Cybersecurity
INSIDERS

2023

RANSOMWARE REPORT

BULLWALL

INTRODUCTION

In the ever-evolving landscape of ransomware threats, cybersecurity professionals must reassess defense strategies and proactively stay ahead of these menacing cyber-attacks. This 2023 Ransomware Report presents insights gathered from a survey of 435 cybersecurity professionals, shedding light on organizations' preparedness and approaches to combating ransomware. The report identifies gaps and obstacles that hinder robust security posture, and outlines strategies for prevention and remediation of ransomware attacks.

Key findings from the survey include:

- There is an increased likelihood of ransomware attacks, with 79% of respondents saying a threat is moderately to extremely likely within the next year.
- Despite the high levels of successful ransomware attacks, organizations remain highly confident in their defensive abilities: 40% of respondents are very or extremely confident in their organization's ability to detect and block threats, while 38% are moderately confident.
- Organizations perceive that customer information (65%), financial data (55%), and employee information (50%) are the data categories most vulnerable to ransomware attacks.
- The most significant negative organizational impacts of ransomware attacks include productivity loss (42%), followed by increased IT security spending (40%) and a significant shift in security strategy towards mitigation (33%).
- Recovery time expectations are optimistic, with 73% of respondents believing they can recover from an attack within a few days. However, other research suggests recovery can take weeks or even months.
- The primary obstacles in enhancing defense strategies are the evolving sophistication of attacks (47%) and budget constraints (45%).

These findings underscore the need to shift from a solely preventive approach, such as relying on EDR, to a more comprehensive strategy that includes swift containment of ongoing attacks. Implementing solutions that can rapidly shut down active attacks enables organizations to limit the inflicted damage, reduce recovery time, and better protect their valuable data and operations.

We thank BullWall for their invaluable support in conducting this essential research. We hope this report will provide informative insights and help you in your ongoing efforts to protect your organization against evolving threats.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

