BLUE PRINT TO DATA-CENTRIC SECURITY

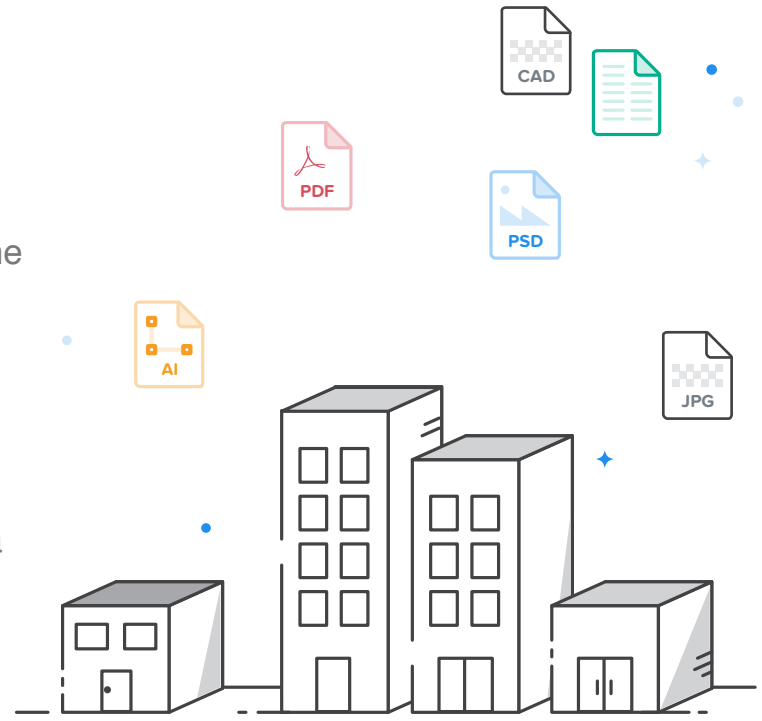
A MANUFACTURER'S GUIDE TO PROTECTING TRADE SECRETS

LIKE IT OR NOT, YOUR INTELLECTUAL PROPERTY IS LEAKING

Once upon a time, it was difficult to remove sensitive information from the enterprise. The mainframe environment consisted of a single access point, one network, and a locked down ecosystem with a few logins. Keeping data secure and preventing unwanted viewers wasn't all that difficult.

Today, the rate at which your employees are sharing confidential data outpaces your team's ability to patch the perimeter, block or quarantine information, and stop confidential data from leaving your control.

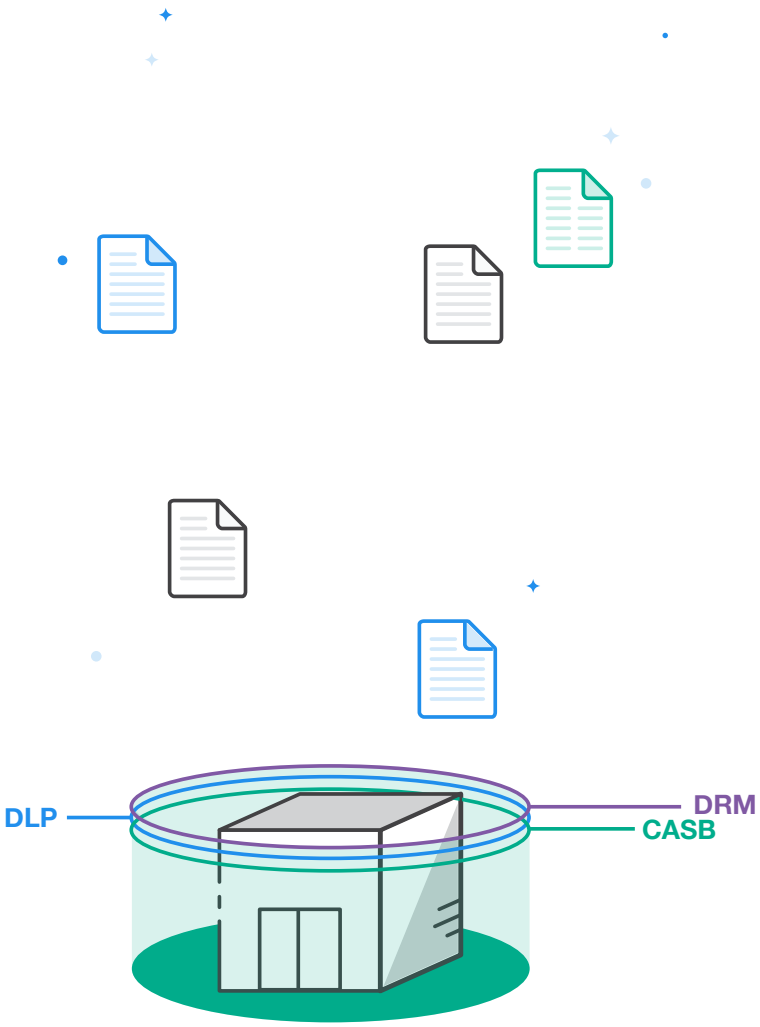
With thousands of vectors for your trade secrets, intellectual property and proprietary manufacturing processes to leave your business—email, Dropbox/Box shared links, managed and unmanaged mobile devices, Slack, or even a good ole' fashioned USB drive—you need a different security strategy to operate in an ever-porous enterprise.



