

# Cyber Security Services for Industrial Automation

Improving our Ability for Customer Security

Brett Nelson, OCS RTA Manager

# Cyber Security in Power and Automation

This is not “fake news”...

PUBLIC

## Stuxnet worm 'targeted high-value Iranian assets'

Analysis confirms coordinated hack attack caused Ukrainian power outage

BlackEnergy was key ingredient used to cause power outage to at least 80k customers.

## BlackEnergy crimeware coursing through US control systems

US CERT says three flavours of control kit are under attack

## Active malware operation let attackers sabotage US energy industry

"Dragonfly" infected grid operators, power generators, gas pipelines, report warns.

## Attackers poison legitimate apps to infect sensitive industrial control systems

Havex operators target mission-critical controllers around the world.

## Computer intrusion inflicts massive damage on German steel factory

Blast furnace can't be properly shut down after attackers take control of network.

## 'CRASH OVERRIDE': THE MALWARE THAT TOOK DOWN A POWER GRID

## Will WannaCry Be Industry's Cybersecurity Wake-Up Call?

The ransomware attack that swept the world last week left most manufacturers unscathed, but exposed the critical vulnerabilities that many have not even begun to address.

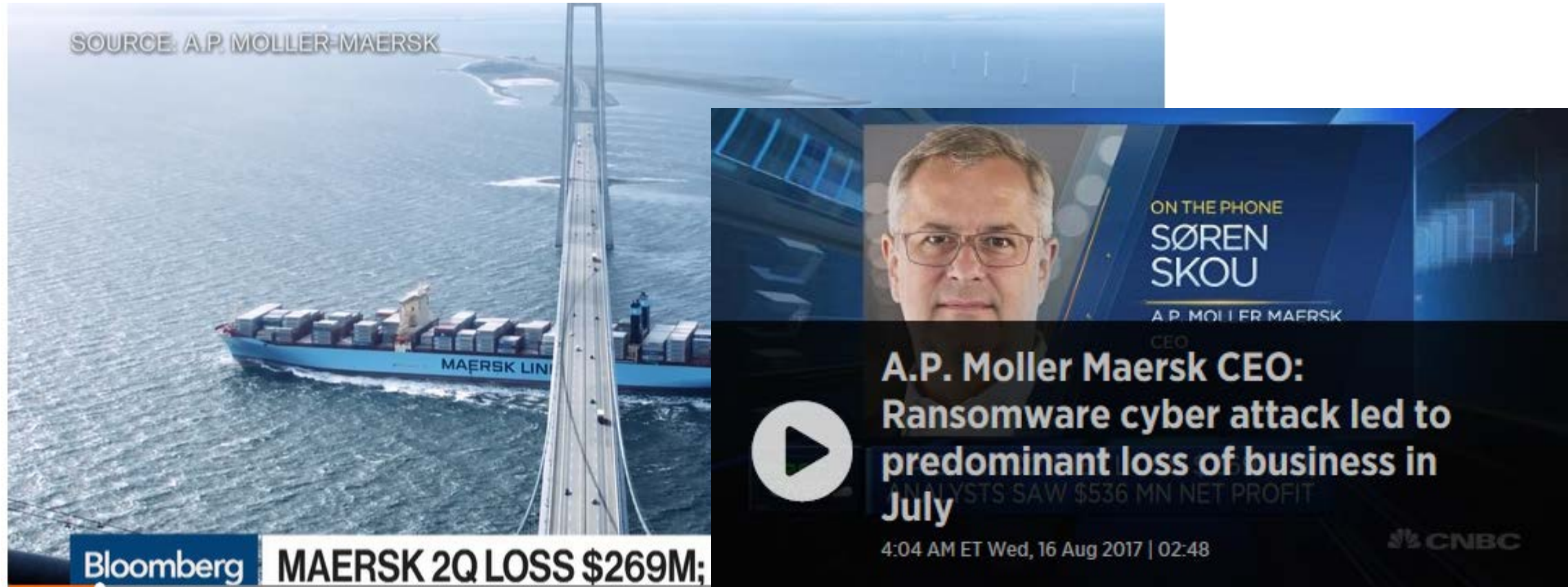
'Petya' ransomware attack strikes companies across Europe and US

Ukraine government, banks and electricity grid hit hardest, but companies in France, Denmark and Pittsburgh, Pennsylvania also attacked

Attacks are real and have an actual safety, health, environmental, and financial impact

# AP Moller Maersk: NotPetya cyberattack will cost as much as \$300 million

“We expect that the cyber-attack will impact results negatively.” CEO Soren Skou



# And that's not all

Other companies materially affected by NotPetya virus

## Beiersdorf (cosmetics)

- Affected IT & telecoms
- Halted production in 17 sites
- Lost \$42 million in sales

The logo for Beiersdorf, featuring the company name in a bold, blue, sans-serif font.

