cpl.thalesgroup.com

THALES
Building a future we can all trust

Reducing Risk of Breach from Identity Compromise in Manufacturing IT, OT & ICS Environments

White Paper

Contents

Who should read this paper?

The Manufacturing Sector is crucial to the economic prosperity and continuity of all countries. Products made by this sector are essential to many other critical infrastructure sectors. An attack on or disruption of certain elements of the manufacturing industry could disrupt essential functions across multiple infrastructure sectors, affecting supply chains, the national economy and security.

The table below provides an overview of the industries that serve as the core of the Critical Manufacturing Sector[1]:

Manufacturing Sector	Industries
Primary Metals	Iron and steel mills and ferro alloy manufacturing Alumina and aluminum production and processing Nonferrous metal production and processing
Machinery	Engine and turbine manufacturing Power transmission equipment manufacturing Mining, agricultural, and construction equipment manufacturing
Electrical equipment, appliance, and component	Electric motor, transformer, and generator manufacturing
Transportation equipment	Vehicles and commercial ships Aerospace products and parts Locomotives, railroad, and transit cars Rail track equipment manufacturing

Decision makers in the Manufacturing Sector should prioritize building a strong cyber security and resilience posture. Their efforts must focus on the identification, assessment, prioritization, and protection of these industries against risks and vulnerabilities to include physical, cyber and personnel threats.

1 https://www.cisa.gov/critical-manufacturing-sector

Introduction

The 2022 IBM X-Force Threat Intelligence Index report unveils that critical manufacturing was the most targeted industry in 2021[2]. Phishing was the most common cause of cyberattacks, paving the way for a growing percentage of ransomware attacks.

IBM's report findings demonstrate that credentials are a top target for cyber criminals. Indeed, another report from Kaspersky highlights that operators of spyware campaigns targeting industrial enterprises hunt for corporate credentials, sending spear phishing emails with malicious attachments from already compromised corporate mailboxes. In fact, phishing campaigns, vulnerability exploitation and compromised credentials are the top three infection vectors leveraged by adversaries seeking to disrupt national infrastructure. More than 50% of attacks against critical infrastructure begin with leveraging user credentials.

Spyware campaigns target industrial enterprises and hunt for corporate credentials, sending spear phishing emails with malicious content from already compromised corporate mailboxes.

Top infection vectors, 2021 vs. 2020

Breakdown of infection vectors observed by X-Force Incident Response, 2020-2021 (Source: IBM Security X-Force)

