

FORTRA

The Definitive Guide to Data Security

Taller walls aren't the answer.





Table of Contents

Introduction	1		
Part I	4	Part III	
The Walls Are Crumbling		The Best Defense: Data Security	22
Our Path to the Present	5	Data-Centric Security for a Borderless World	23
The Old Ways Can't Serve Our New World	7	Security for Data Anywhere and	24
Part II		Everywhere	27
Finding the Four Key Gaps	10	Closing the Security Gaps	
The Behavior Gap	11	Contact Information	28
The Visibility Gap	14		
The Control Gap	16		
The Response Time Gap	18		



Introduction

You don't know what you don't know.

Your data security policies and processes have gaps—places where sensitive information can go astray and end up in the wrong hands.

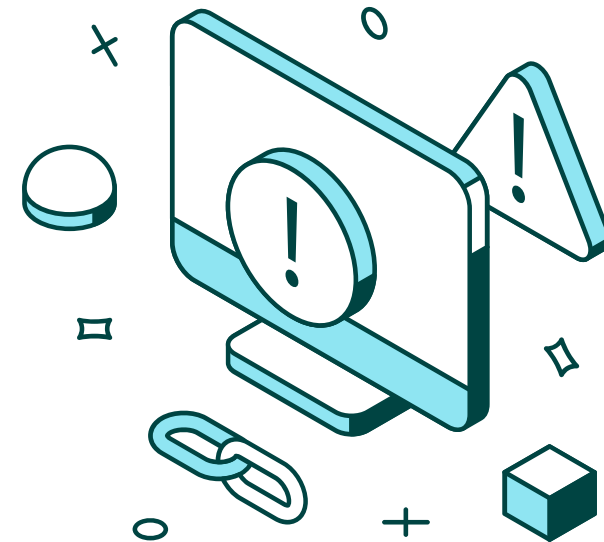
For most businesses, today's information security is built as a series of metaphorical walls—protections and defenses erected around applications, devices, networks, and online identities. Beyond those walls, we rely on each individual employee following policies as a virtual extension of these fortifications.

The good news: we have become expert at building defenses around applications and networks, including perimeter-based security, strong authentication, encryption, mobile device management, and secure containers. All of these solutions offer vital protections.

But when they fail—when there's a breach in our defenses—we try to strengthen the barriers we already have. We don't adapt. And that doesn't work.

Each time you read about another data breach in the paper, some little voice whispers in your brain, *"That can't happen to us, right?"*

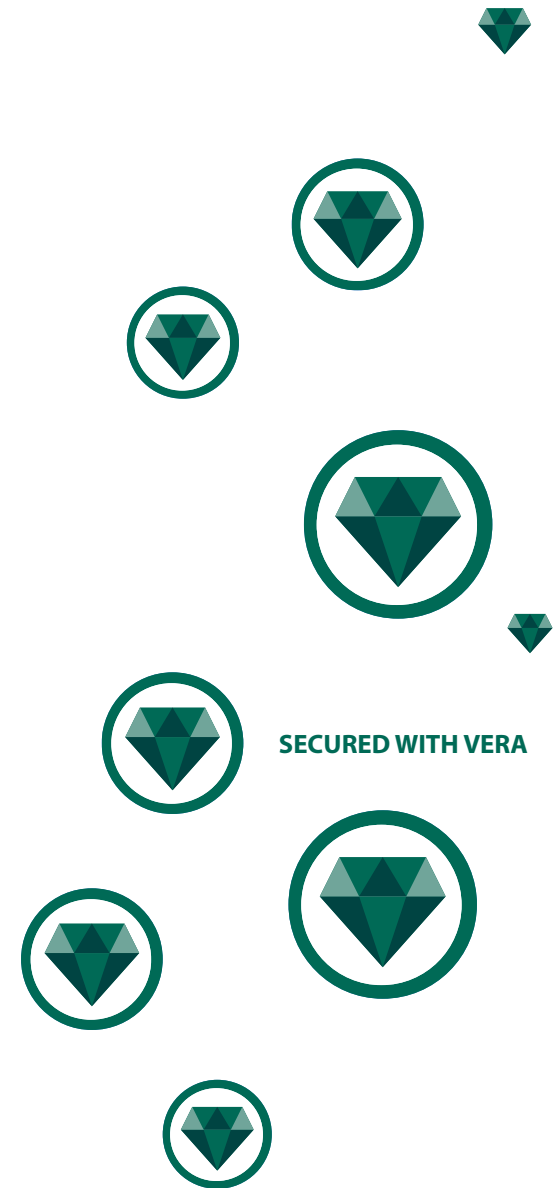
But, deep in your gut, you know sensitive business data may be at risk somewhere out of sight, beyond your reach.





