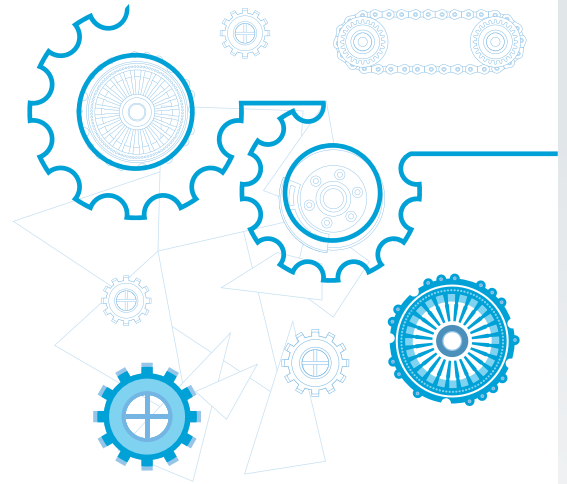




**Cyber securing production and IT,
OT and IoT converged environment
for a leading manufacturer**

Highlights

- ◆ Unique engagement model
- ◆ Comprehensive and segment focused protection options delivered
- ◆ Single platform approach to cover IT-OT converged deployments
- ◆ Ease to deploy and secure



The challenge

IT, IoT, and OT teams are increasingly discovering the need to join hands to deploy cybersecurity solutions across the enterprise; from headquarters, supply chains, remote locations, and the factory floor.

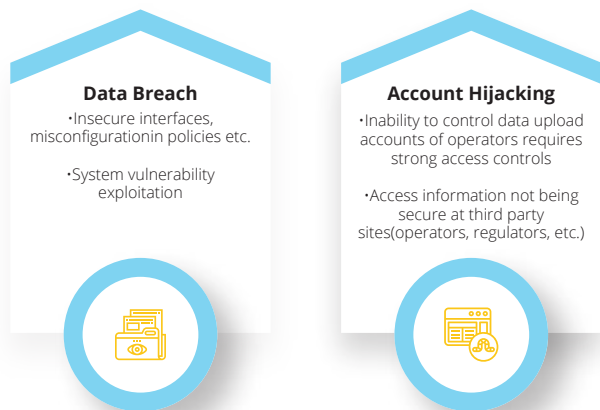
Hackers are today operating with sophisticated malware and methods and with more patience. Malware has been becoming more sophisticated. This indicates more investments and R&D attention is being paid to evolving hard to detect malware for various purposes. Industrial deployments have been specifically targeted for various reasons including:

- Industrial espionage
- IP theft
- Crypto mining
- Data pilferage
- For extracting ransom
- Lateral movement of attacks
- Ransomware
- Cloning devices to divert data traffic

These developments and methods represent a clear threat to every manufacturing entity. Being a diligent manufacturing entity, Anchor Glass understood the need to ward off such threats at the earliest. Anchor Glass wanted to secure its data, operations, infrastructure, and people from all kinds of cyberthreats.

Anchor Glass' existing security measures were more focused on IT security and they identified a gap in their security posture in an IT-OT converged deployment that was incapable of preventing sophisticated inbound cyber attacks. In addition to addressing a significant deterioration in the threat landscape surrounding their manufacturing operations and associated supply chains, Anchor Glass also had to cope with the ever-increasing threat of a major breach that could be caused by insider activity (rogue or involuntary). Keeping these specific threats as key challenges to be addressed, Anchor Glass started scouting for a cybersecurity partner.

Some of the key risks to data that we encounter today are as listed below



About Anchor Glass

Anchor Glass, headquartered in Tampa, Florida, is a leading North American manufacturer of premium glass containers with, strategically-located production facilities throughout the US. Founded in 1983, Anchor serves many iconic and recognizable consumer packaging brands in the beer, beverage, spirits, and food industries, and strives to exceed customer expectations through unrelenting attention to detail.

Anchor Glass' work goes beyond glass making. It serves the unique needs of its customers through innovative solutions that are expressed in a range of design and utility options. Anchor Glass manages the needs of its customers on an end-to-end basis bringing incredible levels of scalability and aesthetic excellence to make their products set the design and functional standards in the industry.

Key risks associated with data

- Insecure data can be accessed by operators to spy on each other
- Customers can be poached based on information from the records
- Data can be also be used by nation states to conduct cyber warfare



Compliance

- Phone numbers and customer information is considered personally identifiable information
- Communication sector is critical infrastructure
- Cyber crime prevention Act of Nigeria, 2015 imposes fines for not safeguarding PII and CII data



Insider Threats

- Rogue employees for monetary benefits (selling data)
- Revenge attacks from disgruntled employees



The solution

Anchor Glass chose Subex to address these challenges by augmenting their existing security controls. Working in a phased manner, Subex came up with a multi-tier project plan to provide eyes on glass view of their security posture that covered:

- Investigations to uncover existing and emerging threats, vulnerabilities in the IT-OT and IoT domains and any risks or compliance mandates that need to be addressed as part of the deployment of Subex Secure
- Asset discovery to identify all assets to be protected
- Identify and help address policy violations.
- Identifying the best practices to minimize lateral movement of attacks between their networks
- Solution deployment to detect, respond, and help recover from threats.
- Post-deployment diligence

The deployment

Subex Secure was deployed rapidly within Anchor Glass to address potential cyber risks, detect critical exploits, monitor, identify and catalog threats in real-time and/or as they are uncovered on Anchor Glass Container Corp.'s network. The product is performing real-time attack surface analysis and automatically identifying suspected issues to help security teams manage them using both reactive and proactive measures. The platform is assisting Anchor Glass, through robust profiling and

detection capabilities to conduct security analysis reported by Subex. Subex Secure is using its signatures, heuristics data analysis, and machine learning to conduct activity profiling at various levels to ensure that any anomaly against normal behavior is detected, reported, and possibly mitigated.

