

7 STEPS TO IMPROVE OT CYBERSECURITY

How to secure access to your OT environment



7 STEPS TO IMPROVE OT CYBERSECURITY

How to secure access to your
OT environment

TABLE OF CONTENTS

Introduction

Step 1: Defining and developing an effective governance model	5
Step 2: Providing equipment and network topography	6
Step 3: Defining segmentation	7
Step 4: Centralizing and securing remote access	8
Step 5: Securing user access	9
Step 6: Securing Endpoints	10
Step 7: Ensuring regulatory compliance	11
Conclusion	13

INTRODUCTION

Companies in the manufacturing and production industries are being challenged to secure their operational technology (OT) environment and to face the increasing risk of being attacked.

The frequency and sophistication of attacks on operational networks have increased recently due to lack of adequate security controls, the use of proprietary protocols on the production systems that cannot be accessed remotely and the organizational misalignment and complexity. Manufacturing and production plants that are trying to close the gap between IT and OT security are encountering several difficulties:


- Lack of internal knowledge in cybersecurity requirements for adequate defense of OT assets
- Absence of robust security frameworks for IT connected OT assets that result in production environment vulnerabilities
- OT Cybersecurity is resource-intensive and without the appropriate guidance the security requirements are relegated to a second place in comparison with the business objectives.
- Without a strong cybersecurity strategy, vulnerabilities on OT systems may go undetected for months or years until they are exploited by hackers to disrupt critical operations, steal data or demand a ransom.
- More and more devices and sensors are interconnected making the threat landscape riskier.

There are many examples of intruders exploiting OT vulnerabilities, gathering information and preparing attacks without being detected. The two most well-known attacks are perhaps Colonial Pipeline and the Florida water treatment plant in the United States, where attackers exploited long-standing vulnerabilities that could have been prevented with software patches, stringent security for remote access and strong multifactor authentication.



Recently a sophisticated attack was carried out against Kiev Power Plant where hackers targeted employees to take over their accounts, then they escalated regular user privileges and laterally moved to OT system to compromise vulnerable devices and caused a power outage.

These examples clearly illustrate the impact of cyberattacks on critical infrastructure and demonstrate the need for an IT/ OT cybersecurity strategy and a security program that help to improve the security posture and resilience to attacks. They also highlight the



“Without a strong cybersecurity strategy, vulnerabilities on OT systems may go undetected for months or years until they are exploited by hackers to disrupt critical operations, stole data or demand a ransom.”

importance of securing identities and controlling remote access to all assets. Cyber-attacks also lead to reputational damage.

In this whitepaper, we offer expert advice on the key steps you need to follow to secure your OT with a special focus on the important role that plays the identity and access management technology.



Step 1: Defining and developing an effective governance model

There are many governance models and compliance requirements for information technology systems that have been adopted globally, however the rapid introduction and convergence of operational technology (OT) to traditional IT networks have created additional challenges to integrate security controls.

Developers of OT devices have largely ignored implementation of security controls in favor of efficiency, reliability, and reduction of

complication to ensure operational capabilities. This lack of control and the variance in technology and capability between devices make it difficult to implement required security controls from governance models without consideration of these specific challenges.

It is beneficial to organizations to look towards a baseline of security policies and procedures so that an inclusive guideline and a well-prepared security program are readily available to staff and administrators. Ultimately, these policies and procedures are focused on the detection, response, and prevention of cybersecurity incidents. Adoption of security governance models and inclusion of standard and evolving hardening techniques for OT devices enable visibility, security control, and response capabilities of an entire environment.

At the base, explicitly written delegation of cybersecurity responsibilities for both implementation of controls and individual roles and responsibilities for monitoring and response to incidents is important for organizations to establish and enforce cybersecurity. These roles and responsibilities determine at the core whether governance will be fully implemented. Within these roles and responsibilities, IT and OT administrators need to have established communication channels to effectively detect and respond to cybersecurity incidents. These communication channels for incident response management should include procedures for reporting of and responding to potential incidents.

Once established roles and responsibilities are developed and finalized, training of all staff

on cybersecurity incident response procedures, threat awareness, and incident reporting channels enhances an organizations overall cybersecurity posture.

