FORTRA

Dynamic Data Protection For Financial Services

Protect Files, Accelerate Secure Collaboration And Drive Innovation

Digital transformation is rewriting what a successful financial services organization looks like.

When looking for an industry in flux due to digital transformation, financial services is often the poster child. Gartner's predicts that by 2030, 80% of heritage financial firms will have gone out of business or have been completely commoditized.[1] Some financial organizations are using the digital revolution to optimize processes, but a more ambitious subset is truly focused on transformation to upend existing structures and drive new lines of revenue.

As financial institutions embrace new ways to do business, data insights and technology advancements become more and more central to how they operate. 72% of financial service providers have a formal digital dexterity program in place as part of their business strategy, and no matter where you look within financial institutions, employees are actively collaborating on significant amounts of data. Ranging from data-driven market forecasts, files containing consumers' personally identifiable information to top- secret merger and acquisition intelligence, day-to-day activities within financial services are increasingly centered around highly sensitive information.

However, running an information-driven business in this sector does not come without its challenges!

Finance is one of the most targeted industries by cybercriminals. The rate of data breaches within financial services has tripled over 5 years, according to a joint report by Accenture and the Ponemon Institute[3].

Due to the highly sensitive data with which they operate, financial services is also one of the most regulated industries and they face serious financial and reputational consequences in the event of a data breach.

However, locking down information in order to prevent leaks is not an option. Whether it be traditional consumer banking services, wealth management, corporate finance activity or the burgeoning fintech sector, all divisions within financial services rely on the free flow of information between internal and external stakeholders. The commercial success of the company depends on this.

As well as needing to secure more traditional platforms, financial institutions are adopting cloud-based information sharing tools to simplify communication between an increasingly mobile workforce and extended third-party networks, as well as finding ways to share restricted information with customers and other external stakeholders in order to defend the investment decisions they make.

So, how do information security teams protect all this sensitive data as it flows through different systems and communication platforms, without slowing down revenue-driving activity?

The Data-Driven World of Financial Services

Information-driven financial services organizations need to share and collaborate on data to drive their business successfully. This information comes in all shapes and sizes; however, invariably is highly sensitive and subject to strict regulations.

One of the biggest risks for financial services companies is that unencrypted data gets into the wrong hands, leading to potential data breaches, regulatory fines, damaged customer trust, leaked IP or loss of competitive advantage. IT teams need a way to enable authorized parties – both internal and external- to freely share, consume, and work with critical data, while maintaining control over user access and permitted actions.

Personal information of customers, employees and recruits

Investment research and financial modeling – the intellectual property of wealth management company's

Packets of client documents for external auditors and legal counsel

Sensitive financial information linked to loans, mortgage applications, auto financing, etc.

Board documents containing mergers and acquisitions information, private equity, preparation of IPOs and bankruptcy coordination, etc.

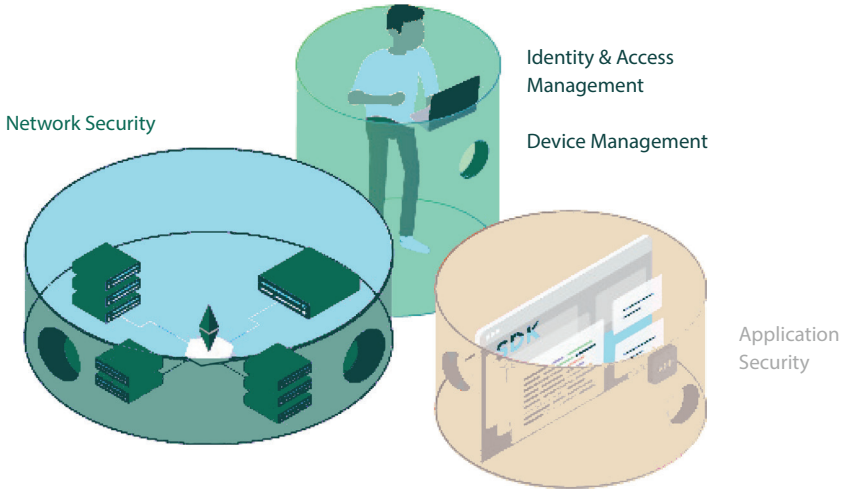
Files for the board's eyes only, including strategy plans, meeting minutes, risk reports and operational information.

