International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Deparameterizing the Oil and Gas Industry Infrastructure with Zero Trust Architecture and Improve the Cyber Security

Suchismita Chatterjee

M.S.-University of North Texas|Cyber Security Product Specialist
suchi5978[at]gmail.com

Abstract: ***The Oil and Gas industry is an important industry and critical industry as many organizations and civil society depends on them for their day-to-day activities. Hence the Oil and Gas industry is always in the crosshair of cyber criminals or enemy state players. Oil and Gas Infrastructure always focus on securing their infrastructure, but since the number of ends point, they operate are in thousand and hundreds of services and sites distributes all over the country makes the security the infrastructure a big challenge. To add to the challenge, there is an ever-evolving nature of the IT infrastructure. The current security posture of the Oil and Gas industry is more static in nature and using mix of latest and traditional security devices. In this paper will be looking into the concept of Zero Trust and Zero trust Architecture. Here we will be looking at different components of the Zero Trust Architecture and explore the concepts where the Zero Trust Architecture can be used to manage the access control at much more granular level and how the architecture can help to identify any new vulnerability or attack in real time and dynamically react to the incident and secure the network and better manage the security posture of the industry.***

Keywords: Zero Trust, Utility Industry, Virtual Asset Management, Cybersecurity, Cyber Hacks, DevSecOps, Automation

1.Introduction

The Oil and Gas Industry is a crucial industry in the current generation, almost all the industry. Households are depended on the Oil and Gas Industry without which society as it is may cease to exist. Hence is it no wonder that the Oil and Gas industry is always a target of the cyber-attack either by enemy nation state or cyber criminals. Security the Oil and Gas industry is very critical but there is lot of hurdles faced in securing these infrastructures as Oil and Gas industry operate in a very heterogenous environment. Oil and Gas infrastructure may be divided to cloud infrastructure, on-prem infrastructure, SCADA server, to SCADA devices, PLC, sensors, and actuators.

Since due to these wide variety of devices present in infrastructure, it is a challenge to have control and visibility over this diverse network entity either they may be present either in Operation or Information technology. At the same time, the current trend employees working from home emerged to covid 19 pandemic, due to which previously isolated equipment which were air gapped from the external network are forced to connect or allow connection from devices outside the isolation zones. This in return increase the treat landscape for the Oil and Gas Industry adding to the difficult of having a visibility of the network and thus overall increasing the difficulty of security the Oil and Gas Infrastructure.

Currently the IT industry is more about sharing the data, collecting data from different end point as it helps the organization in reducing the cost, optimizing, or increasing the efficiency of the system and better react to the needs of the market, Oil and Gas industry is not excepting, even it has adopted this approach to increase its productivity. Due to which the security boundaries with different sections of the industry are eroded. Now we see it more common for the data to be shared from operational devices such as SCADA/IoT devices to IT devices such as Cloud servers or On Cloud Servers. Since the data is travelling unhindered either from one section to another section or move laterally between the devices in the same section. IN this situation if the threat actor can compromise even a single system in any of the sections, it will make it lot easier for them to propagate/attack devices in the same section or devices in the different sections. This the exactly the reason we saw widespread infection of ransomware attack such as WannaCry able to propagate quickly to hundreds of devices and infect them.

2.Current Security Practice in Oil and Gas Industry

Security is of paramount importance for Oil and Gas industry right from day one. Currently Oil and Gas industry employ different security devices and philosophy to secure the infrastructure, let's look at a few security practices currently employed.

- The oil plant network and the corporate plant network are insulated from each other and are not directly connected to each other.
- Firewall are employed when the communication is taking place between two different network and therefore allow the traffic to be filtered.
- Access controls are properly managed to prevent any unauthorized access to the resources.
- Employing the Antivirus protection to prevent any attack arising thorough malware or ransomware infection.
- All the data communication between two remote devices are secured by encrypting the communication via using the VPN (Virtual Private Network).
- Add multi-layer protection and deploy defense in depth to delay the attack from a cybercriminal and deny any uninvited access to critical resources.
- Employ the SIEM technology to collect security related information and analyze the data to identify any traffic

pattern which could generate alert and feed the data to IDPS to identify any attack patterns.
- Cloud infrastructure used by the Oil and Gas industry should provide the same level of CIA security features as it were provided by on-prem security. Proper security measures are implements on the cloud-based infrastructure. Hence cyber criminals attacking the Oil and Gas cloud infrastructure will be mitigated by the cloud service providers.

