FORTRA

A New Approach to Data Security for Manufacturing Companies

A visual guide to the challenges and solution requirements for seurely sharing IP, trade secrets, and other sensitive data.

Your Sensitive Data Is On The Move... Everywhere

Intellectual Property
- Design Plans & Blueprints
- Proprietary Formulas, Techniques, and Other Trade Secrets
- Research & Product Development

Finance
- Corporate Earnings Reports
- Financial Projections
- Budget & Asset Allocations

Sales & Marketing
- Internal Strategy Documents
- Pricing Data/Models
- Private Customer Data

Operational IP
- Manufacturing Specications
- Proprietary Process Documents
- Production Reports/Plans

Legal
- Supply Chain Agreements
- Customer/Retailer Contracts
- Patent Applications

Human Resources
- Condential Employee Data
- Compensation Plans
- Medical/Insurance Information

Widespread collaboration—both internally among employees and externally among 3rd-party and international contract manufacturers and suppliers—is critical to just-in-time production, margin preservation, and ongoing innovation. Simply put, it's an essential building block of your business.

The 3 C's Driving Data Sharing Today

New collaboration technologies emerge daily—many of which are outside IT's control.

Rapid adoption of cloud services results in more data beyond the corporate perimeter.

The work-from-home trend—accelerated by COVID-19 pandemic—pushes data sharing to unprecedented levels.

Greater Sharing = Greater Exposure = Greater Risk

$180B to $540B

estimated annual cost to U.S. companies from the theft of IP/trade secrets.[1]

86%

of manufacturers extensively use cloud storage and solutions to conduct business with 3rd-party contract manufacturers and suppliers.[2]

48%

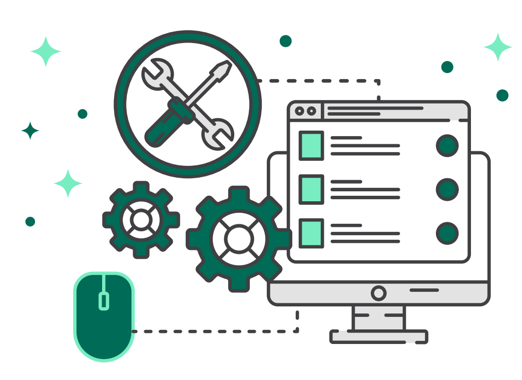
of manufacturers have been subject to a cyberattack and half have suered either nancial loss or disruption to business as a result.[3]

21%

of sensitive les in the manufacturing industry are publicly exposed.[4]

53%

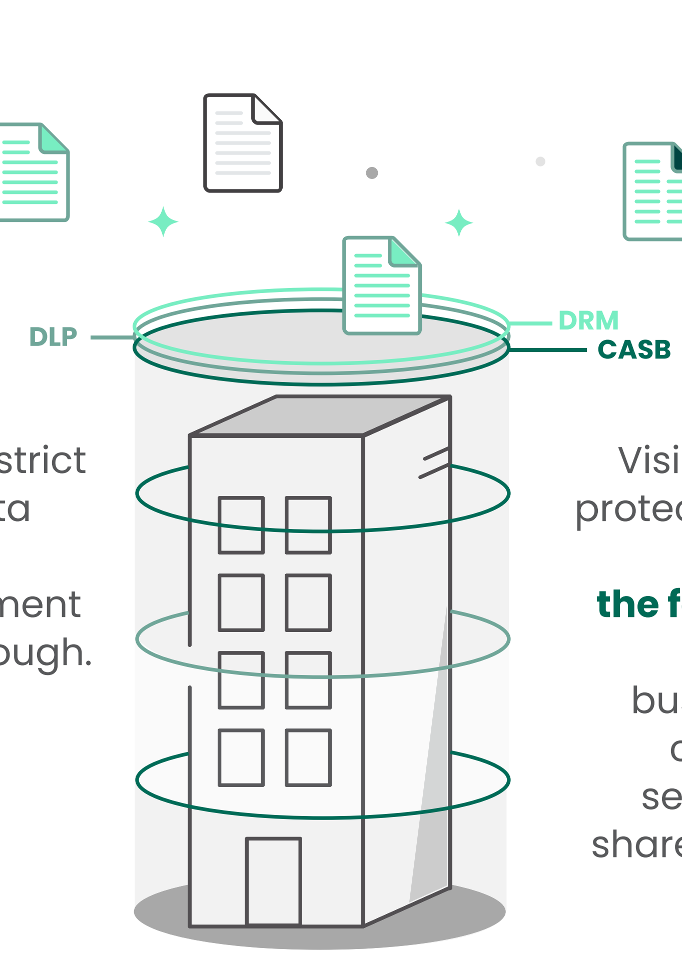
of manufacturers admit their operational technology is vulnerable to cyberattacks.[5]



87

the number of conrmed sensitive data disclosures in the manufacturing industry in 2019.[6]

Why Traditional Data Protection Solutions Fall Short



Having "fences" that restrict the flow of sensitive data and solutions that are cumbersome to implement and maintain is not enough.

Visibility, control, and protection also need to extend **"beyond the fence"** to account for the myriad business-driven use cases that require sensitive data to be shared, both internally and externally.

What Makes Vera Different

Complete data protection that extends beyond the perimeter of your rm and the time of initial sharing/ distribution.

Ease of use that includes the option of viewing and editing via a Vera HTML wrapper, or inline for native applications with the Vera client.

Comprehensive coverage with no limitations on devices, le types, data stores, collaboration tools, or applications.

SECURE — Apply AES 256-bit encryption and granular access policies that travel with your data files regardless of how and where they're shared.

TRACK

AUDIT — Understand exactly who is accessing sensitive data inside and outside of your organization, to maintain visibility/control and thereby minimize the potential for leaks of pre-release content and other IP.

REVOKE — Withdraw access to sensitive files any time after they've been shared, regardless of where and with whom the files now reside.

Ready To Bullet Proof Your Data Security? Contact Vera Today!

LEARN MORE

REQUEST DEMO

emails@fortra.com

Sources:

[1] Annual Intellectual Property Report to Congress, IPEC, 2020.
[2] 2020 Manufacturing and Distribution Report, Sikich, 2020.
[3] Cyber Security and Manufacturing A Brieng for Manufacturers, MakeUK, 2019.
[4] 2019 Data Risk Report, Varonis, 2019.
[5] Threat Detection and Response in Manufacturing, TrapX Security, 2020.
[6] 2020 Data Breach Investigations Report, Verizon, 2020.

 (fta-vr-in-1222-r1-79d)