



eBook

INDUSTRIAL CONTROL SYSTEMS SECURITY



Table of Content

01

History & Statistics

02

Compliance for OT

03

IT/OT Seperation

04

The Use Cases

05

Industry Stories

06

The cyberelements Features



SECTION 1:

HISTORY & STATISTICS



Evolution of the industrial environments

- **PLCs** introduced electronics to production automation for the first time, revolutionizing the process by making it significantly easier to create and modify control logic.

1972

- **Control Systems** are created from control loopsystems which consist of sensors, controllers, and actuators. They can be used to model complex behaviors such as continuous manufacturing processes.

- **Supervisory Control & Data Acquisition (SCADA) & Distributed Control Systems (DCS):** SCADA systems have historically integrated sensors, data transmission, and HMI software for centralized system visibility. DCS provide similar capabilities on a factory scale, with typically less complex networking and communications.

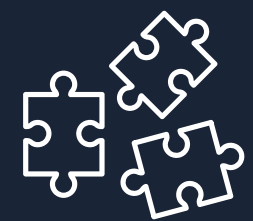
- **Industrial Control Systems (ICS):** Include SCADA, DCS, and PLCs used for managing and automating industrial processes.

- **OT versus IT:** Industrial environments have traditionally been dominated by Operational Technology (OT), focused on physical processes. With digitalisation transformation, we have seen an increased interdependence between IT & OT systems.

- **Internet of Things (IoT) & Industrial Internet of Things (IIoT):** referring to the network of physical devices, machine-to-machine communication, and data analysis .

Present





Industrial Security Main Challenges

90%

of Federal OT leaders report an increase in their agency's prioritization of OT cybersecurity in the past two years

68%

of industrial organizations experienced an OT-related cyber incident in the past year

20%

of industrial organizations grade themselves an 'A' in OT cyber preparedness

MEANWHILE

Top deficiencies in the industrial sector are:



Lack of Network Visibility



Vulnerability & Risk Management



Secure Remote Access & Monitoring



Emerging Needs

After the 4th industrial revolution (Industry 4.0), we have seen a paradigm shift in the manufacturing world. Industries are no more isolated plants that are disconnected from the rest of the world. Instead, IT environments are now interconnected with OT environments since we are now in the era of big data, intelligent machine, and IoT/IIoT. According to the MeriTalk & CLAROTY report “Guardians of Government: The State of Federal OT Security”, 69% of OT teams now report to the CISO – either reporting together with or independent of IT security

We live today in the 5th industrial revolution which emphasizes human-centric design, sustainability, and the integration of advanced technologies to enhance overall well-being. This is why remote working has been now widely adopted worldwide. It offers flexibility, reduces carbon footprint, and maximize resource efficiency.

These technological and cultural changes created a substantial development in the industrial world including the whole ecosystem (e.g. manufacturers and service providers) leading to new cybersecurity needs:



Emerging Needs

- **Securing remote access:** In the old days, you had to physically be in the plant to connect to a device proving thereby your identity. However, it gets more complex when users are connected remotely to OT environment sometimes from personal/untrusted devices.
- **The use of cloud resources:** As big data analysis is becoming essential for machine learning and predictive analytics algorithms; industries rely on cloud solutions which process data to provide various dashboards. In this case, OT environments are open to the cloud and the internet creating the need for proper isolation.
- **File Transfers:** Given the remote working context, file transfers are part of workforce's daily tasks. Industries are required to provide secure file transfer methods for their users to protect OT environments from the external world.
- **IT/OT Segmentation:** The IT/OT interconnection leads us to the need of proper segmentation. It means, managing both IT and OT environments while keeping a clear separation between the two. In other words, ensuring isolation while keeping the interconnection between the two.
- **Traceability:** The need of traceability for OT environments is considerably high given the sensitivity of the industrial sector. Most of the time, disruption of any manufacturing activity can't be afforded. Therefore, it is important to be able to track back all the actions in the case of an incident.



SECTION 2:

COMPLIANCE IN THE INDUSTRIAL SECTOR



Compliance in The Industrial Sector

Given the emerging changes in the industrial sector, cyber threats have been increasing. Furthermore, a breach in the industrial sector can have a catastrophic impact on our society. This is why, governments and cybersecurity authorities worldwide are actively creating and updating their legislations to fortify the industrial sector security.

NIS2

We can consider NIS2 as a continuation of NIS1. The main difference between the two versions is that NIS2 now applies to a wider range of organizations including energy, transportation, manufacturing, and water treatment companies from the industrial sector. These organizations will have to comply by a date which will be set in the national translation of the directive by October 2024.

These new measures include:

Article 18 2d & 21 1b

Supply Chain
Security

Article 21

Access Control Policies &
Asset Management

Article 21 1b

Multi Factor
Authentication

Article 24 & 21 1e

Monitoring &
Auditing



Compliance in The Industrial Sector

ISA/IEC 62443

ISA/IEC 62443 is a series of standards designed to provide a flexible framework for addressing and mitigating current and future security vulnerabilities in industrial automation and control systems (IACS). The standards are developed by the International Society of Automation (ISA) and the International Electrotechnical Commission (IEC) and are widely recognized in the field of operational technology (OT) security.

