SYMMETRY

WHITE PAPER

Cyber Insurance

All organizations and the data they manage have been high value targets for threat actors for decades, resulting in an increase in the demand for cyber insurance. Tremendous efforts have been made by Cyber Insurers to increase the accuracy in pricing the cyber risk of their customers. Premiums have increased exponentially as a result of failure to protect data from credential compromises and ransomware. Current cyber insurance assessment approaches rely on external ratings services, patchy industry data on losses, and time-consuming questionnaire based assessments, not on how well organizations protect the sensitive data the threat actors want to attain. Cyber Insurers need to establish new due diligence approaches that assess their customers ability to protect their most critical and insurable asset, their data.

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

The Cyber Insurance Challenge: Insuring Customer Data

COMPLIANCE AND DATA PRIVACY

The most common loss event underwritten by CyberInsurers remains data breaches. The breach of customer data is subject to increasingly stringent privacy law requirements regardless of jurisdictions and borders, and data breaches may be subject to significant fines from modern privacy regulations – GDPR, CCPA, LGDP, SOX, and others.

EXPLOSION OF DATA

While insureds transition to a hybrid cloud environment, the data accumulated and stored multiple times within these environments with the change in user permissions during the transition create massive risk to the company. This risk is continuously exploited by threat actors. On account of this the costs of incident response have increased by 36%. In 2021 the industry experienced an average cost per breach of $5.85M.

LOSS AGGREGATION FROM SINGLE LOSS EVENTS

Additionally, insurers may be subject to multiple losses from a single event; as credential compromises in a single organization can be used to gain access in other organizations due to reuse of passwords by customers and third parties servicing multiple clients.

Data Security Best Practices with Cloud Adoption

Understand the volume of personal data stored by an insured, how it is accessed, and how it is used, so that coverage can be properly priced and ensure insureds enforce least privilege access permissions to reduce impact from insured events.

Gain visibility into insured's data security posture, e.g., detecting dormant data, while transitioning to hybrid cloud operations.

Help insureds sustain and maintain pace with existing and evolving regulatory requirements (such as GDPR and CCPA) by demonstrating appropriate controls over personal information within their control.

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.

Identify

Discovers, classifies, maps, and monitors sensitive data across cloud, on-prem, and hybrid environments.

Detect

Identifies and creates alerts for abnormal data behaviors and data policy violations in real-time.

Protect

Discovers, classifies, maps, and monitors sensitive data across cloud, on-prem, and hybrid environments.

Respond & Recover

Contain the security and business impact of compromised identities and impacted data with speed and precision.

INTEGRATION INTO YOUR MODERN DATA+AI SECURITY STACK

Cloud Storage

On Premise

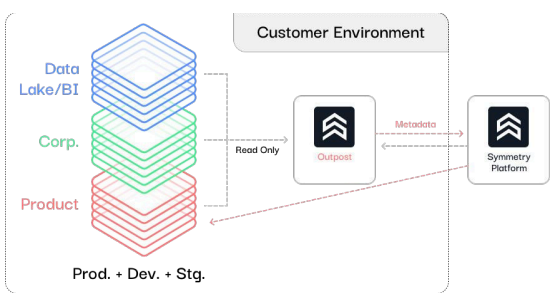
SaaS Storage

Data Governance

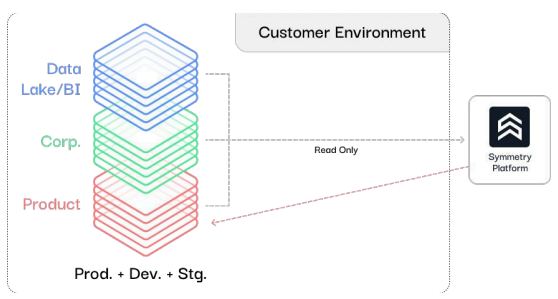
FLEXIBLE DEPLOYMENT MODEL FOR YOUR ENVIRONMENT

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.

SaaS Model



Outpost Model



Air-Gapped/In-Your-Cloud Model*