## Merck (pharmaceuticals)

- Disrupted global operations
- Halted drug production
- Hurt 2017 profits



## Mondelez (food)

- Experienced global IT outage
- Prevented shipping/invoicing
- Lost share value of 2%



## St. Gobain (materials)

- Forced to isolate computers



Who's next?



# What is Cyber Security?



Targeted attacks



Malicious software



Employee Mistake

# This level of business risk makes cyber security a boardroom issue

Today, cyber risks are senior management and shareholder topics

## '50s-70s: Closed proprietary systems



Cyber Risk

**Cyber Security risk: zero**  
Hard-wired analog controls



## '80s-90s: Commodity open systems



Cyber Risk

**Cyber Security risk: low**  
Digital controls & communication



## 2000s: Internet-connected devices



Cyber Risk

**Cyber Security risk: high**  
Internet-connected control and business systems



# Guiding Principles

There are no Silver bullets...

PUBLIC

Reality

There is no such thing as 100% or absolute security

Process

Cyber security is not destination but an evolving target – it is not a product but a process

Balance

Cyber security is about finding the right balance – it impacts usability and increases cost

**Cyber security is all about risk management**

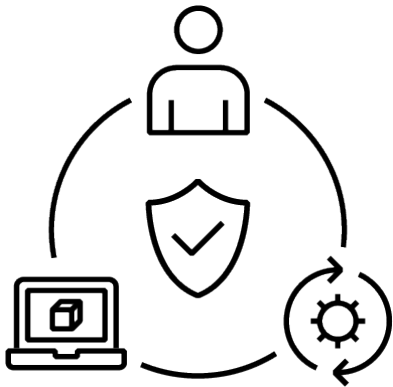


# There are no magic solutions; security maturity takes time

Must engage and educate people, develop and deploy processes, and design and deliver protected technology

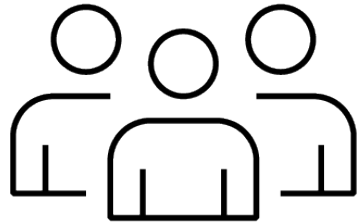
## 3 Cyber Pillars:

- People, Process and Technology: each must be leveraged to protect digital systems



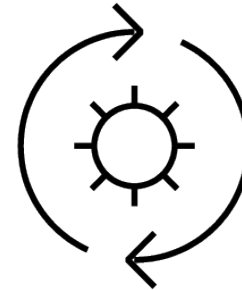
## People

- People are critical in preventing and protecting against cyber threats.
- Organizations need competent people to implement and sustain cyber security technology and processes.



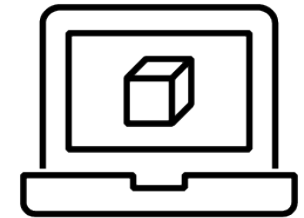
## Process

- Policies and Procedures are key for an organization's effective security strategy.
- Processes should adapt to changes as cyber threats evolve.



## Technology

- Technology is important in preventing and mitigating cyber risks.
- Technology needs people, process and procedures to mitigate risks.





