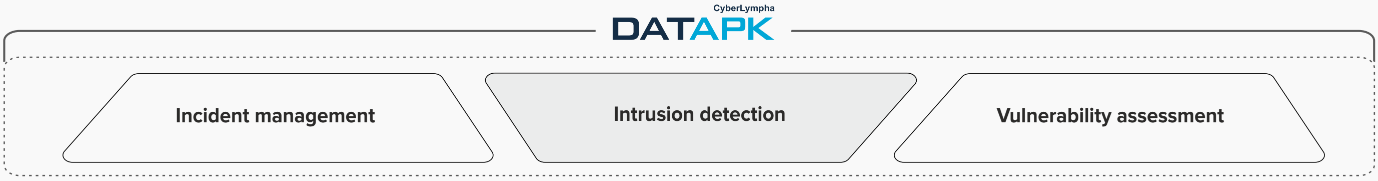
CyberLympha®

CL DATAPK Datasheet

info@sg.cyberlympha.com **cyberlympha.com**

CyberLympha DATAPK

Comprehensive security monitoring solution for industrial control and automation systems, Internet of Things (IoT) and Industrial Internet of Things (IIoT)



- Designed & developed for protecting the OT
- Multiple solution classes united in one product with a single interface
- Deployed on critical infrastructure sites
- Compliance tested with major ICS vendors

CL DATAPK HELPS COMPANIES

- Address multiple tasks with the unified solution designed for industrial enterprises
- Lower direct and indirect costs associated with OT security
- Optimize security management in the enterprise ICS, OT and IoT segments
- Streamline security personnel training
- Automate compliance status verification

100+
Enterprise Customers

150+
Projects completed

1500+
Units deployed

CL DATAPK PROVIDES

- Enhanced visibility across the OT infrastructure
- Automated network nodes detection
- Asset configuration management
- Network interactions and traffic flows detection
- Constant asset security audit:
- Vulnerable protocols detection
- Suspicious network activity detection and analysis
- Detection of traffic exchange with external networks and/or Internet
- Compliance status control for governmental and corporate policies
- Quick and precise attack detection
- Incident generation based on collecting and correlating events from different sources
- Security state deviation detection

OPTIONAL CL DATAPK MODULES

Automated type detection for nodes and traffic flows, based on machine learning algorithms

Automated anomaly detection based on AI/ML technology stack

TECH FEATURES

NETWORK TRAFFIC ANALYSIS

- Non-invasive data acquisition via SPAN or mirroring ports in the network
- Visual maps of network topology and traffic exchange
- Node detection and inventory management
- Illegitimate connections and data flows detection

CONFIGURATIONS MANAGEMENT

- Configuration security status and compliance control
- Agentless data acquisition from arbitrary sources
- Support for new asset types without product
- code modification

INCIDENT DETECTION

- Incident detection based on expert rules
- Agentless data acquisition from arbitrary sources
- Support for new asset types without product code modification

VULNERABILITY MANAGEMENT

- Agentless vulnerability assessment for arbitrary assets
- OVAL-based vulnerability databases
- Automated report generation