Even though the Oil and Gas industry have invested significantly in cyber security and deploy many layers of different security measures, we will see in the later part of the paper why this is not enough in the constantly changing IT landscape.

Zero Trust Architecture:

Zero Trust is a term used for a collection of ideas where it assumes that the network is always compromised, the decision made to give an entity access to a resource at a very granular level and improve the accuracy of the security policy enforcement. On the other hand, there is a plan needed to enforce the Zero trust concept in the ever-complex network infrastructure and operational polices, that is where the Zero Trust Architecture comes. Zero Trust architecture help organizations implement Zero trust policies across their network infrastructure and help improve the organizations security posture.

Zero trust focus on making sure that the data can only be accesses by authorized entity and it should be able to enforce the access controls as granular as possible. Zero trust and Zero trust architecture just focus on authentication and authorization and only allowing the resources to be accessed by approved entities and prevent any untrusted entity, while not affecting the QoS (Quality of Service) of the infrastructure. Least privilege access management is enforced by trying to make the access policy as granular as possible.

Zero Trust Access:

Whenever a subject wants to access a resource such a data or an application. It first must go through the PDP (Policy Decision Point)/PEP (Policy Enforcement Point). Lot of things need to be considered before giving the access to the resource. For each and every request access control will be enforced, it will check if the subject has the right access right, the device where the requested is origination, is it having the right access rights, is the network from where the requested being generated has the access right, the access policy needs to be dynamic where the trust level on the subject can change dynamically based on certain factor, based on the certain incident the trust level of the subject can drop and the access can be removed. For instance, is a network is compromised all the devices in the network can be marked untrusted, and access to the resources to these devices can be removed until the trust level is back to normal.

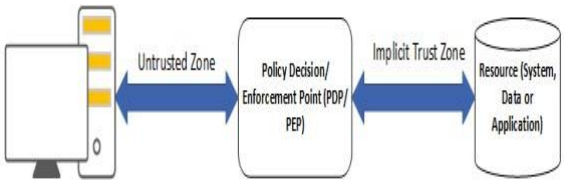

Figure 1: Zero Trust Access

Zero Trust Architecture Logical Components:

ZTA is made up many components. These components work in together when implemented in an enterprise environment. These components work on both the Oil and Gas cloud environment and on their on-premises environment. As we have seen earlier in the paper the importance of Policy decision point PDP, here in this architecture the PDP is divided further into two components policy administrator and Policy engine. In their architecture different control plane is used by the components to communicate with each other while the application data uses a separate data place to communicate data.

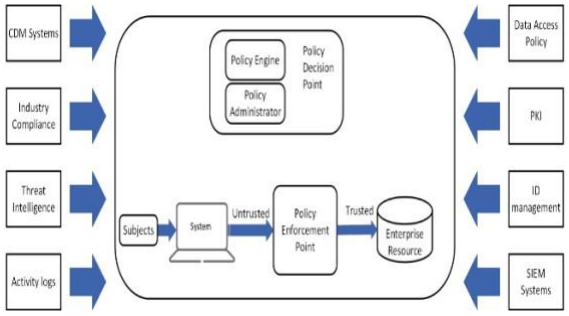

Figure 2: Core Zero trust logical components

Three main components of the Zero Trust Architecture are:

1) Policy Engine
2) Policy Administrator
3) Policy Enforcement Point

- Policy Engine (PE): the decision to give access to a resource for a subject will be made by the Policy Engine only. PE collects information from enterprise policy, and other sources like the threat intelligence service and continuous diagnostics and mitigation system and process the request using the trust algorithm and then the decision about either revoke, deny or grant action for resource. The policy engine will work with policy administrator for doing its duties. The Policy administrator will be the one who will be responsible for implementing the decision, whereas the policy is responsible for creating and logging the policy decisions.
- Policy Administrator PA: the component that will take the decision which communication between the resource and subject will be allow or denied or removed will be done the Policy Administrator. PA works closely with PE, and it uses PE to do all the actions. PE is generating the policy and PA will be responsible for implementing. The tokens that are used by the subjects to access the resource are all generated by the PA. If a previously granted communication or a new communication is rejected will request the connection stoppage to Policy Enforcement Point. The communication between the Policy Administrator and the Policy Enforcement Point will be done over the control place.

Without the confirmation from the Policy Administrator the Policy Enforcement Point will not allow the connection between the resource and subject.
- Policy Enforcement Point: All the connection between the resource and subject will be terminated, allowed, and monitored by the Policy Enforcement Point only. Policy Enforcement Point will take all the decision only after getting the confirmation from the Policy Administrator.

