ACCELERATING INNOVATION

Session 3-1293: Field Protection Against Cyber Attacks with Active Directory and DNP3

22 May 2025

Room 301A

EMERSON EXCHANGE 2025
ACCELERATING INNOVATION

Disclaimer

The information and/or opinions expressed in this presentation are those of the authors and do not necessarily represent official policy or permission of Emerson or Emerson Exchange.

Important Reminders

Photography and audio/video recording is not permitted in any session, or in the exhibition areas, without press credentials or written permission from Emerson or Emerson Exchange.

Inquiries should be directed to:
EmersonExchange@Emerson.com

Eric Cytrynowicz

RTU Product Manager / Emerson

Mike Taccino

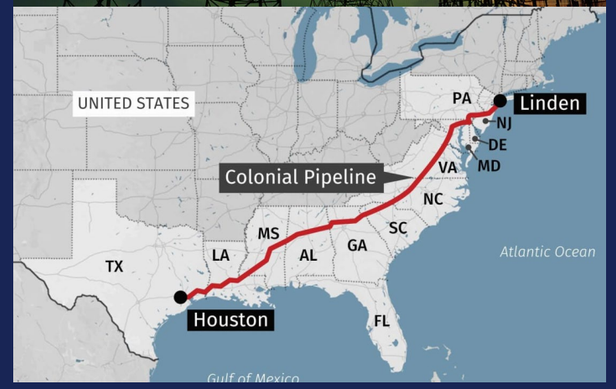
FBxConnect Product Manager / Emerson

EMERSON EXCHANGE 2025

ACCELERATING INNOVATION

Targeted CyberSecurity Attacks are Real and Increasing

- **August 2012 Saudi Aramco & Qatar RasGas Attack**
  - 35,000 Servers and Workstations wiped & destroyed
  - After 17 days oil was given away for free to stabilize the Saudi Kingdom; as business systems run manually on paper
  - 50,000 Hard drives had to be replaced, took 5 months to recover
  - Attributed to Cutting Sword of Justice (Iran)
- **December 2014 Ukraine Power Grid Attack**
  - Modified Firmware, disabling field equipment
  - Shutdown SCADA System, UPS's, compromised Control Network
  - Three separate SCADA systems attacked, partial grid shutdown for 6 hours
  - Attack attributed to Russia
- **May 2021 Colonial Pipeline Attack**
  - Targeted IT but affected OT
  - 12,000 gas stations; 29 refineries; 267 terminals
  - American Airlines temporarily stopped flights
  - Attributed to Russian based ransomware group



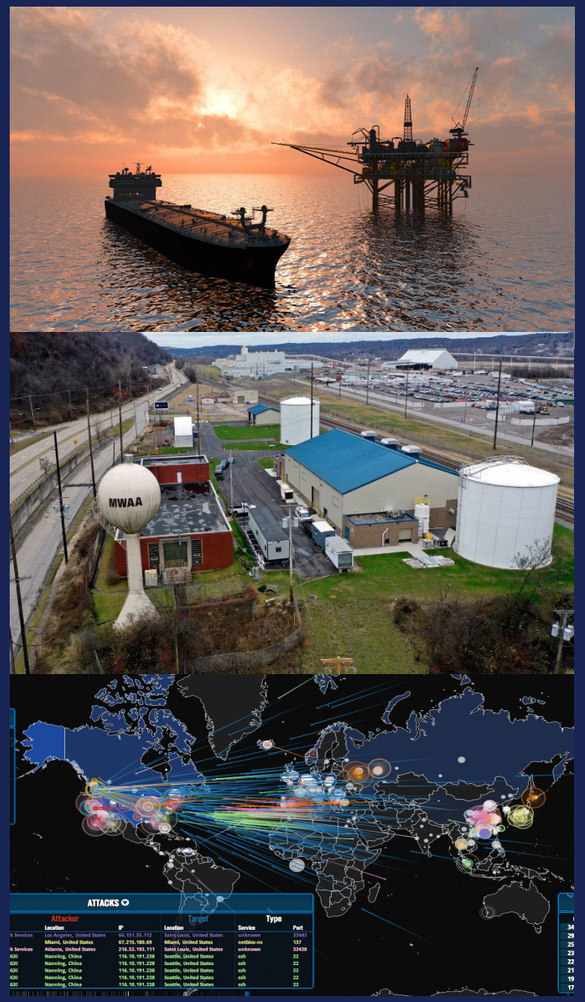
*https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Targeted CyberSecurity Attacks are Real and Increasing

- **February 2022 European Oil Terminals**
  - Multiple Oil Terminals across Belgium Germany attacked
  - Unable to process incoming Oil barges/deliveries
  - Attributed to Russian sponsored hacking group

- **November 2023 Water and WasteWater Shutdown**
  - Anti-Israel graffiti displayed on operation terminals in Aliquippa, PA
  - Operators had to shut down service while removing malware
  - Attributed to Iranian IRGC group

- **January 2023 – January 2024 Global Infrastructure**
  - 420 Million attacks – 13 attacks/second, ranging in magnitude (Vedere Labs)
  - 163 Countries - Primary targets: USA, UK, Germany, India, Japan
  - Threat Actors: China, Russia, Iran



https://www.vox.com/2014/6/26/5845916/watch-cyberattacks-around-the-world-in-real-time

