Ponemon INSTITUTE

# The State of File Security

## Sponsored by OPSWAT

Independently conducted by Ponemon Institute LLC

Publication Date: September 2025

Ponemon Institute© Research Report

# The State of File Security
September 2025

## Part 1. Introduction

The purpose of this research is to learn what organizations are doing to achieve an effective file security management program. Sponsored by OPSWAT, Ponemon Institute surveyed 612 IT and IT security practitioners in the United States who are knowledgeable about their organizations' approach to file security.

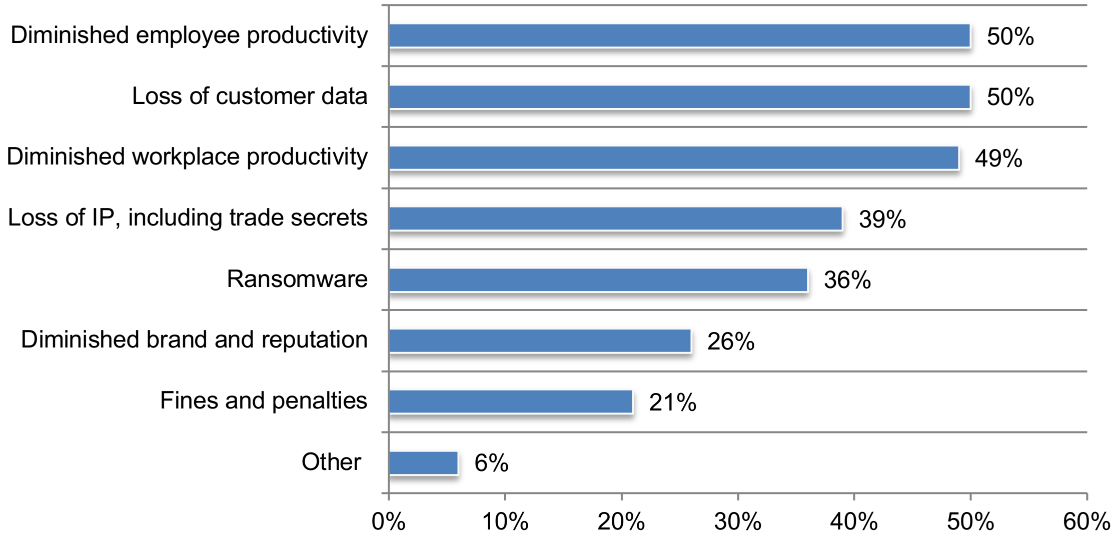
File security refers to the methods and techniques used to protect files and data from unauthorized access, theft, modification or deletion. It involves using various security measures to ensure that only authorized users can access sensitive files and to protect files from security threats. As shown in this research, the most serious risks to file security are data leakage caused by negligent and/or malicious insiders and not having visibility into who is accessing files and being able to control access.

**Attacks on sensitive data in files are frequent and costly and indicate the need to invest in technologies and practices to reduce the threat.** Sixty-one percent of respondents say their organizations have had an average of eight data breaches or security incidents due to unauthorized access to sensitive and confidential data in files in the past two years.

Fifty-four percent of respondents say these breaches and incidents had financial consequences. The average cost of incidents for organizations in the past two years was $2.7 million. Sixty-six percent of respondents say the average cost of all incidents in the past two years was between $500,000 and more than $10,000,000.

According to Figure 1, the bottom line of organizations is impacted by the loss of customer data and diminished employee and workplace productivity. These are the most common consequences from these security incidents.

**Figure 1. The consequences of a data breach or security incident due to unauthorized access to sensitive and confidential data in the past two years.**
More than one response permitted



## Insights into the state of file security

**Insiders pose the greatest threat to file security.** The most serious risk is caused by malicious and negligent insiders who leak data (45 percent of respondents). Other top risks are file access visibility and control (39 percent of respondents) and vendors providing malicious files and/or applications (33 percent of respondents). Only 40 percent of respondents say their organizations can detect and respond to file-based threats within a day (25 percent) or within a week (15 percent).

**Files are most vulnerable when they are shared, uploaded and transferred.** Only 39 percent of respondents are confident that files are secure when transferring files to and from third parties and only 42 percent of respondents are confident that files are secure during the file upload stage. The Open Web Application Security Project (OWASP) released principles on securing file uploads. According to 40 percent of respondents, the principle most often used or will be used is to store files on a different server. Thirty-one percent of respondents say they only allow authorized users to upload files.

The file-based environment that poses the most risk is file storage such as on-premises, NAS and SharePoint, according to 42 percent of respondents. Forty percent of respondents say web file uploads such as public portals and web forms are a security risk.

**Macro-based malware and zero-day or unknown malware are the types of malicious content of greatest concern to file security.** Organizations have encountered these types of malicious content and are most concerned about macro-based malware and zero-day or unknown malware according to 44 percent and 43 percent of respondents, respectively.

**The effectiveness of file management practices is primarily measured by how productive IT security employees are, according to 52 percent of respondents**. Other metrics include the assessment of the security of sensitive and confidential data in files (49 percent of respondents) and fines due to missed compliance (46 percent of respondents). Only about half (51 percent of respondents) say their organizations are very or highly effective in complying with various industry and government regulations that require the protection of sensitive and confidential information.

**Country of origin and DLP are most likely used or will be used to improve file security management practices.** Country of origin is mainly used to neutralize zero-day or unknown threats (51 percent of respondents). The main reason to use DLP is to prevent data leaks of sensitive data and to control file sharing and access (both 44 percent of respondents).

Most companies are also using or planning to use content disarm and reconstruction (66 percent of respondents), software bill of materials (65 percent of respondents), multiscanning (64 percent of respondents), sandboxing (62 percent of respondents), file vulnerability assessment (61 percent of respondents) and the use of threat intelligence (57 percent of respondents).

**AI is being used to mitigate file security risks and reduce the costs to secure files.** Thirty-three percent of respondents say their organizations have made AI part of their organizations' file security strategy and 29 percent plan to add AI in 2026. To secure sensitive corporate files in AI workloads, organizations primarily use prompt security tools (41 percent of respondents) and mask sensitive information (38 percent of respondents).

Twenty-five percent of organization have adopted a formal Generative AI (GenAI) policy and 27 percent of respondents say their organizations have an ad hoc approach. Twenty-nine percent of respondents say GenAI is banned.

## Part 2. Key findings

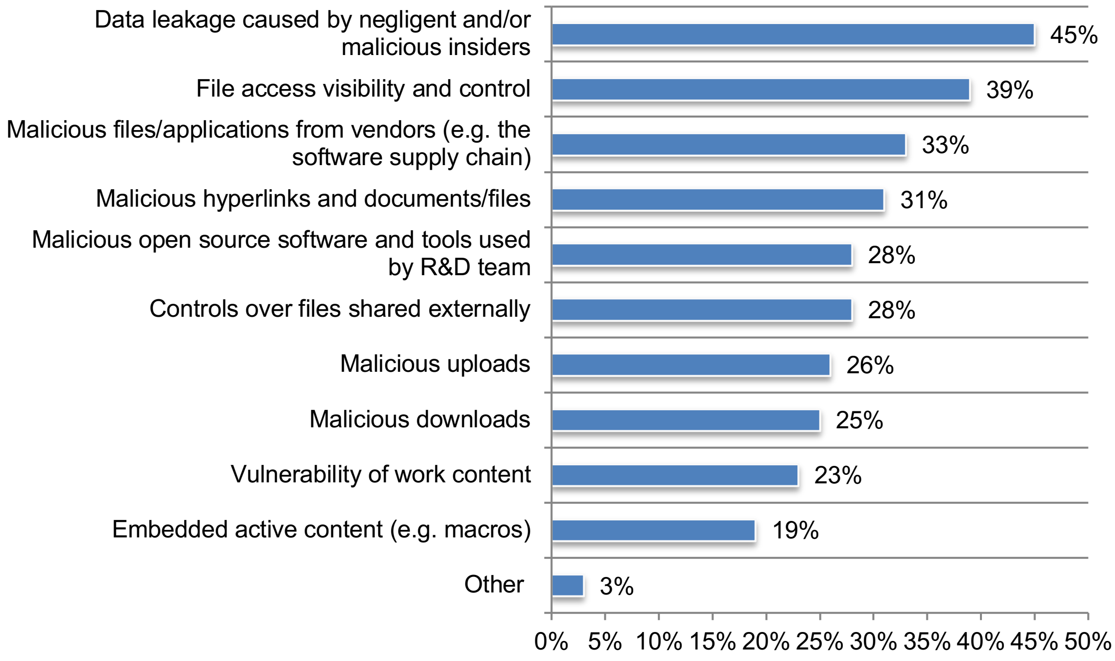
In this section, we provide an analysis of the research. The complete survey findings are presented in the Appendix of this report. The analysis of the research is organized according to the following topics.

- Threats to the security of files
- File security management practices
- AI in file security strategy

## Threats to the security of files

**Negligent and malicious insiders are the greatest threat to file security.** The top three risks to organizations' file security strategies are data leakage caused by negligent or malicious insiders (45 percent of respondents), file access visibility and control (39 percent of respondents) and malicious files/applications from vendors (e.g. the software supply chain) (33 percent of respondents). Only 40 percent of respondents say their organizations can detect and respond to file-based threats within a day (25 percent) or within a week (15 percent).

**Figure 2. What are the greatest risks to your organization's file security strategy?**
Three responses permitted

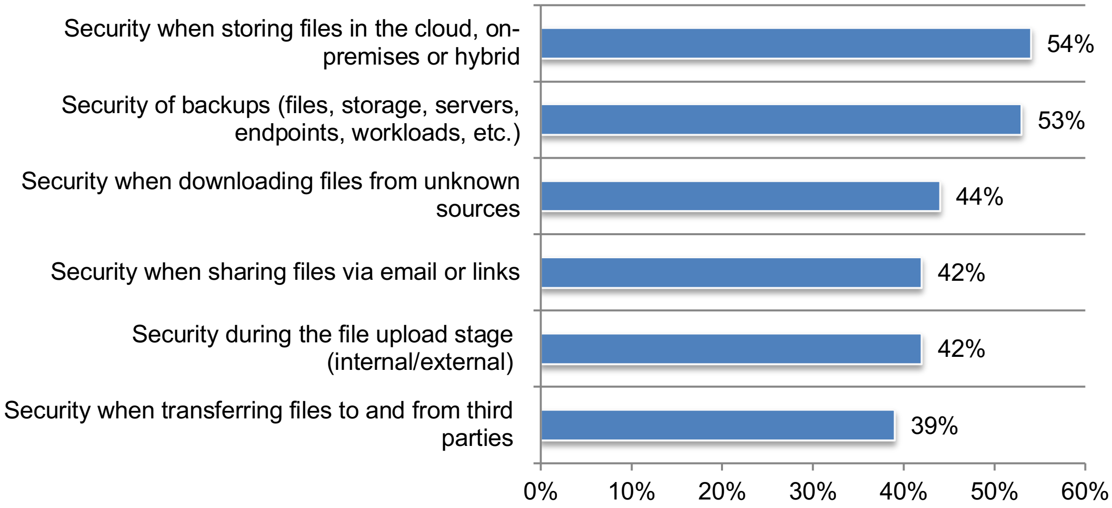


**The security of data files is most vulnerable when transferring files to and from third parties.** Only 39 percent of respondents say their organizations have high confidence in the security of files when transferring them to and from third parties.

