APRIL 2023

Cybersecurity and AVEVA Cloud Products

System Design for Defensible Security

Michael Brost
Sr. Principle Technical Sales Consultant
Community of Practice Leader – America’s Monitoring and Control

Getting data to the Cloud

- Many Consumers of OT Information are Cloud based
  - Browsers, Phones, External Organizations
- OT Network should be isolated from these Consumers
- Data transmission to Cloud secured at Rest and In Motion
- Cloud communication should only be originated from OT Network
  - Transmission must be able to be routed through multiple firewalls and DMZs
  - Consumption back to OT Network must follow the same path.
- Information should be bound to the sending device

AVEVA™

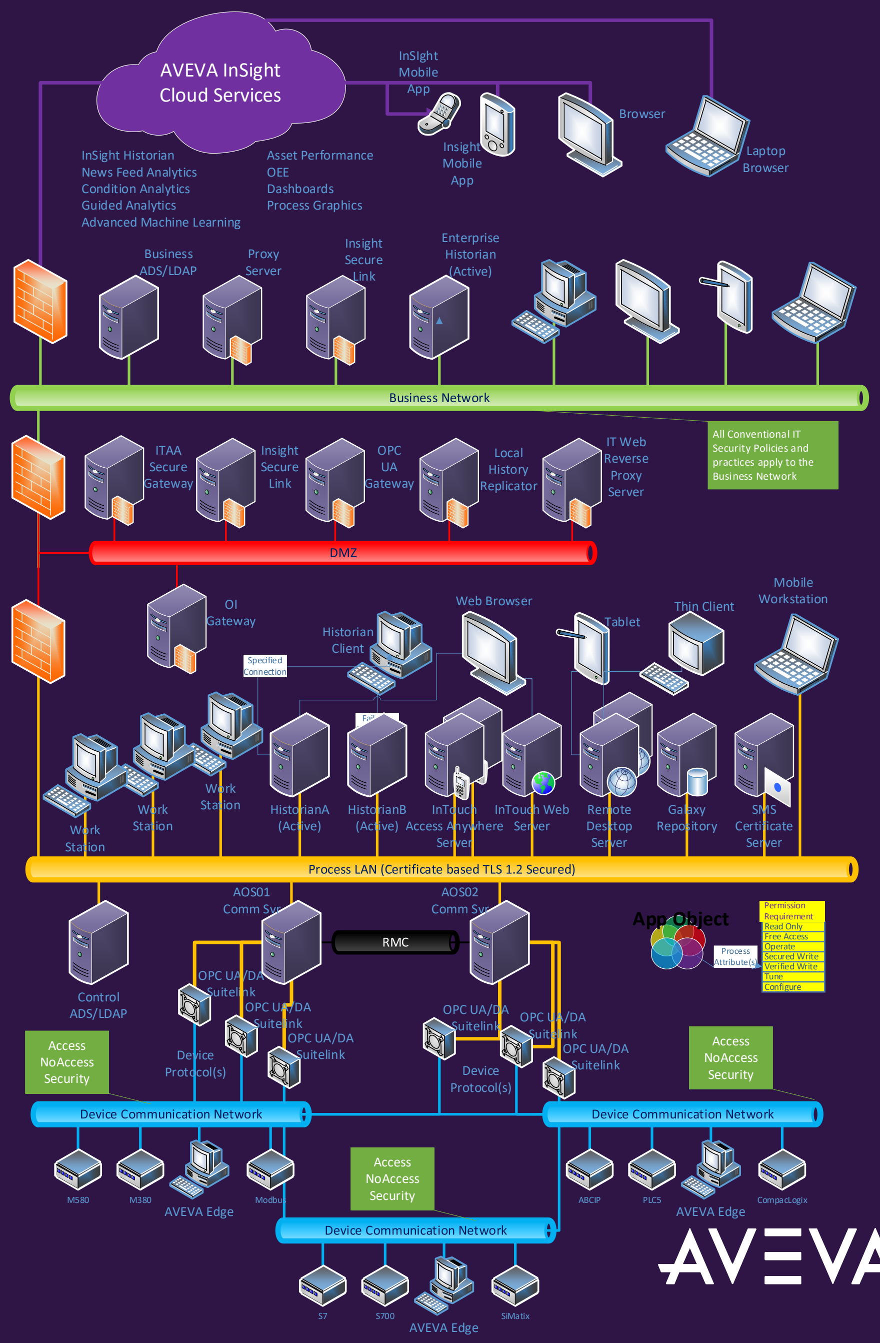
Network Architectures

Network Architecture

Connected and Securely Isolated

- AVEVA Insight Cloud (Purple)
- Business Network (Green)
- Site DMZ Network (Red)
- Process/Control Network (Orange)
- Redundant Message Network (Black)
- Device Network (Blue)
- All Intrusion Protection Active and Enforced
- Firewalls Isolate all Traffic to Control Devices

