

# A New Approach to Data Security for Manufacturing Companies

A visual guide to the challenges and solution requirements for securely 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



**Operational IP**

- Manufacturing Specifications
- Proprietary Process Documents
- Production Reports/Plans



**Finance**

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



**Legal**

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



**Sales & Marketing**

- Internal Strategy Documents
- Pricing Data/Models
- Private Customer Data



**Human Resources**

- Confidential 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 company 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.<sup>1</sup>



of manufacturers extensively use cloud storage and solutions to conduct business with 3rd-party contract manufacturers and suppliers.<sup>2</sup>



of manufacturers have been subject to a cyberattack and half have suffered either financial loss or disruption to business as a result.<sup>3</sup>



of sensitive files in the manufacturing industry are publicly exposed.<sup>4</sup>

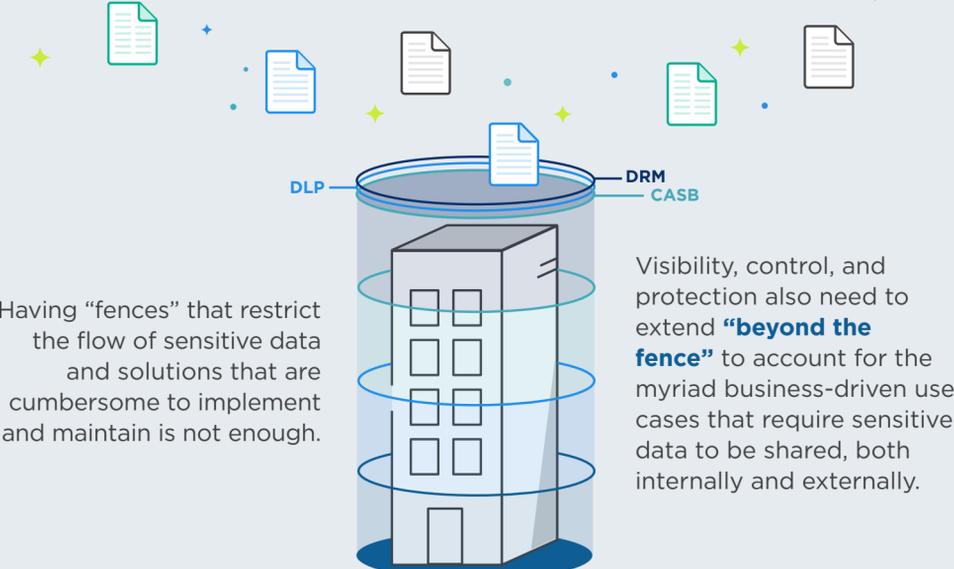


of manufacturers admit their operational technology is vulnerable to cyberattacks.<sup>5</sup>

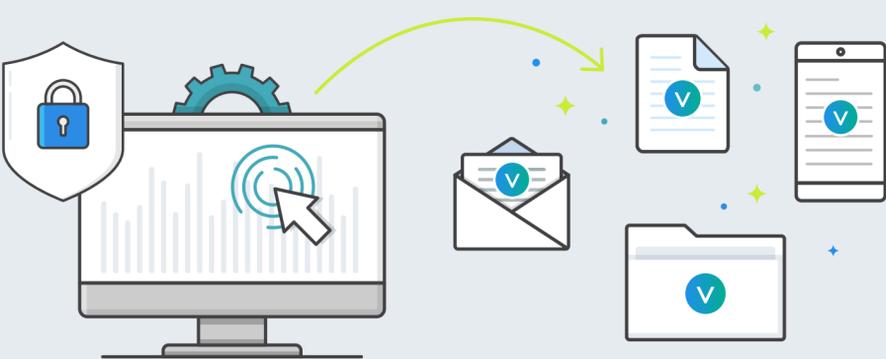


**87** the number of confirmed sensitive data disclosures in the manufacturing industry in 2019.<sup>6</sup>

## WHY TRADITIONAL DATA PROTECTION SOLUTIONS FALL SHORT



## WHAT MAKES VERA DIFFERENT



**Complete data protection** that extends beyond the perimeter of your firm 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, file 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

Understand exactly who is accessing sensitive data inside and outside of your organization, to maintain visibility/control and achieve compliance with applicable regulations and standards (such as ISO/IEC 27001 and the NIST Cybersecurity Framework).

### AUDIT

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

### 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](#)

Call Us: 844-GET-VERA

**Sources:**  
<sup>1</sup> Annual Intellectual Property Report to Congress, IPEC, 2020.  
<sup>2</sup> 2020 Manufacturing and Distribution Report, Sitch, 2020.  
<sup>3</sup> Cyber Security and Manufacturing A Briefing for Manufacturers, MakeUK, 2019.  
<sup>4</sup> 2019 Data Risk Report, Varonis, 2019.  
<sup>5</sup> Threat Detection and Response in Manufacturing, TrapX Security, 2020.  
<sup>6</sup> 2020 Data Breach Investigations Report, Verizon, 2020.