Respondents were asked to rate their confidence in different stages of file security on a scale from 1 = low confidence to 10 = high confidence. Figure 2 presents the high confidence responses (defined as responses rated 7or higher responses).

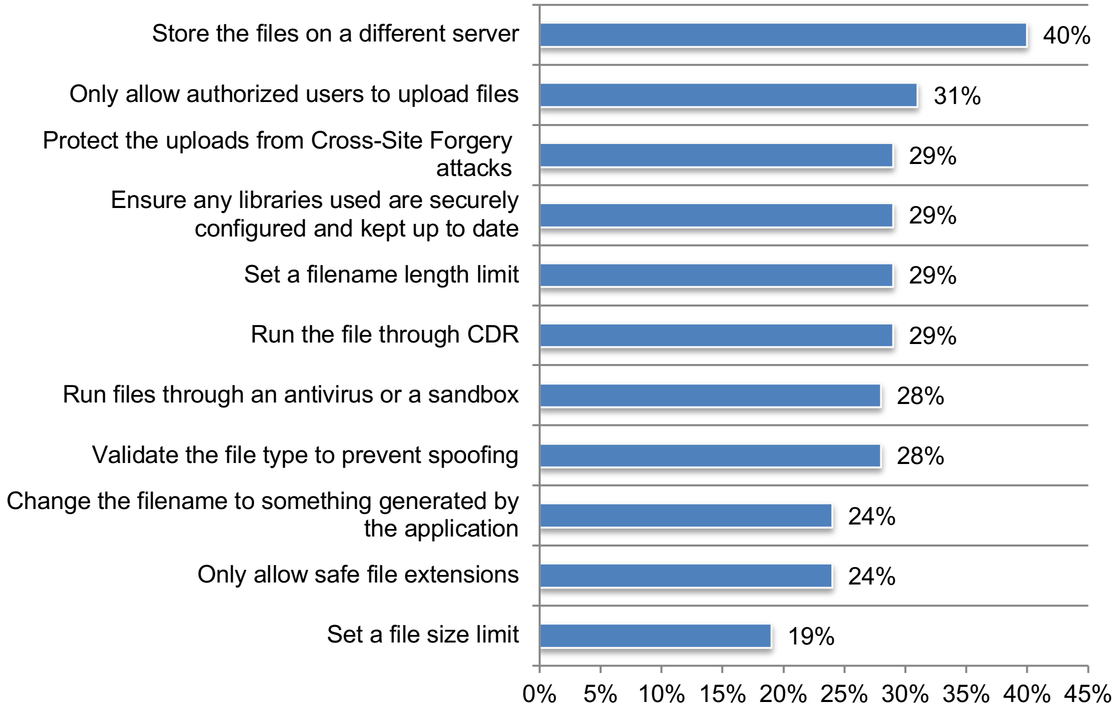
As shown, only 42 percent of respondents have high confidence in the security of files during the file upload stage (internal/external) and when sharing files via email or links. Forty-four percent of respondents say their organizations are highly confident in the security of files when downloading them from unknown sources. Organizations have more confidence when storing files in the cloud, on-premises or hybrid (54 percent of respondents) or in the security of backups (53 percent of respondents).

**Figure 3. Confidence in file security**
On a scale from 1 = low confidence to 10 = high confidence, 7+ responses presented



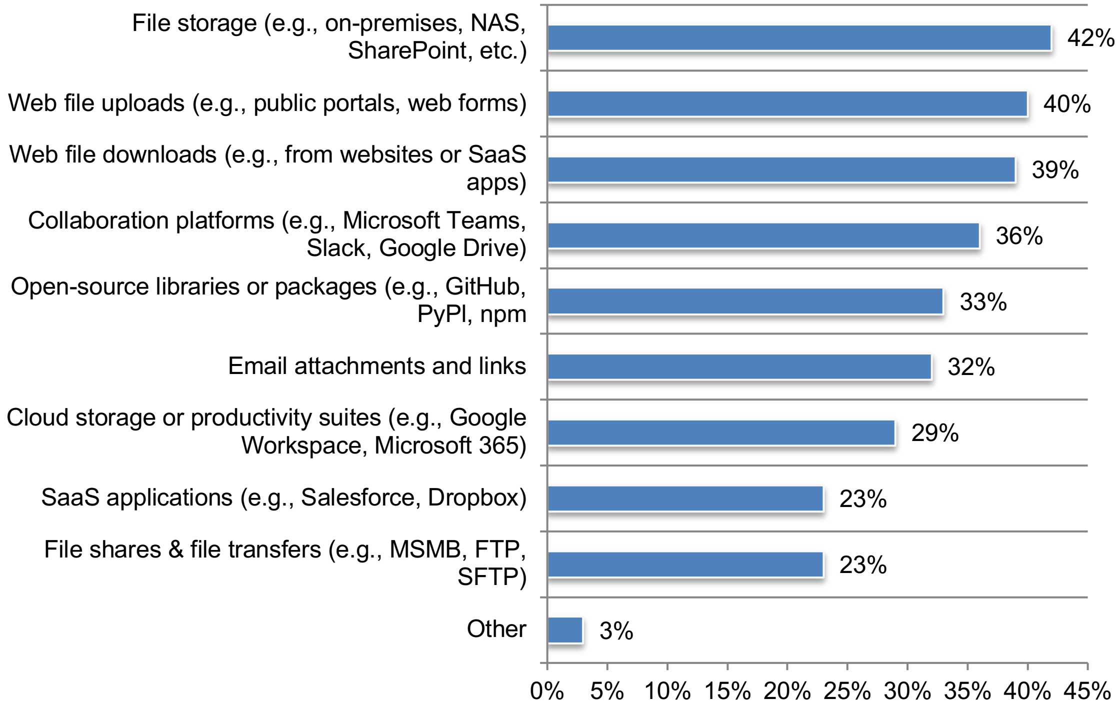
**In recognition of the serious threats to sensitive data in files, the Open Web Application Security Project (OWASP) created principles to reduce the occurrence of security incidents.** These principles focus on securing file uploads. As shown in Figure 4, 40 percent of respondents say the most often used or will use to secure file upload implementation is to store the files on a different server. Only 31 percent of respondents say only allow authorized users to upload files.

**Figure 4. OWASP principles implemented to secure file uploads**
More than one response permitted



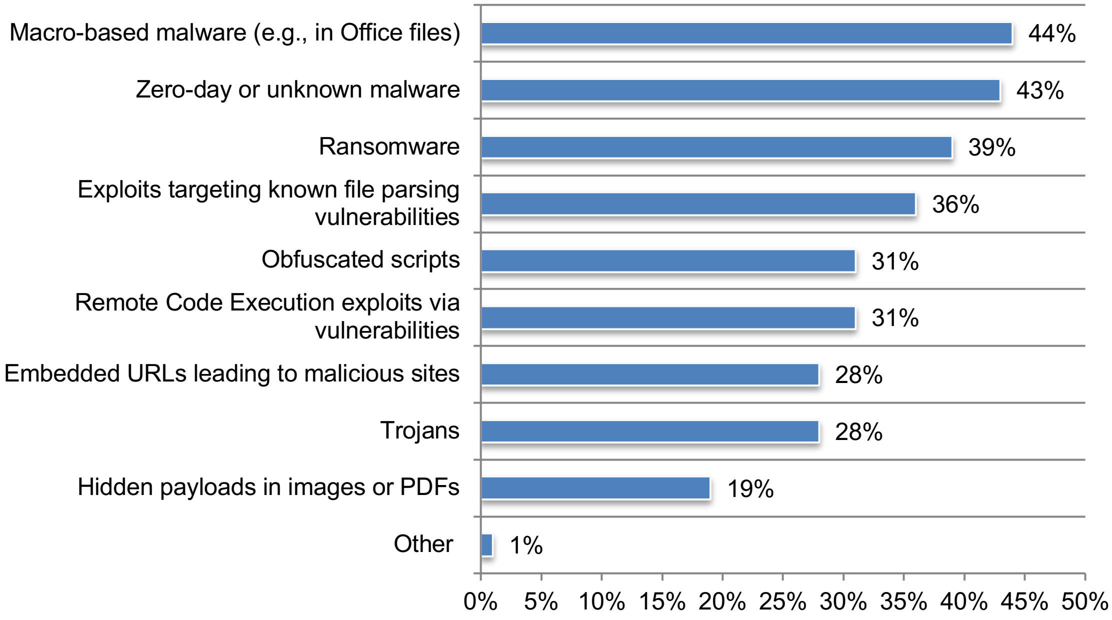
**The security of files is most vulnerable in file storage (e.g. on-premises, NAS, SharePoint).** Respondents were asked which file-based channels or environments create the biggest file security threat. Forty-two percent of respondents say file storage is least secure. According to Figure 5, 40 percent of respondents say web file uploads (e.g. public portals, web forms) and 39 percent of respondents say web file downloads (e.g. from websites or SaaS apps) are vulnerable to a data breach or security incident.

**Figure 5. The file-based channels or environments are the biggest security threat**
Three responses permitted



**Organizations are most concerned about macro-based malware and zero-day or unknown malware in files.** Respondents were asked which types of malicious content their organizations have encountered and are most concerned about in files. According to Figure 6, 44 percent of respondents say macro-based malware and 43 percent of respondents say zero-day or unknown malware pose the greatest risk. Thirty-nine percent of respondents say ransomware is one of the biggest threats.

**Figure 6. The types of malicious content of greatest concern**
Three responses permitted

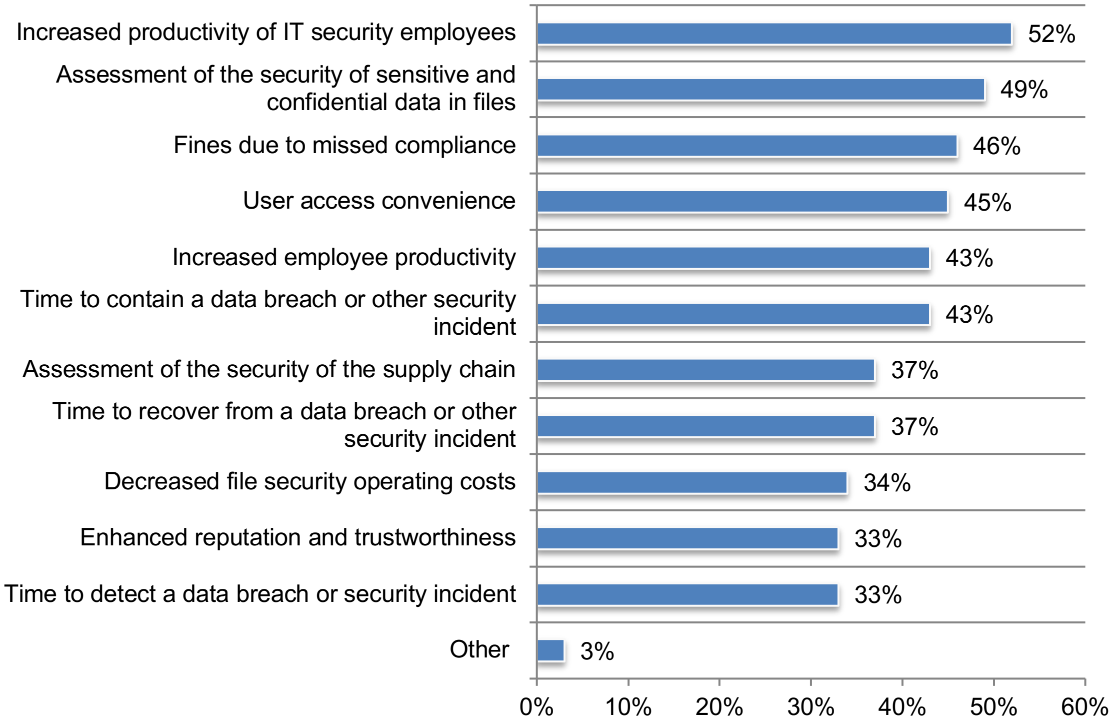


## File security management practices

**To improve the security of file transfer practices, organizations are measuring how file management practices can increase the productivity of IT security staff and other employees.** A key takeaway from the research is that the diminishment of workplace and employee productivity are top consequences from security incidents involving sensitive data in files.