AVEVA System Platform Network Architecture

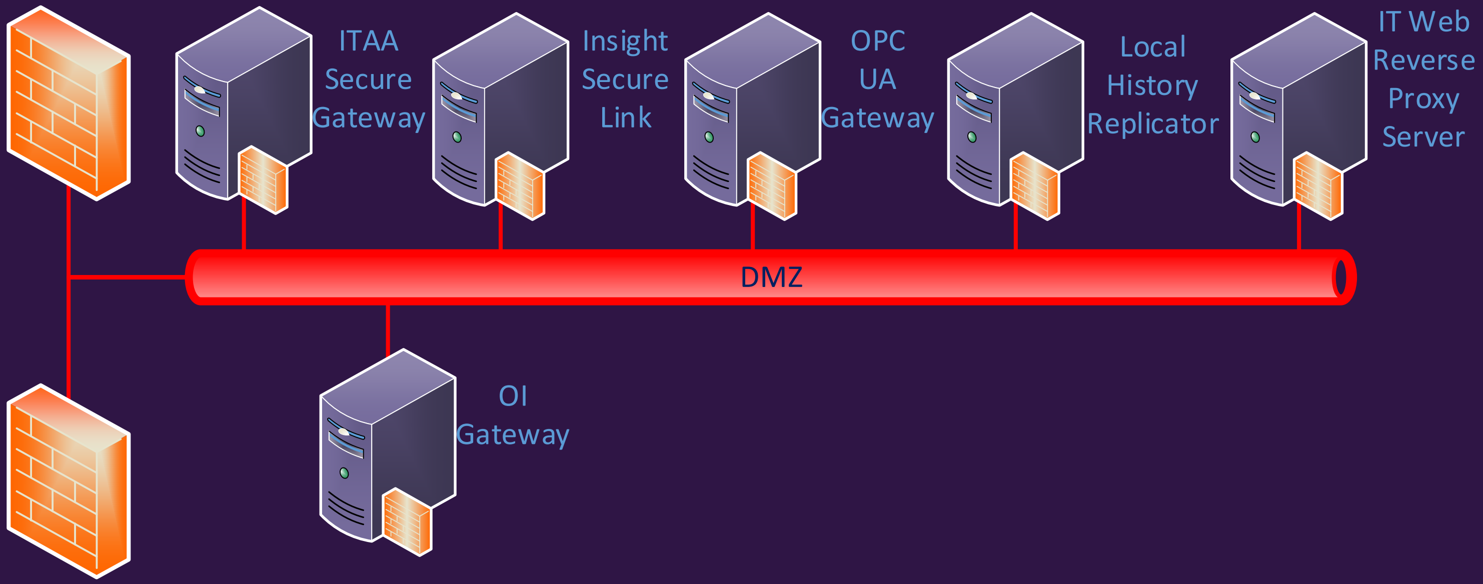


AVEVA

DMZ Network (Red Network)

