End-to-end digital services based on trusted data: value for business, search methods, and typical architecture

aprotech

Powered by KasperskyOS

aprotech Powered by KasperskyOS KasperskyOS

End-to-end digital services for an enterprise

The main value in connecting equipment to cloud-based and local IT systems (platforms) is the capability to create new digital services that not only let you remotely track the operation of equipment, but also provide your business with new models of interaction with partners and customers. However, it is important to understand that these services do not replace existing applications related to real-time enterprise management, such as ICS or SCADA. Instead, they provide additional tools that are either unavailable in most systems or too expensive and difficult to implement.

By using cloud technologies, you can access the latest industrial innovations and services from various enterprise digitalization strategies of the Industry 4.0 concept. A cloud platform is not just a tool for accumulating information. It also provides a wide range of tools for creating applications to manage equipment and evaluate its effectiveness, and provides additional capabilities for integration with external partners and systems.

A crucial data transfer component of connections to these platforms is **Kaspersky IoT Secure Gateway (KISG) 100**, a Cyber Immune data gateway based on the KasperskyOS operating system and designed for the industrial internet of things (IIoT). It ensures the security of connected equipment and protects any transmitted information from being compromised.

For end-to-end digital services, the company Aprotech provides a connection to the Siemens MindSphere digital platform in which you can use the following three different types of services:

- Basic – services provided by the Siemens MindSphere platform to all customers without additional payment (one example is FleetManager);
- Professional – industrial solutions for a specialized field (for example, a service for Overall Equipment Effectiveness, or OEE monitor);
- Custom development – turnkey applications tailored to a specific customer and integrated with other platforms or ERP systems (for example, 1C).

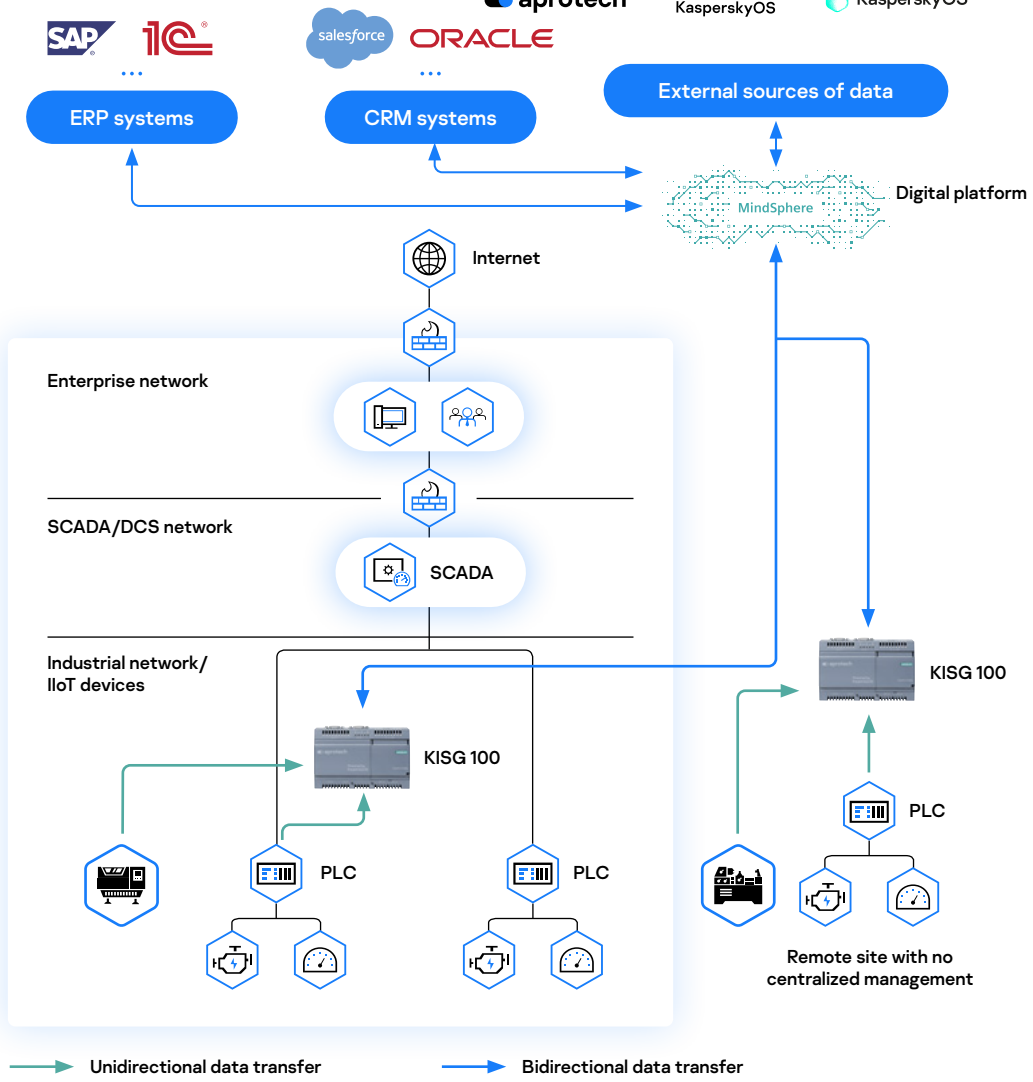
Preconfigured services based on the MindSphere IIoT platform are prepared for quick startup and primary analytics of industrial data.