According to Figure 7, 52 percent of respondents say their organizations measure the increased productivity of IT security staff and 49 percent of respondents say their organizations assess the security of sensitive and confidential in files. Forty-three percent of respondents say increased employee productivity is measured. Also measured are fines due to missed compliance (46 percent of respondents) and user access convenience (45 percent of respondents).

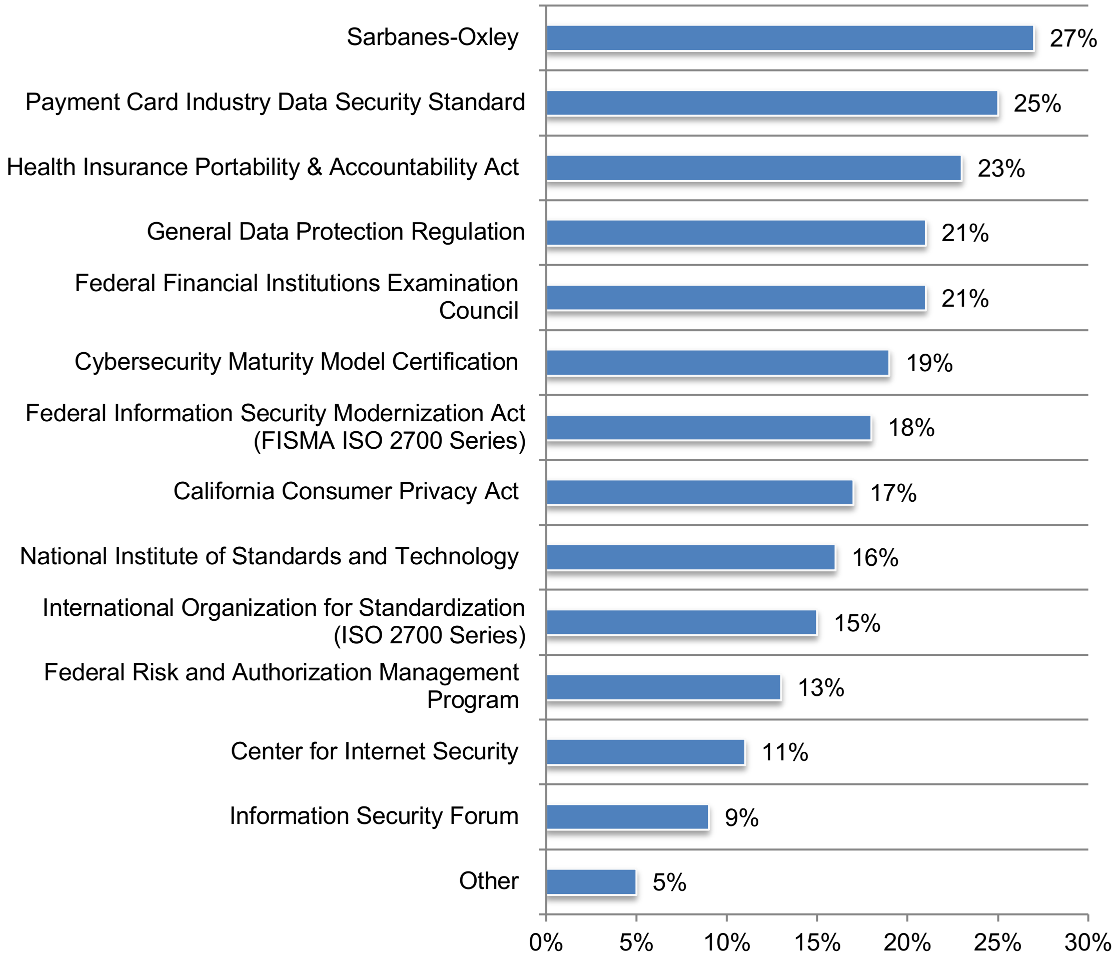
**Figure 7. Metrics used to measure the security of file transfer practices**
More than one response permitted



**Organizations face the burden of complying with standards, laws and regulations.** Figure 8 lists the security and privacy standards and regulations organizations must comply with. Sarbanes-Oxley (SOX) (27 percent of respondents), Payment Card Industry Data Security Standard (PCI-DSS) (25 percent of respondents) and Health Insurance Portability & Accountability Act (23 percent of respondents) affect organizations the most.

Only about half (51 percent of respondents) say their organizations are very or highly effective in complying with various industry and government regulations that require the protection of sensitive and confidential information.

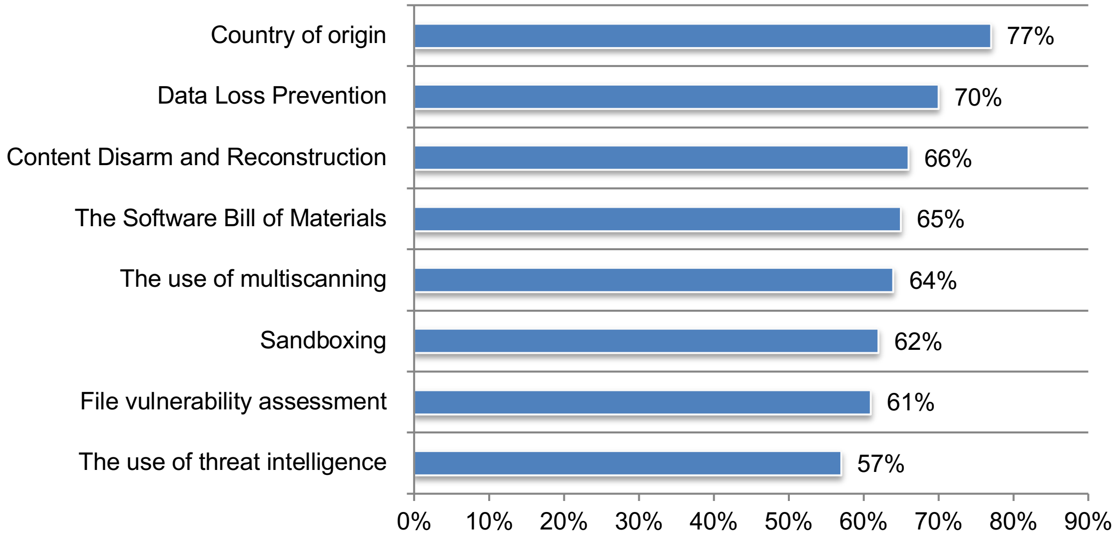
**Figure 8. The privacy and security standards, laws and regulations organizations must comply with**
More than one response permitted



**The following are technologies used to improve file security management practices.** As shown in Figure 9, country of origin and Data Loss Prevention (DLP) are most likely used or will be used to improve the security of files.

Country of origin is used to neutralize zero-day or unknown threats (51 percent of respondents) and to improve operational efficiency (49 percent of respondents). The main reason to use DLP is to prevent data leaks of sensitive data and to control file sharing and access (44 percent of respondents).

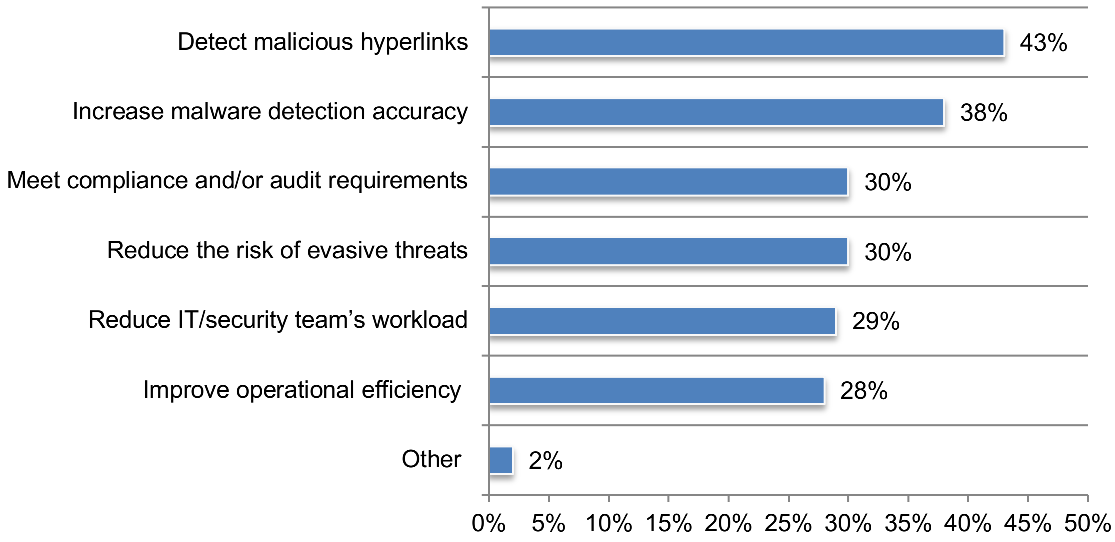
**Figure 9. The current and future use of technologies to secure sensitive data in files**
Currently used and plan to use responses combined



**Multiscanning** refers to running multiple anti-malware engines or anti-virus engines as an advanced threat detection and prevention technology that increases detection rates, decreases outbreak detection times and provides resiliency for single vendor anti-malware solutions.

According to Figure 10, multiscanning is primarily used to detect malicious hyperlinks (43 percent of respondents) and increase malware detection accuracy (38 percent of respondents). Currently 41 percent of respondents say their organizations use multiscanning as part of their file security strategy and 23 percent of respondents say they will adopt in 2026.