Overall, the development and adoption of an effective governance model is dependent on the resources of an organization, currency and completeness of procedures, and training for real-world and applicable scenarios for all staff.



Not only are organizations required to implement cybersecurity programs to protect their assets, reputation, and data, but also to address globally evolving governance, risk and compliance requirements.

Step 2: Providing equipment and network topography

Industrial networks are built slowly as production grows and service providers in charge of deploying new production lines have

deployed heterogeneous brand equipment, network components and process infrastructures from different manufacturers. The result is a multitude of industrial equipment that interconnects together and generates data flows for production, supervision, or industrial control. Interconnection between these networks enables production global digitization of industrial production, and thus the optimization of processes for the purpose of competitiveness and control of raw material and energy consumption.

You can't protect what you can't see - when these networks and devices are scaling at an exponential rate by adding sensors, actuators, and other complex connected operational technologies it is required to adopt solutions that help to gain visibility and control to administrate, maintain and secure resources. Analysis of interconnections and traffic specifics will help to detect new or malicious assets in the industrial control systems (ICS) network

There are many networks topography tools available to regularly scan networks and map out visibility for use by IT and Cybersecurity resources to identify efficiencies, vulnerabilities and threats.

Governments are beginning to see the importance of supply chain risk, data security risk, and privacy risks related to cybersecurity threats which are directly impactful to socioeconomic systems across the globe. With this impact comes a prescribed mitigation

strategy that is mandated for continuation of business operations in many jurisdictions. Organizations must address these mandates quickly and decisively, gain a return on investment in technologies and personnel resources, and be effective in eliminating or significantly reducing the attack surface and vulnerabilities.

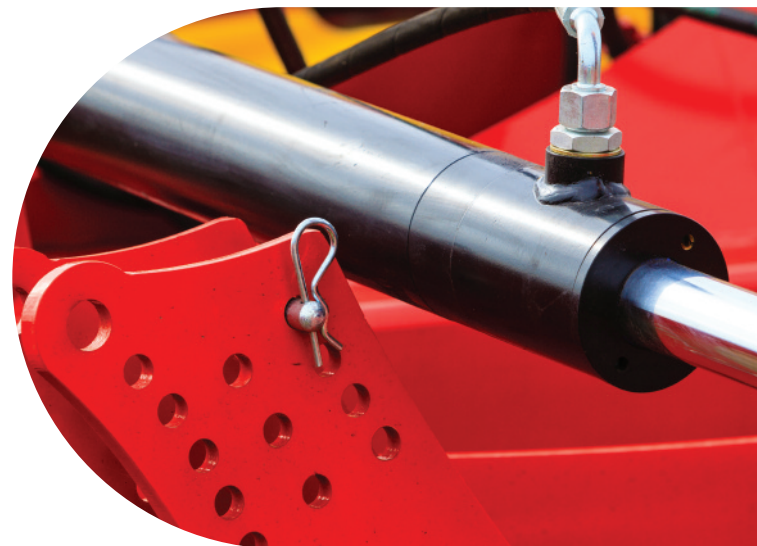
The governance, risk management and compliance (GRC) requirements and the scaling of these networks and devices are growing the need for understanding the risk associated with the full attack surface and threats capable of exploiting vulnerabilities within an OT environment.

Step 3: Defining segmentation

It is advisable to first consider the IT/OT segmentation. More and more data is being used by business tools such as ERP, CRM, IT databases, etc. Similarly, flows for the administration and supervision of the IT/OT systems are going back to the administrative network. It is essential to finely control these exchanges and to reduce them as much as possible in order not to disrupt the production network.

A demilitarized zone (DMZ) dedicated to the OT, also called iDMZ, will naturally find its place at the interface of the IT and OT networks. High availability firewalls and a set of relay components between IT and OT tools (directory / file servers / decontamination server / ...) will be deployed there.