Over 16 Significant Cyber Attacks Reported to CSIS in 2025

*https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

A new threat – Salt Typhoon

- Confirmation that “Salt Typhoon” was behind several attacks on US telecom service providers
- PRC based actors (2019) have maintained extensive persistent access systems in the U.S. and abroad
- Salt Typhoon’s campaign has focused on compromising routers and c network devices to establish persistent access
- Their activities have been primarily espionage-oriented, to collect s data, such as authorized wiretaps, from ISP networks while mainta a low profile
- This threat actor mirrors some tactics from other Typhoon group especially using LOTL techniques to prolong their foothold in targeted environments

An existing threat – Volt Typhoon

- The Cyber attacks against Ukraine were clearly preparation for Russian Invasion
- Since then, the focus of Cyber Attacks has switched to the People's Republic of China
- **In March 2024 CISA warn that "Volt Typhoon" is a huge threat**
- **The PRC have infiltrated US critical infrastructure, including interstate pipelines**
- CISA, Pipeline Operators and major SCADA vendors are working to address the threat
- CISA, and the US Govt believe that this is pre-positioning prior to a potential physical attack elsewhere in the world

https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

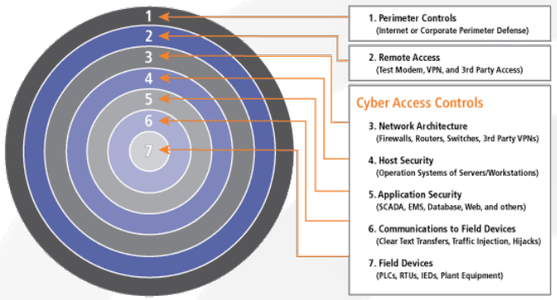
‘Allegations and a Farce’

- China has denied allegations by the US government and Microsoft that a state-sponsored hacking group called the Volt Typhoon has infiltrated US critical infrastructure †
- The country's National Computer Virus Emergency Response Center called the claims a "political farce" orchestrated by US officials in a new report

† *https://www.bloomberg.com/news/articles/2024-10-15/chinese-cyber-agency-rejects-us-hacking-claims-in-new-report?sref=10lNAhZ9*

Cybersecurity and Reactions

- CISA and the European Commission (CRA and NIS2)
- TSA Directives were a call to action (2021 and 2022/2023/2024):
  - Ensure that user accounts are modified, deleted, or de-activated expeditiously for personnel who no longer require access or are no longer employed by the company
  - Ensure appropriate segregation of duties is in place
  - Change all default passwords for new software, hardware, etc., upon installation
  - Cybersecurity team and plan and that is tested (at least) annually
  - Pipeline Reference Architecture (PRA)
- Energy and Transportation Solutions responded by integrating additional security features that hardened our products; Defense in Depth
  - Securing the Products
  - Securing the Connection from field to main office/HQ