Isolation between Control and Business

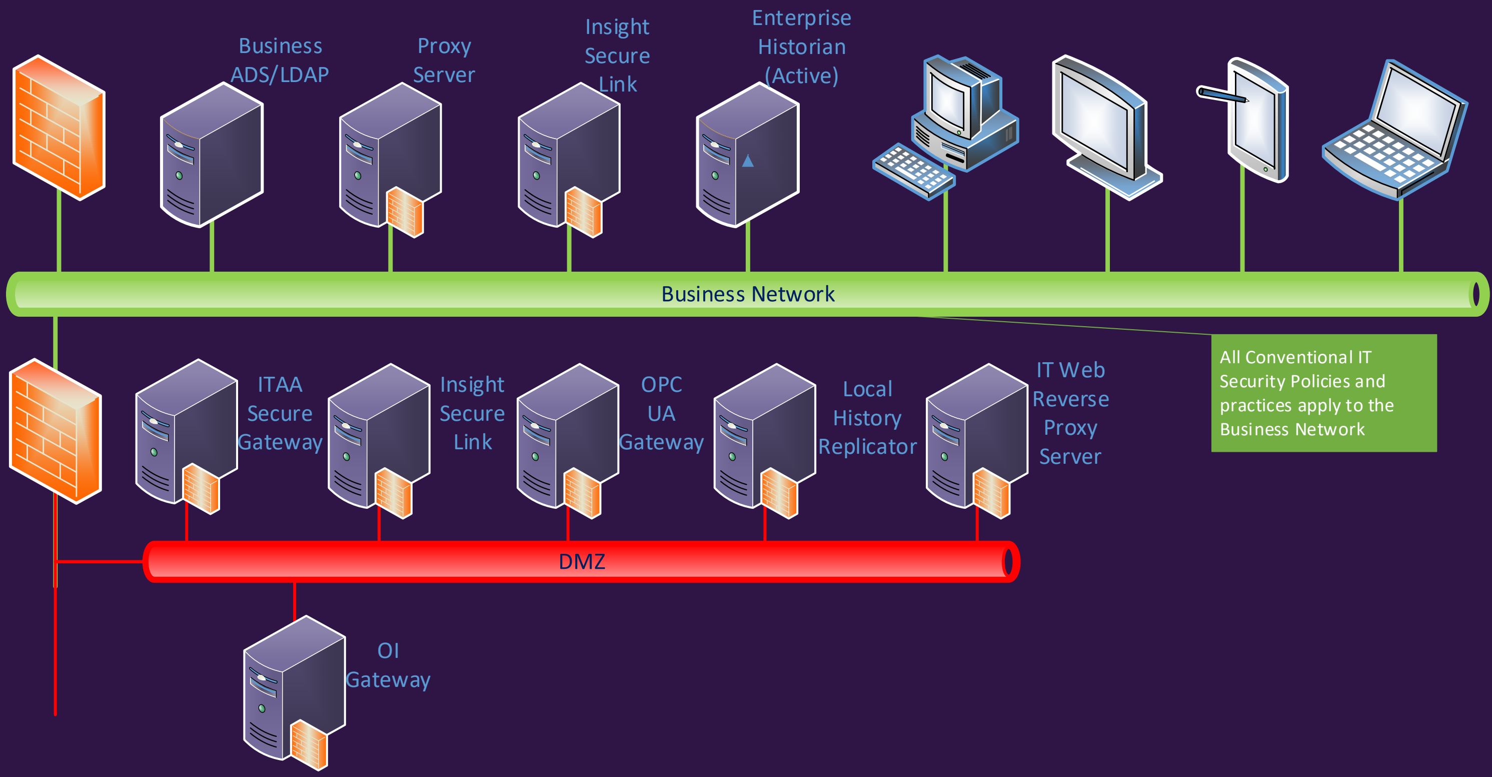
- Firewall Isolated from Control and Business Networks
- Access Routed through Proxies
  - Insight Secure Link
  - Local History Replicator
    - (Currently Enterprise Historian)
  - ITAA Secure Gateway
  - IT Web Reverse Proxy
  - OPC UA Gateway
  - OI Gateway (OPC DA, MQTT, Suitelink, DDE)



Business IT Network (Green Network)

General Purpose Business Network

- IT Security Policies and Practices
  - AI Virus Protection (Cylance or Virsec)
  - Domain Isolation (Business ADS)
  - IT Proxy Server to Internet
  - Insight Secure Link
  - Enterprise Historian (AVEVA or OSI PI)
  - Securely Expose Command and Control Through DMZ
  - Firewalls to DMZ and Internet