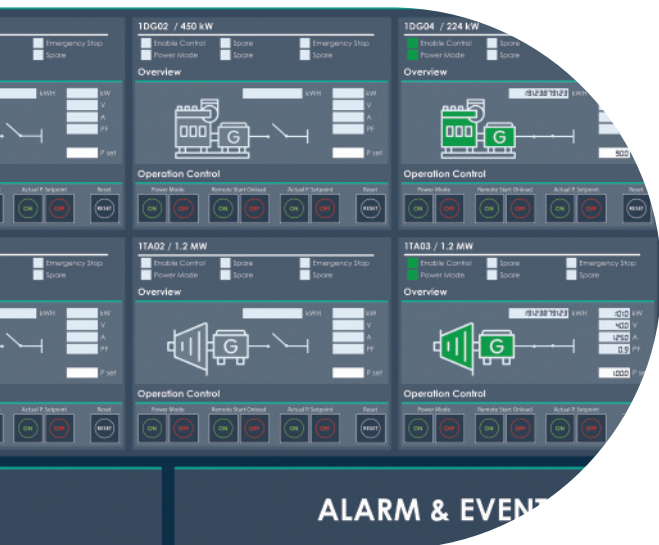
In a second phase, a second process-oriented segmentation will be implemented to partition the flows and components according to the business applications in place. The objective is to maintain active and functional processes in the event of a compromise of a station or a component. The network functionalities from the level 2/3 switching equipment will allow the deployment of VLANs and associated routing. Industrial firewalls capable of interpreting proprietary protocols can also be deployed close to process equipment. Further, security of this segmentation can be achieved through identity and access management through provisioning of public key infrastructure to uniquely identify, authenticate and authorize devices, gateways, and network infrastructure components to communicate internally and



externally. Validated identification of these endpoints is a key piece to securing and ensuring segmentation between them and it is a foundation for zero trust network architectures.

Adopting Identity and access management technologies helps to prevent unauthorized access to the networks, data and applications and reduce the risk of malicious software installation.

remote access solution with a gateway for mobile operators, industrial integrators, or machine builders to perform maintenance operations.



Numerous remote access solutions have emerged in recent years, mainly in the form of VPN access based on an industrial equipment deployed onsite on the production line with an authentication phase on the Internet ensuring the connection to the VPN for any referenced user. However, even if the data encryption within the VPN guarantees a certain level of confidentiality, this type of solution quickly reaches its limits and it's no longer sufficient to ensure production security because it creates points of exposure and leaves the network vulnerable to attack by granting unnecessary rights to users.

Step 4: Centralizing and securing remote access

Ensuring seamless production continuity, optimizing production, reducing raw material consumption, etc. are all industrial challenges to be addressed in a complex context of rationalization of skills and expertise, the COVID-19 pandemic, globalization, and the multiplication of production sites.

In addition, credentials will necessarily be shared, giving access to unreferenced users or third parties. It is very common for an integrator to share an account with a manufacturer to solve a production issue.

Remote accesses in this type of environment has naturally become a widespread practice today.

After the pandemic, remote access tools were particularly targeted, and many vulnerabilities disclosed. The deployment of remote access tools in OT environment increases the global attack surface.

Nowadays, maintaining, programming, and troubleshooting equipment does not necessarily require physical presence at site. Instead manufacturing and production plants can adopt

We can distinguish in particular:

- The multiplication of this type of access, uncontrolled and often not referenced by the OT teams
- The non-centralization of all these access rights
- Basic authentication, which does not

- ensure the real identity of the provider
- A lack of visibility and traceability of the provider's activity
- The inability to control third party providers

This calls for a simple, centralized, secure remote access solution that streamlines privileged access to critical production systems, irrespective of their disparate network topologies. Turning to **Privileged Access Management (PAM) solutions**, which are based on protocol break offers definitively a much more secure environment.

Step 5: Securing user access

Setting up user accounts and credentials, as well as authentication and permission measures, ensures that only authorized employees can access machines and systems.

Authentication mechanisms based on multiple factors ensure that only the authorized provider, or the machine manufacturer can gain access and perform maintenance or change parameters. Multiple authentications based on a second ownership factor (e.g., smartphone validation) should be preferred. The authentication will then be completed by mechanisms to control the user's path.

Maintaining a production line means providing secure access at any time and from any location. Remote connections may require prior approval for increased security. After specifying the user's intentions and the desired connection time, the

approver(s) will authorize the connection based on the rights associated with the user's profile.