Key access security covered by the ISA/IEC 62443:

IEC 62443-3-3 2013 SR 1.6:
Access Control and Policies

IEC 62443-3-3 2013 SR 1.3:
Least Privilege Principle

IEC 62443-3-3 2013 SR 1.1:
Authentication & Authorization

IEC 62443-3-3 2013 SR 2.8 & SR 2.4:
Monitoring & Auditing





Compliance in The Industrial Sector

NIST 800–82, Revision 3

NIST Special Publication 800–82, Revision 3, titled "Guide to Operational Technology (OT) Security" was published on September 28, 2023. It provides comprehensive guidelines and recommendations for securing OT environments, which include Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, and other control systems.

Key access security covered by NIST 800–82, Revision 3:

Section 5.2.6:
Access Control

Section 5.3.4:
Account Management

Section 5.3.6:
Audit and Accountability



SECTION 3:

IT/OT SEPARATION AND NETWORK SEGMENTATION FOR ADVANCED INDUSTRIAL SECURITY





Purdue Model for ICS Security

Despite the increasing adoption of edge computing and direct-to-cloud connectivity, the Purdue model remains relevant when it comes to ICS security.

What is the Purdue Model?

The Purdue model is a structural framework for industrial control system (ICS) security that focuses on segmenting physical processes, sensors, supervisory controls, operations, and logistics. It has long been considered essential for ICS network segmentation to safeguard operational technology (OT) against malware and other threats.

How does it secure the ICS?

At the core of the Purdue model is Operational Technology (OT), which includes systems located in critical infrastructure and manufacturing used to monitor and control physical equipment. At the top of the OT zone, we find the IT zone separated by a DMZ (Demilitarized Zone) ensuring access control between the OT and the IT zones.