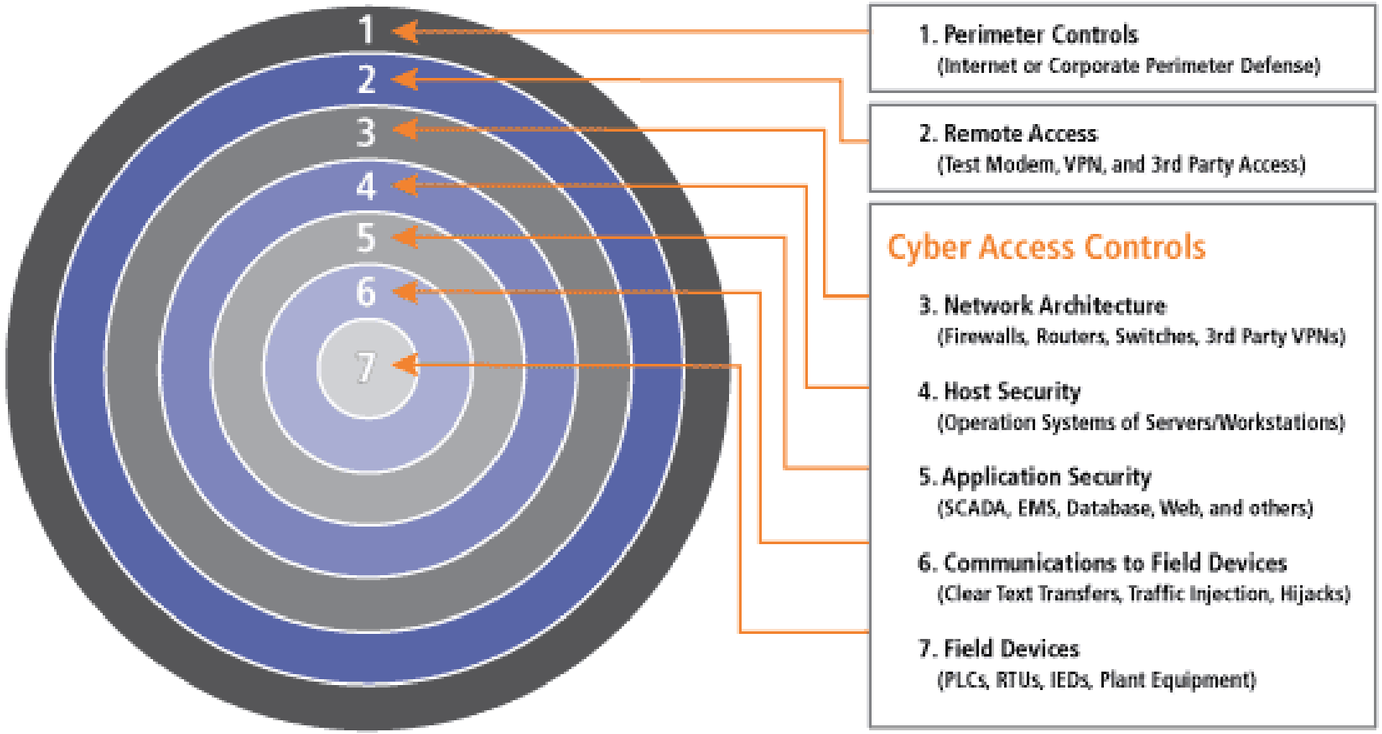


Defense in Depth

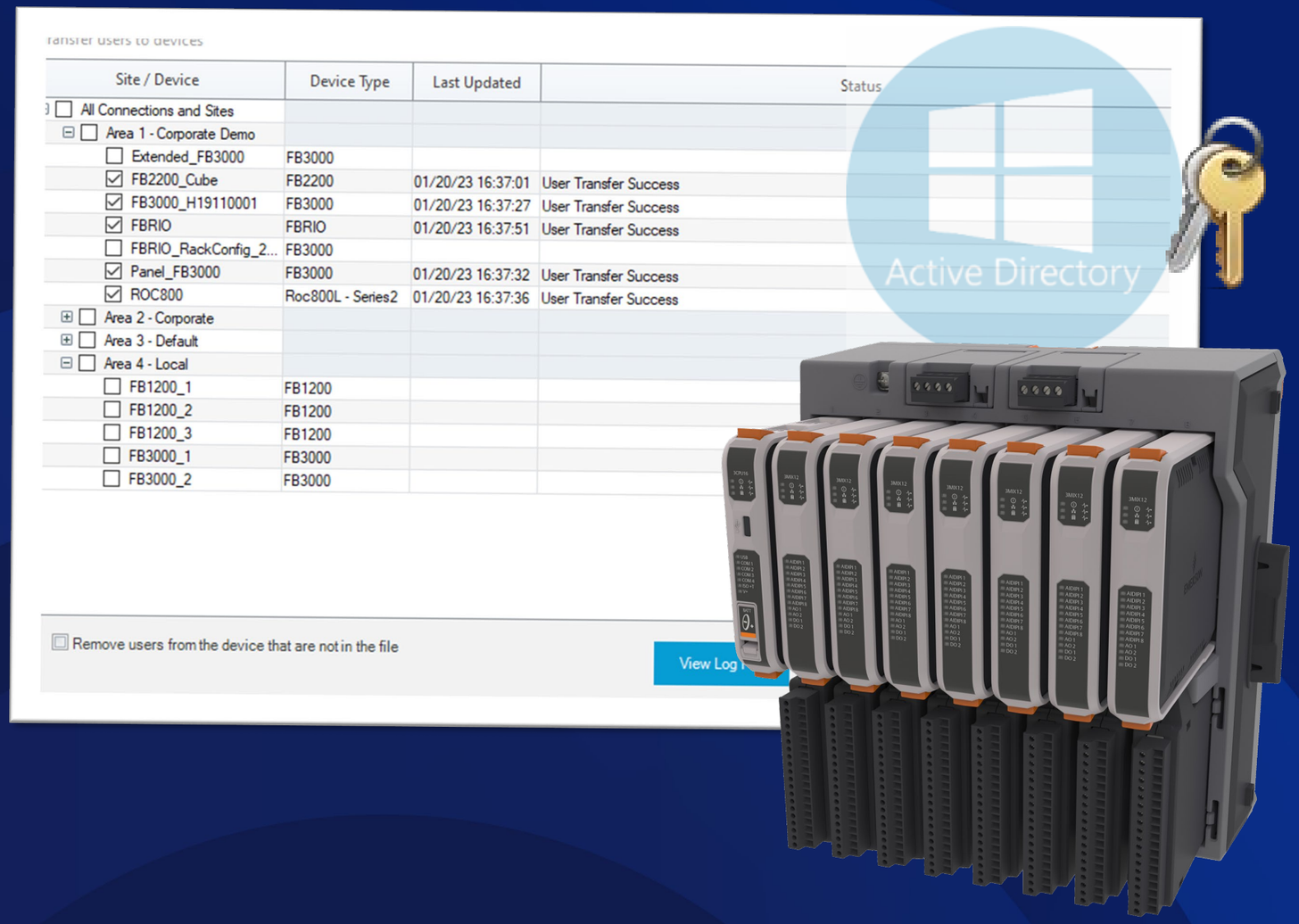
A strategy that leverages multiple security measures to protect an organization's assets

The thinking is that if one line of defense is compromised, additional layers exist as a backup to ensure that threats are stopped along the way

Defense in depth addresses the security vulnerabilities inherent not only with hardware and software but also with people