Indeed, the user does not know the login and password of the components he wants to access. The PAM solution relies on a secure digital vault to store this information and establishes the session for the user by granting him the rights he needs to perform his action.

No more shared admin passwords or post-its in the production environment!



Those solutions also manage an essential part of password hygiene: rotation. Introducing a password management solution to control and manage secrets, passwords and credentials is fundamental. It helps to generate new passwords at defined intervals. The famous "admin" password will only be known by the PAM solution and will remain of higher complexity.

The PAM solution acts as a proxy and ensures a protocol break. It is therefore easy to control the protocols and sub-protocols available to the user. Since the solution can track user actions, it is easy for them to compare behavior with that defined as normal. Connections from foreign IPs or at odd hours are detected, which can be indicators of compromise or attack.

The user's journey is thus secured from end to end, while relying on the "Zero Trust" concept. The zero Trust approach assumes that no activity is by default legitimate – and therefore requires to be proven otherwise before allowing privileged access to sensitive resources. Zero Trust demands equal opportunity verification of credentials, identity, and permissions. It's important to note that Zero Trust does not assume that all users are bad actors; rather, it simply requires that access to a privileged resource is appropriate.

In addition to the Zero trust approach, it is highly recommended to set up a precise traceability of all sessions. Session traceability is ensured within PAM solutions, which provide a complete history of connections, thus enabling compliance with legal requirements. In the same way, the complete recording of sessions and actions ensures total visibility and are very useful for analyzing a cyberattack, or simply an intervention error. PAM gives you the ability to track every activity conducted by every type of privileged account.

Finally, a PAM project in OT is as much technical as organizational. It goes from passwords sent by e-mail to a solution that allows privileged users to respect security rules. To facilitate the adoption

of such a solution, it is necessary to anticipate the obstacles that may appear upstream. It is therefore imperative to clearly define the objectives and challenges of this type of project.

The deployment of a privileged access management solution centralizes and secures all remote accesses used daily in the IT environment.

Step 6: Securing Endpoints

Securing remote access does not allow to secure workstations which remain vulnerable to internal threats such as:

- The use of external devices (USB keys, disks)
- Malware propagation through the network
- Inappropriate user behavior (bouncing, overprivileged identities)
- Leveraging legacy OS vulnerabilities

The criticality of those workstations directly engages the production, and it is not possible to tolerate a compromise on this type of components.

It is therefore essential to secure the behavior and operating systems of those endpoints, while considering the constraints that characterize the OT environment:

- Use of real-time protocols
- Internet connectivity often non-existent
- Operating systems based on product life cycle and therefore old and not updated
- Machines not managed by a domain controller

PAM solutions can reduce user rights and restrict behavior on target machines. Thus, bouncing, elevation of privileges attempts, or the execution of certain applications (e.g.: modification of the registry) can be banned and alerts can be generated if necessary.

perform each person's job (i.e., establishing role-based access control and configuring each role based on the principle of least privilege)", in effect, emphasizing the need for controlled privilege access. By facilitating the least privilege, PAM is a critical component of compliance.



To complete these restrictions and approach a more detailed security, it is advisable to rely on an agent to be deployed on the machine, and which, unlike traditional antivirus, EDR, XDR, will apply the Principle of Least Privilege (PoLP).

The concept of Least Privilege is a practical component of most cybersecurity regulations. Section 5.6 of the NIST Standard, for example, discusses the need for "Defense in Depth," recommending that OT security managers understand and defend against "attacks on privileged and/or shared accounts." The standard includes a recommendation for "Restricting ICS user privileges to only those that are required to

The Principle of Least Privilege states that a subject should be given only those privileges needed for it to complete its task. In other words, any user, program, or process should have only the bare minimum privileges necessary to perform its function. This makes it possible to finally control applications (whitelisting/blacklisting), processes and services to harden the machines, and only authorize the programs and behaviors necessary for the proper functioning of production.

Many malwares rely on privilege elevation mechanisms, and/or data encryption, can thus be defused before their execution. Implementing and maintaining critical control of PoLP help containing attacks at early stages and stopping them from spreading to the OT systems.

