

FORTRAΔ

Definitive Guide to Bullet Proofing Data Security for Technology Companies





Your Data is Leaking and It's at Risk

We live in an increasingly digitally collaborative world, a trend which has been accelerated in no small part by the COVID-19 pandemic. While all of this collaboration—both internally among employees and externally with partners, suppliers, customers—has enabled businesses to maintain higher levels of productivity, it has also increased the risk of sensitive data exposure and loss.

Removing sensitive information from an enterprise used to be difficult. 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 hard. In today's environment, however, 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 intellectual property, product strategies, and financial reports to leave your business—email, Dropbox/Box shared links, managed and unmanaged mobile devices, Slack, or even the traditional USB drive—you need a different security strategy to operate in an ever-porous enterprise environment.






We'll Cut to the Chase.

Data is the lifeblood of any technology company, but to safeguard the crown jewels, there needs to be a shift in the data security strategy to protect what really matters: the data itself.





Your Sensitive Data is at Risk Across the Enterprise

Finance	Sales	Marketing
 <ul style="list-style-type: none">• Corporate Earnings Reports• Financial Projections• Budget & Asset Allocations	 <ul style="list-style-type: none">• SOC2 Reports• Product Pricing• Pipeline Reports	 <ul style="list-style-type: none">• Go-to-market Launch Plans• Internal Strategy Documents• Private Customer Data
Legal	R&D	Human Resources
 <ul style="list-style-type: none">• Customer & Vendor Contracts• Investor Agreements• User/Customer PII	 <ul style="list-style-type: none">• Code• ASIC Designs• Product Functional Specs	 <ul style="list-style-type: none">• Stock Grants• Confidential Employee Data• Health Insurance Information



Standard Tools Can't Be Your Only Line Of Defense Anymore

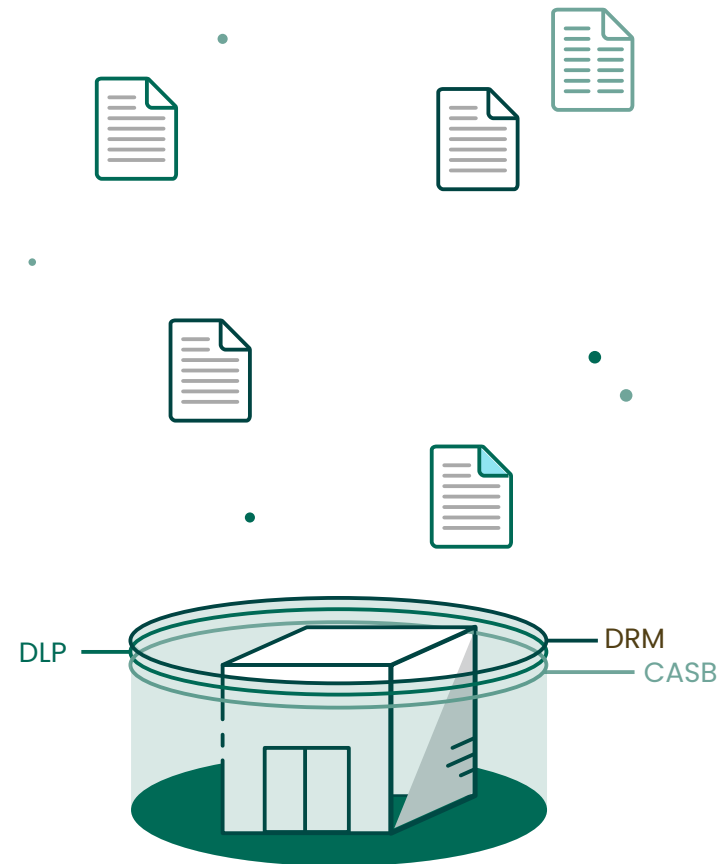
The most common question we hear is:

“Don't I Already Have A Data Security 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 instead of protecting it when it's on the move.

Verizon's 2020 Data Breach Investigations Report found that human error accounts for **22% of breaches in the technology industry**. Human error is defined as misdelivery, misconfiguration, mismanagement of file access, and a lack of encryption when distributing the company's most valuable data assets. And those errors can be costly! According to IBM's 2020 Cost of a Data Breach Report, the average total cost of a data breach was \$3.86 million in 2019. Security experts maintain that a majority of these cybersecurity breaches can be avoided and millions of dollars saved if enterprises simply focus more on controlling the flow and access of sensitive internal data assets.

In a nutshell, having only these tools in place will no longer suffice as a defensive security approach. Once confidential product plans or financial reports are downloaded by an employee, a third-party individual, or otherwise leave your network, your security strategy comes to an end. As your sensitive data travels to unknown endpoints, unknown companies, and unknown domains, all bets are off. You can't see it. You can't control it.