We'll cut to the chase.

Data is the vital stuff of business, but to protect our crown jewels, we have to shift our security strategy to protect what really matters: the data itself.

DLP, CASB, DRM AND CLASSIFICATION TOOLS AREN'T ENOUGH



"DON'T I ALREADY HAVE A DATA-CENTRIC STRATEGY?"

Yes, and no. Data Loss Prevention, Cloud Access Security Brokers, Digital Rights Management and Classification tools offer their own valuable benefits, but they all share the same limitation: **They're all about locking data down.**

A recent Gartner study, *Predictions 2017 Application and Data Security*, found that by 2018, 75% of organizations implementing data classification policies will report limited deployments and see no tangible benefits, and by 2018, 1 in every 10 businesses with integrated DLP will have a well-defined data security governance program in place.

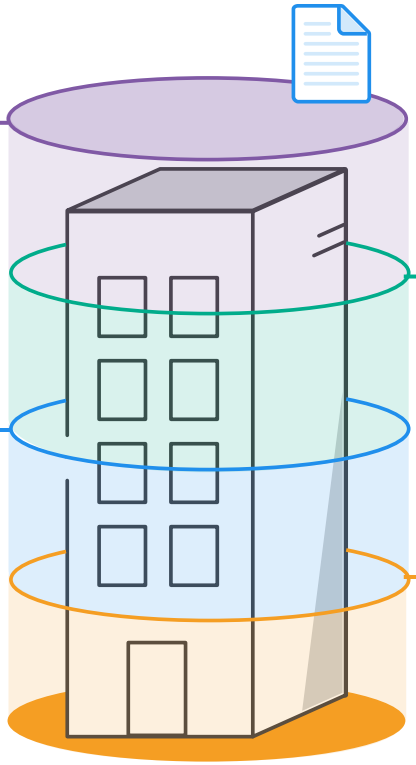
In a nutshell, having only these tools in place isn't enough.

Once confidential R&D leaves your network and is downloaded by an employee or a third-party contractor, your security strategy comes to an end. As your IP travels to unknown endpoints, unknown suppliers, and unknown domains, all bets are off. You can't see it. You can't control it.

These tools rarely work at the most critical moment—when people are working with the information.They can't prevent an external supplier in Europe from saving a copy of your proprietary designs and forwarding to a competitor. They can't secure information "in use." **And once your data moves past the DLP fence and CASB proxy, it's in the wild and unprotected.**

DIGITAL RIGHTS MANAGEMENT (DRM):
An attempt at data-centric security but a cumbersome user experience prevents enterprise-wide adoption and scalability.

DATA LOSS PREVENTION (DLP)
Scans and quarantines confidential information traversing the network but once it leaves, security teams can't see, audit or control what others are doing with mission-critical data.



CLOUD ACCESS SECURITY BROKER (CASB)
Enforce security policies and block information leaving cloud applications (e.g., Box, Salesforce) but once data is downloaded or moved offline, security teams lose all control of what happens next.

CLASSIFICATION:
Tags and classifies sensitive information shared from your business but a classifier won't be able to prevent an internal employee from downloading trade secrets and taking them to his/her next job.