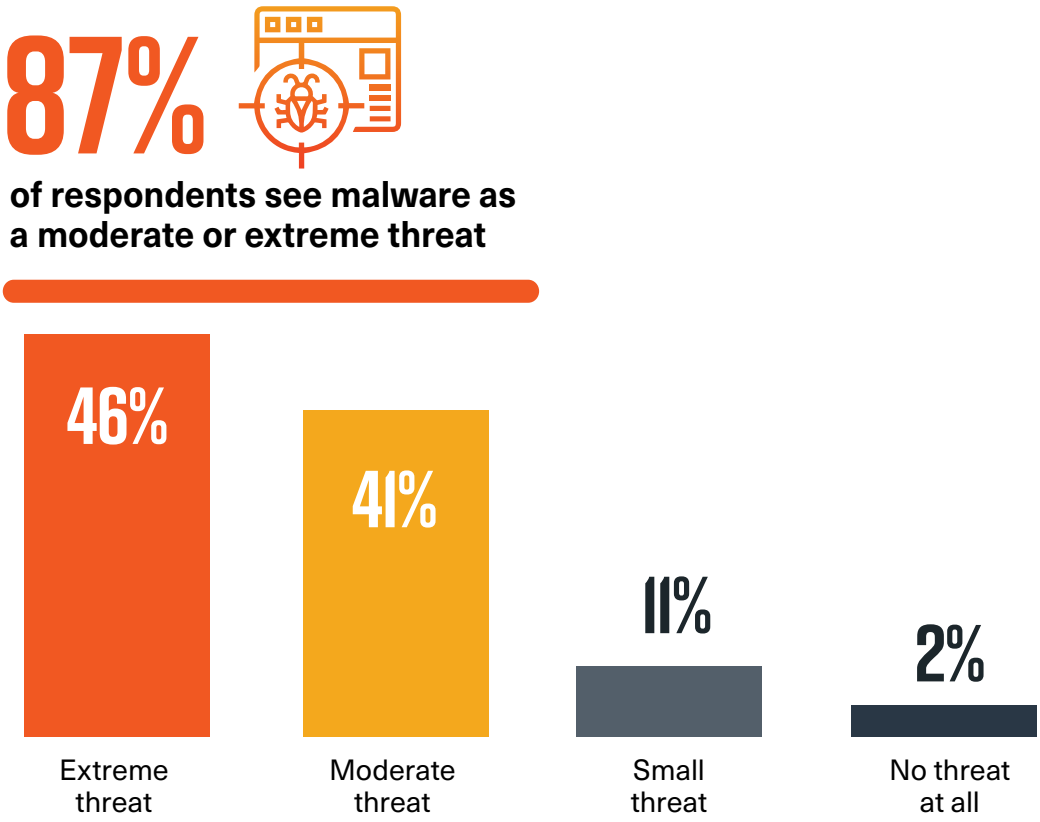
Cybersecurity
INSIDERS

RANSOMWARE THREAT

As cybercriminals continue to evolve their tactics and methods, the risk of ransomware attacks has become more significant, making it crucial for businesses to protect their critical data and IT infrastructure.

A majority of respondents (87%) see ransomware as a moderate to extreme threat to their business. This shows a high level of awareness and concern regarding the potential consequences of a successful attack.

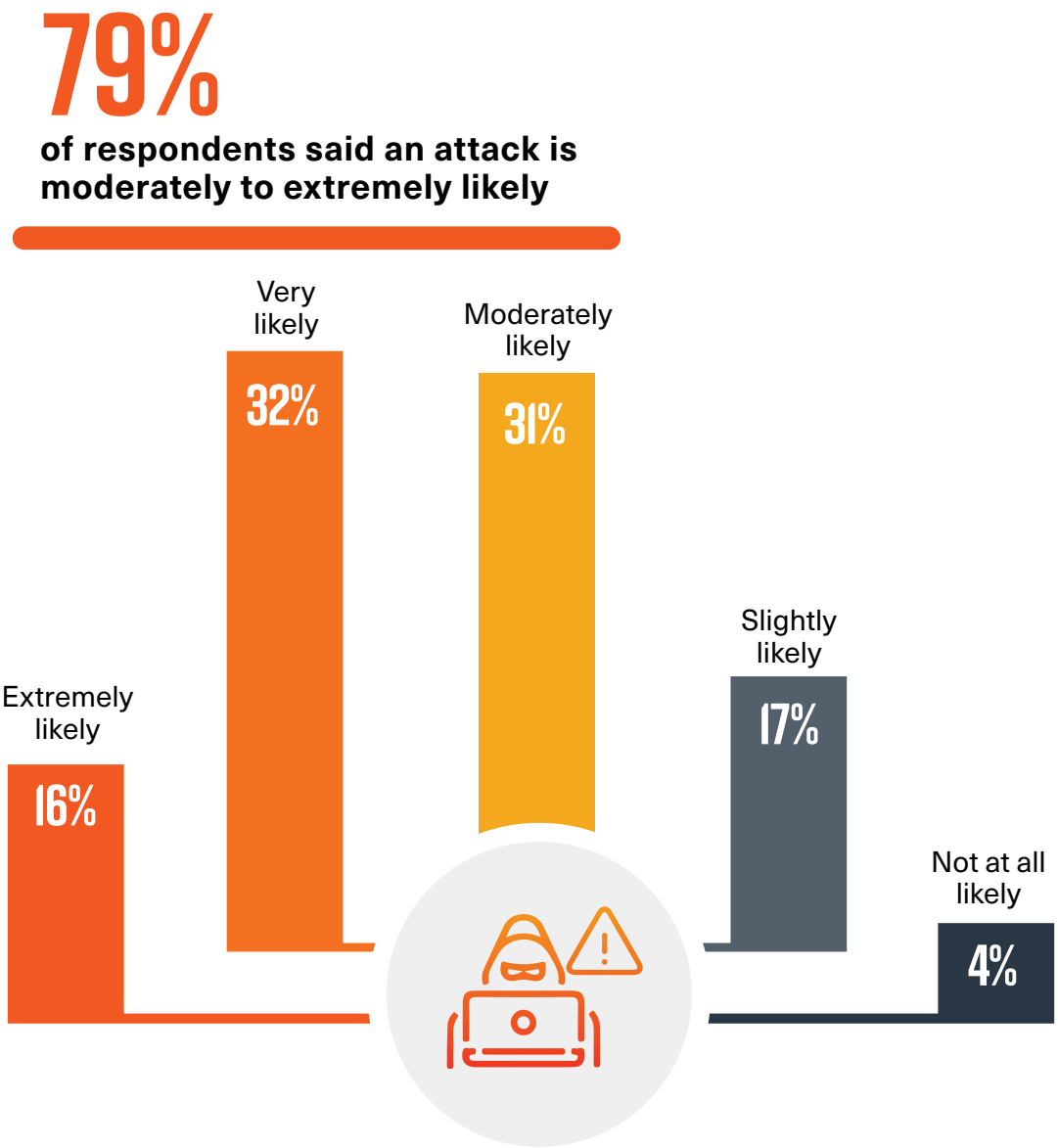
How significant a threat is malware and ransomware to your business?