Model of industrial architecture

Purdue Model ISA- 99

Architecture Example

Standard

IT

L5

Internet DMZ network

L4

Enterprise management

Industrial DMZ

L3

Operational management

L2

Supervision & Control

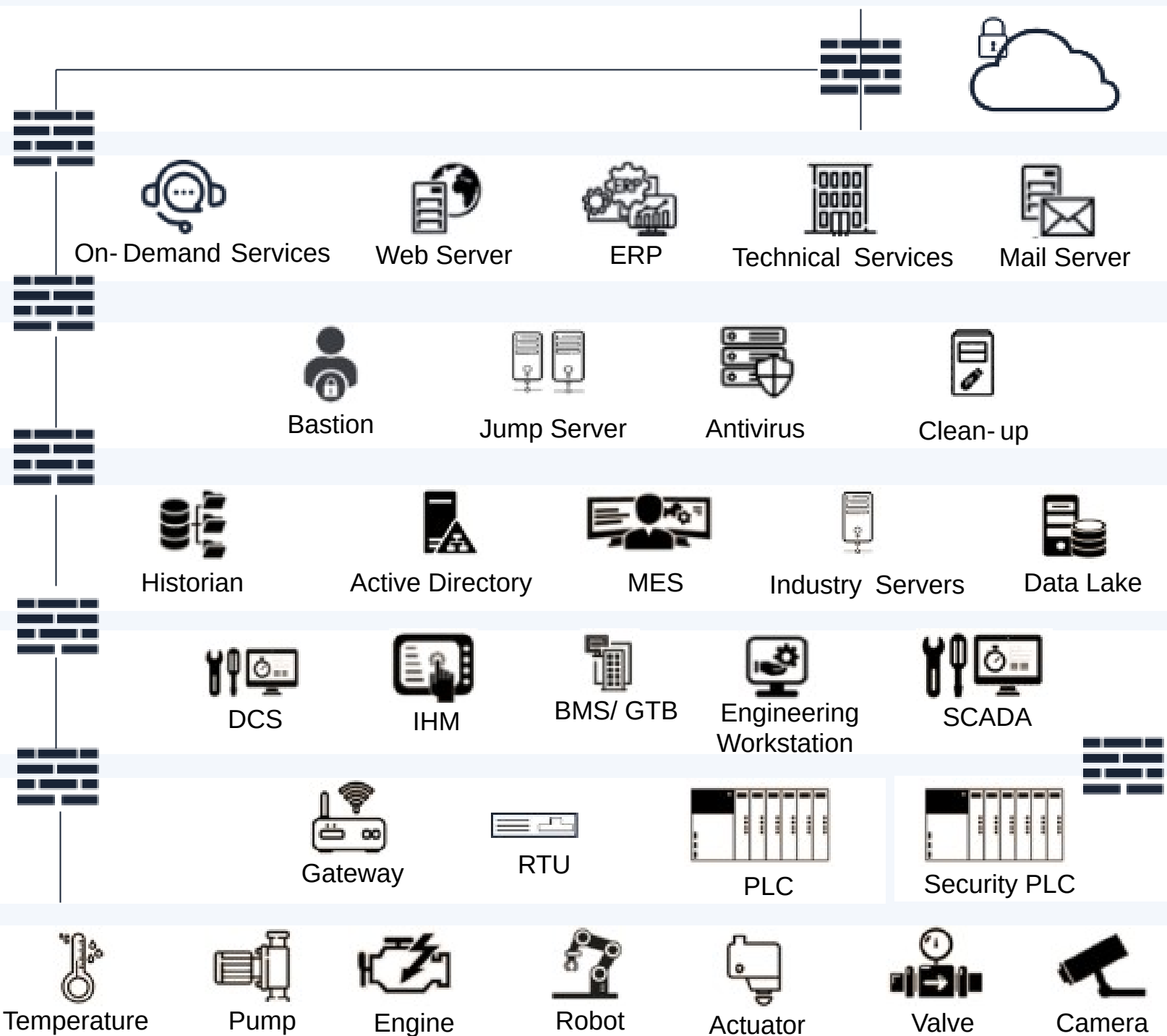
OT

L1

Basic Control

L0

Physical Process





Purdue Model for ICS Security

L0 – Physical Process: This is the physical equipment that actually does the work and is known as the equipment under control. This consists of valves, pumps, sensors, actuators, compressors, etc..

L1 – Basic Control: These are the control devices such as programmable logic controllers that monitor and control Level 0 equipment and safety instrumented systems..

L2 – Supervision & Control: Control logic for analyzing and acting on Level 1 data. Systems include human-machine interface (HMI); supervisory and data acquisition (SCADA) software.

L3 – Operational Management: This level includes systems that support site plant control and monitoring functions. Level 3 systems also aggregate lower-level data that needs to be pushed up to higher level business systems.

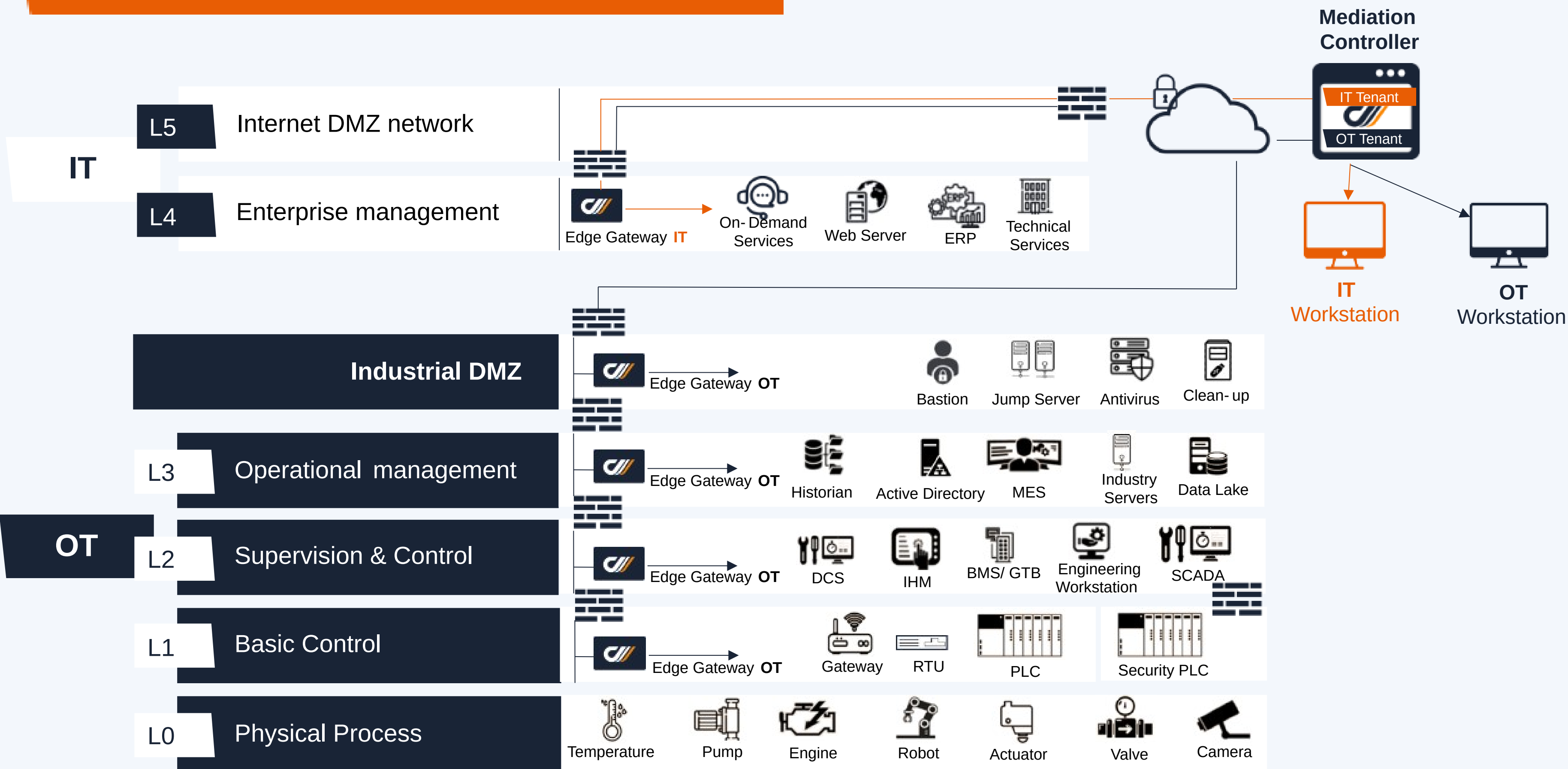
Industrial DMZ (iDMZ): acting as a barrier between the IT and the OT zones preventing any propagation of infection and blocking contamination.

