



Centralized Asset Inventory Management Solution

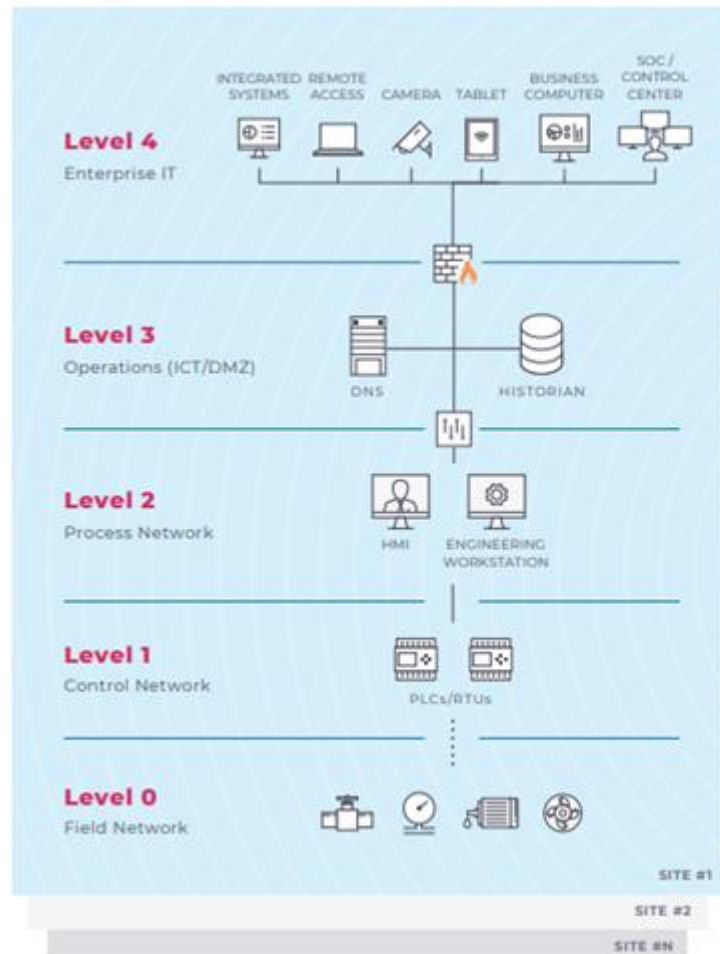
Data Sheet

“You Can’t Secure What You Can’t See”

Today, all asset discovery is done automatically, and the resulting data can be searched and analyzed easily. What asset management really does is to give you a ton of valuable data about your OT infrastructure that makes it much more easy to maintain, protect, and troubleshoot your systems.

The secret to a successful operational technology (OT) cyber security program is **real-time, automated asset inventory management**.

Deployment Architecture - Purdue Model Example



Patch Management



Asset Management



Site Assessment



HTTPS

- IEC61850
- SNMP
- WMI/WinRM
- Modbus, etc.



System Requirement

- Windows 10 & above
- Windows Server 2012 R2 & above
- Disk Space 1GB
- Dual Core Processor

The Industrial Cybersecurity Challenge

Most of the existing solutions use Passive scanning to collect the Asset information. There are some technical limitations to this approach. Silent devices will not be detected, software applications and security patches won't be detected with any reasonable level of accuracy.

SyskeyOT Asset Dashboard was created to help IT and OT teams to overcome this challenge.

SyskeyOT Asset Dashboard

– a Centralized Asset Inventory Management Solution

Scan. Collect. Store. Compare. Alert. Forward

- Monitors the OT/ICS Assets, Document the Asset details and Feeds the Input to Patch update center.
- Collects asset information by using various standard industrial protocols like **IEC61850, SNMP, WMI/WinRM,etc.**
- Forwards consolidated Asset information collected locally to Patch update center with secured connection.

Key Features & Capabilities



Discovers the Available Resources

Discover assets within given IP range and by adding manually



Intuitive Dashboards

Generates macro views as well as detailed information on assets



Create/Custom/Assign Templates

to fetch various data parameters of heterogenous devices



Audit Trails - Syslog RFC5424

Support Syslog protocol to send logs/Audit Trails to Syslog server over RFC5424.



SSO Authentication – RBAC/AD

The system supports active directory SSO login and local user management functionality



Scanning of Devices

Scans Periodically/Manually, Collects/Assigns parameters to device Templates



Collects through **IEC61850(Edition1 and 2), SNMP(V2 and V3), WMI/WinRM, etc.**



Storing/Exporting Asset Information reports

as .XML/.CSV files and also through "API" **Forwarding** to patch update centre over secured connection



Historical Comparison & Alerts

- Compares / Detects changes with reference to History/Baseline
- Rule based Alerts upon change detection



Key Benefits

- Automates Detection & Investigation
- Finds Unauthorized Devices
- Leaves an Audit Trail
- Increases Asset Info Accuracy
- Saves Time



Key Values

- Cost Effective
- Perpetual Validity
- Standard 3yrs Support
- Unlimited Assets & Nodes
- Customize on Demand
- Extended Protocols Support

About Syskey Softlabs

An emerging Software Development firm from India, offering Cybersecurity products/solutions for Operation Technology/Industrial Control Systems (OT/ICS) networks.

Syskey helps the businesses with customized software products for tasks such as obtaining data to help identify security breaches, comply and maintaining the security level of the highest standards within the organization.

Reach us at

sales@syskeysoftlabs.com

support@syskeysoftlabs.com

USA & Canada

464, Sunnyvale, USA

Southeast & MEA

#19 tower B, PSR Aster, Chambenahalli,
Sarjapura Road, Bangalore- 562125, India.