RISING THREAT LEVEL

Facing an increasingly hostile threat landscape, organizations show a practical understanding of the ransomware threat and recognize that they are potential targets for an attack. A majority of organizations are acutely aware of the risks – a striking 79% of respondents believe that a ransomware attack is moderately to extremely likely to occur within the next 12 months. The message is clear: the risk is imminent, and the time to act and bolster defences is now.

What is the likelihood that your organization will be a target of a malware/ransomware attack in the next 12 months?



DATA AT RISK

Cyber attackers monetize their efforts by selling stolen sensitive information or demanding ransom payments for encrypted data. The survey reveals that 65% of respondents believe customer information is at the highest risk, followed by financial data (55%), employee information (50%), and company intellectual property (41%).

Organizations are most concerned about safeguarding sensitive information, as a breach could have severe consequences, including reputational damage, loss of customer trust, and operational downtime for affected organizations. An extreme example of the consequences of a ransomware attack can be seen in the healthcare industry. When hospitals and medical facilities are targeted, essential systems are significantly disrupted, leading to delayed patient care, the postponement of surgeries, and the inability to access vital medical records. In some cases, these disruptions can be life-threatening for patients who require immediate treatment or care.

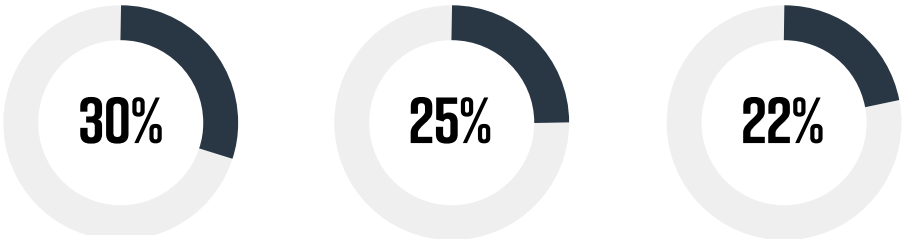
What type of data in your organization is most at risk from malware/ransomware attacks?

