From Legacy to Leading Edge:

Challenges & Solutions in OT Security

Security at the core. Corsha™

For decades, shop floors have been built as isolated enclaves of equipment that are difficult to monitor, patch, program, or analyze. Today, Industry 4.0 is reinventing how businesses and the shop floors design, manufacture, and distribute their products. The Industrial Internet of Things (IIOT), digital engineering platforms, the cloud, AI/ML, robotics, and automation are integral parts of the digital manufacturing thread.

This digital revolution, now being called Industry 4.0, is reshaping traditional industrial systems with a wave of innovation. From manufacturing to supply chain management, connectedness and digital technologies are not just an option – they're a necessity to stay competitive in today's fast-paced world.

The Challenge - Manufacturing equipment is not designed with cybersecurity in mind. Yet with the increased connectivity, effective cybersecurity and most importantly strong Identity and Access Management is critical. In 2020, incidents targeting OT and industrial control systems surged by a staggering 2,000%. [1] According to a recent report, OT environments have become very attractive targets, as they present immense financial potential. This explains why in the past year alone, 70% of industrial organizations fell victim to cyberattacks. 26% face attacks weekly or more. Beyond the immediate consequences of data and revenue loss, these attacks disrupt the continuity of business operations [2].

Several key drivers are fueling the adoption of digital technologies in industrial systems:

Operational Efficiency

Moving past air-gapped enclaves and embracing secure connectivity allows for tedious manual operations today like security scanning, updates, monitoring to be centralized and automated.

Controlled Third Party Access

Vendors often need access either physical or remote to update, configure, and troubleshoot their systems. Enforcing digital identity and access management on third party systems and access reduces risk of external attack vectors being introduced into the equipment or network.

Data-Driven Insights

Applying modern data analytics, system modeling, AI/ML techniques, and more can optimize operations, reduce downtime, minimize configuration errors, and enhance overall efficiency.

Predictive Maintenance

Secure connectivity and real-time data can help anticipate/prevent equipment failures or downtime and maximize efficiency.

Supply Chain Optimization

Bringing in modern digital engineering systems enable companies to easily share and manage technical data packages, optimize supply chains, reduce costs, and respond to market demands swiftly.

1. "X-Force Threat Intelligence Index 2020," IBM Security, February 2020.
2. The State of OT Security 2024' paloalto networks / ABI Research.

As enterprises look to adopt Industry 4.0 processes and technologies into their industrial workflows, securing the communication and data flow across OT and IT systems is the new challenge. Unlike laptops and servers, OT equipment traditionally have long lifetimes often exceeding a decade.

Even if patches or upgrades are available, OT operators may hesitate to implement them due to risk of breaking production lines. OT equipment also leverage network protocols vastly different from traditional IT networks. As OT and IT networks come together, robust cybersecurity measures that balance the unique needs of OT infrastructure with IT security concerns are critical to the adoption of Industry 4.0.

Understanding the OT Landscape

Operational Technology (OT): The Backbone of Industrial Production

Operational Technology encompasses the hardware and software systems designed to manage, monitor, and control physical devices and processes.

OT systems encompass Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems, Programmable Logic Controllers (PLCs), and more. These systems are designed for real-time operations, process automation, and control tasks, making them the backbone of manufacturing, energy, utilities, and transportation sectors.

Challenges in Securing OT Communication

The convergence of OT and IT infrastructure comes with unique challenges, particularly when it comes to securing communication and data flow. Let's delve into these challenges one by one:

Legacy Infrastructure

Legacy OT systems often predate modern IT frameworks, resulting in compatibility issues. OT equipment was not designed with modern cybersecurity controls like strong identity and authentication in mind. Networking these systems with IT infrastructure often requires retrofitting modern security practices onto these OT enclaves.

Long-term Lifecycles

OT have traditionally existed on a more static, long-term schedule than IT systems. While IT systems are accustomed to frequent updates and patches, OT equipment often remains static for stability reasons and has a much longer shelf-life than a server or a laptop, think decades over years because of the cost to refresh.

Optimizing for Uptime

OT systems operate in real-time environments where microseconds can make a difference. Security measures that introduce latency or disrupt processes can lead to catastrophic even physical damage. The environment demands a careful balance between cyber and real-time operations to not adversely impact critical control flow and data movement.

