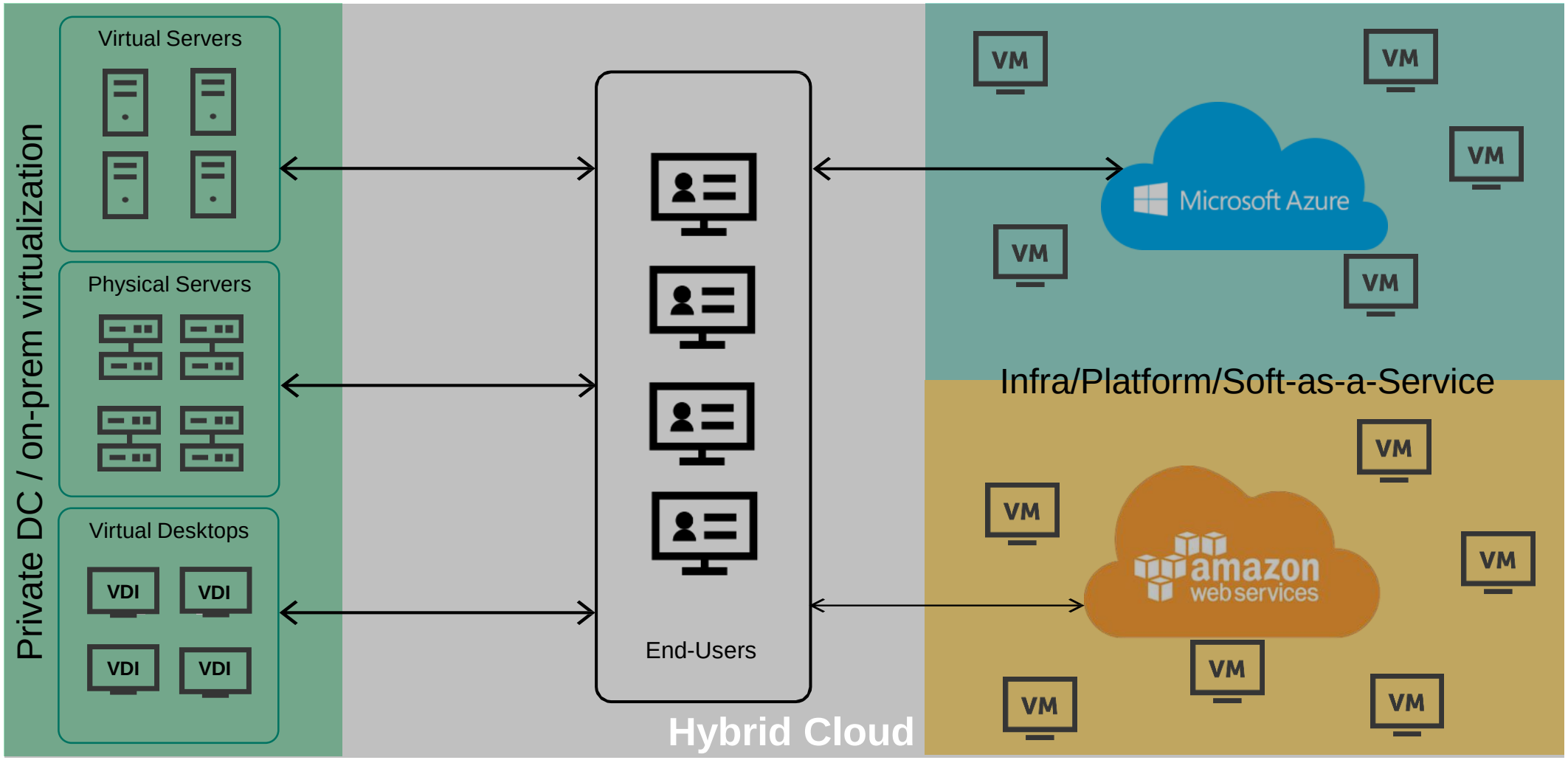
Hybrid cloud coming to ICS: are we ready?