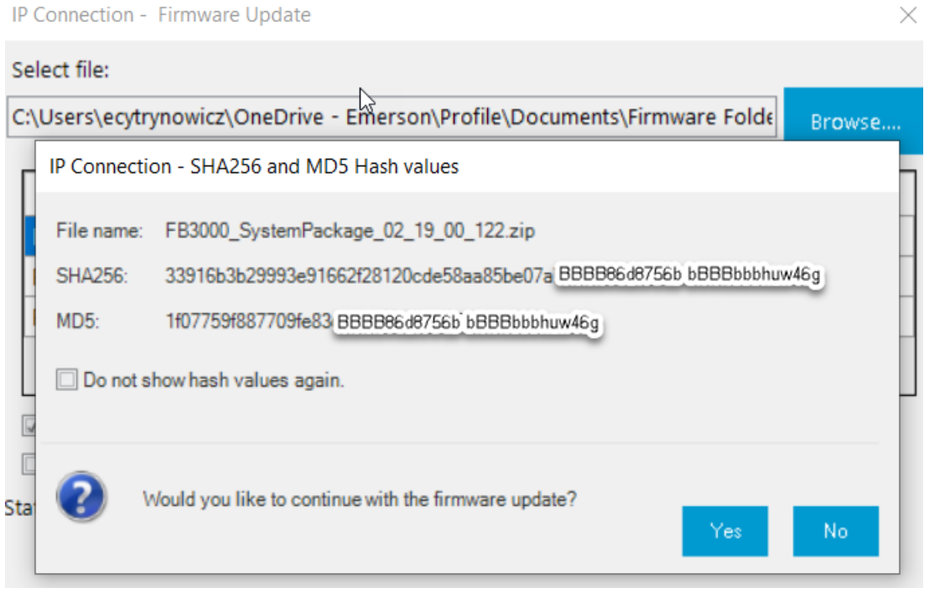
ETS have implemented several features that
when used together
give you a secure, easy-to-use environment
in the same way you are
protected in suit of armor



FB Automation Platform CyberSecurity Features

Securing the Product - FB Automation Platform

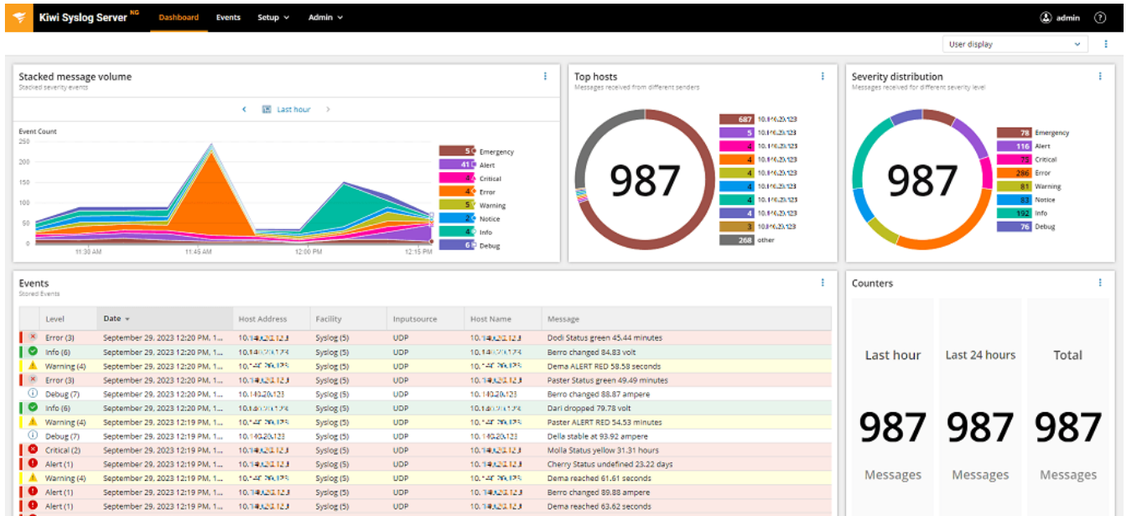
- Firmware (and all software) has published hashes in Guardian – used to manually confirm the product has not been compromised anywhere between Emerson development and the user
- The Firmware itself is also signed so compromised firmware cannot be installed or booted
- Firmware signature constantly monitored by the device – if compromised will revert to known good factory image



Securing the Product - FB Automation Platform

- Firmware (and all software) has published hashes in Guardian – used to manually confirm the product has not been compromised anywhere between Emerson development and the user
- The Firmware itself is also signed so compromised firmware cannot be installed or booted
- Firmware signature constantly monitored by the device – if compromised will revert to known good factory image
- SYSLOG support generates standard ‘security event’ messages received by SIEM servers
  - Event logging is a requirement of TSA, PRA and most security standards
  - Easily configured in FBxConnect (specify server, and types of events)

Multiple Layers of Security Protecting the device – Defense in Depth



Securing the Product - User Accounts and Roles

- “Tunnelling Security” is used by the firmware to identify individual users over DNP3 (unique to Emerson)
- Credentials exceed TSA Requirements (Complex, 30 char username/password, minimum password length, lockouts etc.)
- Role Based security – assign read/write access to areas of functionality and groups of users (Admins, Engineers, Techs etc.)
- Auditing logged to internal Alarm/Event logs; accessible via SCADA and FlowCal CFX
- Managed using Emerson Credential Management Tool
- Typically used by tools, local panels
- Supported by Beijer, RedLion and FBxConnect (only)

Securing the Product - User Accounts and Roles

- “Tunnelling Security” is used by the firmware to identify individual users over DNP3 (unique to Emerson)
- Credentials exceed TSA Requirements (Complex, 30 char username/password, minimum password length, Lockouts etc.)
- Role Based security – assign read/write access to areas of functionality and groups of users (Admins, Engineers, Techs etc.)
- Auditing logged to internal Alarm/Event logs; accessible via SCADA and FlowCal CFX
- Managed using Emerson Credential Management Tool
- Typically used by tools, local panels
- Supported by Beijer, RedLion and FBxConnect (only)