L4 – Enterprise Management: Here we find IT systems that manage manufacturing logistics, communication, and data storage.

L5 – Internet DMZ Network: This level represents the enterprise corporate network. Although not an ICS environment, it collects data from ICS systems to help taking business decisions.



cyberelements PAM for OT





The cyberelements Architecture for OT

The double barrier architecture of cyberelements is specifically designed for this type of infrastructure. It includes two key components: The Mediation Controller and The Edge Gateway, which securely connect users only to the necessary resources for their tasks.

The Edge Gateway:

To maintain separation across different levels, cyberelements provides a gateway for each level. Each level will have an Edge Gateway connected to The Mediation Controller. Additionally, cyberelements allows the segmentation of several (V)LANs if/as needed, without affecting the end-user experience. The OT operator will have visibility of all OT resources through a single “pane of glass.”

The Mediation Controller:

The Mediation Controller features two separate tenants: one for the IT zone and one for the OT zone. This structure ensures that IT workforces connect to the IT zone and OT workforces to the OT zone.

Tenants can also be leveraged to segment regulated (NIS compliance) OT systems and non-regulated OT systems.





The cyberelements Architecture for OT

This unique architecture ensures:

- ✓ Double-barrier architecture with end-to-end encrypted tunneling from the end user device and the OT LAN
- ✓ Organizational (multi-tenant) and network partitioning (gateways with outgoing flows without opening network ports)
- ✓ Protection against attacks thanks to volatile and random ports, url rewriting and display offset isolation.
- ✓ Embedded zero-trust technology: least connection, JIT connection, zero standing connection.
- ✓ Clientless third-party provider access with protocol break and No port opening with no inbound flow: only outgoing traffic flow



SECTION 4:

THE DIFFERENT USE CASES



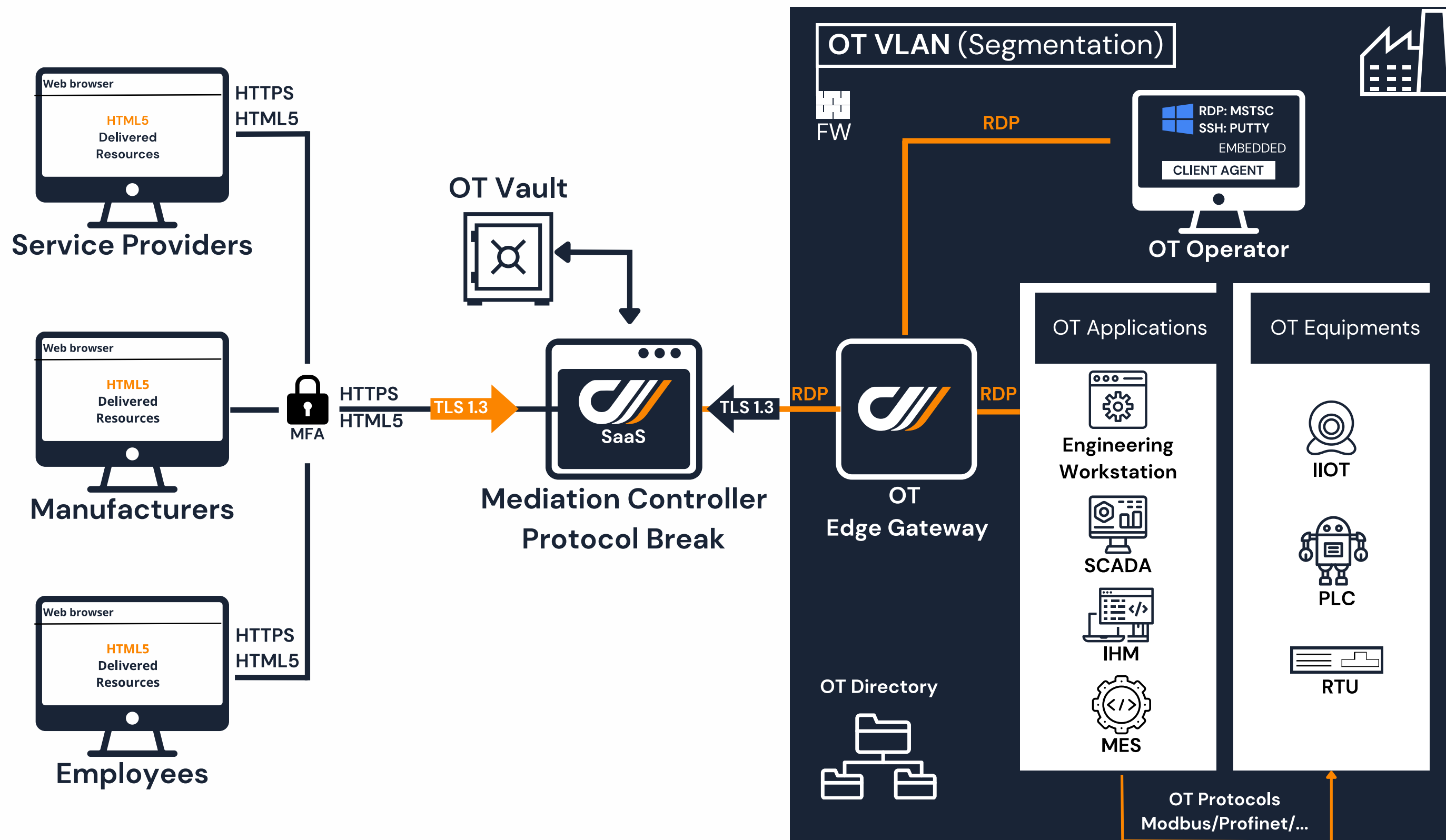
The Use Cases

In the industrial world there are three main remote access use cases. Users need to connect remotely to resources & applications to perform various types of actions: maintenance, update, monitoring, control, etc.

