WAVESTONE

Cloud for OT: Emerging trends

Wavestone Insight Day – April 2024

Kenza MAAMRI
Senior consultant
kenza.maamri@wavestone.com

Victor CHALBOS
Consultant
victor.chalbos@wavestone.com

AGENDA

/ **01** Cloud for OT today

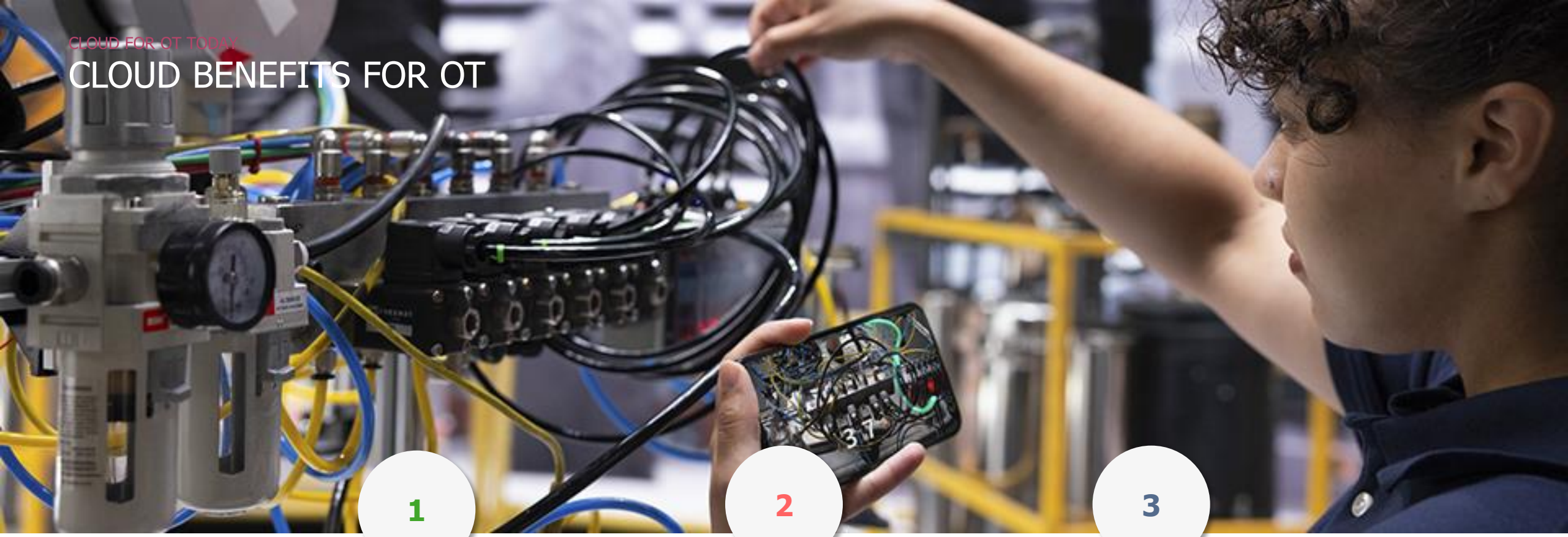
/ **02** Emerging SaaS solutions for OT

/ **03** Move to SaaS: New strategic approach

/ **04** Focus on standards and regulations

/ **05** Key takeaways

CLOUD BENEFITS FOR OT



1

High availability

Cloud environments are **redundant by design** and CSPs offer **high SLAs**.