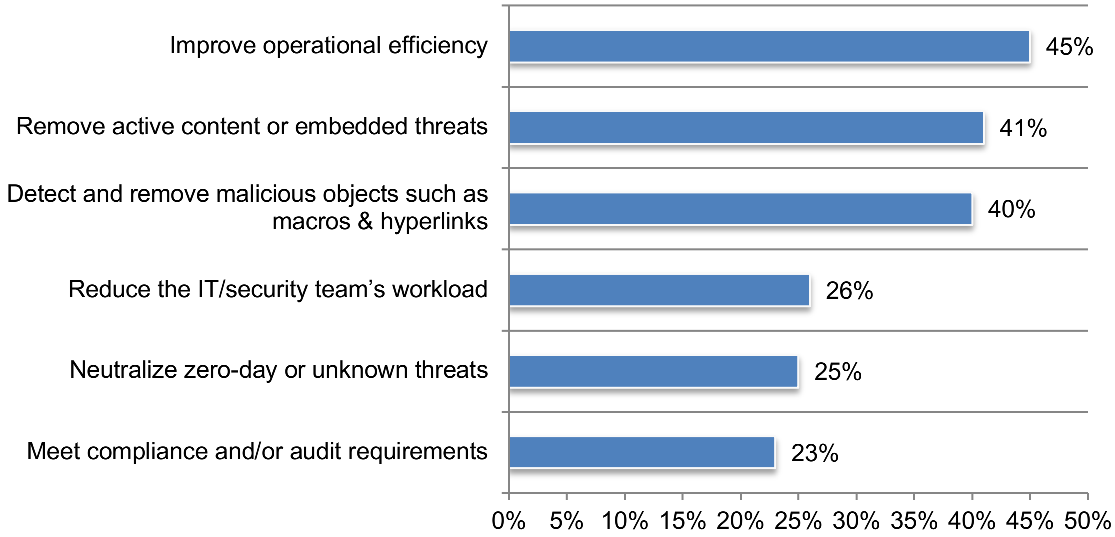
**Figure 10. Reasons to use or plan to use multiscanning**
Two responses permitted



**Content Disarm & Reconstruction (CDR)** is a cybersecurity technology that removes unapproved objects without relying on malware detection. Unlike traditional malware analysis, CDR assumes all files could be malicious and rebuilds them using only the known safe elements. CDR works by processing all incoming files, deconstructing them and removing any elements that do not match the file type's standards or set policies. It then rebuilds the files into clean versions that can be safely delivered to end users.

According to Figure 11, the primary reasons for using or planning to use CDR are to improve operational efficiency (45 percent of respondents) and remove active content or embedded threats (41 percent of respondents). Thirty-five percent of respondents say their organizations are currently using CDR and 31 percent of respondents say they plan to use in 2026.

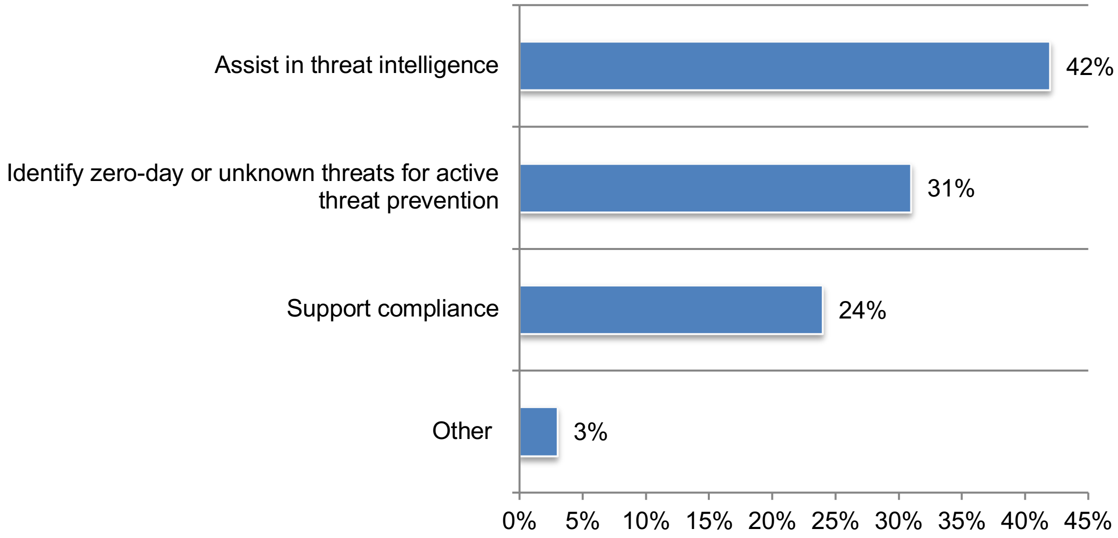
**Figure 11. Reasons to use CDR**
Two responses permitted



**Sandboxing** is a practice of isolating potentially malicious software or code in a secure, controlled environment (a "sandbox") for analysis and testing without risking the main system or network. This isolated environment allows security professionals to execute and examine suspicious files or code, observing their behavior without the risk of harm to the actual system.

According to Figure 12, the top reason for using sandboxing is to assist in threat intelligence (42 percent of respondents). Currently, 43 percent of respondents say their organizations use sandboxing and 19 percent of respondents plan to use in 2026.

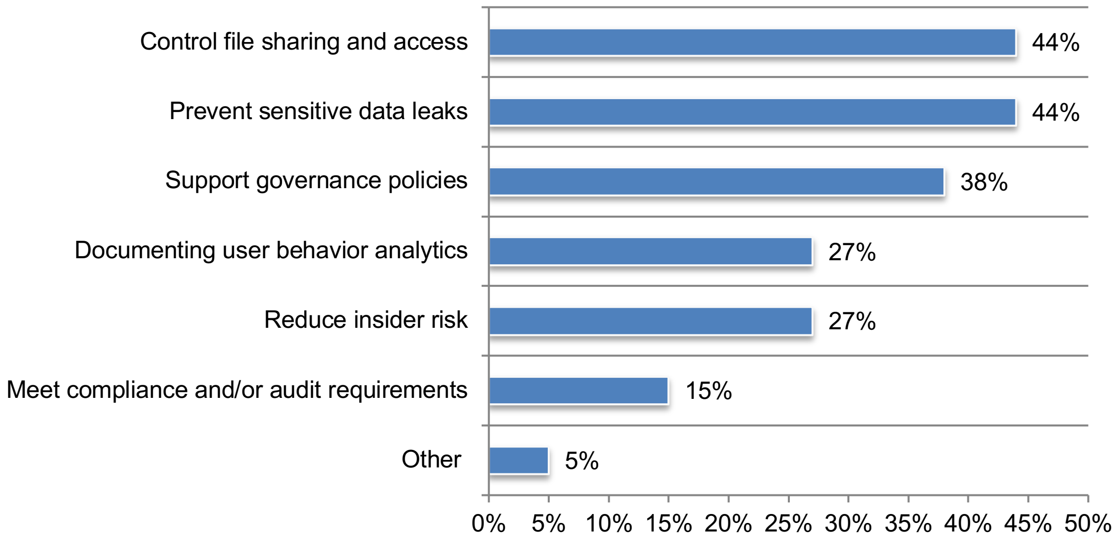
**Figure 12. Reasons to use sandboxing**



**Data Loss Prevention (DLP)** helps prevent potential data breaches and regulatory compliance violations by detecting and blocking sensitive, out-of-policy and confidential data in files and emails, including credit card numbers and Social Security numbers.

According to Figure 13, the top two reasons for using DLP are to prevent sensitive data leaks and control file sharing and access (both 44 percent of respondents). Forty percent of respondents say they are or currently using DLP and 30 percent of respondents say they plan to use it in 2026.

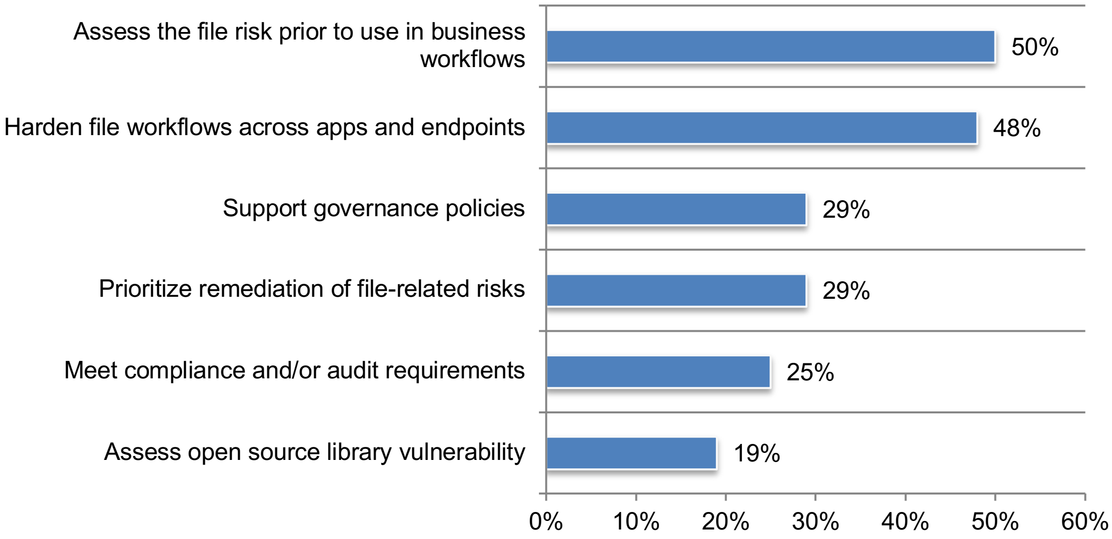
**Figure 13. Reasons to use DLP**
Two responses permitted



**File vulnerability** refers to a weakness within a file or the way it is processed that can be exploited to compromise a system. This can include malicious code embedded in documents, improper file permissions or flaws in file parsing by applications. Attackers often exploit these vulnerabilities to execute unauthorized actions, such as installing malware or gaining elevated access.

According to Figure 14, organizations are using file vulnerability assessment to assess the file risk prior to use in business workflows (50 percent respondents) and harden the workflows across apps and endpoints (48 percent of respondents). Forty percent of respondents say their organizations use file vulnerability assessment and 21 percent plan to use it in 2026.

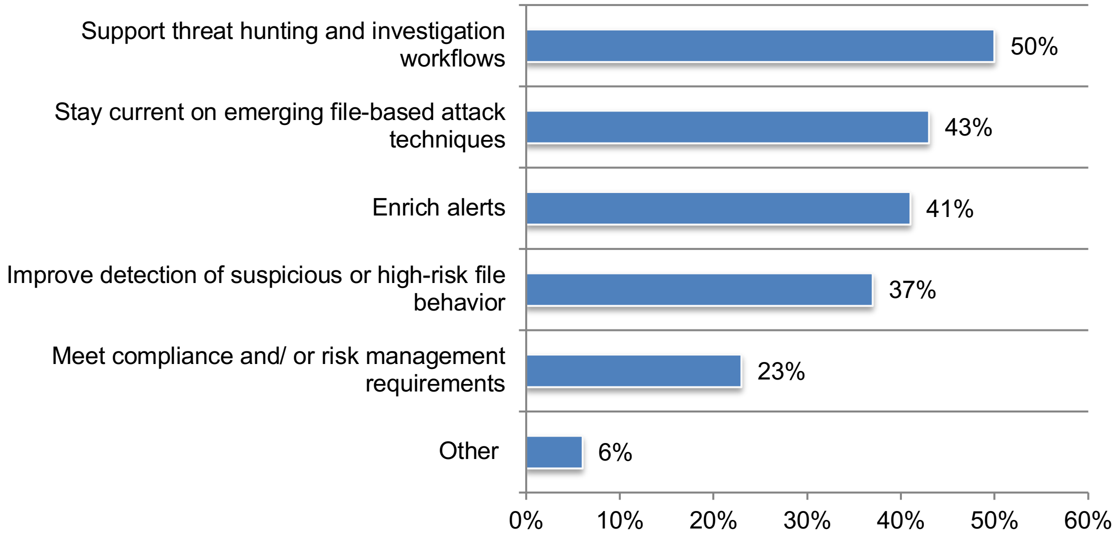
**Figure 14. Reasons to use file vulnerability assessment**
Two responses permitted



**Threat intelligence** is evidence-based knowledge that includes context, mechanisms, indicators, implications and actionable advice about an existing or emerging menace or hazard to assets. This knowledge can be used to make informed decisions about how to respond to a menace or hazard.