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

NOT PROTECTED



SECURED WITH VERA



If you lock everything down, business will grind to a halt.

Building higher walls and stronger perimeter defenses may make you feel safer for a while. But this strategy can't deliver lasting protection, for two reasons:

Walls are crumbling. Physical boundaries and network perimeters are dissolving. The more complex the IT environment becomes, the more difficult it is to protect the systems, devices, people, and networks handling corporate data. Sensitive data escapes through the gaps in the defenses.

Business is storming the walls, from the inside out. Data delivers value when it's being used by employees as well as people outside of your organization, with devices and applications that you cannot control.

Data is the vital stuff of business, but to protect and control our crown jewels (our intellectual property or regulated information) when they're in use by partner or collaborator hands, we can't rely on walls. We have to shift from infrastructure-centric security measures to data-centric approaches to protect what really matters: the data itself.

If your team is struggling to secure sensitive data in a world without well-defined borders, you need to change your approach and understand:

- Why building bigger walls around data, devices, networks, and applications doesn't work anymore
- How to find and detect the four key gaps in your information security architecture
- How to bridge those gaps by protecting data in use

To get out from behind our walls, we first have to understand how we got into our current situation.



PART I

The Walls are Crumbling



Our Path to the Present

Taller, higher, stronger walls

Great minds and innovative companies have spent decades addressing the challenges of information security. As technologies change and expose vulnerabilities, new solutions rush in to fill the vacuum, adding layers to secure the people, places, and things handling business data.

Back in the day, the mainframe environment consisted of a single access point, one network, and only a few privileged accounts to protect. Admins controlled logins to the mainframe and locked down the computer in a secure, temperature-controlled citadel. The mainframe itself took care of the rest.

Then the computing perimeter started expanding, and defenses became more complex.

Distributed client/server computing multiplied the systems and networks needing protection. Computers multiplied. Client devices multiplied. But, most employees still operated within corporate networks.

As information systems expanded to the cloud, logins multiplied. Mobile devices mushroomed at an unprecedented rate.

This expanding technological footprint is reflected in business structures. With constant connectivity and mobility, people around the globe can collaborate with each other. Virtual teams and organizations assemble and disperse for specific projects.

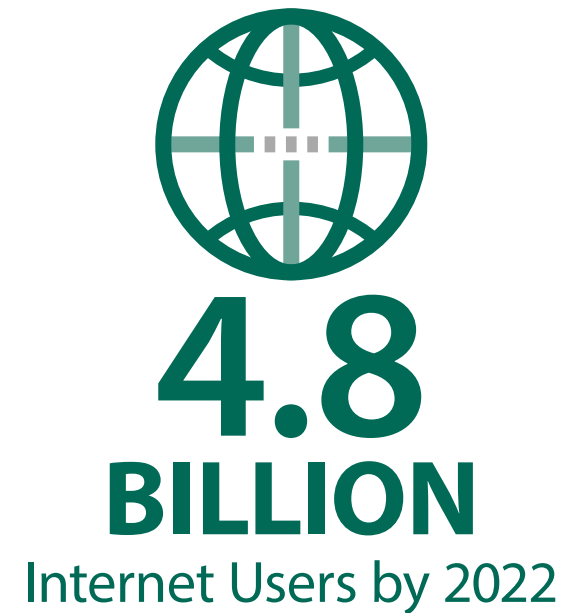




The result? More apps, more data, more networks, and more logins. The numbers continue to grow.

A decade ago, IT could track the networks, connections, and perimeters related to sensitive data. Today, everything connects to everything else, borders have disappeared, and the complexity of the underlying environment continues to increase by orders of magnitude.

In their Virtual Networking Index (VNI), Cisco predicted that there will be 4.8 billion internet users by 2022, up from 3.4 billion in 2017. And IP traffic will continue to skyrocket. They predict that by 2022, more IP traffic will cross global networks than in the first 32 years after the internet was created.



