

Osterman Research

RESEARCH REPORT

Research Report by Osterman Research
Published **October 2026**
Commissioned by **OPSWAT**

The 2026 Enterprise File Security Report: AI Is Exposing the File Security Gap

Executive summary

Files are under sustained attack, and AI is intensifying both the threats coming in and the data leaking out. Security leaders believe their defenses are stronger than the evidence shows. That gap will widen as AI-driven threats accelerate. Something needs to change.

This report presents the data from a recent research initiative exploring the threat and protection dynamics of enterprise files in the age of AI. It examines the effects of the paradigm shift from detection to prevention, where confidence in security posture measurably increases, and assesses the distance between self-assessed maturity for file security and what the evidence actually supports (it's significant). Finally, it proposes a set of grounded actions for organizations to pursue as they strengthen their file security posture for a rapidly intensifying AI-driven threat landscape.

The severe gap between capability and confidence for file security will continue to widen as AI-driven threats rapidly intensify—unless human barriers to better file security posture are urgently addressed.

KEY TAKEAWAYS

The key takeaways from this research are:

- **AI is accelerating threats against files**
  Nearly 60% of respondents expect AI to make file security more difficult for their IT and security teams. That concern is already climbing—worry about AI-driven threats to files has risen by almost 80% across the 24-month window examined, with generative AI and large language model threats rising fastest, up 105%.
- **The maturity gap is severe: the data shows a striking contradiction**
  73.6% of respondents self-assess their file security posture as very or extremely mature. But correlating respondents' actual answers across the survey against a maturity framework shows that no organization gives evidence of either of the top two levels of maturity, and 85.8% evidence no more than "somewhat mature." What leaders believe about their posture is unsupported by their own answers.
- **Threat actors are actively targeting files**
  68.1% of respondents say that cybercriminals are more focused on circumventing their file security protections than 12 months ago.
- **IT and security leaders are conflicted about the way forward**
  27.2% of respondents strongly agree a paradigm shift away from a detection-first approach is needed, the highest agreement of any file security posture statement tested. Yet many still endorse detection-based approaches. The industry is in transition and knows where it needs to go—but hasn't gotten there yet.
- **Barriers are human, not technical**
  The top two reasons why prevention-first solutions aren't deployed are lack of leadership support and lack of knowledge—both human barriers, not technical or cost ones.

ABOUT THIS RESEARCH REPORT

The survey and research report were commissioned by OPSWAT. Information about OPSWAT and details on the survey methodology are provided at the end of the report.

©2026 Osterman Research

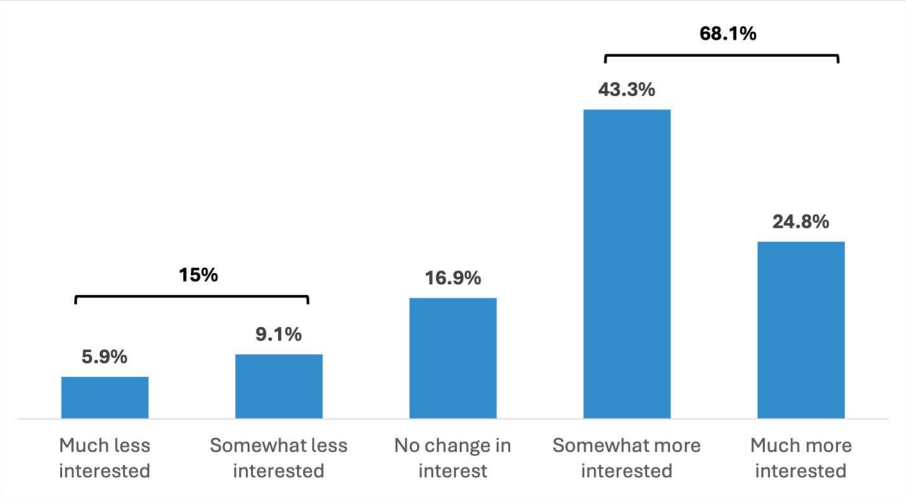
Risks and threats to file security

Are files a security threat for organizations? This section looks at the current risks and threats to file security, including threat actor interest, employee actions, and data breach consequences.

THREAT ACTORS ARE MORE INTERESTED IN CIRCUMVENTING FILE SECURITY PROTECTIONS

68.1% of the respondents in this research say that the activity and targets of cybercriminals over the past 12 months show growing interest in circumventing their organization's file security protections. Only 15% of respondents say that cybercriminals are less interested. See Figure 1.

Figure 1
Interest by cybercriminals in circumventing file security protections over the past 12 months
Percentage of respondents



Source: Osterman Research (2026)

Cybercriminals are increasingly interested in circumventing file security protections.

Examples of this growing interest in circumventing file security protections include:

- High levels of risk from files coming into an organization (e.g., files downloaded from unknown sources) combined with low confidence in ability to prevent malware and other file-related threats from compromising files through those same methods.
- Growing levels of concern for file security due to the use of AI by threat actors, such as using AI to generate threats that evade AI-powered security defenses. On average, the level of concern increases by almost 80% for a range of AI-driven threats over the 24-month timeframe we asked about.
- Looking ahead over the next 12 months, 59% of respondents anticipate heightened impact on the time taken to deal with file-related security activities due to the use of AI by threat actors. Most respondents expect file security to become more difficult due to offensive AI.

©2026 Osterman Research

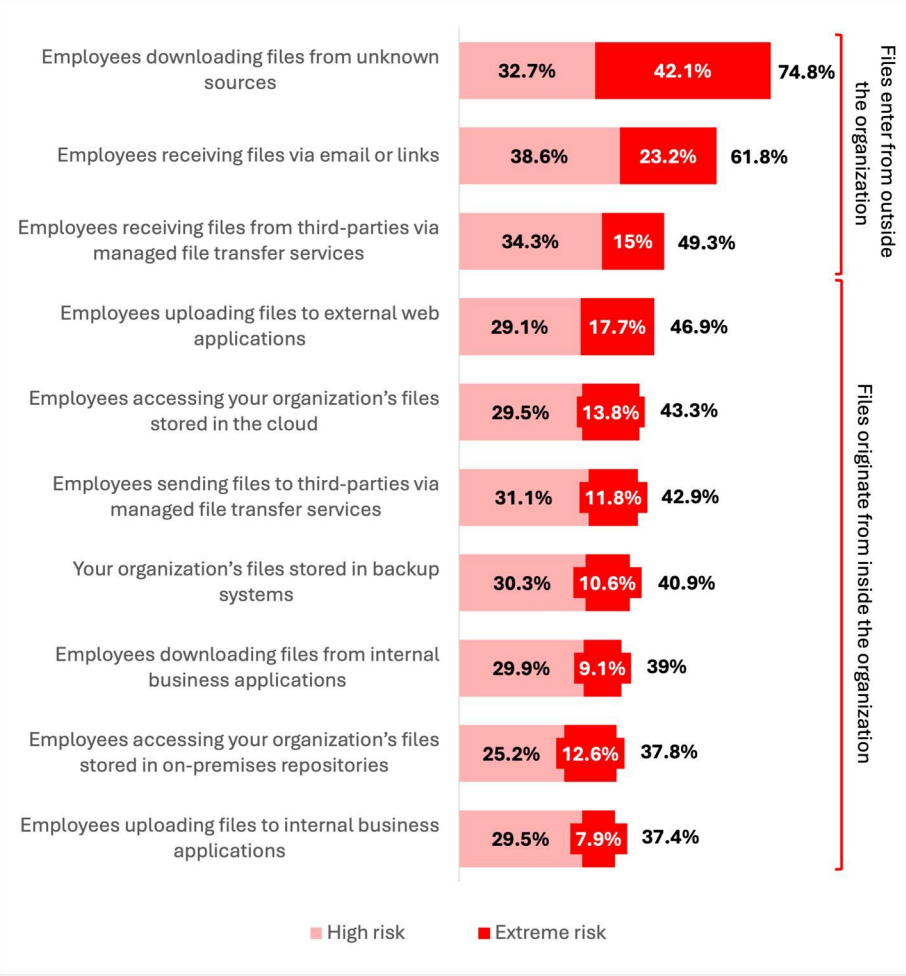
FILES OF ALL KINDS ARE A CYBERSECURITY THREAT

Employees engage with files under many different situations while carrying out their work. The three situations that carry the highest risk all deal with employees downloading or receiving files from outside the organization—by downloading from unknown sources (42.1% of respondents indicate this is an extreme risk), receiving files via email or links, and receiving files via managed file transfer services. On average, respondents report these three situations are a high (35.2%) or extreme risk (26.8%).

The other seven situations we asked about all originate from files managed within the organization. Across these situations, an average of 29.2% of respondents indicate high risk and 11.9% see them as an extreme risk.

See Figure 2.