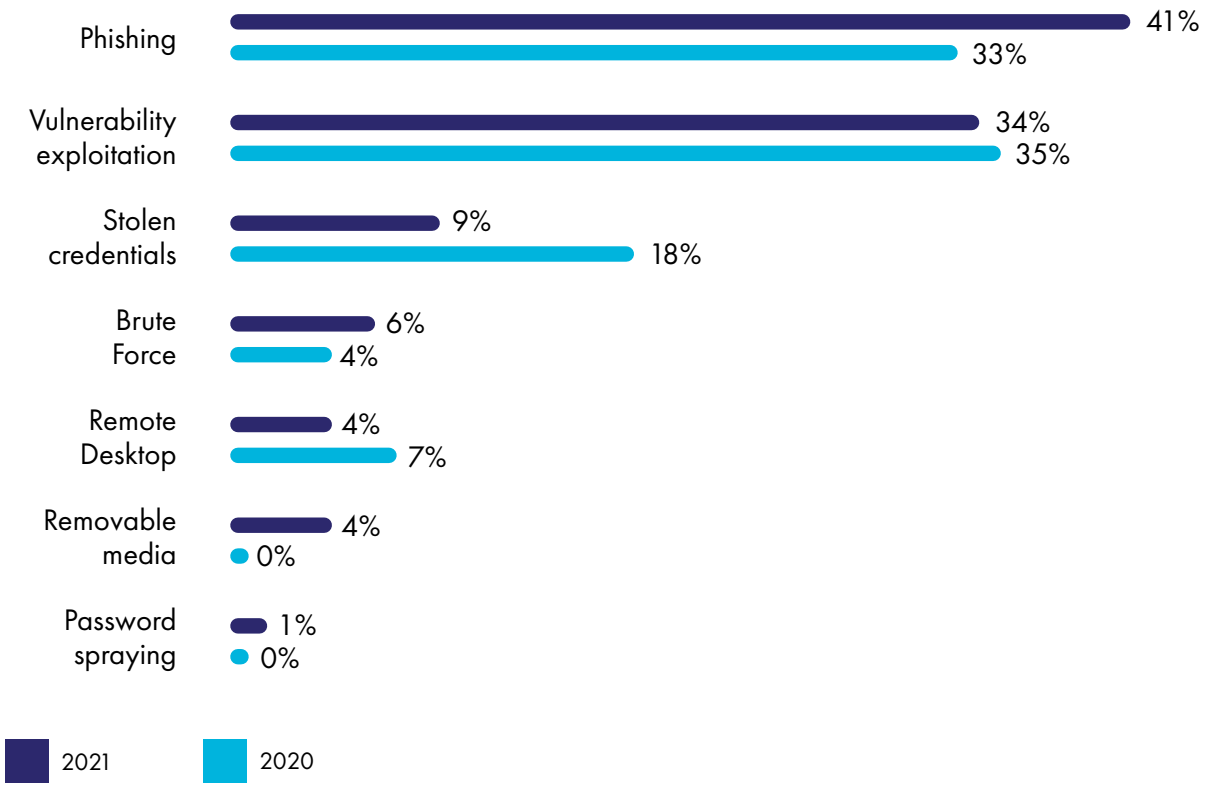


Figure 1: Top Infection Vectors. Source: IBM X-Force

2 https://newsroom.ibm.com/2022-02-23-IBM-Report-Manufacturing-Felt-Brunt-of-Cyberattacks-in-2021-as-Supply-Chain-Woes-Grew

The threat of unauthorized access for manufacturing organizations

Two areas which attackers seek to penetrate in manufacturing companies are the IT corporate network and Operational Technology (OT) systems. Attacks are based on the same concept: gain unauthorized access to the network with compromised credentials, delivery malicious payload, move laterally through the network, and elevate privileges.

Cybersecurity threats in the world of OT are different from IT, however, as the impact goes beyond the loss of data, reputational damage, or the erosion of customer trust.

An OT cybersecurity incident can lead to loss of production, damage to equipment, environmental release and loss of life.

The overlap of IT and OT

The convergence of IT and OT domains have opened once-siloed OT systems to a new world of threats and risks. Increasingly, corporate networks are inter-connected with Industrial Control Systems, such as SCADA and PLC. As a result an attacker can penetrate an IT system and then move laterally to infect and disrupt the OT network. However, disruption to OT systems and the shut-down of manufacturing environments may not necessarily result from a direct attack. The Colonial Pipeline data breach was the result of unauthorized access to the organization's IT network. The mere risk of lateral movement and compromise of OT systems caused them to be shut down immediately, even though these systems were not yet infiltrated. This example shows the convergence of IT and OT and the very high risks posed by the lack of adequate access security, specifically MFA and identity protection.

The manufacturing sector is undergoing digital and cloud transformation, leading many companies to support a hybrid corporate computing environment, where multiple user identities co-exist. Key initiatives include:

- Migrating business workloads Microsoft Office 365
- Leveraging Workday and other HR cloud platforms for sensitive employee information
- Relying on legacy, on-premises SAP systems
- Cloud engineering
- Signal gathering and analysis

A cornerstone to protecting this hybrid environment is building strong access controls with appropriate multifactor authentication methods. The increased reliance on and importance of secure credentials is reflected in industry surveys indicating that manufacturers are mostly concerned with risks related to unauthorized access, intellectual property theft and operational disruption[3]. Attackers are leveraging compromised or poorly managed credentials to spread ransomware or to execute malicious code.