65% Customer information

55% Financial data

50% Employee information

41% Company intellectual property



30% Payroll/HR

25% Product information

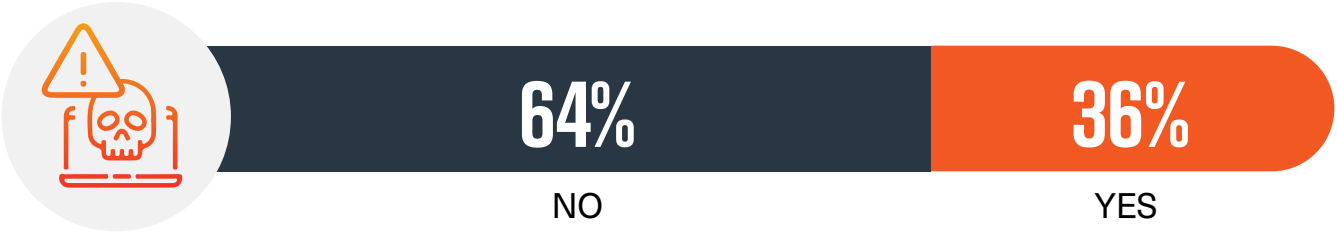
22% Research and design

EXPERIENCED ATTACKS

Understanding the prevalence of ransomware attacks is crucial for gauging an organization's vulnerability and informing appropriate security measures. The survey results show that 36% of respondents have already experienced ransomware attacks and have dealt with the consequences of such attacks, emphasizing the need for more robust security solutions. Taking the rapid growth of ransomware attacks and their increasing sophistication into account, we project that share of organizations experiencing such attacks will rise, reaching up to half of all organizations in the next 12 months.

To tackle this issue, it's essential to implement a multi-layered security approach that includes real-time monitoring and rapid response to ransomware attacks. The rapidly evolving nature of ransomware attack vectors makes effective response critical, including a focus on file-level activity and automatic isolation of compromised users and devices to significantly reduce risk and maintain operational continuity.

Has your organization suffered from ransomware attacks in the past?



Understanding the extent of data exposure following ransomware attacks helps organizations assess potential reputational and compliance risks. The survey results reveal that 5% of respondents confirmed their data was exposed on a ransomware leak site. 60% reported no exposure, and 35% were unsure.

The high degree of uncertainty underscores the importance of proactive monitoring and incident response. To tackle this issue, organizations should implement a comprehensive security approach that rapidly detects and responds to ransomware attacks to minimize data exposure risk.