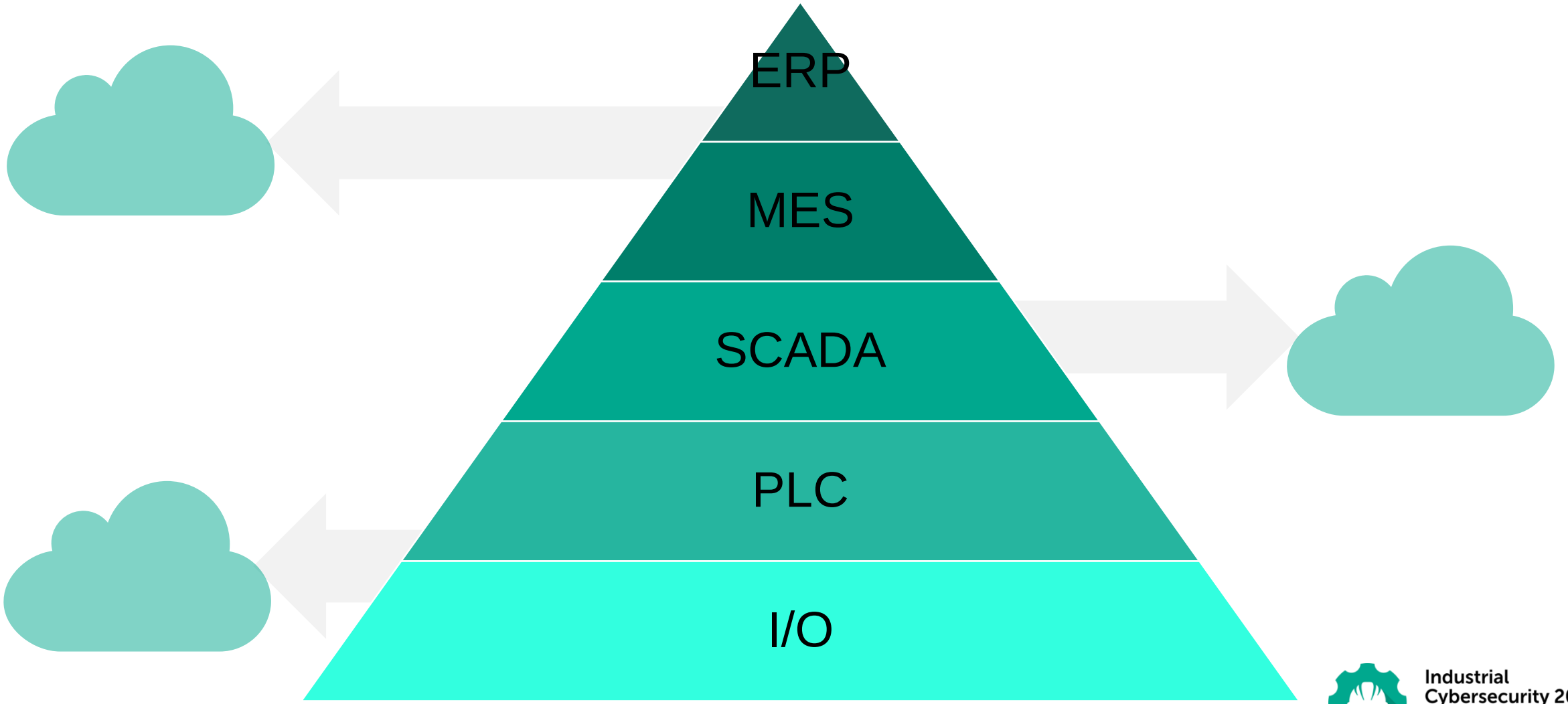
Matvey Voytov | GTM Strategy lead | Hybrid Cloud Security | Kaspersky Lab HQ

Industrial Cybersecurity 2018:
Opportunities and challenges in Digital Transformation

WHAT IS HYBRID CLOUD?



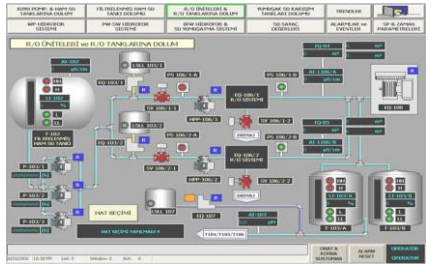
WHAT WE WILL (AND WON'T) DISCUSS TODAY?