Cisco Virtual Networking Index (VNI)



The Old Ways Can't Serve Our New World.

With each new stage, the security industry has developed new solutions and taller walls to fortify systems, secure online identities, defend networks, and protect data.

- 1** Network security measures like firewalls, sniffers, vulnerability scanning, and intrusion detection protect the perimeter.
- 2** Identity and Access Management (IAM) solutions secure, centralize, and manage user authentication.
- 3** Data loss prevention (DLP) systems track sensitive data exiting or traversing corporate networks.
- 4** Digital Rights Management (DRM) restrict access to proprietary information.
- 5** Secure FTP solutions track and manage the transfer of files between networks and entities.
- 6** Secure document vaults protect content in heavily regulated industries like healthcare and financial services.
- 7** Mobile Device Management (MDM) solutions enforce policies for corporate smartphones and tablets.
- 8** Cloud Access Security Brokers (CASBs) manage security policies involved in accessing cloud-based resources.
- 9** Secure sync and share and enterprise collaboration solutions create safe environments for exchanging and sharing information.



In 2015, Gartner estimated that businesses spent \$75 billion on enterprise security. Fast-forward to today, as Gartner predicts 2021 spend in security and risk management will exceed \$150 billion.

And yet even with that investment, the number of data breaches is increasing.





How can we spend this much and still have so many problems?

We've neglected the data. We've been securing infrastructure: the applications, devices, networks, and identities—not sensitive data itself through its entire life cycle. We're building castles designed for a siege, not for trade and commerce. Ponemon research shows that although more than half of organizations send sensitive data in the cloud, only 37 percent have any consistent encryption strategy. This is the problem with building more walls—there are too many gaps for information to slide through.

Our walls expose four critical security gaps. Each security solution outlined above fills an important role, but as the environment continues to get more complex, sensitive data finds the gaps in each layer of defense.



MOST ORGANIZATIONS SHARE THESE FOUR CRITICAL GAPS:

- 1** The Behavior Gap: The difference between what people should do, and what they really do when confronted by a wall
- 2** The Visibility Gap: Where your sensitive data travels, and who accesses it once it's shared beyond your borders
- 3** The Control Gap: The inability to pull back access to lost files or leaked information
- 4** The Response Time Gap: Time lag between a new, risky behavior and your team's ability to correct it

Nearly every business has these gaps.
Take a look and see if they seem familiar.



PART II

Finding the Four Key Gaps



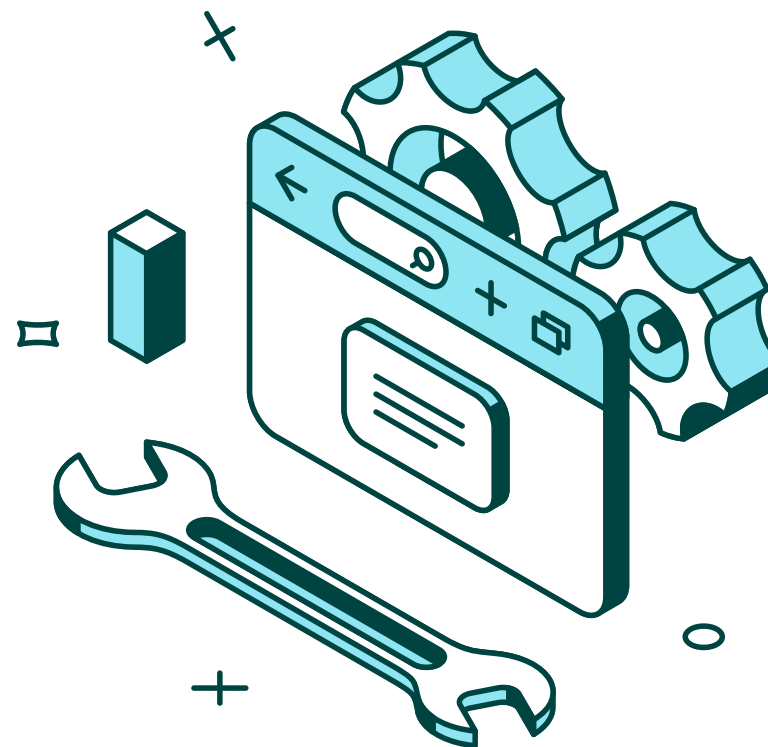
The Behavior Gap

“None of our employees use the security tools we’ve provided.”