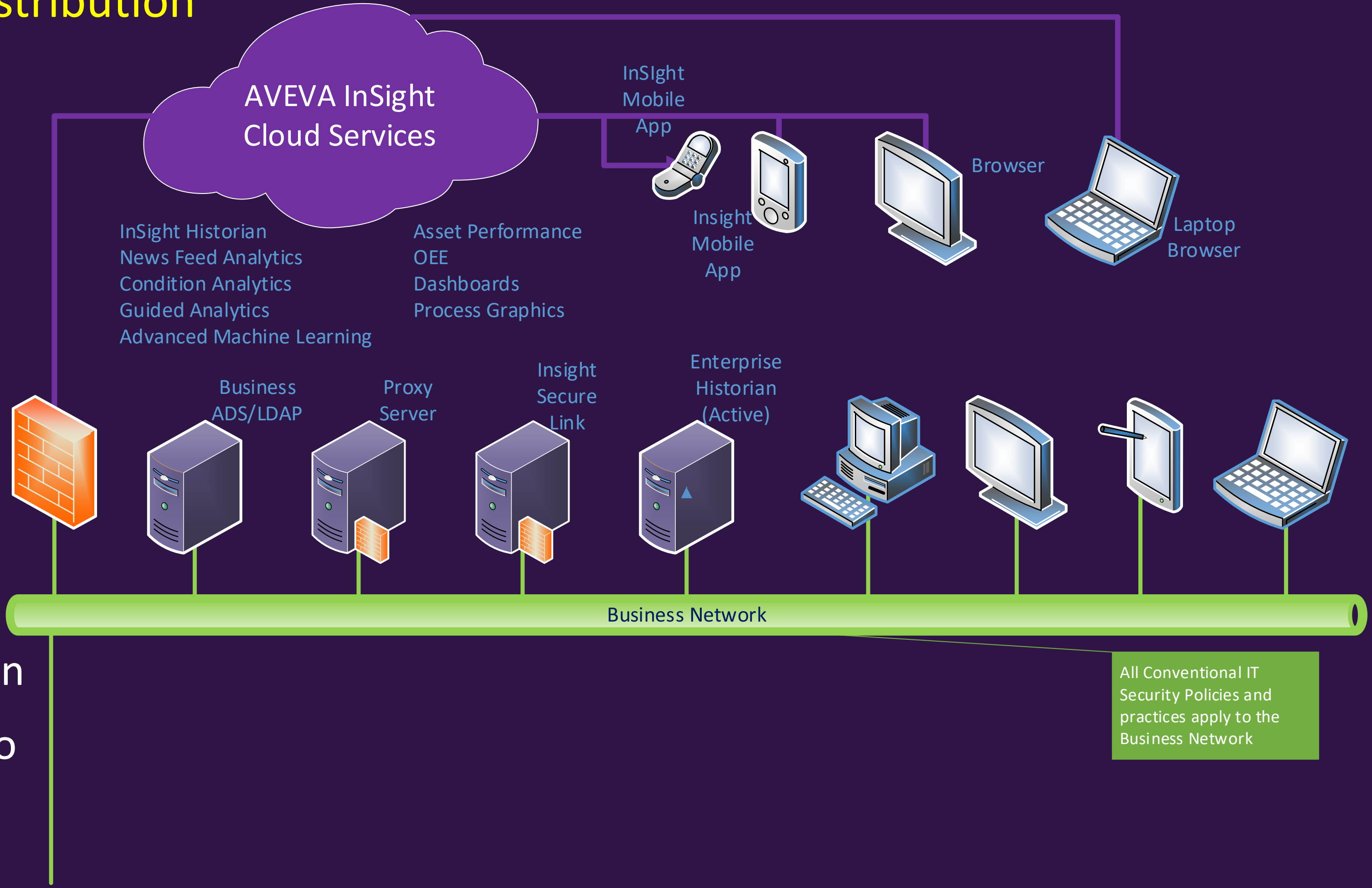


All Conventional IT Security Policies and practices apply to the Business Network

AVEVA Insight Cloud Services (Purple Network)

Cloud based Analytics and Information Distribution

- Secure Data Transmission To/From InSight Cloud via Insight Secure Link
- All Transmission Certificate based and Encrypted with TLS 1.2
- Values are Normalized to 0.0 – 1.0 Identified only by GUID
- MetaData is Identified by GUID
- MetaData and Values stored separately in Insight.
- Transmission Securely from Control Domain
- Cloud Based Analytics Available Securely to Control Domain