Figure 2
Files are a cybersecurity risk under multiple situations
Percentage of respondents (and sum of the two risk statements)



Source: Osterman Research (2026)

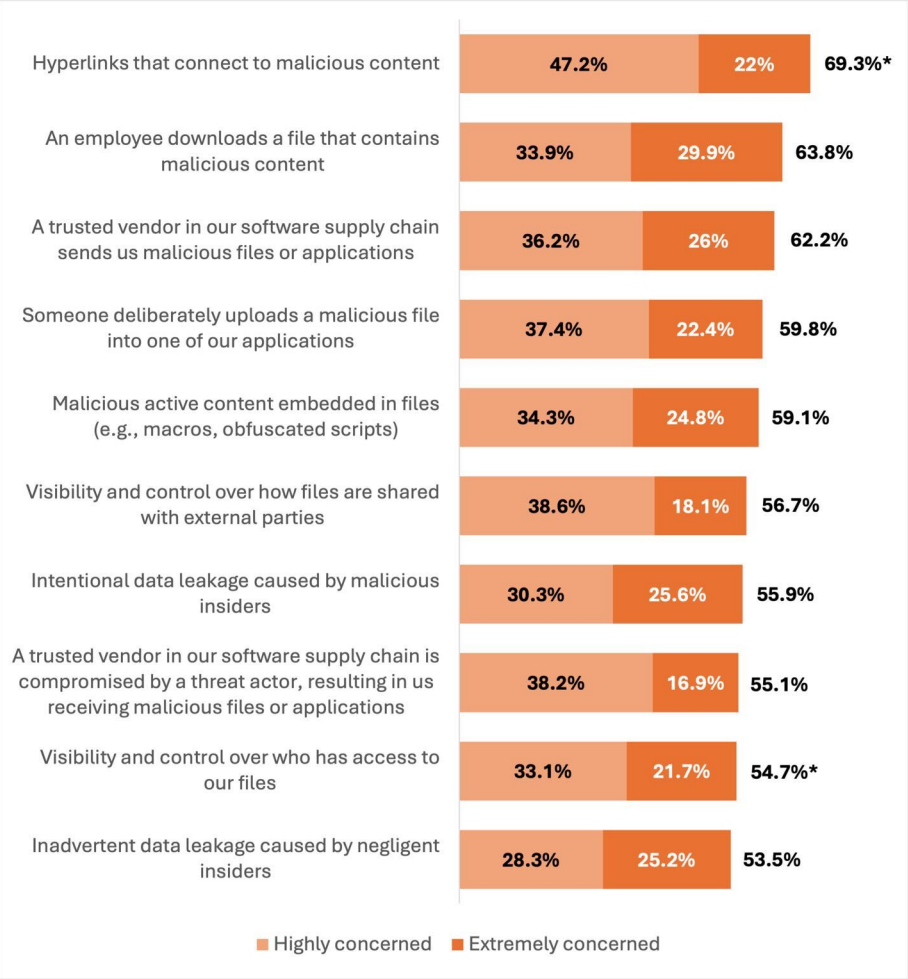
Files entering an organization carry a much higher risk than those originating within the organization.

RISKY ACTIONS AND ACTIVITIES UNDERMINE AN ORGANIZATION'S FILE SECURITY STRATEGY

The respondents in this research are most concerned about undetected and unsanitized malicious content being downloaded, received, or processed within their organization. High concern for this overall risk is seen across a variety of risky actions and activities, e.g., hyperlinks that connect to malicious content, employees who download a file that contains malicious content, and trusted vendors sending malicious files or applications into the organization. See Figure 3.

Extreme levels of concern are highest for direct actions by employees—downloading files with malicious content (29.9%), intentionally leaking data (25.6%), and inadvertently leaking data (25.2%). Employees have authorized access to critical business applications and sensitive data. Without a suitable file security strategy that addresses the risk of employee actions—malicious or otherwise—organizations find themselves both at risk from within and threat from without.

Figure 3
Concern about risks to file security strategy
Percentage of respondents (and sum of the two concern statements)



Source: Osterman Research (2026)
** sum does not match due to rounding of the two underlying numbers*

The risk of downloading, receiving, or processing undetected and unsanitized malicious content is of highest concern in this research.

CONSEQUENCES OF A DATA BREACH OR SECURITY INCIDENT HAVE IMMEDIATE AND LONG-TERM EFFECTS

Concerns about data breaches and security incidents due to unauthorized access to sensitive and confidential data in files are highest when customer data is lost, ransomware prevents access to files, or intellectual property and trade secrets are compromised.

See Figure 4.

Figure 4
Concern about consequences of a data breach or security incident
Percentage of respondents (and sum of the two concern statements)



Source: Osterman Research (2026)
** sum does not match due to rounding of the two underlying numbers*

Consequences of a data breach or security incident have both immediate and long-term effects for organizations—immediate effects when customers act against organizations that fail to secure their data or ransomware hampers operations, and long-term effects when intellectual property and trade secrets fall into the wrong hands and undermine future strategic positioning.

The highest concern of a data breach or security incident is the loss—of customer data, access to files, and intellectual property.

From detection-first to prevention-first

Detection has been the dominant approach for neutralizing threats for decades. Does it still work given the modern and emerging threat landscape?

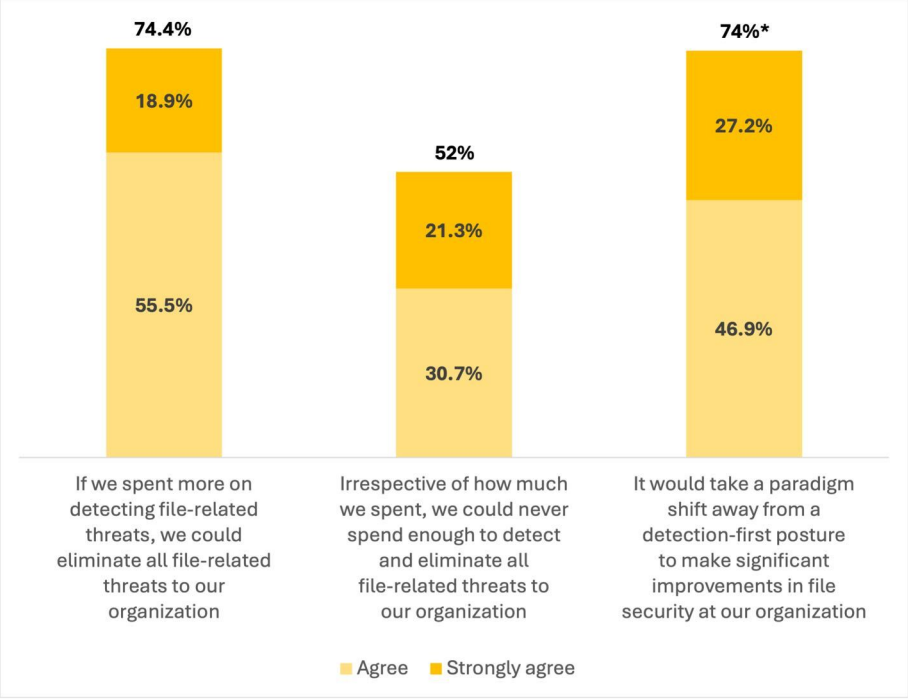
DETECTION-FIRST POSTURE: CRACKS IN THE FOUNDATION

A detection-first posture to file-related threats is the belief that cybersecurity solutions should be designed to detect the presence of cyber threats in files, e.g., malicious content and damaging components. By implication, measuring the efficacy of different detection-first products is done by comparing the difference in detection rates and mitigation actions. Surprisingly, the majority of respondents in this research agree or strongly agree with two opposing perspectives that they rated independently: that eliminating all file-related threats is merely about spending more to detect all threats and that a paradigm-shift away from a detection-first posture would be required to make significant improvements in file security. In the aggregate, this stance doesn't make sense.

To resolve the apparent contradiction, the change in the "strongly agree" rating across the statements in Figure 5 below offers the key. The highest rating is for the need of a paradigm shift away from a detection-first posture (27.2%), followed by the realization that an organization can never spend enough under a detection-first posture to eliminate all file-related threats (21.3%). In last place is the idea that a detection-first posture has ongoing validity (18.9%). See Figure 5.

While a detection-first approach is deeply entrenched, support for a new paradigm is significant.

Figure 5
The dynamics of a detection-first paradigm for file security
Percentage of respondents (and sum of the two agree statements)



Source: Osterman Research (2026)
** sum does not match due to rounding of the two underlying numbers*