YOU NEED A NEW STRATEGY, A DATA-CENTRIC APPROACH, TO EFFECTIVELY SECURE YOUR INTELLECTUAL PROPERTY, EVERYWHERE IT GOES.

DATA-CENTRIC SECURITY: SECURITY FOR THE POROUS ENTERPRISE

Data-centric security is the ability to secure data through its entire life cycle, everywhere it travels, no matter who has it or where it's stored. The goal is to protect confidential data at the point of its greatest vulnerability—when it's being used in others' hands, and as it travels outside our perimeters into unmanaged domains, devices and applications.

The ideal data-centric security solution is characterized by five capabilities with five key benefits:

SECURES ALL FORMS OF DATA

360-DEGREE VISIBILITY

DYNAMIC DATA PROTECTION

INTEGRATES WITH YOUR ECOSYSTEM

INVISIBLE USER EXPERIENCE

THE MANUFACTURING BLUEPRINT ON DATA-CENTRIC SECURITY PROTECTING YOUR COMPETITIVE ADVANTAGE AND IP

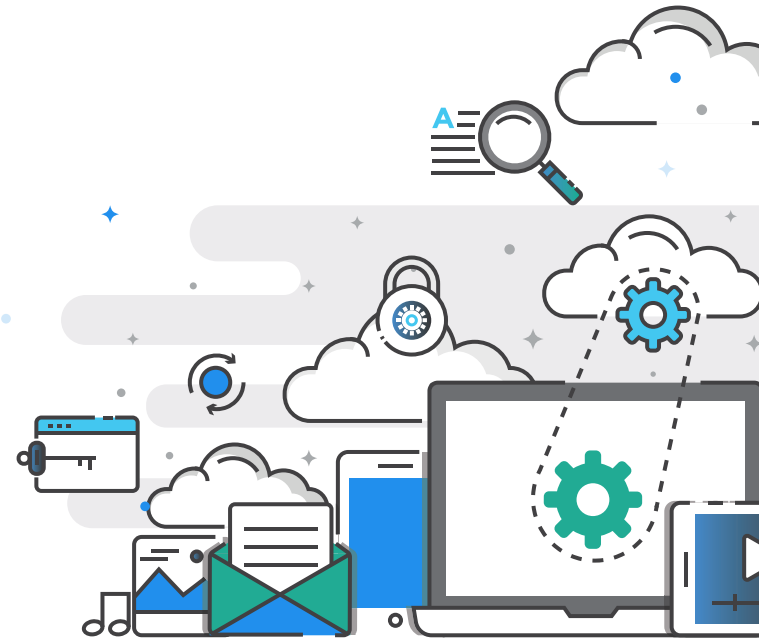
HOW DOES THIS WORK IN THE MANUFACTURING SECTOR?

Security teams in the manufacturing sector are often balancing between two competing demands: securing intellectual property and enabling high-speed production efficiency.

Your team is laser focused on protecting your business' competitive edge and R&D—your product designs, manufacturing specifications and supplier contracts—but to ship successful products, the business must share highly confidential information throughout the supply chain and to employees who may not necessarily be with your company forever.

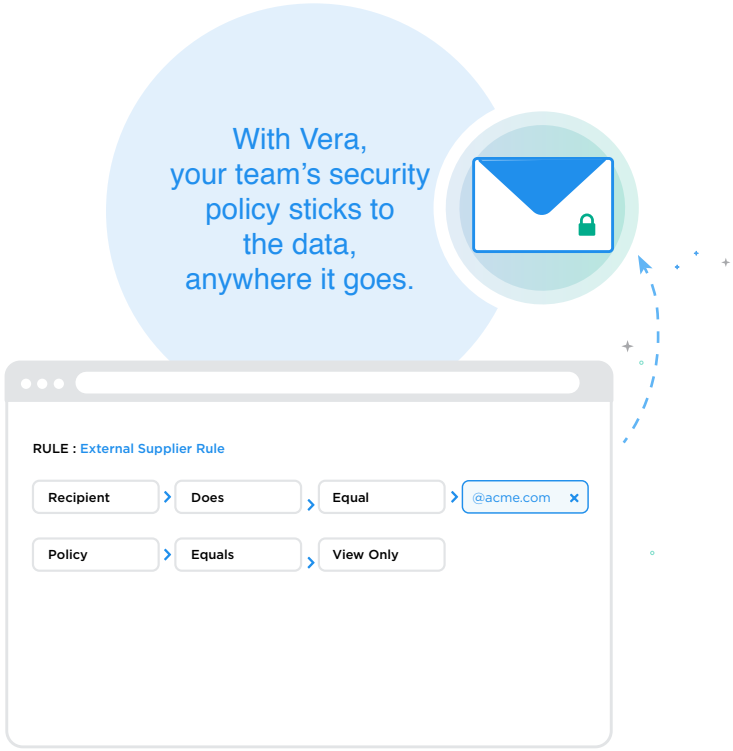
Data-centric security solves that balancing act. Even more, it provides the solution to the questions keeping your team up at night:

