IndusSec

Industrial Network Security System

9three Solutions Inc.

Market Forces

Social / Cultural Change

Generational change -> Data availability is expected and Individuals are more comfortable with accessing, monitoring, and remotely controlling critical infrastructure and sensitive information via web-based and mobile devices.

Including: Industrial Control Systems, Banking, Health Care

Technological Changes

High speed cellular coverage provides an alternative to expensive infrastructure

Legacy devices subject to new attacks (expanded threats)

Economic Changes

Cost/Consequence of Attack has gone up

Examples: Enrichment plants (StuxNet) / Duqu / Nightdragon, Target (Heartbleed), etc.

Cost to Hack has gone down

Easily accessible resources (hacker forums, group attacks), Tools (SHODAN, WireShark, Metasploit)

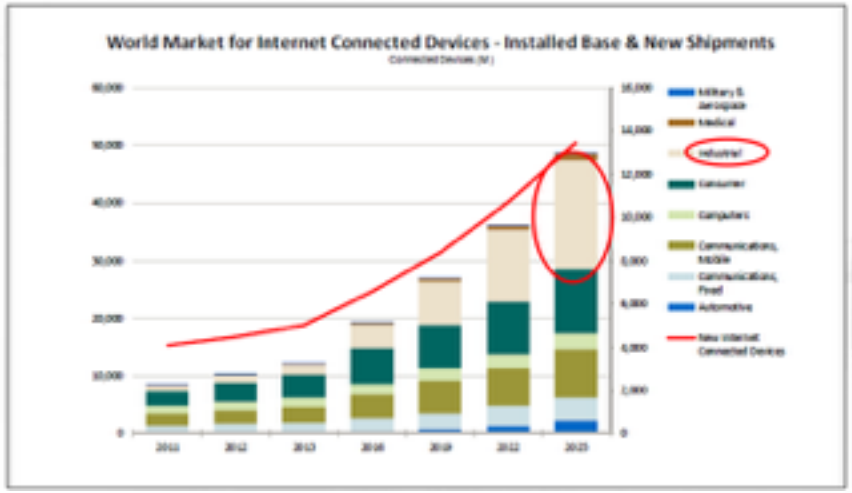
Cost of Solution has gone down

Open-source frameworks and components, Inexpensive cloud services

Market Forces (cont.)

Industrial Internet of Things

- Internet of Things: A network of physical objects that interact with each other to share information and take action
- There are several sub-segments within IoT, with Industrial applications having the most demanding uses



40 Billion
IoT Devices
by 2025

IHS 2013: Internet Connected Devices

ECHELON

The IndusSec System

- Target: Any companies that want to add remote monitoring and control, or already have deployed networks with Industrial Control Systems or house critical information.
- Problem: Unaware or uncertain of their attack vulnerability
- Solution: IndusSec Industrial Security system guards networks with the latest advancements in network security and provides full network isolation.
- Competitive Advantage over Cisco, Barracuda, and OEM VPNs
  - Extremely easy deployment and scalability (little or no configuration)
  - Easy web-based and mobile app data analytics and control.

Market Opportunity

- **Domestic and International Energy and Manufacturing Companies** who are vulnerable to Industrial Control System (ICS) attack, already have secure ICS infrastructure in place and want affordable secure redundancy, or have a need to secure temporary ICS installations.
- **Smaller Business** with security or privacy needs who can't afford the dedicated private infrastructure used by larger enterprises for their ICS installations, but would highly benefit by using the IndusSec System over the internet to build their ICS network.
- **Home Health Care Companies** providing remote monitoring of patient data or the dispensing of medication who are concerned with the security of their networks.
- **Consumers** or highly technical individuals with remotely accessible home automation, security, or surveillance systems and who are vulnerable to attack.

Security Vulnerabilities

Companies are unaware of risk:

Power grids, Machinery, Processes, Data are at risk to outside attack, potentially crippling systems and causing harm.

Number of attacks rose 52% in 2012 and 7200+ companies were at risk according to U.S. Dept. Homeland Security cybersecurity response team ICS-CERT.

Latest Attacks

Latest attack power transmission grids, wind turbines, nuclear plants and oil and gas pipelines. (Security Affairs)

HAVEX Trojan

- from Spam, exploit kits, and vendor websites.

