



# Industrial Cyber Security as a Service (ICSaaS)

*Leveraging the Cloud to Protect Your OT Environment*

**Barak Perelman**

Indegy - Co-founder & CEO



# About the Presenter

*Barak Perelman*

- **CEO & Founder at Indegy – a Tenable Company**
- **15 years hands-on experience in cyber security and ICS.**
- **(Res.) IDF Major, holds a B.Sc in CS and MBA.**

*Indegy provides situational awareness and real-time security for industrial control networks to ensure operational continuity and reliability.*



# Seventy-Five Percent

Of midsize and large organizations

**“Gartner predicts that by 2021, over 75% of midsize and large organizations will have adopted a multi-cloud or hybrid IT strategy.”**

Source: Smarter with Gartner - 5 Approaches to Cloud Application Integration – 14 May 2019



# ICS in the Cloud

**“If you don’t think we’re moving to the cloud then you probably need to update your resume and find a new job – because that’s where we’re all going. This (Indegy CIRRUS) is a perfect example because knowledge is power.”**

John Roosa, CIO, STUPP Corporation  
(Indegy customer)

# What is ICSaaS?

Best practices for architecture

# When should I deploy which?

On premises, virtual, pure or hybrid cloud – benefits and limitations

# What do I gain?

Optimize for your organization

# What is ICSaaS?

Best practices for architecture

## When should I deploy which?

On premises, virtual, pure or hybrid cloud – benefits and limitations

## What do I gain?

Optimize for your organization

# What It Is, Where It Fits

*Industrial CyberSecurity As A Service (ICSaaS)*



**Cloud technology** that enables organizations – global multi-site to small single-site – to experience **industrial cybersecurity** transparently across all assets and locations.

# Industrial Security Context

*What Does It Mean for OT?*



## Live Feed

- 24/7 Live Updates of Threat Intelligence
- Third-party sources such as NVD, ICS-CERT
- Internal data from Indegy Labs and Tenable Research
- Bonus: Automated Software Updates





# Industrial Security Context

*What Does It Mean for OT?*



## Cloud Enterprise Management

- Access to multi-site management from the Cloud
- Enables global access and control to the OT environment from anywhere
- Configure uniform policies and compliance mechanism across the org

# Industrial Security Context

*What Does It Mean for OT?*



## Remote Active Queries

- Active queries over VPN connection from “the cloud”.
- Can be utilized over either private or public cloud infra
- All the advantages of active technology without the hassle of added hardware

# Industrial Security Context

*What Does It Mean for OT?*



## Cloud Collaboration

- Automated learning from anonymized patterns
- Brings industrial analytics expertise to a global footprint (i.e. will alert the entire Indegy user base)
- Integration with Tenable Lumin to provide a full IT/OT Cyber Exposure analysis based on business risk

# What is ICSaaS?

Best practices for architecture



Live Feed



Enterprise Mgmt



Remote Active



Cloud Collab.

# When should I deploy which?

On premises, virtual, pure or hybrid cloud – benefits and limitations

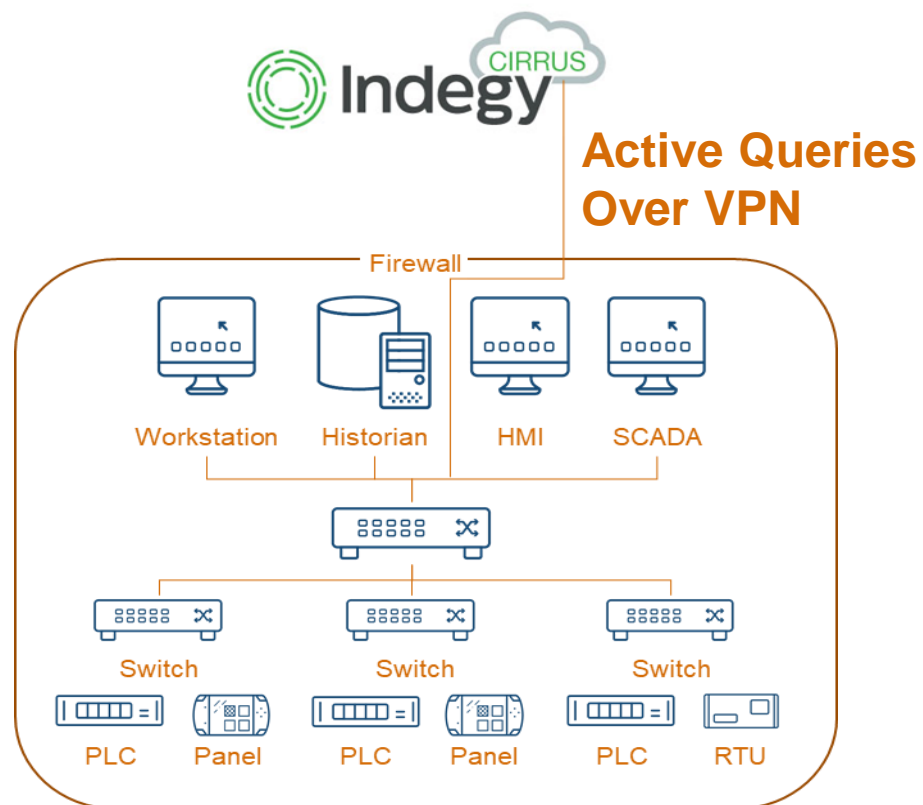
# What do I gain?

