Cybersecurity INSIDERS

2023 Content Security Report

Trends & Best Practices for File Security

VOTIRO

Overview

Content security is a critical concern in today's digital ecosystem, as a growing majority of devastating attacks originate from file-borne threats. We share and receive more content and file formats than ever – through emails, web browsers, cloud apps, and direct transfers – thereby significantly increasing the risk of attacks that utilize weaponized files.

As the attack surface expands and threat actors devise more sophisticated methods to infiltrate organizations, traditional signature-based file security methods prove increasingly inadequate. The dramatic rise in breaches involving malicious files shows that innovative security technologies, such as Content Disarm & Reconstruction (CDR), are essential to address these evolving threats more effectively.

The 2023 Content Security Report, Trends & Best Practices for File Security, provides a deep dive into today's file security landscape and reveals the latest file attack tactics, primary points of entry and their vulnerabilities, and the measures necessary to tackle file-borne threats.

Key findings include:

- **Entry Points and Vulnerabilities:** Files predominantly enter organizations via email (74%), content collaboration and cloud storage (52%), and web downloads to endpoints (50%). Those channels are also recognized as the most vulnerable to file-borne threats.
- **Visibility Concerns:** Over a third of organizations (36%) lack comprehensive visibility into the channels through which files enter. This not only amplifies the risk of undetected threats entering organizations but also negatively affects compliance with regulations governing the handling of sensitive information.
- **File-Borne Security Incidents:** A significant 38% of respondents confirmed their organizations experienced a security incident originating from a malicious file. Another 33% believe this possibly occurred in their organizations. This combined 71% of confirmed and suspected incidents is alarmingly high and signals that current file security measures are largely insufficient.
- **Defensive Measures:** When it comes to countering file-borne threats, 78% rely on antivirus and endpoint security. However, more advanced measures like Content Disarm & Reconstruction are employed by only 33%, suggesting there's room for the adoption of more evolved defenses.

We would like to extend our gratitude to Votiro for their invaluable contribution to this survey.

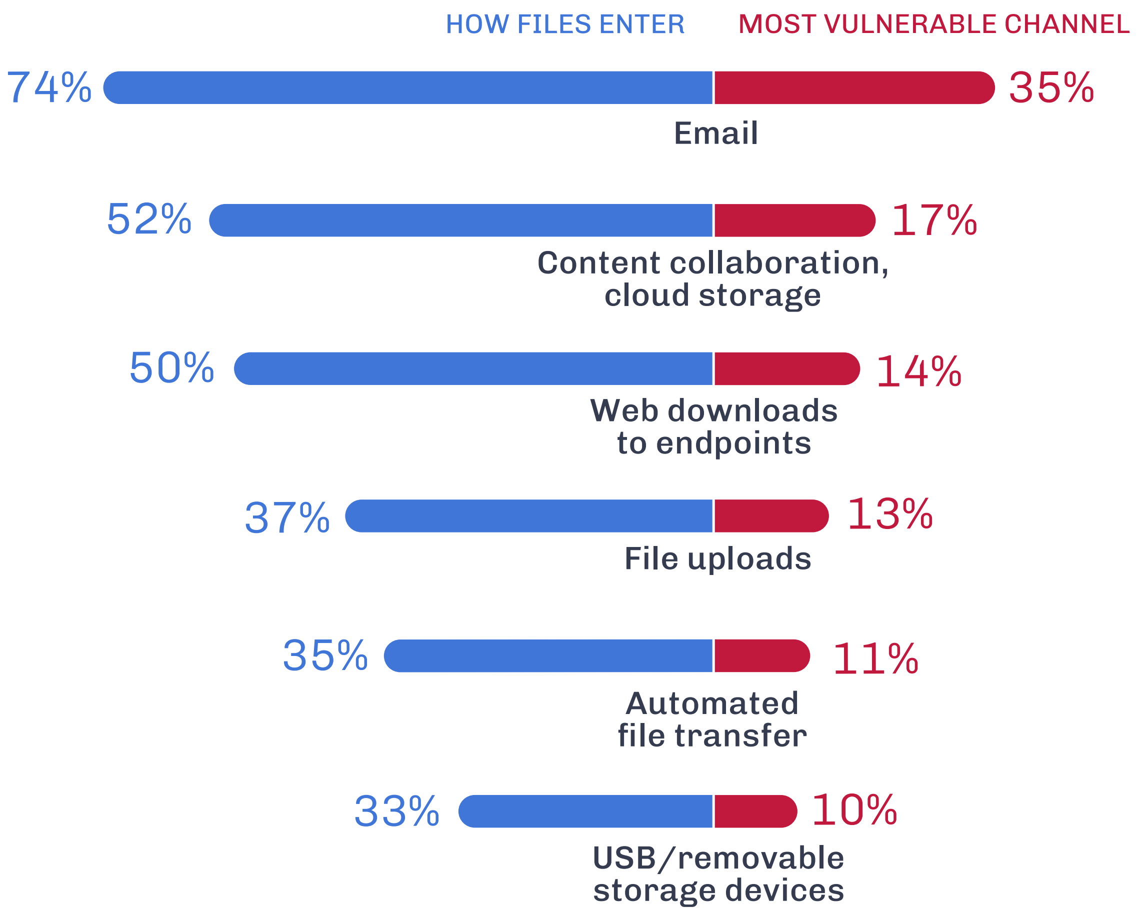
We hope the insights and best practices presented in this report will provide a comprehensive guide for organizations looking to strengthen their content security posture.

Risky File Entry Paths

The contrasting perceptions between common file entry methods and their associated vulnerabilities offer interesting insights for cybersecurity professionals. Email, for instance, was cited by 74% of respondents as one of the most common entry points, and concurrently, 35% marked it as the most vulnerable channel. This high frequency coupled with a high perception of risk makes email a priority for rigorous security measures. What's also noteworthy is the discrepancy between the use and perceived risk of content collaboration platforms and cloud storage. While 52% confirm this is how files enter their organization, only 17% perceive them as high-risk. This could signal an underestimation of the risk involved, thereby leaving a potential security blind spot.

Organizations should aim for a balanced cybersecurity approach that matches perceived risk with actual usage. Since email emerges as both a common and risky channel, its security should be a high priority, employing real-time threat detection and Content Disarm and Reconstruction (CDR) technologies. The relatively neglected areas like content collaboration platforms should not be overlooked, as their high usage rate could make them an attractive target for attackers. Leveraging real-time file sanitization techniques across all channels can offer an added layer of protection.

How do files most commonly enter your organization and which channel is most vulnerable to file-borne threats in your organization?



Balancing Security and User Experience

Content security is undeniably critical, but its impact on the user experience and business operations should not be underestimated. It's noteworthy that 46% of respondents indicate that current security measures increase the workload for security teams, often due to excessive alerts or false positives. This effect could stretch already limited resources and compromise the overall cybersecurity posture.

Interestingly, 37% note that current security measures are triggering complaints from business users, implying that the user experience is impacted to a level that users are vocalizing dissatisfaction.

Additionally, 35% indicate that security measures either create inefficiencies in business processes or slow down file transfers (33%). These two closely related issues can have significant repercussions on productivity and operational speed.