According to Figure 15, the primary benefits of threat intelligence and why organization use it are to support threat hunting and investigation workflows (50 percent of respondents) and to stay current on emerging file-base attack techniques (43 percent of respondents). Thirty-one percent of respondents say their organizations use threat intelligence as part of their organizations' file security strategy and 26 percent plan to use threat intelligence in 2026.

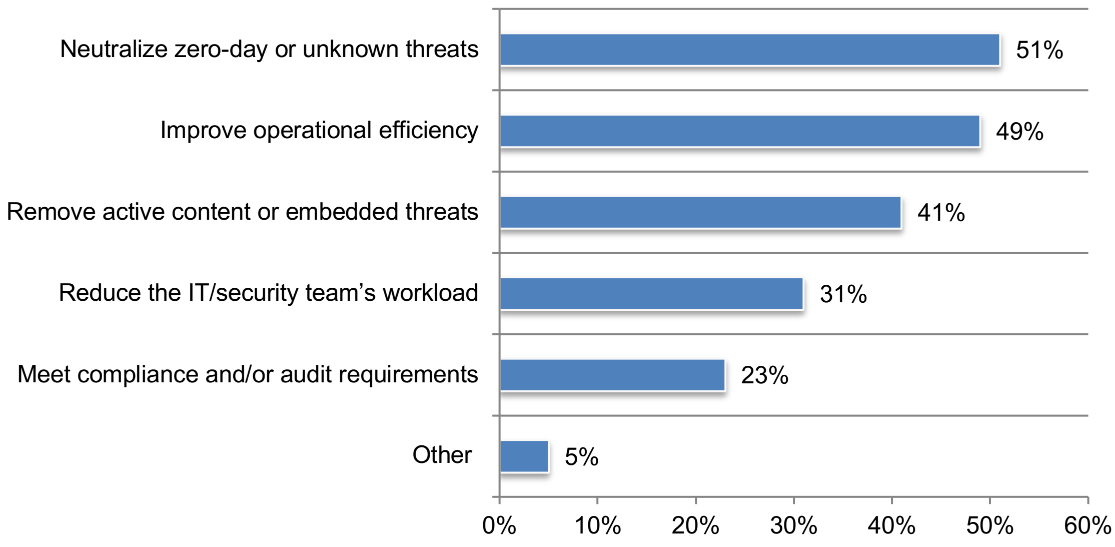
**Figure 15. Reasons to use threat intelligence**
Two responses permitted



**Country of origin** refers to the nation where a software, hardware or digital service was developed manufactured or maintained. This designation is important for assessing potential security risks, as products from certain countries may be subject to foreign influence, espionage or supply chain vulnerabilities.

According to Figure 16, 51 percent of respondents say their organizations are using or plan to use country of origin to neutralize zero-day or unknown threats and 49 percent say their organization use country of origin to improve operational efficiency. Currently, 37 percent of organizations are using country of origin and 40 percent plan to use it in 2026.

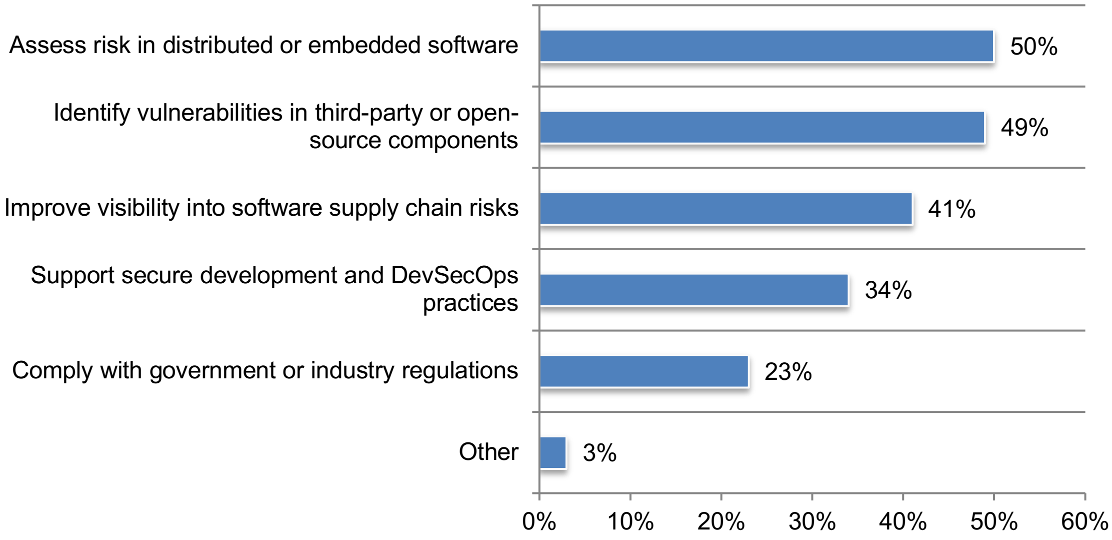
**Figure 16. Reasons to use country of origin**
Two responses permitted



**Software Bill of Materials (SBOM)** is a detailed inventory of all closed and open-source components, libraries and dependencies in an application. In simpler terms, just as a physical product may come with a list of component parts and materials software also has its components.

According to Figure 17, organizations use SBOM primarily to assess risk in distributed or embedded software (50 percent of respondents) and to identify vulnerabilities in third-party or open-source components (49 percent of respondents). Thirty-nine percent of respondents say their organizations use SBOM and 26 percent of respondents say they plan to use it in 2026.

**Figure 17. Reasons to use SBOM**
Two responses permitted

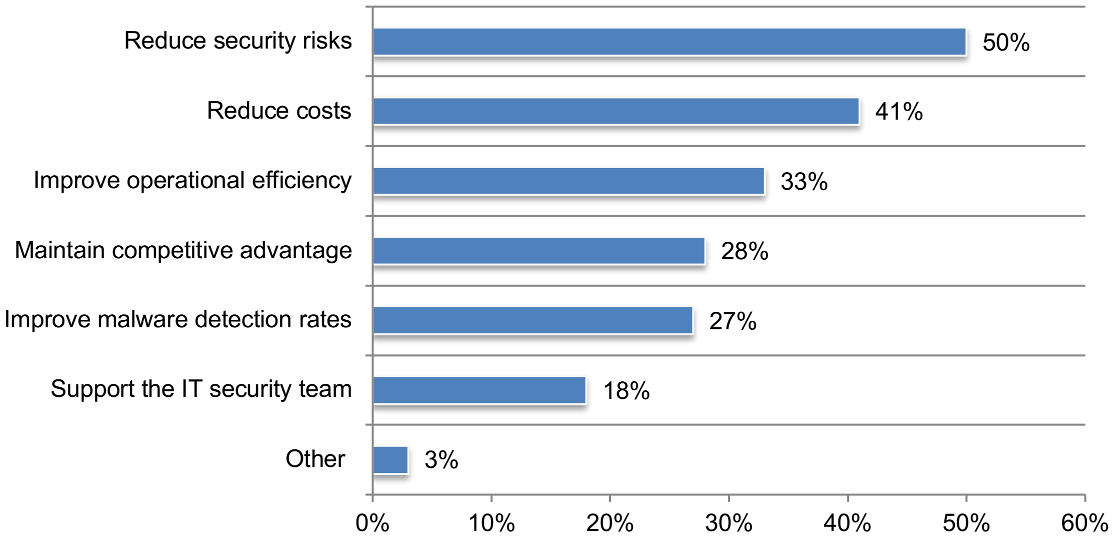


## AI as part of organizations' file security strategy

**Organizations are using AI to reduce file security risks.** Thirty-three percent of respondents say their organizations have made AI a part of their organizations' file security strategy and 29 percent plan to add AI in 2026. Fifty-nine percent of these respondents say AI is very or highly effective in enhancing file security maturity.

As shown in Figure 18, the benefits of AI are reduction in security risks (50 percent of respondents) and cost savings (41 percent of respondents). Thirty-three percent of respondents say AI improve operational efficiency.

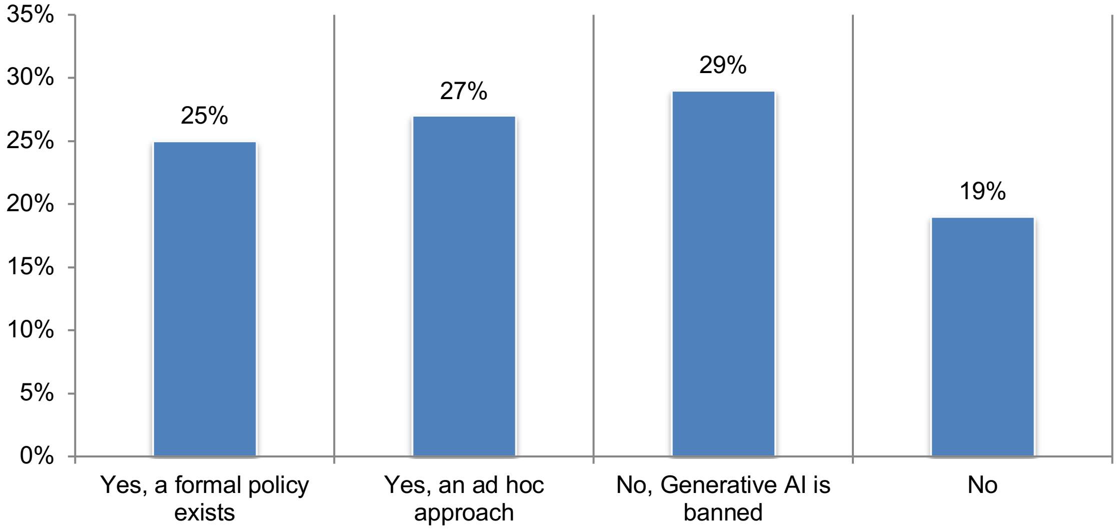
**Figure 18. The top reasons for using or planning to use AI**
Two responses permitted



**Generative artificial intelligence (GenAI)** refers to a category of AI algorithms that generates new outputs based on the large language models (LLMs) they have been trained on. This is unlike machine learning systems that are designed to recognize patterns and make predictions. Recent advancements in GenAI improve threat detection and response capabilities. Dynamic-based generative AI models are better positioned to analyze complex systems, such as network infrastructures or software applications, to identify vulnerabilities, detect novel threats and mitigate risks.

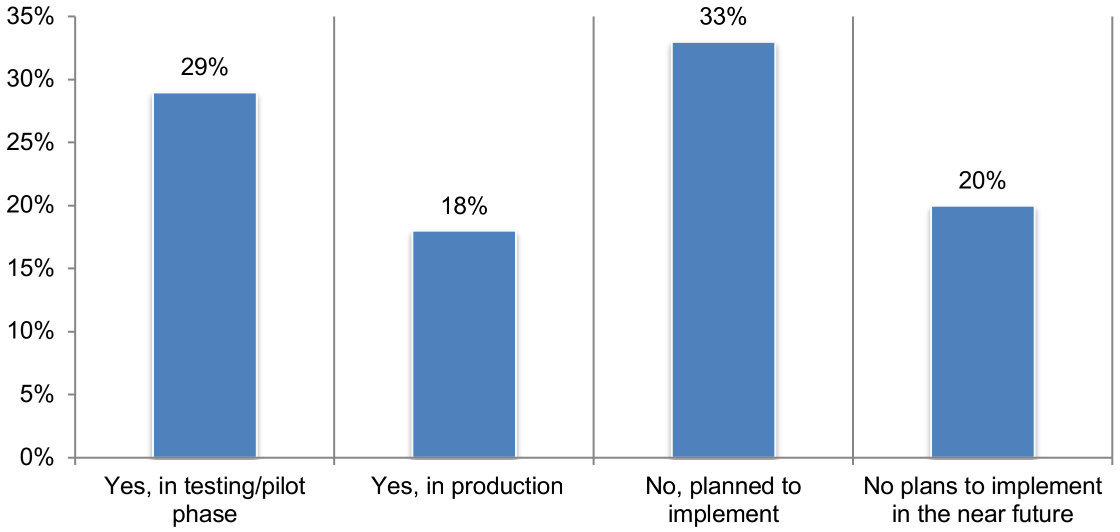
Only 25 percent of respondents say their organizations have adopted a formal GenAI policy and 27 percent of respondents say their organizations have an ad hoc approach. Nineteen percent of respondents say their organizations have no plans to adopt GenAI and 29 percent of respondents say GenAI is banned.