# Cyber Security Best Practices

## Defense in Depth

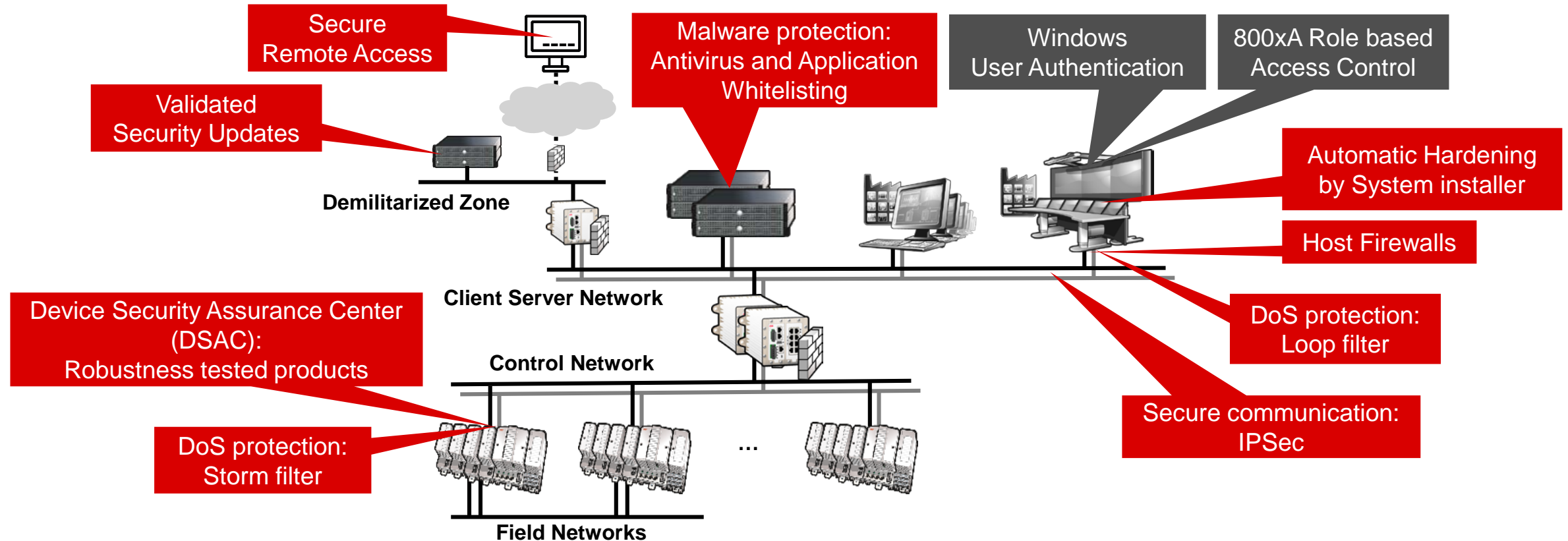
The coordinated use of multiple security measures, addressing:

- People
- Technology
- Operations



# Defense in Depth in 800xA

## Who/What, Protect Hosts



# Why ABB for Cyber Security Services?

## Key advantages

### Operational System Knowledge

- Protecting operational technology systems require both IT and OT knowledge. ABB service resources have extensive system and control experience
- Avoid system disruptions when implement cyber solutions



### Decade of Implementing solutions

- ABB have been implement cyber solutions for years. We leverage common IT solution to protect system assets
- Safer implementation through connecting OT & IT with partnerships



### Proven approach

- We have hundreds of successful implementations of our cyber security solutions in every industry
- ABB Customers want us to secure systems from other vendors because they trust us



# How ABB Can Help with Cyber Security Management

- Cyber Security Fingerprint and remediation of deficiencies
- Service Port Cyber Channel
- Software Update Services
- Software Backup services
- Security Workplace
- Secure Remote Access
- Training

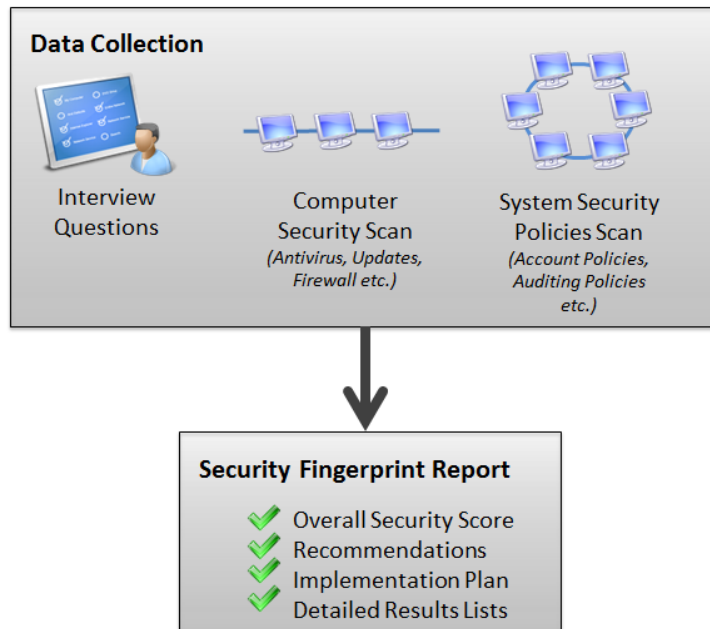




# Cyber Security Fingerprint

## Security in depth

A security services based on defense in depth and we are covering all these 7 layers within the report



- Physical Security
- Procedures and Policies
- Firewalls and Architecture
- Computer Policies
- Account Management
- Security Updates
- Antivirus Solutions