EMERGING AI-DRIVEN THREATS ARE CHANGING THE DYNAMICS OF CYBER RISK

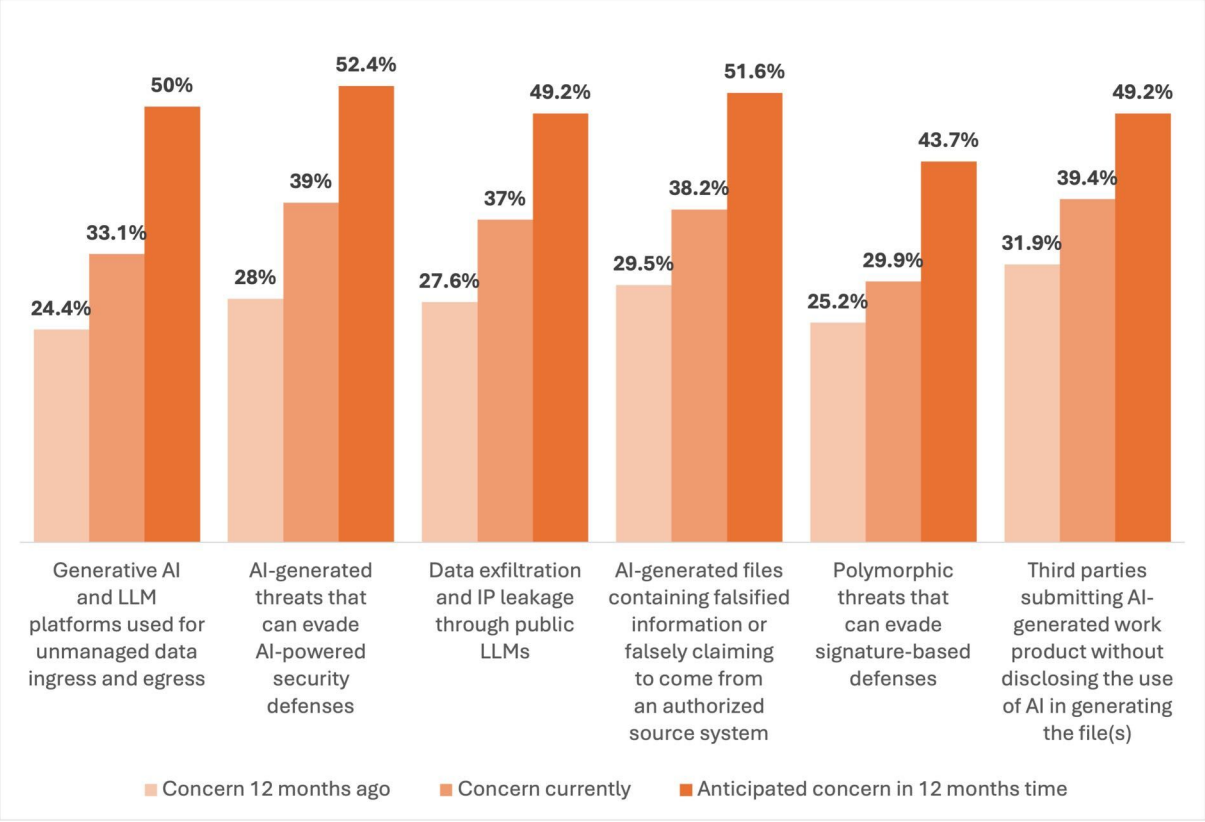
The urgent need for the paradigm shift to prevention-first is amplified by what's happening on the AI threat side. Concern about AI-driven threats to files are growing rapidly—from an average across the six threat types of 27.8% of respondents with high or extreme concern 12 months ago to an average of 49.3% with an anticipation of high or extreme concern in 12 months. That's an average increase of 78.9% from 12 months ago to anticipated concern in 12 months. See Figure 6.

Average concern about emerging AI-driven threats to files increases by 78.9% over the three time periods we asked about.

AI-driven threats to files that evidence the highest increase in concern are:

- **Unmanaged data ingress and egress via generative AI and LLMs (105% increase)**
  When new AI services ignore data governance policies for data entering and leaving the organization, therefore creating data risk and exposure.
- **AI-generated threats that can evade AI-powered security defenses (87% increase)**
  When threat actors use AI to create threats with advanced capabilities to bypass the AI-powered security defenses implemented by organizations.
- **Data exfiltration and IP leakage through public LLMs (79% increase)**
  When employees unintentionally or unwittingly share corporate data with a public LLM to accomplish a task (e.g., summarize, find related data, fact check), failing to recognize the sensitive nature of the data they have exposed.

Figure 6
Concern about AI-driven threats on cybersecurity defenses and file security over three time periods
Percentage of respondents indicating "highly concerned" or "extremely concerned"



Source: Osterman Research (2026)

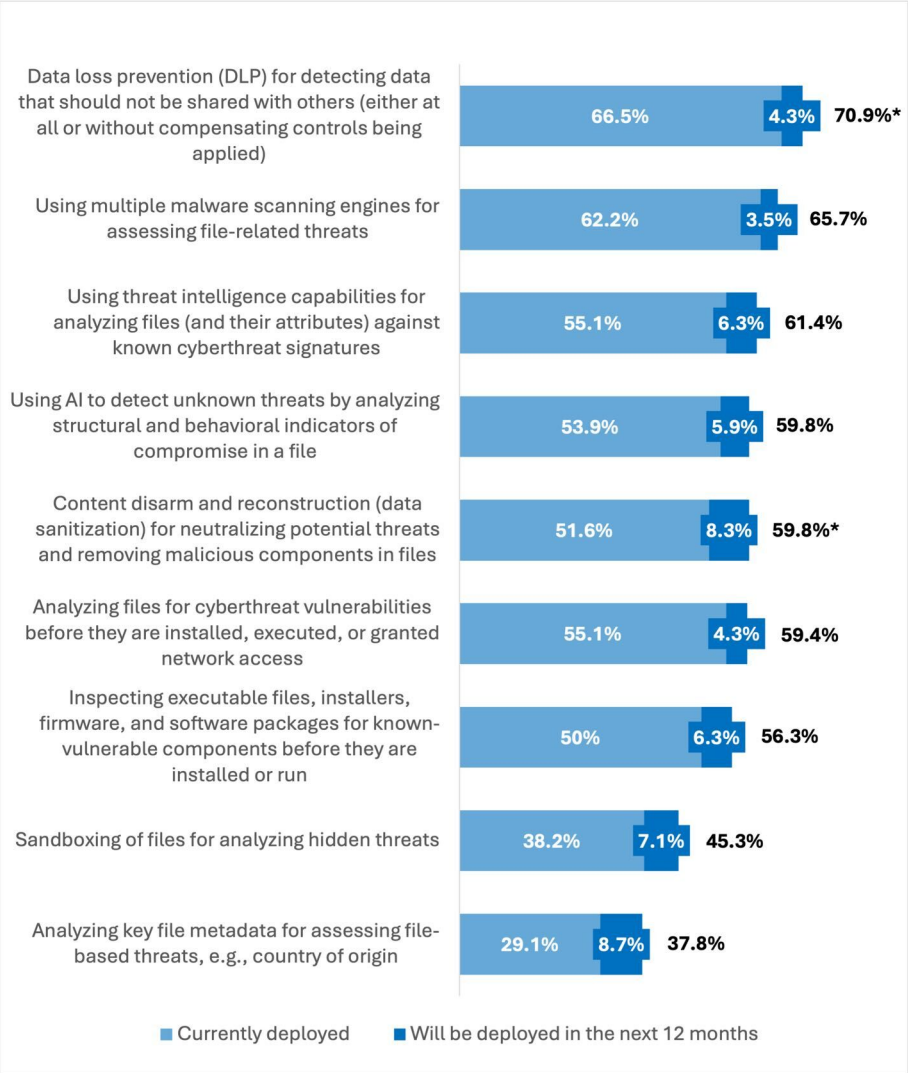
Current security posture for files

How are organizations currently securing files? In this section, we look at the technologies being used, along with what is and isn't working.

TECHNOLOGIES USED FOR SECURING FILES—CURRENT AND OUTLOOK

Data loss prevention (DLP) and the use of multiple malware scanning engines are the most used technologies for securing files currently. These also have the highest overall deployment expectation once deployment plans for the upcoming 12 months are factored in. The two technologies with the highest intent to deploy are analyzing key file metadata for assessing file-based threats (8.7%) and content disarm and reconstruction (8.3%). Content disarm and reconstruction is one of the key technologies for organizations embracing a paradigm shift away from a detection-first posture. See Figure 7.

Figure 7
Technologies used for securing files – current and 12-month outlook
Percentage of respondents (and sum of the two deployment statements)



Source: Osterman Research (2026)
** sum does not match due to rounding of the two underlying numbers*

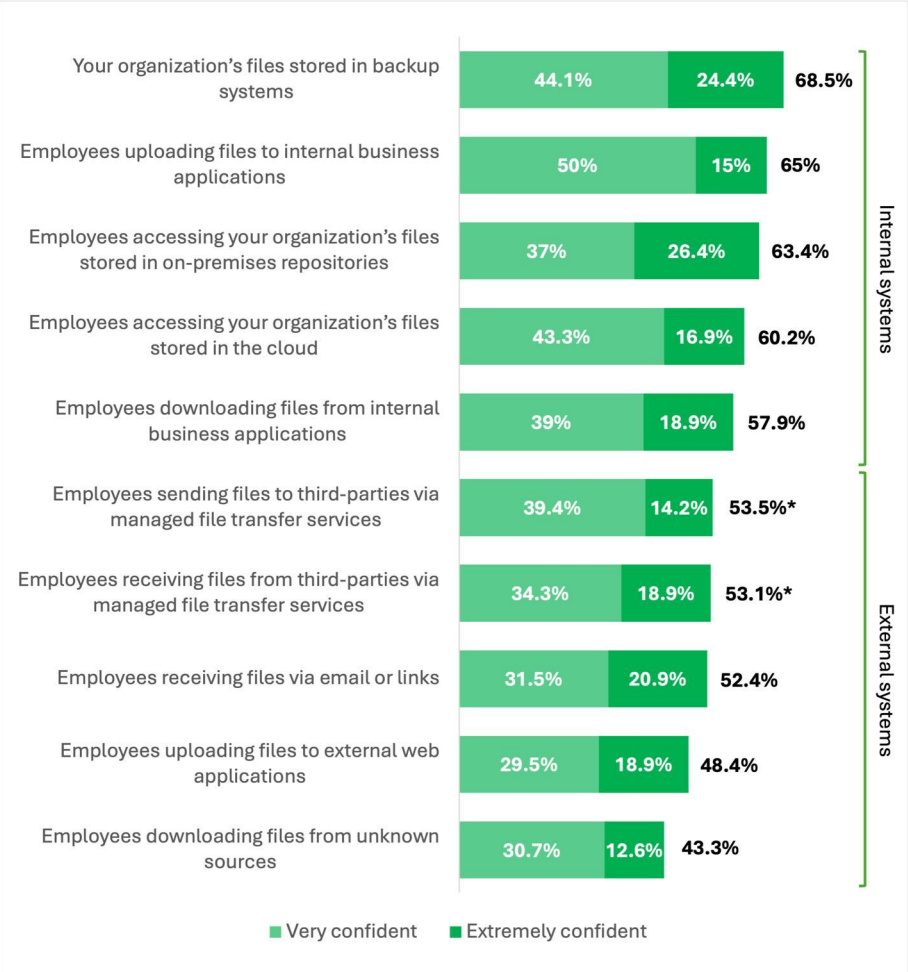
Organizations are making high use of detection-first technologies and plan on increasing usage of prevention-first options.