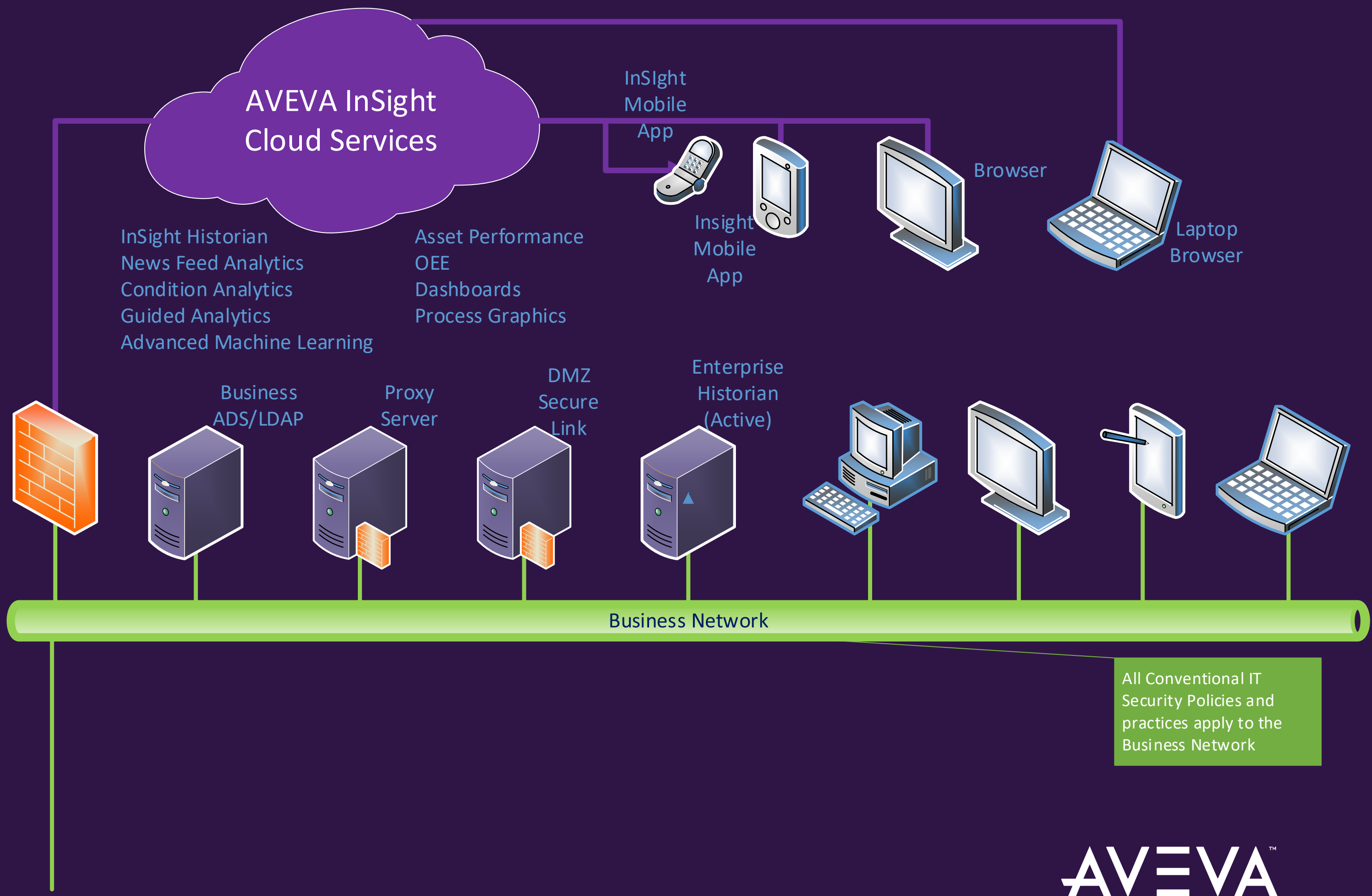


All Conventional IT Security Policies and practices apply to the Business Network