2

Large scalability

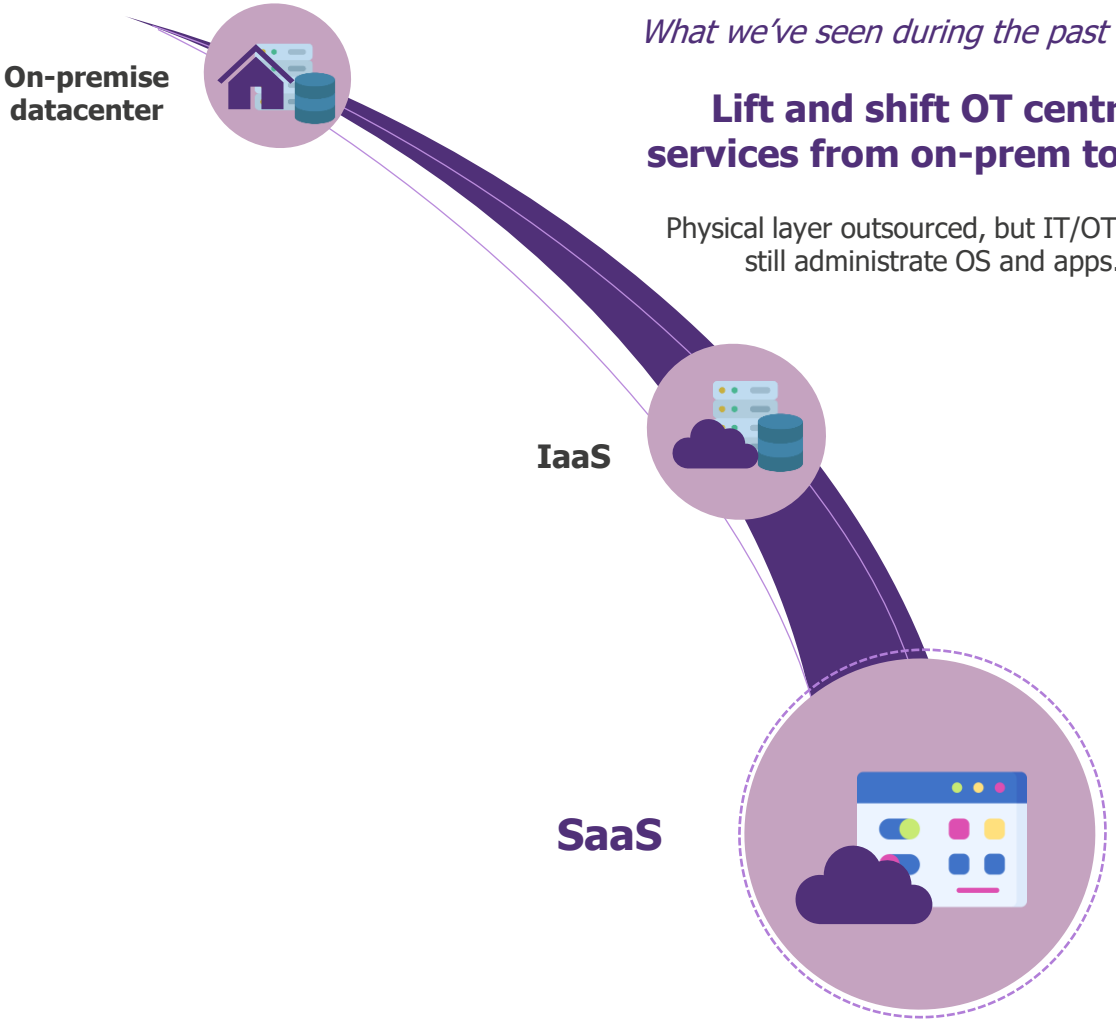
Cloud environments allow to **mutualize global services** for multiple sites located in **wide geographical areas**.

3

Optimization

Through more efficient **production planning tools, predictive maintenance** and **cloud-based supply chain management**, oftentimes AI enabled and provided by CSPs.

CLOUD FOR OT IS NOT A NEW THING

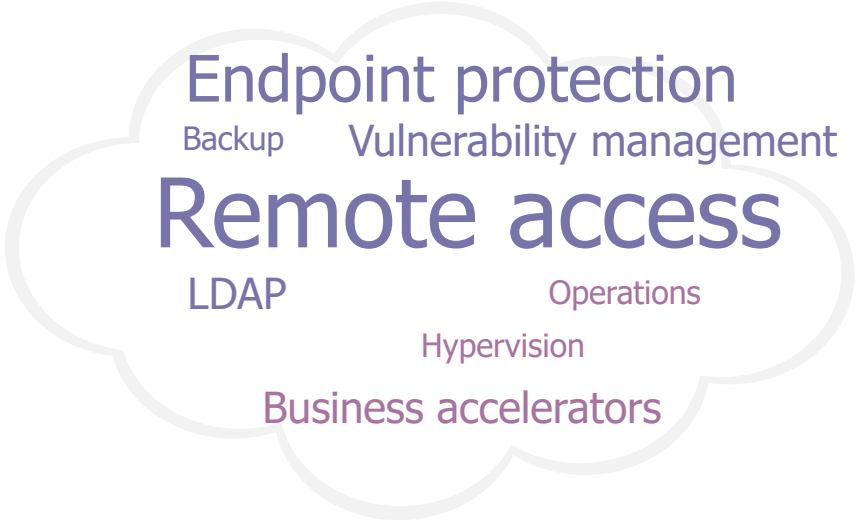


What we've seen during the past years...

Lift and shift OT central services from on-prem to IaaS

Physical layer outsourced, but IT/OT teams still administrate OS and apps.

Main usages among few PIC clients using Cloud services (IaaS)



What is coming now...

Move OT applications and services to SaaS?

SaaS applications **offer new services** for business.

What risks and opportunities for business and cybersecurity?

EMERGING SAAS SOLUTIONS FOR OT

OT SaaS SOLUTIONS ARE GROWING IN NUMBER

Business applications

Supervision and operations

Monitor the state of equipment and processes

- YOKOGAWA OpreX Asset Health Insights
- AVEVA PI System
- CODESYS CodeSys Automation Server
- Seeq Seeq

Optimization

Analyze data to identify inefficiencies and improvement

- Rockwell Automation FactoryTalk Optix
- Honeywell Forge Performance
- Schneider Electric EcoStruxure Asset Advisor
- inhand InConnect Service
- TrendMiner TrendMiner
- secomea Data Collection Cloud
- EMERSON Plantweb Optics Data Lake