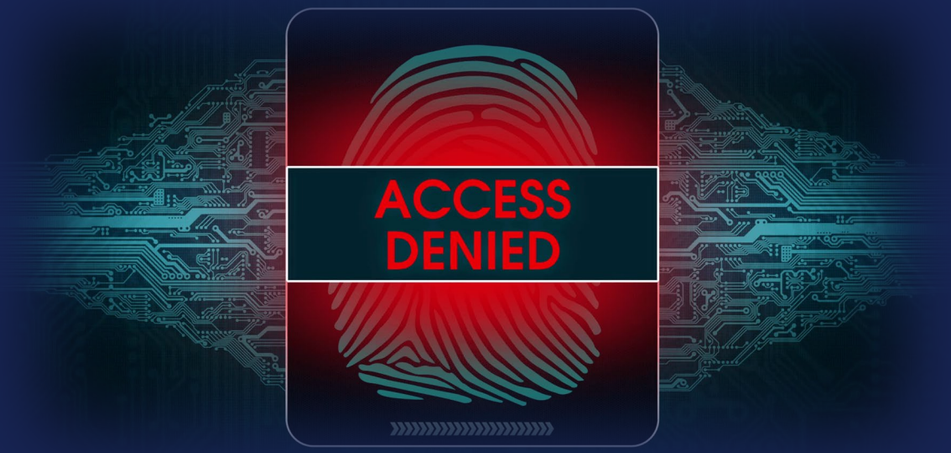
Ideal for customers with a small number of devices

Most large corporate customers & CyberSecurity specialists will recommend centralized, industry standard security

Can be a challenge managing the accounts

Securing the Product - DNP3 Secure Authentication v5 (SAv5)

- Every device has a unique update key (user provided) installed
- ‘Critical’ actions are individually authenticated
- Prevents introduction of malware, compromised or unauthorized devices/software into the network
- ‘Session’ keys changed every few minutes to protect against longer term monitoring
- Network Monitoring/Analysis/Intrusion detection is still possible with standard tools
- Emerson Key Management tools allow keys to be installed and managed in a controlled environment
- Technicians can also be authorized to install keys from encrypted files
- FB3000 RTU, FB2000 Series, FB1000Series Flow Computers and ControlWave support DNP3 SAv5



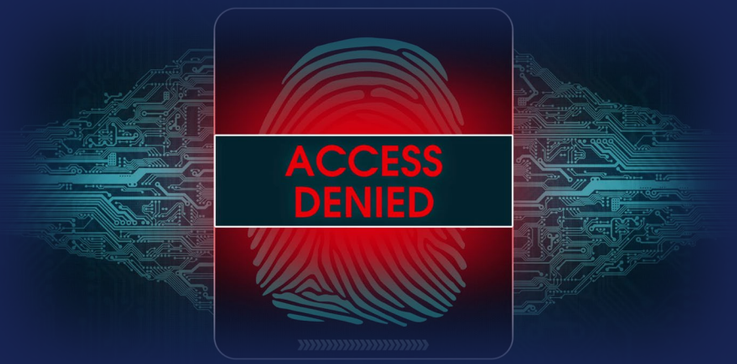
Securing the Product - DNP3 Secure Authentication v5 (SAv5)

- Every device has a unique update (user provided) key installed
- ‘Critical’ actions are individually authenticated
- Prevents introduction of malware, compromised or unauthorized devices/software into the network
- ‘Session’ keys changed every few minutes to protect against longer term monitoring
- Network Monitoring/Analysis/Intrusion detection is still possible with standard tools
- Emerson Key Management tools allow keys to be installed and managed in a controlled environment
- Technicians can also be authorized to install keys from encrypted files
- FB3000 RTU, FB2000 Series, FB1000Series Flow Computers and ControlWave support DNP3 SAv5

DNP3 SAv5 is a widely used, open standard with no known significant vulnerabilities

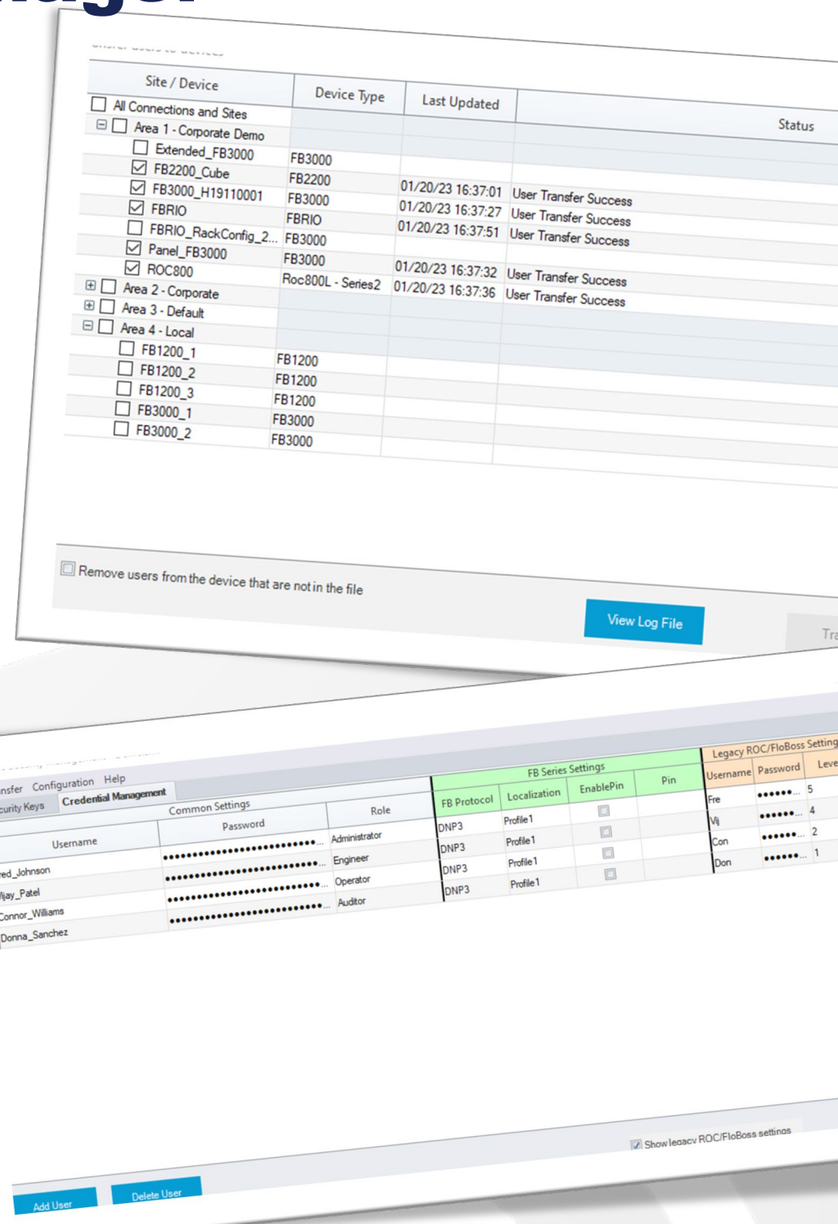
Used for over a decade on NIST, NERC certified electrical SCADA