Why is information still leaking, despite extensive information security technology investments?

The way we work has changed forever.

Recent years have seen the rise of mobile and remote workforces sharing large amounts of data on the go, liaising with complex networks of third parties, and uploading critical data to external SaaS and IaaS platforms.

Security that relies on locking information down within internal walls no longer works for the modern financial institution. Enterprise security perimeters are porous, and data will inevitably travel.



Security that relies on locking information down within internal walls no longer works for the modern financial institution. Enterprise security perimeters are porous, and data will inevitably travel.

DEFENSIBLE SECURITY:

How Do Financial Services Prove They Are Doing Enough To Protect Data?

Financial services are solving increasingly complex information sharing requirements from the business within an increasingly hostile threat landscape. With ever-evolving cyber threats targeting the industry, 100% security can no longer be guaranteed.

Organizations need to prepare for the possibility of data breaches, and part of that preparation is being able to show that they have done everything in their power to protect critical information and regulated data across the extended enterprise. They need to be able defend security investments to customers, board members, shareholders, and external auditors.

As well as assessment of the security controls around their technology stack, there are often systemic and cultural issues that stand between IT and non-IT employees that hinder efforts to remain secure and compliant.

IT needs a pragmatic approach that enables its workforce to stay productive and achieve business outcomes, while operating in a secure fashion.

For a program to be defensible there are both technology and business best practices that must be followed to ensure success.

What Is "Defensible" Security?

A security program that can demonstrate in an audit that the organization does enough to protect its information and can defend decisions in the event of an incident.

Do You Have A Defensible Security Strategy?

- Are you assessing both technology and business processes information security best practice?
- How does your security regime's performance compare with industry averages?
- Do your information security practices extend beyond IT into all employees' daily operations?
- Are you prepared for audit in the event of a security incident?
- Do you retain data that can defend security posture at different points in time?

Technology Best Practice For Defensible Data Security

1. Encrypt All Non-Public Info Shared Internally And Externally

Financial services must ensure that data is protected at rest and in transit with encryption to prevent malicious or unauthorized access. As data is shared across email, cloud tools and cloud storage and other systems, IT needs technologies in place that can apply data-in-use protections that limit what recipients can do with non-public data.

2. Attach Security Policies To The Data Itself

As financial institutions operate in increasingly complex technology ecosystems, it becomes less and less effective to define access at the system, device, or perimeter level. Data is regularly stored on multiple repositories, both within the organization and across different external audiences. By deploying encryption at the file level, with security policies that follow documents wherever they travel, information is protected as it is stored and forwarded across any system.

3. Implement An Audit Trail To Show User Access And Data Use

Demonstrating regulatory compliance to financial services mandates such as GLBA and FFIEC requires increasing levels of visibility across complex systems. Firms need to ensure they have robust data mapping and know what information is stored where. They need an automated way to track logs and monitor access privileges, to provide a full audit trail of where data has traveled, who has accessed it, and what actions they have performed with that data. Crucially, this needs to extend outside the organization when there are third parties and customers accessing sensitive.

4. Deploy Access Controls That Work In Real-time

Common encryption solutions and security tools like Data Loss Prevention (DLP) are great technologies, but lack the ability to make real-time updates to access rights, especially once non-public information is sent beyond the organization. Financial services must retain control of data through its entire lifecycle and ensure that they have technological solutions in place that can allow them to adapt to changes in personnel, expire access after certain time periods and authorize or revoke user access on a granular level, at any time.

Business Best Practice to Protect Your Information

Data security for financial services does not end with technology solutions. Security investments that are made in isolation of the business, and interfere with the way they operate on a daily basis are often doomed from the outset. Securing data across dynamic organizations requires a security-aware culture that extends far beyond the IT security team and a focus on usability that seamlessly embeds secure practices into day-to-day tasks.

1. Expand Accountability For Security Beyond The IT Team

CIOs and CISOs need to provide clear leadership and communication of the organization's security strategy, however to ensure successful roll-out of security investments accountability for security programs should be expanded across department leaders, for example human resources and legal. Involving department heads in decision-making and ensuring they are aware of the risks within their departments can help successfully implement secure practices.