«Industrial digitalization enables substantial savings on expenses (3.2% reduction per year) and higher revenues (increase by 2.7% per year)»

Source: PwC report – Global Digital Operations Study (2018)

In partnership with Siemens, Aprotech provides additional services for auditing and consulting in the area of technology circuits simplifying the transition to new technologies and enabling faster optimization of business processes.

aprotech Powered by KasperskyOS KasperskyOS



CLOUD SERVICES:

1. Basic monitoring

FleetManager:

- Monitoring and primary analysis of data on the performance of connected equipment;
- Additional capabilities for geographically displaying the fleet of devices and generating notifications about various events.

2. Service for Overall Equipment Effectiveness (OEE)

OEE visualization at the level of the production line and individual machine:

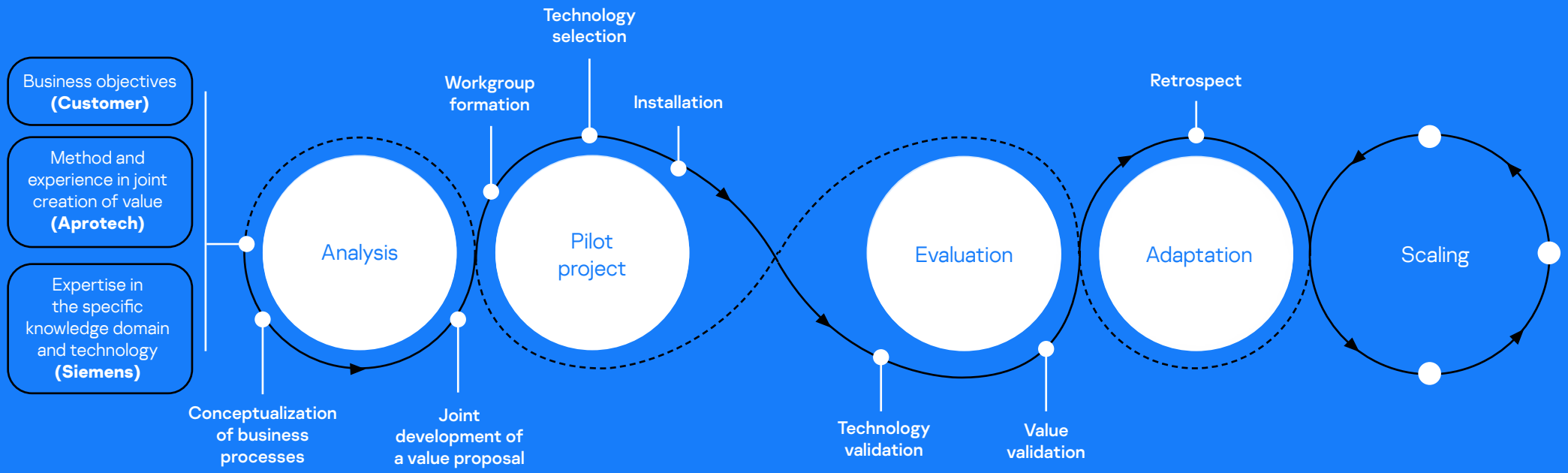
- Data modeling and preprocessing of input data for key performance indicators of OEE;
- Correlation of machine data to OEE monitor application data;
- OEE information dashboard, including productivity, availability and quality for the selected time interval and machine/line.