IIoT vs Cloud SCADA



Modbus	DNP 3	OPC
ICCP	ControlNet	BBC 7200
ANSI X3.28	DCP 1	Gedac 7020
DeviceNet	DH+	ProfiBus
Tejas	TRE	UCA




- Field Devices
- Sensors
- Meters

Acquisition

LAN /WAN

Conversion

- PLC
- IED
- RTU

LAN /WAN

- Protocols
- Network equipment

Communication

Internet

Control

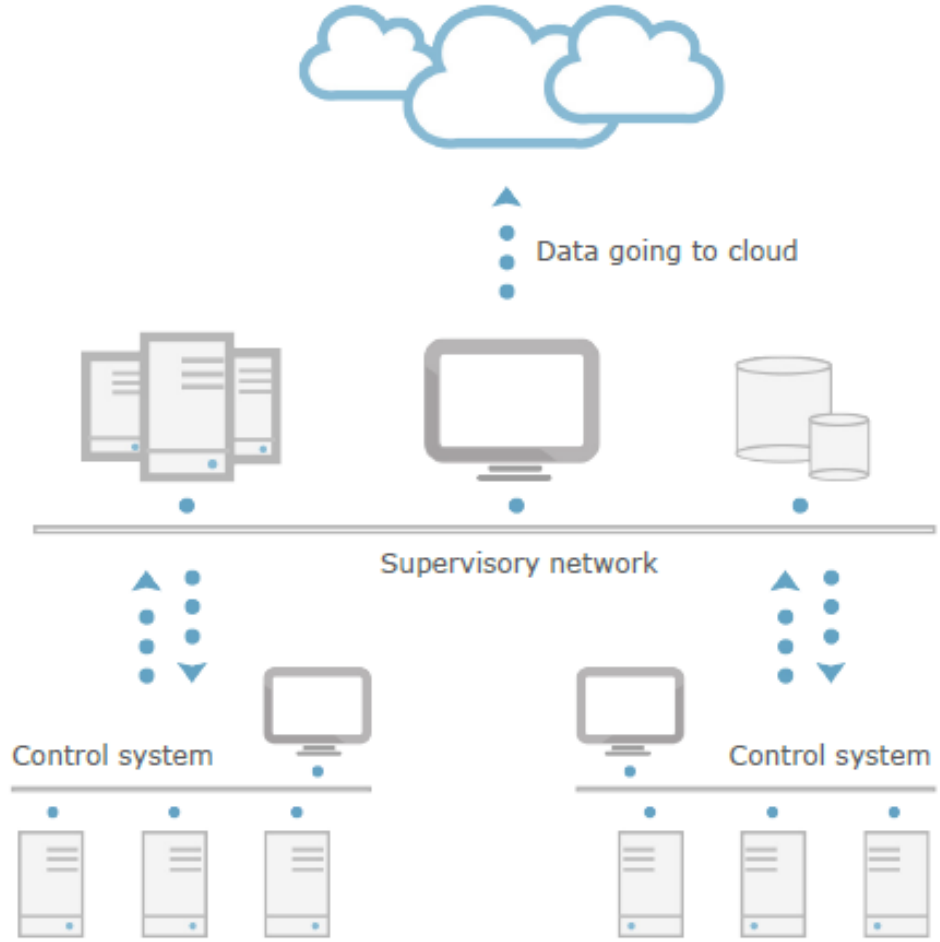
- SCADA
- HMI

Internet

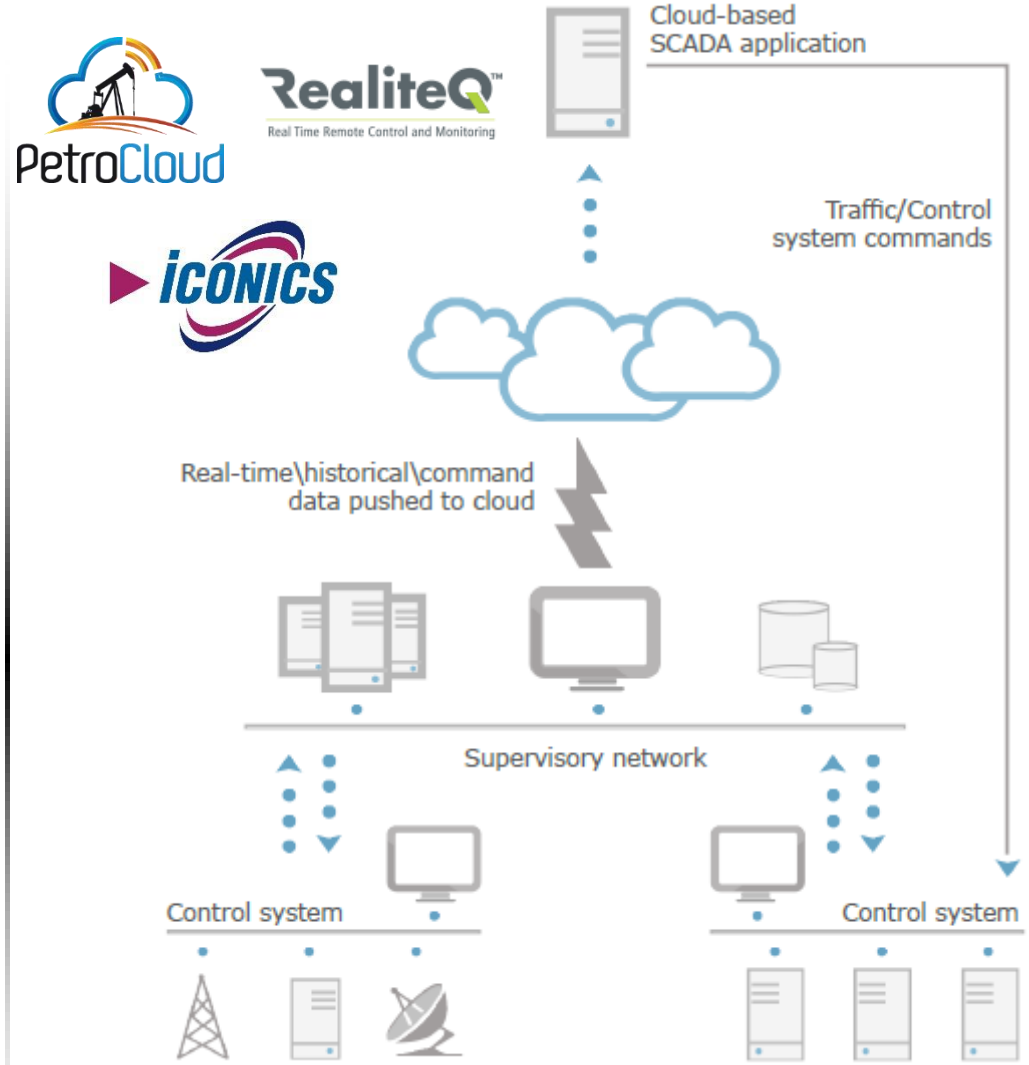
IIoT


Industrial Cybersecurity 2018:
Opportunities and challenges in Digital Transformation

