



WHITE PAPER

Energy, Oil & 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.



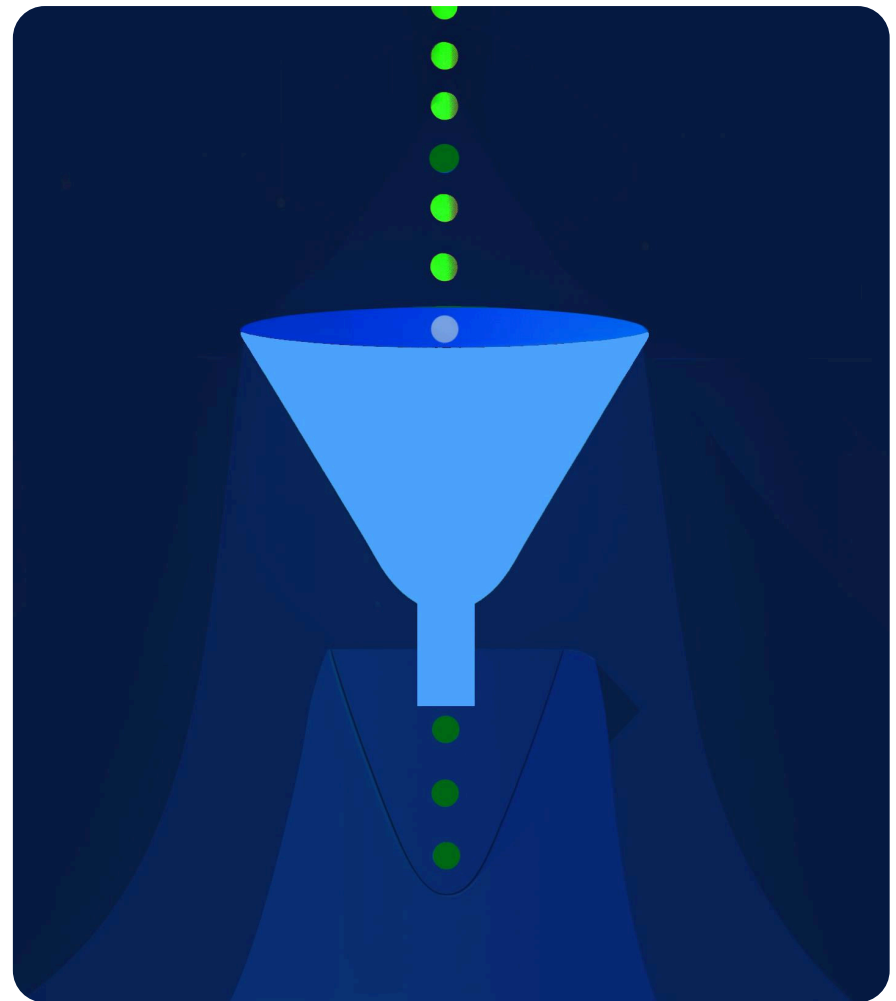
The Energy, Oil & Natural Gas Data Security Challenge: Attack Velocity and Compliance

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

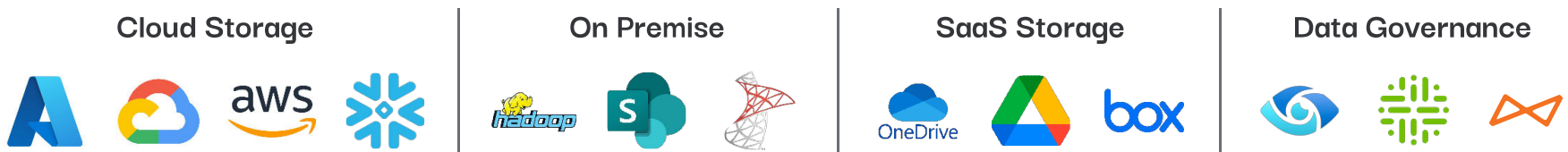
Symmetry's platform is engineered specifically to address modern data security and privacy challenges at scale from the data out, providing organizations the ability to innovate with confidence. With total visibility into what data you have, where it lives, who can access it, and how it's being used, Symmetry safeguards your organization's data from misuse, insider threats, and cybercriminals, as well as unintended exposure of sensitive IP and personal information through use of generative AI technologies.

WHAT WE DO

Symmetry offers comprehensive visibility and control over your data, addressing all aspects of your data security requirements, including the full spectrum of functions outlined in the NIST Cybersecurity Framework.

 <h3>Identify</h3> <p>Discovers, classifies, maps, and monitors sensitive data across cloud, on-prem, and hybrid environments.</p>	 <h3>Detect</h3> <p>Identifies and creates alerts for abnormal data behaviors and data policy violations in real-time.</p>
 <h3>Protect</h3> <p>Discovers, classifies, maps, and monitors sensitive data across cloud, on-prem, and hybrid environments.</p>	 <h3>Respond & Recover</h3> <p>Contain the security and business impact of compromised identities and impacted data with speed and precision.</p>

INTEGRATION INTO YOUR MODERN DATA+AI SECURITY STACK



FLEXIBLE DEPLOYMENT MODEL FOR YOUR ENVIRONMENT

Our deployment model is tailored to your operational needs and risk appetite. Whether it's air-gapped, fully in your cloud, traditional SaaS, or hybrid-cloud - we have done it.