Lack of Protocol Standardization

In the realm of OT, a lack of standardized protocols and diverse connections mechanisms from ethernet to serial and further a reliance on proprietary vendor protocols hinders the implementation of uniform security measures. OT protocols vary widely across sector and vendor. Standards like OPC-UA are promising but still gaining broader adoption.

Asset Complexity

Industrial environments encompass a diverse array of assets, from legacy machinery to modern IoT devices produced by a diverse set of vendors. Each asset has different security capabilities and operational requirements. Cybersecurity solutions need to support this complex compatibility matrix.

Implications of Unprotected Communication

Picture a scenario where a manufacturing plant's OT systems, responsible for controlling critical machinery, are compromised due to unsecured communication with the organization's IT infrastructure. The potential outcome? Production halts, deadlines are missed, and revenues plummet. The interconnectedness that fuels efficiency transforms into a vulnerability that disrupts operations and erodes productivity.

Seamless connectivity across a shop floor, centralized dashboards of uptime, health, and job progress, the real-time flow of data into digital twins in the cloud are the symbols OT efficiency and innovation. Yet, within this vision comes a new risk – unprotected and vulnerable access to OT assets. The consequences of neglecting security measures in this arena can ripple far beyond the surface, impacting operations, physical safety, critical infrastructure, and regulatory compliance.

Data Breaches and Loss of Intellectual Property

Exposing OT equipment on a network also exposes access to sensitive operational data. Imagine a cybercriminal gaining unauthorized access to OT systems, stealing runtime job data or proprietary designs. Such a breach not only jeopardizes operational stability but also exposes valuable intellectual property or supply chain data to theft.

Safety and Human Risk

In industries like energy, healthcare, and transportation, unsecured OT to IT communication poses direct threats to human safety. A hacker gaining control over critical energy infrastructure as in the case of the Colonial Pipeline [3], water plants [4], transportation systems, or medical devices can put human lives at risk.

Regulatory Violations and Legal Consequences

The regulatory landscape is evolving rapidly, with compliance requirements becoming more stringent. [5] Organizations failing to secure OT to IT communication may find themselves on the wrong side of regulatory bodies and put ongoing operations at risk.

3. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years
4. https://www.nsf.org/blog/consumer/water-utilities-cyberattack-target
5. https://csrc.nist.gov/news/2024/the-nist-csf-20-is-here

Reputation Damage

News of a cyberattack due to unsecured OT to IT communication can spread like wildfire. Customer trust takes years to build and seconds to shatter. A security breach can lead to a loss of credibility, customer exodus, and a tarnished brand image

Financial Losses

The financial implications of unsecured communication can be substantial. Beyond immediate revenue loss due to disrupted operations, organizations must also factor in the costs of incident response, recovery, regulatory fines, and potential legal battles.

As industries continue to evolve, the integration of OT and IT must be guided by the principle that secure connectivity is not an option but an imperative.

Securing OT to IT Communication

There are a range of strategies organizations can adopt to enhance the security of OT to IT communication.

Identity and Authentication

Identity for machinery and critical infrastructure systems is often limited to static network identifiers like IP addresses or MAC addresses and occasionally basic authentication like passwords. These are easily stealable and spoof-able and easy targets for adversaries. Although OT communications are largely machine-to-machine and automated, controls like role-based access, least privilege, and multi-factor authentication provide the necessary parallels from human identity and access management.

Observability and Continuous Monitoring

For many OT ecosystems, the first step is to develop a digital inventory of all the equipment and assets under operation. Then real-time monitoring is an indispensable aspect of modern IT networks and security operations centers that translates well to OT environments with the added benefit of providing real-time visibility into networked production lines and critical infrastructure.