Optimize for your organization

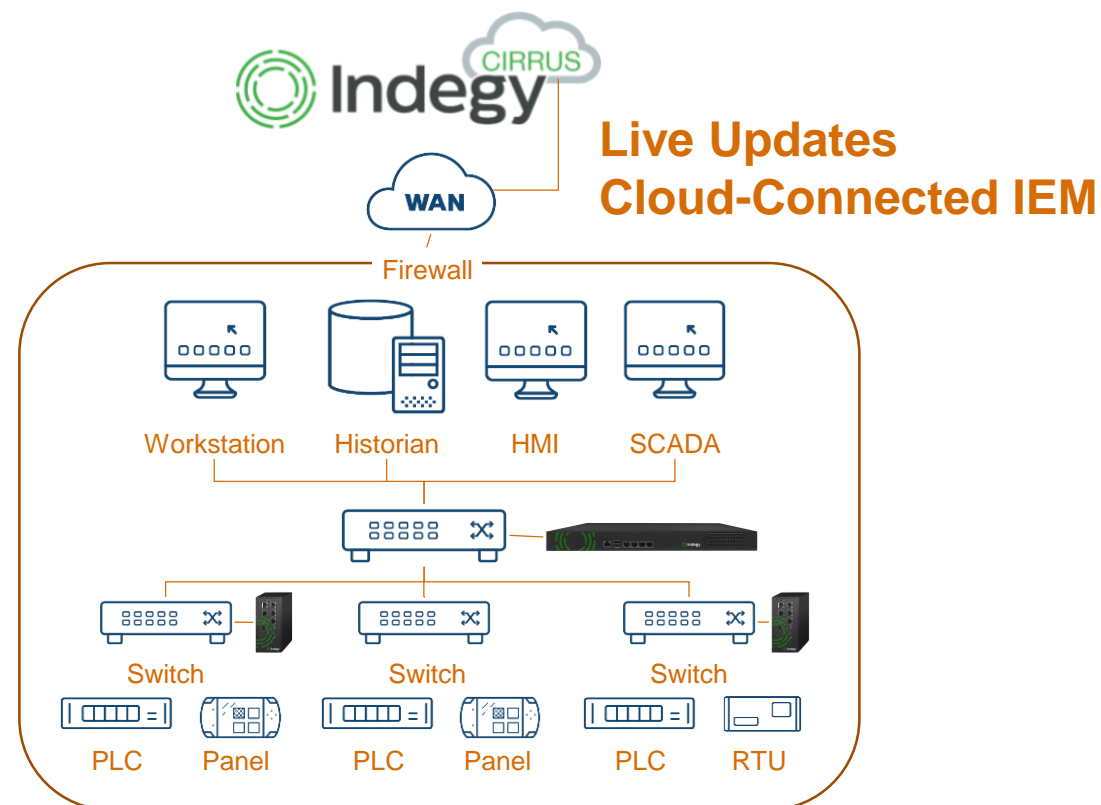
# Indegy CIRRUS

## Topology

### Pure Cloud



### Hybrid Cloud





# Examples of Industrial Deployments



- e.g. municipal water treatment facility
- Typically deployed for regional HQ
- Does not require ongoing trained personnel on premises



- e.g. drill station for oil & gas
- Typically deployed for multi-site remote locations
- Outsources personnel or operates without any need for on-site expertise



- e.g. automotive plant
- Typically deployed at HQ to secure critical assets
- HQ acts as hub and aggregation point for all locations
- Requires trained personnel

