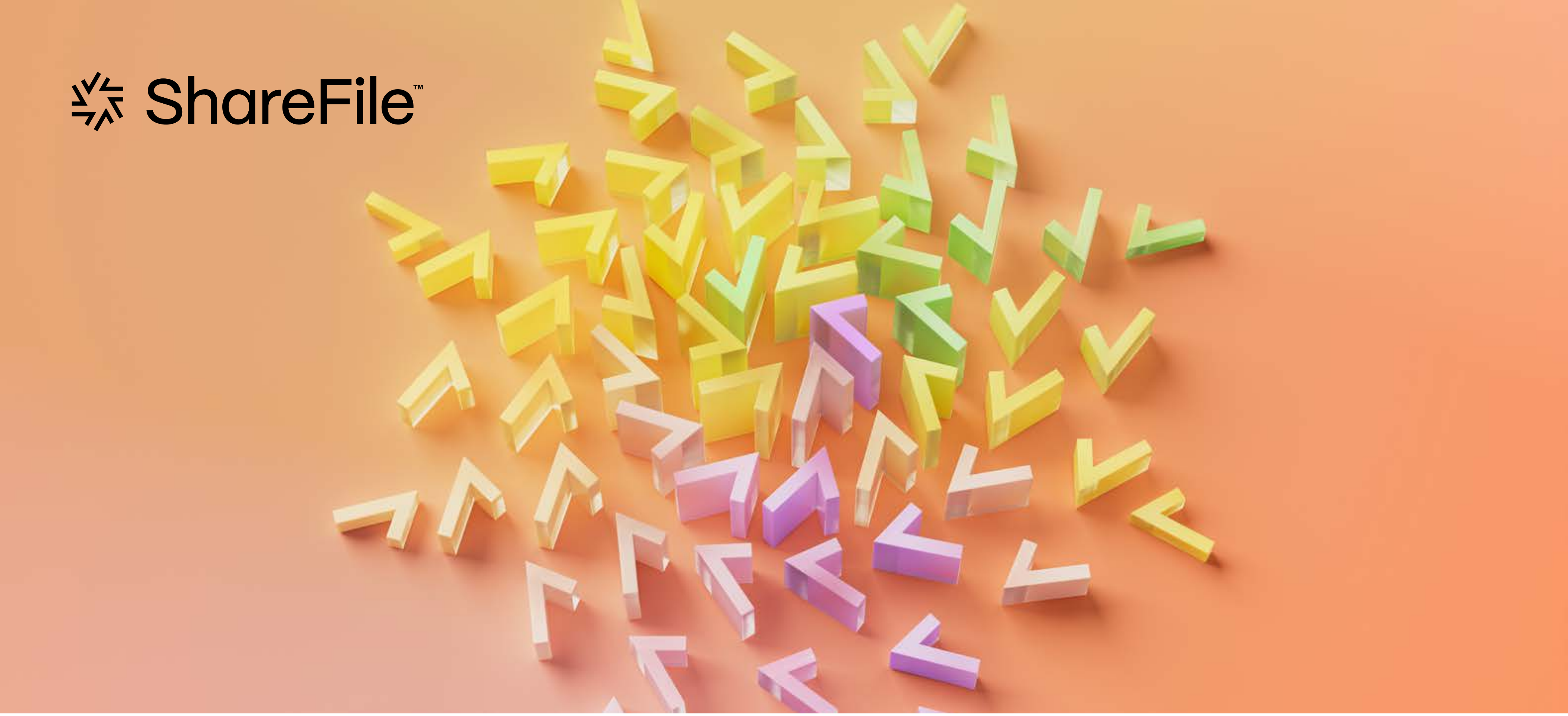
ShareFile™



# Modern data security for small and mid-sized law firms

## A complete guide to safeguarding your clients' and your firm's data with secure document sharing

# Executive summary

To boost revenues and better respond to the increasing online demands of both courts and clients, many law firms are adopting cloud technologies. These solutions give legal teams a fast, scalable way to leverage the latest technology tools without the need for substantial upfront capital investment. Plus, they value having anytime, anywhere access to their data, predictable monthly expenses, and reliable data backup.

But they also recognize that these solutions come with a big risk: security.

And it's with good reason. More than a quarter of law firms say they've experienced a data breach.

But in spite of these "warning signs," many firms, especially small and mid-size ones, still aren't implementing the necessary security precautions. In the ABA 2022 Legal Technology Survey, only 40% reported using any standard cybersecurity practices—and almost one in five revealed they employed no security measures at all!

> "The continuing lack of attention to confidentiality, security, and due diligence issues remains a serious and disturbing concern."
>
> – 2022 American Bar Association Cloud Computing Report,
> Legal Technology Survey

Legal teams are responsible for gathering, sharing, and securing thousands of legal documents. Given their exposure to cyberattacks, why aren't they taking the right steps to secure sensitive data? And just how safe are they from potential lawsuits themselves? One possible reason could be that law firms are selecting solutions without vetting them for the appropriate security features. Another reason could be that their existing tools don't include the necessary security features that employees can self-manage easily, without the need for robust IT support.