Given the complexities, it's essential for organizations to adopt file security solutions that are not only robust but also streamlined for positive user experience and operational efficiency. Implementing solutions that offer real-time, intelligent alert systems can reduce the security team's workload while still maintaining a high level of protection. Moreover, opting for solutions that offer seamless integration with existing systems can mitigate slow file transfer times and inefficiencies.

How does your current file security process impact the user experience or business?

1 **Increases workload for the security team**
46%

2 **Triggers complaints from business users**
37%

3 **Slows down business processes**
35%

4 **Slows down file transfer process**
33%

5 **Breaks files**
(flattens or damages files, impacting usability)
31%

6 **No negative impact**
23%

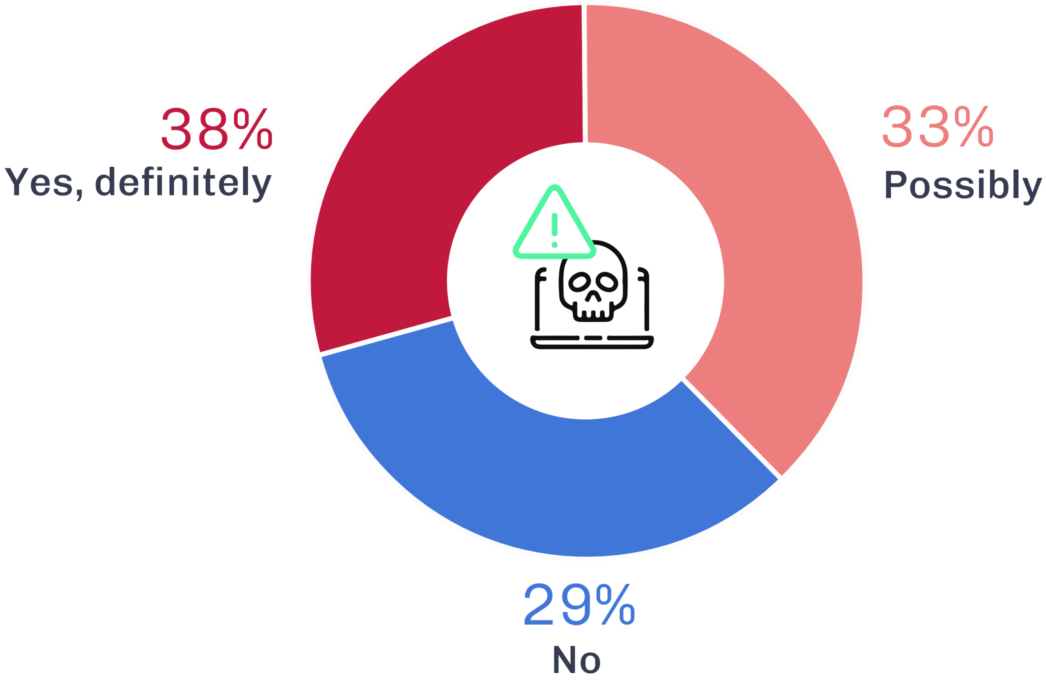
Malicious File Incidents

Understanding the frequency of incidents related to malicious files provides valuable metrics for evaluating the efficacy of an organization's cybersecurity posture. This is particularly crucial as organizations rely increasingly on a variety of file transfer methods, each with their own security implications.

The most telling data point is that more than one-third of respondents (38%) have definitively experienced an incident due to a malicious file in the past year. This is alarmingly high and signals that current file security measures are insufficient. Furthermore, the 33% that stated they possibly experienced an incident suggests a lack of full visibility into their file security posture.

Given the high percentage of known and possible incidents, organizations should conduct a thorough risk assessment of their current file security strategies, evaluating the types of files entering their environment and the associated security measures. Consider deploying more advanced technologies that go beyond traditional anti-malware tools; solutions that can disassemble, analyze, and reconstruct incoming files to neutralize threats without affecting usability may offer a more effective security layer.

In the past 12 months, has your organization experienced an incident due to a malicious file?



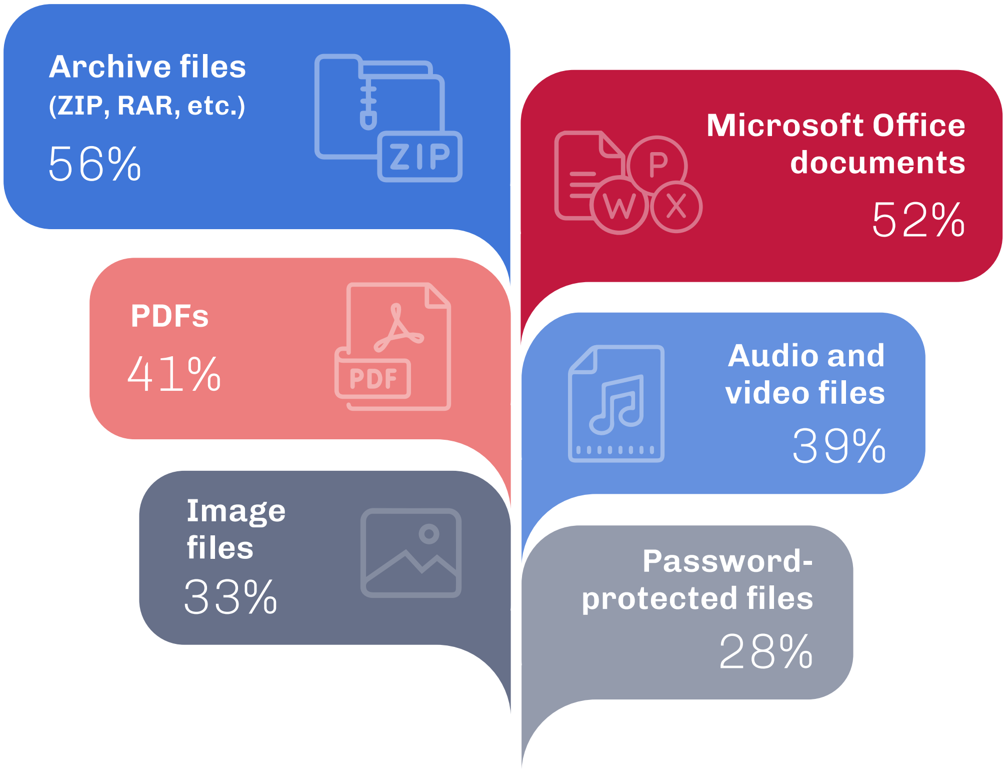
High-Risk File Formats

File formats vary not only in their functionality but also in the level of risk they pose to an organization's IT environment. Understanding which formats are considered risk-prone is critical for implementing targeted Content Disarm and Reconstruction (CDR) solutions and other advanced security measures.

Archive files like ZIP and RAR top the list, with 56% considering them to be of highest risk, followed closely by Microsoft Office documents at 52%. The high number of survey participants who consider Microsoft Office files risky is striking given the suite's widespread use in organizations. This highlights the urgent need for specialized security for these common, yet vulnerable file types frequently used in cyber attacks. PDFs are also a significant concern at 41%, likely due to their complexity and ability to carry embedded malicious code. On the other hand, audio and video files, which are typically considered less traditional vectors for attacks, have a significant perception of risk at 39%.

