SYMMETRY SYSTEMS

Industry Solution Brief

Energy, Oil and Natural Gas

Energy, oil & natural gas organizations keep our modern world running. These organizations have access to large volumes of intellectual property, client and customer data, and other critical information. They have the ability to control the supply of energy, oil pipelines, gas pipelines, refineries, and other critical infrastructure. Threat actors, nation-state sponsored hackers and cyber criminals are keenly aware of the benefits they might attain by breaching an energy, oil & natural gas businesses network, and collecting its data. Companies in this industry cannot have a purely reactive security program focused on defending the perimeter, they need to build a world-class cyber security program starting from data security and expanding out into all parts of their global footprint.

The Energy, Oil & Natural Gas Data Security Challenge: Attack Velocity and Compliance

Attack Volume and Velocity

Ransomware attacks have been growing in volume and in effectiveness over the past few years. Ransomware by nature seeks to take control of data and a lot of times organizations aren't able to evaluate if the data is sensitive, protected, or mission critical. In order to properly evaluate the risk or or impact of ransomware attacks, energy, oil & natural gas organizations need to classify their data. They also need to have data security measures in place to make sure that ransomware actors cannot move laterally across cloud data stores, picking and choosing the data they consider worth holding for ransom.

Compliance and Data Privacy

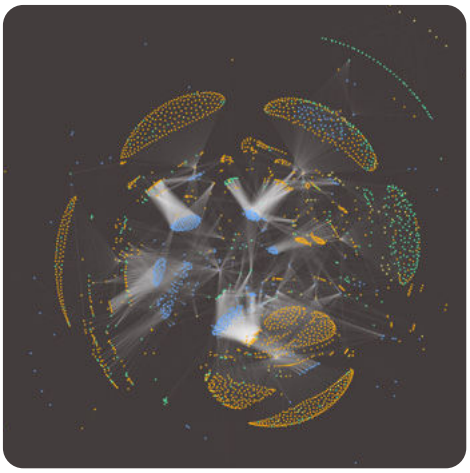
Energy, oil & natural gas companies collect massive volumes of data and operate across multiple jurisdictions and borders. It is a tremendous challenge for them to maintain pace and compliance with various evolving privacy law requirements – GDPR, CCPA, and more.

Data Security Best Practices with Cloud Adoption

- Understand where data is stored, how it is accessed, and how it is used, so that proper access permissions can be enforced.
- Gain visibility and effectively manage data security posture, e.g., detecting dormant data, while transitioning to hybrid cloud operations.
- Sustain and maintain pace with evolving regulatory requirements (such as NERC, GDPR, etc.) while differentiating services from competition.

Symmetry Systems DataGuard

DataGuard is a **data security posture management (DSPM)** solution that extends the Zero Trust philosophy to hybrid cloud data stores. Energy, oil & natural gas industry cybersecurity teams use DataGuard to develop a complete understanding of what data they have, where it is located, who has access to it, how it is secured and in what manner it has been used. DataGuard enables businesses with a single source of truth about their data security posture and associated data risks across AWS, GCP, Azure, and on-premise environments – **without having data ever leaving their environment.**



DataGuard produced Environment Graph

The cybersecurity industry is saturated with security solutions that focus on peripheral security and protection within the environment. DataGuard directly addresses data objects and examines the cross-section of identity, data store, and data flow to answer important questions:

- **Where is our sensitive data?**
- **Who has access to it?**
- **What operations have they performed against it?**

With DataGuard, cross-functional teams such as security operations, cloud security, compliance, and identity & access management, can enforce least privilege, sustain regulatory compliance, improve their data security posture, and outpace ever-growing data security risks and threats.

Identify Your Data

Perform agentless scans of all data living across AWS, Azure, GCP and on-premise cloud for a real-time snapshot or historical comparisons. DataGuard enables compliance and cloud migration teams to identify where sensitive data resides without having the data leave their cloud environment. With DataGuard, security teams can easily maintain compliance with challenging industry regulations such as **GDPR, CCPA, NERC,** and others.

Gain Full Visibility

Gain visibility into the entire data landscape with a complete, read-only data security posture map. DataGuard surfaces inactive accounts, dormant data stores, anomalous data flows, and cross-account permissions. It simplifies risk, event detection, incident remediation, and forensics for cloud engineering, security operations teams, and incident response teams.

Detect and Respond

Uncover unsafe data access practices and risky operations detected by DataGuard's built in data firewalls. Alert on violations and potential data breaches to minimize cyber risk exposure. DataGuard provides meaningful, evidence-based insights so that security operations teams can shorten the mean-time-to-recovery (MTTR) while reducing the attack surface for malicious acts, such as ransomware.

Protect Your Data

Deploy least privilege permissions on IAM, cloud accounts, and data store access. Cloud security teams can adopt DataGuard provided data firewall recommendations to tighten access control and minimize blast radius. DataGuard bakes data security into your data ecosystem versus adding peripheral protection.

SYMMETRY SYSTEMS

symmetry-systems.com | hello@symmetry-systems.com

LinkedIn / symmetry-systems-inc

Twitter / @SymmetrySystems