Infects Software Update installers allows network access and OPC enumeration. (COM/DCOM)

Ugly Gorilla and PLA Unit 61398 (China) scouting and preparation

- Stole lists of field sites, such as block valve stations and compressors, that could be manipulated remotely, as well as SCADA log-ons and user manuals for servers.
- Pipeline schematics
- Security-guard patrol memos
- SCADA logons to systems that regulate the flow of natural gas. (could cause outages or explosions)

Why? IT / Systems Integrator Gap

There is an interesting gap between the world of systems integrators who want high reliability and simple configuration and traditional IT support personnel who want secure high speed systems. This can lead to inconsistent and sometimes non-existent policies.

Many of the systems identified in the cyber security attack reports “have either weak, “default, or nonexistent logon credential requirements.”

The IndusSec System Solution

IndusSec System Component

- IndusSec Secure Network Appliance w/w 4G LTE
- Private Cloud Routing Servers
- Web-based Analytics and Control Panel
- iPhone / Android / Windows Store App
- IndusShell Diagnostic Utilities
- Windows PC / Linux Access Client

Problems Solved

- Security, Flexible Connection, & Easy Deployment
- Full Network Isolation & Redundancy
- Control, Detection, Analytics
- Convenience & Accessibility
- Interactivity

IndusSec

Secure Network Appliance

9three Solutions

IndusSec Secure Network Appliance Features

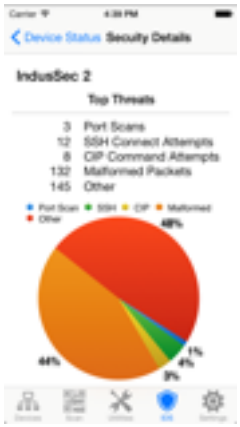
- 3 Step “Plug and Play” Ease of Use
- “Locked-Down” Operating System
- Device-Based Authentication
  - Ethereal Public Key encryption (No Passwords, Regenerates every hour)
- 120v AC or 7-18v DC Power
- 10 /100 / 1000 Mb Ethernet
- Diagnostic Utilities over SSH or Serial Port
- Compliance
  - CE EN 61000-6-3 (2005)
  - CE EN 61000-6-2
  - FCC Part 15
- Flexible Communications – can use
  - Supplied Internet connection
  - Interact and bypass corporate firewalls
  - Use optional 4G LTE Wireless Communications Card with GPS.
- Optional Outdoor Enclosure
  - IP65 Rated, Complete protection from dust, oil and other non-corrosive material
  - Complete protection from contact with enclosed equipment
  - Protection from water (up to water projected by a nozzle against enclosure from any direction.
  - Flat or Pole Mounting