It authenticates DEVICES not people….



Securing the Connection - Credential Manager

- Centralized Security reduces management costs to meet TSA Requirements
- Manages credentials for Emerson RTUs and Flow Computers
- ControlWave, ROC, FB107 and FB3000 Support
- Add/Remove Users from Multiple devices Remotely
- Change Roles Remotely
- Change Credentials for users remotely
- Bulk Edit credentials across all remote devices or groups (and device types)
- Credentials/Configuration Securely Saved locally (for backup)
- Requires DeltaV™ FBxConnect with additional registered license (protects against unauthorized use)
- Logs security changes
- Manage and backup DNP3 Security Keys



Securing the Connection - Credential Manager

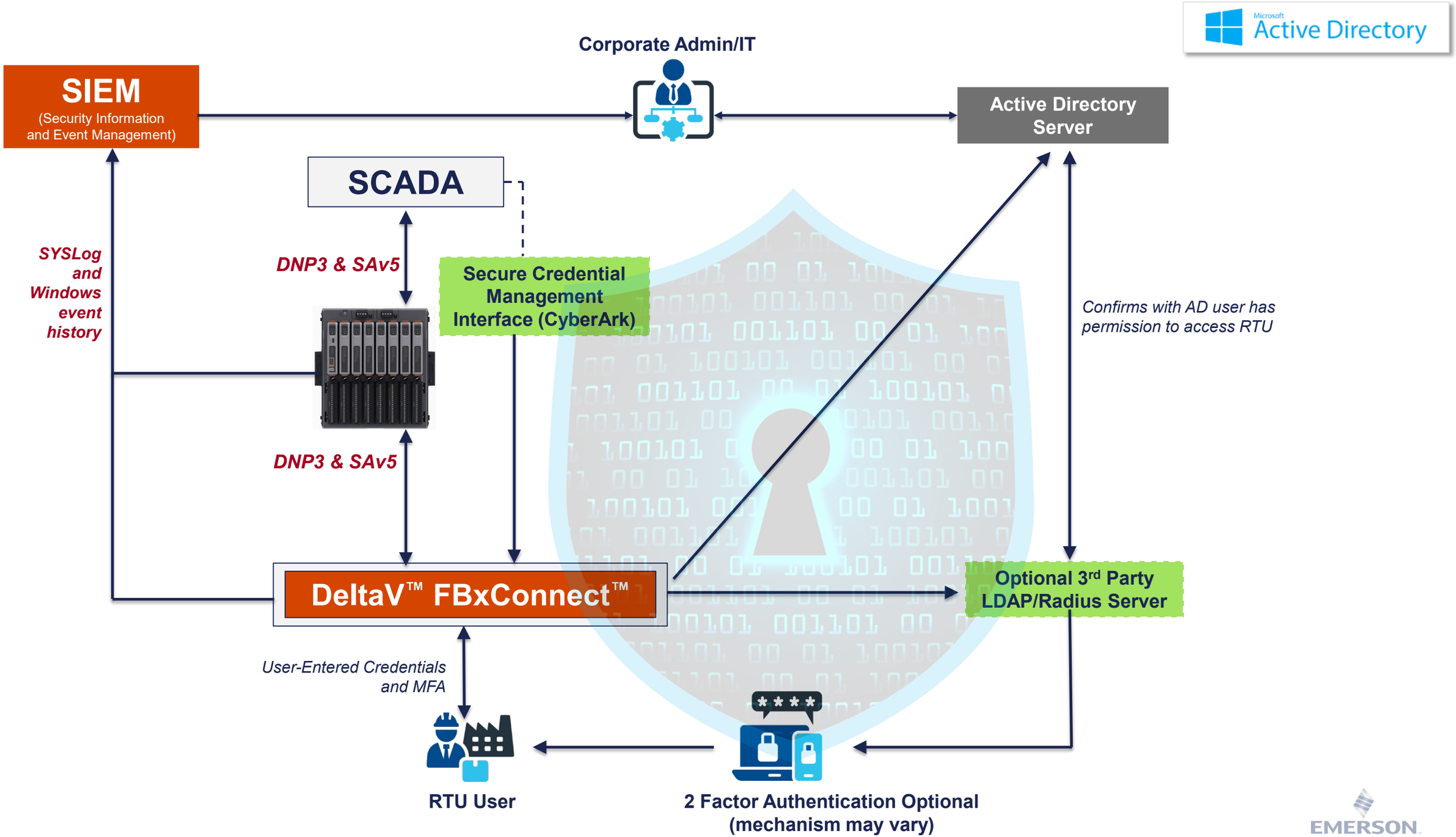
- Centralized Security reduces management costs to meet TSA Requirements
- Manages Credentials for Emerson RTUs and Flow Computers
- ControlWave, ROC, FB107 and FB3000 Support
- Add/Remove Users from Multiple devices Remotely
- Change Roles Remotely
- Change Credentials for users remotely
- Bulk Edit credentials across all remote devices or groups (and device types)
- Credentials/Configuration Securely Saved locally (for backup)
- Requires DeltaV™ FBxConnect with additional registered license (protects against unauthorized use)
- Logs security changes
- Manage and backup DNP3 Security Keys