2. Align With Proven Best Practice And Standards

An important part of running a defensible security program is to align with established industry standards such as the NIST cybersecurity framework, ISO/IEC 27001/2, and CIS Critical Security Controls. Business are recommended to create an Information Security Charter for their organization – a short document that establishes accountability for protecting sensitive info and provides directives for executives managing the program.

3. Establish Privacy-By-Design From The Outset

According to research from the CPO Magazine, 1 of 2 organizations allocate less than 5% of their governance, risk and compliance budget on data protection and privacy. With increasingly strict data privacy regulations, organizations need to establish privacy-by-design approaches. IT needs to retrospectively apply data security controls to existing systems, and ensure privacy is prioritized as new systems are planned and developed. To do this effectively, CIOs must engage senior leadership, educating them about the significant consequences – spanning regulatory fines, financial loss, and executive job losses – in the event of a breach. Senior leaders across all departments must help drive a privacy-aware culture across the organization and partner with Security to drive a mature data governance framework.

4. Focus On Simplicity And User Experience

By ensuring that data security controls are centered around current and evolving user behaviors, and making it easy to securely share information, IT teams will improve adherence to policy and dramatically advance governance and security.

Let's take a look at some scenarios within financial services, where applying technological and business best practice can protect business-critical information as it flows between internal and external stakeholders.

Secure Information Sharing Between Employees

The Data-Driven World of Financial Services

The way we work is changing. We are increasingly information-driven, and need to collaborate on information in real-time to remain productive. Employees are increasingly tech-savvy and rather than waiting to take IT's lead on the methods they use to communicate, IT change will increasingly be driven forward by the needs of employees.

How does your information security team secure data as it flows between employees, prevent unauthorized access, without getting in the way of employees' work?

Mobile connectivity and a remote workforce has let to an increasingly "always on" culture, with employees working with sensitive information outside traditional devices.

Certain files need to be closely guarded within small, authorized circles such as the board, the C-Suite or departments handling sensitive information such as human resources and legal.

The "insider threat" means sensitive information is at risk of being leaked by disgruntled and malicious employees.

Secure Information Sharing Between Employees

SOLUTION: Data-Centric Protection That Works Behind the Scenes

Financial services companies need to seamlessly embed encryption into the sharing of data – no matter how and where employees wish to collaborate. The secret? Data–centric security that encrypts the file at its source, with security policies that move with it across any platform or device.

VERA'S TOP TIPS:

- Automate encryption so that no additional steps are required from users to share securely
- Deploy security controls that are invisible to authorized users, meaning you never slow them down
- Track all sensitive files, retain a centralized view of where data resides and deploy real-time controls to quickly adapt to personnel changes
- Use security policies to prevent data leaving the corporate network without permission
- Prioritize usability to avoid employees circumventing official processes to speed up information sharing
- Empower your workforce with self-service security options that do not always require intervention from the central IT team to grant or revoke access to files

case study

CASE STUDY:

Large finance corporation secures remote working with Vera technology One of the top 10 US banks leveraged the Vera Cloud Platform to encrypt files traveling out of the traditional network and to enable remote working.

REQUIREMENTS

- Secure files sent to employees' personal devices (BYOD) Encrypt and manage data shared on cloud platforms (Dropbox, Box & SharePoint)

SOLUTION

Using Vera, the company switched to a data-centric security strategy that protected files at the source and supported flexible working habits across their employees.

Secure Information Sharing Between Employees

Central to the way that many financial institutions operate is collaboration with external stakeholders, often around highly sensitive information.

How do you retain visibility and control of sensitive data once it leaves your organization?

Wealth management firms risk valuable intellectual property being leaked when sharing investment advisories with customers and other external stakeholders.

Information is shared across supply chains with finance organizations outsourcing a variety of functions, for example, credit risk assessments and collections.

As a highly regulated industry, external auditors need access to large swathes of sensitive client data and documents.

When employing services such as legal counsel, financial services organizations need a way to share and collaborate on information that cannot be leaked to wider audiences.

Secure Information Sharing Between Employees

SOLUTION: Security That Follows Your Files Anywhere They Travel

To allow easy collaboration with external parties, without risking leaked data or regulatory action, financial services need a solution that can retain control over access even once it has been sent to an external party.

Financial services companies can use data security technology to deploy automated encryption and decryption, allowing authorized parties to freely share information while dramatically reducing the risk of data breaches.