To understand the Behavior Gap, let’s follow the story of a fictional media company, Pageantry Media.

In media and entertainment businesses, creative capital and assets drive revenue and growth. Pageantry Media carefully guards plots and scripts ahead of releases, so its competitors cannot see what’s coming up next. Hundreds of people work with the intellectual property: designers, artists, marketers doing focus groups and game developers. Everyone wants to use their own tools, and everyone operates on tight deadlines. Faced with pressure to get the job done, people find ways to work around security systems, and those precious story lines leak out into the world.

No matter what industry you’re in, this story probably sounds familiar. Sensitive data falls into the Behavior Gap.





Why Does the Behavior Gap Exist?

Businesses are made up of people. We're human, not programmable. And we want to find the fastest, most effective way to do our jobs.

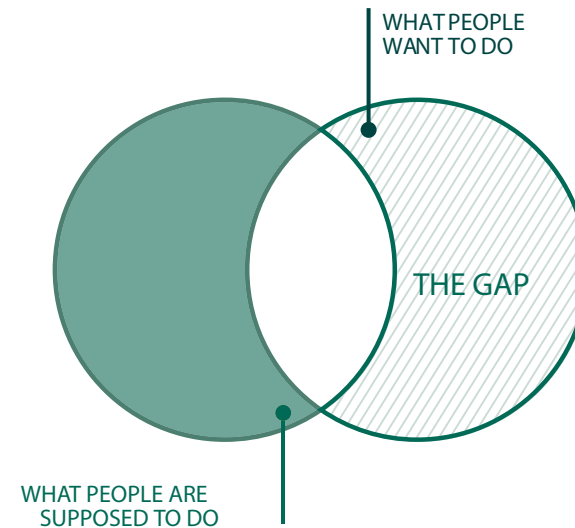
Most employees want to do the right thing with sensitive data. But more importantly, they need to get their work done. People are evaluated and paid based on goals accomplished. When security makes their jobs more difficult, it creates an inherent conflict. When people have to jump over too many hurdles, they're likely to look for another path.

Usability is the Achilles' heel of information security solutions.

When security tools are difficult to navigate, people will look for alternatives:

- Putting sensitive files on a USB stick so they can work on another device
- Bypassing the secure FTP server and mailing themselves files as attachments so they can work on personal devices
- Copying and pasting data from a secured file into an unsecured document "for convenience"

These actions put sensitive data at risk.





Why Does This Gap Exist?

People don't usually tell you about the ways they're misusing data, so you'll have to guess.

Here are a few signs that your Behavior Gap may be larger than you think:

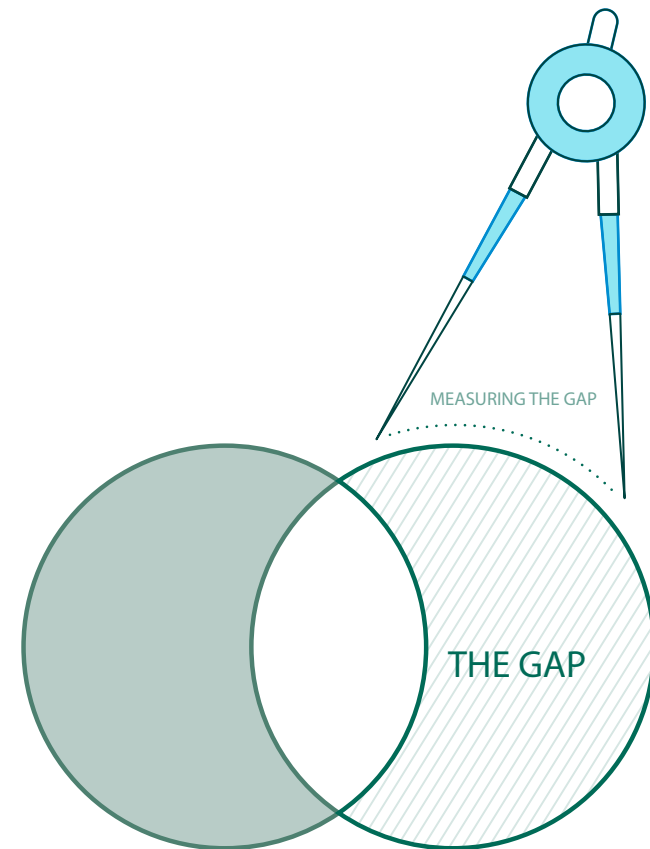
- Is your help desk swamped with calls with people trying to figure out how to get things done in your secure environment? The ones who don't get answers are probably finding a better way.
- Do people get more work done on the weekends, from home, than in the office using secure systems?
- Do people ever express frustration with the applications or processes?