Ideal for small/midsize customers

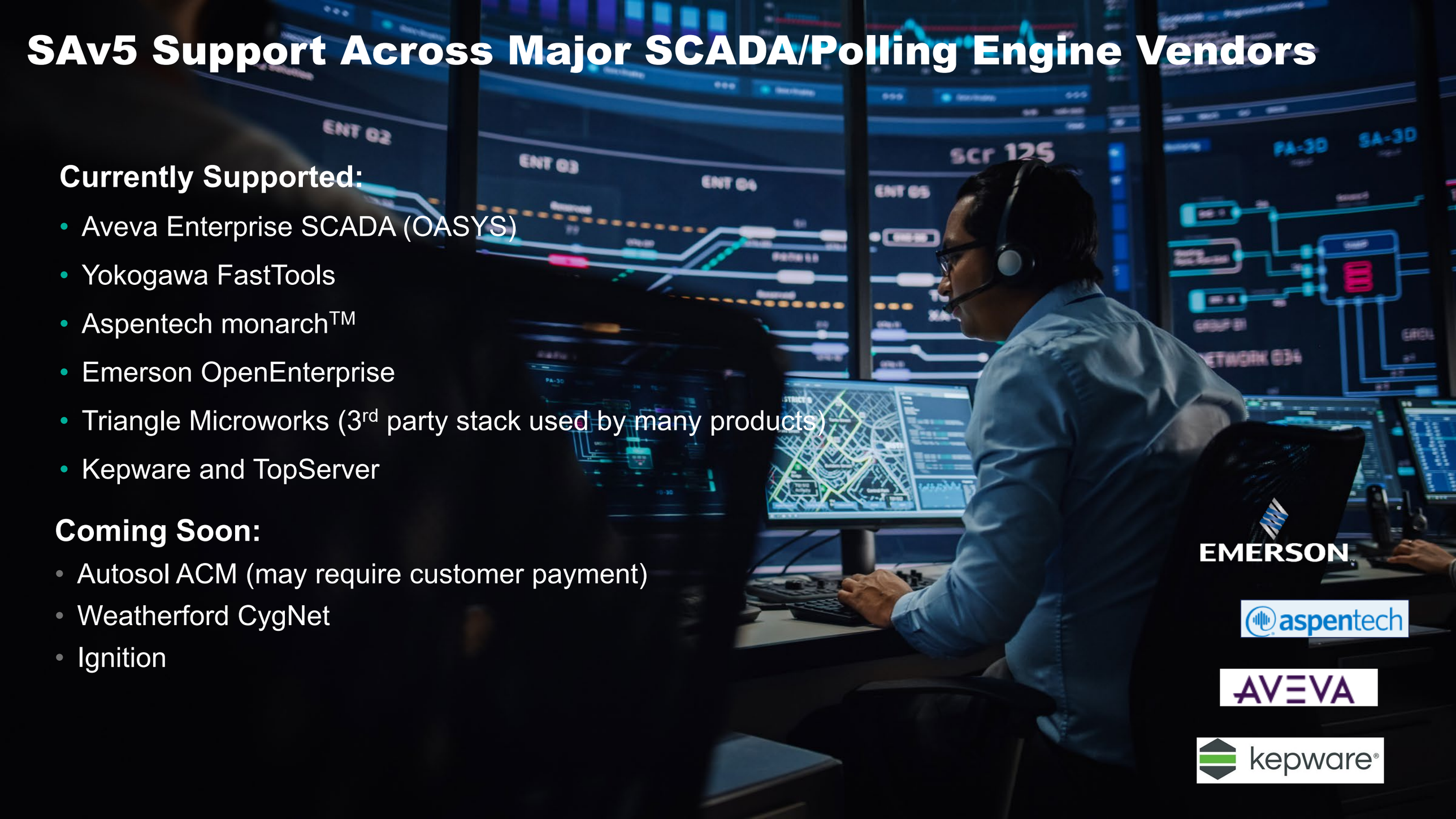
Larger customer may look to integrate into corporate security

Securing the Connection - Active Directory

- Extend corporate credentialing beyond the office walls and out into the field
  - Operations Technology (OT) can more easily sync up with Information Technology (IT)
  - Field Techs can use the same logins on RTUs and Flow Computers that they use for network access
  - Easier access on Field Devices for more efficient workflows
  - Allows IT controls of user access
  - Makes compliance with TSA regulations easier
  - Supports automation roles