Users can come from third-party service providers, industrial manufacturers, and internal workforces. Even if not the preferred or nominal access, there is a growing need for securing such remote access in the industrial sector. This is why cyberelements provides a converged platform that covers all these access use cases.



Use Case 1: Giving secure remote access to an engineering workstation hosting an ICS application





Use Case 1: Giving secure remote access to an engineering workstation hosting an ICS application

In this case, the engineering workstation is located in the OT LAN and users need to connect from their devices to OT/ICS applications running on this engineering workstation.

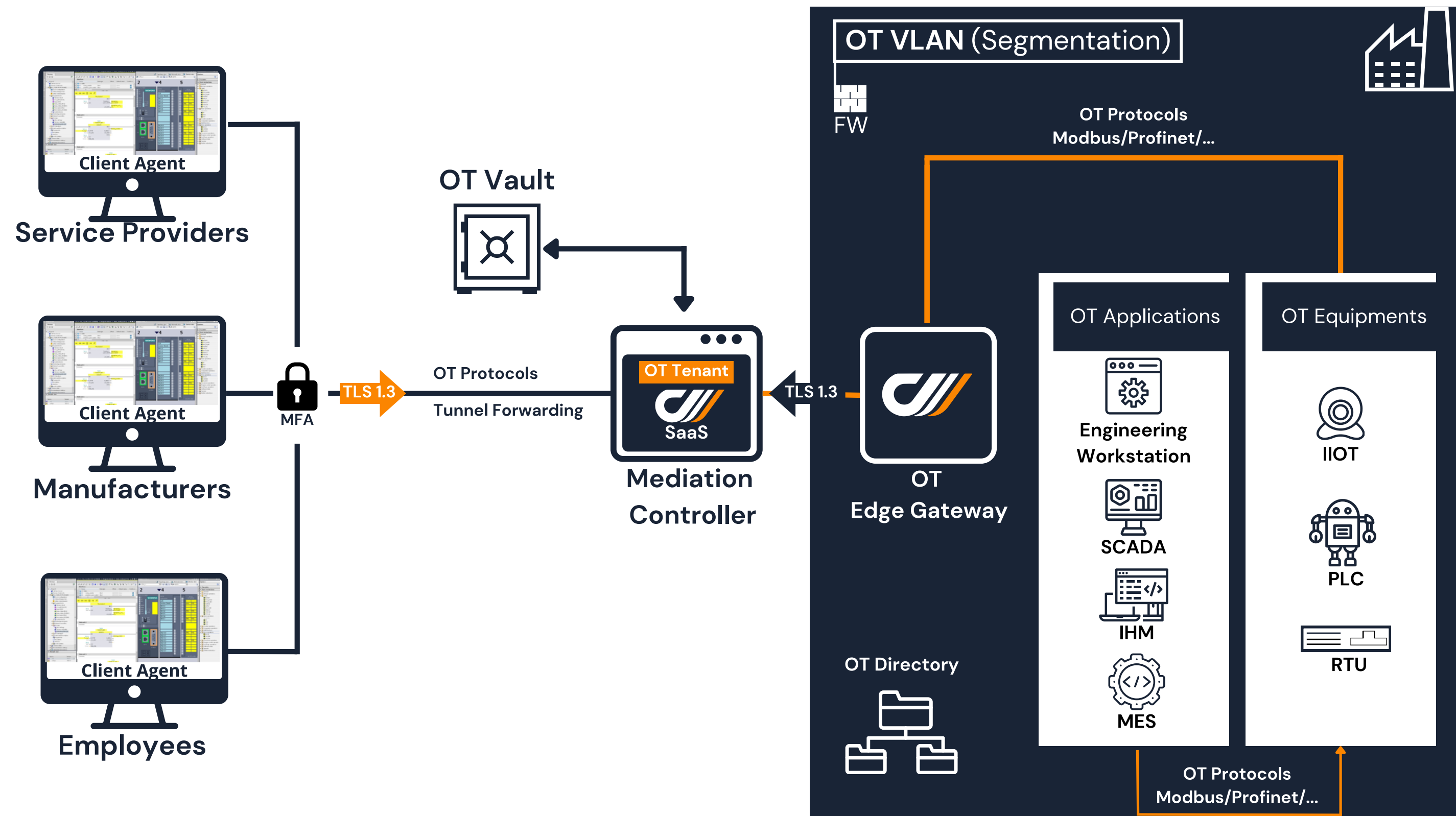
The cyberelements capability of web delivery, allows your users to securely connect from any web browser without to install any client. Once users are connected to the OT applications via cyberelements, they can perform the required actions on the OT equipment using appropriate industrial protocols. Only images are transmitted to the end user device and only keyboard and mouse flows are transmitted from the end user device.