Infrastructure services

Remote access

Connect and control processes remotely

- DISPEL Zero Trust Access
- Systancia Cleanroom
- Delinea Delinea PAM
- PHOENIX CONTACT mGuard Secure Cloud
- wallix Remote Access

Backup

Copy and secure storage of critical data

- VERITAS ALTA Backup as a Service
- Acronis Acronis Cyber Backup Cloud

Vulnerability management

Assess and mitigate emerging threats

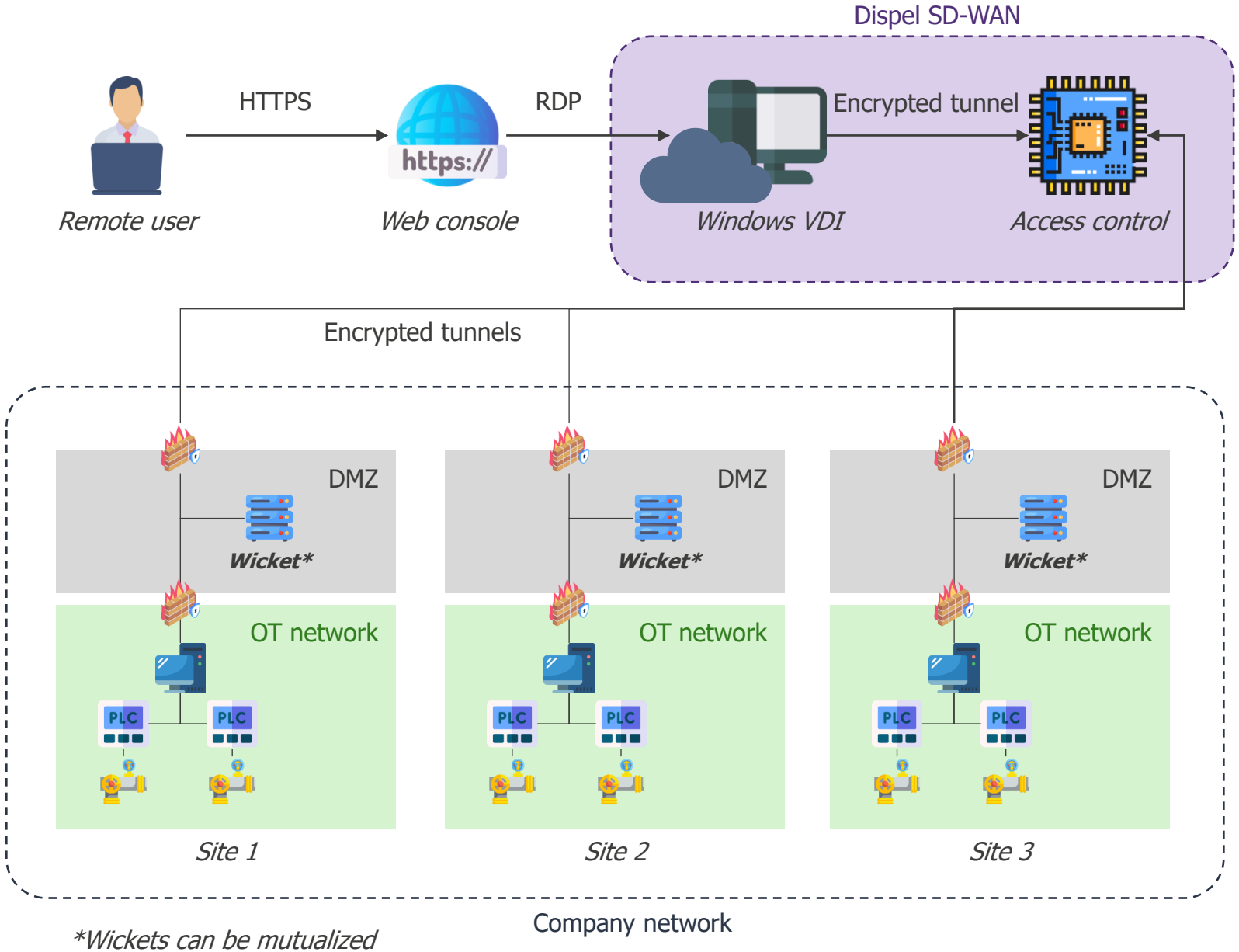
- DRAGOS Dragos Platform
- SKYBOX SECURITY Vulnerability Control

Network detection

Analyze network traffic to identify anomalies

- NOZOMI NETWORKS Nozomi Vantage
- Microsoft Defender for IoT
- CISCO Cisco Umbrella
- paloalto NETWORKS Palo Alto Prisma