Organizations should tailor their file security solutions to focus on these high-risk formats. A Zero Trust approach to files, especially for commonly-used but risky formats, should be the cornerstone of an effective cybersecurity strategy. Advanced CDR solutions can prove invaluable, as they dissect and neutralize potentially harmful elements in various file formats without disrupting business operations.

Which file formats do you consider to be of highest risk for your IT environment, potentially necessitating CDR?



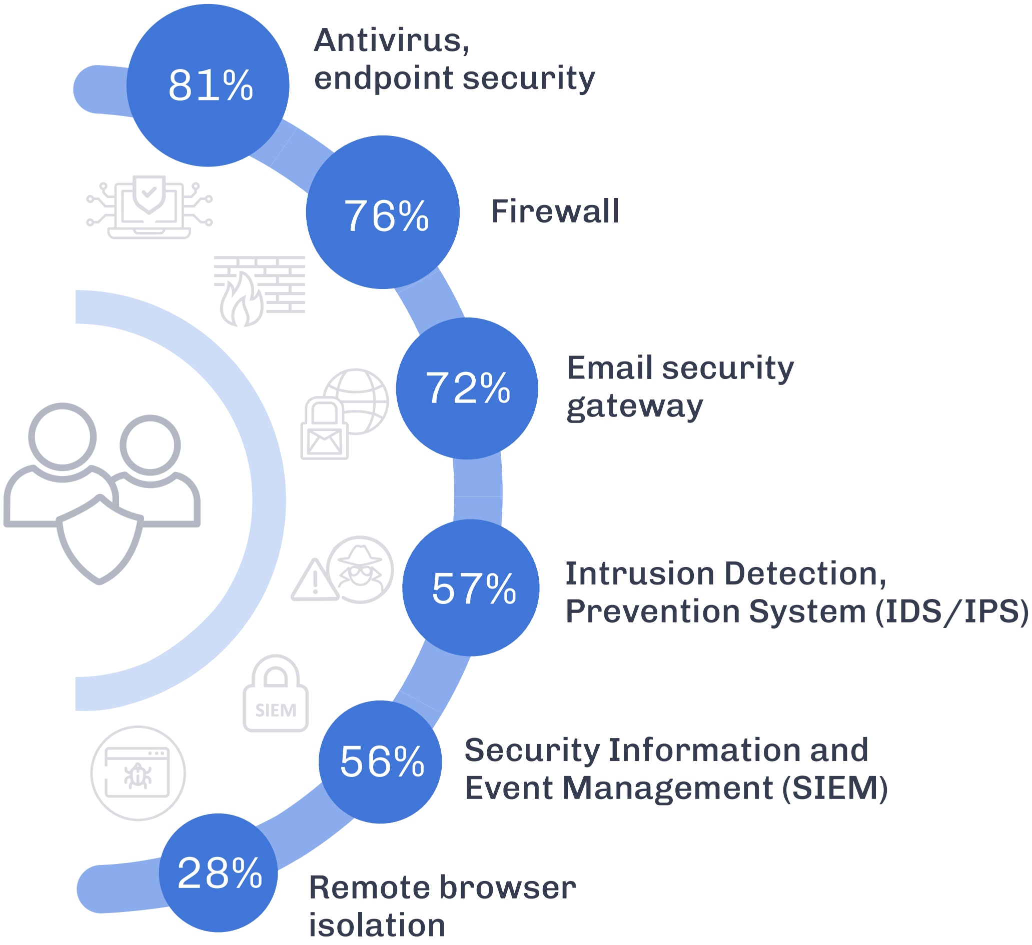
Cybersecurity Tools Landscape

Understanding which cybersecurity solutions are deployed is crucial for comprehending the defense matrix of an organization. This also helps to identify any potential gaps that need to be addressed for a comprehensive security posture.

The data shows a clear prioritization of foundational solutions, with antivirus/endpoint security (81%), firewall (76%), and email security gateway (72%) leading the pack. Intrusion Detection/Prevention Systems (IDS/IPS) and Security Information and Event Management (SIEM) hold the middle ground at 57% and 56%, respectively.

Organizations are advised to reassess their security stack, paying close attention to advanced solutions that complement traditional tools for a more robust cybersecurity posture. Considering solutions that proactively disarm file-borne threats, rather than just detecting them, can add an extra layer of security that's particularly useful in today's landscape of increasingly sophisticated attacks.

Which of the following cybersecurity solutions does your organization currently use?



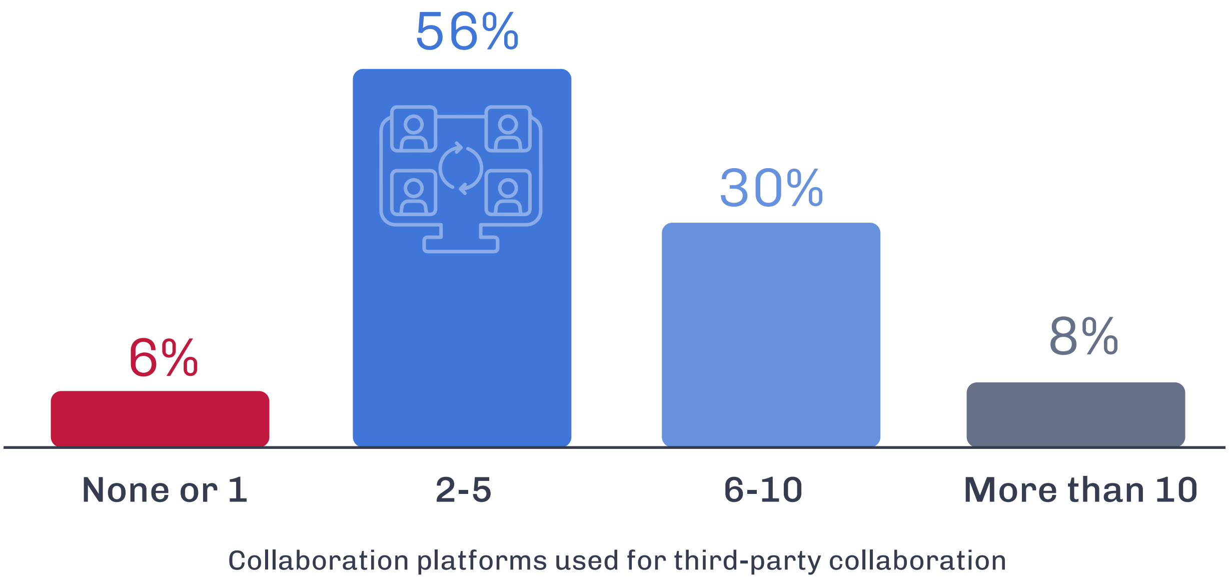
Collaboration Platform Complexity

In today's interconnected, digital-first business ecosystem, the number of collaboration platforms an organization uses is often indicative not only of its size and complexity but also of its vulnerability surface. As the frequency and depth of third-party interactions grow, so does the importance of securing the numerous channels through which files may enter an organization.

More than half of the organizations (56%) are using between 2 and 5 collaboration platforms (such as Salesforce, Slack, and SharePoint) for third-party collaboration, emphasizing the growing reliance on these tools. A surprising 30% report using 6 to 10 platforms, which speaks to the extensive, yet potentially convoluted, digital environment that companies are operating in. The 8% of organizations using more than 10 platforms likely have a considerable challenge in ensuring file security across all these vectors.

