Kaspersky Industrial Cybersecurity Conference 2024

SUPCON

The Practice of ICS Cybersecurity in the Fusing Age of IT/OT

Supcon Technology Co., Ltd
Yu Mengda
Oct. 2024

kaspersky

Kaspersky Industrial Cybersecurity Conference 2024

SUPCON

Supcon Technology，Yu Mengda

Position Title:
Senior engineer, SUPCON Industrial CyberSecurity Business Manager. (SPDT Director, General Manager of Industrial Cyberecurity Product Dept.)
Deputy General Manager of Zhejiang Guoli Security.

kaspersky

Cybersecurity in Overseas Petrochemical Industries

Saudi Aramco & SUPCON

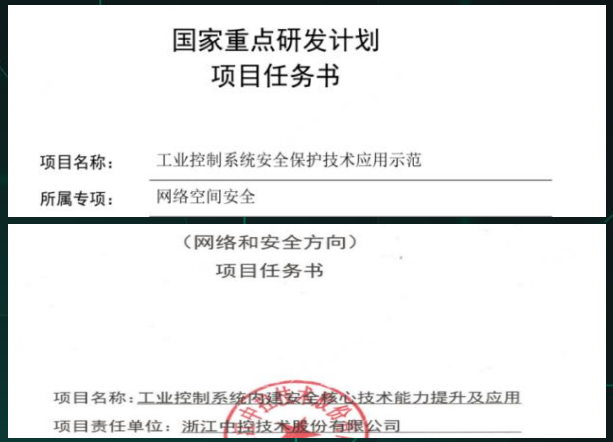
ATG & SUPCON

IMI & SUPCON

3-level Industrial Security Operations Solution

Built-in Security Control System in Large Refineries

Industrial Cybersecurity Research Program



国家重点研发计划
项目任务书

项目名称： 工业控制系统安全保护技术应用示范

所属专项： 网络空间安全

（网络和安全方向）
项目任务书

项目名称：工业控制系统内建安全核心技术能力提升及应用

项目责任单位：浙江中控技术股份有限公司

Application of Data Security in Petrochemical Industry

NG Secure Control System

Zero Trust Architect

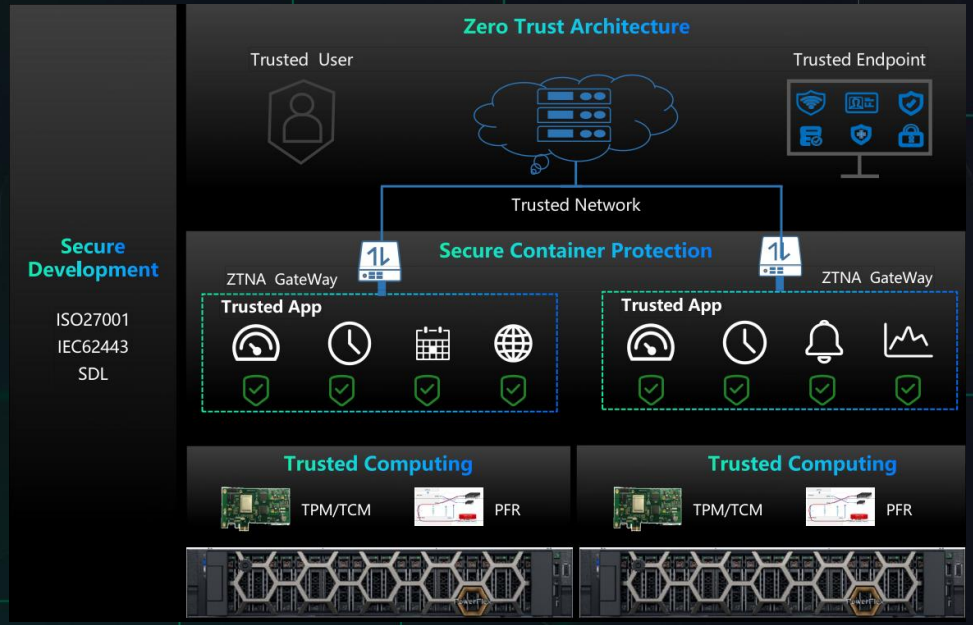
- Access Control Based on IAM
- Verify continuously & Dynamic policy
- End-to-end Encryption

Secure Container Protection

- Image signing and trust booting
- Micro-segmentation between Containers
- Vulnerability Scan

Software Defined Security

- Virtualization Security Resource Pool
- Distribution on demand and unified control



Nyx - 1st Universal Control System

As the "Gate" for computer to enter industrial control system for maintenance, the entire maintenance operation is safely controlled.