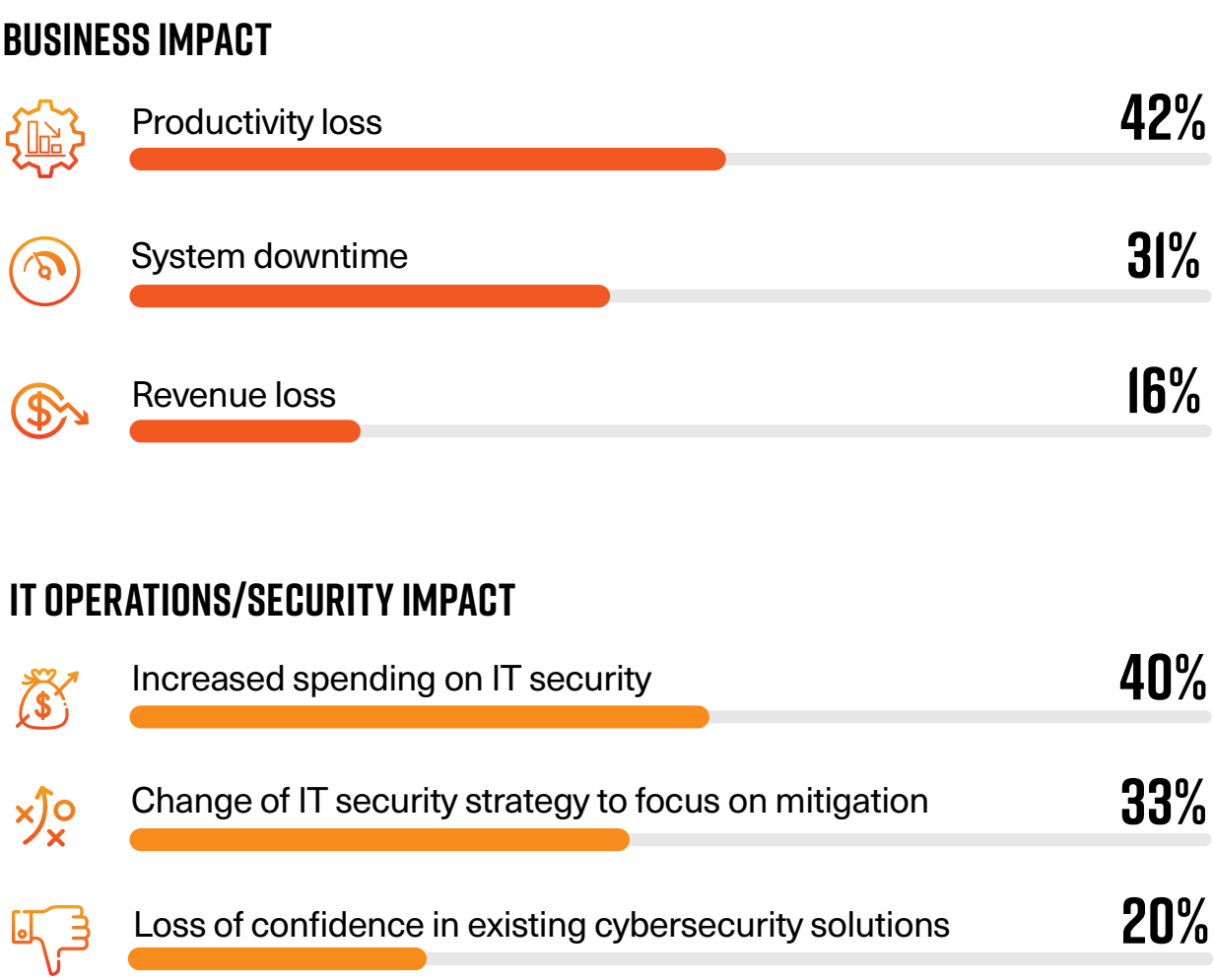
If your organization suffered from a ransomware attack, was your organization's data exposed on a ransomware leak site?

IMPACT OF RANSOMWARE ATTACKS

Ransomware attacks directly affect the business – and often at its core. Understanding the consequences of ransomware attacks helps organizations prioritize cybersecurity efforts and resources. The survey reveals that the most significant negative impacts of ransomware in the past 12 months were productivity loss (42%), followed by increased IT security spending (40%) and a significant shift in security strategy towards mitigation (33%) as organizations realize that preventing ransomware attacks has become increasingly difficult.

Other notable impacts of ransomware attacks include system downtime (31%), loss of confidence in existing cybersecurity solutions (20%), and revenue loss (16%).

What has been the impact of ransomware attacks on your organization in the past 12 months?