3 https://www2.deloitte.com/us/en/pages/energy-and-resources/articles/smart-factory-cybersecurity-manufacturing-industry.html

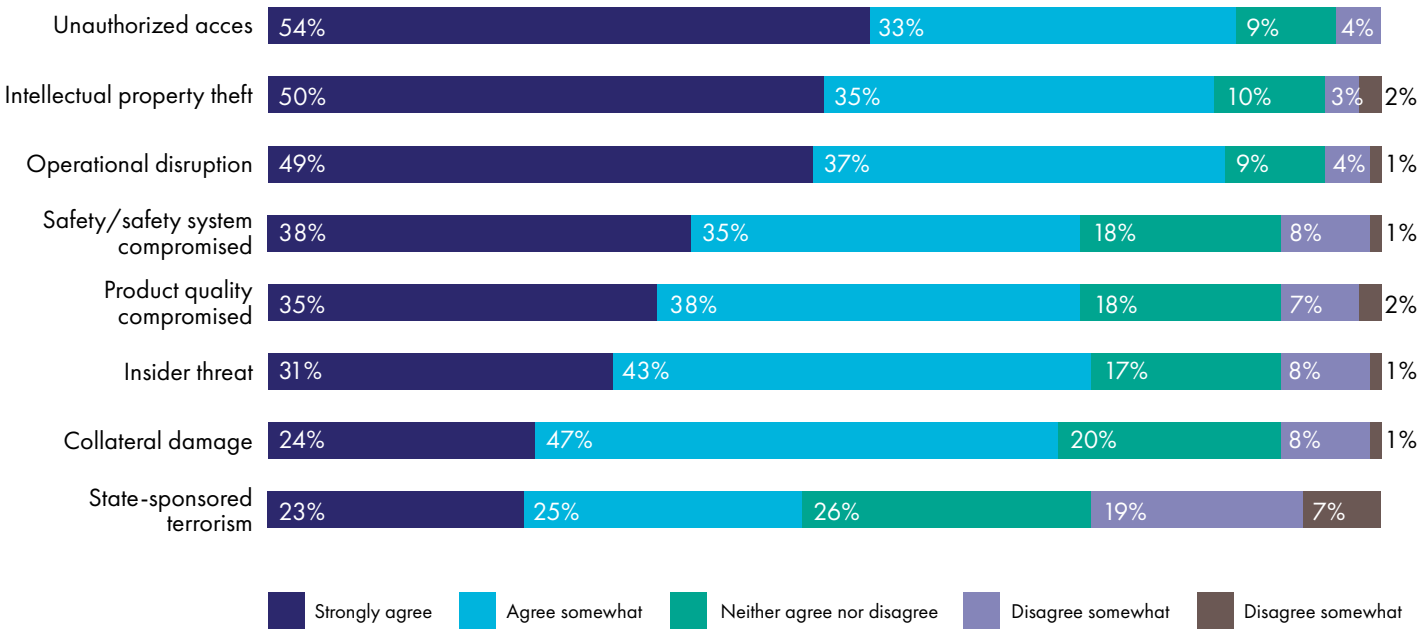


Figure 2: Cyber Risks in Manufacturing Industries. Source: Deloitte

OT system–related investment decisions are often made on the factory floor by leaders within operations, with less involvement from corporate IT and security departments. This can lead to a heterogeneity of technologies, often with different security control capabilities that will need to be integrated to and managed using existing IT infrastructures.

The convergence of IT and OT security can be a challenging task, since routine IT procedures, such as antivirus software updates or even patching, can lead to significant production disruptions, even potentially shutting down entire production lines.

The table below describes the top cyber security concerns related to IT and OT ecosystems.

OT system characteristics	Cybersecurity concerns
The complexity of IT and OT convergence	• OT is typically managed by engineering, automation, and operations rather than IT. • Deep knowledge of the industrial processes, technology assets, network architectures, risks, and security approaches are often essential, leading to the need for integrated teams across both IT and OT working together.
Update paradox	• Traditional application of security controls such as patching, or vulnerability scanning cannot usually occur without detailed evaluation due to potential effects. • No single approach for patching or updating systems is possible. This can make it difficult to be responsive when vulnerabilities are detected, often driving the need for defense-in-depth approaches to be adopted.
Legacy systems	• Many systems have long life cycles (10+ years) and were not built to be externally connected. With the increase in edge computing, cloud platforms, and the adoption of other smart factory technologies, air gapping is no longer a viable option.

