Securing Energy Industries

Forcepoint

Brochure

X-Force Threat Intelligence Index 2022 :

"...the energy sector ranked as the fourth most affected sector in 2021, accounting for 8.2% of all observed attacks."

Securing Energy Industries

Electric and Gas organizations that deliver vital energy services around the world are constantly under pressure to defend against cyberattacks. As well as fending off malicious threats they must also maintain the system availability and integrity on which the business, customers, and communities depend.

As the industry continues to move towards digitalization, cyberattacks on energy and utility companies are growing in frequency and sophistication. Over the last five years the energy industry has become a prime target for cyberattacks. According to the X-Force Threat Intelligence Index 2022 ***"...the energy sector ranked as the fourth most affected sector in 2021, accounting for 8.2% of all observed attacks."***

In May 2021, the hacker group Darkside, executed a ransomware attack on the Colonial Pipeline, an American oil pipeline system, encrypting data for the ransom amount of $4.4 million USD and causing a five-day system shutdown. In another attack in early 2022, 17 oil refinery terminals in Germany, Belgium and the Netherlands had their supply networks halted due to a cyberattack. The threat landscape for the energy industry is expanding daily as threat actors continue to target one of our most important critical industries.

The unique intersection of digital systems and physical infrastructure of the energy industry requires flexible security solutions. Ones that can maintain the integrity of their sensitive controls and connected systems, including both IT and OT networks.

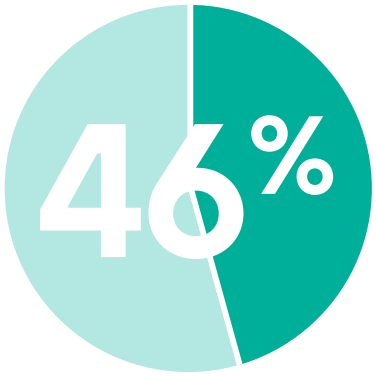
As we move to implement zero trust architectures and approaches to protect critical industries. It remains critical to ensure the security of nations energy industries that remain vital to our economies.

.

Challenges for Energy Industries

Phishing

Phishing attacks remain a favorite among cyber criminals, targeting employees and privileged users. Phishing emails are a severe threat, with Verizon estimating that "46% of organizations received malware via email" (Verizon Data Breach Report. (DBIR) 2020)



Percentage of organizations receiving email malware

Web-borne Threats and Malvertising

Hackers use spoof sites or even legitimate websites to carry exploits and malware. One form of this is malvertising, where usual legitimate ads on well-known websites are infected with malware. When a user navigates to an infected site, they may end up infecting their device. Malvertising is the no. 1 source of malware infection and alerts as of March 2022, according to the Center for Internet Security.

System Vulnerabilities

Most malware depends on software vulnerabilities. For example, malvertising aims to install malware without the user's knowledge. Malware can only be downloaded to a device if the software has a vulnerability that can be exploited, allowing it to install.

Zero Day Attacks

A zero day attack is a software vulnerability that is previously either unknown or unpatched. Why are zero day attacks so dangerous to critical industries? Because they defeat the majority of detection-based cybersecurity defenses, can cause significant hardware damage, and are the most used type of malware in ransomware attacks.

Ineffective Security Measures

A company's choice in security measures can often be the difference between data loss and data security. Cybersecurity is not a one-size-fits-all solution. Ensuring that appropriate measures are deployed for specific security needs is crucial.

Forcepoint Energy Services Product Portfolio

Forcepoint provides a comprehensive portfolio of products designed to help providers of power and energy utility services meet these challenges.

Forcepoint Zero Trust Content Disarm & Reconstruction (CDR): Zero Trust CDR works with the High Speed Verifier (HSV) to deliver malware-free data without using detection. It works by extracting the valid business information from files, verifying the extracted information is well-structured and then building brand new files to carry the information to its destination. This unique zero trust approach is applied to all data, irrespective of whether it contains a threat or not. It renders IT files such as Office and PDF documents and images threat-free and can also be applied to the web application traffic.

Forcepoint One: Forcepoint ONE is an all-in-one cloud-native security platform that makes it easy to adopt Security Service Edge (SSE) by unifying crucial security services.

With Forcepoint ONE, security teams can now manage a single set of policies across websites, cloud apps, and private apps, from one cloud-based console, through one endpoint agent, with agentless support for unmanaged devices.

Forcepoint iX Appliance with High Speed Verifier (HSV): Also referred to as a bidirectional diode, HSV is deployed as a physical on-premises appliance. Using verification in hardware logic ensures the appliance only receives safe, valid data. Using the HSV's hardware logic, not software, to send sensitive data and verify integrity reduces the potential attack surface and prevents malware attacks.

Forcepoint Data Guard: Data Guard enables the bidirectional, automated transfer of highly complex data — including real-time streaming video across segregated networks. With deep content inspection and highly granular policy-based control over source, destination, and content, Data Guard is ideally suited to cross-domain data transfer as it targets specific high assurance security requirements.

Forcepoint FlexEdge Secure SD-WAN and Next-Gen Firewall (NGFW): From the enterprise core to remote sites, FlexEdge Secure SD-WAN and Next-Gen Firewall combine seamless connectivity and industry-leading network security to connect and protect people and data. With applications designed from the ground up for high availability and scalability —as well as centralized management with full 360° visibility — Forcepoint network security provides consistent security, performance, and operations across physical, virtual, and cloud systems.

Forcepoint Data Diode / Unidirectional Gateway: Data Diode ensures secure one-way transfer with optical isolation, enabling organizations to create boundaries between trusted and untrusted networks by creating a physically secure one-way communication channel. Ideally suited to unidirectional protocols, Data diodes enable you to send data from one secure network to another; data is transferred using light instead of electrical signals, ensuring that data can enter but never exit.

Forcepoint Insider Threat (FIT): Forcepoint Insider Threat has been identifying and stopping threats from within for government and Fortune 100 customers for more than 15 years. With more than 1 million endpoints deployed, Forcepoint Insider Threat's proven solution protects some of the most sensitive organizations on the planet. One Fortune 100 retail client realized 60% ROI in the first year of deployment. Insider Threat empowers your organization, saving your team time and effort by automatically scoring and prioritizing your riskiest users, reducing the need to dig through thousands of alerts. This frees your team to focus on high-priority tasks and improves efficiencies. Forcepoint Insider Threat also provides the context and forensic evidence needed for undeniable attribution and chain of custody– simplifying investigations, prosecution, and compliance.

Forcepoint Solutions Summary

SCENARIO	REQUIREMENTS	CONSIDER THESE SOLUTIONS
Ring-fencing the enterprise	A zero-trust security posture for all inbound content arriving at the enterprise network	• High Speed Verifier with Zero Trust CDR • Secure SD-WAN and NGFW • Forcepoint ONE • Forcepoint Insider Threat • Behavioral Analytics
Monitoring networks from the cloud	Secure and reliable data transfer with no data loss	• High Speed Verifier with Zero Trust CDR • Secure SD-WAN and NGFW
Combatting phishing attacks, ransomware and zero-day exploits		• Zero Trust CDR • Forcepoint ONE • Forcepoint Insider Threat • Behavioral Analytics
Web browsing upload and download		• Zero Trust CDR • Forcepoint ONE • Data Loss Prevention (DLP) • Remote Browser Isolation
Email and file transfer		• Zero Trust CDR • Forcepoint ONE • DLP
Assured instant messaging		• Zero Trust CDR • Zero Trust CDR with iX Appliance • Forcepoint ONE

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on www.forcepoint.com, Twitter and LinkedIn.

[Securing Energy Industries Brochure]16Sept2022