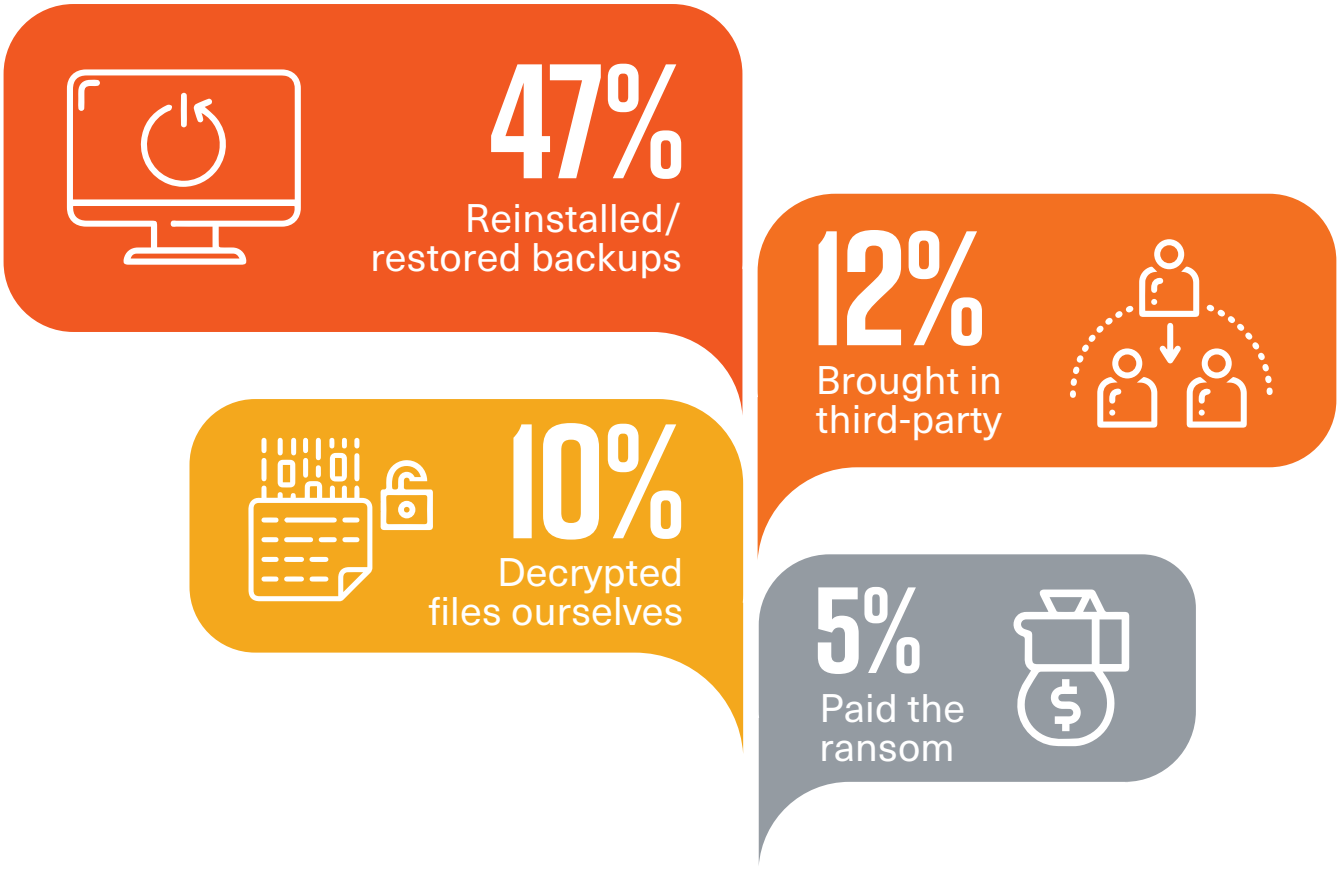
Negative press/bad publicity 13% | Damage to company reputation 13% | Loss of confidence from customers and/or partners 9% | Senior IT staff (CIO, CISO) lost their jobs 7% | Other 4%

RECOVERY TACTICS

The low percentage of organizations paying ransoms (5%) is transforming the ransomware game. While 47% of organizations recovered from an attack by reinstalling or restoring backups, this approach may not fully protect organizations from attackers threatening to sell or publicly leak their data.

To tackle this evolving threat, organizations should adopt a proactive and comprehensive security strategy. This includes real-time monitoring, rapid response to ransomware attacks, and automatic isolation of compromised users and devices. By focusing on detecting malicious file encryption and preventing data exposure, organizations can better defend against extortion attempts and maintain operational continuity.

If your organization suffered from a ransomware attack, how did your organization recover from the attack?