VERA'S TOP TIPS:

- Auto-encrypt files whenever they leave the corporate network with technology that decrypts information for authorized recipients, mitigating the risk of unsanctioned access to sensitive information
- Deploy technology that can track files even when downloaded onto external devices, so you still maintain visibility of where your data resides externally
- Attach security policies to data as it travels, with clear parameters that define how external stakeholders can use proprietary information – e.g. forward, copy & paste, print, edit, etc.
- Attach security to files that can follow across any system, giving employees the flexibility to collaborate in the way that suits them

case study

CASE STUDY:

Financial management organization uses Vera to automatically encrypt every file

This firm offers money management and investment advisory, and every file shared is classified as highly-sensitive.

REQUIREMENTS

- Automated encryption of sensitive financial information when shared internally and externally
- Invisible protection that does not disrupt current work-flows

SOLUTION

The Company deployed Vera to encrypt and secure over 1 million files. The SaaS deployment was smooth, and they quickly got peace of mind that information was secure, without slowing down information sharing

Secure Information Sharing Between Employees

SaaS platforms such as Dropbox, Box and OneDrive provide financial services with simplified file-sharing between global, mobile and remote workforces and their extended enterprise of partners, customers and shareholders. Financial services IT teams are under increasing pressure to deploy this type of information sharing, even files containing highly regulated data. If they don't enable the business, they risk a shadow IT scenario with employees sharing unencrypted information outside of sanctioned systems.

How do you ensure that data is protected when it is residing or shared on a SaaS file-sharing platform?

Loss of visibility and control of files including customer data, intellectual property and financial reports

Danger of restricted data being breached after being downloaded onto external devices from cloud platforms

Risk of cloud providers accessing non-public information that is being stored on their platforms

Risk of cloud providers accessing non-public information that is being stored on their platforms

Secure Information Sharing Between Employees

SOLUTION: Data Security That Is Custom-Fit For Cloud Collaboration

Financial institutions need a security solution that is custom-fit for this way of sharing data, and that works seamlessly across any cloud collaboration platform.

VERA'S TOP TIPS:

- Encrypt data whenever it is uploaded to a SaaS platform
- Assign specific permissions to files to determine how different recipients can use data and how long they have access for
- Use automated controls which integrate seamlessly into popular SaaS platforms to avoid slowing down access to data
- Track data as it is shared in the cloud and after it is downloaded onto external devices
- Retain logs on which users have opened files and where they have been forwarded to give you a full audit trail for

case study

CASE STUDY:

Major stock exchange uses Vera to secure Dropbox implementation

The Company wished to adopt popular file-sharing platform, however, due to the sensitive nature of its information, they required assurance that all files were fully protected.

REQUIREMENTS

- Clear security strategy for cloud file-sharing, prior to adoption of Dropbox
- Encryption of all data stored and shared in the cloud

SOLUTION

Pre-built integration between Vera and Dropbox addressed security concerns and allowed the widespread roll-out of the technology. They deployed military-grade encryption of all files uploaded to the cloud, and continued to track files once downloaded externally.

Planning A Roll-Out Of Cloud Data Sharing Tools? Ask These Questions First!

Let's always remember that the core focus of cloud file-sharing platforms is accessibility of data, not security. Therefore, information security teams must have a clear strategy from the outset when adopting cloud collaboration tools. They need to ensure they do not lose all control of data if it is accessed and downloaded off a cloud tool onto an external device.

Thinking through security controls and encryption requirements from the outset saves the painful job of retrospectively fitting suitable solutions after adoption.

How do I automate encryption and decryption of files shares on cloud to ensure secure practices across all teams?

How do I retain control over who views files once they have been downloaded off the cloud repository?

Can I prevent visibility into the content of my sensitive files by cloud vendors?

What tool do I have in place to prevent any unauthorized forwarding of my information saved on the cloud?

Am I storing data in the cloud in a way that in compliant with data protection laws?

Do I have an audit trail of data as it travels across cloud platforms and beyond?

Secure Information Sharing Between Employees

IaaS provides cost-effective and scalable solutions, which are a game-changer for storage and are being adopted by an increasing number of financial services companies to move data off-premise and to run applications more efficiently. Most cloud storage options provide an array of security measures, however, cloud security is often dependent on the company correctly configuring these and understanding exactly where the service provider's responsibility ends, and the cloud customer's responsibility begins.

