



Security Fabric for Operational Networks

Ionut Davidoiu

Cisco BDM RRC Romania

What is Digitization? What is IoT ?

“Use Technology to change Business Outcomes – transform business”

- **Business Outcomes**
- **Data Driven**
- **Continuous Innovation**
- **Sustaining Competitive Differentiation**

“IoT is an enabler for Digitization”

Industrialization of Hacking

There is a multi-billion dollar global industry targeting your prized assets

\$450 Billion
to
\$1 Trillion


Malware
Development
\$2500
(commercial
malware)


Bank
Account Info
>\$1000 depending
on account type
and balance


Facebook
Accounts
\$1 for an
account with
15 friends



Social
Security
\$1



Mobile
Malware
\$150



Exploits
\$1000-
\$300K



Spam
\$50/500K
emails



Credit Card
Data
\$0.25-\$60



DDoS as
A Service
~\$7/hour



Medical
Records
>\$50

Recent attacks on IoT

Thu Feb 25, 2016 6:52pm EST

Related: WORLD, TECH, CYBERSECURITY

U.S. government concludes cyber attack caused Ukraine power outage

WASHINGTON | BY DUSTIN VOLZ

U.S. MAR 30, 4:54 PM EDT **International Business Times**

TECHNOLOGY

Hackers' Ransom Attack On California Hospital More Proof Healthcare Cybersecurity Is Floundering

BY JEFF STONE ON 02/17/16 AT 7:45 AM

Home > SCADA / ICS



1,400 Flaws Found in Outdated CareFusion Medical Systems

By [Eduard Kovacs](#) on March 30, 2016

FBI investigating cyber attack at MedStar Health

By [Andrea S. McDermis](#) and [Ian Dawson](#) - [Contact Reporters](#)
The Baltimore Sun



Suspected cyber attack at MedStar Health

MARCH 24, 2016, 6:27 PM

Hackers attacked the computer system at [MedStar Health](#) on Monday, forcing thousands of employees in the state's second-largest health care provider to resort

Related

3 more Southland hospitals attacked by hackers using ransomware

Nov. 22, 2015

\$17,000 Illinois ransom paid by hospital to hackers sparks outrage

Nov. 19, 2015

Cyber Attacks Threatening Oil and Gas Sector Severely Now Than Ever Before

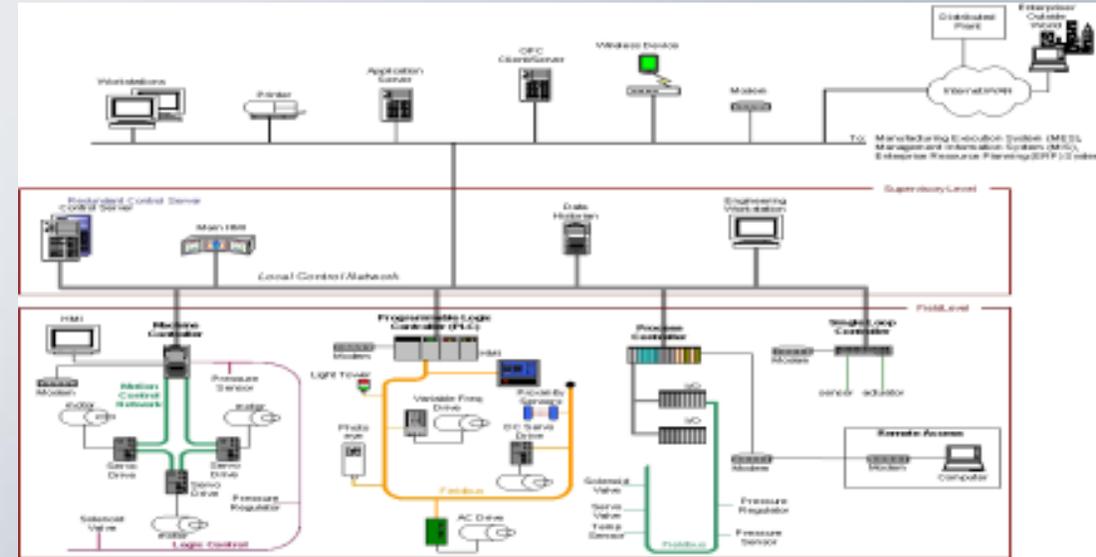
By [Ryan De Souza](#) on January 17, 2016 [Email](#) [@hackread](#) [CYBER ATTACKS](#) [CYBER EVENTS](#) [SECURITY](#)

