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 them 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 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

DataGuard is a **data security posture management (DSPM)** solution that extends the Zero Trust philosophy to hybrid cloud data stores. Manufacturing industry cybersecurity teams use DataGuard to develop a complete understanding of what data they have, where it is located, who has access to it, how it is secured and in what manner it has been used. DataGuard enables businesses with a single source of truth about their data security posture and associated data risks across AWS, GCP, Azure, and on-premise environments – **without having data ever leaving their environment.**

The cybersecurity industry is saturated with security solutions that focus on peripheral security and protection within the environment. DataGuard directly addresses data objects and examines the cross-section of identity, data store, and data flow to answer important questions:

- **Where is our sensitive data?**
- **Who has access to it?**
- **What operations have they performed against it?**

With DataGuard, cross-functional teams such as security operations, cloud security, compliance, and identity & access management, can enforce least privilege, sustain regulatory compliance, improve their data security posture, and outpace ever-growing data security risks and threats.
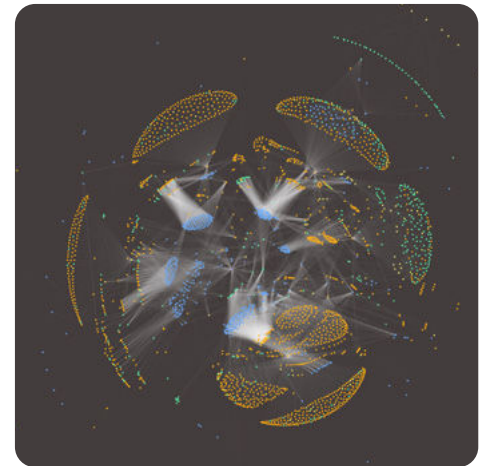
DataGuard produced
Environment Graph

Identify Your Data

Perform agentless scans of all data living across AWS, Azure, GCP and on-premise cloud for a real-time snapshot or historical comparisons. DataGuard enables compliance and cloud migration teams to identify where sensitive data resides without having the data leave their cloud environment. With DataGuard, security teams can easily maintain compliance with challenging industry regulations such as GDPR, CCPA, and others.

Gain Full Visibility

Gain visibility into the entire data landscape with a complete, read-only data security posture map. DataGuard surfaces inactive accounts, dormant data stores, anomalous data flows, and cross-account permissions. It simplifies risk, event detection, incident remediation, and forensics for cloud engineering, security operations teams, and incident response teams.

Detect and Respond

Uncover unsafe data access practices and risky operations detected by DataGuard's built in data firewalls. Alert on violations and potential data breaches to minimize cyber risk exposure. DataGuard provides meaningful, evidence-based insights so that security operations teams can shorten the mean-time-to-recovery (MTTR) while reducing the attack surface for malicious acts, such as ransomware.

Protect Your Data

Deploy least privilege permissions on IAM, cloud accounts, and data store access. Cloud security teams can adopt DataGuard provided data firewall recommendations to tighten access control and minimize blast radius. DataGuard bakes data security into your data ecosystem versus adding peripheral protection.