VERA'S TOP TIPS:

- Ensure sensitive data is encrypted when stored in the cloud
- Keep access logs and monitor for unusual behavior among cloud users
- Ensure you have clarity on liability in between you and your cloud provider in advance of a security incident

Misconfiguration of security controls within cloud storage platforms and failure to encrypt sensitive data

Lack of clarity about where the cloud user's responsibility to keep their environment secure

Inadequate visibility into where security failings lie across multiple cloud accounts

Insufficient identity and access management allowing unauthorized access to cloud accounts and sensitive data

Regulatory Compliance

On the Horizon: A Regulatory Crackdown

And lastly... It wouldn't be an eBook about security for financial services without talking compliance!

Financial services have a comprehensive set of existing compliance requirements specifically for their industry, but are also navigating an increasingly complex web of state, national, and international regulation focusing on consumer privacy.

The concept of defensible security is upping the ante on how far financial organizations need to go to demonstrate in an audit they have sufficient security protections in place through their technical controls and business processes.

Compliance mandates targeting the financial services such as GLBA, FFIEC require firms to demonstrate how they protect consumer data within financial systems, with extensive auditing requirements.

GDPR

Increasingly numbers of international regulations, for example GDPR (Europe) and PIPEDA (Canada) making data protection a priority for any organizations touching consumer data in those locations.

CCPA

State-level regulations in the United States are raising data protection requirements domestically, for example CCPA (California) introduces legislation on how companies can handle and store personal information

PCI

Firms handling any credit card data must comply with PCI DSS, which introduces updated requirements periodically and require annual audits

Regulatory Compliance

Organizations who fail to encrypt personal data and secure data shared with third parties risk falling foul with serious consequences.

As financial institutions prepare for a future of zero-tolerance of leaking personal information, they need to embed security into their data sharing processes whenever it touches consumer information and credit card data.

VERA'S TP TIPS:

- Deploy strong encryption technologies to prevent access from malicious parties
- Automatically encrypt files containing personal data to address evolving data protection regulations
- Achieve a centralized view of where critical data resides to simply the process
  of verifying and demonstrating compliance
- Establish an audit trail of file sharing to provide internal and external auditors transparency into who has accessed what information and demonstrate security over time
- Retain granular control of files containing personal data when shared with third parties to prevent external stakeholder leaking restricted data.

Remember, even if it is a third party that leaks your data it is your organization that is exposed to regulatory action.

Why Financial Services Work With Vera to Advance Their Data Security Strategy

At Vera, we have a unique approach to data security that can quickly solve the headache of securely sharing and collaborating on sensitive files both internally and externally. This ultimately allows a secure way to guarantee the free-flow of information between external and external stakeholders, allowing your institution to thrive in an information-driven world.

Data-centric security that travel with any file, across any platform, and any device

Military-grade encryption that keeps bad actors out and prevents unauthorized users viewing your content

Maintains control of sensitive files even after they have been shared with external users via cloud collaboration tools

Restricts access to files containing PII and PCI to support compliance with data protection and financial regulations

Centralized dashboard and extensive reporting capabilities to support auditing

Simple SaaS deployment and pre-built integrations with major cloud tools and popular IAM solutions

How Vera Extends Your Current Data Security Investments

Many organizations use DLP to successfully block sensitive data from leaving the corporate network. Vera integrates seamlessly with DLP solutions to extend this protection to files that need to move externally through encryption and granular security policies.

CASB has provided financial organizations with a way to monitor access to files stored in the cloud and enforce security policies. Vera integrates with existing CASB technologies to extend protection to files downloaded from cloud tools onto external devices in order to allow collaborators to work with information on their own desktop without the organization losing control or visibility of proprietary information.

Most financial organizations use data classification tools to determine the sensitivity of its data and files containing intellectual property. Vera leverages existing data classifications to automate which security controls are applied to different levels of data.

Financial organizations have put a number of technologies in place to protect their data, such as Data Loss Prevention (DLP), Cloud Access Security Broker (CASB) and data classification. These can be a great first line of defense to monitor and block information loss within corporate networks and cloud applications.

Vera's solution works seamlessly with existing data protection technologies, providing a vital additional layer of security that focuses on flexibility and movement of data across the modern extended enterprise.

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.

fta-vr-gd-1022-r1-79d