CURRENT TECHNOLOGIES AREN'T ASSURING CONFIDENCE IN PROTECTING FILES FROM MALWARE AND OTHER FILE-RELATED THREATS

The respondents in this research have the highest confidence that they can protect files from malware and other file-related threats across variants of internally managed systems over which the organization has a high degree of control. The average level of confidence (very or extremely confident) across the five internal systems in Figure 8 below is 63%. The average for files that cross organizational boundaries—inwards or outwards—is lower at 50.2%. In principle, this differential makes sense given the different control dynamics. See Figure 8.

From the perspective of overall confidence level, however, it is concerning that across all 10 approaches in Figure 8, respondents' average level of confidence (very or extremely confident) in their ability to prevent compromise to their files due to malware and other file-related threats is only 56.6%. In aggregate, that means almost half of respondents are not confident in their ability to protect against long-running types of threats.

Figure 8
Confidence to prevent malware and other file-related threats
Percentage of respondents (and sum of the two confidence statements)



Source: Osterman Research (2026)
** sum does not match due to rounding of the two underlying numbers*

Almost half of respondents are not confident in their ability to protect against long-running types of threats against files.

ORGANIZATIONS WITH A PREVENTION-FIRST MINDSET AND APPROACH HAVE HIGHER CONFIDENCE LEVELS

To test the impact of a prevention-first mindset and approach on confidence levels to prevent malware and other file-related threats, we split the respondents into two groups:

- **Group one**. Respondents who give evidence of a prevention-first mindset and approach. Specifically, we looked for respondents that met two tests: they agreed on the need for a paradigm shift to file security, and they are currently using content disarm and reconstruction. This netted 102 respondents (40.2% of respondents in this research).
- **Group two**. All other respondents in the research—152 (59.8%)—who do not meet the above two tests and therefore do not give evidence of a prevention-first mindset and approach.

When the confidence data from Figure 8 above is correlated by whether the organization evidences a prevention-first mindset and approach (group one) or not (group two), average confidence levels at both the very confident and extremely confident levels are higher for group one than group two. See Figure 9 on the next page.

Organizations embracing a prevention-first strategy are more likely to be extremely confident that they can prevent malware and other file-related threats.

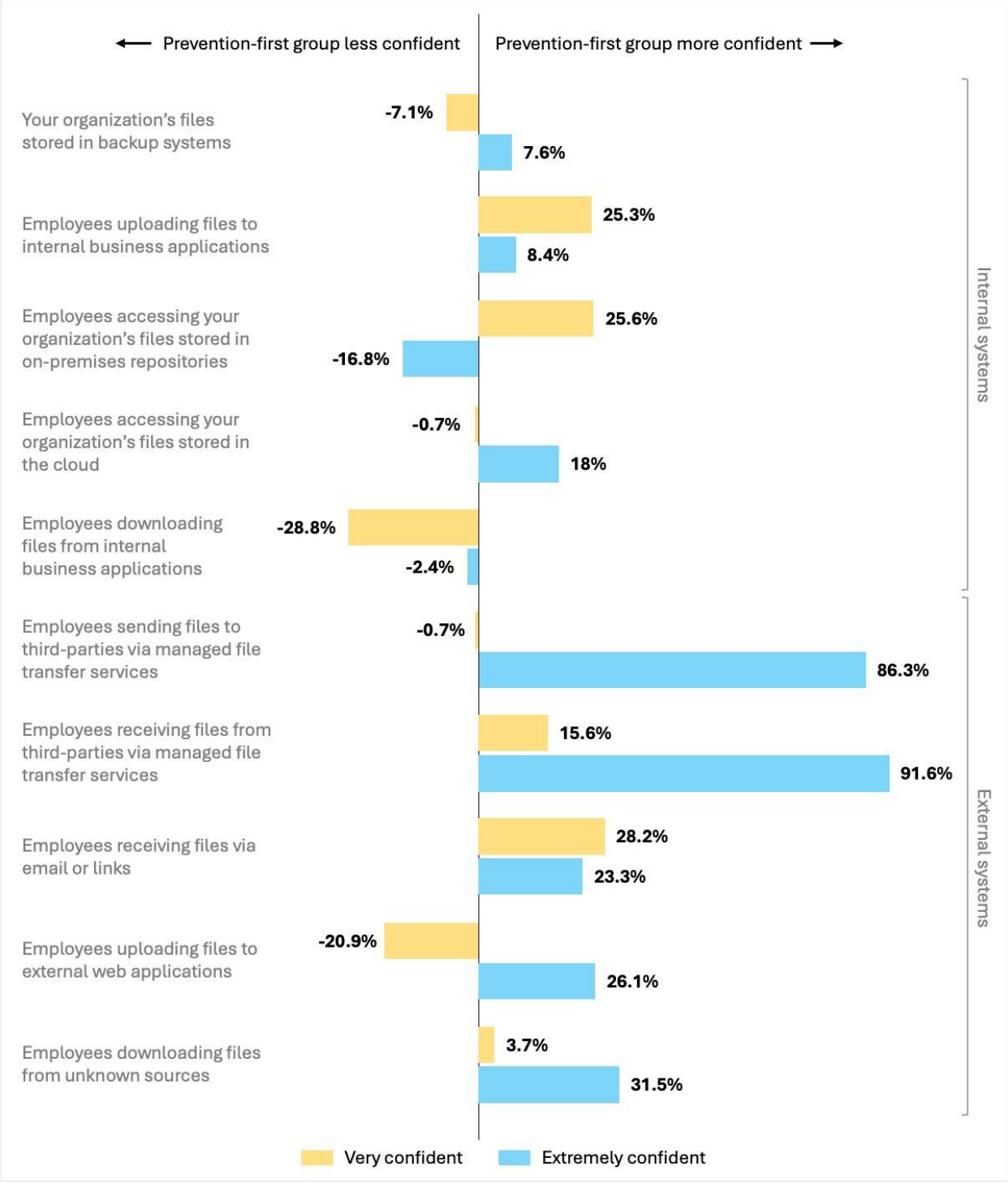
Across the 10 situations where employees send or receive files, the data says:

- In 8 of the 10 situations, organizations with a prevention-first mindset and approach (group one) exhibit higher levels of extreme confidence that they can prevent malware and other file-related threats versus everyone else (group two).
- The variation at the extremely confident level for group one is particularly noticeable for the approaches that cross organizational boundaries, e.g., receiving files from third parties via managed file transfer services (91.6% higher confidence at the extremely confident level).
- In 2 of the 10 situations, the group one organizations have lower levels of confidence at the extremely confident level compared to group two—this is shown as -16.8% for employees accessing files stored in on-premises repositories, and -2.4% for employees downloading files from internal business applications. The negative numbers mean that the organizations in group two said their confidence was higher. Both situations are for internal systems under the direct control of the organization, and hence where other file security approaches are active and the impact of content disarm and reconstruction is less noticeable (by design).
- There is less of a differential between the confidence rates of the two groups for internal systems under the direct control of the organization, likely because other file security approaches are active. The highest percentage variation for internal systems at either the very confident or extremely confident level is 28.8% (negative), while the highest percentage variation for the external systems is 91.6%.

Overall, while a prevention-first mindset and approach does not give evidence of an uplift in confidence across all 10 situations, the dominant pattern by far is that the level of extreme confidence is higher for group one, and that this effect is particularly noticeable for systems that cross organizational boundaries.

See Figure 9.

Figure 9
Confidence to prevent malware and other file-related threats: Prevention-first mindset and approach (group one) versus everyone else (group two)
Percentage improvement due to a prevention-first mindset and approach

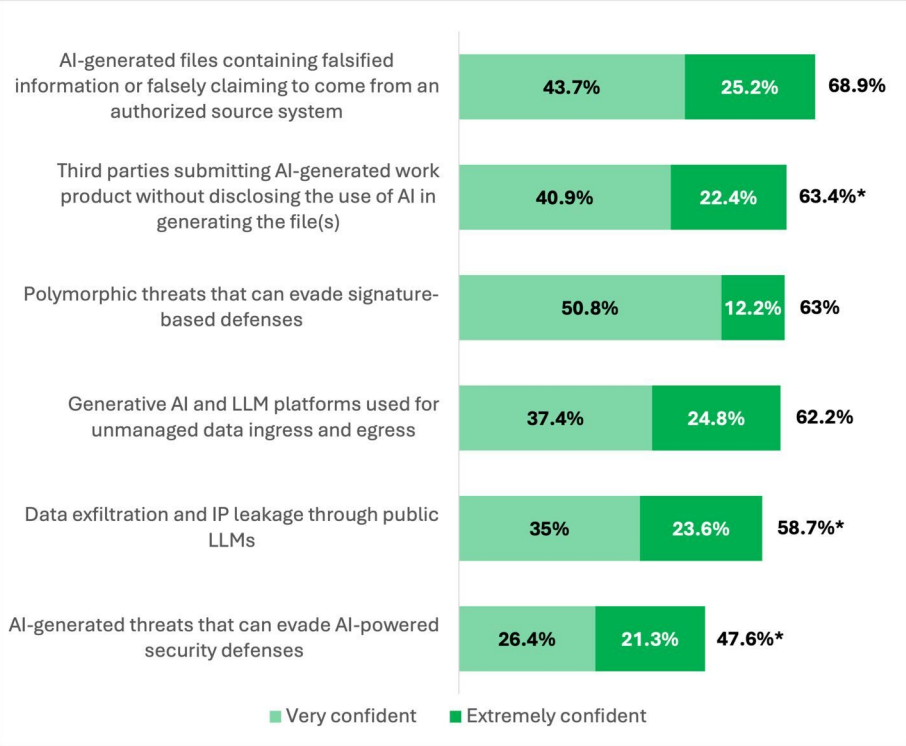


Source: Osterman Research (2026)

CURRENT TECHNOLOGIES AREN'T ASSURING CONFIDENCE IN PROTECTING FILES FROM EMERGING THREATS

Given the technologies for file security that organizations are currently using, an average of only 60.6% of respondents indicate high confidence in their ability to detect and prevent emerging types of threats to files. Out of all respondents, only 21.6% say they have the highest level of confidence. See Figure 10.