Managing file security becomes exponentially complex with the increase in the number of collaboration tools. Organizations should seek scalable solutions that can seamlessly integrate with a variety of platforms, ensuring uniform security protocols. This adaptability allows companies to stay ahead of threats regardless of the source or the type of files being shared.

Approximately how many collaboration platforms (e.g., Salesforce, Slack, SharePoint, Box) does your organization use for third-party collaboration?

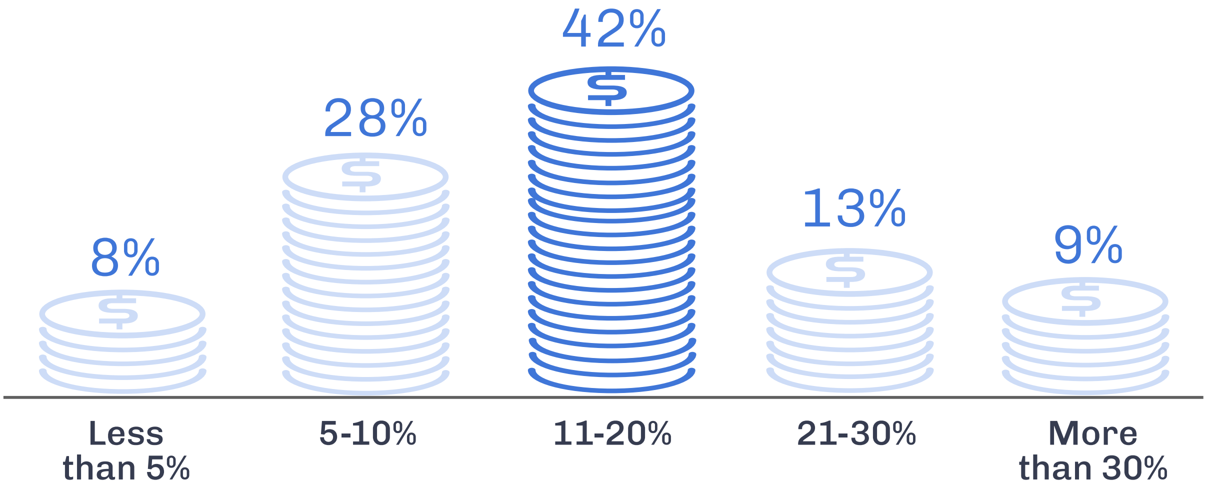


Cybersecurity Budget Allocation

Understanding the portion of the IT budget allocated to cybersecurity is a sound indicator in gauging an organization's readiness to defend against digital threats. Notably, the largest percentage of organizations (42%) are investing 11-20% of their IT budget in cybersecurity measures. Surprisingly, a not-insignificant 9% allocate more than 30% of their IT budget towards cybersecurity, indicating a higher awareness of its criticality, perhaps depending on the nature of the business. On the lower end, only 8% invest less than 5% of their budget in cybersecurity.

Organizations should reassess their cybersecurity investment relative to the current threat landscape, particularly if they fall into the 8% allocating less than 5%. For those organizations that may find it challenging to increase their cybersecurity budget immediately, leveraging innovative and more effective technologies can offer better protection with existing resources. Investing in adaptive Content Disarm and Reconstruction (CDR) technology can not only enhance your existing tech stack but potentially replace less effective solutions, making it a cost-effective approach to file security.

What percentage of your organization's IT budget is allocated to cybersecurity?



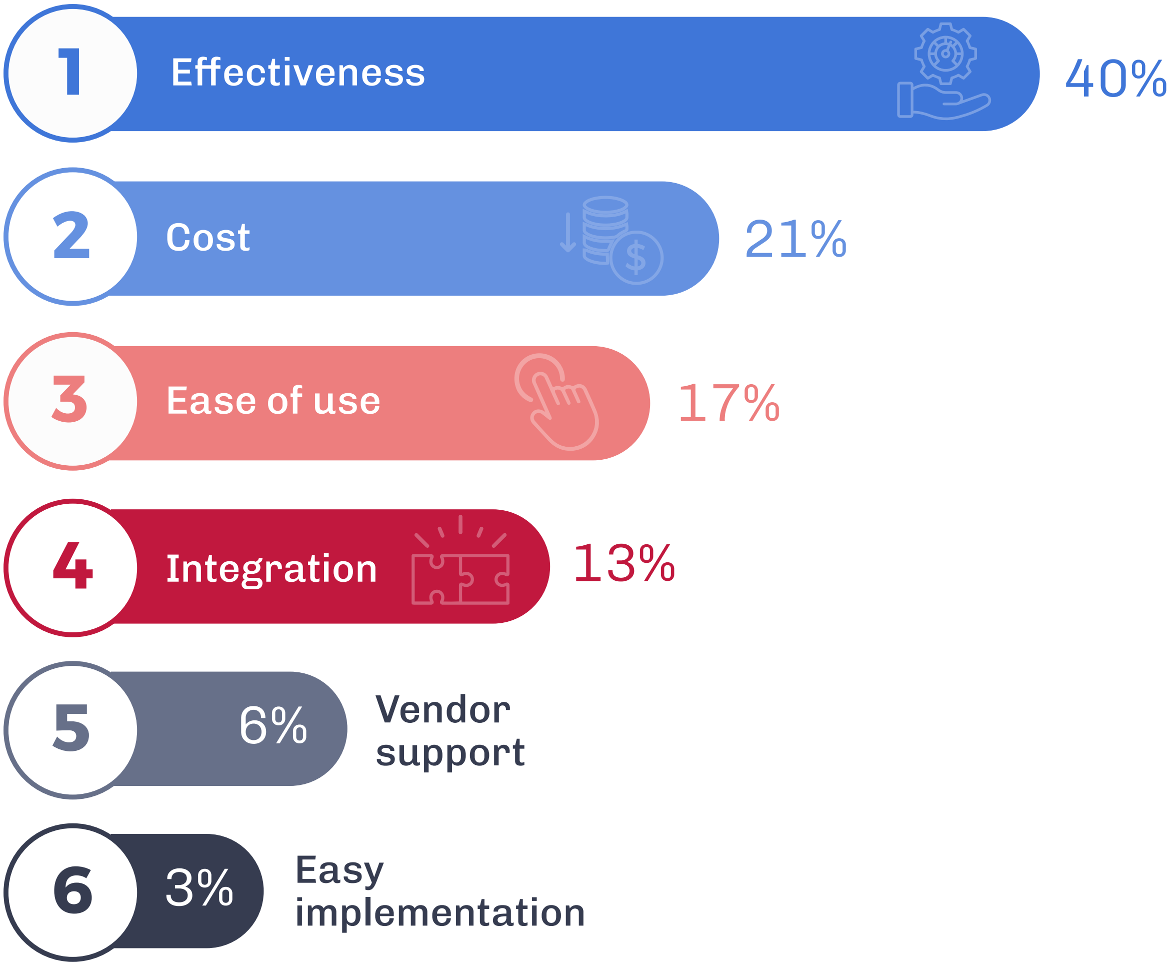
Percentage of IT budget allocated to cybersecurity

Cybersecurity Selection Criteria

When it comes to adopting new cybersecurity solutions, organizations rank effectiveness against advanced threats (40%) as the most important factor, followed by cost considerations (21%) and ease of use (17%). This emphasis on capability against sophisticated threats showcases a keen awareness of rapidly evolving cybersecurity risks. On the flip side, factors like vendor reputation and support scored lower, revealing that companies are somewhat less swayed by brand reputation than by efficacy.