In this eBook, we'll provide some clarity about the essential features that cloud-based client collaboration solutions must have to ensure the security of your firm and client data and enhance your firm's overall security posture. It also offers a practical framework for you to compare different options and make an informed purchase decision.

# Three impacts resulting from poor document-sharing and security practices

## 1. Exposure to cyberattacks

Cybercriminals know that legal files often contain valuable data—financial records, Social Security numbers, patent specifications, M&A plans, personally identifiable information, and more. Because of this target-rich environment, about one in every 40 cyberattacks is now directed at the legal industry.

These actors search for—and often find—weak links in a firm's document storage and sharing processes. Sadly, most weaknesses are due to human error.

For small and mid-sized firms without a dedicated IT team, those weak links can be:

- Easy-to-guess passwords (such as Password123)
- Employees reusing the same password across multiple tools and platforms
- Employees keeping the same password for an extended period
- No multi-factor authentication to confirm that only authorized recipients are accessing the data
- Phishing emails that dupe team members into sharing information or allowing access

One in every 40 cyberattacks is now directed at the legal industry.

## 2. Reputation damage

Because of the potential damages—and widespread publicity—that often comes with a data breach, law firm clients are taking notice and taking action.

A recent ABA survey revealed that 33 percent of respondents have been asked by clients and potential clients about their security capabilities. More to the point, five class action suits were filed in Q1'23 alleging the legal operations of prominent law firms failed to protect their data from potential cyberattacks.