Figure 10
Confidence to detect and prevent emerging threats to files
Percentage of respondents (and sum of the two confidence statements)



Source: Osterman Research (2026)
** sum does not match due to rounding of the two underlying numbers*

Only 21.6% of respondents have the highest confidence that they can detect and prevent a range of emerging threats to files.

The confidence portrayed in Figure 10 is perplexing for two reasons:

- Average confidence for protecting files from new and emerging threats (Figure 10) is higher than average confidence for protecting files from long-running threat types such as malware (see Figure 8). In principle, confidence for long-running threat types should be higher, because organizations have more experience in defending against incidents and attacks over multiple waves and changes in their defensive posture.
- The lowest result for the extremely confident rating in Figure 10 is polymorphic threats that can evade signature-based defenses (12.2%). This is the longest-running threat type of the six emerging threats and yet has the lowest level of extreme confidence. In principle, confidence levels to detect and prevent this threat type should set the high mark for the other types.

Whether the confidence levels shown in Figure 10 are based on pre-sales vendor hype or post-sales incident data will be tested over the coming 12–24 months.

©2026 Osterman Research

ORGANIZATIONAL PRACTICES FOR FILE SECURITY ARE MUCH LESS MATURE THAN WHAT RESPONDENTS BELIEVE

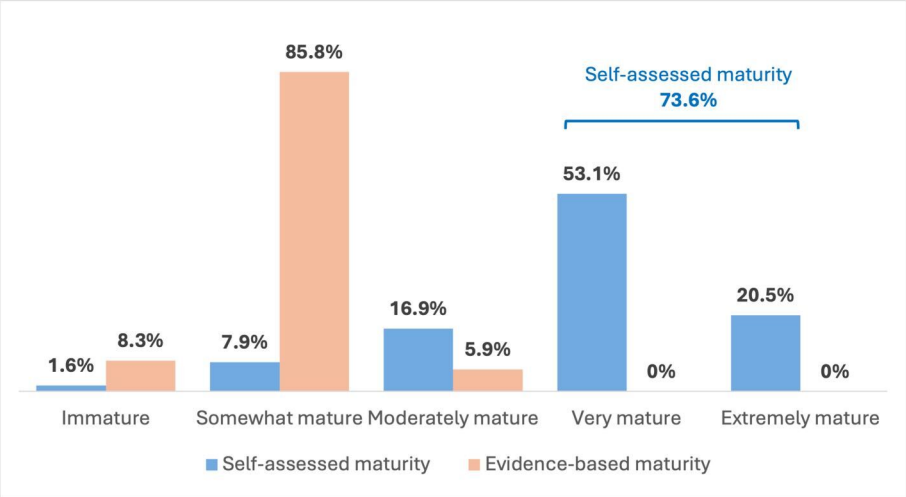
73.6% of respondents self-assess that their file security posture, after taking into consideration everything they are doing to address the threats against files in their organization, is very or extremely mature. Maturity in this case means an assessment of how well the organization is positioned to respond to threats against files, encompassing their use of technology, their approach to training and readiness of people, and the efficacy of their security processes. See Figure 11.

To test the accuracy of this self-assessment, we correlated the data given by each respondent across the survey to create an evidence-based maturity model, with data analyzed from multiple perspectives. We combined the analysis from each perspective to derive an aggregated maturity rating for each organization. In looking at the variations between claimed and evidenced maturity, the data says:

- Only 2% of organizations evidence the same level of maturity that they claim. A further 3.5% of organizations evidence a higher level of maturity than what they claim. In combination, a mere 5.5% evidence the same or higher level of maturity than what they claim.
- The majority—by a long way—over-assess their maturity compared to the evidence of their actual file security posture (94.5%). Their claim of maturity is undermined by their actual approach.
- Across all respondents, the weight of evidence shows that actual maturity is significantly lower than claimed maturity. Most organizations are only "somewhat mature" (85.8%) given how they actually approach file security. See Figure 11.

94.5% of organizations assess their maturity with file security at a higher level than the evidence allows.

Figure 11
Maturity of file security strategy and approach: self-assessed maturity versus evidence-based maturity
Percentage of respondents

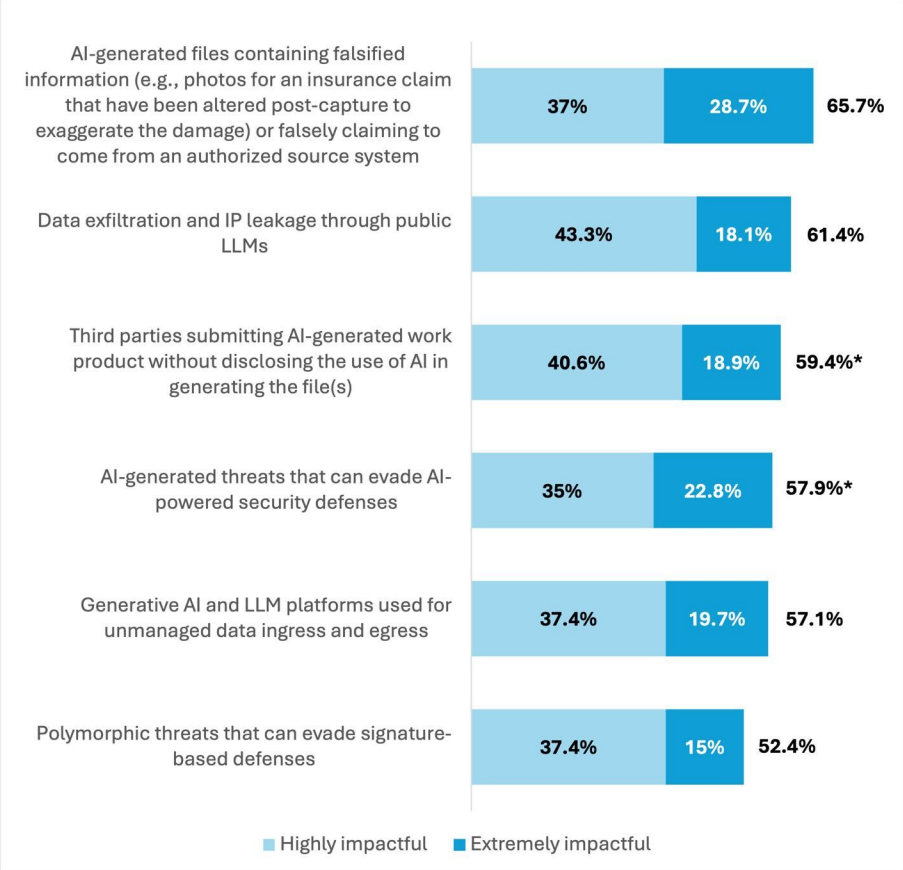


Source: Osterman Research (2026)

EMERGING THREAT TRENDS ANTICIPATED TO INCREASE TIME ON FILE SECURITY ACTIVITIES

An average of 59% of respondents say that a group of emerging threat trends will be highly or extremely impactful on the time taken by IT and security teams to deal with file security activities over the next 12 months. The two trends anticipated to have the highest impact are falsified AI-generated files and data exfiltration, along with IP leakage through public LLMs. See Figure 12.

Figure 12
Anticipated impact of emerging threat trends on time taken to deal with file security activities
Percentage of respondents (and sum of the two impact statements)



Source: Osterman Research (2026)
** sum does not match due to rounding of the two underlying numbers*

IT and security teams already spend 42.5% of their time dealing with file-related security issues, and 63% of respondents expect this time to increase.

The data from this research says:

- IT and security teams already spend an average of 42.5% of their time in dealing with file-related security activities.
- 63% of respondents expect IT and security teams to spend more time on file-related security activities over the next 12 months, and a further 22.4% expect the time spent to remain the same. Only 14.6% anticipated time to decline.

