SYMMETRY

WHITE PAPER

Healthcare

Healthcare organizations are a primary target for hackers, nation-state sponsored threat actors and cyber criminals. With patient data at stake, a cyberattack places healthcare providers, hospitals, medical centers, their vendors, and their partner organizations at significant risk for cyber attacks. Obtaining private identifiable information (PII) is a lucrative goal for threat actors, as the data can be sold on the dark web, or otherwise utilized for nefarious purposes. Legacy cybersecurity technologies and processes are designed to defend the perimeter and endpoints, not the data the threat actors want to attain. Healthcare industry cybersecurity teams need to establish data security practices to protect their most critical asset, their data.

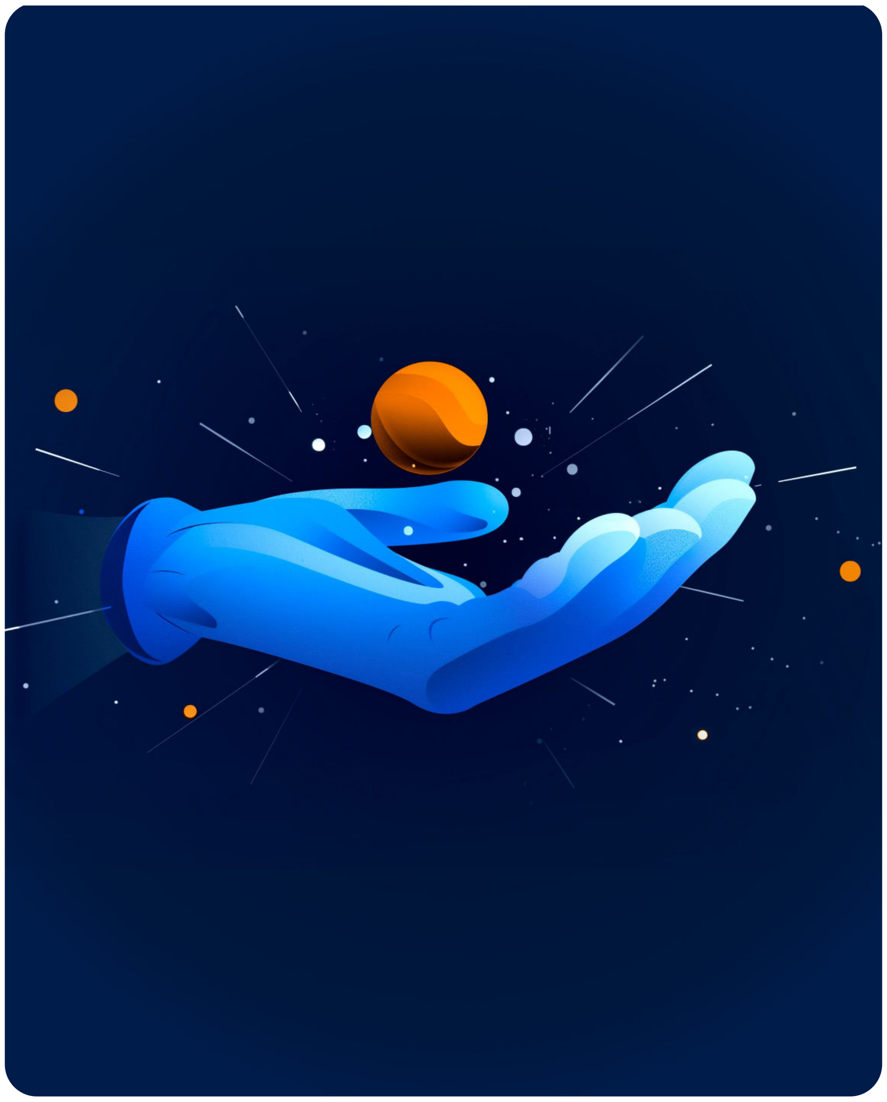
The Healthcare Data Security Challenge: Protecting Patient Data

COMPLIANCE AND DATA PRIVACY

Industry regulations such as HIPAA and HITECH demand information security around many elements, including data security, data visibility, and access control. Increasing cloud adoption, as well as widely adopted telemedicine spurred by the COVID pandemic, has increased vulnerabilities and threats to healthcare organizations. This has increased cyber risk exposure for healthcare organizations and has made security and compliance efforts even more painstaking.

TRANSITION TO HYBRID CLOUD

With continued data migration to the cloud, the healthcare industry is experiencing the associated challenges of exploding data volumes and inevitable data sprawl. Healthcare security operations teams are often forced to find a needle in a haystack using solutions not purpose-built for data security that often require manual tasks. The healthcare industry had the worst per-data-breach cost of $9.23M in 2021, a 30% increase from $7.13M in 2020*. Pharmaceuticals was $5.04M*.



Data Security Best Practices with Cloud Adoption

Conform to HIPAA, French HDS, ISO 27799, HITRUST and other health data regulatory compliance/ standards while moving into hybrid cloud operations.

Minimize potential data risks and exposure with visibility into the enterprise data across cloud environments.

Automate data management and security tasks on a single console for the hybrid cloud.

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.

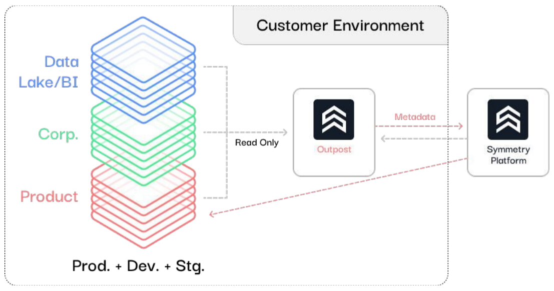
INTEGRATION INTO YOUR MODERN DATA+AI SECURITY STACK

Cloud Storage | **On Premise** | **SaaS Storage** | **Data Governance**

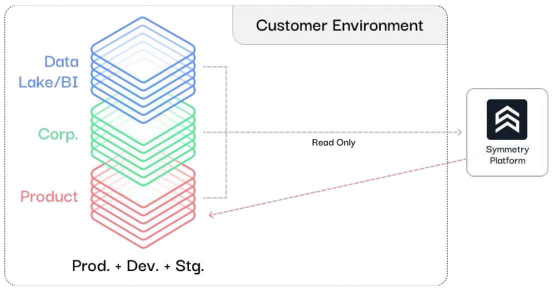
FLEXIBLE DEPLOYMENT MODEL FOR YOUR ENVIRONMENT

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.

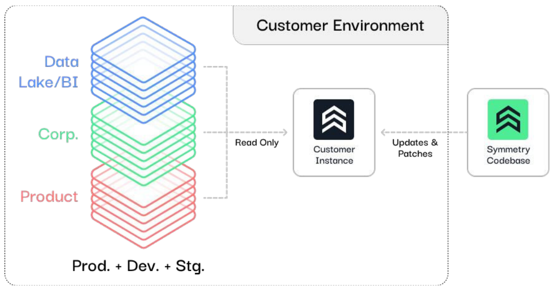
SaaS Model



Outpost Model



Air-Gapped/In-Your-Cloud Model*


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