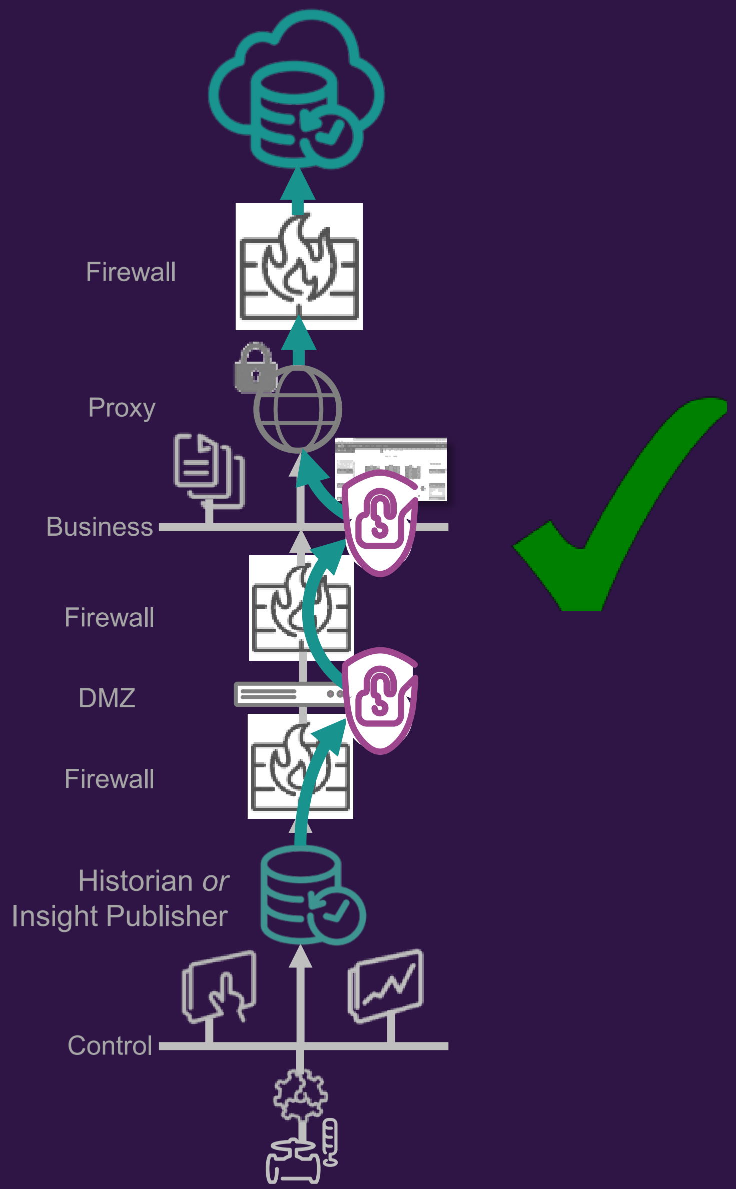
AVEVA Insight Cloud Services (Purple Network)

Cloud based Analytics and Information Distribution

- InSight Historian for Time Series Data
- OEE for Machine Performance
- News Feed for Unsupervised Analytics
- Condition Based Analytics
- Guided Analytics for Asset Specific AI
- Advanced Analytics for Multi-Variate AI
- Dashboards
- Process Graphics
- Securely Distribute Information to Cloud Consumers
- OData and REST API