# Cyber Security Monitoring Service

Maintain security via continuous monitoring

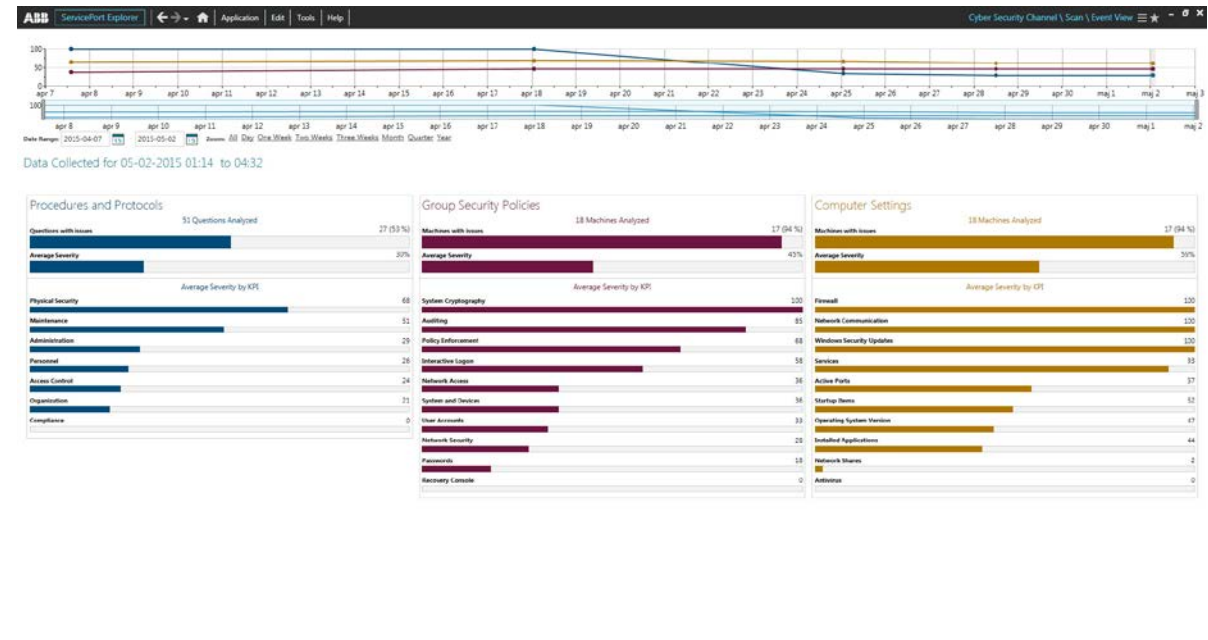
## Overview

The continuous version of the Cyber Security Fingerprint

- Based on **ABB ServicePort™**  
a remote-enabled service software platform.




### Features:

- **Automatic**, non-invasive data gathering – centralized/multi system
- **Proactive analysis** of KPIs to detect possible security weaknesses
- On-demand analysis
- On-site or **remote access** (RAP) for site personnel or ABB experts
- Configurable **alerts** (locally and e-mail)



# Cyber Security

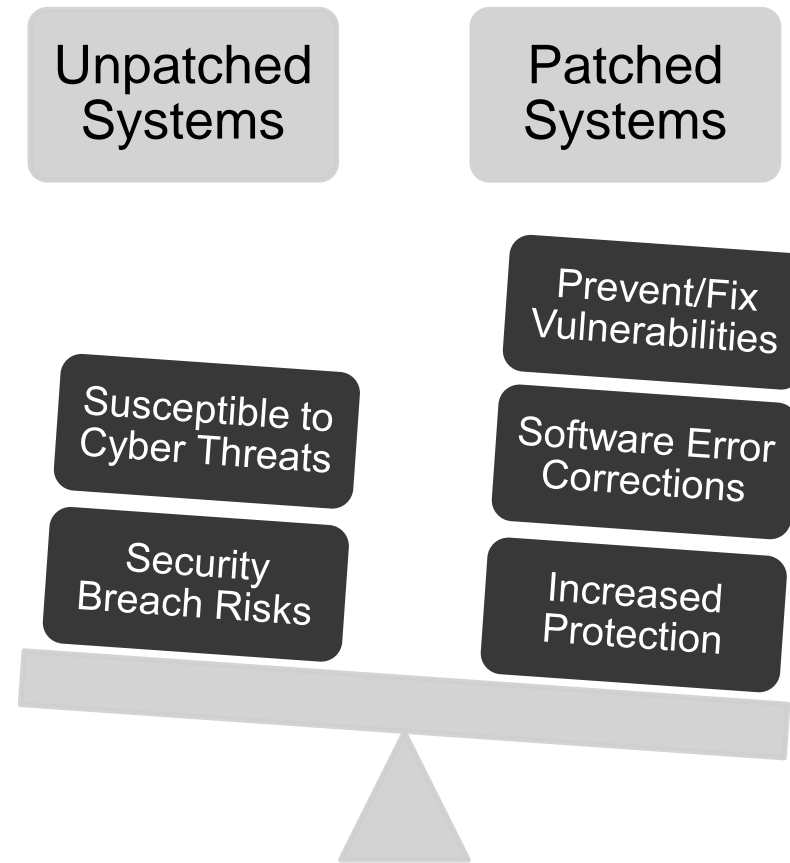
## Benchmark, Fingerprint and Monitoring Service