OT system characteristics	Cybersecurity concerns
Destabilized infrastructure	• Older equipment often uses proprietary communication protocols that can be easily disrupted if data communication within the network segments increases. • Existing networks and associated architectures were not designed to handle the data flows required for the adoption of these new technologies.
Operational constraints	• Real-time capabilities are typically essential; introducing additional security controls could introduce latency. • Making network or other changes could require downtime or an outage. Downtime due to maintenance should be limited to absolute minimums. • Software updates are often not possible due to the proprietary nature of products or contracts or equipment age. • Establishment of clear responsibilities across IT and OT functions can be crucial. It is important to approach addressing cybersecurity risks using cross-functional teams, considering the strengths and weaknesses of each group.

OT vulnerabilities exploited remotely

Another area which reflects a growing convergence between IT and OT is that OT systems are being integrated with advanced technologies such as connected sensors and aggregation platforms. These systems can remotely track and control production in real time, plan resources, and diagnose and minimize production errors. Besides the advantages and opportunities that connected OT systems offer, they can also multiply the potential vulnerabilities of the smart factory. In fact, CISA lists more than 1,200 known OT system–related security issues, vulnerabilities, and exploits from more than 300 OEMs and system providers[4]. Most of the top discovered weaknesses are centered on managing digital identities[5].

Given the rapid pace at which new technologies are added to factories via smart factory use cases, IT and OT leaders may be unprepared to respond to new threats that arise. According to a survey by Deloitte[6], even though 90% of manufacturers report capabilities to detect cyber events, very few companies have extended monitoring into their OT environments, and fewer than half of manufacturers have performed cybersecurity assessments within the past six months.

These responses indicate that surveyed manufacturers seem more confident in their cyber preparedness than the maturity and capabilities they may have to respond to and recover from a cyberattack, especially when new technologies come online in periods between risk assessments. It is likely that some manufacturers are not aware of the new threats they face when leveraging IoT devices and other emerging technologies in a smart factory environment. Even if they know that something bad could happen, often they do not understand how.

4 https://www.cisa.gov/uscert/ics/advisories
5 https://claroty.com/2h21-biannual-report/
6 https://www2.deloitte.com/us/en/pages/energy-and-resources/articles/smart-factory-cybersecurity-manufacturing-industry.html

Use Cases

Toyota

Denso, a top Toyota supplier, reported an unauthorized access to their networks in Germany without affecting Toyota's operations. Pandora, the group that allegedly accessed Denso's systems, threatened to disclose the supplier's trade secrets including email, invoices and part diagrams on a website on the dark web. Another attack on a Toyota's supplier forced the company to shut down operations for a day, auto industry experts estimate might lead to a 5% drop in Toyota's monthly production.

Sources:
https://portswigger.net/daily-swig/toyota-shuts-down-production-after-cyber-attack-on-supplier
https://www.bloomberg.com/news/articles/2022-03-13/top-toyota-supplier-denso-hit-by-suspected-cyberattack-nhk-says

Colonial Pipeline

Colonial Pipeline was hit by an extensive ransomware attack on their IT domain. As a precaution, the company decided to shut down the production side of the business (OT domain) to prevent further exposure. Colonial Pipeline is responsible for 45% of the gasoline, diesel fuel and natural gas transported from Texas to New Jersey. A shutdown of this magnitude created a negative economic impact and disrupted the lives of millions of people residing in the East Coast.

Source:
https://www.tripwire.com/state-of-security/ics-security/industrial-cybersecurity-guidelines-protecting-critical-infrastructure/

BlackEnergy malware

BlackEnergy malware, utilized in the first recorded targeted cyberattack on an electrical grid, compromised an electrical company via spear-phishing emails sent to users on the IT side of the networks. From there, the threat actor was able to pivot into the critical OT network and used the SCADA system to open breakers in substations. This attack is reported to have resulted in more than 200,000 people losing power for six hours during the winter.

Source:
https://www.infosecurity-magazine.com/opinions/blackenergy-malware-infrastructure/

The emerging regulatory environment

Attacks affecting the manufacturing sector and critical national infrastructure as a whole are becoming more advanced and more disruptive. The examples are numerous (Colonial Pipeline, JBS, Toyota). To address the growing threat, governments are increasingly releasing and mandating security policies and strategies to minimize the impact of such attacks.