**Figure 19. Has your organization adopted GenAI?**



According to Figure 20, of those organizations using GenAI, 29 percent of respondents say it is in the testing/pilot phase to use it to unlock files and 18 percent of respondents say it is in production. Thirty-three percent of respondents say there is a plan to implement. Twenty percent of respondents say there are no plans to use GenAI to unlock files.

**Figure 20. Does your organization us GenAI to unlock files?**



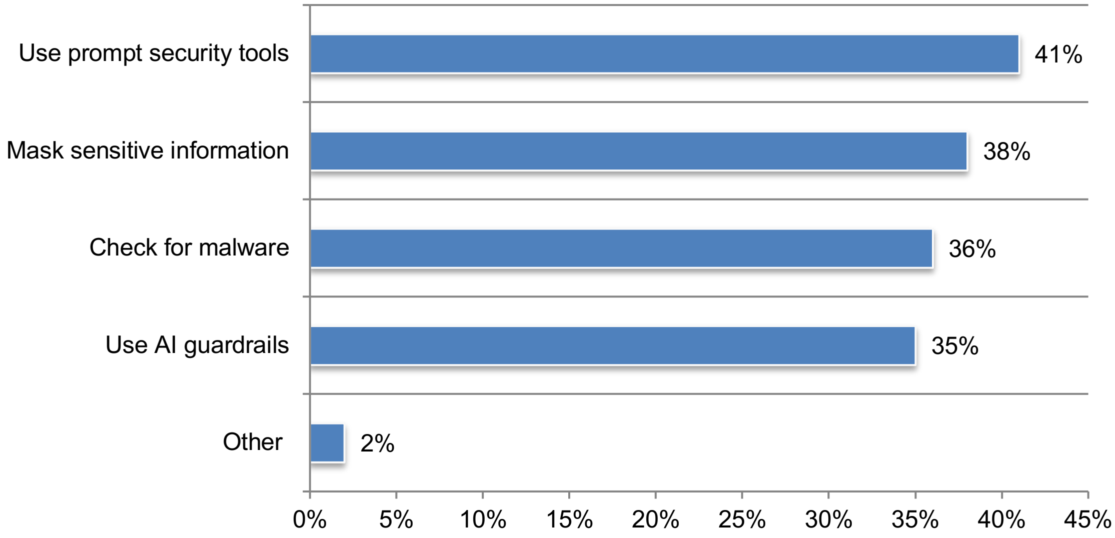
**AI workloads** refer to the tasks and processes that AI systems perform. These can range from data processing and machine learning model training to real-time inference and decision-making.

**AI guardrails** are sets of policies, rules, and mechanisms designed to ensure AI systems operate safely, ethically, and within defined boundaries. They act as safety measures, preventing AI from generating harmful, biased, and/or inappropriate outputs, and guide its behavior in line with organizational standards and legal requirements.

**Prompt security tools for AI** help protect GenAI models from malicious inputs (prompt injections, jailbreaks) and harmful outputs (sensitive data leakage, inappropriate content).

Thirty-seven percent of respondents say their organizations take steps to secure sensitive corporate files in AI workloads. According to Figure 20, the steps most often taken are to use prompt security tools (41 percent of respondents), mask sensitive information (38 percent of respondents), check for malware (36 percent of respondents) and use AI guiderails (35 percent of respondents).

**Figure 21. Measures taken to secure sensitive corporate files in AI workloads.**
More than one response permitted



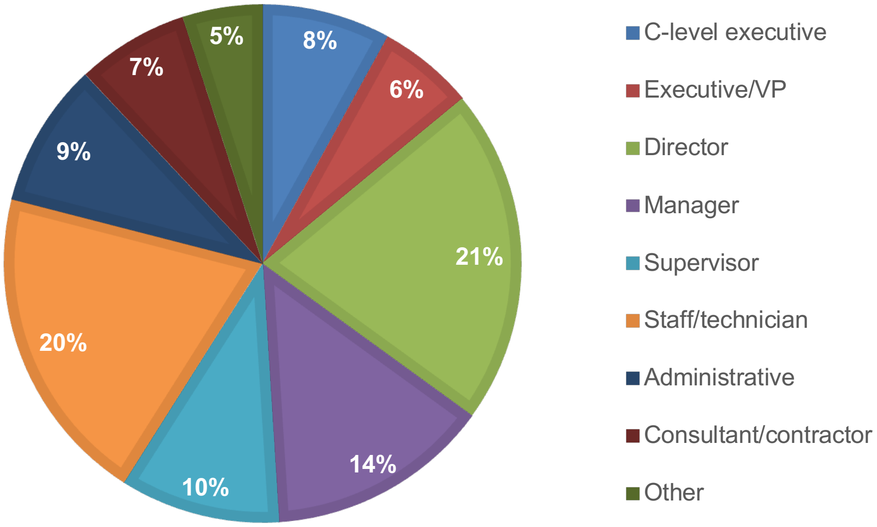
## Part 3. Methodology

A sampling frame of 18,602 IT and IT security practitioners in the United States, who are knowledgeable about their organizations' approach to file security were selected as participants to this survey. Table 1 shows 688 total returns. Screening and reliability checks required the removal of 76 surveys. Our final sample consisted of 612 surveys or a 3.3 percent response rate.

| **Table 1. Sample response** | Freq | Pct% |
|---|---|---|
| Sampling frame | 18,602 | 100.0% |
| Total returns | 688 | 3.7% |
| Rejected or screened surveys | 76 | 0.4% |
| Final sample | 612 | 3.3% |

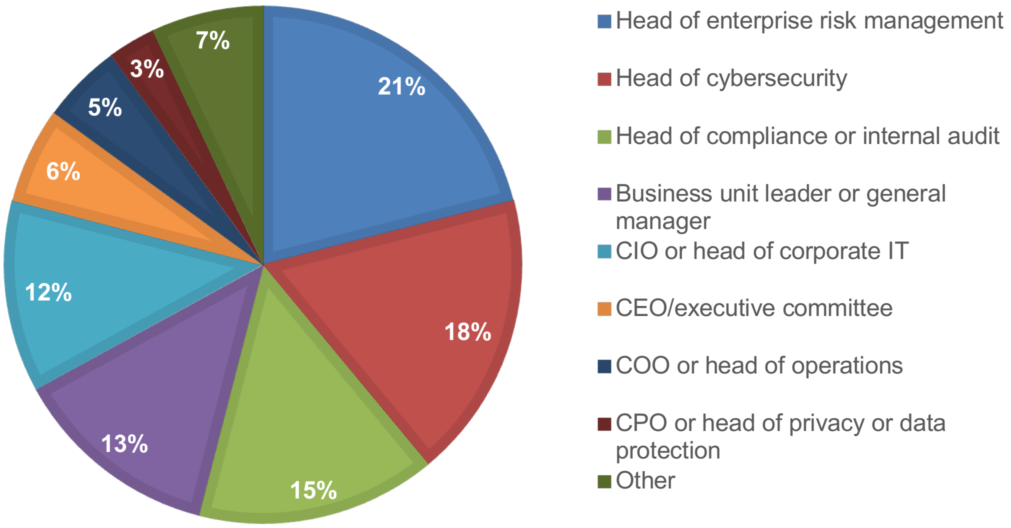
Pie chart 1 reports the respondent's organizational level within participating organizations. More than half (59 percent) of respondents are at or above the supervisor level. The largest category at 21 percent of respondents is director.

**Pie chart 1. Current position within the organization**



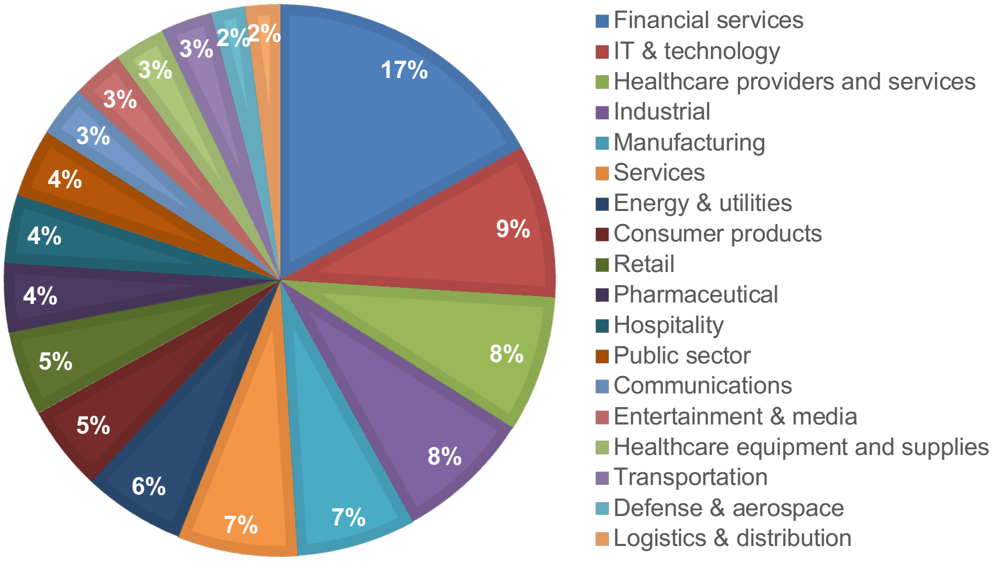
As shown in Pie chart 2, 21 percent of respondents report to the head of enterprise risk management, 18 percent report to the head of cybersecurity, 15 percent report to the head of compliance or internal audit, 13 percent report to a business unit leader or general manager and 12 percent report to the CIO or head of corporate IT.

**Pie chart 2. Direct reporting channel**



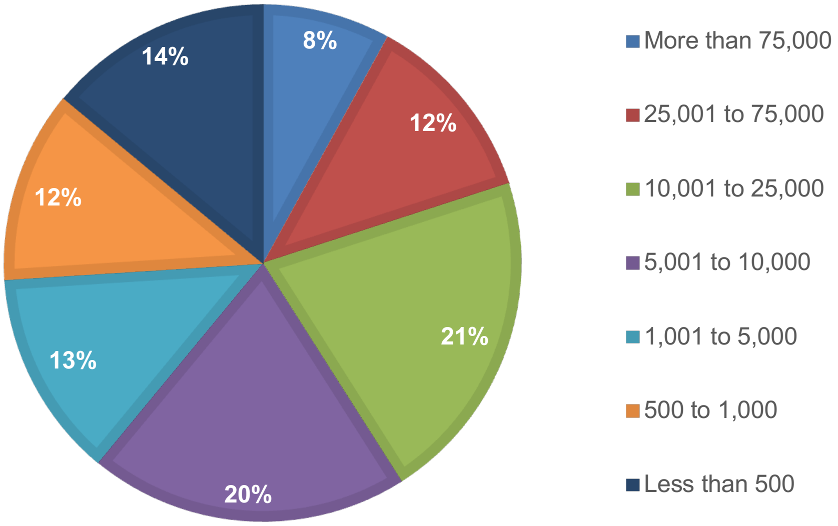
Pie chart 3 reports the industry classification of respondents' organizations. This chart identifies financial services (17 percent of respondents) as the largest industry focus, which includes banking, investment management, insurance, brokerage, payments and credit cards. This is followed by IT & technology (9 percent), healthcare providers and services (8 percent), industrial (8 percent), manufacturing and services (each at 7 percent).