	Benchmark 	Fingerprint 	Monitoring Service 
Key Performance Indicators	26	26	26
Automatic, non-invasive data gathering	✓	✓	
Automatic, non-invasive scheduled data gathering			✓
Automatic cloud-based analysis	✓		
Analysis performed by cyber security experts		✓	
Automatic local analysis			✓
Proactive analysis of cyber security posture	✓	✓	✓
Stoplight report of security status	✓		
Detailed findings report with recommendations		✓	
Detailed findings report with recommendations and historic data			✓
On-site access to experts		✓	✓
Remote access to experts			✓
Ongoing analysis of KPIs			✓
Daily reports of security status			✓
Yearly performance analysis report			✓
E-mail notifications when KPIs are outside site-specific thresholds			✓
Education in ABB's tools			✓

# Patch Management Services

## Overview – Why Patching?

- Adversaries target unpatched systems
- U.S. Department of Homeland Security lists Patch Management in 7 Strategies to Defend ICSs
- In 2015, 295 incidents were reported to ICS-CERT
- Many more went unreported or undetected
- 29% of ICS-CERT reported incidents mitigated by Patch Management





---

# Patch Management Services

## Program Services

Provides anti-virus software updates and Windows patches in several service levels

### Service Options Include:

- **Basic** – Security Patch Disc (monthly approved patches)
- **Select** – Security Patch Disc + Quarterly system report
- **Proactive** – ABB installs patches periodically + system report
- **Remediation** – One-time site visit to update system with current patches
- **Cyber Security Workplace** – Centrally Managed Server

### Centrally Managed Options:

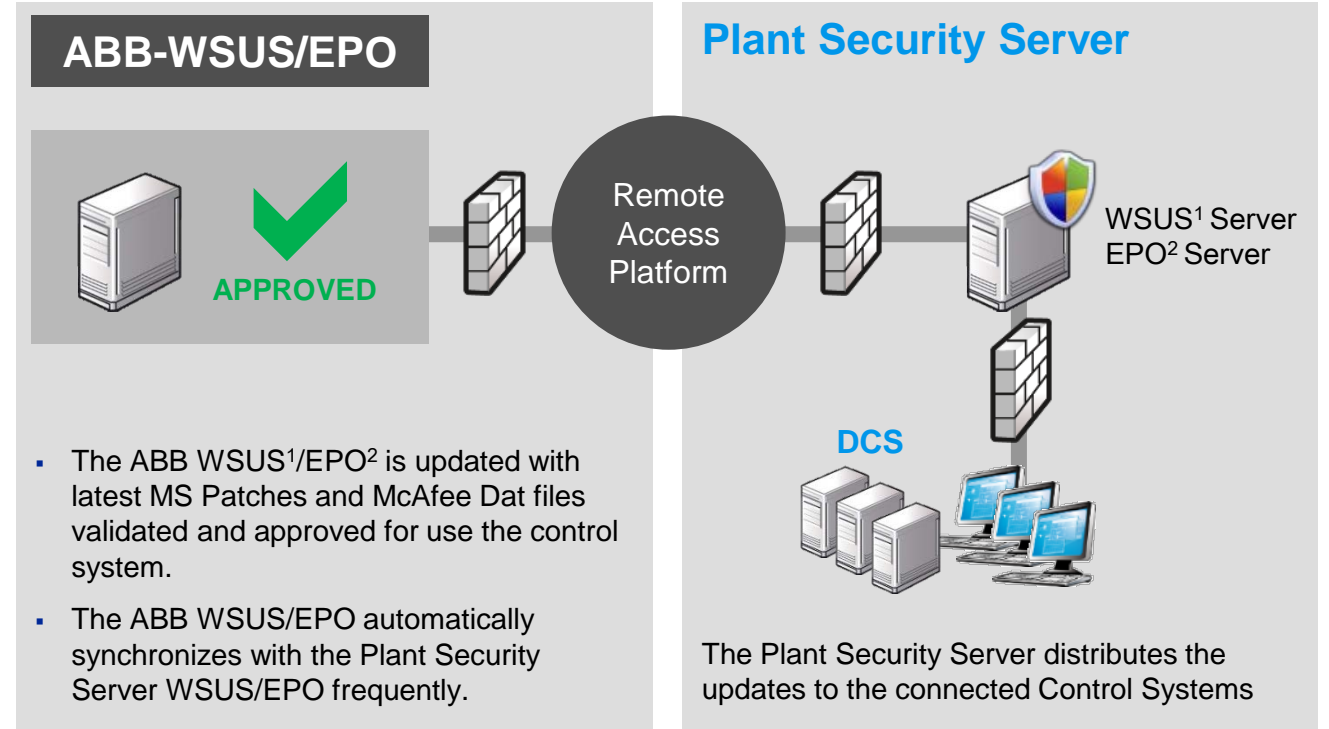
- **Cyber Security Workplace** – Centrally Managed Server
- **Security Update Service** – Centrally Managed Server while using a RAP Connection