QUICK FOCUS ON DISPEL ZERO TRUST ACCESS



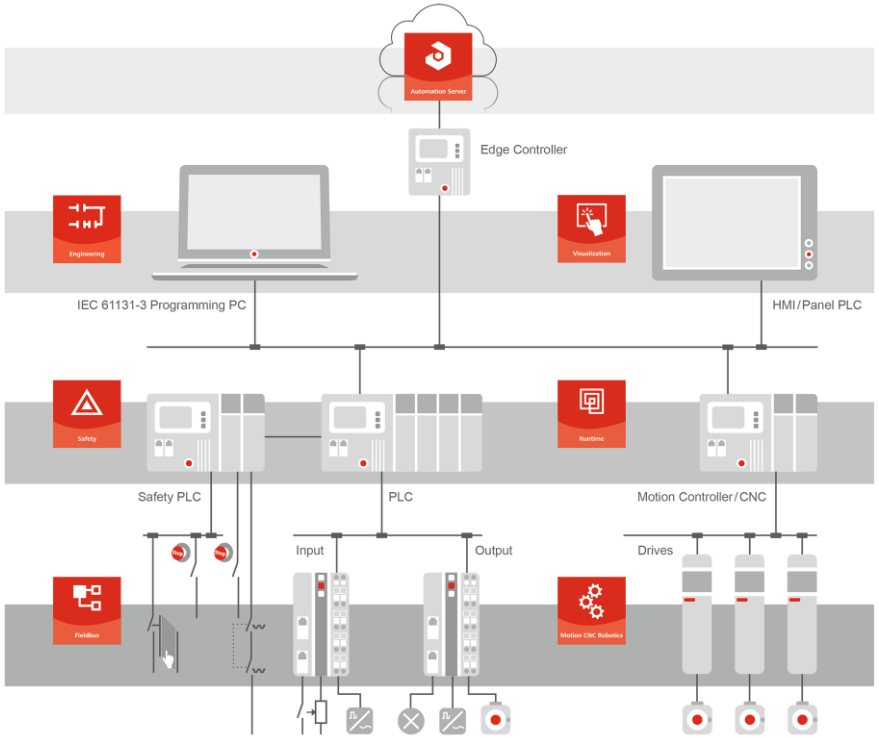
Dispel offers an **"almost full SaaS" remote access solution**.

The wicket is the **only component** to be deployed and maintained on-premise.

This gateway permits to keep control of the connections with the SaaS, **in line with the DMZ purpose.**

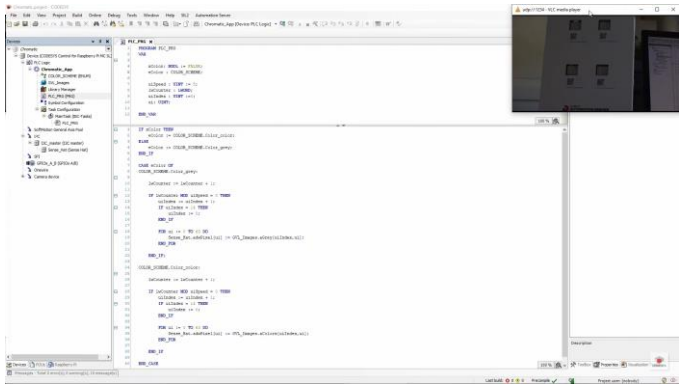
QUICK FOCUS ON CODESYS AUTOMATION SERVER

CODESYS Automation Server is **a SaaS solution**, connected to an on-premise Edge Gateway, aiming to **perform remote operations**.

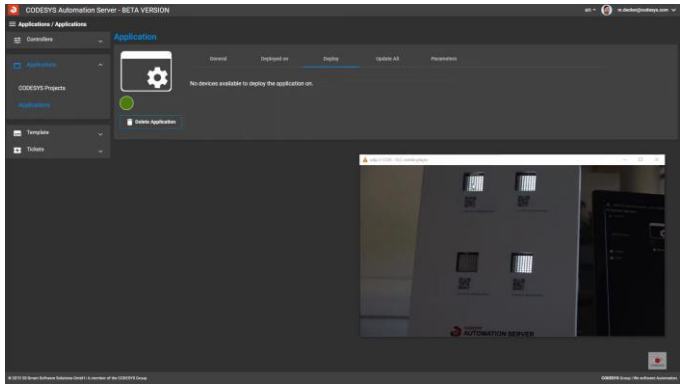


Source: The System (codesys.com)

An operator can **upload a PLC program** on the web console...



...and **deploy it remotely** on the PLC:



Source: Webinar - CODESYS Automation Server (EN) (youtube.com)

SaaS solutions are more and more deployed in OT, it's a fact!

OT cybersecurity teams must address them the right way

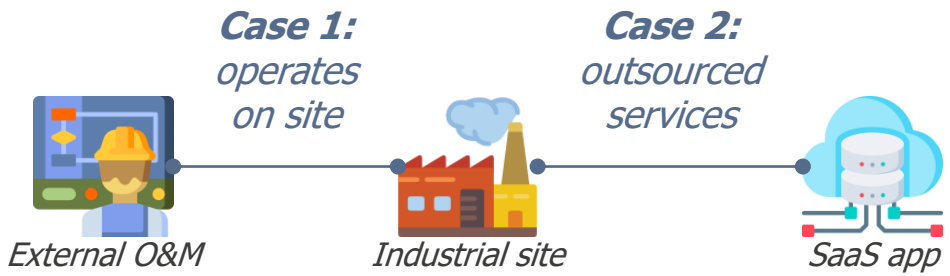
SaaS FOR OT: CYBERSECURITY CHALLENGES

SaaS for OT

3RD PARTIES DEPENDENCIES

SaaS applications are not "lift-and-shift"-friendly. Your dependence on suppliers increases – cybersecurity must be included into contracts.