If you answer yes to one of these questions, you may have a significant Behavior Gap.

20%

Compromised credentials were responsible for 20% of data breaches globally.

IBM Security's Cost of a Data Breach Report (2021)





The Visibility Gap

"I can't tell where, when, or how my data is being used."

Everyone at Turret Financial Services understands the importance of protecting financial and customer information to comply with the SEC, FDIC, SOX, and other regulations. But, Turret Financial must collaborate with external auditors, lawyers, customers, and investors. The IT team worries how their partners and investors will use the firm's sensitive data. Compliance officers lay awake at night worrying:

- Has material financial information been disclosed prematurely?
- Have investment strategies been forwarded to competitors?
- Who is accessing our customers' information?

Once files are shared beyond Turret systems and servers, they fall into the Visibility Gap.

The Visibility Gap is everything you cannot see. It's the unmanaged territory where data flows when it leaves the devices, networks, and applications that you directly control. Information crosses the Visibility Gap when your business collaborates with external partners or entities. Often, the real work gets done outside of your scope of vision.

Why does this gap exist?

Once you send a file as an email attachment outside of your managed domain, it disappears into the wild. The same thing happens when someone copies protected information into an Evernote file or saves a file on a personal USB. It disappears from your view.

This gap grows in proportion to the complexity of the information environment. You only see into some of the pieces of the puzzle, while employees can access an almost limitless number of devices and applications. What you don't know can hurt you. If data is regulated, you bear responsibility for it, even when you cannot see it.



The Visibility Gap



How big is your Visibility Gap?

By definition, the Visibility Gap is difficult to see. Information in the gap lies outside of your monitoring, auditing, and tracking technologies.

But you can detect its path, like the wake left by a large ship.

- Where does your data live?
- Is it secure?
- Who has access to it?
- How often are files and data sent outside your organization?
- How many third-party partners do you collaborate with?
- What kind of information do you send to consultants and third-party contractors?
- Can you track and audit who accesses the data, even when it's not within your servers or on your devices?

Fortra Cybersecurity Challenges in Financial Services - Market Survey Report



The Control Gap

"I can't proactively lock down access to lost files or leaked information. Once it's out, it's out."

Stronghold Health is a regional network of hospitals and clinics, with thousands of members and affiliated physicians and clinicians. Every physician and care provider is carefully trained on the importance of protecting Personal Health Information (PHI) to comply with the HIPAA Privacy Rule. But physicians routinely consult with others on problematic cases. A simple email malfunction like accidentally sending an email containing PHI to the wrong email address or hitting "reply all" by mistake can result in a potential violation. The hospital's compliance officer has no choice but to report a breach in these situations, because there's no way to shut down access to the PHI record once it has left the system.

The Control Gap

Stronghold Health suffers from the Control Gap—the lack of ability to limit or revoke access to information once it's outside of managed networks and systems. It leads to anxiety, uncertainty, compliance violations and breach notifications.

Do the symptoms sound familiar? Chances are that you've got a Control Gap, too.



Why does this gap exist?

You control most of the path:

- You can control access to enterprise logins with Identity and Access Management
- You can monitor and manage access to cloud-based file sharing applications with Cloud Access Security Brokers
- You can scan files that leave the organization with Data Loss Prevention (DLP) systems
- You can shut down an employee's corporate device with Mobile Device Management

But not the last mile—where data is in use. In the course of doing businesses, data leaves the systems and networks within your sphere of influence. Someone downloads the spreadsheet, or copies and pastes the description of your as-yet-unreleased product into a personal document.

The Control Gap is the natural extension of the Visibility Gap: once a file leaves the networks, devices, and applications that you manage, it's effectively out of your control

How big is your Control Gap?