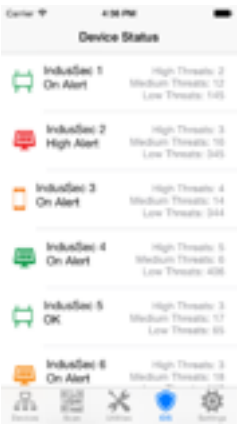
IndusSec

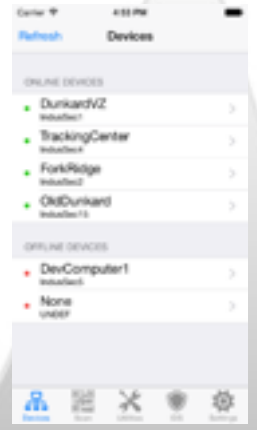
Private Cloud Routing Servers

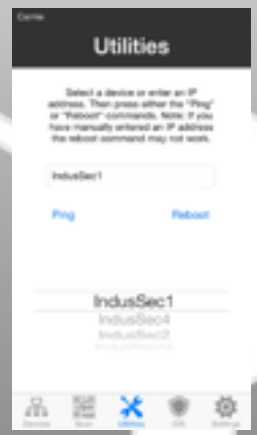
Private Cloud Routing Server Features

- Multi-tiered East-West coast Master-Master Application and Database Replication
  - Highly Scalable
  - Highly Available
  - Disaster Resistant
- Isolates control system networks from other networks. Application and Routing Isolation
- Can forward all Layer 2 and above traffic including non-TCP/IP (i.e. CIP, token ring)
- Accommodates existing network configurations
  - typically no need to re-configure network or add security exceptions
- Military Grade Encryption
  - Certificate-based Trusted Authority Authentication
  - 4096 Bit RSA Key Exchange, 256 Bit AES Cypher
- Email and Text Alerts
- Reverse-Proxy and Load Balancing
- Smart Traffic Detection
- Intrusion Detection System
  - CIP Commands
  - Connection Attempts
  - Port Searches
  - Deep Packet Inspection
- Remote testing and diagnostic utilities
  - Speed Tests
  - Reboot
  - Wireless LTE Network Utilities
- Web Control Panel with Analytics
- RESTful APIs for Easy end-user application development.