An Increased Focus On Data Security Is Now A Necessity

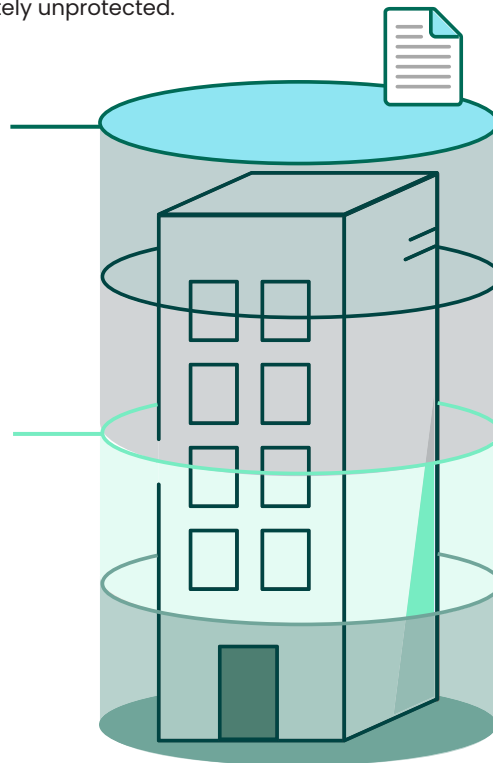
Data Loss Prevention, Cloud Access Security Brokers, Digital Rights Management, and Classification rarely work at the most critical moment—when people are working with the information. Unfortunately, these tools can't prevent a vendor or partner you're working with from saving a copy of your proprietary product and service information and forwarding it to a competitor to gain favor. They are unable to secure information "in use" and track who it's going to. And once your sensitive data moves past the DLP fence and CASB proxy, it's in the wild and completely 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)

Enforces security policies and blocks information leaving cloud applications (e.g., Box, Salesforce) but once data is downloaded or moved offline, security teams lose all control of what happens.

Classification:

Tags and classifies sensitive information shared from your business but 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 SENSITIVE DATA, EVERYWHERE IT GOES.



Data-Centric Security: Securing Data Through It's Entire-Lifecycle

A truly effective data-centric security approach is one that can secure data through its **entire lifecycle**, 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 other persons hands, and as it travels outside your perimeters into unmanaged domains, devices, and applications.

Key Capabilities of a Data-centric Security Solution



Secures All Forms
of Data



360-Degree
Visibility



Dynamic Data
Protection



Integrates with
Your Ecosystem



Invisible User
Experience



Technology Companies Need a Winning Game Plan for Data-Centric Security Success

How Does This Work In The Technology Sector?

Security teams at high-tech companies struggle to balance between two competing demands: securing sensitive product and business information while still being able to use it to accelerate the delivery of innovative products and services. Without the right tools and strategy in place to help your IT staff overcome this obstacle, how can you ensure that your sensitive data is safe?

Another significant area of concern for high-tech companies is the deployment of so many new systems heavily based in the cloud. While the cloud enables many attractive options for using, sharing, and storing one's data, it also exposes new security vulnerabilities and avenues of attack. Not only are these attack surfaces emerging at a record pace, the amount of data in motion is exploding. As a result, companies now need to protect much more company data and customer information, often dispersed far beyond enterprise walls and accessible via an ever-widening array of end points. But how?

Deploying a data-centric security approach solves the balancing act: providing robust protection for sensitive data while still enabling it to be used wherever and however it's needed to drive the business forward. Such an approach provides answers to the toughest questions keeping your team up at night.

How do I control how suppliers, distributors, and other partners consume or share our sensitive data?

How do I prevent leaks to unauthorized partners or competitors once an employee or third-party users have access to our sensitive files?

How do I track the flow of our sensitive documents throughout their lifecycle?

How do I confidently revoke access to proprietary information after employment or a partnership has ended?



SECURE Sensitive Data You Need to Distribute

Securing your data is the first step in the **STAR** approach, providing the confidentiality, control, and oversight you didn't have previously. With a single mouse click, you can protect documents, presentations, videos or images with AES 256-bit encryption and granular access policies that travel with the associated files regardless of the methods by which they are shared.