- Have you ever accidentally sent a sensitive email to the wrong person?
- Have you ever suspended a relationship with a vendor or contractor, then worried about what they would do with the files they had?
- Has someone ever left your company on less-than-ideal terms?
- Do you work with any regulated data that has sensitive deadlines or timelines, or that should “self-destruct” once a specific time period is past?

Unless you live in a ideal world, you've got a Control Gap.

We've all done it

Made an **unintentional error** when **sharing data**

Sent information to the **wrong person**

Accidentally forwarded les to an **unauthorized recipient**





The Response Time Gap

"Our security team is always reacting."

Chivalric Consulting helps its clients leverage cutting edge technologies for competitive advantage. Chivalric's consultants are constantly chasing the next innovation and trying the newest technologies. The company's security team is always playing catch-up, formulating and spreading policies to protect confidential client information as its consultants continue evaluating and deploying new applications.

Like many businesses, Chivalric Consulting has a significant Response Time Gap. The Response Time Gap is caused by the delay between a new application or behavior that affects sensitive data and your ability to understand and respond to that behavior. It might be weeks or months, during which you don't know what's happening with sensitive information.



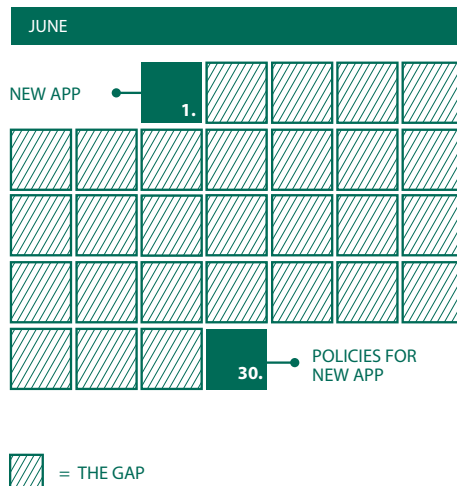


287days

It took organizations worldwide an average of 287 days to identify and contain a data breach.

Part 2

IBM Security's Cost of a Data Breach Report (2021)



Why does this gap exist?

Technology changes quickly. In many organizations, employees bring their own devices, applications, and expectations for how to work. Departments purchase applications and devices, which in turn generate more sensitive, proprietary information.

In the rush to get business done, security is often left to play catch-up. And security breaches may be the unintended consequences of this gap.

You could try locking down sensitive data, banning new applications, and standing your ground. But it's like standing in front of a moving freight train.

You might have time to see it coming, but eventually you won't be happy.

You need security that operates at the speed of business, with flexibility to adapt to the unknown.

How big is your Response Time gap?

Your Response Time Gap may be measured in days, weeks, months, or quarters. The longer it is, the greater the risk of people taking measures into their own hands, or sensitive data going untracked into new applications.

To detect the length of this gap, you'll need to understand:

- How many unanswered requests do you have to evaluate or support new applications?
- How long does it take, on average to fill those requests?
- How important is it for your employees to be current with the latest technologies?
- How long does it take to find out about new applications or devices that employees are already using?



The Limitations of Existing Defenses

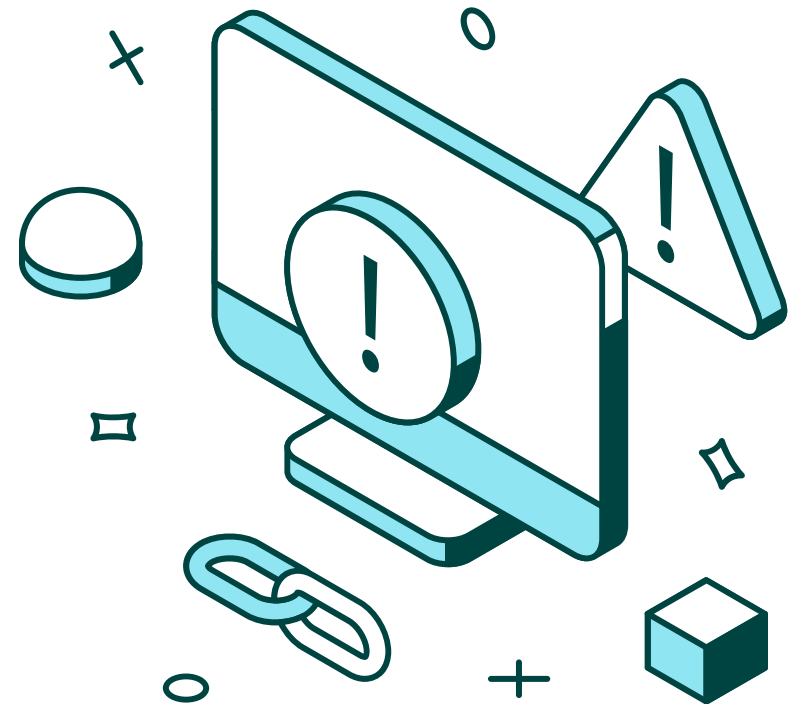
"We're going to need a bigger moat."