Bottom line: *act now before it's too late.*

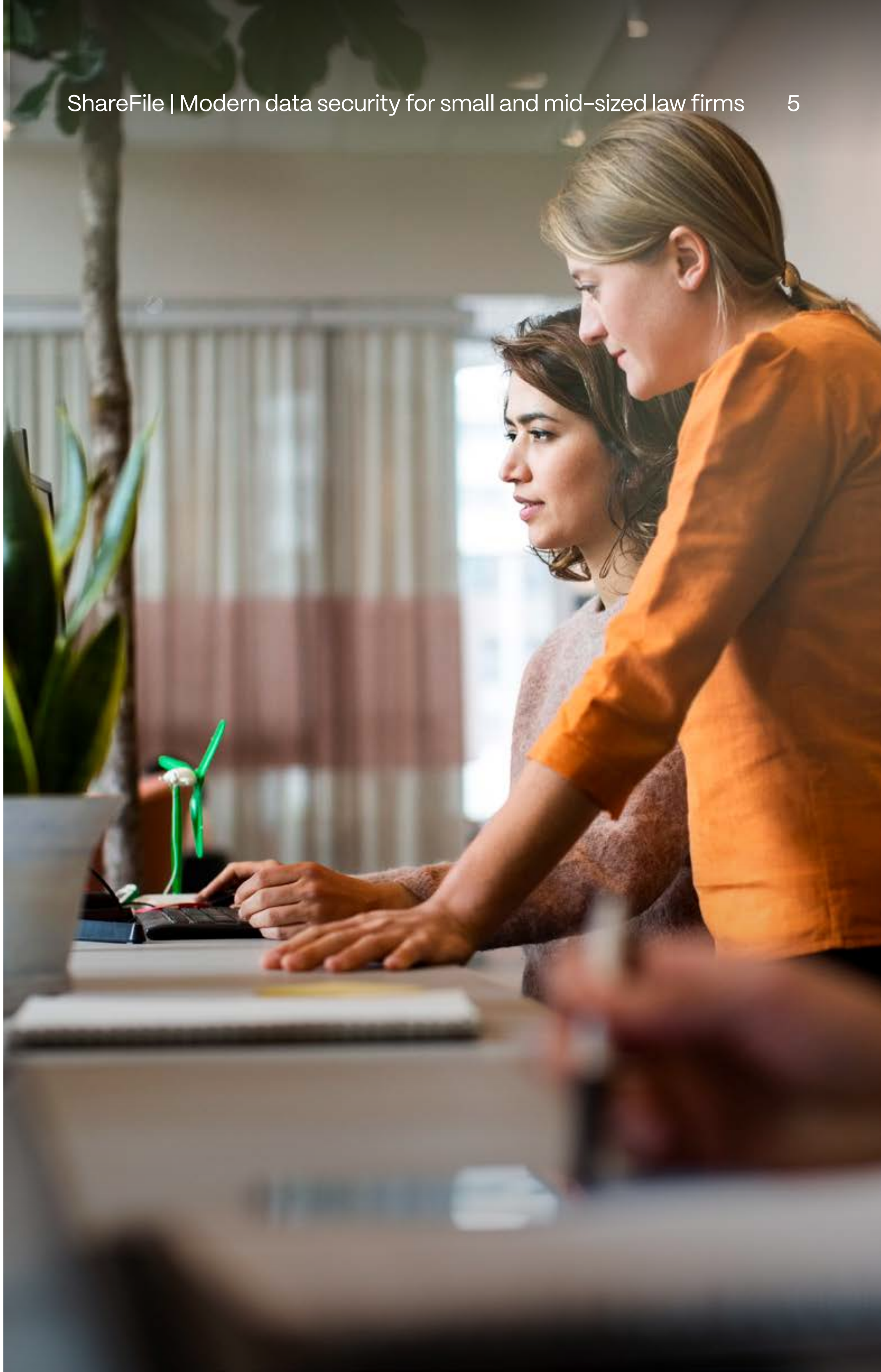
## 3. Revenue loss

Once a firm becomes a cyberattack victim, the road to recovery is long and expensive.

In 2022, the average time (across all industries) to identify a data breach was 207 days. The average time to contain it was 70 days.

That's valuable time, effort, and expense that legal and IT teams must spend on data recovery and remediation—time that should be spent on servicing clients and generating billable hours.

> "The average cost of a data breach could reach $5 million by next year."
>
> – Acronis Cyberthreats Report 2H2022



# Three key capabilities every law firm needs to safeguard their data

As cybercriminals deploy more sophisticated attacks using artificial intelligence, larger firms are increasingly using tools such as managed detection and response, security information and event management (SIEM) systems, and advanced identity and access management (IAM) solutions to protect themselves.

However, smaller law firms typically don't have the same level of financial and technology resources available.

To best protect your firm and client data, smaller firms should invest in a cloud-based client collaboration solution that provides the following security capabilities:

1. **Secure document management controls** – Enables your firm employees—without IT involvement—to create security and sharing guidelines and permissions for clients and third parties to control who can view, edit, and share data
2. **Secured collaboration** – Safely transmits documents using encrypted file and email communication
3. **Security threat alerts** – Delivers real-time alerts when a security threat is detected so admins can respond swiftly

In the following pages, we'll explore the various software features that enhance these capabilities.

## Secure document management controls

A chief concern among legal teams is accidentally sharing protected documents with opposing counsel, or not redacting sensitive information within documents and correspondence. Teams can also be geographically dispersed or operate in remote/hybrid work environments. Yet, they still need solutions that facilitate seamless access and exchanging of documents from anywhere.

Secure document management provides an efficient process for protecting your information and ensuring only authorized users can gain access throughout the duration of a case.

**Look for a solution that provides:**

**Strong password hygiene** – Creates and sets guidelines for password complexity and periodic password changes (usually every 90 days) to ensure that only authorized individuals gain access

**Watermark features** – Quickly applies unique identification marks to deter downloading and printing of sensitive documents

**Download restrictions and sign-in requirements** – Restricts document sharing and viewing by limiting the number of individuals who can download and view documents

**Multi-factor authentication (MFA)** – Enforces a 2nd form of validation (such as text link or email authorization) to confirm that client documents are only accessed by your desired recipients

**Remote wipe** – When laptops are stolen or misplaced, IT admins can quickly "lock" them or erase their data to prevent data theft or unauthorized access

**Secure communications and file storage** – Automatically protects all shared documents and email communications with AES-256 encryption (one of the most secure encryption algorithms available) without human involvement

## Secure collaboration

A strong legal strategy depends on effective client communication and collaboration. However, it can't come at the expense of protecting your data. The best solution is one that delivers the security protection your organization (and client) requires without changing how people prefer to work.

**Look for a solution that provides:**

**Sharing permissions and authentication** – Sets up authentication access on a document level to control who can access, edit, and share documents

**Use of links instead of email attachments** – Eliminates restrictions imposed by email size limits and facilitates safer email practices

**Secure client portal** – Creates a single, secure location where everything related to a case—document, communications, workflows, contacts, etc.—is stored and easily accessed by all authorized users

**Seamless co-editing** – Allows users to provide immediate feedback, edits, and approvals within documents to eliminate the need for separate, unsecured email correspondence

**Secure data transfer** – Automatically encrypts all documents and communications being shared with clients and third parties

**Activity reporting** – Assigns tasks and deadlines for your team members and clients while enabling everyone to stay current on the status of legal workflows

## Security threat alerts

Security threat alerts immediately notify your team of any unauthorized document access or sign-in attempts. That way, you can identify and address them promptly and potentially stem financial losses.