Web delivery limits the interaction with the end user device, isolating it from the OT systems. cyberelements enacts a built-in protocol break technology coupled with url rewriting ensuring full OT protection against any contamination possibility from any infected devices.

Therefore, the cyberelements platform allows you to give a fully secure access to any type of user located anywhere in the world, whatever the device (s)he uses, provided it has a web browser available.



Use Case 2: Remote use of the manufacturer's application via the bastion



Use Case 2: Remote use of the manufacturer's application via the bastion

In the second use case, the OT/ICS applications are located in the datacenter of a contractor (service provider, vendor, ...), whose users connect remotely to the organization's OT LAN where the industrial equipments are located. In other words, users are connected from an external untrusted network. In this case access should be secured with a Privileged Access Management (PAM) solution.

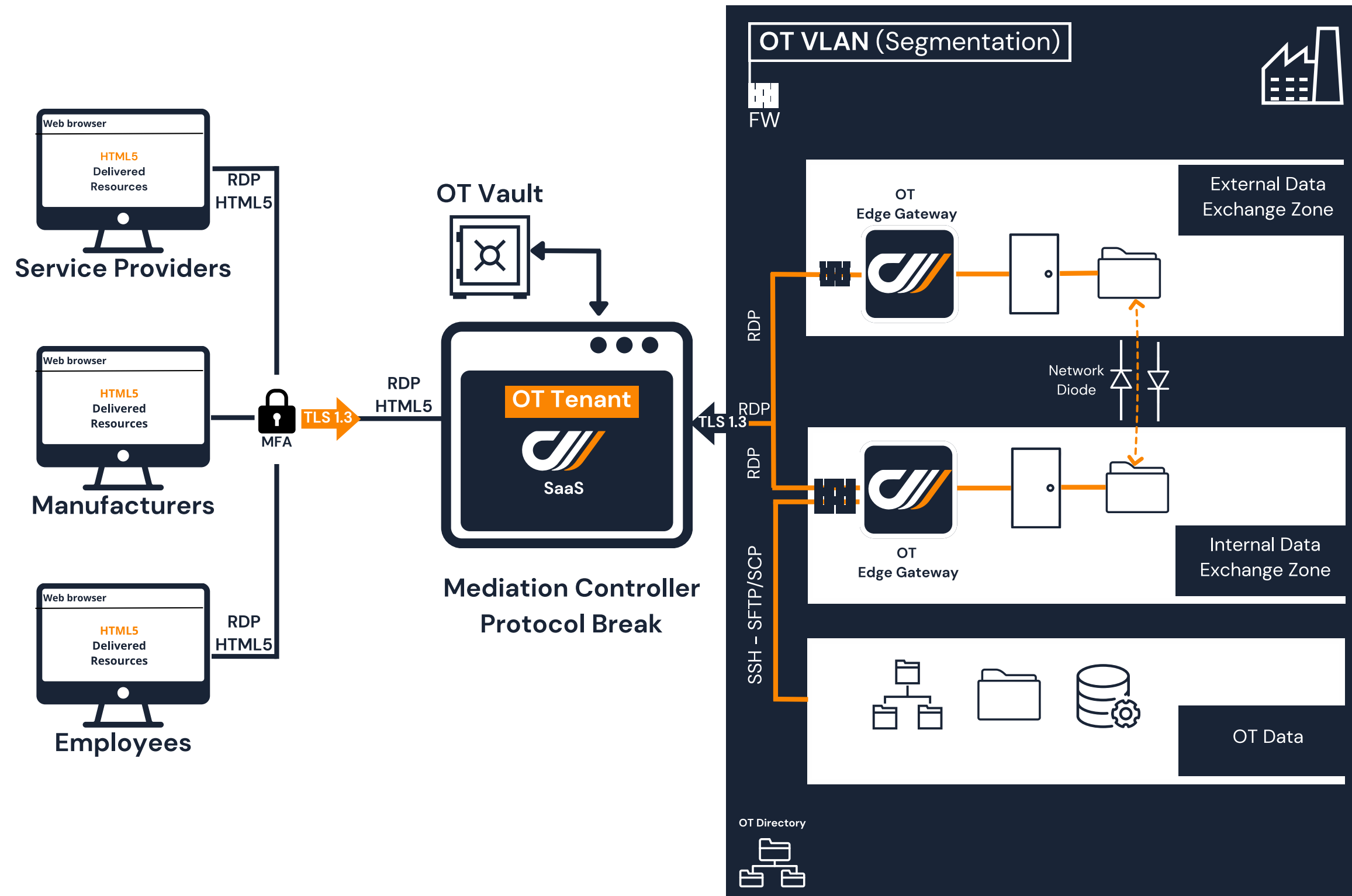
cyberelements is designed to offer such remote PAM capabilities. In such a case, an end-to-end tunnel is created between the end user device and the OT Edge Gateway deployed in the OT LAN, and the tunnel between the Gateway and the cyberelements Controller is outbound (only outgoing flows, no port opening).

The solution allows then to configure a "port forwarding" resource, which allows to convey the OT proprietary protocols all the way through the tunnel, until it reaches the Gateway which routes it to the targeted industrial equipment.