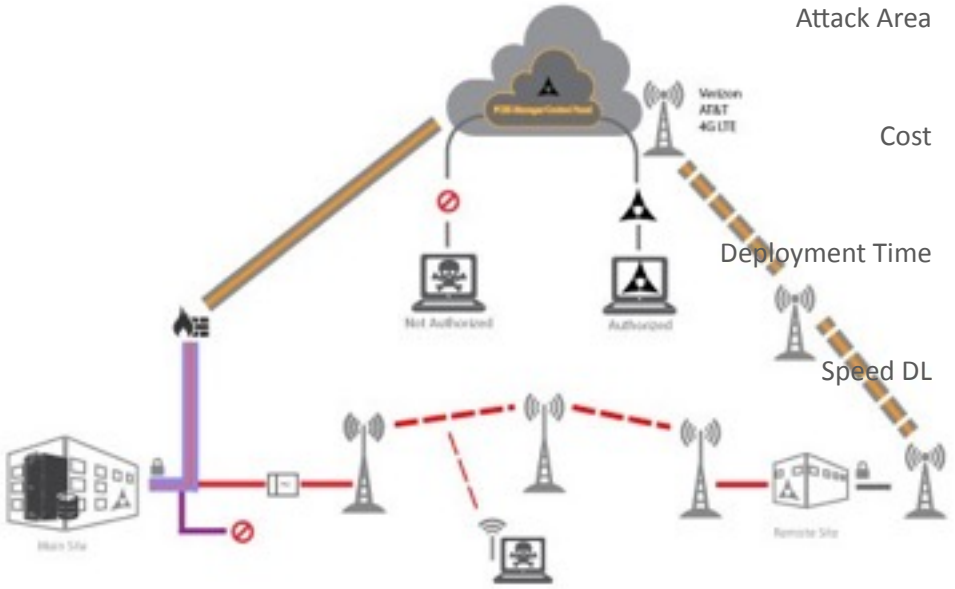
INDUSSEC

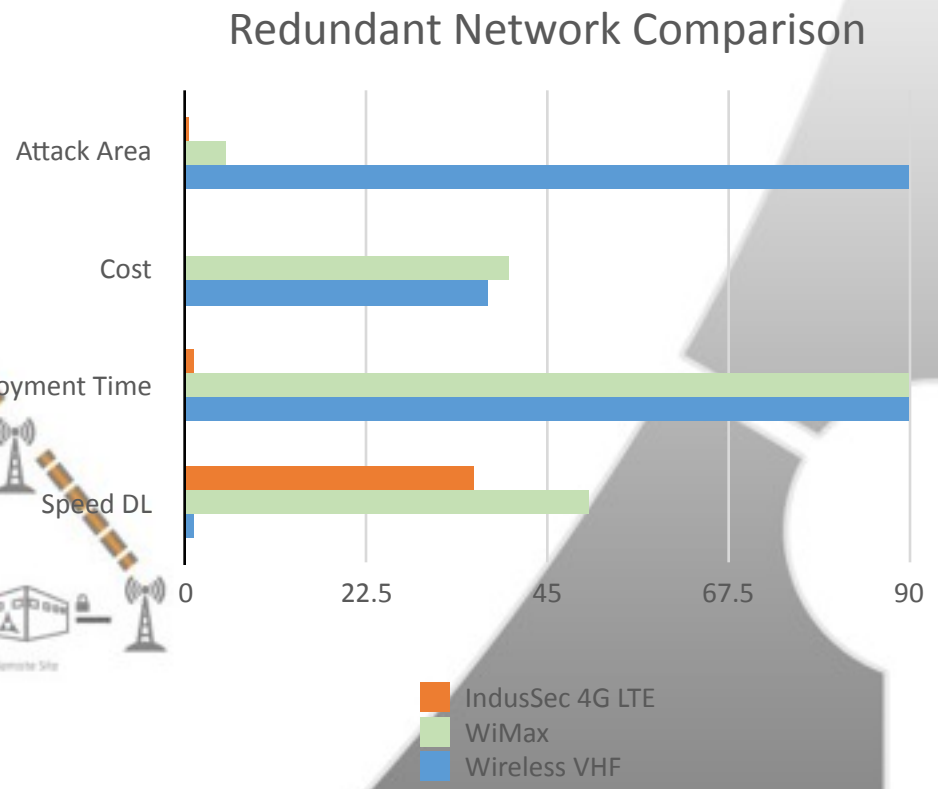
iPhone / Android* / Windows Store* App

PC / Mac / Linux Access Applications

9three Solutions

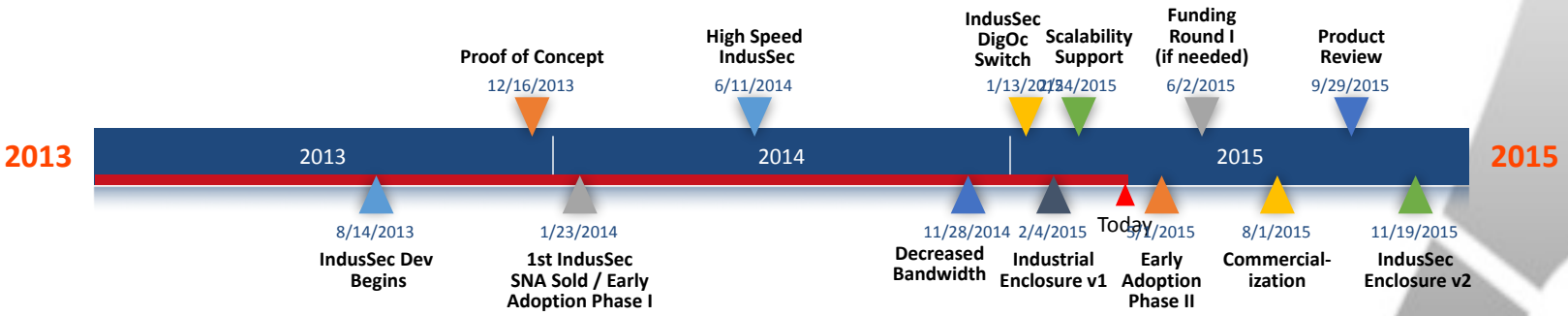
Case Study: 138kV Communications Diagram and Network Comparison





9three Solutions

Milestones and Commercialization Timeline



Key Partners / Players / Early Adopters:

- Murray American Energy, Netgate / PC Engines GmbH, American Intertech, Comdel Manufacturing and Fulfillment, Robert C. Byrd Institute

Questions?

Mike Lyons – mike.lyons@9threeSolutions.com
t: 304-241-5965 c: 304-685-7842

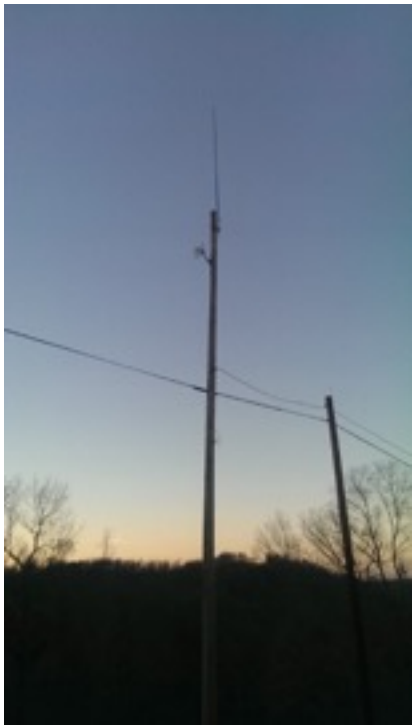
138kV Substation Installation

138kV Control Building Installation

Communications Center Installation

Underground Mine Ventilation Fan

9three Cellular Repeater Installation



9three Solutions

9three Mine Ventilation Fan House Installation