These four security gaps are products of applying current approaches to an increasingly complex information security environment.

You cannot fill pervasive security gaps by doing more of the same things.

It's time to put aside our siege mentality, and look at protecting the data as it works out in the world, beyond our walls.

Data is the vital stuff of business. You need layered, data-centric security that works in a world without walls, from the start of the data's journey to wherever it travels.





PART III

The Best Defense: Data Security



Data-Centric Security for a Borderless World

Protecting people, places, things...and data

Don't I already have data security?

You've already invested in multiple solutions, including:

- Data loss prevention (DLP) solutions that alert you to or prevent sensitive data from leaving corporate networks;
- Data encryption solutions that encrypt data in transit and at rest on networked storage or mobile devices; and
- Digital rights management (DRM) tools that restrict access to copyrighted or proprietary information.

These solutions often take a limited view of the data to be protected. They handle files on a server, or emails leaving the network. And they still depend on the ideas of walls—systems, devices, or networks that enclose data. They're all about locking data down.

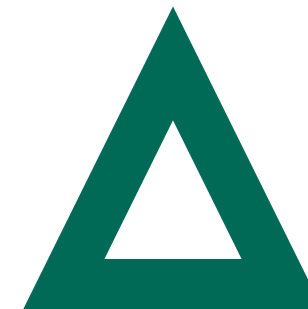
They rarely work at the most critical moment—when people are working with the information. Once data leaves the secure environment of those solutions, it's in the wild and unprotected.

**Data is only valuable to your business when someone uses it.
Let it free—on your terms.**

Collaboration, innovation, partnerships, business development—the behaviors that drive business growth depend on trusted exchanges of vital information.

By locking data down tightly, you slow down business, and potentially diminish the value of the information.

You need a data-centric security solution that lets your business grow and thrive.





Security for Data Anywhere and Everywhere

Vera protects data in use —when it counts

At Vera, we're trying to close the data security gaps by protecting what really matters: the data itself.

Vera secures sensitive data through its entire life cycle, everywhere it travels, no matter who has it or where it's stored. Our 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.





How Vera enhances your data security

We won't get into all of the details of how it works, but here are some important points:

- Vera is storage-agnostic. It doesn't matter what software, storage, network, or other systems you use. Security policies remain with your files anywhere they're stored, including Box, Dropbox, Google Drive, Microsoft, on-premise storage, and more.
- Vera supports many types of data. Vera secures any type of file, including Office documents, PDFs, creative content and medical images. We're actively working to expand the scope of protected information beyond files to application sessions and other places your data travels.
- Vera doesn't store your data. We never scan the contents of your data and only keep encryption keys and policy information. Business users can easily access protected data without downloading Vera, even if they work outside your organization.
- Vera integrates with your existing security. We fit into your ecosystem. Connect Vera with Active Directory and Single-Sign On. Vera also has native integrations with Dropbox, Box, and Office 365. Use the
- Vera SDK or API to add encryption to any home-grown or custom business application.



By adding a cloud-based tether to data access, you can set your data out into the world to drive the business forward, while closing the security gaps.