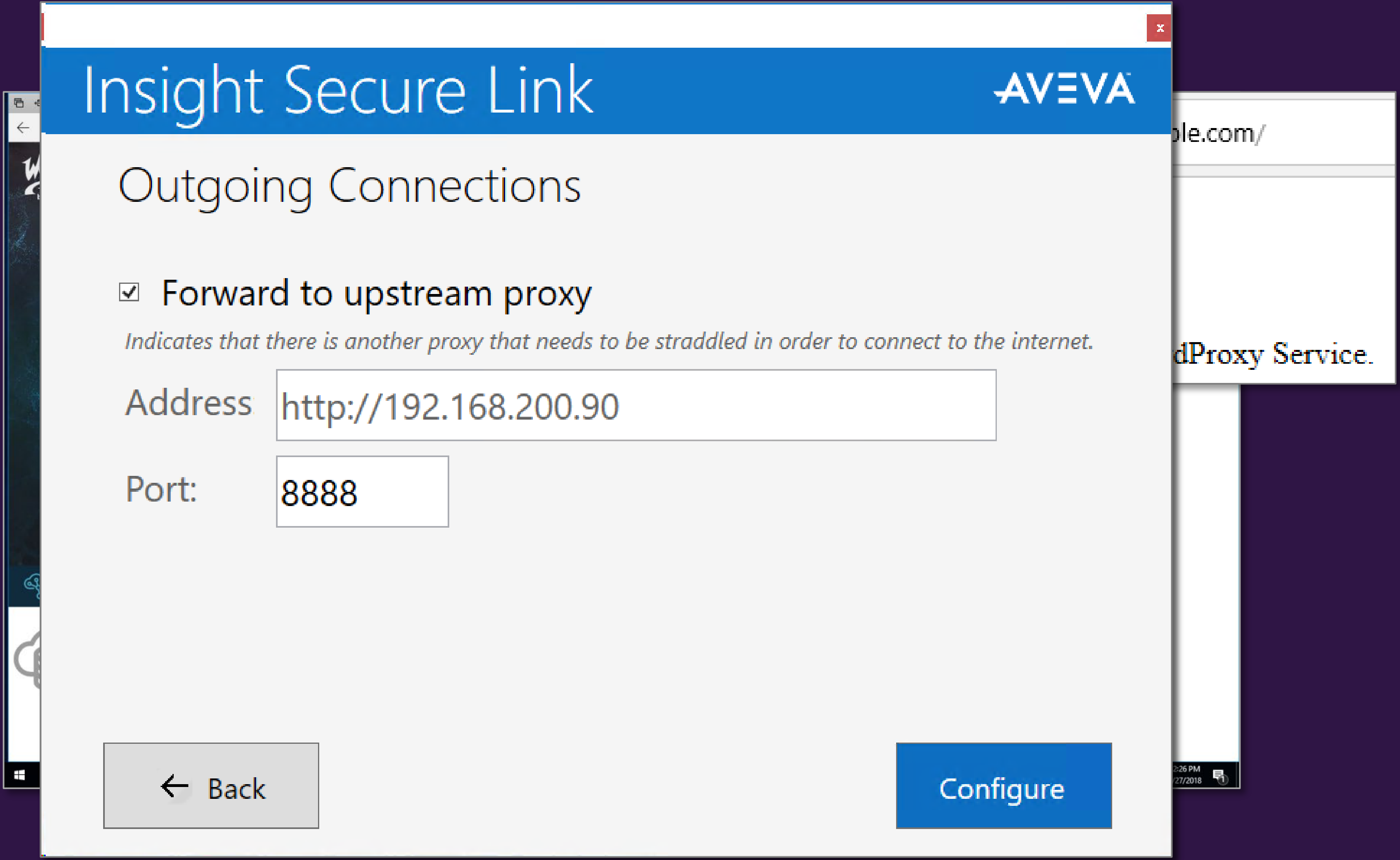


Insight Secure Link



- Single outbound-only port (443)
- No inbound connection
- All traffic encrypted (TLS)
- Anonymous HTTP proxy
- DMZ
- Can be chained together
- Whitelist maintained from AVEVA Cloud

InSight Secure Link Provides Limited Internet Access To/From Control Domain



Insight Secure Link

Outgoing Connections

☑ Forward to upstream proxy

Indicates that there is another proxy that needs to be straddled in order to connect to the internet.

