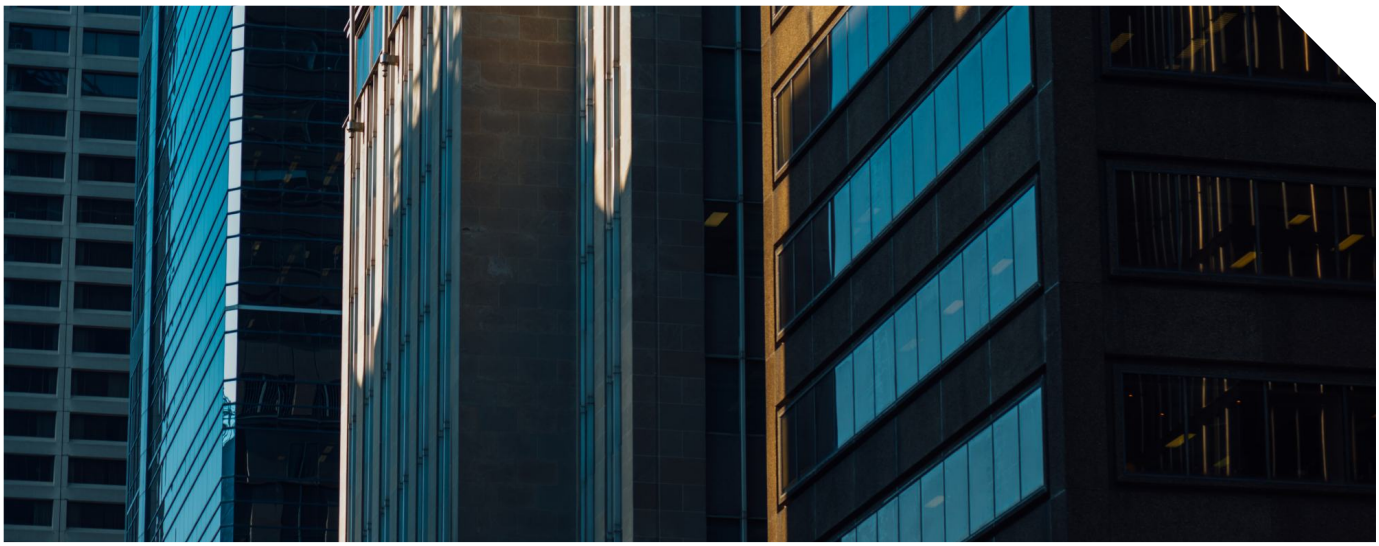
EVERFOX

BROCHURE

Securing Energy Industries



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 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.

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.

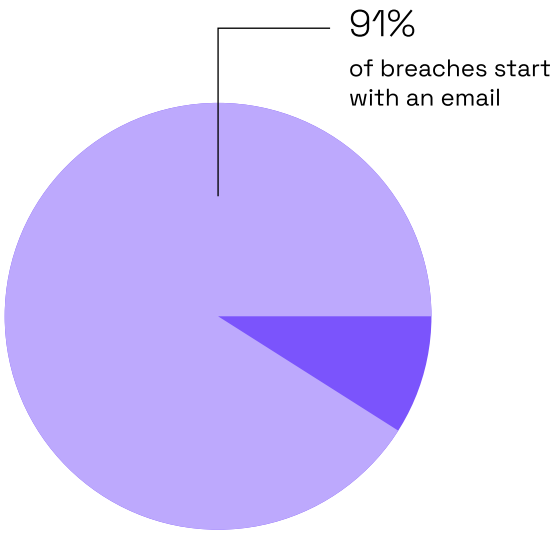
As we move to implement zero trust architectures and approaches to protect critical industries. It remains critical to ensure the security of nations energy industries that remain vital to our economies.

> “The energy sector ranked as the fourth most affected sector in 2024, accounting for 11.1% of all observed attacks”
>
> X-Force Threat Intelligence Index 2024

Challenges for Energy Industries

Email Security

Email security is a critical challenge for financial services due to an increase in malware, ransomware, phishing attacks and insider threats. With over 91% of breaches starting with an email. These challenges necessitate robust and adaptive email security measures



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.

Everfox Energy Services Product Portfolio

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

High Speed Verifier (HSV)

Everfox HSV combines the best of data transfer solutions with the added benefits of dual one-way data transfer and builtin threat removal. As a bi-directional data verifier, the way the HSV conveys information and hides the attack surface of the destination server makes it suitable for protecting your sensitive data.

Data Guard

Everfox 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 and targets specific high assurance security requirements.

Everfox Data Diode

The Everfox Data Diode enables rapid data transfers from one network to another, while ensuring that no information passes in the opposite direction. The Data Diode can be used to get information out of a critical network without introducing any means by which that network can be attacked.

Information eXchange (IX)

iX operates inline at the network perimeter to eliminate potential malware in business content, including unstructured formats like Office, PDF and structured data like XML, JSON.

Everfox Insider Risk

Everfox Insider Risk Solutions is a User Activity Monitoring (UAM) and Analytics platform which drive improvements in your insider risk program. Giving analysts and investigators the right tools needed to collect, explore, and gain insight into risky behavior.

Everfox Energy Services Product Portfolio

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

Content Disarm and Reconstruction (CDR)

Everfox CDR works 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

CDR for Mail: Microsoft 365

Email is the most common attack vector for cyber threats such as phishing, malware and ransomware. Resulting in organizational disruption, financial damage, and data loss. Get comprehensive protection for your most critical business investment. Everfox CDR for Mail: Microsoft 365 stops advanced malware, zero-days and unknown attacks that can lead to ransomware and other devastating impacts.

Application eXchange (AX)

Everfox Application eXchange (AX) is a set of APIs developers can use to access our Content Disarm and Reconstruction-as-a-Service (CDRaaS) and integrate it into workflows and applications. The CDR engine transforms Office, PDF, image files and more, removing evasive, zero-day malware, known and unknown threats. Eliminating even steganography threats often concealed in images.

Gateway eXtension (GX)

Extend the capability of your perimeter web defense with the Everfox Gateway eXtension (GX). Ensure complete protection from the ever-increasing onslaught of known, zero-day, and unknown content threats.

Solution 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 Everfox CDR • Everfox Insider Risk • Behavioural Analytics
Monitoring networks from the cloud	Secure and reliable data transfer with no data loss	• High Speed Verifier with Everfox CDR
Combatting phishing attacks, ransomware and zero-day exploits		• Everfox CDR • Everfox Insider Risk • Behavioural Analytics
Web browsing upload and download		• Everfox CDR • Gateway eXtension
Email and file transfer		• Everfox CDR • Data Guard • Data Diode
Assured instant messaging		• Everfox CDR • CDR with iX Appliance

About Everfox

Everfox, formerly Forcepoint simplifies security for global businesses and governments. Everfox'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.

Learn More

www.everfox.com