Expert analysis for OEE diagnostics:

- Analysis of OEE trends and comparison of similar objects over time;
- Recommendations on improving OEE at the level of the machine/line.

Digital consulting/audit of an enterprise production line

In partnership with Siemens MindSphere, Aprotech provides methodologies for searching for business value and conducts digital consulting/auditing of an enterprise production line for the purpose of identifying weak points (bottlenecks) and subsequently implementing a digital service.



SIEMENS

Silver Partner

MindSphere

On-site visit	Creation of solutions	Pilot assignment	Installation	Continual improvements
· Interview with the customer's team · Information collection · Systemization of gathered information	· Clustering of problems and proposed improvements · Creation of solutions	· Prioritization of solutions · Joint selection of the objective for the pilot project	· Implementation of the pilot project (Proof of Value)	· Evolutionary development and scaling of solutions
2 DAYS	**2–3 WEEKS**	**2 DAYS**	**1–2 MONTH**	**-**

Kaspersky IoT
Secure Gateway (KISG) 100

Kaspersky IoT Secure Gateway 100 is the first Cyber Immune data gateway designed for the industrial internet of things. It is built upon the KasperskyOS operating system and the Siemens SIMATIC IOT2040 hardware platform.

Developed by Aprotech together with its parent company Kaspersky, this product lets you directly connect to industrial equipment to collect data on its operation and send this data to cloud and local systems. A direct connection is the quickest, securest and most effective way to collect information. The gateway serves as a universal tool for not only connecting and preprocessing a data stream, but also for protecting connected equipment.

Cooperation between Aprotech and Siemens

Processor	Intel Quark X1020
Memory	1 GB
Connections	Support for 100 Mbps LAN 2 x Ethernet (RJ45) 1 x USB client
I/O interface	2 x COM port (RS 232, RS 485)
Storage	microSD

Kaspersky IoT Secure Gateway 100 is the key component for securely connecting equipment to digital services that help substantially enhance the effectiveness of an individual unit of equipment and the entire production facility.

The fundamental security of KasperskyOS is ensured by its unique proprietary microkernel and security system that block all unauthorized actions by default, and by the isolated components that cannot affect each other's operations. This means that the system will always perform its critical functions even in a hostile environment. This Cyber Immune gateway is resistant against the overwhelming majority of cyberattacks and protects any data that is transmitted from devices to a cloud platform.

Kaspersky IoT Secure Gateway 100 essentially operates as a software data diode at the OS level, which means that the data stream flows only in one direction (from the field level to the cloud). It thereby protects connected equipment against external influence by potential cybercriminals.