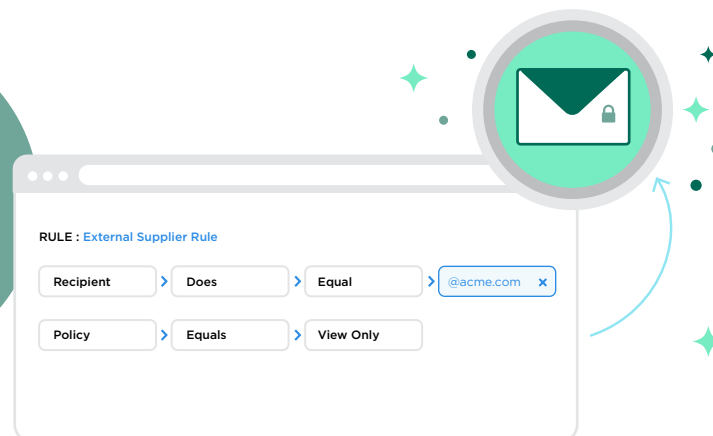
Automatically Secure Sensitive Data Emailed Outside Your Organization

One of the most common workflows our technology companies leverage is automatically securing all sensitive files sent over email, for example, to their investors or manufacturing partners. Leveraging Vera's smart rules engine, all attachments sent to a specific company (example: @Acme.com) are automatically secured without requiring your employees to take any manual steps. If the data is ever forwarded to a party that doesn't belong to the @Acme.com domain, that third party won't be able to access that file until they're specifically provided with the access.

Prevent Leaks, Even After Sensitive Data is Downloaded From File Sharing Systems

High-tech companies store test results, confidential reports, competitive go-to market strategies,

With VERA,
your team's
security policy
sticks to the data,
anywhere it goes.



Vera's Solution To Helping You Implement Data-Centric Security

At Vera, we've helped many technology companies bullet proof their data security by implementing the STAR solution as in below:

SECURE
TRACK
AUDIT
REVOKE



Prevent Leaks, Even After Sensitive Data is Downloaded From File Sharing Systems

High-tech companies store test results, confidential reports, competitive go-to market strategies, customer information, and process documents 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 sensitive data—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. Vera is the best type of companion — one that keeps data safe wherever it goes.



Secure Designs and Specs Generated From Home-Grown Apps

Many of the most sophisticated IT teams in the technology sector leverage the Vera SDK/API to weave and build data security into their homegrown and custom apps. With the Vera SDK, machine-generated files and custom designs uploaded and shared from homegrown systems or third-party apps are automatically secured—giving you a powerful data security fabric for your entire ecosystem and extended enterprise.





TRACK and AUDIT Sensitive Data You Have Distributed

Tracking and auditing your sensitive data to understand who's accessing it are the next step in the STAR approach. Knowing whose hands are on your sensitive data is always a luxury companies wish they had after the fact, but with Vera you can track the complete lifecycle of any file that's no longer inside your own company walls.

Follow the Path of All Your Sensitive Data

High-tech companies leverage Vera's tracking and auditing capabilities to understand exactly who is accessing sensitive company files inside and outside of the organization, track all access attempts (authorized or not), and receive granular metrics on usage and adoption, as well as to create required audit and compliance reports. Vera's easy-to-use web-based portal allows you to easily track and audit file access, duration, location, actions taken, device type used, export types and counts, and general system events (both admin and connector activities).

REVOKE Access to Sensitive Data You Have Distributed

Revoking access to sensitive files you've shared is the last step in the STAR approach. This level of control comes in handy for a variety of reasons, such as after a disgruntled employee leaves the company, the severing of partner or supplier relationship, losing an employee to a competitor, or simply because you want to restrict file access after a certain amount of time.

Remove Access to Files to Maintain Your Data Security Integrity

Relationships come and go in any high-tech company and sometimes people are tempted to take sensitive files and proprietary information to give them a leg up. That's not an option with Vera integrated within your enterprise. Technology companies leverage Vera's dynamic data protection to revoke access to data a user has appropriated throughout the course of their time engaging with your company—even if it's been moved to a personal account. In one click, all copies of product plans and important financial reports are shut off, providing your company with complete control over the data that matters most to it.

Vera data-centric Security Solution

FINANCE

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

SALES

- ✓ SOC2 Reports
- ✓ Product Pricing
- ✓ Pipeline Reports

MARKETING

- ✓ Go-to-market Launch Plans
- ✓ Internal Strategy Documents
- ✓ Private Customer Data

LEGAL

- ✓ Customer & Vendor Contracts
- ✓ Investor Agreements
- ✓ User/Customer PII

R&D

- ✓ Code
- ✓ ASIC Designs
- ✓ Product Functional Specs

HUMAN RESOURCES

- ✓ Stock Grants
- ✓ Confidential Employee Data
- ✓ Health Insurance Information

... and many more!



Secure, track, audit, and revoke any file, on any device. With Vera, a single click, protects documents, presentations, videos or images with AES 256-bit encryption and granular access policies that travel with the file. And a simple, consistent interface on every platform promotes secure behavior and dissuades your employees, vendors, and customers from choosing risky, insecure workarounds when handling your data

Ready to Bulletproof Your Data Security?

We'd love to help. Visit us at vera.com/data-security-technology

Learn More

FORTRA

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.