There are other components in the Architecture that work along with PE, PA, and the PEP. Some of them are:

- Continuous Diagnostics and Mitigation system: This component provides information about subject to the policy engine, if the subject device is properly patched, and not running unwanted software.
- Industry compliance system: This component makes sure that the Oil and Gas industry is following all the applicable compliance.
- Threat Intelligence feed: Oil and Gas Industry will get information about the latest vulnerability from both internal and external sources, and this will be provided to PE that enables it to make better policy decisions.
- Network and System activity logs: This component show the security posture of Oil and Gas Industry by analysis security logs of devices on the infrastructure.
- Data Access Policy: This represents the access permission for the resources, and these will be defines based on the Oil and Gas Industry service requirements and roles of the users and projects.
- Enterprise public key infrastructure: The Oil and Gas service resource will be provided a PKI certificates; these certificates are managed by this component.
- Security Information and Event Management: this component will collect the security logs and identify any vulnerability and generate the alerts accordingly.
- ID management system: This component will use services like Light Weight Directory Access Protocol to manage enterprise user account. This will have all the information about the users.

3.Challenges Of Implement The ZTA

Adopting the Zero trust architecture in oil and gas is going be very difficult and challenging, especially since the Oil and Gas industry has primarily focus on the traditional approach of implicit trust. IN the traditional approach the authorization is not done frequently, once does the entity remains authorized for a long time, the policy that are used for access management are in static and not dynamics meaning the policy should be changed manually by the team. The cost of transformation from the traditional to the Zero Trust Architecture is also going to be expensive, as we will have to change the legacy system to the system that support the Zero Trust Architecture. More planning is required to integrate the Cloud.

infrastructure of the Oil and Gas industry with the On-prem infrastructure which support the Zero Trust Architecture. Different IT teams and the Senior Leadership Executive should be able to coordinate properly and should be able to take decision in time which can be as issue at time. But if the organization can overcome these challenges the Oil and Gas industry will be able to better protect its resources in constantly changing IT land scape.

4.Network Prerequisite for ZTA Implementation

Before the ZTA can be implement their certain network requirement that needs to be meet, these are:

- All the devices in the Oil and Gas infrastructure should be connect to the network.
- The infrastructure should be able to distinguish between the devices in the network that is owned by the Oil and Gas industry and once that are not.
- The Oil and Gas infrastructure should be able to monitor all the traffic.
- The PEP should be used before access the Oil and Gas resource.
- The PEP should be reachable from all the Oil and Gas assets.
- Policy administrator should not be access by any other components other than the PEP.
- It should not be required for assets to travers through the enterprise network to access the Oil and Gas cloud resources.
- It should block the enterprise assets like the manager laptop to be able to access the resource if they are accessing outside the geographical boundary that is set. For instance, restrict access outside the country.
- Components that are making the access decision should be scalable and their service should not bottle neck.

5.ZTA In Different Scenarios

Even though there is lot of challenges in implementing the ZTA in the Oil and gas industry, but it is still possible to implement them, as Oil and Gas industry will already have some form of ZT being utilized in the enterprise infrastructure. They may also have dynamic security policy management in some form. At the same time ZTA emerged in the situation where the organization was large critical and geographically distributed just the Oil and Gas Industry.

- **Integrating Remote Site, Cloud Platform and Enterprise**

Oil and Gas Industry have geographically distributed site and have many employees working remotely either working from company provided devices like laptops or personal laptops also. There may be many devices in the satellite site. All these devices may want to connect to the resources either on the enterprise network or on the cloud infrastructure. It a traditional practice to route the traffic to cloud resource only via Enterprise infrastructure, but it may not be ideal especially when the bandwidth of the network is an issue. In these situations, it is ideal to have the PE/PA in the cloud environment, hence Oil and Gas industry remote client and different site devices will be able to connect to the cloud resource without have the need to route all the traffic to cloud via the enterprise network itself.

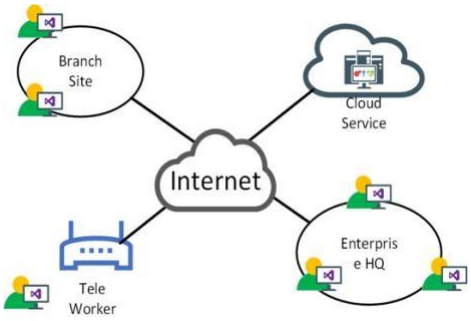

Figure 3: Remote employees in an Enterprise Environment.