# What is ICSaaS?

Best practices for architecture

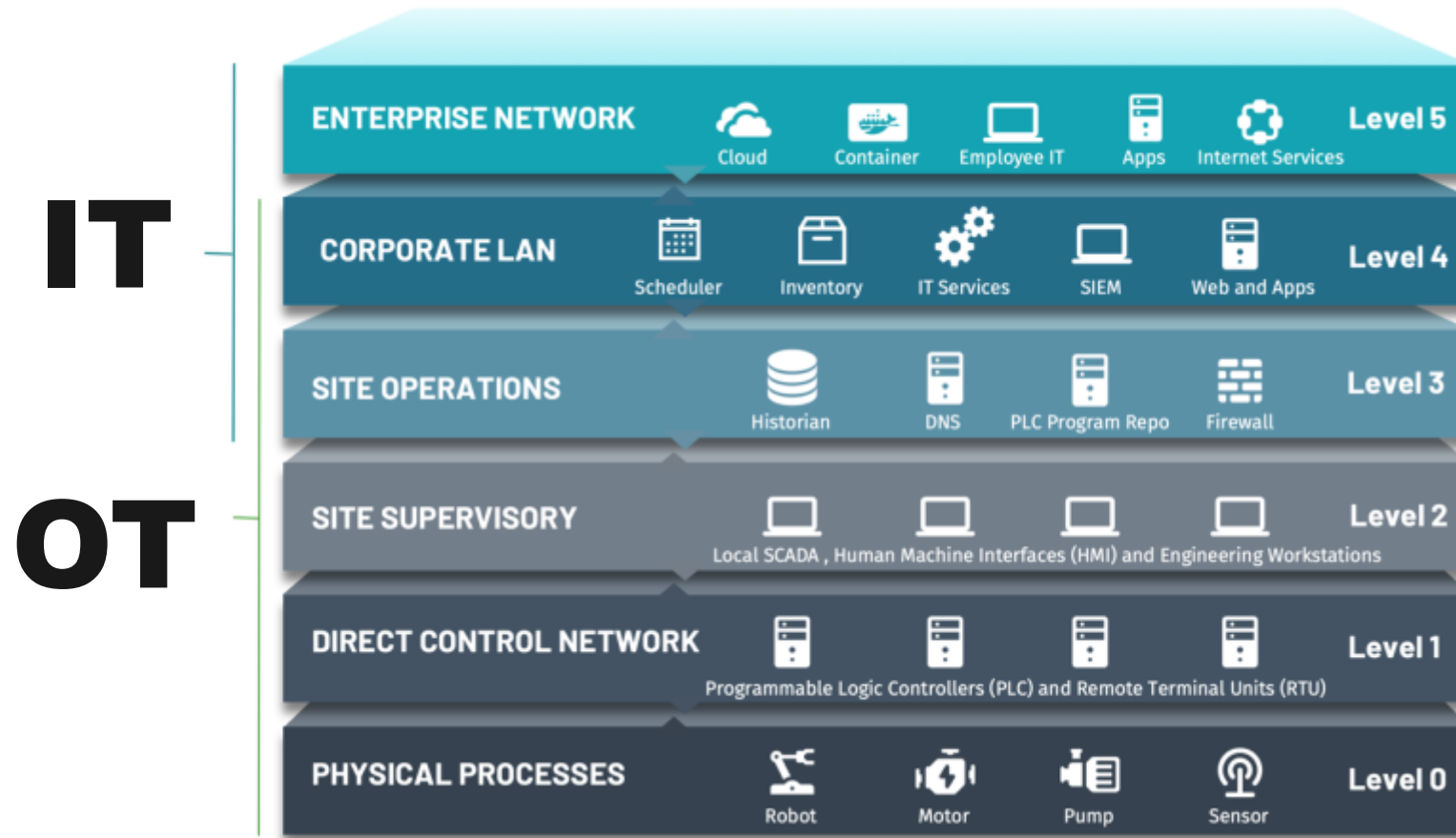
# When should I deploy which?

On premises, virtual, pure or hybrid cloud – benefits and limitations

# What do I gain?

Optimize for your organization

# Optimization: Is bringing cloud & IT & OT together



Unified  
Visibility to  
**Risk-based  
IT/OT Security**

# Manage Your Cyber Exposure



ITSM



SOAR



REMEDIATION



ANALYTICS

## CYBER EXPOSURE MANAGEMENT

Scoring, Business Insights, Risk-based Trending, Benchmarking

### CORE APPS

Tenable.sc

Tenable.io VM

Web Application  
Security

Container Security

New

OT Security

### TENABLE DATA PLATFORM

### DATA SENSORS

IT & Infrastructure Sensors  
Nessus, Agents

AppSec Sensors CS

Third Party Data

New

Indegy OT Sensors

Public Cloud Sensors  
Cloud Connectors

# Thank You

For more information, contact us at:

[tenable.com](https://tenable.com)