In the United States:

- The IoT Cybersecurity Act 2020[7] was enacted to provide guidelines for federal agencies and partners on how to strengthen the security of IoT connected devices used in OT/Industrial Control System (ICS) environments. The Act requires all internet of things (IoT) devices owned or controlled by either the government or enterprises doing business with the government to meet specific minimum security standards. Manufacturing companies fall within the scope of the IoT Cybersecurity Act 2020.
- The White House published in May 2021 the Executive Order on Improving the Nation's Cybersecurity[8] which aims at strengthening the cybersecurity posture of critical national infrastructure with the goal of minimizing future incidents. The EO provides a framework of actions around:
  - Improving information sharing
  - Modernizing cybersecurity standards with the adoption of a zero-trust architecture and the deployment of multi-factor authentication and encryption
  - Improving software supply chain security
  - Creating a playbook for responding to cyber incidents
- In January 2022, the Office of Management and Budget (OMB) released a federal strategy to move all critical infrastructure industries toward a "zero trust" approach to cybersecurity[9]. The strategy on Zero Trust Architecture mandates all enterprises and federal agencies to achieve five zero trust security goals by the end of 2024:
  - Deploy phishing-resistant MFA to protect personnel digital identities from sophisticated cyber-attacks
  - Inventory all devices they operate and prevent, detect, and respond to incidents on these devices
  - Encrypt all network traffic and segment perimeters into isolated environments
  - Continuously monitor and test all applications for vulnerabilities or security bugs
  - Protect all data based on sensitivity and monitor access to sensitive data
- CISA has also published the Critical Manufacturing Sector Security Guide[10] which consolidates effective industry security practices into a framework for Critical Manufacturing owners and operators to select and implement security activities and measures that promote the protection of personnel, public health, public safety, and public confidence.

7 https://www.congress.gov/116/bills/hr1668/BILLS-116hr1668eh.pdf
8 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
9 https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf
10 https://www.cisa.gov/publication/critical-manufacturing-sector-security-guide

In the European Union:

- The Directive on Security of Network and Information Systems (NIS Directive)[11] is the overarching directive requiring Operators of Essential Services – including critical manufacturing industries – to adopt and enforce certain policies and controls to prevent cyber-attacks from happening. The Directive aims to ensure a culture of security across all sectors that are vital for the EU economy and society and that rely heavily on IT technology. The Directive is currently under review[12] and a revised version will most likely be published within 2022.
- The European Union Agency for Cybersecurity (ENISA) has released many guidelines that help critical national infrastructure industries align their efforts toward meeting compliance with the NIS Directive. The most recent, "Boosting Your Organization's Cyber Resilience"[13], was published jointly with CERT-EU and provides best practices for all European organizations and agencies to enhance their state of cyber resilience. Most notably, the guidelines include provisions such as:
  - Protection of all remotely accessible services with multi-factor authentication. Organizations should avoid using SMS and voice calls as authentication methods. Instead, they should consider "deploying phishing-resistant tokens such as smart cards and FIDO2 (Fast IDentity Online) security keys"
  - Deployment of multi-factor authentication whenever supported by an application
  - Control third-party access to corporate networks and systems to prevent inheriting threats and attacks
  - Change all default credentials and disable all protocols that do not support multifactor authentication
  - Implement network segmentation and micro-segmentation

11 https://digital-strategy.ec.europa.eu/en/policies/nis-directive
12 https://digital-strategy.ec.europa.eu/en/library/proposal-directive-measures-high-common-level-cybersecurity-across-union
13 https://www.enisa.europa.eu/news/enisa-news/joint-publication-boosting-your-organisations-cyber-resilience

Towards an IAM blueprint for securing manufacturing environments

Identity and Access Management (IAM) is the security discipline that enables the right entities to access the right resources, either hardware or IT applications, at the right times for the right reasons. IAM addresses the need to ensure appropriate access to resources across increasingly heterogeneous technology environments and to meet increasingly rigorous compliance requirements.

In many cases, OT/ICS systems and devices use simple passwords to both access and configure them or default passwords that are well known and cannot be changed easily. OT systems and devices that are not protected properly by secure authentication methods are open to attacks by cybercriminals.