Given these findings, organizations should rigorously evaluate the efficacy of potential cybersecurity solutions against advanced threats as their first criterion. As a secondary focus, the cost-effectiveness of the solution should also be scrutinized, but without compromising quality. It may be beneficial to look into next-gen technologies that have a high efficacy in neutralizing advanced threats while also being cost effective and easy to deploy.

Which factors are most important when considering new cybersecurity solutions?

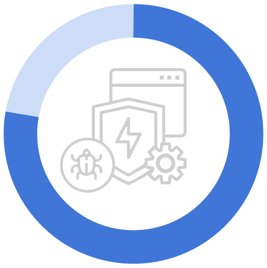


File-Borne Threat Defenses

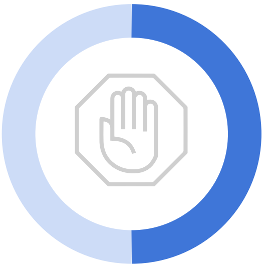
File-borne threats are a significant vector for cyber attacks, which makes the selected modes of protection pivotal. A notable majority (78%) rely on antivirus software, which although essential is not always sufficient against more advanced threats. Half of the respondents (50%) take the measure of blocking zipped and password-protected files, and nearly as many use intrusion detection and prevention (48%). However, measures like blocking files outright or stripping their function can impede business operations and render the files useless.

Given these insights, companies should consider a multi-layered approach for mitigating file-borne threats. While antivirus solutions serve as a basic line of defense, they should be complemented with more advanced technologies such as CDR, which can effectively neutralize unknown and zero-day threats in files. Incorporating a well-architected blend of these methods can provide a more comprehensive file security stance.

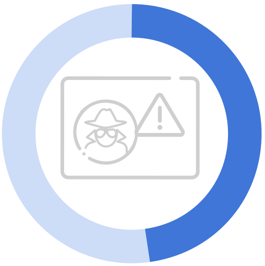
When it comes to file-borne threats, how are you currently protecting your organization?



78%
Antivirus software



50%
Blocking zipped and password-protected files



48%
Intrusion Detection, Prevention Systems (IDS/IPS)

43%
File integrity monitoring

33%
Content Disarm & Reconstruction (CDR)

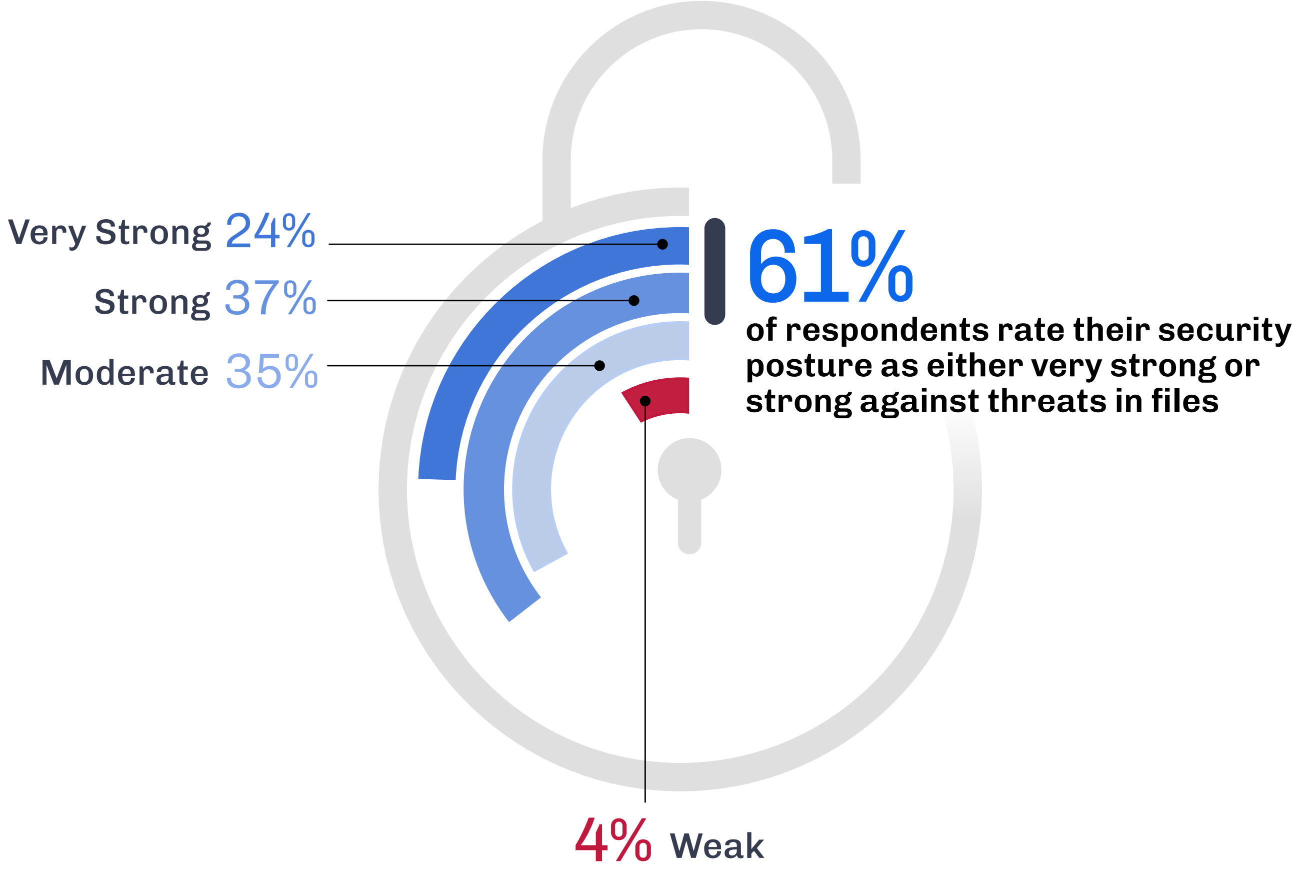
26%
Sandboxing

File Security Confidence

File threats are a relentless and ever-evolving challenge in cybersecurity. 61% of respondents rate their security posture as either very strong or strong against threats in files, both known and unknown. However, another 35% perceive their defenses as merely moderate, and a concerning few (4%) even consider their posture weak.

The evident confidence among the majority suggests that many organizations feel adequately prepared for file-based threats, but this self-assessment may not necessarily reflect the reality of an ever-evolving threat landscape. To ensure this confidence is well-placed, organizations should routinely audit their current security measures against emerging threat vectors and integrate advanced technologies capable of handling unknown risks in files.

How would you rate your organization's current security posture in terms of protection against threats in files (known & unknown)?



