OPSWAT.

Energy Sector Case Study

Critical Infrastructure Protection

A major US energy company turned to OPSWAT to implement a consistent process for securing 10+ critical networks by eliminating the risks resulting from vulnerabilities, malware or zero-day attacks. By implementing MetaDefender® Kiosks and MetaDefender Vault to secure the transfer of files into and out of their critical infrastructure, the company meets existing and emerging NERC CIP regulatory requirements.

CHALLENGES

Securing data and device transfer across the entire perimeter

The company featured in this case study is a major US energy company who has requested to remain anonymous. Future references will be "EnergyCo" to protect their identity. EnergyCo produces and distributes power and fossil fuel products throughout the United States.

EnergyCo air-gapped systems are continually modified with system updates, maintenance, and upgrades using data downloaded from employee's and contractor's portable devices, including CDs, USB flash drives, laptops, external hard drives, memory cards, PDAs and other removable media.

Their objective was to mitigate the risk of all potential malware on all devices before entering a facility. Also, the company believes that implementing OPSWAT's zero-trust governance of all devices, data and ICS will help meet new NERC CIP requirements — regarding Transient Cyber Assets (TCAs), Removable Media (RM) and reliability

Meets NERC CIP Requirements

10+ Air-Gapped Networks Protected

IT & OT OPSWAT Academy CIP Certified

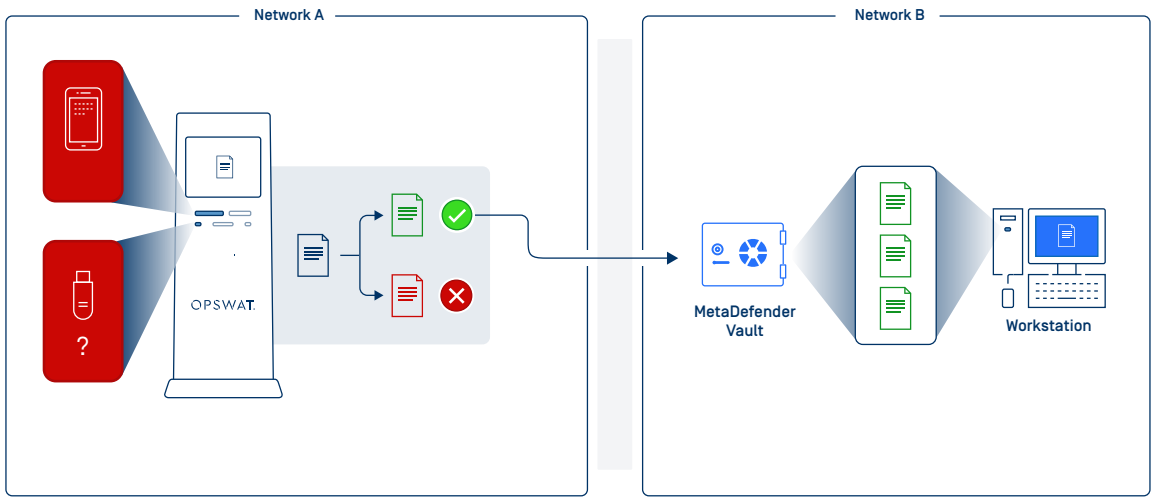
2021.01.11 CS-NA (AAB)

standards (i.e., NERC CIP-005-6, CIP-010-3 and CIP-013-1). Given recent developments, EnergyCo wants to implement good governance best practices that will help meet cybersecurity requirements that may result from the Bulk Power Executive Order (#13929) legislation.

SOLUTION

MetaDefender Kiosk + MetaDefender Vault

OPSWAT products have been successfully protecting 98% of America's nuclear facilities for years. Based on a recommendation from a nuclear facility partner, EnergyCo decided to test the OPSWAT Cross-Domain solution, comprised of MetaDefender Kiosks and MetaDefender Vault. They wanted to have the same level of security as their nuclear partner.



MetaDefender Kiosk Interface shows processing of USB with direct on-screen feedback

EnergyCo chose MetaDefender Kiosk and MetaDefender Vault because it prohibits employees, contractors, and visitors from introducing infected media into any company facilities. They placed the Kiosks at guarded entry points for all air-gapped networks across over 10 locations and focused access into and out of the facilities through those gates. The MetaDefender Kiosks provides EnergyCo with:

- **Digital Perimeter Control –** Secure control of the transfer of files and devices across security levels, systems, and physical transfer points.
- **Enforced Secure Data Transfer Processes –** Enforcement of secure file transfer processes, continuous scans for malware, and added digital signatures to ensure files are free from risk infection, while in transit or at rest.
- **Breach Prevention –** Proactive visibility and control of sensitive data at every transfer point across their networks.

EnergyCo also implemented MetaDefender Vault across the organization. Vault provides secure file storage and retrieval integrated with Microsoft Active Directory, allowing only approved access to sanitized files within a secured network. Vault provides EnergyCo with:

- **Outbreak Prevention –** A file entering the network is now thoroughly scanned against continuously updated virus definitions. Suspicious files are sanitized, blocked, and redacted based on EnergyCo security policies. Every file entering Vault is encrypted, and access is blocked for a containment period to prevent latent outbreaks and zero-day attacks.
- **Secure Data Flow Processes –** Data entering the organization is encrypted and secured with Advanced Encryption Standard (AES), and multi-stage approvals based on RBAC help enforce workflow rules.
- **Visibility and Control –** All storage and retrieval activities are logged and fully-auditable, including notifications for response management.

As part of the implementation, EnergyCo turned to the OPSWAT Academy Critical Infrastructure Protection (CIP) Certification Program to help educate and certify their IT/OT staff on best practices, and efficient use of OPSWAT solutions to maximize protection against malicious attacks.

RESULTS

Controlling the Risk of Malware and Zero-Day Attacks

EnergyCo now has a consistent process across its 3,000+ employees that sanitizes all suspicious files entering the organization. It protects them from file-based exploits utilizing 30+ industry-leading multiscanning anti-malware engines with automated workflows aligned with the company's strict security policies.

The company is now able to govern and secure data and device transfer for air-gapped and segmented network environments, by detecting and controlling the threats from malware and zero-day attacks before they enter from a device or file into the network.

About OPSWAT

To learn more about OPSWAT Critical Infrastructure Protection solutions, contact us today.

2021.01.11 CS-NA [AAB]