Anchor Glass Container Corp. is now leveraging this platform to validate their security gaps and harden their network security. The services Subex offers is helping them enhance their cyber posture against new and advanced cyber threats, defense against threats emerging from multiple interconnected heterogeneous subsystems

Subex Secure Engagement

- Subex Secure consulting engagement to review their current security policies to strengthen their OT plant perimeter security.
- Consulting engagement to segregate their IT-OT networks

Technology Components

- Subex Edgetech (Data Acquisition Appliance)
- Subex Secure Platform for reporting and remediation of threats
- Subex device discovery and vulnerability detection
- Automated Actionable workflow module for autonomous threat response and integration to other systems
- Subex Denver Security Operations Center (SOC) provides 24x7 eyes on glass coverage with incident triage, investigation, and forensics
- Subex Honeypot Threat Intelligence (Managed by Subex)

Features

- Advanced Threat Management: protection at the true critical infrastructure level
- Comprehensive Security: against existing and emerging threats including those posed by Advanced Persistent Threat Groups
- Low touch: easy to run, manage to allow Anchor Glass to optimize issue identification and analysis time on potential threats, and take necessary actions against them. The solution is also completely managed to reduce the overhead of maintenance costs.
- Scalability: horizontal and vertical scalability to meet the emerging needs of the company

Benefits

Improved risk posture

At a time when many manufacturers in North America (even the National Association of Manufacturers was attacked) were attacked by hackers, Subex could secure Anchor Glass' manufacturing infrastructure against such attacks that were not just sophisticated and persistent but also designed to disrupt operations on a massive scale.

Enhanced compliance capabilities

With Subex's offerings, Anchor Glass was able to ramp up its ability to comply with multiple cybersecurity-related mandates.

Business focus

With Subex taking care of security, Anchor Glass gained the ability to focus on its business priorities.

Visibility into incidents

By offering comprehensive reporting capabilities, Anchor Glass gained deep insights into various aspects of the engagement including incidents, threats, management, and mitigation processes as well as enhancements.

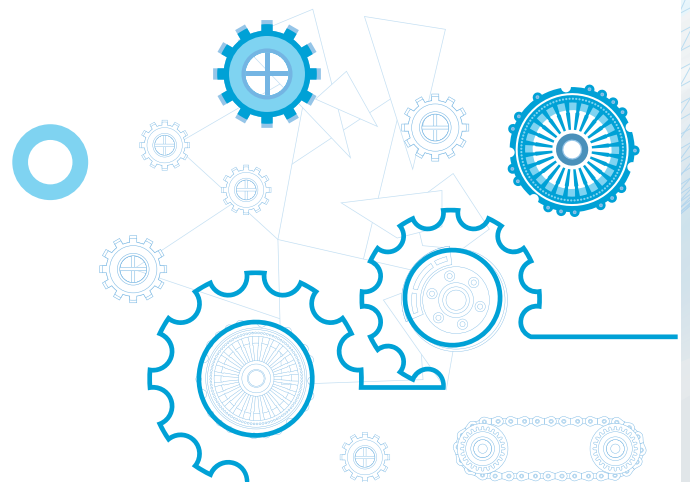
Single source of protection

Subex could meet all of Anchor Glass's security needs on one platform mitigating the need for having multiple vendors and complex and opaque relationships.

Optimal model

Subex's engagement with Anchor Glass has become a model for others in the industry. With the threats against manufacturers rising by the day, such a model that is robust, scalable, and backed by an award-winning platform is essential to ensure the attainment of various goals.

"We decided to choose Subex Secure after multiple rounds of diligence and we are happy to report that the engagement has worked to our advantage. Not only is our critical infrastructure more protected now, but thanks to the diligent manner in which this engagement was managed from inception onwards, Subex has earned our recommendation and kudos" said Christina Shannon, Vice President of Information Technology(CISO) at Anchor Glass.





Subex is a leading provider of IoT and OT Security solutions and allied services to a range of industries including manufacturing, smart cities, oil and gas, telcos, retail, aerospace, and more. Through our mature portfolio, we serve to protect the assets, data, and operations of our customers through unique cybersecurity approaches that are based on tested and proven frameworks and approaches. Our offerings are backed by one of the largest honeypot networks in the world that delivers segment focused threat intelligence enabling us to deliver protection against emerging threats in real-time.

Subex Limited

RMZ Ecoworld,
Devarabisanahalli,
Outer Ring Road,
Bangalore - 560103 India

Tel: +91 80 6659 8700
Fax: +91 80 6696 3333

Subex, Inc

12303 Airport Way,
Bldg. 1, Ste. 390,
Broomfield, CO 80021

Tel : +1 303 301 6200
Fax : +1 303 301 6201

Subex (UK) Ltd

1st Floor, Rama
17 St Ann's Road,
Harrow, Middlesex,
HA1 1JU

Tel: +44 0207 8265300
Fax: +44 0207 8265352

Subex (Asia Pacific) Pte. Limited

175A, Bencoolen Street,
#08-03 Burlington Square,
Singapore 189650

Tel: +65 6338 1218
Fax: +65 6338 1216