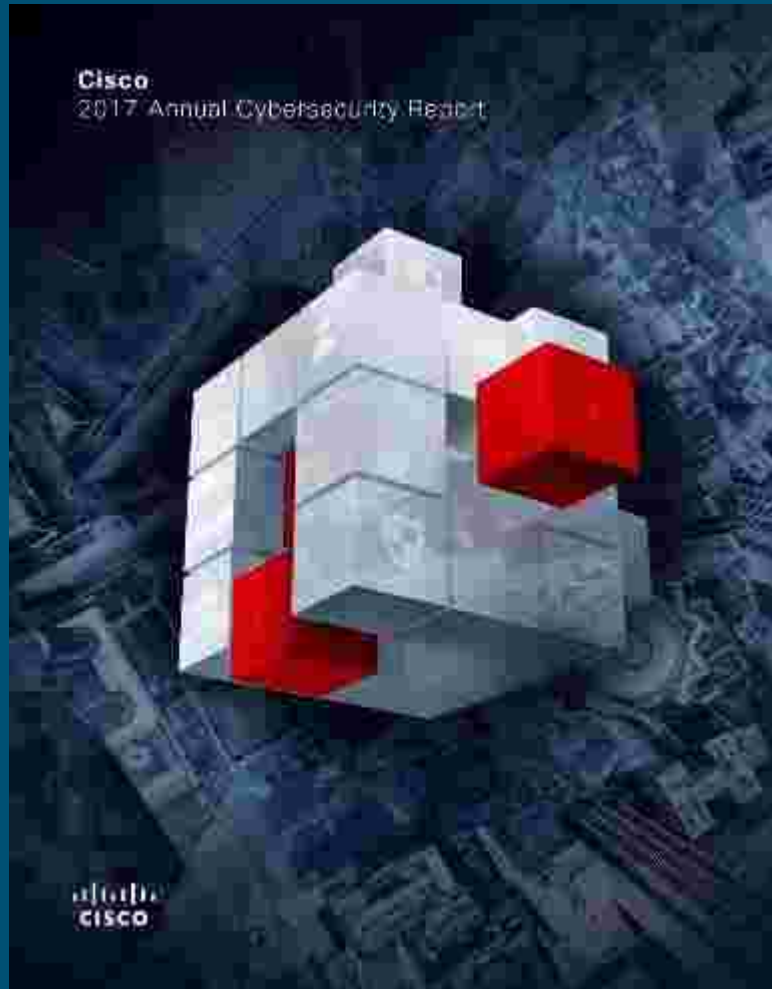
Windows SMB Exploit
MS17-010

WannaCry Defense



Cisco 2017 Annual Security Report

Cisco 2017 Midyear Cybersecurity Report



<https://www.cisco.com/c/en/us/solutions/industries/manufacturing.html>



Garrick Ng - CTO: garng@cisco.com

Shania Ting - Security Sales Manager: hoting@cisco.com

Eric Tsoi – Security Consultant: eritsoi@cisco.com

Raymond Poon – IoT Consultant: rayphoon@cisco.com