Here's how it works:

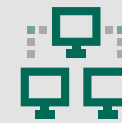
- You (the people in your business) tell Vera which files or systems contain sensitive data. You decide who should have access and what they can do with the data (access rights).
- Vera encrypts the data and enforces those access rights with a secure wrapper around the information.
- Whenever someone attempts to open a file or access the data, Vera confirms access rights and decrypts the data if the person is approved.
- Business users see exactly what they can do with the data. Can they print it? Share it? Save it or change it? Those policies are visible and enforced. Otherwise, the security is nearly transparent to the person working with the data.
- External collaborators can access secured information from the browser without needing to install Vera. Your access controls and policies will persist in the browser as well.
- Your IT team will be able to use Vera's administrative dashboard to see where your data has gone and who has tried to access it. Change policies or revoke access in an instant, even if the data itself is far beyond your corporate networks, on someone's personal computer halfway across the world.

People shouldn't have to change the way they work. Vera makes it easy to get work done, and nearly impossible to do the wrong thing.

VERA PROTECTS DATA IN USE



**Secure any data
(files, email, SaaS)**



**Share any
way you want**



**Track and audit
every access**



**Change policy or
revoke access at will**



Closing the Security Gaps

Closing the Behavior Gap

Vera closes the Behavior Gap by making it easy and obvious to do the right thing with data, without having to learn new applications or change the way you work.

When security travels with the data itself, people don't have to jump through hoops or learn new software. Files open in their native applications; they look and feel like ordinary files. People within your business and beyond can work with the data according to the permissions you grant them.

Vera doesn't force people to change the way they work. It simply adds a layer of security to protect the data in motion, in use, or at rest.

Once someone opens a file, they'll see the Vera policy bar, so they know exactly what they can do with the data.

Closing the Visibility Gap

Use Vera, and sensitive data stays on your radar, even when it's beyond your reach.

From the cloud, Vera tracks when someone requests access to a protected file. You know where the data is and who has accessed it, from anywhere in the world, and you'll get a complete audit trail for compliance purposes.

You'll see when secured data is:

- Accessed, for how long, and from which device
- Accessed by unauthorized users
- Opened in unknown locations



Closing the Control Gap

Vera gives you control of your data through its entire life cycle, as it moves beyond your own systems, through the proverbial “last mile” to another partner’s desktop, phone, or cloud application.

When you first share the data, you can define the level of access that the recipient can have. Vera offers flexible, customizable policies, including:

- The ability to view the data only once
- Automatic “expiration” after a defined time period or date
- Restriction from offline access
- Different levels of watermarking
- Printing and copying restrictions

Better yet, you can change your mind, extending or revoking access as needed.

Have you ever sent an email attachment to the wrong person? Using Vera, you can instantly revoke access. It’s an Undo button that actually works.

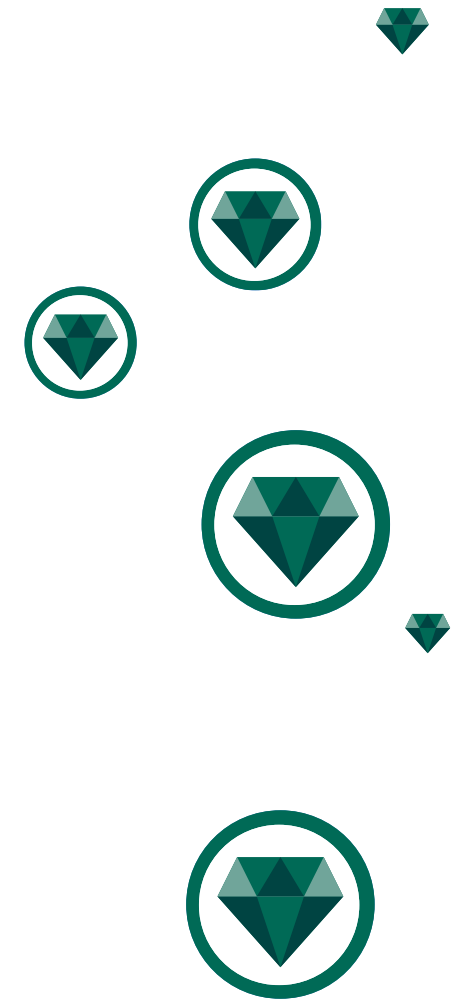
Closing the Response Time Gap

Vera closes the Response Time Gap by giving you the ability to proactively establish access rights, and to change your mind at any time.

Spot unauthorized attempts to access data, and take immediate steps. You can revoke access instantly if an account is compromised, no matter where the data is.

If employees want to use the newest technology or latest apps—great! You still keep control of your data.

We believe security shouldn’t get in the way of business agility.



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.