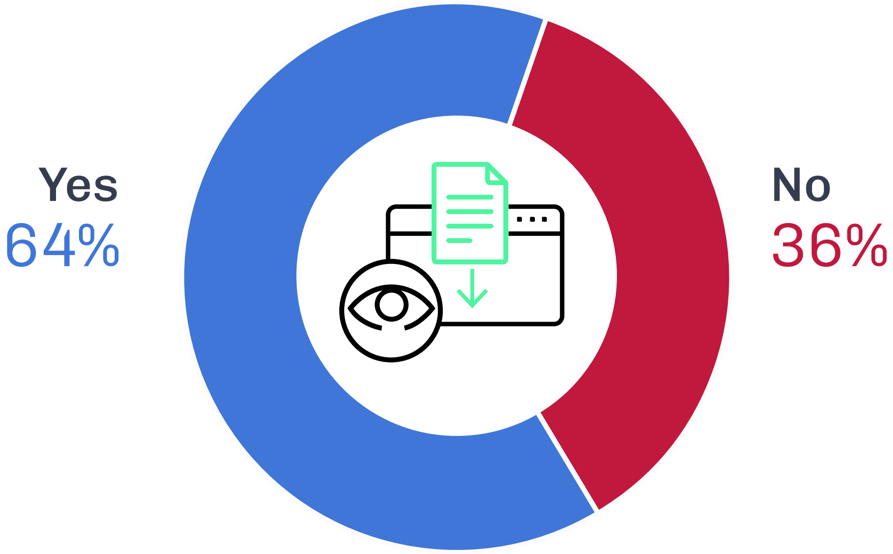
Visibility Gaps

Because you can only manage what you can observe, visibility into every channel through which files enter an organization is foundational to building a strong security posture. In the survey, a significant majority of respondents (64%) believe they have full visibility into all entry points. However, 36% indicated that they lack such comprehensive insight.

The sizable portion lacking full visibility should raise concerns, as it leaves a considerable margin for error and vulnerability. This gap suggests that despite advancements in cybersecurity technologies, many organizations are still blind to many of the paths through which threats can infiltrate their systems. To remedy this, organizations should consider incorporating comprehensive monitoring and analytics solutions that offer an end-to-end view of file entry points.

Gaining full visibility into all the channels through which files enter your organization isn't just about improving security; it's also a catalyst for demonstrating ROI. By identifying gaps and actively thwarting threats, security teams can tangibly prove the value and effectiveness of their security solutions.

Do you feel like you have visibility into all the channels through which files enter your organization?

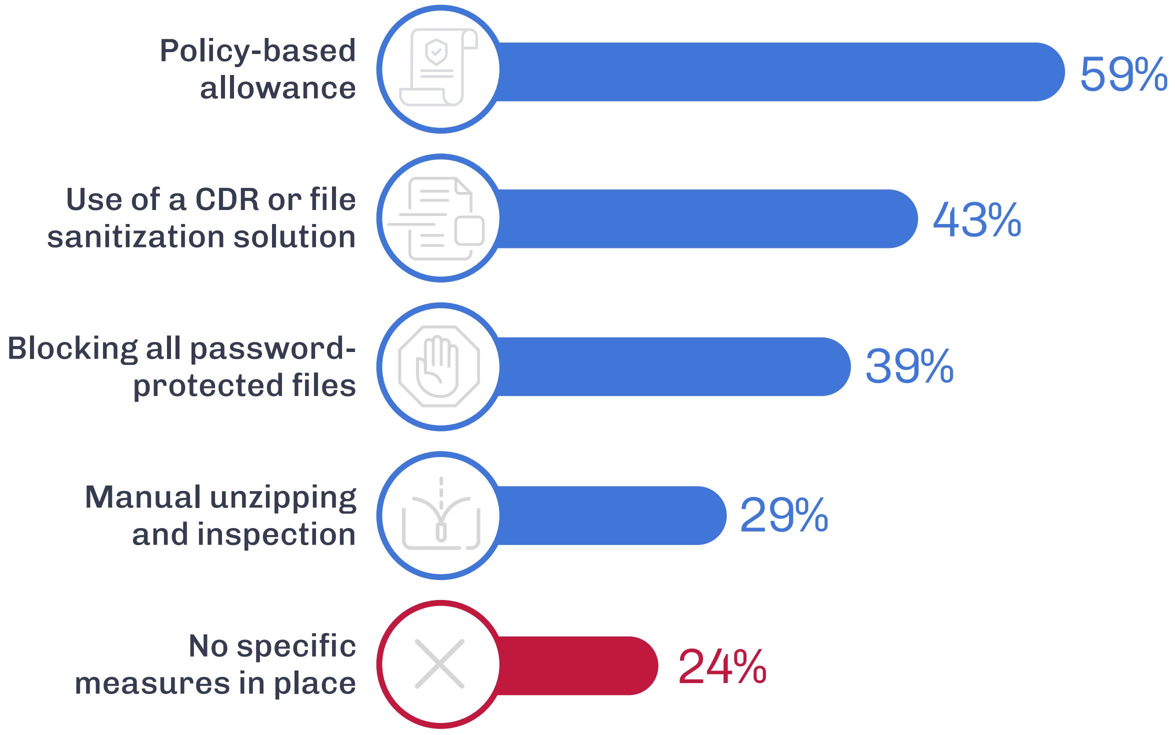


Securing Encrypted Files

Password-protected or encrypted files can often serve as Trojan horses for hidden threats. A substantial 59% of respondents rely on policy-based allowance of such files, which can be both effective but also risky if policies are circumvented or not regularly updated. Additionally, 43% deploy a CDR or file sanitization solution for this specific issue.

Surprisingly, 24% have no specific measures in place at all— a gaping vulnerability. The absence of any measures by a quarter of respondents is concerning and calls for immediate action. Organizations should strongly consider modern security solutions designed to disarm threats in encrypted files without impacting business operations.

How do you protect against hidden threats in password-protected or other encrypted files?

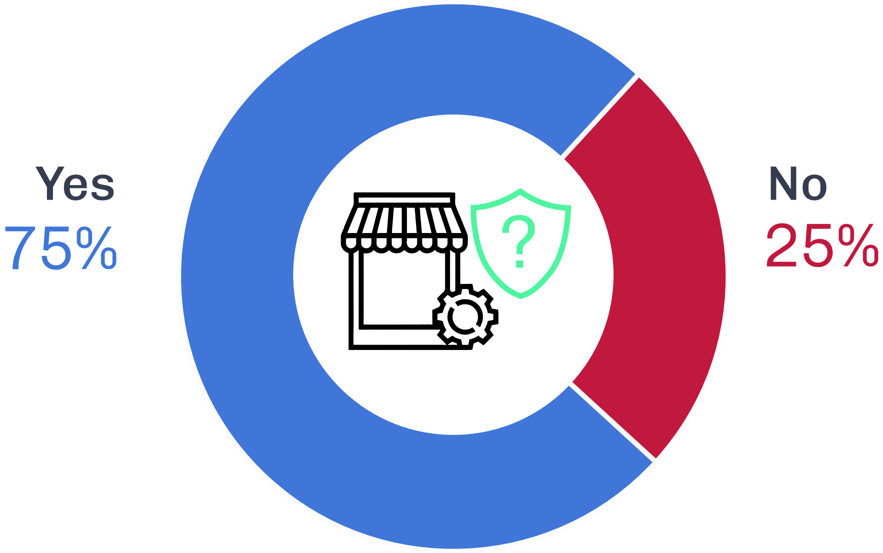


Trust in Third Parties

Third-party risk management, including vendors, partners, and customers, is a cornerstone of a robust cybersecurity posture. The survey reveals that 75% of respondents trust the security measures of their third-party associates, which might indicate a high level of confidence but could also be a point of vulnerability if that trust is misplaced, especially when considering recent high-profile security breaches involving third-party vulnerabilities.