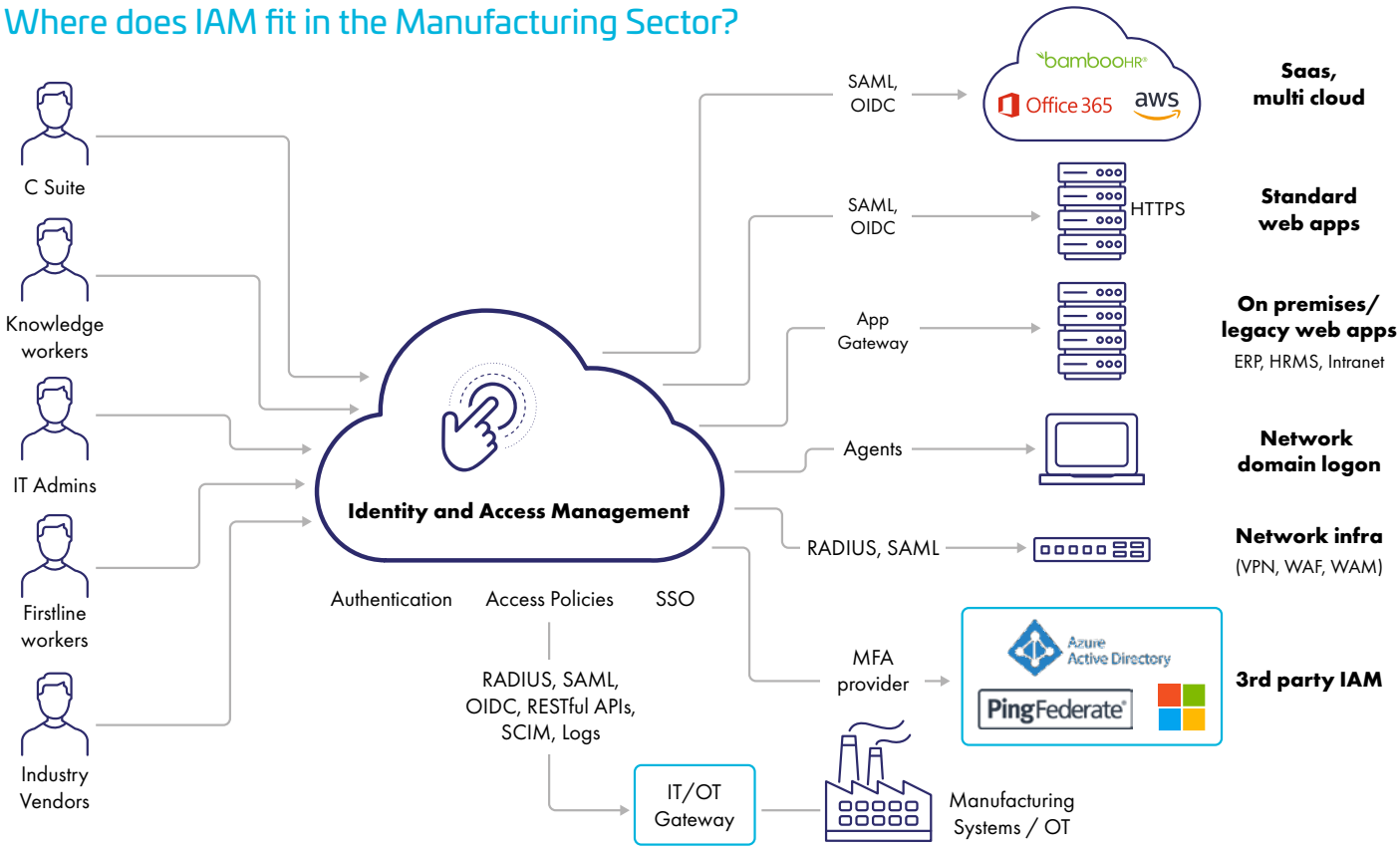
The convergence of IT and OT domains in support of the digital transformation efforts of the manufacturing industry has emerged another infection vector – weak access controls to authenticate knowledge employees into a wide range of cloud-based and on-premises systems. Once an attacker establishes a foothold on a business system, they can implement reconnaissance and privilege escalation to pivot into the OT domain, bypassing firewalls or other network controls.