The tunnel is encrypted end-to-end, and it can be encrypted with the organization's own key, so that nobody else – including cyberelements – can "see" the flow between the applications and the PLC, for example.



Use Case 3: File Transfer Security



Use Case 3: File Transfer Security

Manufacturing companies handle highly sensitive data that must be protected with a robust security strategy. At the same time, OT infrastructures need to be maintained and updated, and this can only be done with vendors' file upload to the OT LANs. And often, data must be extracted from the OT LANs to a cloud where it can be processed, to leverage the computing power of the cloud and the AI capability of industrial analytics tools.

So, file transfer in the industrial world is unavoidable. This is where combining PAM with 'diode' (one-way) file transfer technology comes into play.

The diode technology is a cybersecurity appliance ensuring full isolation between different network zones at the physical level by ensuring unidirectional flow of data.

cyberelements provides a PAM solution that is integrated with the diodes to fully secure data transfer in the OT environment:

Users will have to connect to the External Data Exchange Zone where data will be verified before being transferred to the Internal Data Exchange zone through the diode. No other way can be used to perform data transfer.

This way, cyberelements ensures full isolation and segmentation of OT environments from the external world.






Inside the elements: A video Guide of PAM use cases in cyberelements

Watch Now



SECTION 5: **INDUSTRY STORIES**





Centralizing Remote Access to IT & OT systems for a Food & Beverage Leader

Aim: Centralizing and securing both internal and external access to IT and OT systems while guaranteeing the full IT/OT separation.

4000 employees | 15 production sites

Challenges:

- Implementation of **Zero Trust principles**.
- **Centralizing and tracing access** to target infrastructures according to the possibilities offered by **manufacturers and industrial protocols**: access to control applications on an engineering station, access to equipment from the engineering station running on **the service provider's or manufacturer's workstation**.
- Setting up **fully isolated control zones** for IT and OT.

The cyberelements solution


- Control and traceability over all the accounts and complete visibility: who did what, when and on which system. Therefore, guaranteeing the accountability of all accesses to the industrial infrastructure.
- The Implementation of Zero Trust Principles for the industrial infrastructure and the adoption of the least privilege principle.
- Centralize access to IT & OT systems from a converged platform, while guaranteeing a full separation between the two. Operational teams can thus deploy their administration tools (supervision, patch management, etc.) on production networks.



Centralizing Remote Access to IT & OT systems for a Food & Beverage Leader

Key Features:

- › Detailed access logs
- › Granular access policies
- › Device conformity check (the workstation)
 - › Just-in-Time access
- › Multi-Factor Authentication
 - › Converged platform
- › Single Infrastructure for OT and IT access security



Securing Remote Access for an International Supply Chain Leader

Aim: Implementation of a secure bastion host, compatible with the existing tools offering the best user experience, for remote maintenance.

1000 employees | 50 countries

Challenges:

- Improve and **secure remote maintenance** of software and systems deployed at customer sites.
- Offer the most seamless and fluid **user experience** possible, by enabling the use of existing tools (RDM) and **federated SSO** on an existing password vault.
- Comply with the **ISO27001 standard**.

The cyberelements solution

- Secure access to software and PLCs deployed at customers' sites: Designed for remote access, cyberelements secures access to customers' IT & OT resources for the organization and its service providers.
- Seamless, and fluid user experience allowing the use of existing tools: The integration of cyberelements and RDM is therefore "native", without disrupting the user experience: from the RDM, users can access (direct access) all their resources, without re-authentication, while relying on the existing password vault.
- A perfect seal among customers: Operating remotely and securely on various customer infrastructures. As a Managed Service Provider (MSP), customers can use the solution as well.
- Thanks to the multi-tenant ownership of the platform and the use of gateways deployed in separate LANs. Each gateway is connected to the Controller corresponding to the appropriate client, and a user only access and "sees" the resources of the organization that has given him or her the rights.



Securing Remote Access for an International Supply Chain Leader

Key Features:

- › Session Recording when accessing to RDP, SSH or web-based resources, without the need for a bounce server.
- › Recorded sessions are stored on the customer's premises and can be accessed by both the customer and the supply chain company.
 - › Credentials are managed without uncovering them.
 - › A double-barrier architecture preventing customers IT systems from exposure.
- › A clientless web interface, meaning there is no need to install it or to download it on the workstation.
- › The protocol break technology limits both the interaction with the workstation and the risk of spreading any malicious load present on the workstation.
 - › A multi-tenant solution with a gateway deployment for each separate LANs.



Energy Sector: Complying to NIS2 by securing service providers' access

Aim: Replacing existing PAM solution to secure external third party according to the NIS2 directive.

1000 employees | 21 sites | 100+ external service providers

Challenges:

- › Provide a secure remote access for external service providers to both IT and OT systems.
- › The need for a solution that has the ability to be integrated with a data transfer security solution.
- › Comply with the NIS2.

The cyberelements solution

- › A secure solution that can be seamlessly enabled in a few minutes, without any technical deployment.
- › A native Zero Trust security approach thanks to a double barrier architecture.
- › An advanced user experience allowing external service providers to securely access their resources through a web portal.



