SYMMETRY

WHITE PAPER

Communications & Media

Threat actors love to target communications & media companies. The business model for these organizations relies heavily on collecting customer data, payment processing data, advertising data, and more. If a threat actor is able to breach a communication & media organization, they will likely be able to collect data that can be used to conduct sophisticated attack reconnaissance or develop spear phishing campaigns against their customers. They could also collect personally identifiable information (PII) and payment card data that they can use for financial gain immediately.

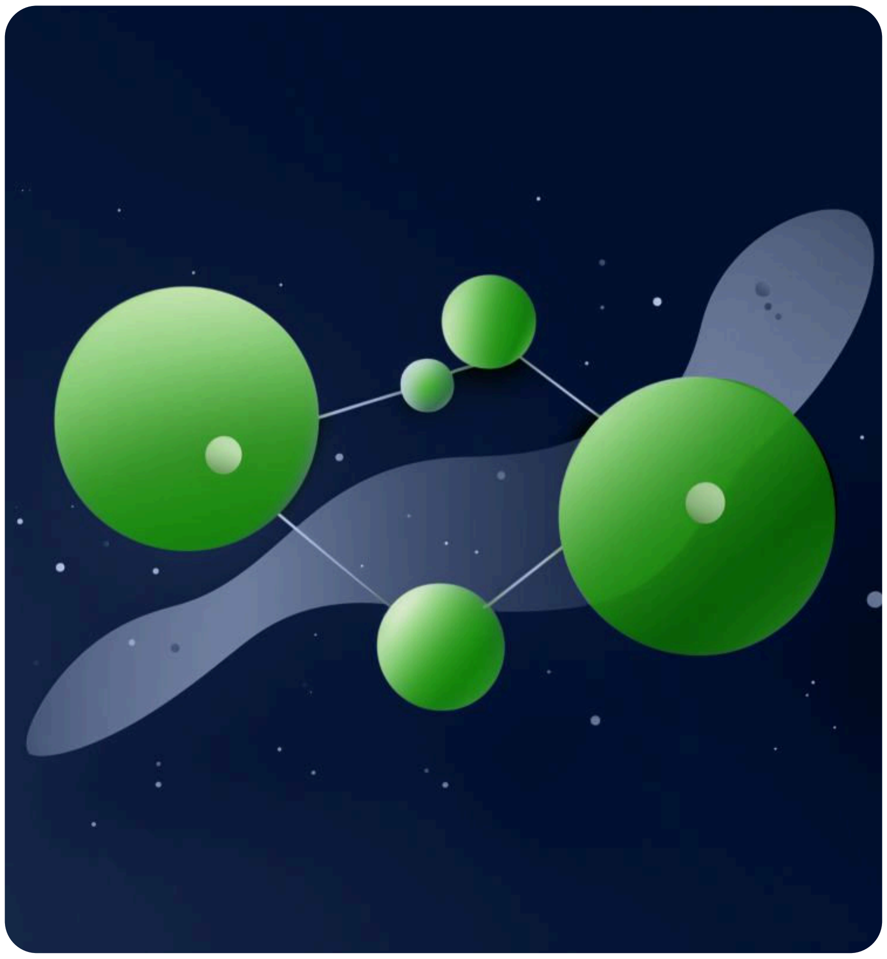
With millions of users, thousands of clients, dozens of interconnected technologies and applications, and a vast infrastructure that is challenging to protect, these companies have numerous entry points for third-party attacks.

The impact of successful attacks can be significant and far reaching. Business reputations can be ruined, stock prices can drop and the organization’s ability to grow and succeed can be impeded. Legacy cybersecurity technologies were designed to defend the perimeter and endpoints, not the data the threat actors want to attain. Communications & media security teams need to establish data security practices to protect their most critical asset, their data. They must protect their reputations, revenue, and trustworthiness by defending their data.

The Communication & Media Industry Data Security Challenge: Protecting Customer and Proprietary Business Information

THIRD-PARTY RISK

Media & communication companies and their products combine mobile, network, hardware, software, and data storage capabilities. These 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

Communication & media 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.

CUSTOMER DATA PROTECTION

It has been reported 69% of consumers would be less inclined to do business with a breached organization. Communication & media companies, business-to-business and business-to-consumer, collect customer data in droves. The sheer volume of customer data that is collected in the sales and marketing process, as well as user data that is generated throughout the life of the technology is tremendous. In order to protect customer data, 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 regulatory requirements (such as 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

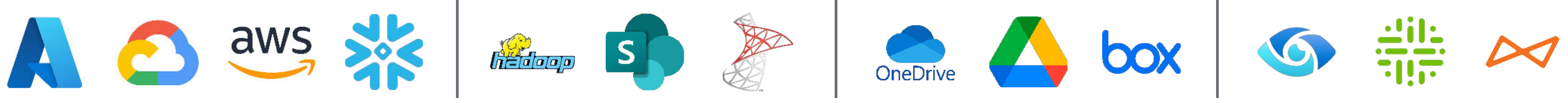
Discovers, classifies, maps, and monitors sensitive data across cloud, on-prem, and hybrid environments.

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

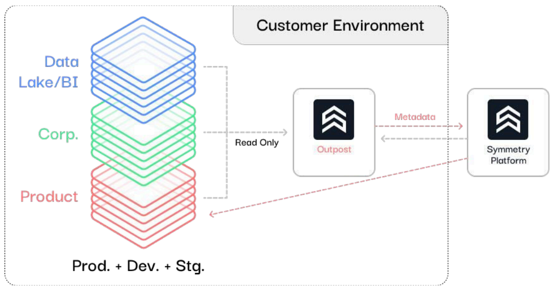
Cloud Storage | On Premise | SaaS Storage | Data Governance



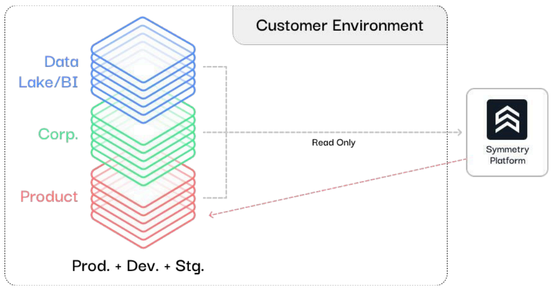
FLEXIBLE DEPLOYMENT MODEL FOR YOUR ENVIRONMENT

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.

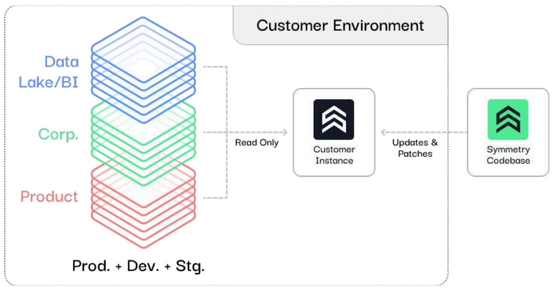
SaaS Model



Outpost Model



Air-Gapped/In-Your-Cloud Model*


Customer Environment
Data Lake/BI
Corp.
Product
Prod. + Dev. + Stg.
Read Only
Customer Instance
Updates & Patches
Symmetry Codebase