Untrusted Zone

O&M Personnel

- Enterprise technicians
- Technicians of manufacturers
- Classified protection evaluators
- Superior inspectors

USB Key

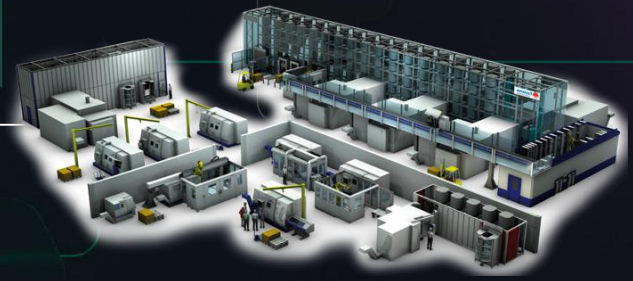
Operate and maintain computers

- Outreach checks
- Peripheral checks
- Screen recording

Security O&M Terminal

- Attack interception
- Malicious code checking
- High-risk command interception
- Access control
- Process audits
- Secondary Licensing

Trusted Zone



Objects to be operated and maintained

Industrial Assets Monitoring and Management

Assets Discovery
- **Category** (Upper Computer, Switch, Controller, etc)
- **Information** (Hardware, Software Version, Fault Information)

Status Monitoring
- **Running Status** (Controller, Network Device, Security Device, Configuration)
- **Risk Identification**

Baseline Verification
- **Assets** (Configuration Baseline, Device Baseline, Security Baseline)
- **Network**

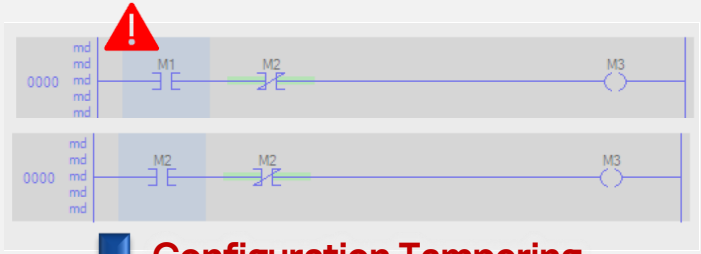
Unclear assets status → Database → Discover → Analyze → Monitor → Diaplay → **Clear assets status**

Controller Monitoring & Recovery

Professionally identify controller risks, **restore baseline configuration** without disruption

Identify attack specifically targeting the controller and block them, protect controller without affecting production.

Control Behavior



Configuration Tampering Monitoring

Baseline File Restore

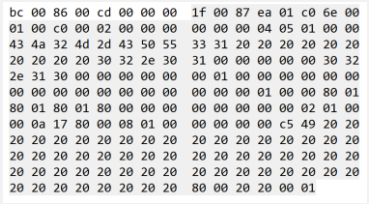
Multiple serious vulnerabilities

Controller

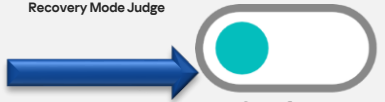
Patch affects system operation
Dare not install patches