OPERATION MODES

OBSERVATION MODE

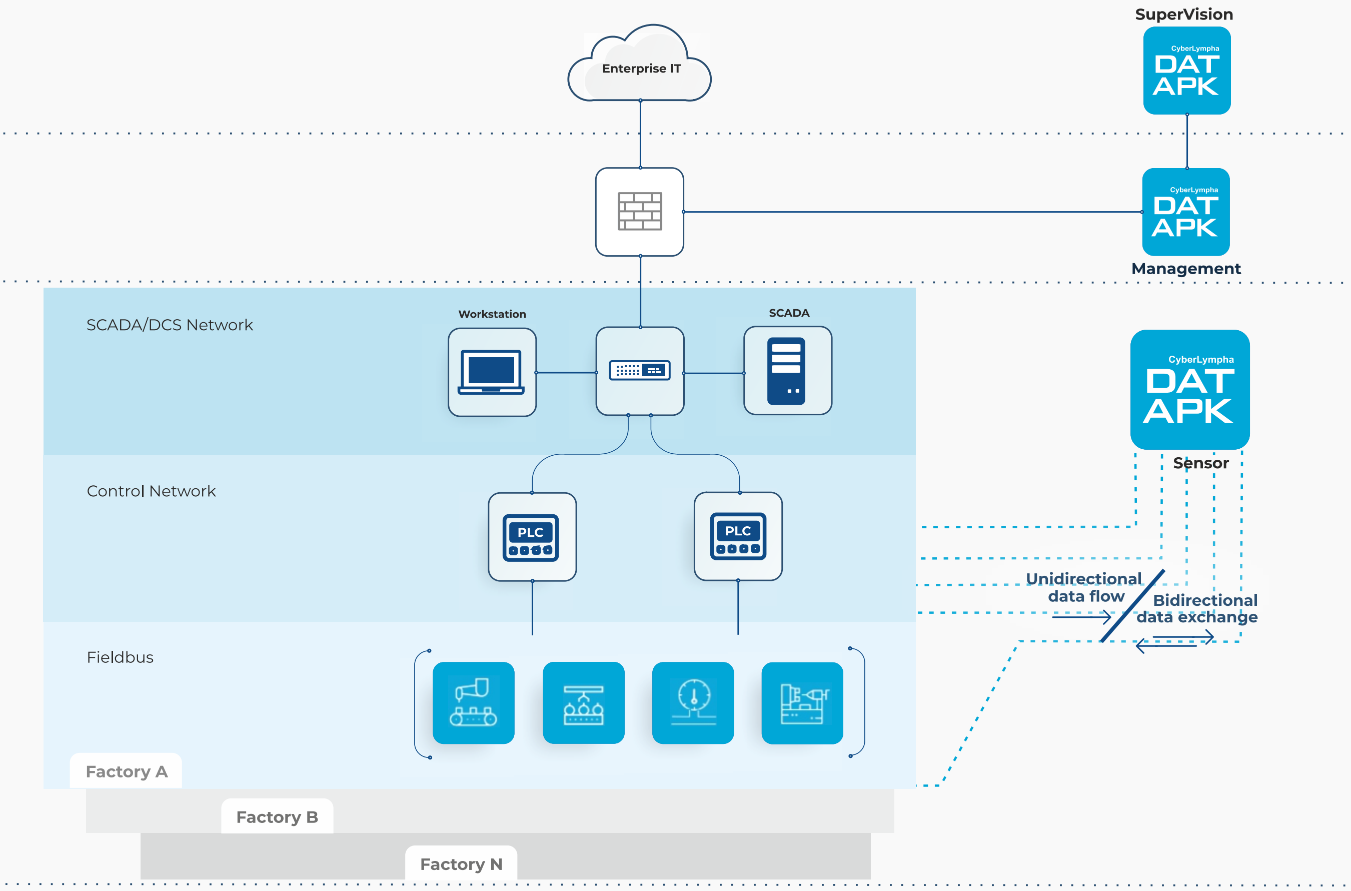
- Unidirectional traffic flow
- Network traffic and events processing

QUERY MODE

- Bidirectional traffic exchange with the protected assets
- Asset configurations and events processing

Functionality	Observation mode	Query mode
Security events collection	Partial	Yes
Attack detection	Yes	Yes
Network anomalies detection	Yes	Yes
Configurations management	No	Yes
Asset inventory	Yes	Yes
Asset modification detection	Yes	Yes
Vulnerability assessment	Partial	Yes

DATAPK ARCHITECTURE



SOLUTION ARCHITECTURE

CL DATAPK Sensor

- ICS assets detection
- ICS data flows detection
- Network-based attacks detection
- Protocol-specific commands and parameters detection and validation
- Security events collection, registration and pre-processing
- Asset configurations and inventory information collection

CL DATAPK Management

- Data collection from the underlying CL DATAPK Sensors
- Asset catalogue and data flows management
- Automated topology visualization based on detected data flows
- Asset configurations management and compliance control
- Security assessments and status control for compliance with the implemented security policy
- Security events processing and management
- Security incident generation based on correlation of the events received from multiple sources
- Alerts via email service and SCADA integration

CL DATAPK SuperVision

- Enterprise-level asset security status visualization based on the data collected from all underlying CL DATAPK Sensor and Management instances
- Enterprise-level security incident reporting
- Centralized management for the deployed CL DATAPK hierarchy
- Centralized update management for the CL DATAPK expert packages and software
- Integration with adjacent security solutions

PARAMETER	CL DATAPK		
	SENSOR	MANAGEMENT	SUPERVISION
Software specs			
Installation on a virtual machine	Yes		
Virtualization support	VMWare, HyperV, KVM, other virtualization engines support available upon request		
Base operating system	CentOS 7.6 and up, RHEL 6.5 and up, other Linux distributions support available upon request		
Hardware specs			
General note	Rugged appliance recommended	Standard rack server or virtual machine	
CPU	Intel Core i7 (4+ cores, with 3.2 GHz minimum frequency)	Intel Xeon (8+ cores, with 2.5 GHz minimum frequency)	
RAM	32 GB	64 GB	
Disk	512 GB SSD	2 x 960 GB SSD RAID1	4 x 960 GB SSD RAID10
Network	6 x 100/1000 Ethernet, extendable recommended	2 x 1G, 2x10/100 Ethernet	2 x 1G
Virtual machine specs			
vCPU	4 (3.2 GHz minimum frequency)	8 (2.5 GHz minimum frequency)	
RAM	32 GB	64 GB	
Disk	512 GB	2x960 GB	4x960 GB
Network	6 x 100/1000 adapters	2 x 1G adapters 2x 10/100 adapters	2 x 1G adapters