No fundamental change with on-premise services operated or maintained by external companies:

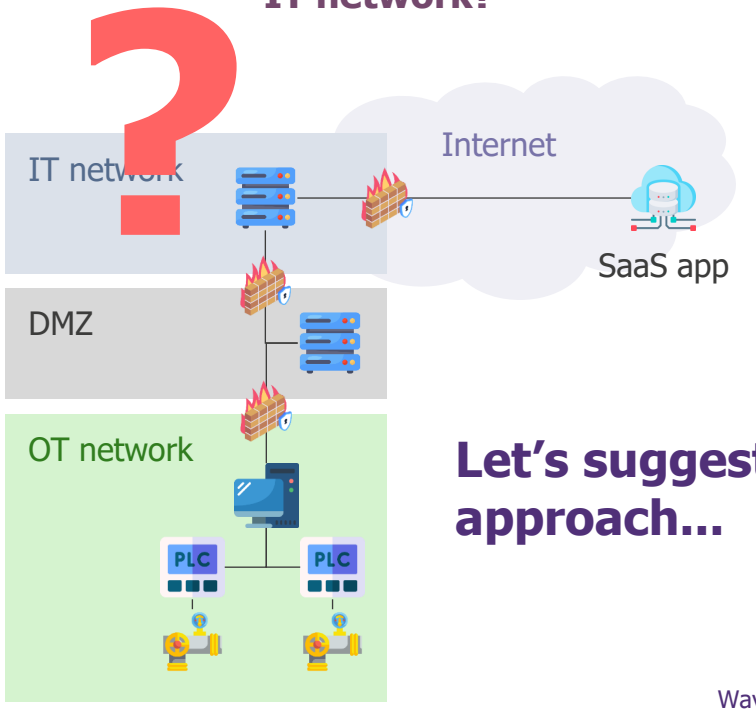


Both rely on external expertise!

INCREASED CONNECTIVITY

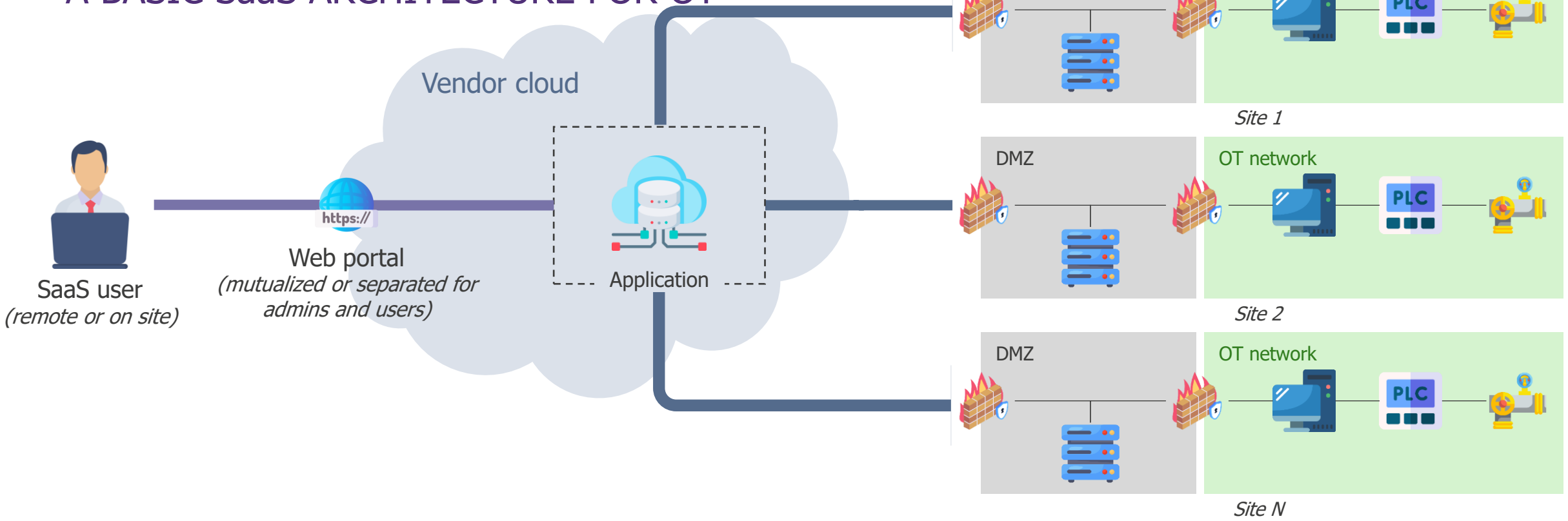
OT SaaS must be considered as OT environment and be segregated from other environment.

Should your SaaS-OT connection go through your IT network?