- How do I control how suppliers consume our sensitive designs?
- How do I prevent leaks to unauthorized partners or competitors once an employee or third-party supplier has access to our R&D?
- How do I audit our data throughout the supply chain?
- How do I revoke access to proprietary information once an employee leaves the company?



THE MANUFACTURING BLUEPRINT

At Vera, we've helped leading manufacturers solve these same challenges. We've also seen a blueprint emerge on how manufacturing security teams are leveraging data-centric security to automate their job and become a value-driven enabler to the core business.



1 AUTOMATICALLY SECURE TRADE SECRETS EMAILED TO THIRD-PARTY SUPPLIERS

One of the most common workflows our manufacturers leverage is automatically securing all trade secrets sent to third-party suppliers over email (e.g., Microsoft Outlook, Apple Mail, etc.).

Leveraging Vera's smart rules engine, all attachments sent to a supplier (example: @acme.com) are automatically secured without requiring your employees to take any manual steps to secure data.

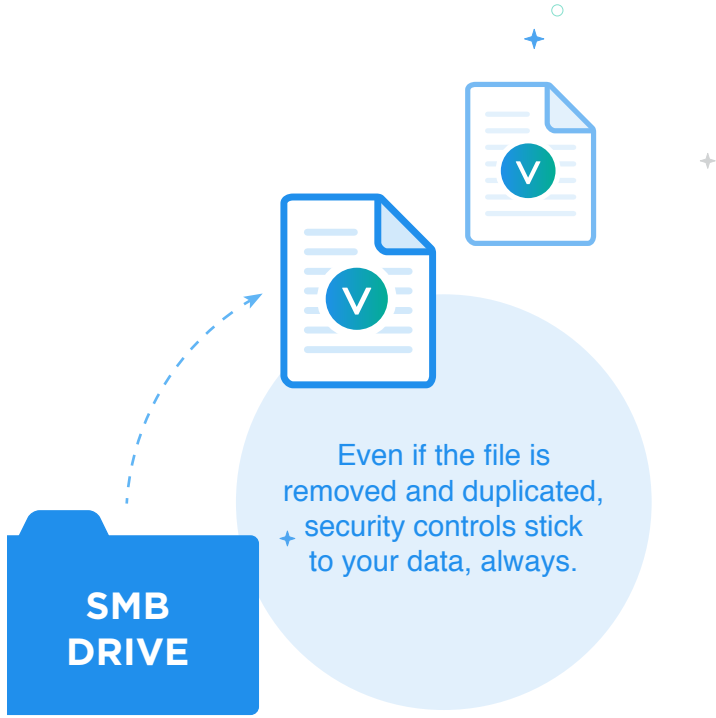
If data is ever forwarded to a party that doesn't belong to the Acme domain, that third party will never be able to access your company's crown jewels.

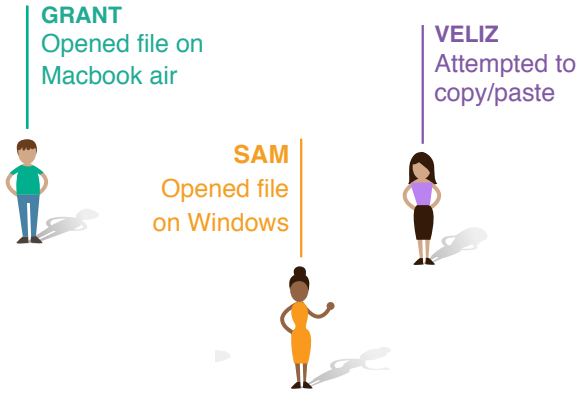
2 PREVENT LEAKS, EVEN AFTER INTELLECTUAL PROPERTY IS DOWNLOADED FROM YOUR SYSTEMS

Manufacturers store sensitive patents, trademarks, customer information and processes across multiple storage platforms: local file shares, Box, Dropbox, SharePoint, OneDrive, and more.