Endpoint security is part of the "defense in depth" principle and it complements remote access security and network segmentation.

Step 7: Ensure regulatory compliance

As previously mentioned, addressing cybersecurity concerns in operational technologies is an increasing effort by governments around the globe

and they continue to produce and evolve cybersecurity governance requirements and standards some of which include:

- **The IEC 62443** provides a single, harmonized set of standards to meet global and government security requirements. It simplifies procurement specification processes by establishing corporate standards and definitions that all stakeholders can easily understand.

The IEC 62443 standards provide common terminology and define the process of implementing OT cyber security. They describe how security practitioners, system integrators and control system manufacturers should interact to ensure security and safety – from the level of components, right up to entire facilities. The standards include guidelines for industrial automation security management systems and for the security architecture of the industrial network. They include definitions for security requirements across the complete system and throughout the entire lifecycle of components.

- **NIST's Guide to Industrial Control Systems (ICS) Security** helps industry strengthen the cybersecurity of its computer-controlled systems. By providing guidance on how to tailor traditional IT security controls to accommodate unique ICS performance, reliability, and safety requirements, NIST helps industry reduce the vulnerability of computer-controlled systems to malicious attacks, equipment failures and other threats.

- **MITRE ATT&CK for ICS** is a knowledge base useful for describing the actions an adversary may take while operating within an ICS network. It's an

overview of tactics, techniques, and mitigations that can be met and apply in the OT cyber kill chain.

These tools and standards are used as part of a process of compliance with local regulations, including:

- **EU's General Data Protection Regulation (GDPR)** of the European Parliament and of the Council of 06 April 2016. The Regulation is designed to harmonize data privacy laws across Europe for the protection of individuals regarding the processing of personal data and the free movement of such data.

- **EU Network and Information Security directive** is the first piece of EU-wide cybersecurity legislation. Every EU member state has started to adopt national legislation, which follows or transposes the directive through three pillars: National capabilities / Cross border collaboration / National supervision of critical sectors.

- **U.S. Health Insurance Portability and Accountability Act (HIPAA)** is an act that protects people covered by health insurance and makes rules about storing personal medical data. Internal audits play a key role in HIPAA compliance by reviewing operations with the goal of identifying potential security violations. With these regulations come penalties and non-compliance financial, reputational, and data security risks.

A cybersecurity program based on governance guides organizations to a successful strategy to reduce risk rather than attempting to develop a customized program internally. Implementation of some or all the solutions mentioned in this paper pave the way to a regulatory compliant organization and reduces cybersecurity, legal,

data security, and financial risk while enabling organizations to prevent, detect, and respond to cybersecurity incidents rapidly thus minimizing impact.

Conclusion

The convergence of OT & IT represents a true revolution in technology and requires (?) automation. But, like many advances in industry, it creates new risks. The distributed, multi-entity, multi-device configuration of OT networks increases potential security vulnerabilities which can be exploited for unauthorized access.

WALLIX with its PAM4ALL solution and ATOS join forces to help manufacturing and production plants secure their OT environments, defend systems against internal vulnerabilities and those originating from a perimeter server or device. This collaboration lowers business risk through cyber and operational incident prevention, and ensures simplified compliance.

About WALLIX

A software company providing cybersecurity solutions, WALLIX is the European specialist in digital Identity and Access Security Solutions. WALLIX's technologies enable companies to respond to today's data protection challenges. They guarantee detection of and resilience to cyberattacks, which enables business continuity. They also ensure compliance with regulatory requirements regarding access to IT infrastructures and critical data. WALLIX has a strong distribution network of more than 300 resellers and integrators worldwide. Listed on the Euronext (ALLIX), WALLIX supports more than 2000 organizations in securing their digital transformation.

OT Security is a WALLIX brand dedicated to the security of digital access and identities in industrial environments.

ot • security
by WALLIX

WWW.OT.SECURITY



About Atos

Atos is a global leader in digital transformation with 112,000 employees and annual revenue of c. € 11 billion. European number one in cybersecurity, cloud and high performance computing, the Group provides tailored end-to-end solutions for all industries in 71 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea), listed on Euronext Paris and included in the Next 20 Paris Stock index.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.