Baseline Configuration Project

Reverse restore and mapping



Recovery Mode Judge

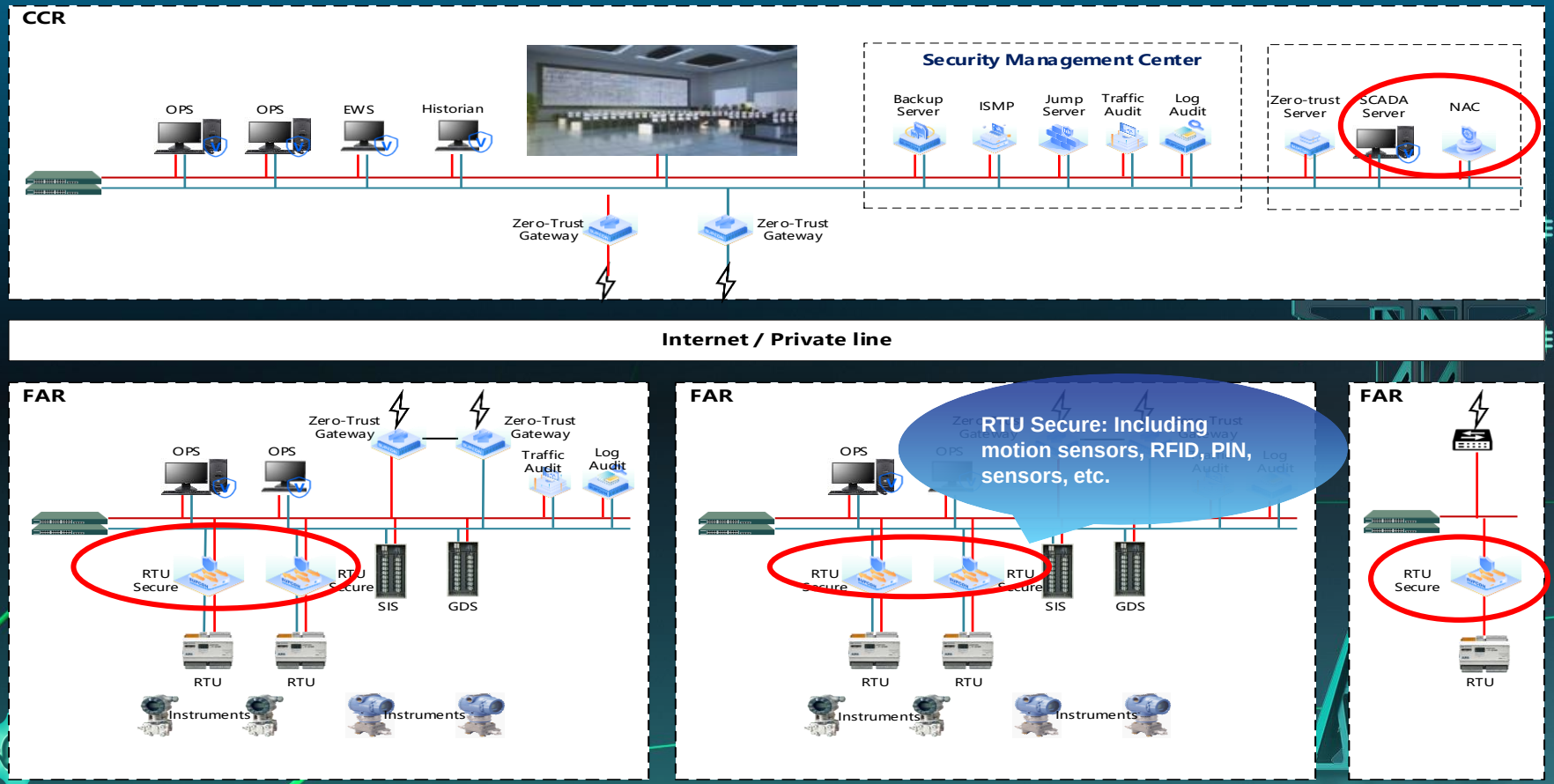


Enable Configuration Recovery Module

Controller Attack Prevetion

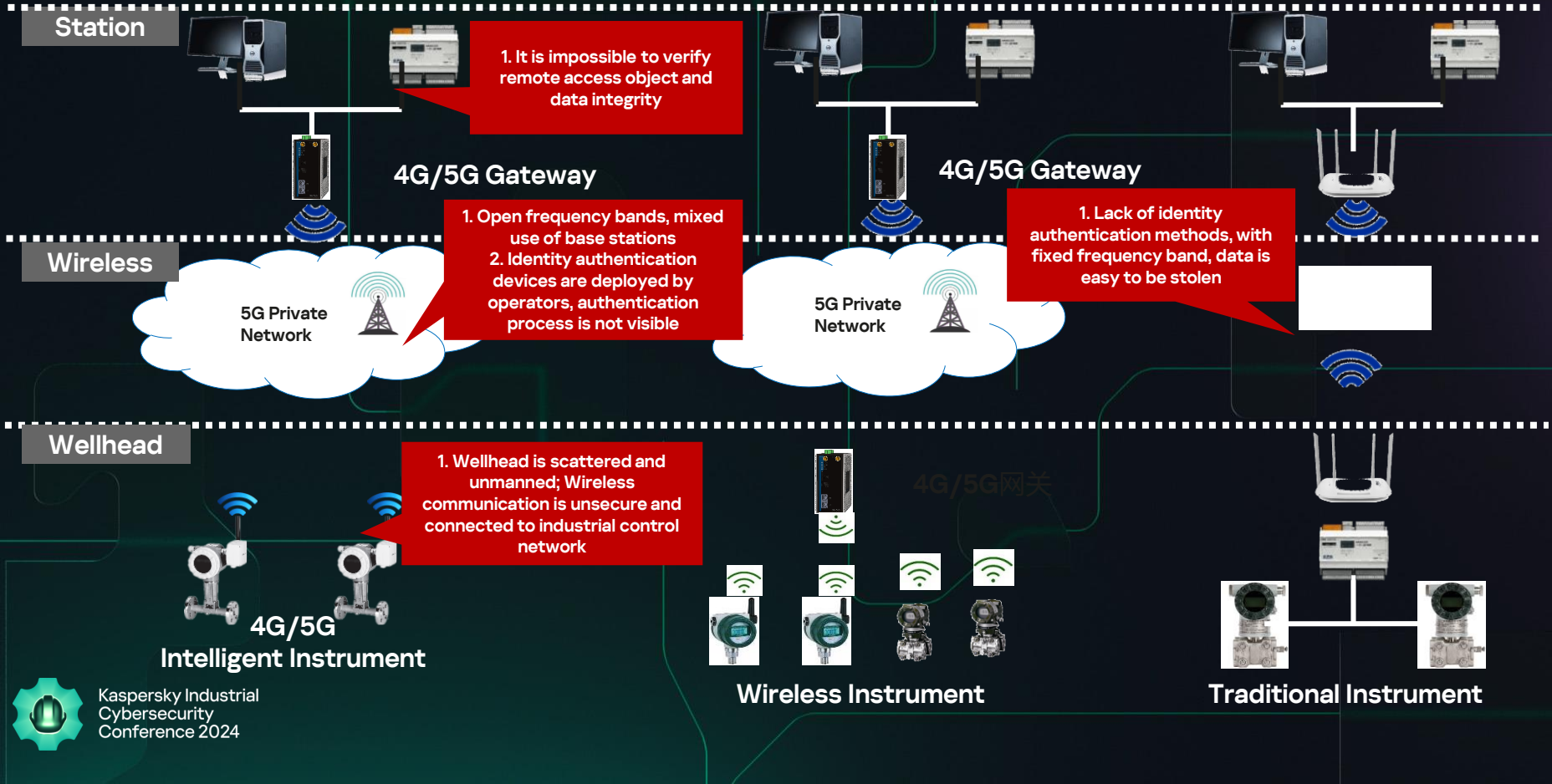
Controller Monitoring and Recovery

Rockwell Automation · GE · Mitsubishi Electric · ABB · SIEMENS · Honeywell · Emerson · YOKOGAWA · Schneider Electric


CCR
OPS
OPS
EWS
Historian
Security Management Center
Backup Server
ISMP
Jump Server
Traffic Audit
Log Audit
Zero-trust Server
SCADA Server
NAC
Zero-Trust Gateway
Zero-Trust Gateway
Internet / Private line
FAR
Zero-Trust Gateway
Zero-Trust Gateway
OPS
OPS
Traffic Audit
Log Audit
RTU Secure
RTU Secure
SIS
GDS
RTU
RTU
Instruments
Instruments
FAR
RTU Secure: Including motion sensors, RFID, PIN, sensors, etc.
OPS
RTU Secure
RTU Secure
SIS
GDS
RTU
RTU
Instruments
Instruments
FAR
RTU Secure
RTU