Priority shifts in IoT

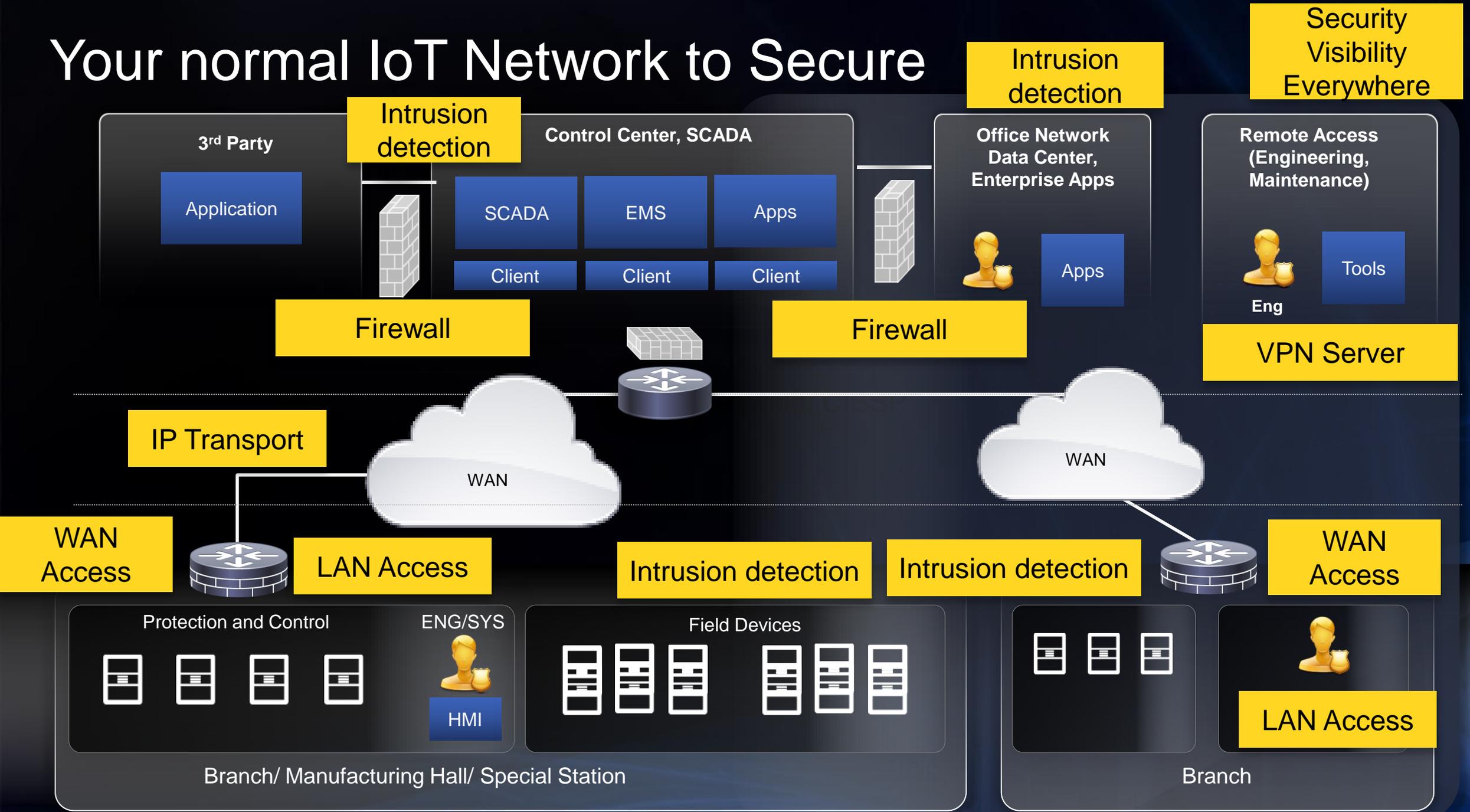
| Security Policies | IT Network | IoT Network |
|----------------------------------|--|---|
| Focus | Protecting Intellectual Property and Company Assets | 24/7 Operations, High OEE, Safety, and Ease of Use |
| Priorities | Security in IoT networks is crucial as people, communities, and financial systems could be negatively impacted by cyber/physical security breaches | |
| Types of Data Traffic | Control, Voice and Video (Hierarchical) | Information, Safety and Motion (P2P & Hierarchical) |
| Implications of a Device Failure | Top priorities are availability, safety, and ease-of-use | |
| Threat Protection | Detection | |
| Upgrades and Patch Mgmt | ASAP During Uptime | Scheduled During Downtime |
| Infrastructure Life Cycle | Equipment | (years) |
| Deployment conditions | Control | (c) |