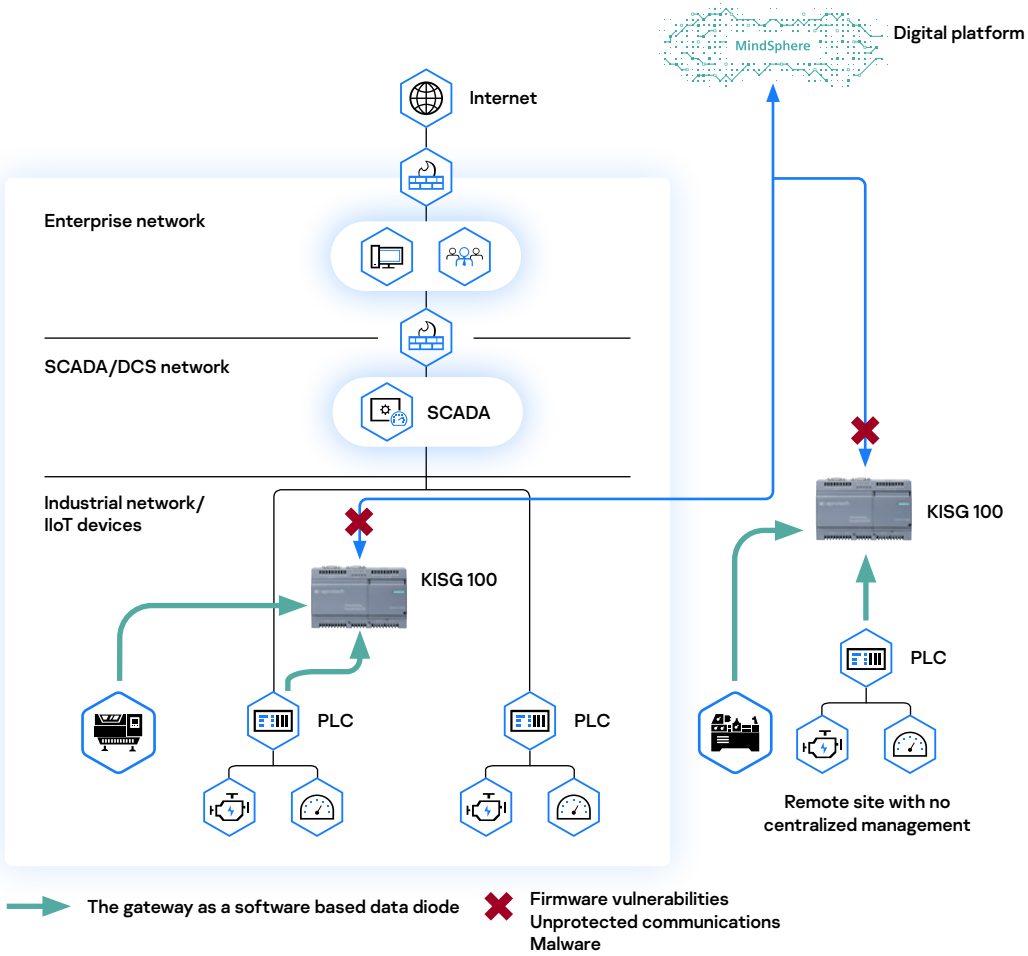
The first version of KISG 100 supports connections over the universal OPC UA protocol and prepares data for transmission to the Siemens MindSphere industrial IoT platform.

«World Leading Internet Scientific and Technological Achievement» award from China's major World Internet Conference 2020 (Wuzhen Summit)

aprotech Powered by KasperskyOS SIEMENS KasperskyOS

KasperskyOS
Be Immune

The foundational principles of KasperskyOS essentially enable the gateway to operate as a data diode at the operating system level (Software-Based Data Diode)



«Cyber Immunity means that an IIoT device can be combined into a network with other automation devices without the need for additional security features. This makes it significantly easier to connect equipment to IT systems»

ARC Advisory report, March of 2021

The gateway can be employed not only at sites with an already prepared security infrastructure, but also at remote sites that have not yet deployed a centralized security and control system.

R&D Adaptive Production Technology
(Aprotech)

**Contact our team
to go digital with us!**

start@aprotech.ru
+7 (495) 970-71-17

aprotech.ru
os.kaspersky.ru