**Pie chart 3. Primary industry classification**



As shown in Pie chart 4, more than half (61 percent) of respondents are from organizations with a headcount of more than 5,000 employees

**Pie chart 4. Worldwide headcount**



## Part 4. Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.

- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are cybersecurity and IT security practitioners. We also acknowledge that the results may be biased by external events such as media coverage. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.

- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide accurate responses.

## Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to survey questions. All survey responses were captured in June 2025.

| **Survey response** | **Freq** |
|---|---:|
| Sampling frame | 18,602 |
| Survey returns | 688 |
| Rejected surveys | 76 |
| Final sample | 612 |
| Response rate | 3.3% |

| S1. What best describes your organizational role or area of focus? Please select one choice only. | Pct% |
|---|---:|
| Cybersecurity C-level executive | 9% |
| Cybersecurity VP | 7% |
| Cybersecurity director/manager | 9% |
| Cybersecurity staff/operations | 11% |
| IT C-level executive | 6% |
| IT VP | 9% |
| IT director/manager | 10% |
| IT operations | 9% |
| Security architect | 13% |
| Security engineer | 12% |
| None of the above (stop) | 5% |
| Total | 100% |

| S2. How familiar are you with your organization’s approach to file security? | Pct% |
|---|---:|
| Very familiar | 32% |
| Familiar | 30% |
| Somewhat familiar | 26% |
| Not familiar (stop) | 12% |
| Total | 100% |

**Part 2. Background on file security practices**

| Q1. Who has overall accountability for file security? Please select one choice only. | Pct% |
|---|---|
| Business unit leader | 14% |
| Chief executive officer (CEO) | 5% |
| Chief information officer (CIO) | 17% |
| Chief technology officer (CTO) | 14% |
| Chief risk officer (CRO) | 11% |
| Chief information security officer (CISO) | 16% |
| Data protection officer (DPO) | 6% |
| No one person has overall accountability | 15% |
| Other (please specify) | 2% |
| Total | 100% |

| Q2a. Did your organization have a data breach or a security incident due to unauthorized sensitive and confidential data in files in the past 2 years? | Pct% |
|---|---|
| Yes | 61% |
| No (please skip to Q4) | 32% |
| Unsure (please skip to Q4) | 7% |
| Total | 100% |

| Q2b. If yes, how frequently did these data breach or cybersecurity incidents occur in the past 2 years? | Pct% |
|---|---|
| Only once | 31% |
| 2 to 5 times | 27% |
| 6 to 10 times | 31% |
| 11 to 50 times | 8% |
| 50+ times | 3% |
| Total | 100% |
| Extrapolated average | 8.425 |

| Q2c.  If yes, what were the consequences? Please select all that apply. | Pct% |
|---|---|
| Diminished brand and reputation | 26% |
| Fines and penalties | 21% |
| Loss of customer data | 50% |
| Loss of IP, including trade secrets | 39% |
| Diminished employee productivity | 50% |
| Diminished workplace productivity | 49% |
| Ransomware | 36% |
| Other (please specify) | 6% |
| Total | 277% |

| Q3a.  Did these incidents have financial consequences? | Pct% |
|---|---|
| Yes | 54% |
| No (please skip to Q4) | 46% |
| Total | 100% |

| Q3b.  If yes, what was the cost of all incidents experienced in the past 2 years? Your best estimate is welcome. | Pct% |
|---|---|
| Less than $50,000 | 4% |
| $50,000 to $100,000 | 6% |
| $100,001 to $250,000 | 8% |
| $250,001 to $500,000 | 16% |
| $500,001 to $1,000,000 | 25% |
| $1,000,001 to $5,000,000 | 21% |
| $5,000,001 $10,000,000 | 13% |
| More than $10,000,000 | 7% |
| Total | 100% |
| Extrapolated value | **$ 2,744,500** |

| Q4. Which security and privacy standards, laws and regulations must your organization comply with? Please select all that apply. | Pct% |
|---|---|
| California Consumer Privacy Act (CCPA) | 17% |
| Center for Internet Security (CIS) | 11% |
| Cybersecurity Maturity Model Certification (CMMC) | 19% |
| Federal Financial Institutions Examination Council (FFIEC) | 21% |
| Federal Information Security Modernization Act (FISMA ISO 2700 Series) | 18% |
| Federal Risk and Authorization Management Program (FedRAMP) | 13% |
| General Data Protection Regulation (GDPR) | 21% |
| Health Insurance Portability & Accountability Act (HIPAA) | 23% |
| Information Security Forum (ISF) | 9% |
| International Organization for Standardization (ISO 2700 Series) | 15% |
| National Institute of Standards and Technology (NIST) | 16% |
| Payment Card Industry Data Security Standard (PCI-DSS) | 25% |
| Sarbanes-Oxley (SOX) | 27% |
| Other (please specify) | 5% |
| Total | 240% |

| Q5. Using the following 10-point scale, please rate the effectiveness of your organization’s ability to comply with various industry and government regulations that require the protection of sensitive and confidential data from 1 = low effectiveness to 10 = high effectiveness. | Pct% |
|---|---|
| 1 or 2 | 12% |
| 3 or 4 | 19% |
| 5 or 6 | 18% |
| 7 or 8 | 19% |
| 9 or 10 | 32% |
| Total | 100% |

| Q6. Which of the following poses the greatest risk to your organization’s file security strategy? Please select the top 3 that are of greatest concern. | Pct% |
|---|---|
| Malicious uploads | 26% |
| Malicious downloads | 25% |
| Malicious files/applications from vendors (e.g. the software supply chain) | 33% |
| File access visibility and control | 39% |
| Malicious hyperlinks and documents/files | 31% |
| Vulnerability of work content | 23% |
| Embedded active content (e.g. macros) | 19% |
| Data leakage caused by negligent and/or malicious insiders | 45% |
| Controls over files shared externally | 28% |
| Malicious open source software and tools used by R&D team | 28% |
| Other (please specify) | 3% |
| Total | 300% |

**Part 3. File security solutions**

| Q7a. Does your organization measure the security of its file transfer practices? . | Pct% |
|---|---|
| Yes | 68% |
| No | 32% |
| Total | 100% |
| | |

| Q7b. If yes, what metrics are used. Please select all that apply. | |
|---|---|
| The prevention of attacks on sensitive data in files based on threat intelligence | Pct% |
| Time to detect a data breach or security incident | 33% |
| Time to contain a data breach or other security incident | 43% |
| Time to recover from a data breach or other security incident | 37% |
| Fines due to missed compliance | 46% |
| Increased employee productivity | 43% |
| Increased productivity of IT security employees | 52% |
| Decreased file security operating costs | 34% |
| Enhanced reputation and trustworthiness | 33% |
| Assessment of the security of the supply chain | 37% |
| Assessment of the security of sensitive and confidential data in files | 49% |
| User access convenience | 45% |
| Other (please specify) | 3% |
| Total | 455% |

| Q8. Does your organization use or will use multiscanning as part of its file security strategy? | Pct% |
|---|---|
| Yes | 41% |
| Plan to use in 2026 | 23% |
| Interested, but no plans to use at this time (please skip to Q10) | 21% |
| No plan to use (please skip to Q10) | 15% |
| Total | 100% |

| Q9. What are the top two reasons for using or planning to use multiscanning? Please select the top two reasons only. | Pct% |
|---|---|
| Increase malware detection accuracy | 38% |
| Reduce the risk of evasive threats | 30% |
| Improve operational efficiency | 28% |
| Reduce IT/security team's workload | 29% |
| Meet compliance and/or audit requirements | 30% |
| Detect malicious hyperlinks | 43% |
| Other (please specify) | 2% |
| Total | 200% |

| Q10. Is Content Disarm and Reconstruction (CDR) part of your organization's file security strategy | Pct% |
|---|---|
| Yes | 35% |
| Plan to use in 2026 | 31% |
| Interested, but no plans to use at this time (please skip to Q12) | 19% |
| No plan to use (please skip to Q12) | 15% |
| Total | 100% |

| Q11. What are the top two reasons for using or planning to use CDR? Please select the top two reasons only. | Pct% |
|---|---|
| Neutralize zero-day or unknown threats | 25% |
| Remove active content or embedded threats | 41% |
| Improve operational efficiency | 45% |
| Reduce the IT/security team's workload | 26% |
| Meet compliance and/or audit requirements | 23% |
| Detect and remove malicious objects such as macros & hyperlinks | 40% |
| Other (please specify) | 0% |
| Total | 200% |

| Q12. Is sandboxing part of your organization’s file security strategy? | Pct% |
|---|---|
| Yes | 43% |
| Plan to use in 2026 | 19% |
| Interested, but no plans to use at this time (please skip to Q14) | 15% |
| No plan to use (please skip to Q14) | 23% |
| Total | 100% |

| Q13. What is the top reason for using or planning to use Sandboxing? | Pct% |
|---|---|
| Assist in threat intelligence | 42% |
| Identify zero-day or unknown threats for active threat prevention | 31% |
| Support compliance | 24% |
| Other (please specify) | 3% |
| Total | 100% |

| Q14. Is Data Loss Prevention (DLP) part of your organization’s file security strategy? | Pct% |
|---|---|
| Yes | 40% |
| Plan to use in 2026 | 30% |
| Interested, but no plans to use at this time (please skip to Q16) | 14% |
| No plan to use (please skip to Q16) | 16% |
| Total | 100% |

| Q15. What are the top two reasons for using or planning to use DLP? Please select the top two reasons only. | Pct% |
|---|---|
| Prevent sensitive data leaks | 44% |
| Reduce insider risk | 27% |
| Control file sharing and access | 44% |
| Support governance policies | 38% |
| Meet compliance and/or audit requirements | 15% |
| Documenting user behavior analytics | 27% |
| Other (please specify) | 5% |
| Total | 200% |

| Q16. Is file vulnerability assessment part of your organization’s file security strategy? | Pct% |
|---|---|
| Yes | 40% |
| Plan to use in 2026 | 21% |
| Interested, but no plans to use at this time (please skip to Q18) | 20% |
| No plan to use (please skip to Q18) | 19% |
| Total | 100% |

| Q17. What are the top two reasons for using or planning to use file vulnerability assessment? Please select the top two reasons only. | Pct% |
|---|---|
| Assess the file risk prior to use in business workflows | 50% |
| Prioritize remediation of file-related risks | 29% |
| Harden file workflows across apps and endpoints | 48% |
| Support governance policies | 29% |
| Assess open source library vulnerability | 19% |
| Meet compliance and/or audit requirements | 25% |
| Other (please specify) | 0% |
| Total | 200% |