Let's suggest another approach…

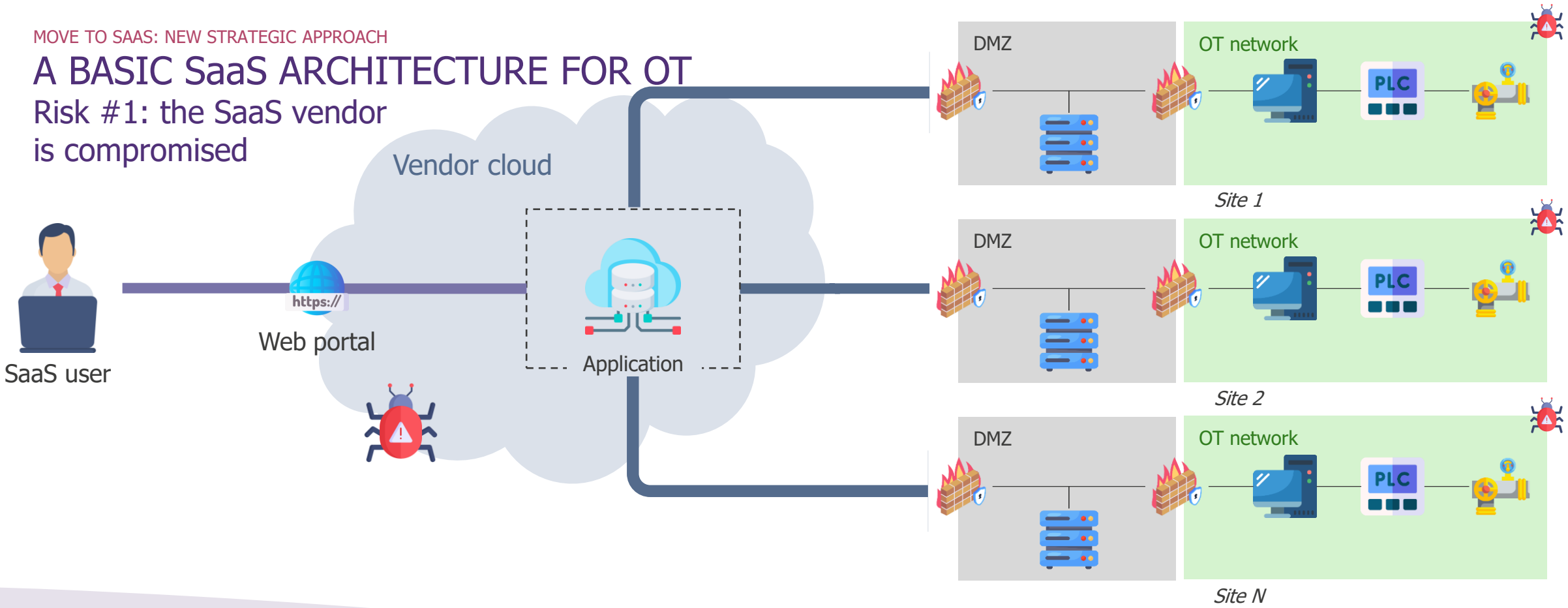
A BASIC SaaS ARCHITECTURE FOR OT



MOVE TO SAAS: NEW STRATEGIC APPROACH

A BASIC SaaS ARCHITECTURE FOR OT

Risk #1: the SaaS vendor is compromised



Reconnaissance

- Audit your vendors and request certifications

Intrusion

- Include IRP clauses for incident notification
- Vendor must conduct network detection