Common Security Issues in IoT Networks

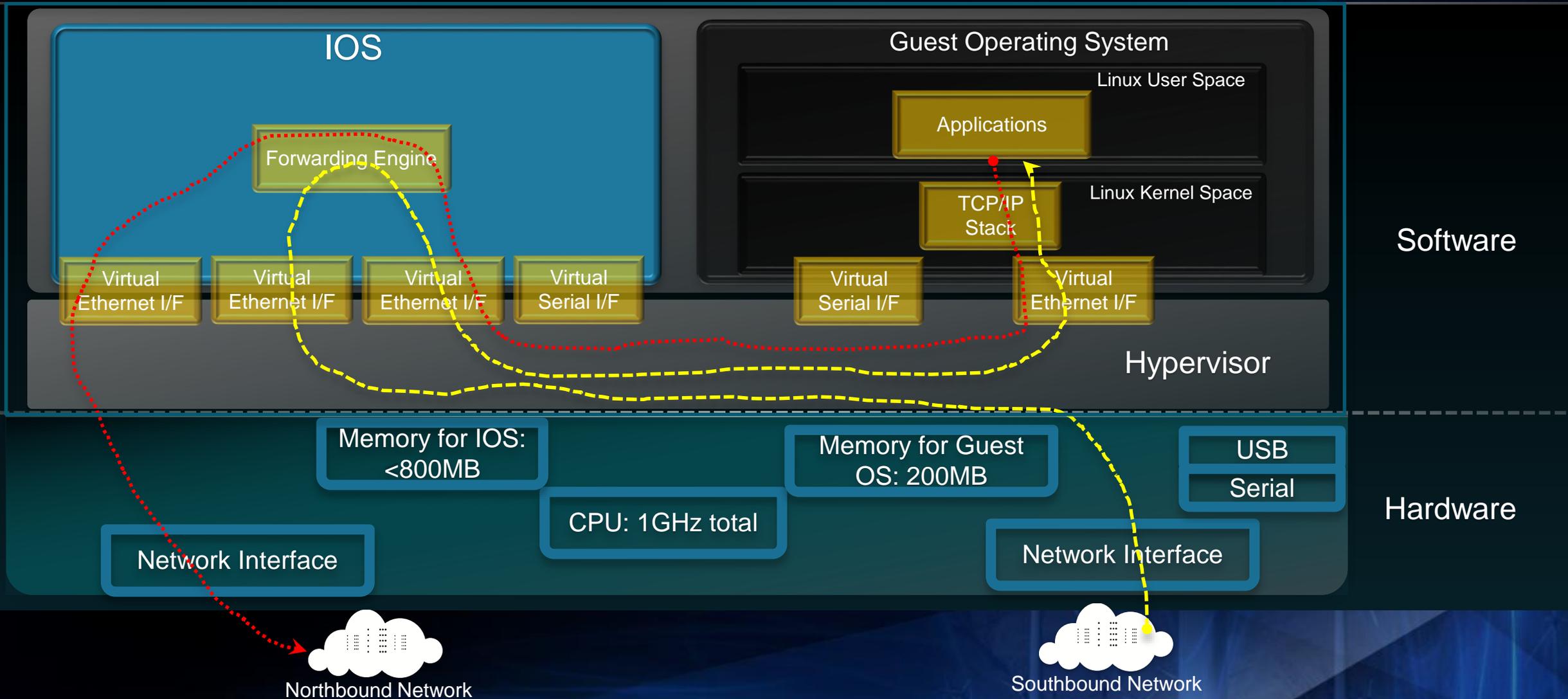
- **Weak Access controls to Monitoring and other equipment**
 - Separation of duty for operator, administrator, audit
 - Little or no Password management
- **Physical segmentation**
 - Dual-homed servers or PLCs act as Firewall
 - Segmented network has only physical security
- **Unauthenticated command execution**
- **Communication is un-encrypted**
- **Outdated operating systems left unpatched**
- **Rogue wireless access points without encryption**
- **Insufficient controls on contractors (i.e. access policy, laptops, etc.)**