The success of digitalization of the critical manufacturing sector depends on establishing trust relationships between internal employees, remote employees and partners, devices, and services. IAM systems provide security professionals with technologies to provision, authenticate, authorize, and audit the digital identities of a variety of entities, including:

- Factory manager and executive board
- CISO/CSO
- CTO and Head of Engineering
- Data Protection Officer and Compliance Officer
- Manufacturing floor and warehouse operator
- Knowledge workers (i.e., sales, engineers, HR, finance, etc.)
- Shift workers
- Machinery vendors
- All 3rd parties

To accommodate these diverse stakeholders, the IAM component architecture should provide the required flexibility and elasticity to support deployments in a variety of scenarios and support a range of authentication journeys. IAM acts as the bridge that creates a trusted connection between the IT domain and the OT environment, enabling the authenticated and authorized access of all personnel regardless of their role or position.

Where does IAM fit in the Manufacturing Sector?



To protect this increasingly heterogeneous operational environment, IAM solutions must support a variety of protocols per use case:

- RADIUS for legacy, on-premises applications, and systems
- SAML, OpenID Connect, or OAuth for web and cloud based apps
- RESTful APIs, agents and gateways for non-standard applications
- System for Cross-Domain Identity Management (SCIM) for user and account management

In addition to the above integration and federation capabilities, an IAM solution should provide phishing-resistant multi-factor authentication methods, such as FIDO2 and PKI-based authentication, to support the security requirements of government regulations, acts and guidelines and reduce the potential of advanced attackers breaking authentication through social engineering campaigns.

Thales SafeNet Trusted Access: Powerful authentication and access security for manufacturing environments

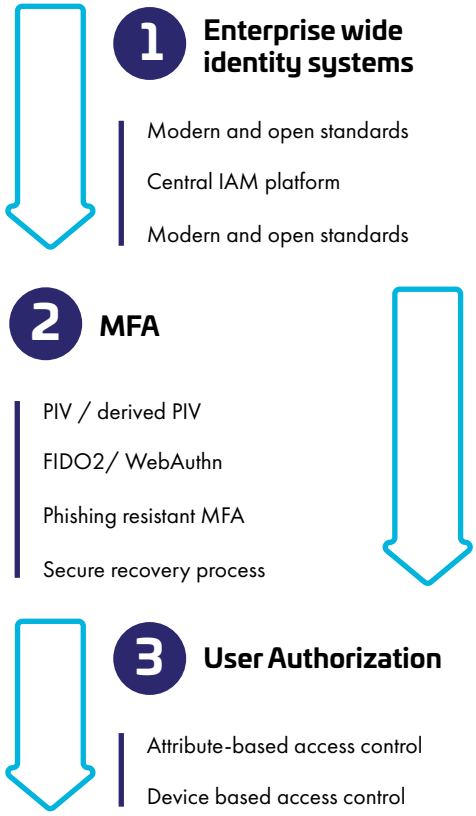
SafeNet Trusted Access is an access management solution that accelerates cloud transformation initiatives and secures your hybrid infrastructure, including OT, IT and ICS systems. SafeNet Trusted Access secures access to both cloud services and enterprise operational applications with an integrated platform combining policy-based access, multi-factor authentication, adaptive/contextual authentication, conditional access and single sign-on.

SafeNet Trusted Access comes with powerful authentication capabilities to support a broad range of use cases within a manufacturing environment:

- Secure access leveraging access management, adaptive and multi-factor authentication for both OT and IT worlds
- Clientless authentication suited to shared workstations and mobile-free environments (Pattern-based, FIDO)
- Authentication for knowledge workers and privileged users, depending on their user circumstances
- Meet the guidelines for MFA that is resistant to Man-in-the-Middle attacks (FIDO2 and PKI certificate-based authentication)

SafeNet Trusted Access offers unparalleled efficiency acting as a single identity provider for both enterprise and OT/ICS domains. It can act as a centralized identity provider or integrate with other IDPs and IAM solutions that may already be deployed in an organization, providing the necessary breadth and range of authentication methods needed to address a broad range of use cases. The solution comes with a variety of flexible deployment options, supporting both cloud-based and on-premises deployment. On-premises deployment allows manufacturing industries to protect segmented OT islands. In addition, SafeNet Trusted Access offers diverse integration capabilities, supporting protocols like RADIUS, OAuth, SAML, OpenID Connect and SCIM that allow interoperability with both standard and non-standard applications.

