SYMMETRY

WHITE PAPER

Technology

Technology companies drive innovation and economic growth. The Internet unleashed businesses to optimize their operations, scale to support growth and enhance customer experiences. However, the Internet of Things, machine learning, artificial intelligence, remote work technologies, communication technologies, and many more have opened up a plethora of cyber risks that businesses must utilize to protect themselves and their data from.

Legacy cybersecurity technologies and processes are designed to defend the perimeter and endpoints, not the data the threat actors want to attain. Technology cybersecurity teams need to establish data security practices to protect their most critical asset, their data. Technology companies must protect their reputations, revenue, and trustworthiness by protecting their data.

The Technology Data Security Challenge: Protecting Proprietary Business Information and IP Theft

VENDOR/PARTNER RISK

Technology companies and their products combine mobile, network, hardware, software, and data storage capabilities. These multi-provider networks create dependencies and a massive volume of data that needs to be stored and protected. Businesses, vendors, and customers are interconnected via APIs, portals, and, most importantly, data. If one customer or vendor experiences a breach, this might create a domino effect in which customer data, business data, vendor data, and mission critical data is exposed or stolen.

COMPLIANCE AND DATA PRIVACY

Most technology companies operate across multiple jurisdictions and borders, and are challenged to maintain pace and compliance with various evolving privacy law requirements – GDPR, CCPA, and more.

INTELLECTUAL PROPERTY (IP) THEFT

Technology businesses are targets for IP theft. These organizations protect data such as blue prints, chemical formulas, trade secrets, company contacts, go to market strategies, and more. In order to protect IP, technology companies need to know where it is stored, who has access to it, and what is being done with that data.

Data Security Best Practices with Cloud Adoption

Understand where customer 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 information security standards and regulatory requirements (such as SOC2, ISO 27001, ISO 27017, ISO 27018, ISO 27701, CIS Standards, CSA STAR, FedRAMP, StateRAMP, TX-RAMP, GDPR and CCPA) 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.

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

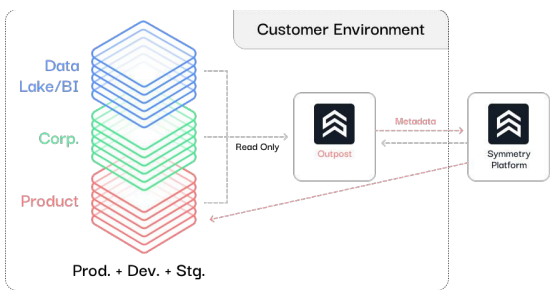
SaaS Storage

Data Governance

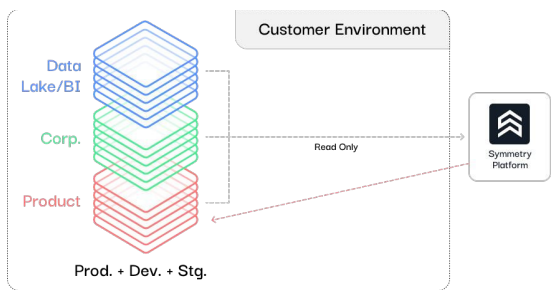
FLEXIBLE DEPLOYMENT MODEL FOR YOUR ENVIRONMENT

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*