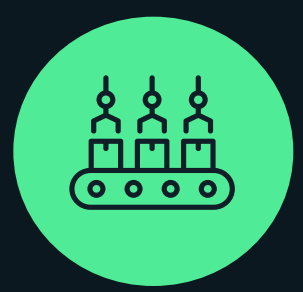
SYMMETRY



WHITE PAPER

Manufacturing

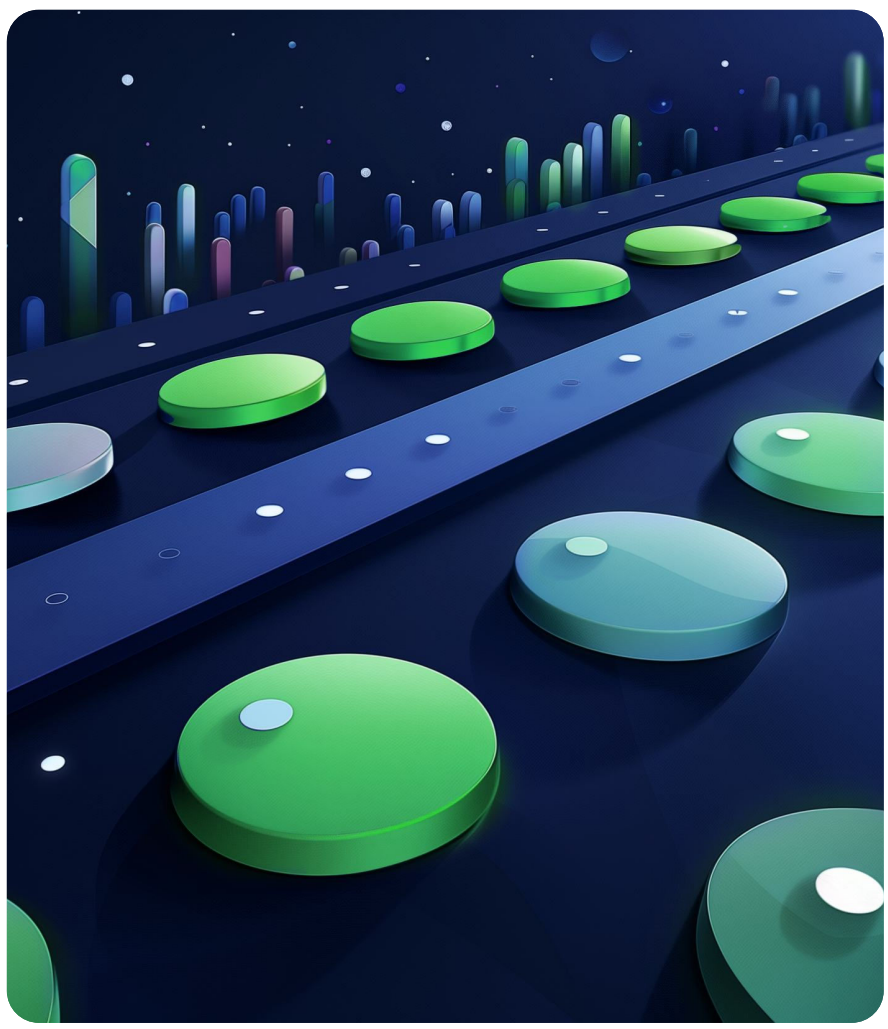
Manufacturing organizations are the backbone of the global economy. These organizations collect vast amounts of data from their customers, supply partners, research & development projects, and more. In the last few years there has been a boom in terms of manufacturing organizations using automation, Internet of Things, artificial intelligence, and cloud computing to optimize their businesses and compete in international markets at a higher velocity. However, the faster a manufacturing organization moves to innovate and automate, the faster their security team must move to secure the business from cyber threats.

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

The Manufacturing Data Security Challenge: Protecting Customer and Proprietary Business Information

SUPPLY CHAIN PARTNER RISK

Manufacturing companies are highly susceptible to supply chain attacks. Threat actors will happily attack supply chain partners to laterally move through their networks, collect identity and access control credentials for manufacturing partners, and will then breach their main target organization. These supply chain partnerships create dependencies, shared user credentials and access to portals, and a massive volume of data that needs to be stored and protected. If one supply chain partner 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

Manufacturing organizations 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, manufacturing 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 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

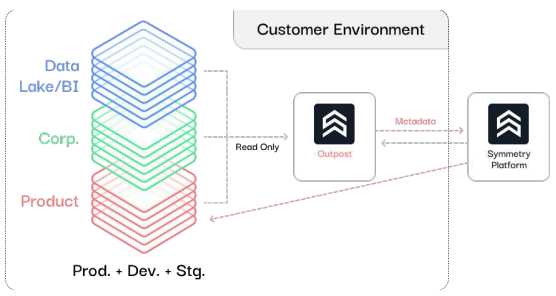
SaaS Storage

Data Governance

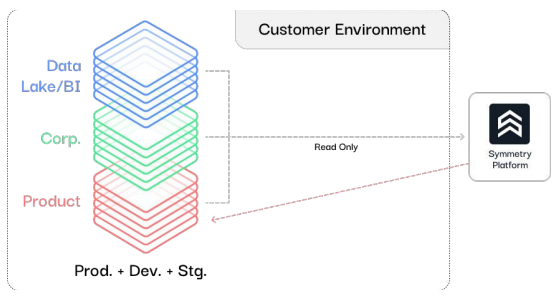
FLEXIBLE DEPLOYMENT MODEL FOR YOUR ENVIRONMENT

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*