©2026 Osterman Research

Exploring gaps in file security

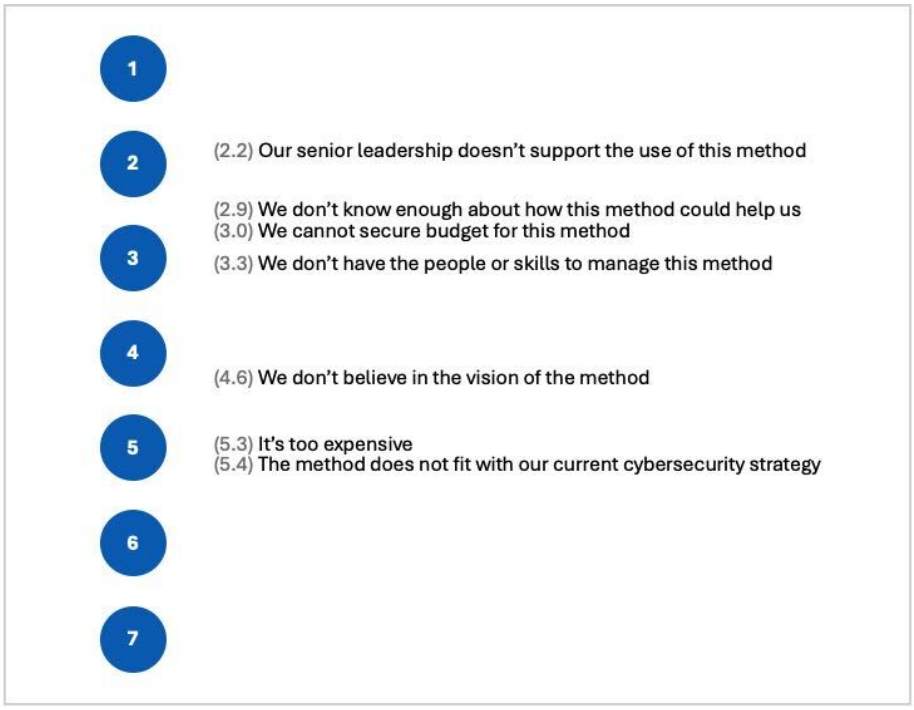
What's driving the gap in file security posture for organizations—and what does the gap cost in terms of data breaches and cybersecurity incidents?

REASONS WHY ORGANIZATIONS ARE NOT USING FILE SECURITY SOLUTIONS – LACK OF KNOWLEDGE IS KEY

An average of 42.6% of respondents indicated their organization has no current plans to use one or more of the nine file security solutions we queried in the survey. We asked respondents to rate the importance of seven different reasons why they were not currently using each of these solutions.

Figure 13 lists the average ranking of the seven reasons across the nine file security solution types, with the most important reason at the top of the list being that senior leadership doesn't support the use of the solution. Second place is where respondents don't know enough about how the solution could help their organization. The least important reason is that the solution doesn't fit with their organization's current cybersecurity strategy.

Figure 13
Reasons why file security solutions are not used–aggregated order
Average position in the list of reasons – from most (1st) to least important (7th)



Source: Osterman Research (2026)

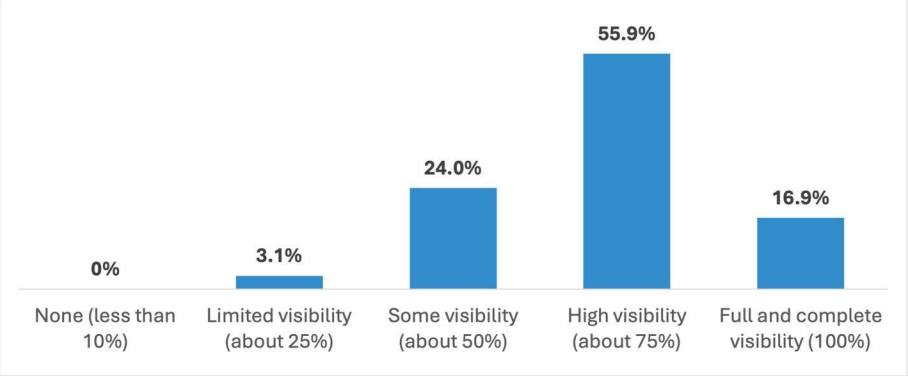
New file security solutions aren't used due to lack of leadership support and poor knowledge – human factors, not technical ones.

The takeaway for decision-makers is that addressing the lack of knowledge on any given solution presents the most actionable approach for changing the importance of the other reasons. Leadership support (first place) and hence budget (third place) and the availability of people (fourth place) cannot go where knowledge has not already been.

VISIBILITY ACROSS THE FILE LIFECYCLE AND VARIOUS ENVIRONMENTS IS LACKING

Visibility into the lifecycle of files across an organization, including the identification and resolution of any security issues, is lacking for most respondents. Only 16.9% claim full and complete visibility, with the most common option being high visibility of about 75% (at 55.9% of organizations). That means over half of organizations know they can't see about 25% of what happens across the lifecycle of their files, including any security issues. See Figure 14.

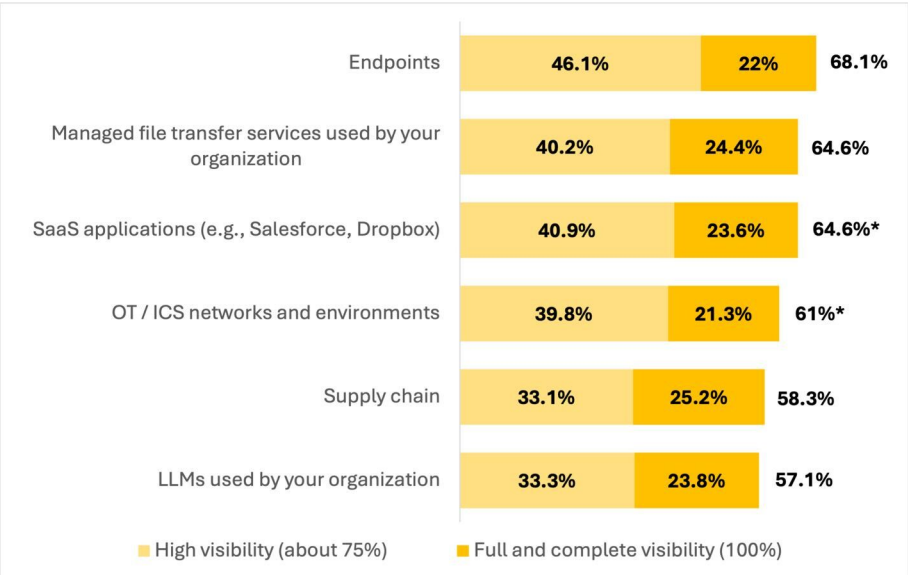
Figure 14
Visibility into the lifecycle of files
Percentage of respondents



Source: Osterman Research (2026)

Visibility is also lacking into file-related threats across various networks, environments, and applications across an organization. On average, only 23.4% of respondents say their organization has full and complete visibility. See Figure 15.

Figure 15
Visibility into file-related threats
Percentage of respondents (and sum of the two visibility levels)



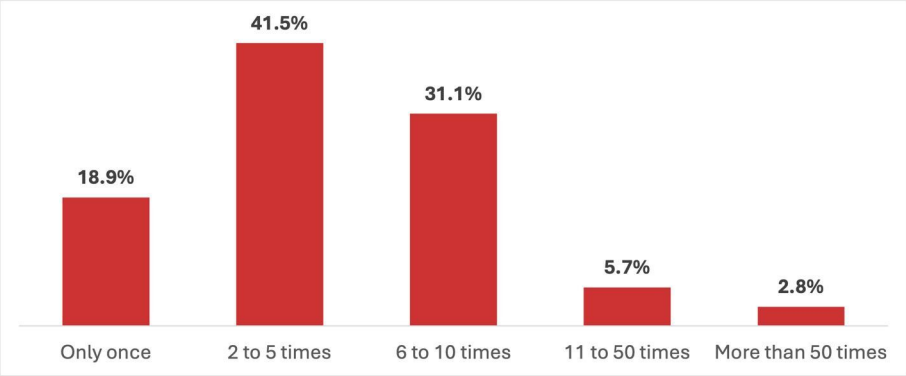
Source: Osterman Research (2026)
** sum does not match due to rounding of the two underlying numbers*

Over half of organizations know they can't see about 25% of what happens across the lifecycle of their files, including any security issues.

MANY ORGANIZATIONS HAD FILES COMPROMISED BY A DATA BREACH OR CYBERSECURITY INCIDENT

41.7% of respondents said their organization suffered a data breach or cybersecurity incident during the past two years where sensitive or confidential data in files was accessed by someone without authorization (e.g., due to negligence or malicious intent by an employee, an external actor, or an AI agent or process). These organizations experienced an average of 8 data breaches or cybersecurity incidents over the past two years. See Figure 16.

Figure 16
Frequency of data breach or cybersecurity incidents over the past two years
Percentage of respondents who acknowledged suffering a data breach or incident

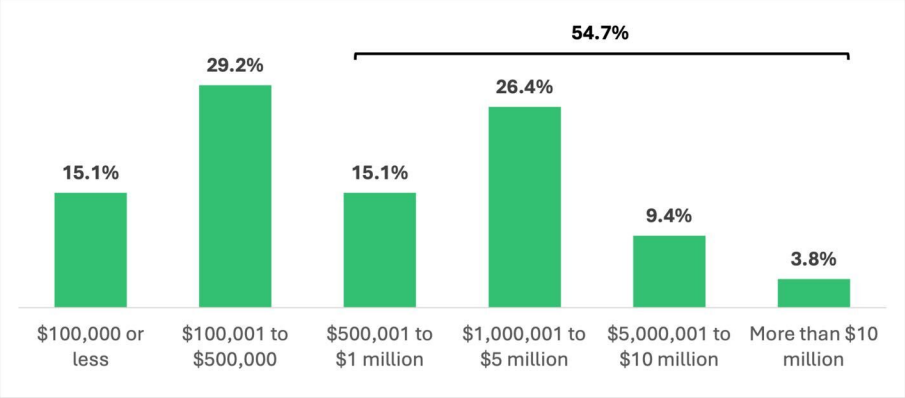


Source: Osterman Research (2026)

58.3% of respondents report their organization did not suffer a data breach or cybersecurity incident over the past two years. In looking at the data, 83% of these respondents lack full visibility into the lifecycle of files across their organization, including security incidents. By implication, the percentage of organizations experiencing a data breach or cybersecurity incident is underrepresented, because without full and complete visibility, there's no way of ruling out such incidents.