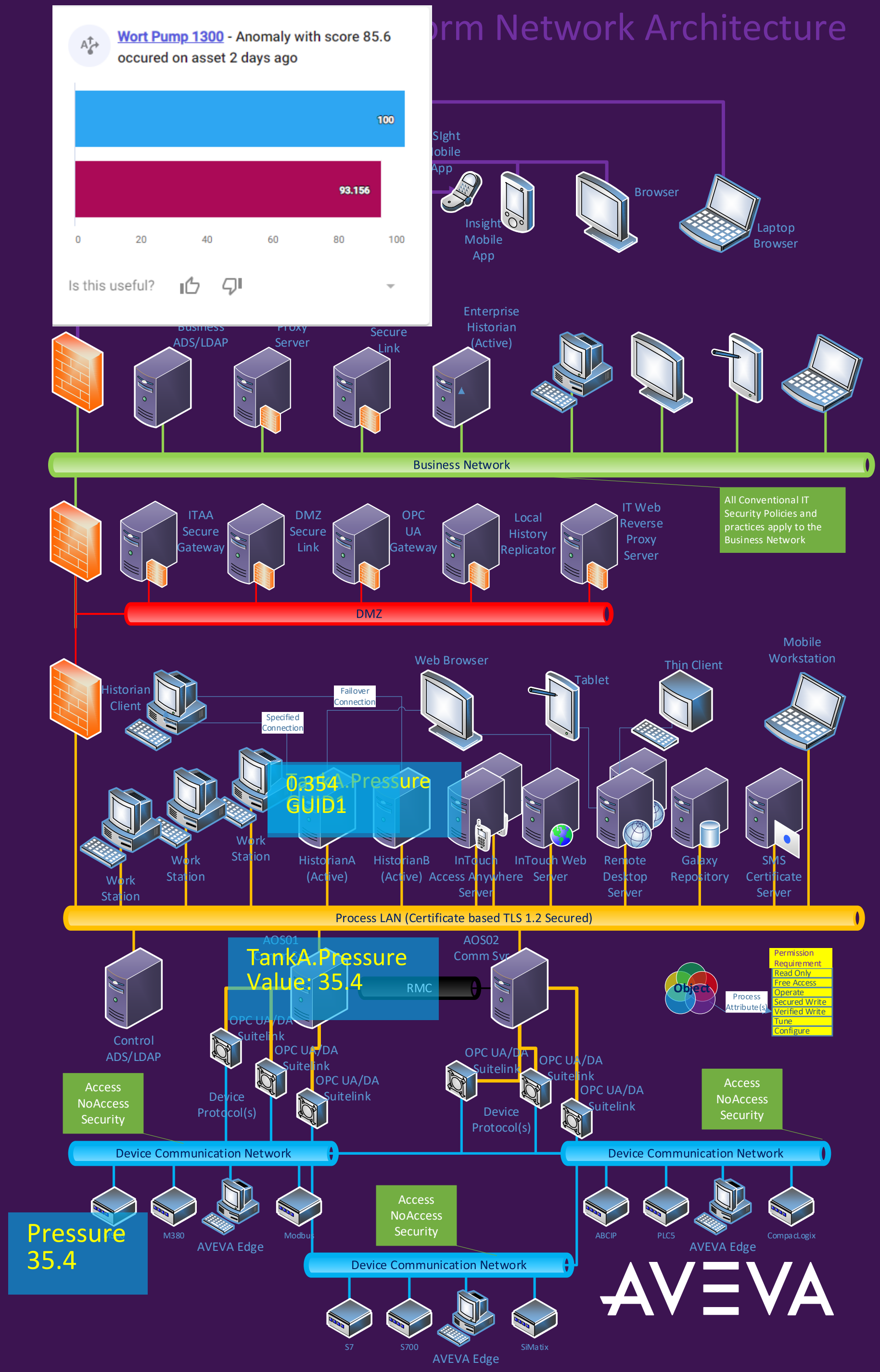
Address http://192.168.200.90

Port: 8888

Securing Data To AVEVA InSight

Connection can Only be originated from Process LAN

- Device to Application Server Object
- Object to AVEVA Historian
  - Encrypted Certificate based TLS 1.2
- Historian to Insight Secure Link
  - Denies all Outbound Traffic, Except to AVEVA InSight
  - Denies all Inbound Traffic, Except from AVEVA InSight
  - Encrypted Certificate based TLS 1.2
  - Tag Metadata Keyed by GUID, Sent on Change
  - Value reduced to 0.0-1.0 Keyed by GUID
- DMZ Insight Secure Link to Business Insight Secure Link
- Business Insight Secure Link to Proxy Server
- Proxy Server to Business Firewall to InSight Cloud
- InSight Combines Metadata and Value Together
- InSight Content Delivered Back Through Firewall/Proxy Chain



Wort Pump 1300 - Anomaly with score 85.6 occured on asset 2 days ago

Is this useful?

?

This presentation may include predictions, estimates, intentions, beliefs and other statements that are or may be construed as being forward-looking. While these forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could result in actual outcomes differing materially from those projected in these statements. No statement contained herein constitutes a commitment by AVEVA to perform any particular action or to deliver any particular product or product features. Readers are cautioned not to place undue reliance on these forward-looking statements, which reflect our opinions only as of the date of this presentation.

The Company shall not be obliged to disclose any revision to these forward-looking statements to reflect events or circumstances occurring after the date on which they are made or to reflect the occurrence of future events.

linkedin.com/company/aveva

@avevagroup

ABOUT AVEVA

AVEVA is a global leader in engineering and industrial software driving digital transformation across the entire asset and operational life cycle of capital-intensive industries.

The company’s engineering, planning and operations, asset performance, and monitoring and control solutions deliver proven results to over 16,000 customers across the globe. Its customers are supported by the largest industrial software ecosystem, including 4,200 partners and 5,700 certified developers. AVEVA is headquartered in Cambridge, UK, with over 4,400 employees at 80 locations in over 40 countries.

aveva.com

AVEVA