Your normal IoT Network to Secure



LAN Access(for machines) – security and normalization



Cisco Identity Services Engine

All-in-One Enterprise Policy Control Solution Leveraging Real Context that is Practical for Today's Threat Landscape

Provides ability to transfer your security policy from paper into technical rules that will be enforced electronically

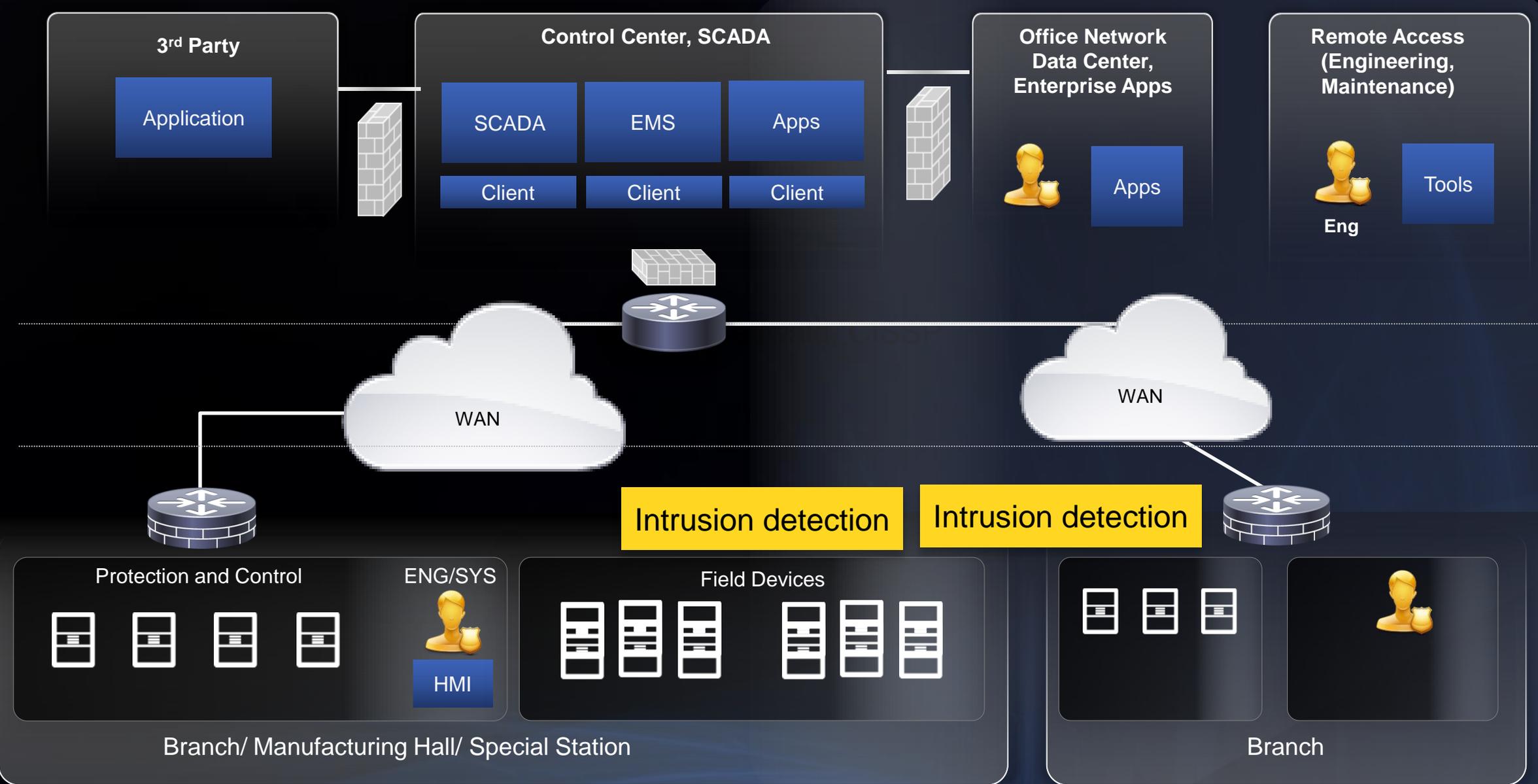
- 
-  - Who are you? → Bob
 -  - What Device? → Contractor/Employee
 -  - Where are you? → Plant 1 zone 2
 -  - When? → 11:00 AM on April 10th
 -  - How ? → Wired, Wireless, or VPN