The overall average cost of these incidents is $2.2 million for the organizations in this research. Over half experienced costs of more than $500,000. See Figure 17.

Figure 17
Total cost of data breach or cybersecurity incidents over the past two years
Percentage of respondents who acknowledged suffering a data breach or incident



Source: Osterman Research (2026)

41.7% of respondents said their organization suffered a file-related data breach or cybersecurity incident over the past two years – and most of those claiming no incidents lack the data to rule it out.

Roadmap for improving file security

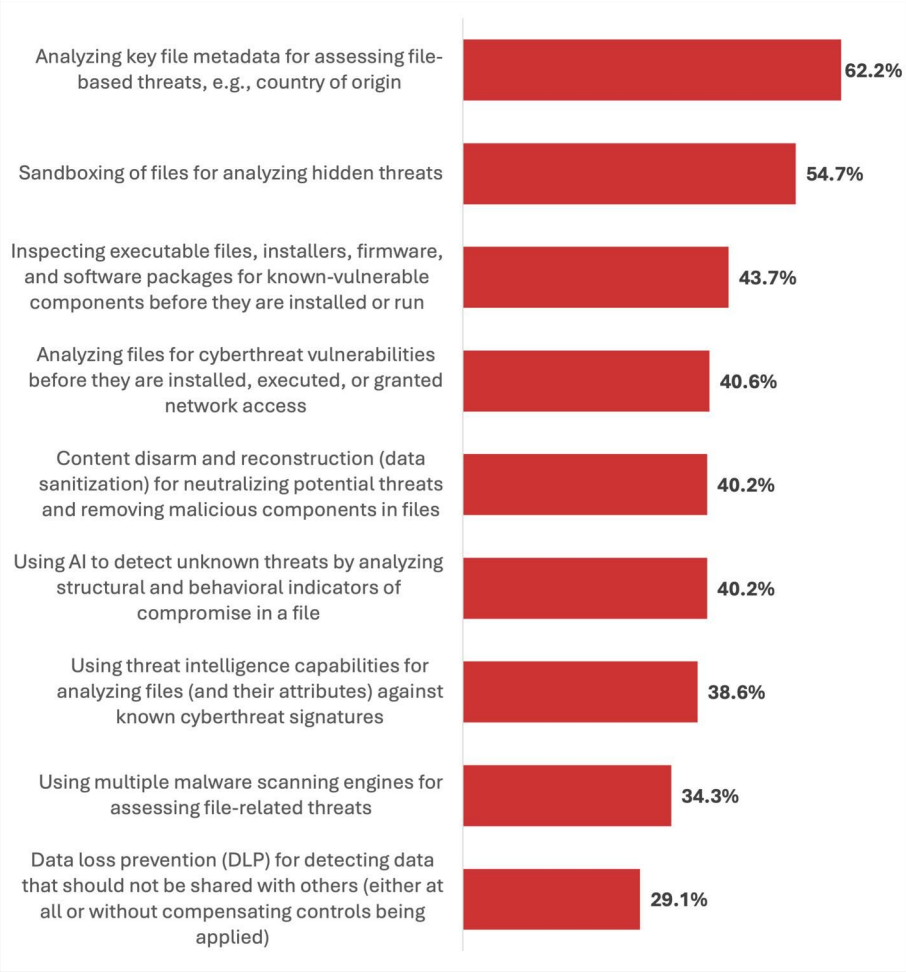
What do organizations need to do to improve file security to adapt to the changing threat environment exposed in this investigation?

INVESTIGATE THE FILE SECURITY SOLUTIONS NOT YET DEPLOYED

This research has investigated how organizations are dealing with current and emerging cyber threats against their files, and in particular the solutions that make up their cybersecurity posture for files. The data says that, on average, 51.3% of organizations are already using the file security solutions we asked about, and a further 6.1% will do so within the next 12 months. That leaves an average of 42.6% of organizations not using file security solutions that are designed to strengthen prevention activities, increase detection efficacy, and stop current and emerging threats from leading to data breaches and cybersecurity incidents.

See Figure 18.

Figure 18
File security solutions that are not currently deployed or planned for deployment in the next 12 months
Percentage of respondents



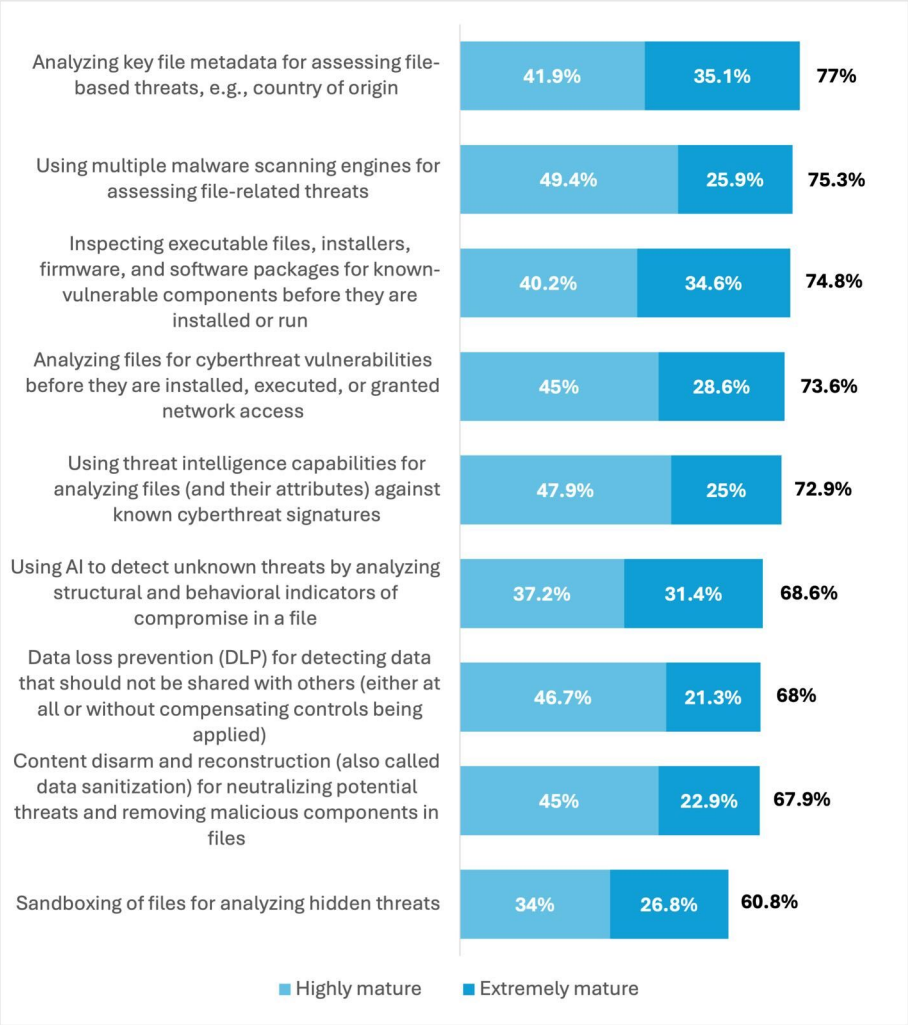
Source: Osterman Research (2026)

New file security solutions strengthen prevention, increase detection efficacy, and stop current and emerging threats from leading to data breaches and cybersecurity incidents.

IMPROVE THE MATURITY OF FILE SECURITY SOLUTION DEPLOYMENTS

On average, only 28% of respondents using the file security solutions we asked about in this research say their deployment has reached the highest level of maturity. At the extremely mature level, the lowest results are for DLP (21.3%) and content disarm and reconstruction (22.9%)—key file security solutions for stopping data breaches, cybersecurity incidents, and embracing a prevention-first approach. Deploying file security solutions is only the first step; driving towards higher levels of maturity in the deployment is the essential second step. See Figure 19.

Figure 19
Maturity of deployment of file security solutions
Percentage of respondents using a file security solution (and sum of the two maturity statements)



Source: Osterman Research (2026)

Key action point: Drive towards higher levels of maturity in the deployment of file security solutions.

STRENGTHEN SECURITY POSTURE AGAINST EMERGING THREAT TYPES

Respondents indicate a doubling of the priority at their organization for strengthening their security posture to address emerging threat types, with new AI-driven threats high on the list. The emerging threat types shown in Figure 20 will increasingly affect all organizations with greater intensity, driving costly data breaches and cybersecurity incidents that undermine customer trust dynamics and damage organizational data.