Vera has built out-of-the-box integrations to all of these storage systems to automatically secure any file uploaded or downloaded from those platforms. That way, your employees work exactly the way they normally would, and Vera works seamlessly behind the scenes to protect your IP—everywhere it moves.

If data ever leaks or is downloaded from your storage solution, Vera's security sticks to the file anywhere it goes, making sure only authorized parties are working with your information.





3 TRACK PROPRIETARY R&D THROUGHOUT THE SUPPLY CHAIN

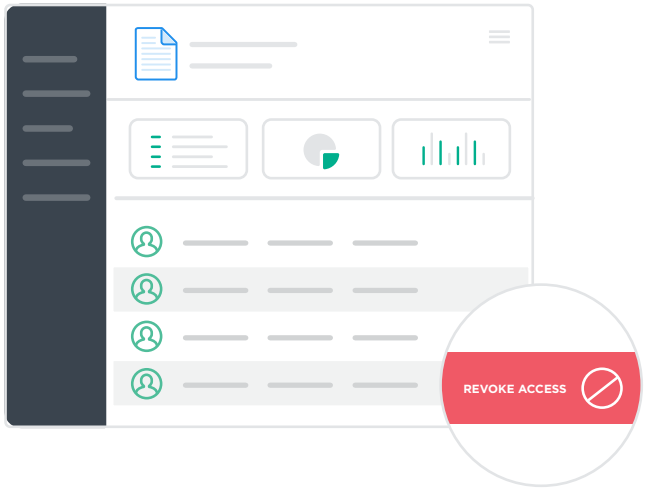
Manufacturers leverage Vera's audit capabilities to understand exactly who is accessing R&D throughout the supply chain, track all access attempts (authorized or not), and get granular metrics on usage and adoption.

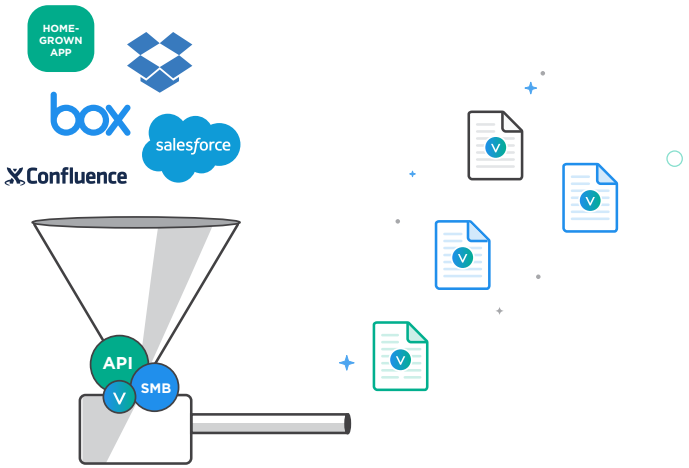
4 REVOKE ACCESS TO DATA KEPT BY DEPARTING EMPLOYEES

Employees come and go in any manufacturing company—and sometimes they're tempted to take proprietary designs to their next venture.

Manufacturers leverage Vera's Dynamic Data Protection to revoke access to data a departing employee has appropriated throughout the course of his/her employment—even if it's been moved to a personal account.

In one click, all copies of secured designs are shut off, and manufacturers retain complete control over their critical IP.





5 SECURE DESIGNS AND SPECS GENERATED FROM HOME-GROWN APPS

Our most sophisticated manufacturing teams leverage the Vera SDK/API to weave and build data security into their home grown and custom apps.

With the Vera SDK, machine-generated files and custom designs uploaded and shared from home-grown systems or third-party apps are automatically secured—giving you a powerful data security fabric for your entire ecosystem and extended enterprise.

READY TO GET STARTED?

We’re ready to help.
visit us at www.vera.com/industries/manufacturing to learn more.