Common Wireless Communication in Oilfield Wells

SUPCON



Kaspersky Industrial Cybersecurity Conference 2024

Cooperation with Kaspersky in ICS Security: Removable Media Protection & Secure Data Ferry

NG USB Guard (Kaspersky inside)

Whitelist & Antivirus Protection

- Both whitelist and antivirus techniques
- World-leading anti-virus engines —— Kaspersky
- Provides a detection rate of over 99.9% for known malicious code

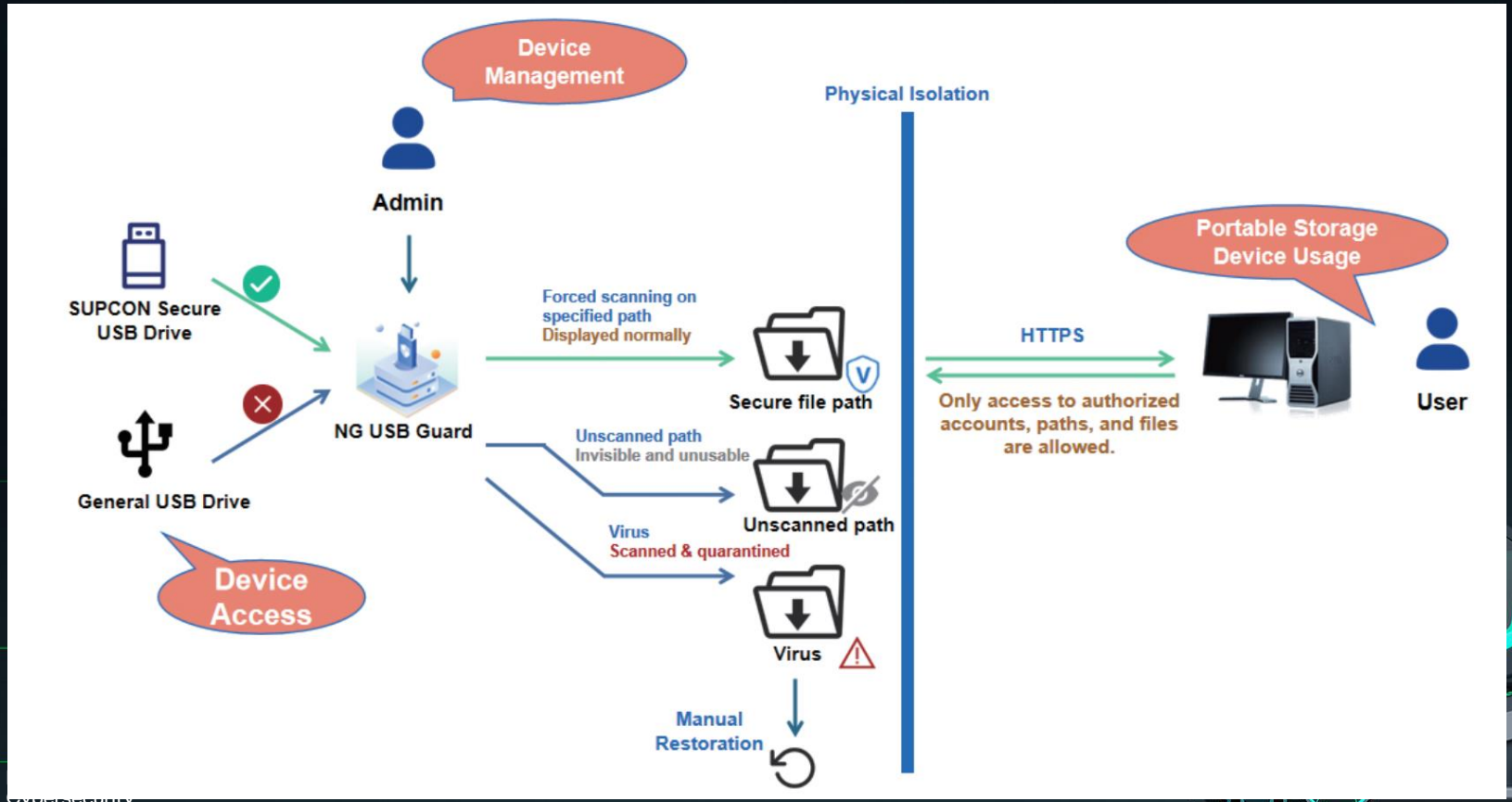
Secure Automatic AV Update

- Automatic online antivirus updates on IT (information technology) networks
- Automatic offline antivirus updates on OT (operational technology) networks with SUPCON Secure USB Drives
- Issues antivirus database updates to VxDefenders across the whole domain

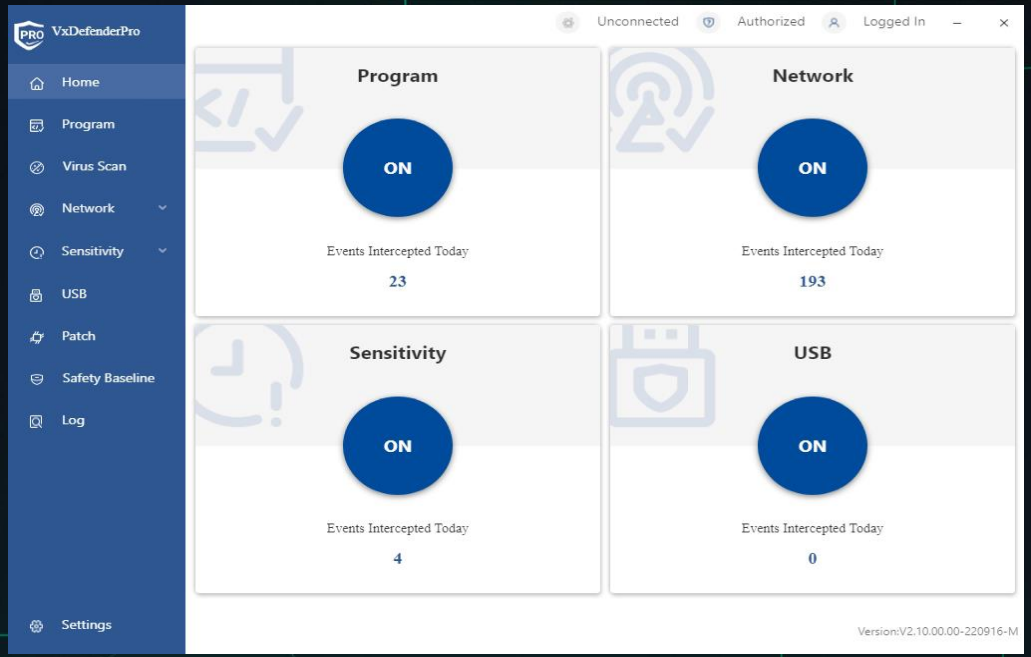
Comprehensive Management and Audit

- Allows for easy user management through Windows Active Directory domains and supports synchronization of AD users;
- Provides security management features such as storage device binding, user authorization management, and user behavior monitoring;
- Multiple security audits —— time, user, operation, path, target file, and device ID, etc.

Removable Media Protection & Secure Data Ferry



Host Security: VxDefenderPro



VxDefenderPro (Kaspersky AV)

kaspersky

Whitelist & Antivirus Protection

- Both whitelist and antivirus techniques
- World-leading anti-virus engine —— Kaspersky
- Provides a detection rate of over 99.9% for known malicious code

Security Baseline

- Enable security baselines with one-click using common and custom rules that involve system configuration, account and log management
- Provides support for the configuration of all commonly industrial hosts

Centralized management

- Unified deployment of functional configuration
- Patch management of computer hosts
- Group immunity technology for host viruses

“1+1+2” Three-level Operations

SUPCON

Thank You!

Supcon Technology

Yu MengDa

SPDT Director

www.supcon.com

kaspersky