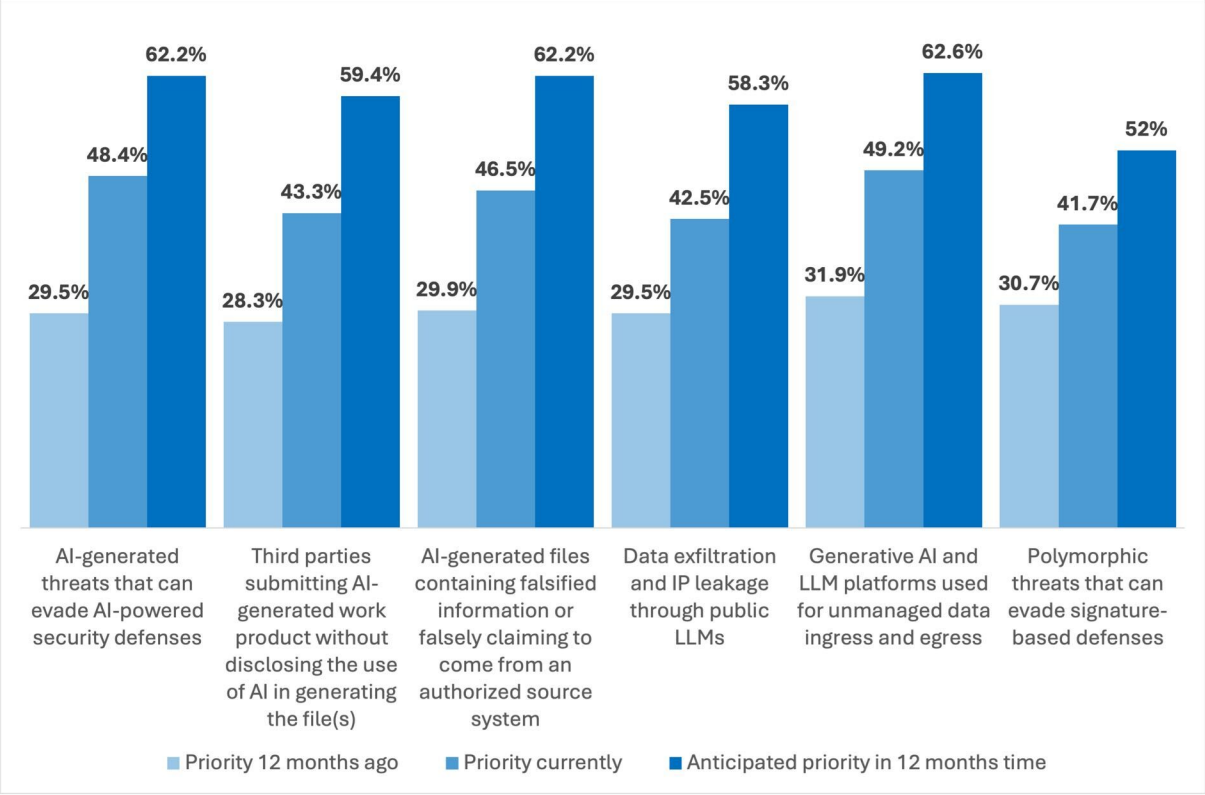
For the organizations in this research, the data (see Figure 20) says the highest increase in priority is to address:

- AI-generated threats that can evade AI-powered security defenses (111% growth in priority from 12 months ago to anticipated priority in 12 months).
- Undisclosed AI in work product submitted by third parties (110%). Doing so could have contractual implications.
- AI-generated files containing falsified information or falsified provenance signals (108%).

Organizations with sufficiently mature deployments of file security solutions against these specific threats may not need to place as high a priority on addressing them. However, as threat dynamics change over the next 12 months, relative solution efficacy may decline.

Emerging threat types will increasingly affect all organizations, driving data breaches and cybersecurity incidents.

Figure 20
Priority on improving security posture due to emerging threat types over three time periods
Percentage of respondents indicating “high priority” or “extreme priority”



Source: Osterman Research (2026)

DRIVE ELEVATED MATURITY IN APPLYING AND ENFORCING CONSISTENT FILE SECURITY POLICIES ACROSS CHANNELS

Inconsistent file security policies across the channels employees regularly use results in threats against files slipping through unnoticed. The average at the extremely mature level across the nine channels is 26.5%. See Figure 21.

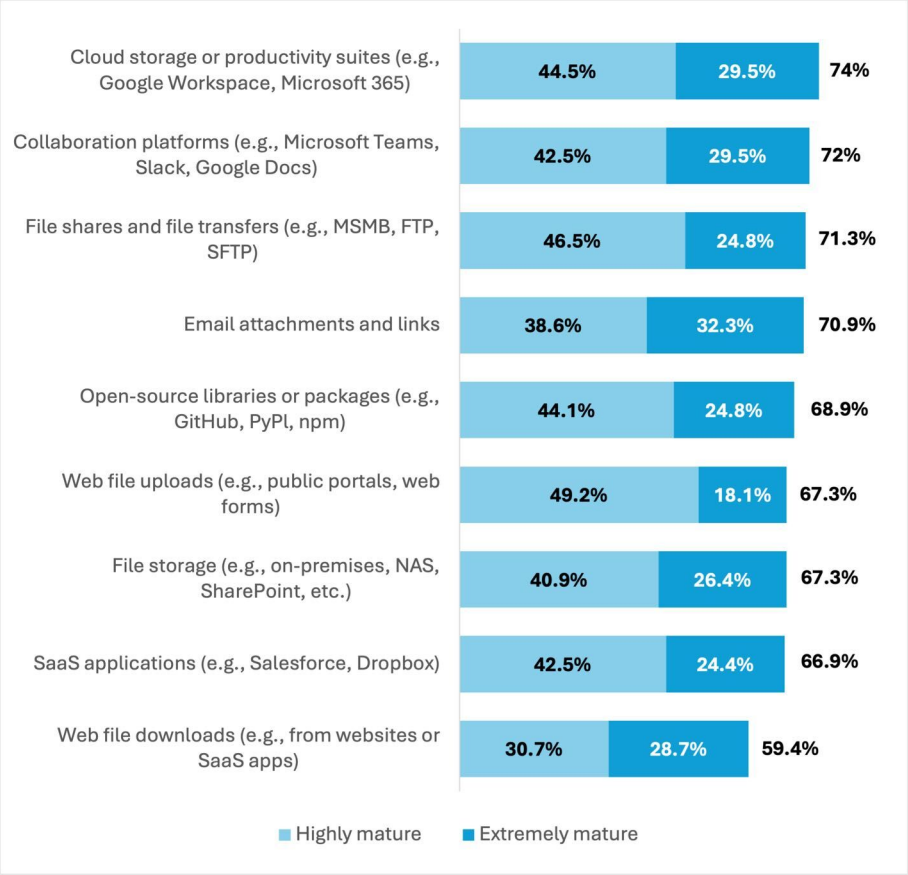
The channel with the highest level of maturity in applying and enforcing consistent file security policies for the organizations in this research is email (covering attachments and links), at only 32.3%. While this is the highest result, it is low for a channel so frequently used by employees for work processes and threat actors for unleashing cyberattacks. You will recall from Figure 2 that employees receiving files via email or links was the second highest risk.

Organizations seeking stronger protections against existing and emerging cyber threats which compromise files will need to:

- Implement new file security solutions where they are missing;
- Drive elevated deployment maturity where they are already deployed; and
- Invest in either a centralized policy hub or a policy orchestration engine that works across the channels used within the organization.

Key action point: Apply and enforce consistent file security policies across all the channels employees use in carrying out their work.

Figure 21
Maturity of applying and enforcing consistent file security policies across channels
Percentage of respondents (and sum of the two maturity statements)



Source: Osterman Research (2026)

Conclusion

Files are already under increasing attack and new emerging threat types—particularly those that leverage rapidly-advancing offensive AI capabilities—are amplifying the risk of costly data breaches and cybersecurity incidents. Most organizations are under-prepared for the coming wave of attacks, and far too many lack confidence that their current security posture is up to the task. The data in this research demands an urgent re-evaluation of how files are secured, one that more than merely seeks to detect current and emerging threats better than yesterday. An investigation into the benefits of investing in prevention-first approaches should be high on the priority list for cybersecurity decision-makers.

> ***The data in this research demands an urgent re-evaluation of how files are secured.***

About OPSWAT

Since 2002, OPSWAT has protected the world's critical infrastructure by preventing known, unknown, and AI-generated threats before they disrupt operations. The MetaDefender™ Platform is OPSWAT's AI-powered cybersecurity platform for IT, OT, and cross-domain environments, securing files, devices, and data transfers across cloud, on-premises, and air-gapped environments. By combining AI, machine learning, advanced threat prevention, and purpose-built hardware, OPSWAT protects critical operations through file security, peripheral media protection, managed file transfer, optical firewall technology, data diodes, and specialized training. Trusted worldwide, OPSWAT safeguards the systems modern society depends on.

Learn more at www.opswat.com.

OPSWAT.

www.opswat.com

@OPSWAT

Methodology

This research report was commissioned by OPSWAT and conducted by Osterman Research. Osterman Research surveyed 254 organizations in the United States during July 2026. Organizations were randomly selected to participate. To qualify, respondents had to work at organizations with at least 100 employees and work in one of eight designated roles. Respondents were required to have responsibility (themselves or their direct team) for four aspects of file security at their organization. The survey was cross-industry, and no industries were excluded or restricted.

ORGANIZATION SIZE

100 to 999 employees	28.7%
1,000 to 5,000 employees	37.8%
More than 5,000 employees	33.5%

JOB ROLE

IT manager, director, or VP	40.2%
Director of security	12.6%
CIO	13.4%
CISO	10.6%
Director of information security	9.1%
Another role that has security management responsibility	7.5%
Another role that has IT management responsibility	5.1%
AI security architect or senior developer	1.6%

INDUSTRY

Healthcare	11.8%
Hospitality, food or leisure travel	11.8%
Information technology	11.8%
Financial services	10.6%
Industrials (manufacturing, construction, etc.)	10.2%
Retail or ecommerce	9.1%
Transport or logistics	6.3%
Data infrastructure or telecom	5.9%
Computer hardware or computer software	5.5%
Public service or social service	4.7%
Energy or utilities	3.1%
Life sciences or pharmaceuticals	2.8%
Professional services (law, consulting, etc.)	2.8%
Education	2.4%
Media or creative industries	0.8%
Agriculture, forestry, or mining	0.4%

©2026 Osterman Research

© 2026 Osterman Research. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, nor may it be resold or distributed by any entity other than Osterman Research, without prior written authorization of Osterman Research.

Osterman Research does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.