

Data Security for *Manufacturers*

Manufacturing organizations invest years developing the CAD files, product designs, formulas, production processes, and trade secrets that define their competitive position. These assets move constantly: across engineering teams, to external partners and contract manufacturers, through supply chain collaboration portals, and into AI tools built for computer vision, robotics, and design prototyping. Legacy data loss prevention (DLP) tools were not designed to follow this path.

As manufacturing became the most targeted industry for cyberattacks for the fifth consecutive year, the gap between what security programs can see and what is actually leaving the environment demands a different approach.

27.7%

of all cyber attacks targeted manufacturing in 2025, the most attacked industry for the fifth consecutive year

IBM X-Force Threat Intelligence Index 2026

40%

of manufacturing cyberattacks involved data theft targeting financial assets and intellectual property, including trade secrets

IBM X-Force Threat Intelligence Index 2026

80.5%

of GenAI tools used in manufacturing are classified as medium to critical risk

Cyberhaven 2026 AI Adoption and Risk Report: Manufacturing

How Cyberhaven Protects Manufacturing IP



Protect IP Without File Tags or Production Disruption

Cyberhaven uses context, including where data was created, who created it, and how it has moved, to identify and protect CAD files, product designs, formulas, and production processes without requiring manual file tags or content labels. Security policies apply from the moment IP is created and follow it across every application.



Maintain Visibility Across the Supply Chain

Manufacturing organizations share sensitive designs and specifications with hundreds of suppliers, design partners, and contract manufacturers. Cyberhaven tracks data from internal creation to external destination, detecting when proprietary files leave authorized channels.



Govern AI Adoption Before It Becomes an IP Exposure

Manufacturing organizations use AI for industry-specific needs: computer vision, robotics, multimedia creation, and model prototyping. 80.5% of those tools carry medium-to-critical risk. Cyberhaven tracks what design files, specifications, and process data enter AI applications in real time.

The Data Lineage Difference

Cyberhaven's Data Lineage technology traces every piece of data from its origin, recording every copy, move, edit, and share across engineering workstations, SaaS tools, supply chain portals, and AI applications. That complete context is what makes IP classification accurate and investigations fast, without requiring manual tagging or policy maintenance every time a new tool enters the environment.



**Identify IP Exposure
Without Pre-Built Policies**



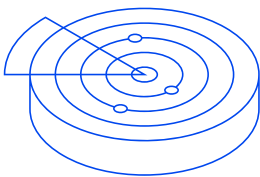
**Protect IP Across Complex
Engineering File Formats**



**Accelerate Insider and
Supply Chain Investigations**

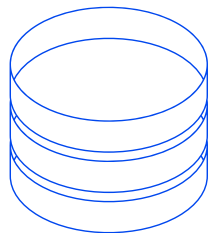
One Platform: DLP, DSPM, IRM, and AI Security

Cyberhaven delivers a unified platform so your security team maintains full context in a single console, with no tool-switching and no lost lineage between products. Surface actionable findings instead of raw alerts, and respond without disrupting engineering workflows or production operations.



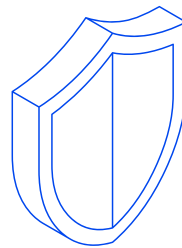
DLP

Data loss prevention (DLP) that stops exfiltration of CAD files, IP, and process data across email, web, cloud, and endpoints, with real-time coaching to guide behavior before incidents occur.



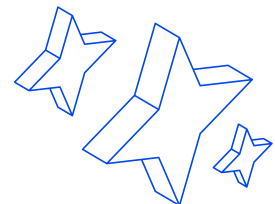
DSPM

Data security posture management (DSPM) that discovers and classifies sensitive engineering and operational data, then detects risk as it flows between clouds, SaaS tools, and devices.



IRM

Insider risk management (IRM) that combines data movement and behavior signals to surface abnormal access patterns, off-hours bulk transfers, and supply chain staging activity before data leaves the organization.



AI Security

AI Security that tracks what design files and process data enter AI tools, enforces policies on unapproved applications, and governs the specialized AI workflows, including computer vision and robotics tools, that manufacturing teams depend on.

See What Is Happening to Your IP

Protect your competitive edge without slowing down engineers, supply chain teams, or production operations.

[Request a demo](#)

About Cyberhaven

Cyberhaven reimagines data security. AI-based classification combined with Data Lineage technology analyzes billions of data workflows to understand every piece of data within an organization, identify when it is at risk, and take action to protect it. To learn more, visit cyberhaven.com.