SAv5 Support Across Major SCADA/Polling Engine Vendors



Currently Supported:

- Aveva Enterprise SCADA (OASYS)
- Yokogawa FastTools
- Aspentech monarch™
- Emerson OpenEnterprise
- Triangle Microworks (3rd party stack used by many products)
- Kepware and TopServer

Coming Soon:

- Autosol ACM (may require customer payment)
- Weatherford CygNet
- Ignition

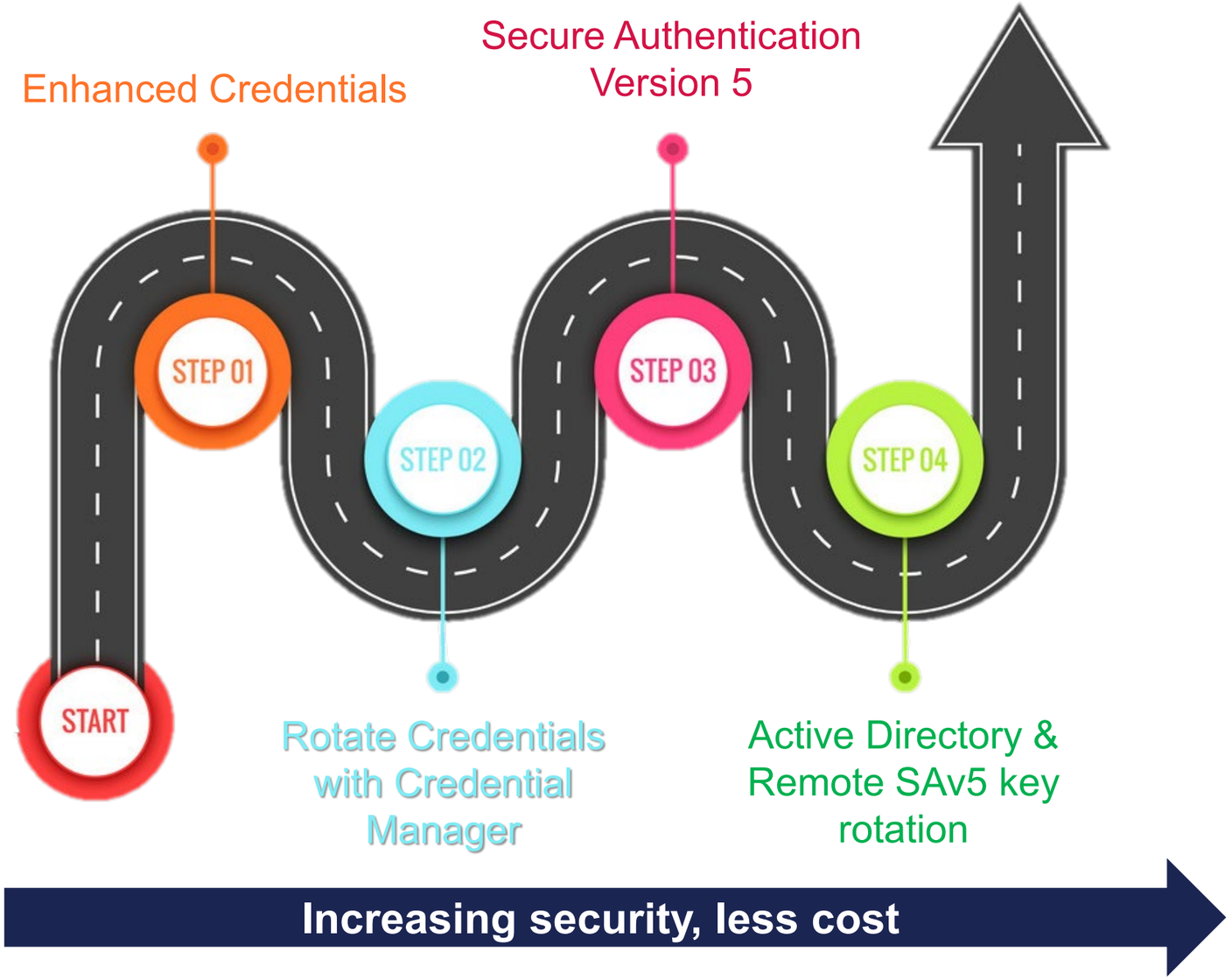
EMERSON

aspentech

AVEVA

kepware

Effective Cybersecurity is a Journey …



ETS understands that you may need to learn and upgrade security in steps, and we can support you each step of the way

Results

- Major Gas distributor/pipeline operator with over 6000 field devices
- TSA Compliance on legacy devices requires visits to each field device every 30 days. This solution completely removes those visits
  - *Handled centrally and automatically*
  - *Reduction in manpower and $ and an Increase in security*
- If an employee leaves organization, their access to all devices can be removed at a click of button
  - *Previously all 6000 devices would need to be re-configured*
- Standardized technology (AD, LDAPS, CyberArk) is overlap with common IT practices, reducing cost compared to proprietary solutions
- Syslog provides independent validation/reporting of security events across the OT network, matching visibility traditionally only available within IT systems
- DNP3 SAv5 gives the maximum interoperability between different vendors' equipment
  - *Specifically designed for challenging (low bandwidth, lack of uptime, etc) WAN involved in O&G SCADA*

EMERSON EXCHANGE 2025
ACCELERATING INNOVATION

Thank You

Booth 250