# Security Update Service

## Automated and Controlled

A service that allows an onsite WSUS and EPO server to be updated with ABB approved patches and DAT files on a daily basis.



# Security Workplace

## Package overview



### Security Workplace

#### MAINTAIN

##### **Centralized Microsoft Patching\***

Centralized Antivirus Management

Centralized, Automated Backup and Recovery

#### COMPLY

Security Event Monitoring

Configuration Change Management

ICS Asset Management

Automated Compliance Reporting

Policy Management

Workflow Automation Suite

#### DEFEND OPTIONS

##### **File Sanitizer (ODI-X)\***

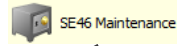
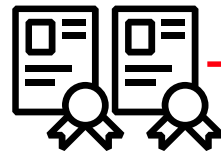
Intelligent Whitelisting

Network Segmentation and DMZ Implementation

# Application Whitelisting

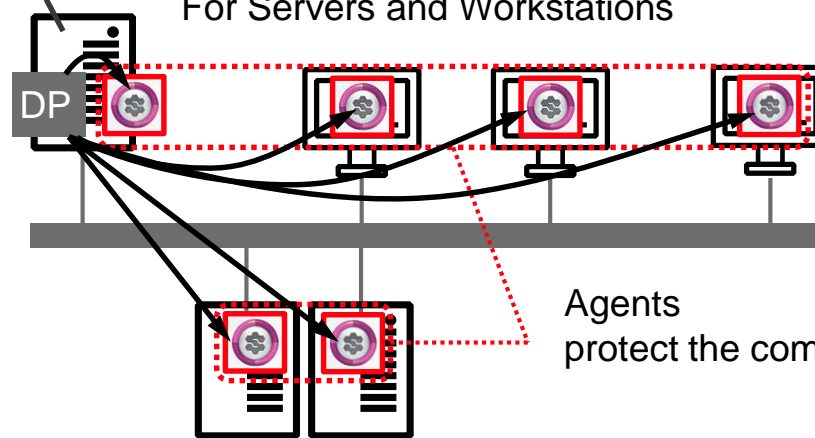
## Malware protection with Application Whitelisting

Antivirus: Blacklisting	Application Whitelisting
Block “known” malware	Allow known SW to run
Hopeless battle 😞	Easier task 😊



800xA SE46 Application Whitelisting  
For Servers and Workstations

- Central Management and Distribution:
  - Application Certificates
  - Policies (Monitor/Block)
  - Log collection
- Premade Application Certificates for
  - Windows and other required 3<sup>rd</sup> party SW
  - ABB SW