| Q18. Does your organization use threat intelligence as part of your organization's file security strategy? | Pct% |
|---|---|
| Yes | 31% |
| Plan to use in 2026 | 26% |
| Interested, but no plans to use at this time (please skip to Q20) | 22% |
| No plan to use (please skip to Q20) | 21% |
| Total | 100% |

| Q19. What are the top two reasons for using or planning to use threat intelligence? Please select the top two reasons only. | Pct% |
|---|---|
| Stay current on emerging file-based attack techniques | 43% |
| Improve detection of suspicious or high-risk file behavior | 37% |
| Enrich alerts | 41% |
| Support threat hunting and investigation workflows | 50% |
| Meet compliance and/ or risk management requirements | 23% |
| Other (please specify) | 6% |
| Total | 200% |

| Q20. Is Software Bill of Materials (SBOM) part of your organization's file security strategy? | Pct% |
|---|---|
| Yes | 39% |
| Plan to use in 2026 | 26% |
| Interested, but no plans to use at this time (please skip to Q22) | 24% |
| No plan to use (please skip to Q22) | 11% |
| Total | 100% |

| Q21. What are the reasons for using or planning to use SBOM? Please select the top two reasons only. | Pct% |
|---|---|
| Identify vulnerabilities in third-party or open-source components | 49% |
| Improve visibility into software supply chain risks | 41% |
| Support secure development and DevSecOps practices | 34% |
| Assess risk in distributed or embedded software | 50% |
| Comply with government or industry regulations | 23% |
| Other (please specify) | 3% |
| Total | 200% |

| Q22. Does your organization use country of origin as part of your organization's file security strategy? | Pct% |
|---|---|
| Yes | 37% |
| Plan to use in 2026 | 40% |
| Interested, but no plans to use at this time (please skip to Q24) | 14% |
| No plan to use (please skip to Q24) | 9% |
| Total | 100% |

| Q23. What are the top two reasons for using or planning to use country of origin? Please select the top two reasons only. | Pct% |
|---|---|
| Neutralize zero-day or unknown threats | 51% |
| Remove active content or embedded threats | 41% |
| Improve operational efficiency | 49% |
| Reduce the IT/security team's workload | 31% |
| Meet compliance and/or audit requirements | 23% |
| Other (please specify) | 5% |
| Total | 200% |

**Part 4. The use of AI in organizations' file security strategy**

| Q24. Is Artificial Intelligence (AI) part of your organization's file security strategy? | Pct% |
|---|---|
| Yes | 33% |
| Plan to use in 2026 | 29% |
| Interested, but no plans to use at this time (please skip to Q31) | 27% |
| No plan to use (please skip to Q31) | 11% |
| Total | 100% |

| Q25. What are the top two reasons for using or planning to use AI? Please select the top two only. | Pct% |
|---|---|
| Improve operational efficiency | 33% |
| Reduce costs | 41% |
| Support the IT security team | 18% |
| Maintain competitive advantage | 28% |
| Reduce security risks | 50% |
| Improve malware detection rates | 27% |
| Other (please specify) | 3% |
| Total | 200% |

| Q26. Using the following 10-point scale, please rate the effectiveness of AI in enhancing file security maturity on a scale from 1 = low effectiveness to 10 = high effectiveness. | Pct% |
|---|---|
| 1 or 2 | 11% |
| 3 or 4 | 9% |
| 5 or 6 | 21% |
| 7 or 8 | 28% |
| 9 or 10 | 31% |
| Total | 100% |

| Q27. Has your organization adopted Generative AI? | Pct% |
|---|---|
| Yes, a formal policy exists | 25% |
| Yes, an ad hoc approach | 27% |
| No, Generative AI is banned | 29% |
| No | 19% |
| Total | 100% |

| Q28. If yes, does your organization use Generative AI to unlock files? | Pct% |
|---|---|
| Yes, in testing/pilot phase | 29% |
| Yes, in production | 18% |
| No, planned to implement | 33% |
| No plans to implement in the near future | 20% |
| Total | 100% |

| Q29. Does your organization take steps to secure sensitive corporate files in AI workloads? | Pct% |
|---|---|
| Yes | 37% |
| No | 63% |
| Total | 100% |

| Q30. If yes, what measures does your organization take to secure sensitive corporate files in AI workloads? Please select all that apply. | Pct% |
|---|---|
| Mask sensitive information | 38% |
| Check for malware | 36% |
| Use AI guardrails | 35% |
| Use prompt security tools | 41% |
| Other (please specify) | 2% |
| **Total** | 152% |

**Part 5. Threats to file security**

| Q31. Using the following 10-point scale, please rate your organization's confidence in the security of files during the file upload stage (internal/external) from 1 = low confidence to 10 = high confidence. | Pct% |
|---|---|
| 1 or 2 | 15% |
| 3 or 4 | 20% |
| 5 or 6 | 23% |
| 7 or 8 | 21% |
| 9 or 10 | 21% |
| Total | 100% |

| Q32. Using the following 10-point scale, please rate your organization's confidence in the security of files when downloading files from unknown sources from 1 = low confidence to 10 = high confidence. | Pct% |
|---|---|
| 1 or 2 | 15% |
| 3 or 4 | 18% |
| 5 or 6 | 23% |
| 7 or 8 | 21% |
| 9 or 10 | 23% |
| Total | 100% |

| Q33. Using the following 10-point scale, please rate your organization's confidence in the security of files when sharing files via email or links from 1 = low confidence to 10 = high confidence. | Pct% |
|---|---|
| 1 or 2 | 17% |
| 3 or 4 | 20% |
| 5 or 6 | 21% |
| 7 or 8 | 22% |
| 9 or 10 | 20% |
| Total | 100% |

| Q34. Using the following 10-point scale, please rate your organization's confidence in the security of files when transferring files to and from third parties from 1 = low confidence to 10 = high confidence. | Pct% |
|---|---|
| 1 or 2 | 22% |
| 3 or 4 | 13% |
| 5 or 6 | 26% |
| 7 or 8 | 23% |
| 9 or 10 | 16% |
| Total | 100% |

| Q35. Using the following 10-point scale, please rate your organization's confidence in the security of files when storing files in the cloud, on-premises or hybrid from 1 = low confidence to 10 = high confidence. | Pct% |
|---|---|
| 1 or 2 | 18% |
| 3 or 4 | 12% |
| 5 or 6 | 16% |
| 7 or 8 | 33% |
| 9 or 10 | 21% |
| Total | 100% |

| Q36. Using the following 10-point scale, please rate your organization's confidence in the security of backups (files, storage, servers, endpoints, workloads, etc.) from 1 = low confidence to 10 = high confidence. | Pct% |
|---|---|
| 1 or 2 | 14% |
| 3 or 4 | 13% |
| 5 or 6 | 20% |
| 7 or 8 | 22% |
| 9 or 10 | 31% |
| Total | 100% |

| Q37. How quickly does your organization detect and respond to file-based threats? Please select one choice only. | Pct% |
|---|---|
| Immediately (real time) | 14% |
| Within a few hours | 16% |
| Within a day | 25% |
| Within a week | 15% |
| More than a week | 10% |
| Don't know | 20% |
| Total | 100% |

| Q38. Which file-based channels or environments does your organization believe to be the biggest file security threat? Please select the top three choices only. | Pct% |
|---|---|
| Web file uploads (e.g., public portals, web forms) | 40% |
| Web file downloads (e.g., from websites or SaaS apps) | 39% |
| File storage (e.g., on-premises, NAS, SharePoint, etc.) | 42% |
| File shares & file transfers (e.g., MSMB, FTP, SFTP) | 23% |
| Collaboration platforms (e.g., Microsoft Teams, Slack, Google Drive) | 36% |
| Email attachments and links | 32% |
| SaaS applications (e.g., Salesforce, Dropbox) | 23% |
| Cloud storage or productivity suites (e.g., Google Workspace, Microsoft 365) | 29% |
| Open-source libraries or packages (e.g., GitHub, PyPl, npm | 33% |
| Other (please specify) | 3% |
| Total | 300% |

| Q39. Which types of malicious content has your organization encountered or are most concerned about in files? Please select the top three choices only. | Pct% |
|---|---|
| Ransomware | 39% |
| Trojans | 28% |
| Macro-based malware (e.g., in Office files) | 44% |
| Remote Code Execution (RCE) exploits via vulnerabilities | 31% |
| Obfuscated scripts | 31% |
| Zero-day or unknown malware | 43% |
| Embedded URLs leading to malicious sites | 28% |
| Hidden payloads in images or PDFs | 19% |
| Exploits targeting known file parsing vulnerabilities | 36% |
| Other (please specify) | 1% |
| Total | 300% |

| Q40. Which OWASP principles to secure file upload implementation has your organization implemented or plan to implement in the future? Please select all that apply. | Pct% |
|---|---|
| Only allow safe file extensions | 24% |
| Validate the file type to prevent spoofing | 28% |
| Change the filename to something generated by the application | 24% |
| Run the file through CDR | 29% |
| Set a filename length limit | 29% |
| Set a file size limit | 19% |
| Only allow authorized users to upload files | 31% |
| Store the files on a different server | 40% |
| Run files through an antivirus or a sandbox | 28% |
| Ensure any libraries used are securely configured and kept up to date | 29% |
| Protect the uploads from Cross-Site Forgery (CSRF) attacks | 29% |
| Total | 310% |

**Part 6. Organizational and respondents' demographics**

| D1. What best describes your position level within the organization? Please select one choice only. | Pct% |
|---|---|
| C-level executive | 8% |
| Executive/VP | 6% |
| Director | 21% |
| Manager | 14% |
| Supervisor | 10% |
| Staff/technician | 20% |
| Administrative | 9% |
| Consultant/contractor | 7% |
| Other (please specify) | 5% |
| Total | 100% |

| D2. What best describes your reporting channel or chain of command? | Pct% |
|---|---|
| CEO/executive committee | 6% |
| COO or head of operations | 5% |
| CFO, controller or head of finance | 0% |
| CIO or head of corporate IT | 12% |
| CPO or head of privacy or data protection | 3% |
| Business unit leader or general manager | 13% |
| Head of compliance or internal audit | 15% |
| Head of enterprise risk management | 21% |
| Head of cybersecurity | 18% |
| Other (please specify) | 7% |
| Total | 100% |

| D3. What best describes your organization’s primary industry classification? | Pct% |
|---|---|
| Communications | 3% |
| Consumer products | 5% |
| Defense & aerospace | 2% |
| Energy & utilities | 6% |
| Entertainment & media | 3% |
| Financial services | 17% |
| Healthcare providers and services | 8% |
| Pharmaceutical | 4% |
| Healthcare equipment and supplies | 3% |
| Hospitality | 4% |
| Industrial | 8% |
| IT & technology | 9% |
| Logistics & distribution | 2% |
| Manufacturing | 7% |
| Public sector | 4% |
| Retail | 5% |
| Services | 7% |
| Transportation | 3% |
| Other (please specify) | 0% |
| Total | 100% |

| D4. What range best describes the full-time headcount of your global organization? | Pct% |
|---|---|
| Less than 500 | 14% |
| 500 to 1,000 | 12% |
| 1,001 to 5,000 | 13% |
| 5,001 to 10,000 | 20% |
| 10,001 to 25,000 | 21% |
| 25,001 to 75,000 | 12% |
| More than 75,000 | 8% |
| Total | 100% |

**For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or call at 1.231.938.8800.**

**Ponemon Institute**
***Advancing Responsible Information Management***

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.