On the flip side, the 25% who do not trust third parties' security measures are appropriately skeptical. If the majority's trust is based on thorough third-party risk assessments and regular audits, that's positive. However, it's crucial to underscore the importance of a Zero Trust approach— always verify, never trust– thereby ensuring robust protection even when a trusted source is compromised unknowingly. An organization should implement additional security measures, such as CDR technology, when receiving files from third parties to ensure that trust is supplemented with robust security measures.

Do you trust the security measures of third parties (vendors, partners, and customers) you work with?

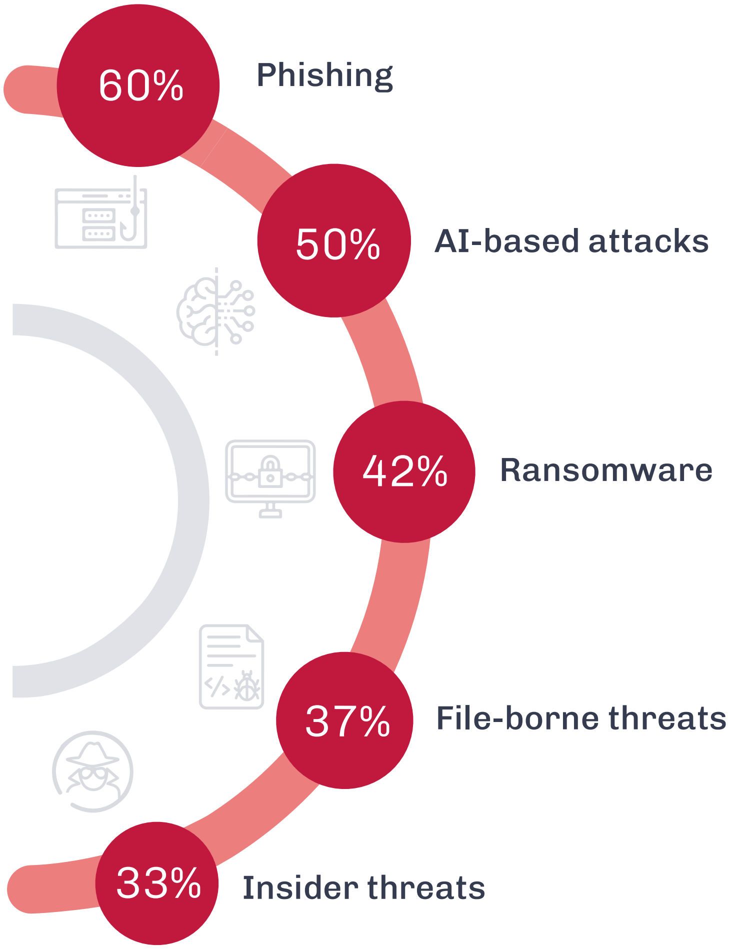


Future Threat Landscape

Understanding and anticipating future threats is crucial for proactive cybersecurity planning. The survey indicates that phishing is expected to be the most prevalent threat in the next 2-3 years, selected by 60% of respondents. AI-based attacks follow closely at 50%, while ransomware comes in third at 42%.

It's noteworthy that these top concerns span different vectors and methods, from social engineering to advanced technology-based threats. Given the diverse set of challenges on the horizon, a multi-layered security approach is crucial. Leveraging technologies that can address a wide range of threats, from phishing prevention to mitigating risks from advanced, file-borne malware, will be increasingly important. Strategically augmenting existing cybersecurity solutions with emerging technologies can provide comprehensive protection against both known and unknown future threats.

Which cybersecurity threats or challenges do you expect to become more prevalent in the next 2-3 years?



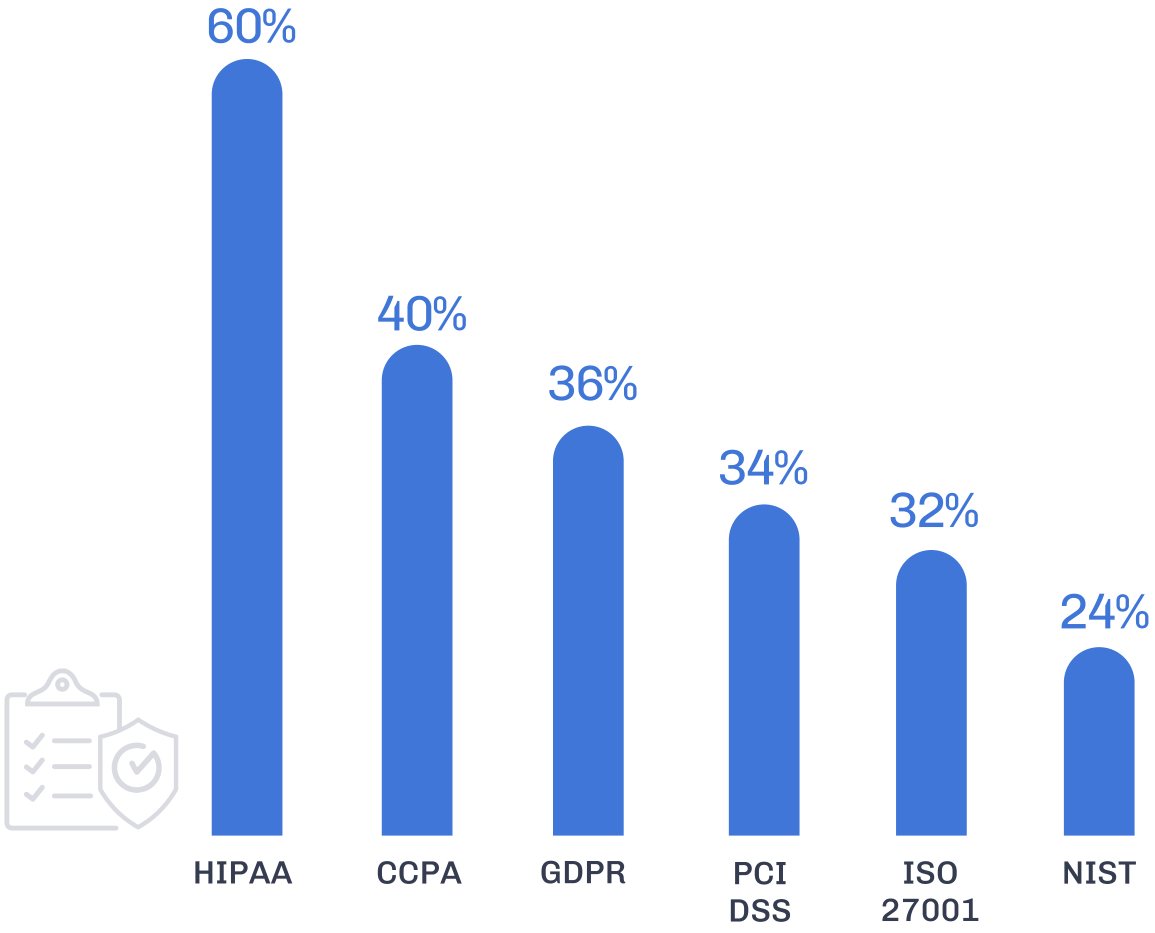
Supply chain attacks 31% | Advanced Persistent Threats (APTs) 29% | Zero-day exploits 27%

Compliance Complexity

Adhering to industry standards and regulatory frameworks is an obligatory facet of modern cybersecurity. Among the compliance mandates, HIPAA takes the lead with 60% of respondents acknowledging its relevance for their organization, followed by CCPA at 40% and GDPR at 36%.