Network Segmentation versus Isolation

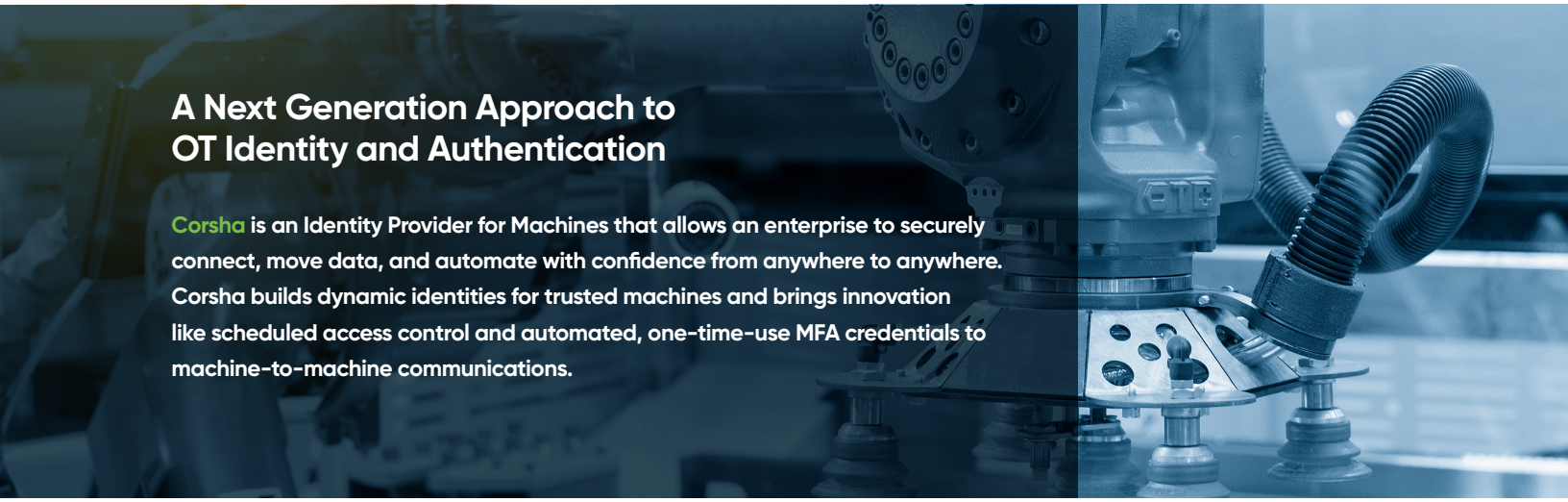
Network segmentation is like creating isolated zones within a network. This strategy helps thwart cyber attackers by restricting their movement across different segments and significantly reduces the blast radius and potential damage in the event of a breach. Specifically for OT networks this could help to further isolate high-risk enclaves or equipment offering a layered defensive alternative to air-gapping.

Collaboration and Training

Establishing a collaborative environment between OT and IT teams fosters a shared responsibility for security. Regular training sessions keep employees informed about evolving threats, best practices, and the importance of adhering to security protocols.

As industries continue to embrace digital transformation, securing the communication and data flow across OT ecosystems is critical to open up connectivity between OT and IT networks. In effect, cybersecurity has the unique opportunity to not be a blocker but a bridge to Industry 4.0.

About Corsha



A Next Generation Approach to OT Identity and Authentication

Corsha is an Identity Provider for Machines that allows an enterprise to securely connect, move data, and automate with confidence from anywhere to anywhere. Corsha builds dynamic identities for trusted machines and brings innovation like scheduled access control and automated, one-time-use MFA credentials to machine-to-machine communications.

Corsha's mission is to secure data in motion and bring zero trust to critical machines, systems, and services. Today Ops and security teams often are forced to compromise by using static, long-lived, or static identifiers like IP addresses, MAC addresses, keys, tokens, and certificates as weak proxies for machine identity and access. Corsha helps teams move past insecure secrets and generates dynamic identities for trusted machines, bringing innovation like automated, one-time-use MFA credentials, scheduled access, and deep discovery to machines. The Identity Provider also offers visibility and control over automated traffic and enables real-time revocation of access and rotation of identity without disrupting other workloads.

Whether it is across hybrid cloud infrastructure, data centers, or your manufacturing shop floors, Corsha reimagines machine identity to keep pace with the scale of data and automation needed for Industry 4.0. The platform ensures automated communication from anywhere to anywhere is pinned to only trusted workloads, servers, controllers, and more. Corsha's Identity Platform helps an organization move past outdated secrets management approaches and unlock secure connectivity, zero trust, and data movement at scale.

Reach out to us to learn more about how Corsha's technology can act as a cyber bridge for you in crucial automation and data movement workflows within and beyond your OT ecosystem.

To learn more about Corsha's approach to securing OT to IT communication request a demo here

Security at the core.

Corsha™