ISE



Dynamic Segmentation Options:
VLANs, DACLs, or TrustSec

Intrusion Detection(for Things)

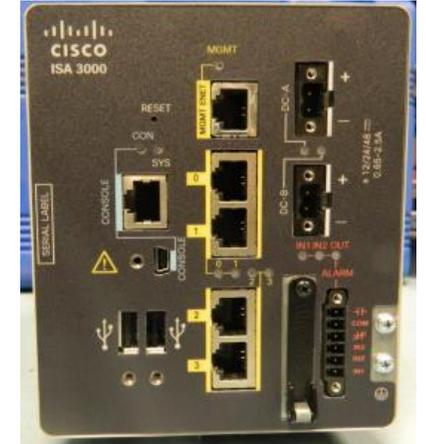


ISA3000 Summary

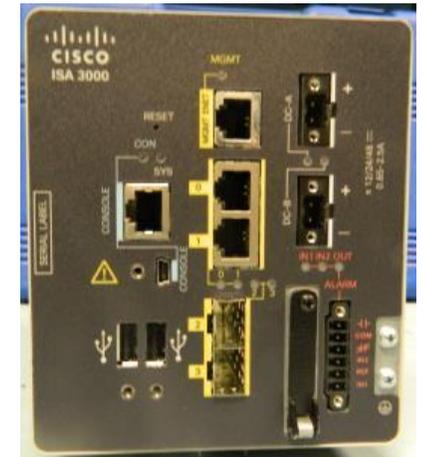
- Industrial, Energy, Marine, Railway Applications
 - Additional Certifications post-FCS
- Services include Firewall, VPN and IPS, DHCP, and NAT
- Two SKU's
 - Copper: 4x10/100/1000BaseT
 - Fiber: 2x1GbE (SFP), 2x10/100/1000BaseT
 - LED scheme is OT Ready
- Follows the Industry Leading Industrial Ethernet (IE) look/feel
- DIN Rail mounting with optional Rack Mounting
- Connectors: Management Interface (RJ45 and USB); Power supports 24-12 AWG; Factory Reset
- Thermals: -40C to 60C no airflow; -40C to 70C with 40LFM; -34C to 74C with 200LFM
- Hazloc with nA protection
- IEEE 1613, IEC 61850-3
- EFT in Summer '15 and Launch in Fall '15

© 2013-2014 Cisco and/or its affiliates. All rights reserved.