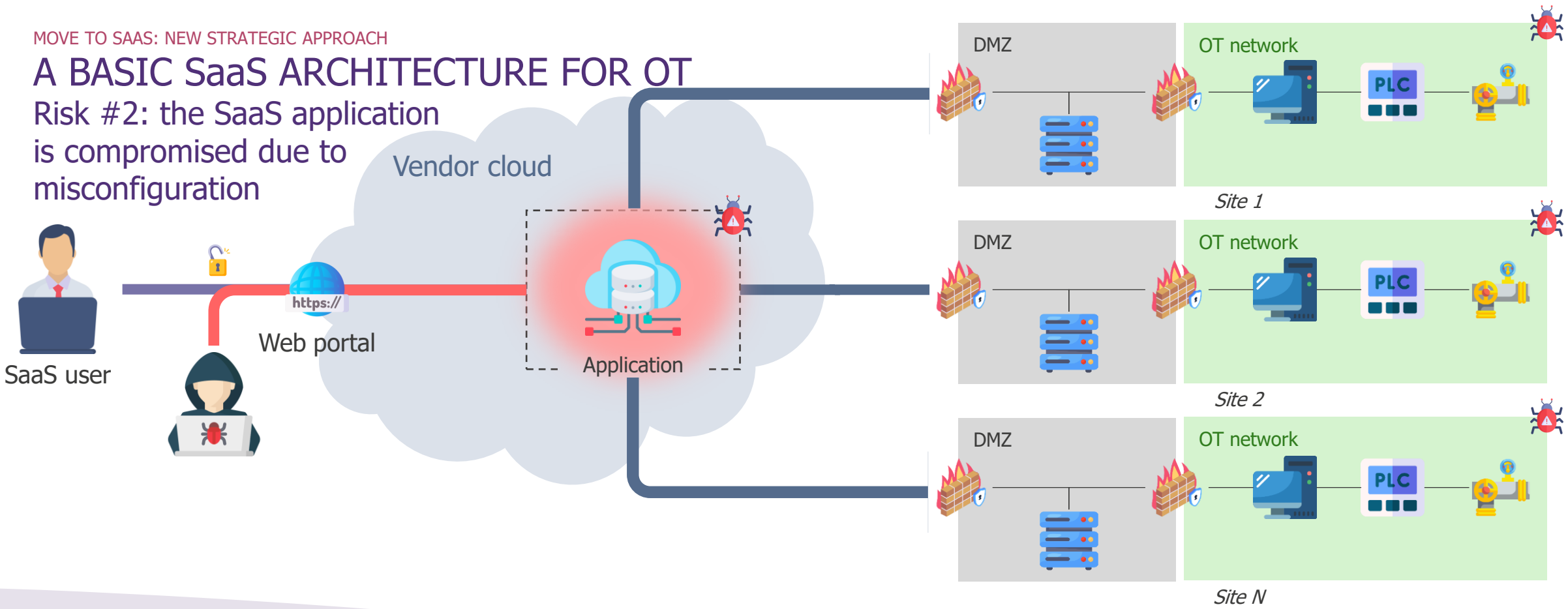
Exploitation / Lateralization

- Ensure SaaS/Site connections are initiated by sites
- Maintain this critical relay
- Collaborate on IRP between provider and client
- Ensure the SaaS provider has DRP
- Plan downgraded operational modes

MOVE TO SAAS: NEW STRATEGIC APPROACH

A BASIC SaaS ARCHITECTURE FOR OT

Risk #2: the SaaS application is compromised due to misconfiguration



Reconnaissance

- Restrict admin web console access to trusted devices (PAW)

Intrusion

- Implement robust authentication mechanisms (MFA) and segregate IT and OT accounts
- Provide training for administrators to prevent misconfigurations
- Include IRP clauses for incident notification
- Identify and monitor all external connections (H2M, M2M)

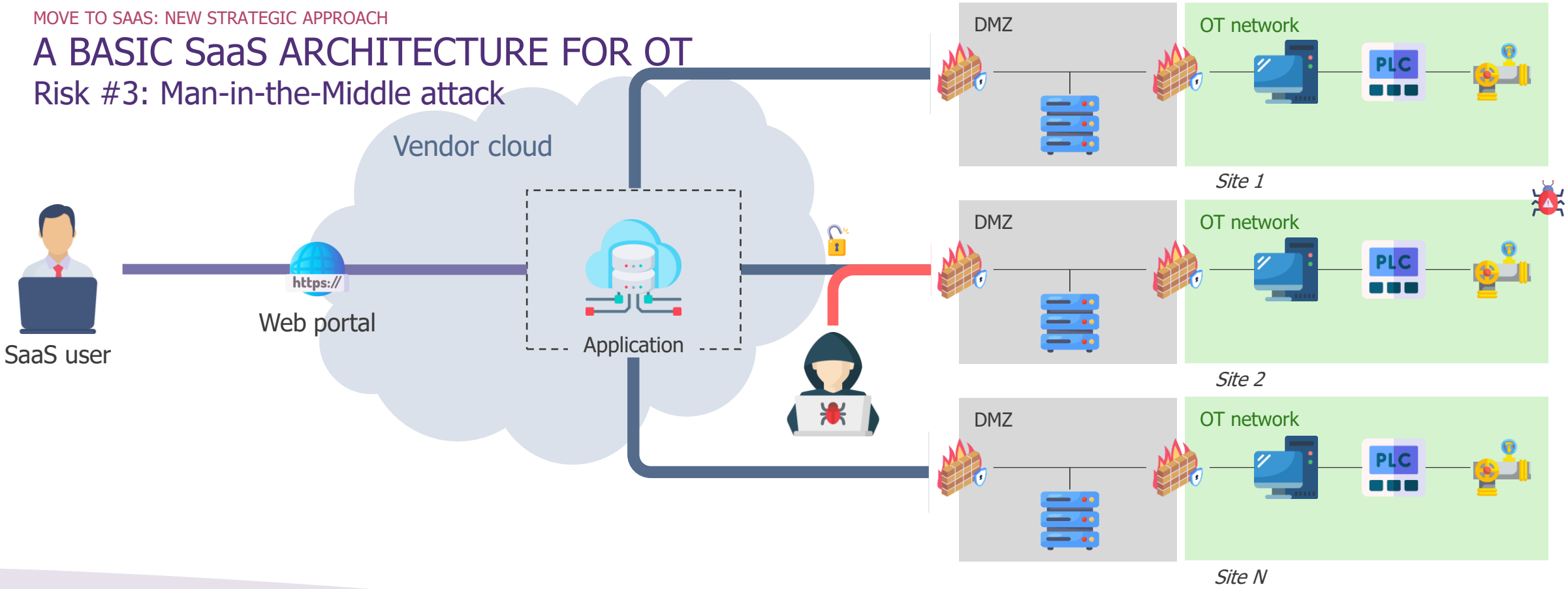
Exploitation / Lateralization

- Implement RBAC model
- Implement fine-grained delegation
- Collaborate on IRP between provider and client
- Ensure SaaS provider has a defined DRP
- Ensure SaaS/Site connections are initiated by sites
- Maintain this critical relay
- Plan downgraded operational modes.