Agents  
protect the computers



---

# Software Backup Services Essential Features

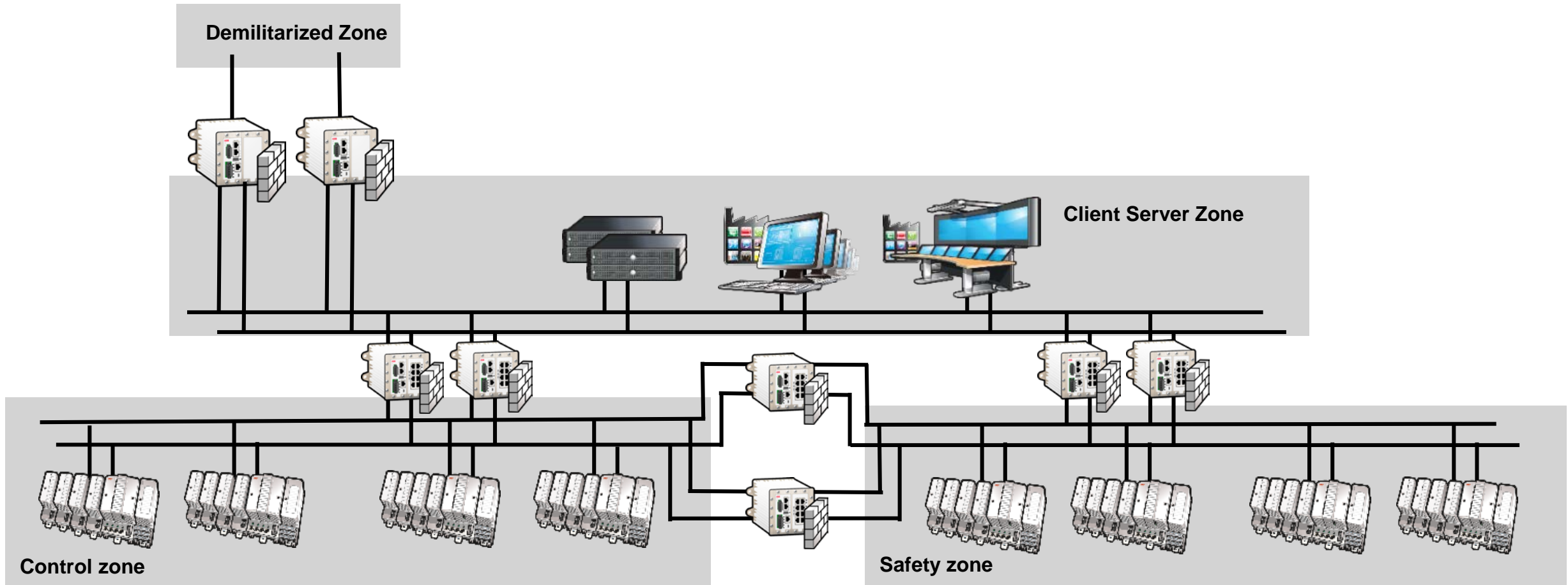
## Preserve and Protect

- Hard drive imaging to a central server for rapid recovery
- Configuration backups in addition to imaging
- Scheduling and scripting to automate the update of images
- Tested bandwidth and CPU utilization to avoid performance problems
- Full domain integration
- Backup image testing
- Restoration training for technicians who will have to recover in the middle of the night



# Restricted data flow

Security zoning with redundancy



# Secure Remote Access

## Security in depth

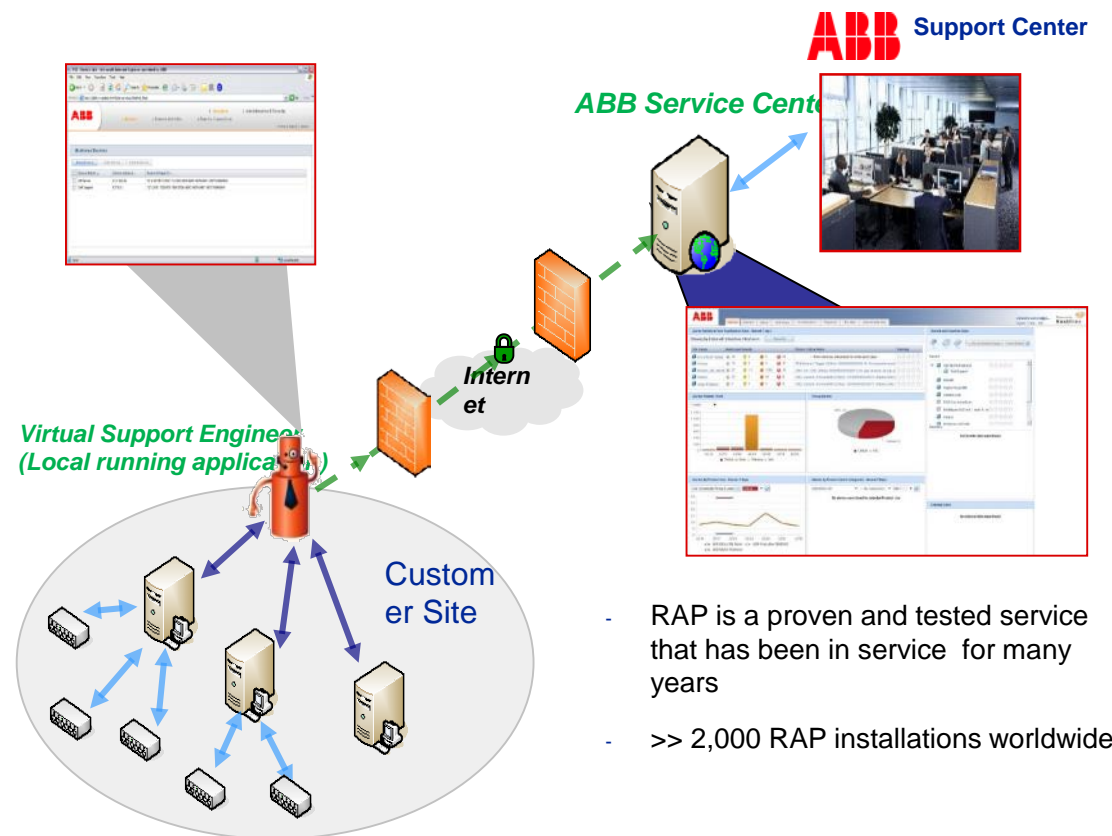
Connection to Corporate Network via Router w/ Firewall or DMZ.