SCADA-as-a-SERVICE – OPTIONS

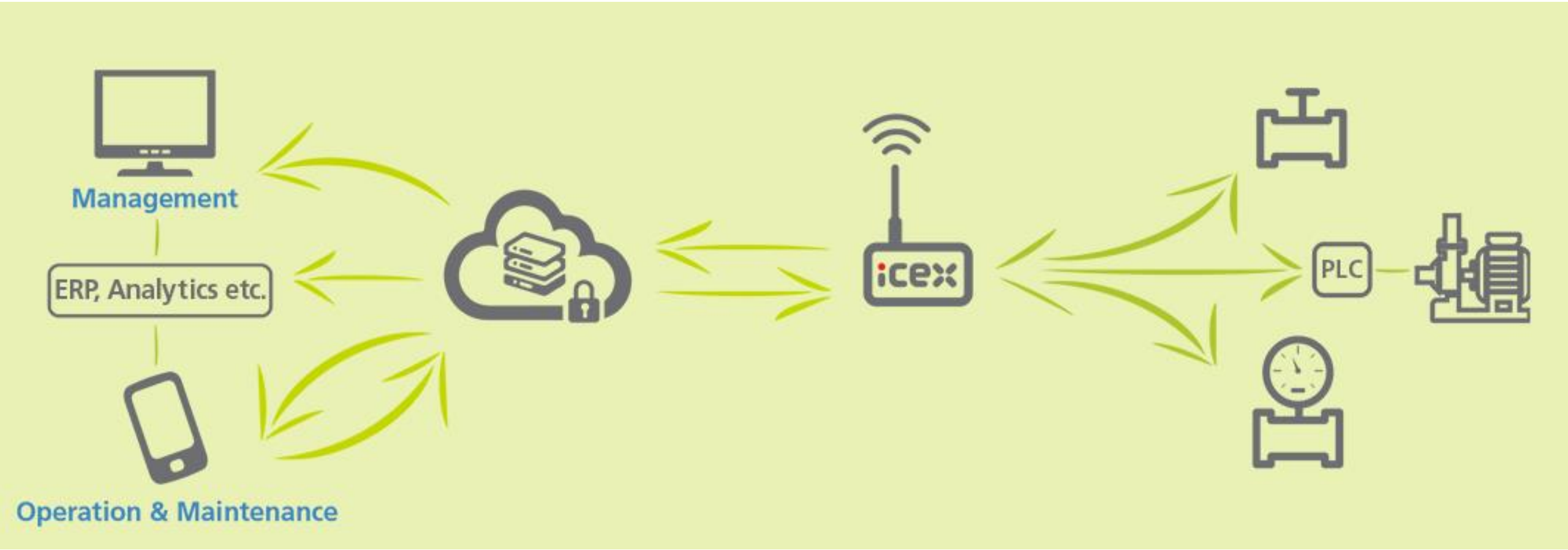


Internally hosted SCADA application where data is externally pushed



SCADA application entirely hosted in the cloud

SCADA-as-a-SERVICE architecture



SCADA-as-a-SERVICE BENEFITS (?)

	Traditional SCADA	SCADA-as-a-Service
MAINTENANCE	• Delivering updates to OS/SCADA/Security • Complex migration processes	• Full technical support for the system is included in the annual hosting fee • Testing advantages
DATA LOGGING	• Relational databases require routine maintenance • Historian packages add significant costs	• Data is collected and timestamped by the edge device and sent to the cloud for storage. DB maintenance is performed on a regular basis as part to the annual hosting fee.
DATA SECURITY	• Data backups are typically the responsibility of the end user	• Data is typically stored in a Tier Level 3 data center with back-up power generation, redundancy, and building access control
CYBER SECURITY	• Full responsibility of customer	• All data transmissions are encrypted and the connection is verified using TLS certificates. There are no need in VPN firewall
REPORTING / WEB and MOBILE INTERFACE / ALERTS	• Additional costs for additional services • Access to local/web servers for notifications	• No additional costs (??) • Integrated notification services

SaaS/PaaS/IaaS THREATS

➢ Loss of control

- Organizations moving sensitive data into the cloud must determine how these data are to be controlled and kept secure.