MOVE TO SAAS: NEW STRATEGIC APPROACH

A BASIC SaaS ARCHITECTURE FOR OT

Risk #3: Man-in-the-Middle attack



Reconnaissance

- Encrypt network flows

Intrusion

- Identify and monitor external connections (allowlisting)
- Provide training for administrators to prevent misconfigurations (firewalls, etc.)

Exploitation / Lateralization

- Ensure SaaS/Site connections are initiated by sites
- Maintain this critical relay
- Develop an incident response plan
- Plan downgraded operational modes

OT NETWORKS ARE MORE AND MORE CONNECTED

Network isolation is not the main countermeasure anymore

SELECT YOUR VENDORS

- Take cybersecurity into consideration in RFPs
- Audit your vendors and request certifications (SecNumCloud, ...)

SECURE YOUR ARCHITECTURE AND TRAIN YOUR ADMINS

- Identify and monitor your external connections (H2M, M2M)
- Train your admins to avoid misconfigurations
- Ensure SaaS/Site connections are initiated by sites
- Encrypt data in transit

THE CLIENT IS IN CHARGE

FOCUS ON IAM

- Implement strong authentication mechanism (MFA)
- Segregate IT and OT accounts / IdP
- Implement an RBAC model and a fine-grained rights delegation model

THE SOLUTION OFFERS THE FUNCTIONNALITIES
THE CLIENT IS IN CHARGE OF CONFIGURATION

PREPARE YOUR INCIDENT RESPONSE

- Ensure your SaaS vendors have mature detect, response and recovery capabilities
- Set up dedicated channel between SOCs
- Set up network detection on site
- Plan downgraded modes for critical functions

THE CLIENT AND THE PROVIDER WORK HAND IN HAND

CLOUD SECURITY STANDARDS

Current existing standards are not dedicated to OT environments and may require some tailoring to take into account OT specific business and security constraints

SecNumCloud

Developed by **ANSSI**.

Offers a set of **security rules** to follow guaranteeing a high level of requirements from a **technical, operational or legal** point of view.

All types of cloud service providers are eligible for qualification: software as a service (SaaS), platform as a service (PaaS), container as a service (CaaS), and infrastructure as a service (IaaS).

NIST 800-144

Security and Privacy Guidelines in Public Cloud Computing : provides an in-depth overview of security and privacy challenges in cloud computing and offers suggestions on how today's companies can overcome them.

NIST Cloud Computing Program (NCCP) : a **cloud security framework** – a blueprint that defines the way in which a cloud infrastructure should be built.

The NCSC has published new guidance on **cloud-hosted Supervisory Control and Data Acquisition** (SCADA), to help organizations identify some of the key considerations required before deciding on migrating SCADA to the cloud.

WHAT FUTURE FOR THE CLOUD AND EUROPE'S TECHNOLOGICAL INDEPENDENCE?

This is what is currently being played out in Brussels during negotiations on the **EUCS (European Union Cybersecurity Certification Scheme for Cloud Services)**, which must define the certification scheme for Cloud services in Europe and which is none other than the European adaptation of the famous French SecNumCloud. The law which will define the requirements, in terms of cybersecurity, between the different members of the EU in the cloud.

The EU plans to compile a set of rules, in the form of an **EU Cloud Rulebook** and a Guidance on public procurement of data processing services. The Rulebook will provide a single European framework relevant binding and non-binding rules for cloud service users and providers in Europe.

KEY TAKEAWAYS

SaaS for OT

SaaS solutions are growing – OT does not escape the rule

SaaS offers huge advantages for business, no doubt about it. OT cybersecurity teams must address these new usages with the right approach.

Network isolation is not the main countermeasure anymore

OT networks are more and more connected – select your vendors, secure your architecture, train your admins, focus on IAM and prepare your incident response.

Some industrial sectors are more likely to deploy cloud solutions

Sectors such as logistics (warehouses, distribution centers, ...) are already highly connected with external services. Also, renewable companies often have a large number of sites, located in wide geographical areas, with less than one FTE per site, for which mutualized services are a huge added value. However, cloud solutions might not fit all sectors, especially regulated one.

SaaS usage can also be an opportunity for cybersecurity

Moving business applications to SaaS might offer security measures that were neglected before, especially for IAM (MFA, RBAC, nominative accounts, ...).

The Positive Way

WAVESTONE

Kenza MAAMRI
Senior consultant
kenza.maamri@wavestone.com

Victor CHALBOS
Consultant
victor.chalbos@wavestone.com

wavestone.com

Wavestone