Allows for Remote Diagnostics for Control System support

Can Support WSUS (Windows Update) and Anti Virus Updates

Allows for Remote Operator and Engineering Clients

- Secured as Read-Only
- Configured for off-site Operation and Maintenance



- RAP is a proven and tested service that has been in service for many years
- >> 2,000 RAP installations worldwide

---

# Training Available from ABB University

## Security in depth

US925 course covers:

- Patch Management
- Antivirus
- Software Backup Systems

US926 course covers:

- Standards, policies, basic principles, and best practices
- Network architecture
- Hacking / penetration testing tools
- Audits and assessments
- Hardening
- IPSec and whitelisting
- Event monitoring



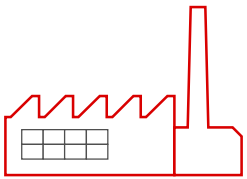


# Cyber Security Services

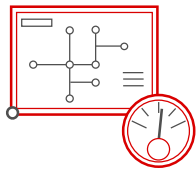
Can be applied to any digital system and is non-invasive

## Benefits

Improves system availability by reducing security risk



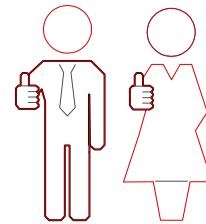
Accelerates problem solving with collaboration and analysis of digital asset key security indicators



Identifies trends and develops mitigation plans to protect against security weaknesses



Manages security settings to align with customer requirements



Reduces response time and travel expenses by providing remote access to ABB experts for troubleshooting



Ensures continuous improvement of your security status



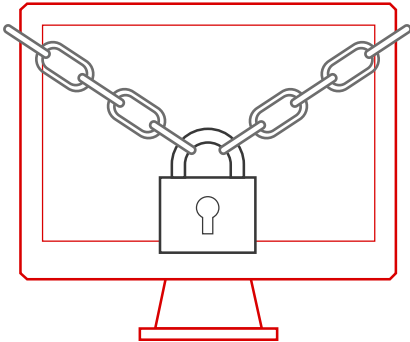
# Cyber Security

## In Closing

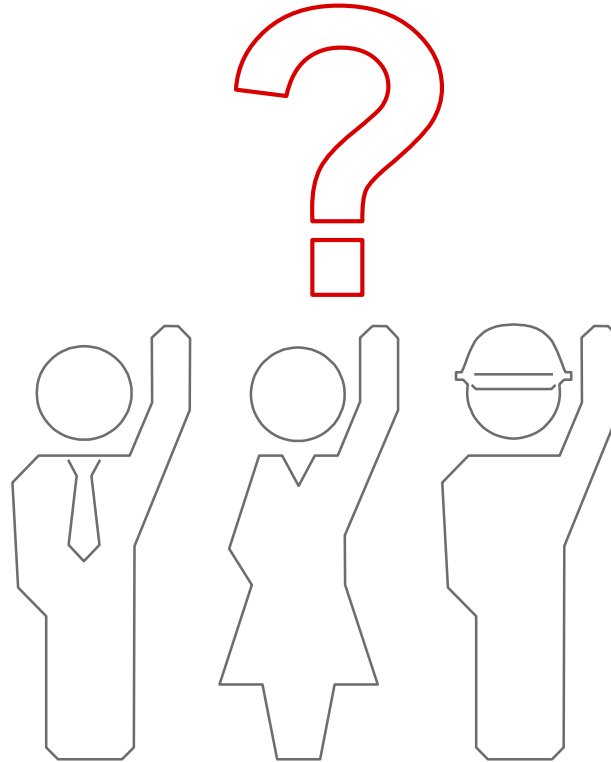
### Final Thoughts

“The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts.”

*Eugene H. Spafford\**



### Questions



### Contact

If you have further questions, please contact:

Brett.Nelson@us.abb.com

– Links to:

- [Cyber Security on ABB.COM](https://www.abb.com/cybersecurity)



**ABB**