- **Oil and Gas Multi cloud Infrastructure**

As the IT is evolving the more and more resources are being moved to cloud, it is possible that the Oil and Gas industry may be running their services on different cloud providers, in some cases it may be possible for these cloud services to interact with each other. in a non-zero trust approach the traffic between the different cloud providers will be routed through the enterprise network and hence stressing the enterprise network. ZTA proposes that enterprise and external connected network (Cloud Environment) should be treated equally and there should not require the traffic to be routed through enterprise network. The PE and PA services may be in the cloud itself, hence the client will connect to the policy enforcement point directly, hence allowing the enterprise infrastructure to manage the all the access remotely and effectively.

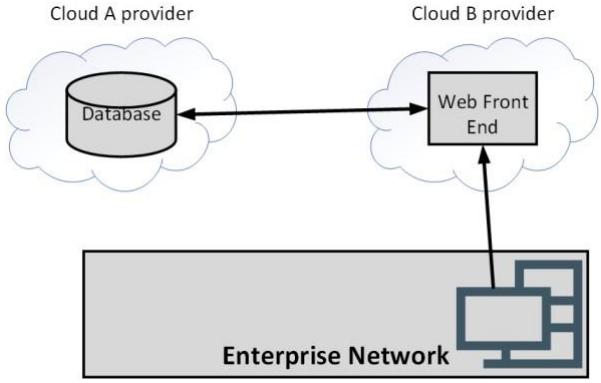

Figure 4: Multi Cloud usage along with Enterprise network

- **ZTA in Oil and Gas for Contract Employees and Non-Employees:**

Since their lot of different devices in an oil and gas facility, ranging from IoT devices, programmable logic controller, and other devices, it may be quite common to have contracts and non-employees to be on the site and they might need access to the internet to perform their duties. Traditionally it means if a contractor is given access to internet also means we must give access to the enterprise network, when implemented the ZTA and contractor or anyone else will be given access to internet, but they will not be able access the enterprise network, actual employees will be able to access the ONG enterprise network. ONG client may have agent installed on devices or access a portal through which they can access the enterprise network, and this communication in managed by the PA/PE which is either hosted on the LAN or Cloud.

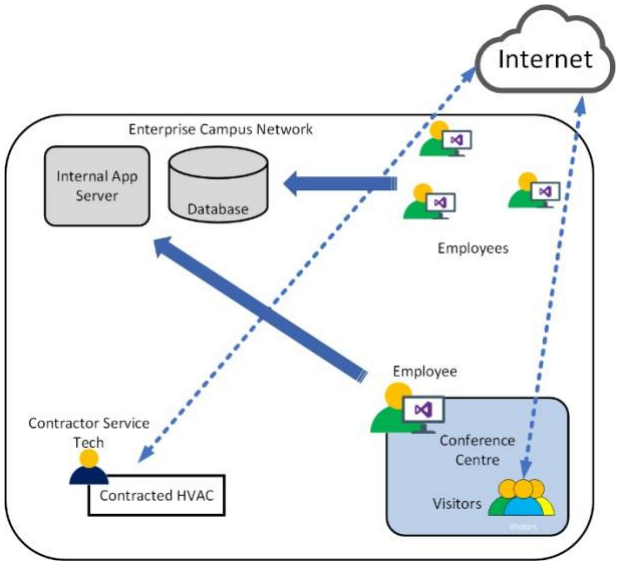

Figure 5: Visitors and others in an Enterprise environment

6.Conclusion

In this article we have seen how the Oil and Gas industry is constantly working towards making the security better in this infrastructure. We also have seen the challenges faced in implementing security and the infrastructure contains thousands of end points, integrating multi cloud environment and a mix of old and new security devices. One of the other factors that increase the challenge to provide security is the static nature of the access control policy and heavy dependence on the Oil and Gas enterprise infrastructure to manage all the access controls.

Here in the article, we have explored the concept of Zero trust and Zero Trust architecture where the no subject is trusted by default, every action of accessing the resource need to go through Policy Enforcement Point and the PEP will work together with the Policy Administrator and the Policy Engine and then decide if the subject can access the resource. We have also explored the challenges in implementing the Zero Trust Architecture. Finally, we saw how the challenges can be overcome and implement the Zero Trust Architecture in the Oil and Gas enterprise infrastructure and successfully monitor and manage access to the devices, different employees, and nonemployees and how the access control policy can be moved to cloud for cloud related services hence reducing the dependence on the enterprise infrastructure for managing the access control.