The spread of compliance requirements across many different standards reveals a complex regulatory landscape that organizations must navigate. The implication here is a call for flexible cybersecurity solutions that can meet and adapt to multiple compliance requirements to reduce the complexity and resource strain involved in meeting these multifaceted regulatory demands.

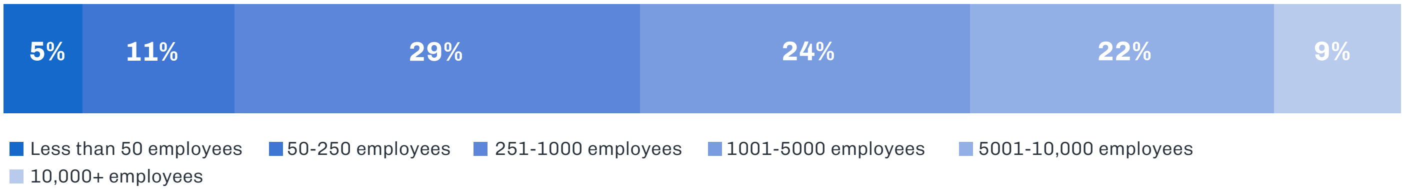
Which of the following compliance and regulatory requirements apply to your organization?



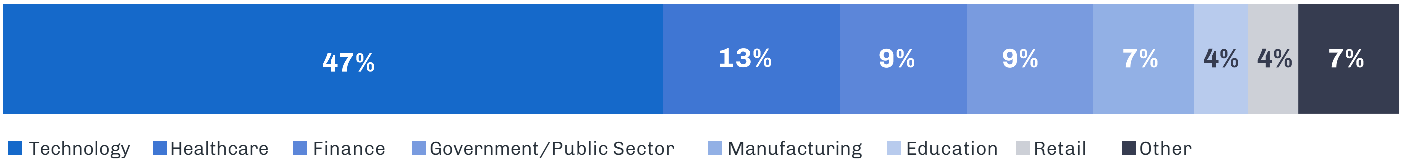
Methodology and Demographics

This 2023 Content Security Report, Trends & Best Practices for File Security, is based on the results of a comprehensive online survey of 342 cybersecurity professionals, conducted in September 2023, to gain deep insight into the latest trends, key challenges, and solutions. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

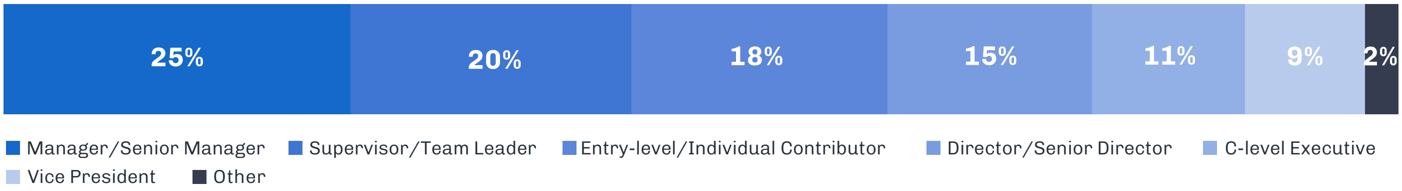
Company size



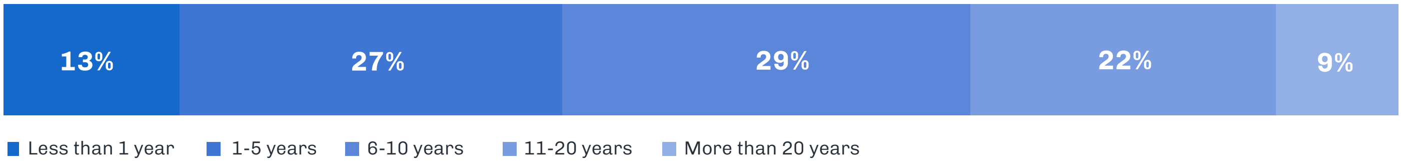
Primary industry



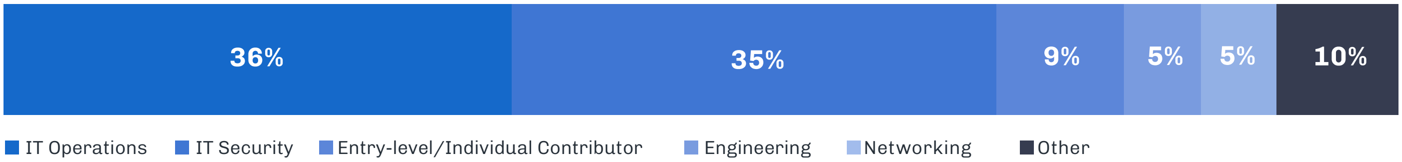
Career level



Years of experience



Job function



About Votiro

Votiro is a Zero Trust Content Security company trusted by industry leaders around the world to deliver billions of safe files between commercial and government organizations, their employees, and the customers that rely on them. The Votiro Cloud solution is an open-API that detects, disarms, and analyzes content at the speed of business – delivering teams with fully-functional files, reduced risk, lower costs, and increased productivity. Votiro Cloud proactively eliminates file-borne threats targeting email environments, collaboration platforms, data lakes, supply chains, web downloads, B2C digital interactions, and more.

Votiro is headquartered in Austin, TX, with offices in Australia, Israel, and Singapore. Votiro Cloud is SOC 2 Type II compliant and certified by the international standard of Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408). Learn more at **www.votiro.com**.

SCHEDULE A DEMO

VOTIRO

Cybersecurity

INSIDERS

Cybersecurity Insiders brings together 600,000+ IT security professionals and world-class technology vendors to facilitate smart problem-solving and collaboration in tackling today's most critical cybersecurity challenges.

Our approach focuses on creating and curating unique content that educates and informs cybersecurity professionals about the latest cybersecurity trends, solutions, and best practices. From comprehensive research studies and unbiased product reviews to practical e-guides, engaging webinars, and educational articles - we are committed to providing resources that provide evidence-based answers to today's complex cybersecurity challenges.

Contact us today to learn how Cybersecurity Insiders can help you stand out in a crowded market and boost demand, brand visibility, and thought leadership presence.

Email us at info@cybersecurity-insiders.com or visit cybersecurity-insiders.com