SafeNet Trusted Access Meets Zero Trust Identity Protection requirements for Critical Manufacturing



SafeNet Trusted Access acts as a single identity provider for both enterprise IT and OT/ICS domains.

Case Study: Compliance with regulations for major clean energy provider

Centralized access management with MFA for critical systems.

Challenge

A North American clean energy provider with major corporate customers needed a solution to protect its network of on-site fuel cell production facilities.

As an energy utility, it needed to comply with cybersecurity mandates from the Federal Energy Regulatory Commission (FERC) and North American Electric Reliability Corporation (NERC).

Required a scalable, flexible and resilent mult-factor authentication (MFA) solution to protect access to distributed facilities.

Solution

The customer chose cloud-based SafeNet Trusted Access to protect VPN access to all critical assets and access points.

Multi-Factor Authentication with convenient and flexible authentication methods added strong security while ensuring adoption and usability.

Centralized access management allowed for granular access governance based on compliance and security requirements.

Results

Enforced centralized access management and authentication to help compliance with energy industry regulations and mandates.

Achieved successful protection of critical systems from external and internal threats, increasing resilience of critical energy production systems.

Allowed for expansion into access control management for switches and other systems in an increasingly diverse IT infrastructure.

Currently expanding number of users from 1,400 to 2,500.

What is next?

Securing your critical manufacturing environment requires concrete steps that can help you identify all potential attack vectors, detect vulnerabilities, and take preventive measures. Risks to physical and cyber assets in the manufacturing sector can originate from multiple sources, including deliberate, malicious human actions (e.g., crime, sabotage, and terrorism); non-malicious human actions (e.g., accidents and negligence); technological deficiencies; and natural disasters.

Critical manufacturing security programs will vary, as they are tailored to the specific facility characteristics, needs, and risk profiles. However, facility owners and operators engaged in security programs for their companies should consider common security program administrative and strategic fundamentals, such as:

- Comprehensive risk analysis
- Personnel and resources dedicated specifically for security
- Partnerships with federal, state, and local officials
- Information-sharing with other organizations

Identifying critical assets and mapping out who is accessing them represents the first step in systematically increasing identity protection. The following checklist, focused on identity and access management, can help you assess your risk and security environment and take action to close any gaps.

Identify your security regulatory context	
☐	IoT Cybersecurity Act 2020
☐	Executive Order on Improving the Nation's Cybersecurity
☐	OMB Memorandum on Zero Trust Cybersecurity Principles
☐	CISA Critical Manufacturing Sector Security Guide
☐	EU Directive on Security of Network and Information Systems (NIS Directive)
☐	EU NIS Directive Toolkit
☐	ENISA Boosting Your Organisation's Cyber Resilience

Identify your personnel	
☐	Who are they (executives, knowledge workers, factory floor workers, shift workers, etc)?
☐	What are their roles and responsibilities?
☐	What applications are they accessing?

Identify your OT assets	
☐	What are they?
☐	What protocols do they support?
☐	Which individuals access OT systems and from where?
☐	Where are they?
☐	What type of data do they process?

Select your IAM solution	
☐	Can the system integrate with IT, enterprise and OT applications – both on-premises and in the cloud
☐	Does the solution support multiple authentication journeys to support multiple user needs?
☐	Does the solution support multiple MFA methods, including phishing-resistant ones?
☐	Does the solution offer flexibility and scalability?

For further information please contact:
Natalie Britton
Marketing Manager
Email: natalie.britton@bluecubesecurity.com
Blue Cube Security Ltd
+441342363134
https://bluecubesecurity.com

THALES
Building a future we can all trust

Contact us

For all office locations and contact information,
please visit cpl.thalesgroup.com/contact-us

> cpl.thalesgroup.com <