References

[1] S. Rose, O. Borchert, S. Mitchell, and S. Connelly. 2020. Special Publication 800-207: Zero Trust Architecture, National Institute of Standards and Technology, Gaithersburg, MD, USA, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf.
[2] Peter Black (09/2018) Cyber Security, the Cloud, and Oil and Gas, Conference: SPE Annual Technical Conference and Exhibition
[3] Et. al. Mohamed Jumah ALDhanhani (May 2021) Review of Cyber Security on Oil and Gas Industry in United Arab Emirates: Analysis on the Effectiveness of

the National Institute of Standards and Technology's (NIST) Cybersecurity Framework Turkish Journal of Computer and Mathematics Education (TURCOMAT)
[4] Rashid S. Mohammad, Naseer Ahmed, Waqar hazoor, Feb 2020, Cyber Security of Oil and Gas over the Cloud
[5] Atdhe Buja, Marika Apostolova, Artan Luma, Ylber Januzaj. 06/2022. Cyber Security Standards for the Industrial Internet of Things (IIoT)– A Systematic Review, International Congress on Human-Computer Interaction, Optimization and Robotic Applications
[6] Bowen Hou, Donald Paul. 04/2021. Security Implications of IIoT Architectures for Oil & Gas Operations, SPE Western Regional Meeting.
[7] Z. S. Irani, R. George, R. Dayal. 10/2023. Technology for Continuous Cyber Monitoring of Offshore Assets. Abu Dhabi International Petroleum Exhibition and Conference (ADIPEC).
[8] Huma Afzaal, Mohamed Salama, Colin Turner. 01/2023. Digitization, Cybersecurity and Risk Management in the Oil and Gas Sector in the post COVID world: A Systematic Review. AHFE International Conference on Human Factors in Design, Engineering, and Computing (Human-Centered Design and User Experience
[9] Identity Theft Resource Center, "Annual Data Breach Report Sets New Record for Number of Compromises," 2022. [Online]. Available: https://www.idtheftcenter.org/post/identity-theftresource-center-2021-annual-data-breach-report-setsnew-record-for-number-of-compromises/
[10] Onome Edo, Imokhai Tenebe, Egbe-Etu Emmanuel Etu, Atamgbo Ayuwu. 7/2022. Zero Trust Architecture: Trend and Impact on Information Security. International Journal of Emerging Technology and Advanced Engineering
[11] Ms. Divya, Sherin Sithara. 5/2022. A Zero Trust Framework Security to Prevent Data Breaches and Mitigate the Cloud Network Attacks. International Journal for Research in Applied Science & Engineering Technology (IJRASET).
[12] Yuanhang He, Daochao Huang, Lei Chen, Yi Ni, Xiangjie Ma. 06/2022. A Survey on Zero Trust Architecture: Challenges and Future Trends. Wireless Communications and Mobile Computing 2022.
[13] oan-Alexandru Dumitru, 04/2022. Zero Trust Security. International Conference on Cybersecurity and Cybercrime.
[14] Nabeel Sheikh, Mayur Pawar, Victor Lawrence. May 2021. Zero trust using Network Micro Segmentation. IEEE INFOCOM 2021 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS).
[15] Qigui Yao, Qi Wang, Xiaojian Zhang, Jiaxuan Fei. 10/2020. Dynamic Access Control and Authorization System based on Zero-trust architecture. CCRIS 2020: 2020 International Conference on Control, Robotics, and Intelligent System.
[16] Yuanhang He, Daochao Huang, Lei Chen, Yi Ni, Xiangjie Ma. 06/2022. A Survey on Zero Trust Architecture: Challenges and Future Trends. Hindawi Wireless Communications and Mobile Computing Volume 2022.
[17] Yogesh Patil, 10/2023. A secure privacy preserving and access control scheme for medical internet of things (MIoT) using attribute-based signcryption. International Journal of Information Technology.
[18] Alex Sharpe, 2023, Zero Trust Guiding Principles. Cloud Security Alliance, Bellingham, WA 98225, USA
[19] Zero Trust Maturity Model. April 2023. Cybersecurity and Infrastructure Security Agency Cybersecurity Division. Web Link: https://www.cisa.gov/sites/default/files/202304/zero_trust_maturity_model_v2_508.pdf
[20] Paul Simmonds, Zero Trust as a Security Principle.2023. Cloud Security Alliance, Bellingham, WA 98225, USA