Securing Remote Access for an International Supply Chain Leader

Key Features:

- › Zero Trust architecture allowing only outgoing flow and ensuring no port opening.
 - › Clientless and serverless web session recording.
 - › Clientless service providers' access through a web portal.
- › Protocol break isolating the organization's OT LAN from endpoints preventing any contamination.
- › Seamless integration with secure data transfer solutions ("network diodes").

SECTION 6:

THE CYBERELEMENTS FEATURES





Authentication

By supporting a diverse range of authentication methods, cyberelements ensure flexibility and scalability for organizations of all sizes. This integration enables users to access applications and services effortlessly, while robust security measures protect against unauthorized access and data breaches. With cyberelements advanced authentication features, businesses can make access management more efficient and enhance security posture.

cyberelements incorporates advanced **multi-factor authentication (MFA)** technology and **biometric verification** to protect user data and prevent unauthorized access:

- Azure AD
- OTP (Mail, SMS)
- TOTP
- FIDO2
- Certificate
- RSA/Radius
- Neomia Pulse (Behavioral Biometrics)

cyberelements offers an authentication system that **seamlessly integrates with various identity sources**:

- Local/Embedded directory,
- corporate AD,
- third-party IDP

cyberelments, thanks to its **Single Sign-On (SSO/secondary authentication)** feature, ensures that third party providers get access without the need of sharing any credentials with them: **no divulcation of credentials**



Access Control

Access control is a fundamental feature of our security framework, designed to ensure that only authorized users can access critical resources within your organization.

Conditional access ensures that access to resources is granted only under secure, predefined conditions. cyberelements enhances security by evaluating the context of access requests: Device, Network, Browser, OS, AV, EDR/XDR, Location, Presence of file, Time slots

cyberelements provides Zero-trust access policies that are based on a "never trust, always verify" approach.

- least privilege, limiting access to only what's necessary
 - just-in-time (JIT) privilege, granting temporary permissions when needed
 - Zero standing privilege, avoiding ongoing elevated access.
- This approach minimizes security risks by continually validating access and avoiding unnecessary permanent permissions.

Role based access policies of cyberelements use Active Directory (AD) groups to manage permissions based on user roles. This ensures users have only the necessary access for their jobs.

The Just-In-Time (JIT) access request workflow management granting temporary access rights as needed. Users request elevated permissions, which are reviewed and approved before being granted. Ensuring that elevated access is automatically revoked after tasks completion.

Privilege elevation of cyberelements temporarily grants users higher access rights for specific tasks. Managed through structured requests and automated workflows, it allows users to perform tasks requiring elevated access while maintaining security.



Account management

In operational technology (OT), account management plays a crucial role in securing critical systems. cyberelements ensures robust account management by providing key features for managing privileged accounts, facilitating user-driven accounts, and enforcing credential policies.

Credential policy enforcement ensures that all user credentials comply with rigorous security standards. cyberelements facilitates the implementation of a credential rotation policy, which mandates the regular updating of passwords and authentication methods.

Cyberelements provides privileged accounts to users that need to access critical OT resources. These accounts allow authorized personnel to perform high-level tasks such as system configuration, troubleshooting, and maintenance.

cyberelements User-Driven Accounts introduce flexibility within the OT environment through dynamic and personal aliases. These accounts empower users to perform their roles by promptly granting and revoking in accordance with organizational policies and user needs.



Session management

Session management in cybersecurity refers to the process of managing and monitoring user interactions with a system from the time they log in until they log out. It is a crucial component for ensuring that user sessions are secure, consistent, and tracked throughout their lifecycle.

cyberelements also supports session sharing (four hands), which allows multiple authorized users to collaborate within a session. This feature ensures that critical actions are performed with the necessary approvals and checks.

Detailed audit trail, providing advanced traceability of all user activities. This feature ensures that every action taken by users is logged, allowing for precise accountability and easy tracking of changes across the system.

The session recording feature captures all interactions within a session for review and compliance purposes. The recordings are saved in a video format with advanced search possibility for forensic analysis.

Alert-driven actions on live sessions enabling real-time responses to potentially risky behaviors: Administrators are notified, and the session will be automatically paused.

The industrial sector is traditionally rooted in physical processes, with a focus on tangible outputs. This operational mindset often contrasts with the abstract world of information technology. As a result, integrating cybersecurity solutions can be a challenging endeavor. cyberelements offers a solution to bridge the gap between these two cultures.

cyberelements is a multi tenant solution allowing admins to create a dedicated instance for OT users. Through one single solution, it is possible to secure both IT and OT systems. Encapsulating by that complex IT security measures within tangible and physical devices.

By providing a centralized authentication mechanism, SSO eliminates the need for multiple logins, streamlining access to various systems and applications. This simplification aligns perfectly with the industrial preference for efficiency and straightforward processes.

cyberelements is designed with user experience in mind, prioritizing simplicity and intuitiveness. Recognizing the diverse skill sets within industrial environments, our platform offers a clean, uncluttered interface that is easily navigable by both IT and operational personnel.

cyberlements.io is the Zero-Trust and Identity-First access platform for business performance, allowing organizations to be better insured against cyberattacks without compromising workforce productivity.

It provides secure access and identity management capabilities, for both remote and on-site employees, third-party providers and industrial operators to access the business applications and privileged systems of the organization.

Start Now for Free