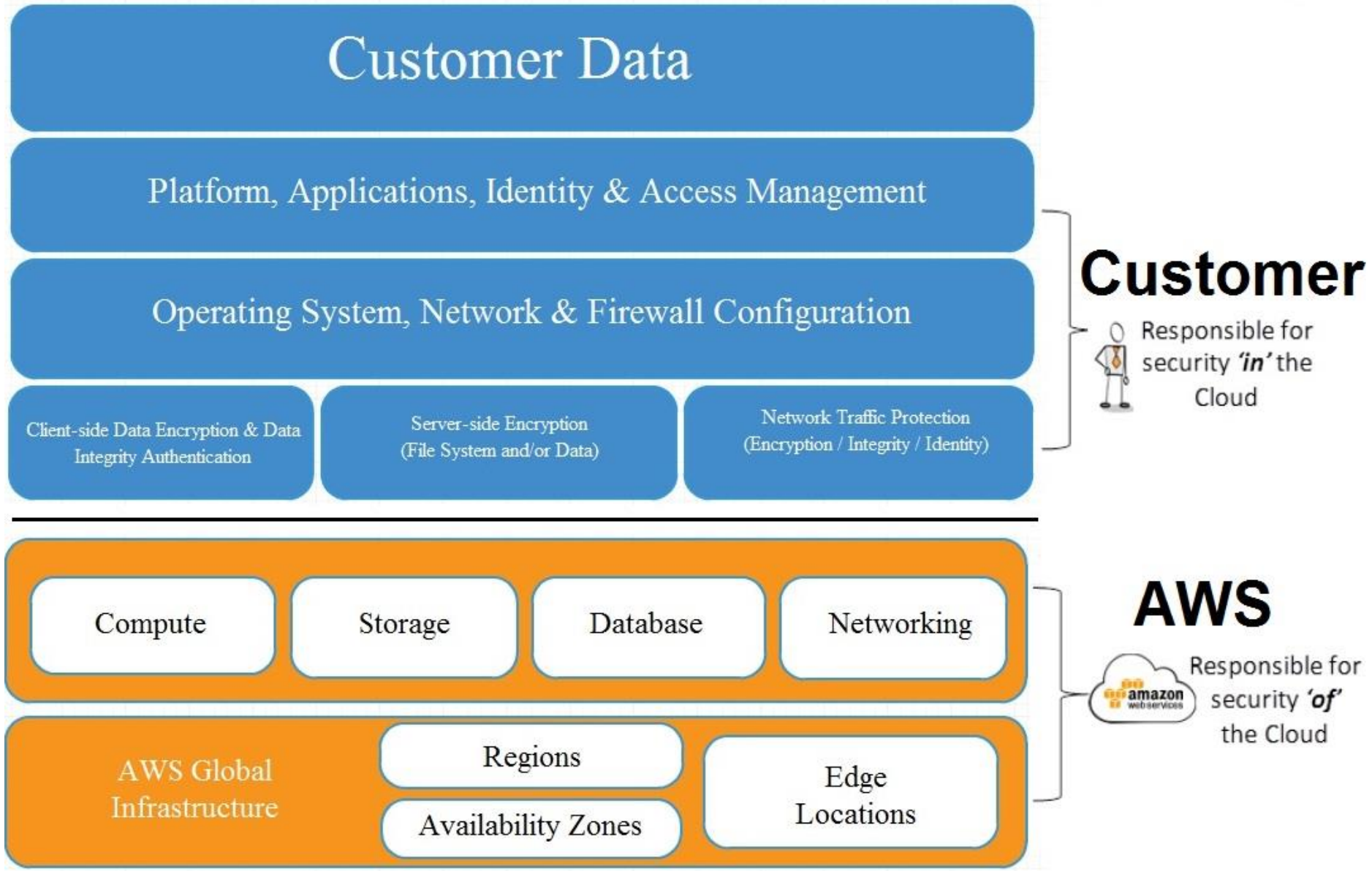
➢ Increased network threats

- Web application attacks that target exposed interfaces.
- In case of PULL, there will be open network ports on the control infrastructure

➢ Shared infrastructure

- Authentication issues – an attacker could pose as a subscriber to exploit vulnerabilities from within the cloud environment to gain unauthorized access.

WHY NOT IaaS?


Customer Data
Platform, Applications, Identity & Access Management
Operating System, Network & Firewall Configuration
Client-side Data Encryption & Data Integrity Authentication
Server-side Encryption (File System and/or Data)
Network Traffic Protection (Encryption / Integrity / Identity)
Customer
Responsible for security 'in' the Cloud
Compute
Storage
Database
Networking
AWS Global Infrastructure
Regions
Availability Zones
Edge Locations
AWS
Responsible for security 'of' the Cloud

HYBRID CLOUD @ ICS: TAKE AWAYS

➢ Hybrid cloud already came to ICS:

- IIoT
- SCADA/Control network virtualization
- Scada-as-a-Service / Scada at Cloud
- Cloud-based ICS security

➢ SCADA-as-a-Service is still a rare bird:

- Works well yet for greenfields, SMB, non-critical infras
- Brings some significant cloud benefits
- Brings attack surface increase

https://cloudsecurityalliance.org/

CSA cloud security alliance℠

Industrial Cybersecurity 2018:
Opportunities and challenges in Digital Transformation

LET’S TALK?

Matvey.voytov@kaspersky.com

Industrial
Cybersecurity 2018:
Opportunities and challenges
in Digital Transformation