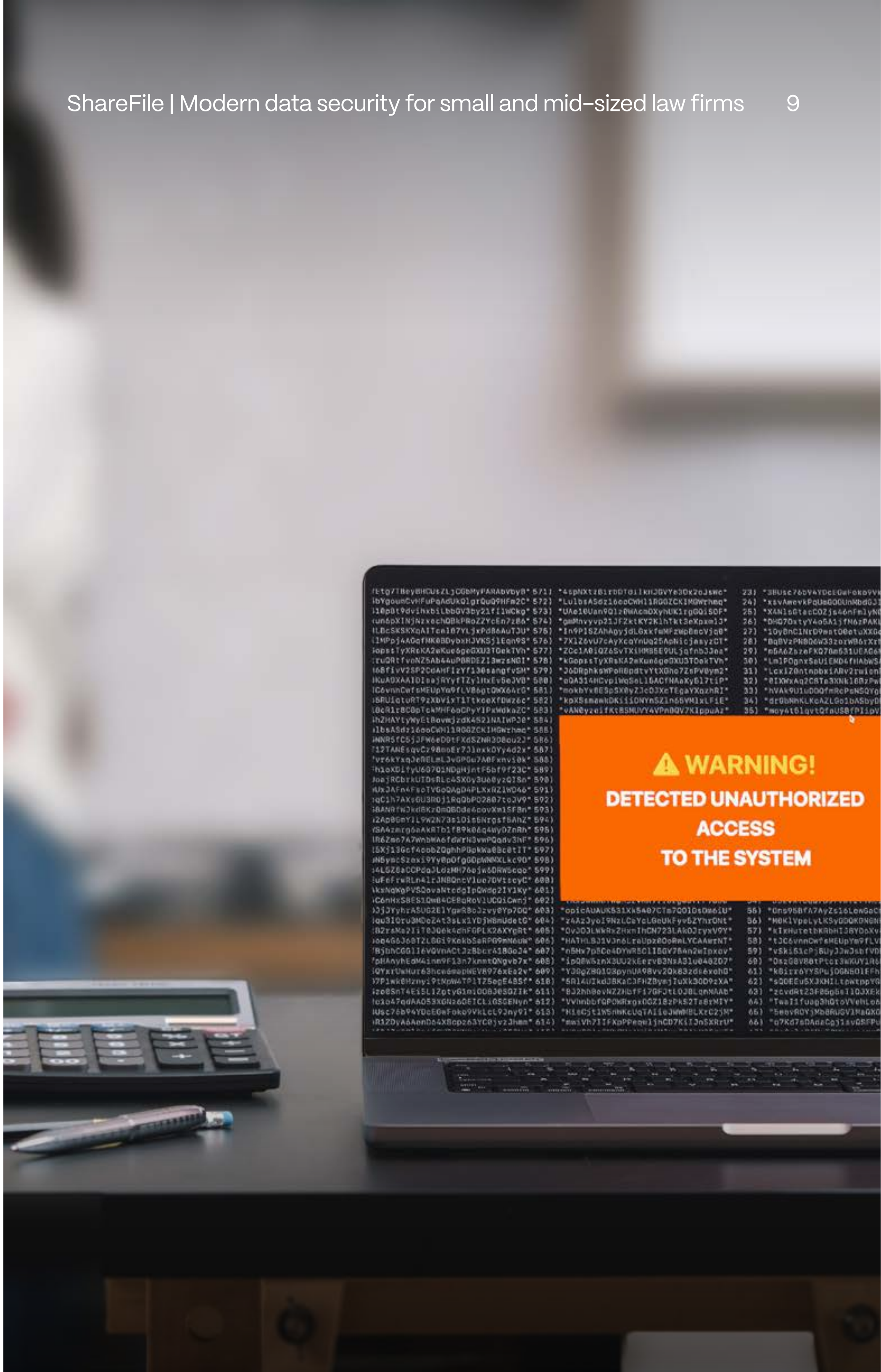
**Look for a solution that provides:**

**Unusual sign-in threat alerts** – Prevents real-time notifications of unauthorized access from suspicious user locations (such as access from a foreign country) or devices

**Multiple failed sign-in alerts** – Delivers real-time alerts when person or entity is making multiple attempts to gain unauthorized access

**Malware upload alerts** – Blocks (and alerts you about) malware uploads to prevent widespread damage or data loss

The average daily cost of a data breach in the US is $8,640 per day.



# Secure your operations and create better client engagements with ShareFile

Every law firm believes in putting their clients first. But now, it's just as essential to put their case data first as well.

With ShareFile for legal, small and mid-size firms finally have a secure, easy-to-use workflow solution that allows team members to streamline document-heavy workflows, enhance security protection, and offer seamless client experiences—without compromises.

Discover how ShareFile can give your firm:

- **Peace of mind** – Gives clients confidence that their content is secure from the initial exchange through project completion
- **Proactive security** – Enables team members to quickly address security risks when handling client documents with security alerts
- **Threat identification** – Locates threats related to unusual access and malware upload based on events

**Visit ShareFile.com to learn more.**