ISA 3000 Copper



ISA 3000 Fiber



Cisco's Next Generation Firewall



- ▶ World's most widely deployed, enterprise-class ASA stateful firewall
- ▶ Granular Cisco® Application Visibility and Control (AVC)
- ▶ Industry-leading FirePOWER next-generation IPS (NGIPS)
- ▶ Reputation- and category-based URL filtering
- ▶ Advanced malware protection

Next Generation Firewall - AMP

Overview **Analysis** Policies Devices Objects FireAMP Health System Help admin

Context Explorer Connections Intrusions **Files > Network File Trajectory** Hosts Users Vulnerabilities Correlation Custom Search

Network File Trajectory for 0517f034...588e1374

File SHA-256 0517f034...588e1374

File Name [WindowsMediaInstaller.exe](#)

File Type [MSEXE](#)

File Category [Executables](#)

Current Disposition ✖ Malware

Threat Score ●●●○ High

First Seen 2013-12-06 10:57:13 on [10.4.10.183](#)

Last Seen 2013-12-06 18:17:27 on [10.4.10.183](#)

Event Count 7

Seen On 4 hosts

Seen On Breakdown 2 senders → 3 receivers

Trajectory

Events Transfer Block Create Move Execute Scan Retrospective Quarantine

Dispositions Unknown Malware Clean Custom Unavailable

Events

| Time | Event Type | Sending IP | Receiving IP | File Name | Disp... | Action | Protocol | Client | Web Ap... | Description |
|---------------------|------------------|-------------|--------------|---------------------------|----------|--------------------|-------------|---------|-----------|------------------------------------|
| 2013-12-06 10:57:13 | Retrospectiv... | | | | Malwa... | | | | | |
| 2013-12-06 17:40:28 | Transfer | 10.4.10.183 | 10.5.11.8 | WindowsMediaInstaller.... | Unkn... | Malware Cloud L... | HTTP | Firefox | | Retrospective Event, Fri Dec 6 ... |
| 2013-12-06 18:06:03 | Transfer | 10.5.11.8 | 10.3.4.51 | WindowsMediaInstaller.... | Unkn... | | NetBIOS-... | | | Retrospective Event, Fri Dec 6 ... |
| 2013-12-06 18:10:03 | Transfer | 10.5.11.8 | 10.5.60.66 | WindowsMediaInstaller.... | Unkn... | | NetBIOS-... | | | Retrospective Event, Fri Dec 6 ... |
| 2013-12-06 18:14:10 | Retrospectiv... | | | | Malwa... | | | | | |
| 2013-12-06 18:14:23 | File Quaranti... | | 10.5.11.8 | WindowsMediaInstaller.... | Malwa... | | | | | |
| 2013-12-06 18:17:27 | Transfer | 10.4.10.183 | 10.5.11.8 | WindowsMediaInstaller.... | Malwa... | Malware Block | HTTP | Firefox | | |

Centralized management - FireSIGHT

Can be managed as other ASA with FirePOWER Services

- Management for multiple devices
- Comprehensive visibility and control over network activity
- Optimal remediation through infection scoping and root cause determination



FireSIGHT Management offers:

Superior reporting and visibility



MiTM Attack

- Intercept communication between two or more devices
- Modify and inject packets
- Many tools available

Ettercap

Cain and able

Dsniff

- Scope of attack: modify cause of transmission field (CoT)
- Intercept and set an invalid CoT value
- Detection with Snort(ISA3000)

- Source: <http://www.slideshare.net/pgmaynard/man-inthemiddletalk>

Scada Strangelove

- *“Group of security researchers focused on ICS/SCADA security to save Humanity from industrial disaster and to keep Purity Of Essence”*
- Scada Scanner readily-available
 - Simple python script
 - Return device-name, IP, software version



Cisco CyberSEC Assesment

THANK YOU!