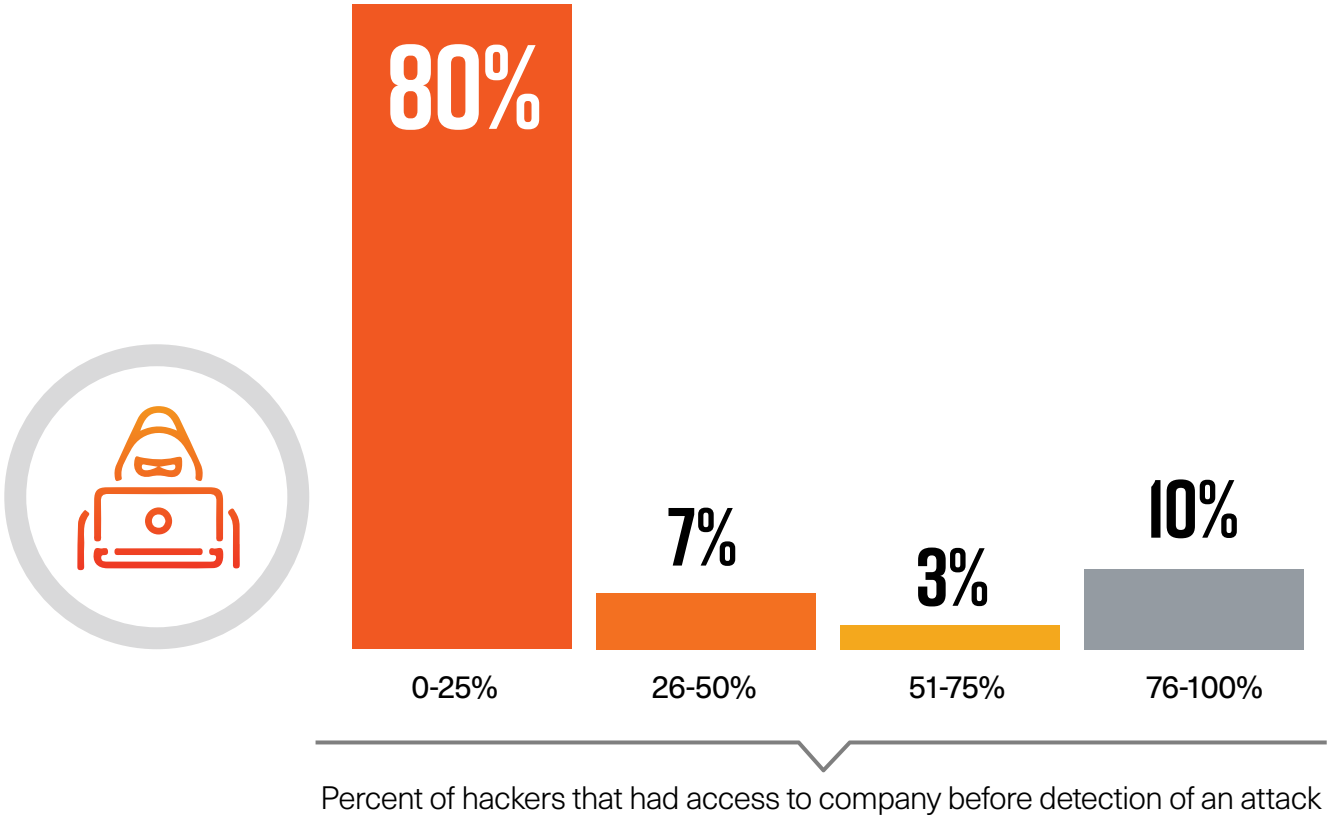


HACKER ACCESS LEVELS

Identifying the extent of unauthorized access to company data helps organizations assess potential risks and improve their security posture. The survey shows that 80% of respondents believe they detected hackers when they had access to only 0-25% of company data.

To minimize unauthorized access and its potential impact, organizations should implement an active defense strategy focused on real-time monitoring and rapid detection of malicious activities to limit the scope of attacks and their impact on the business.

What percentage of access did hackers have of company data before you detected them in your organization?

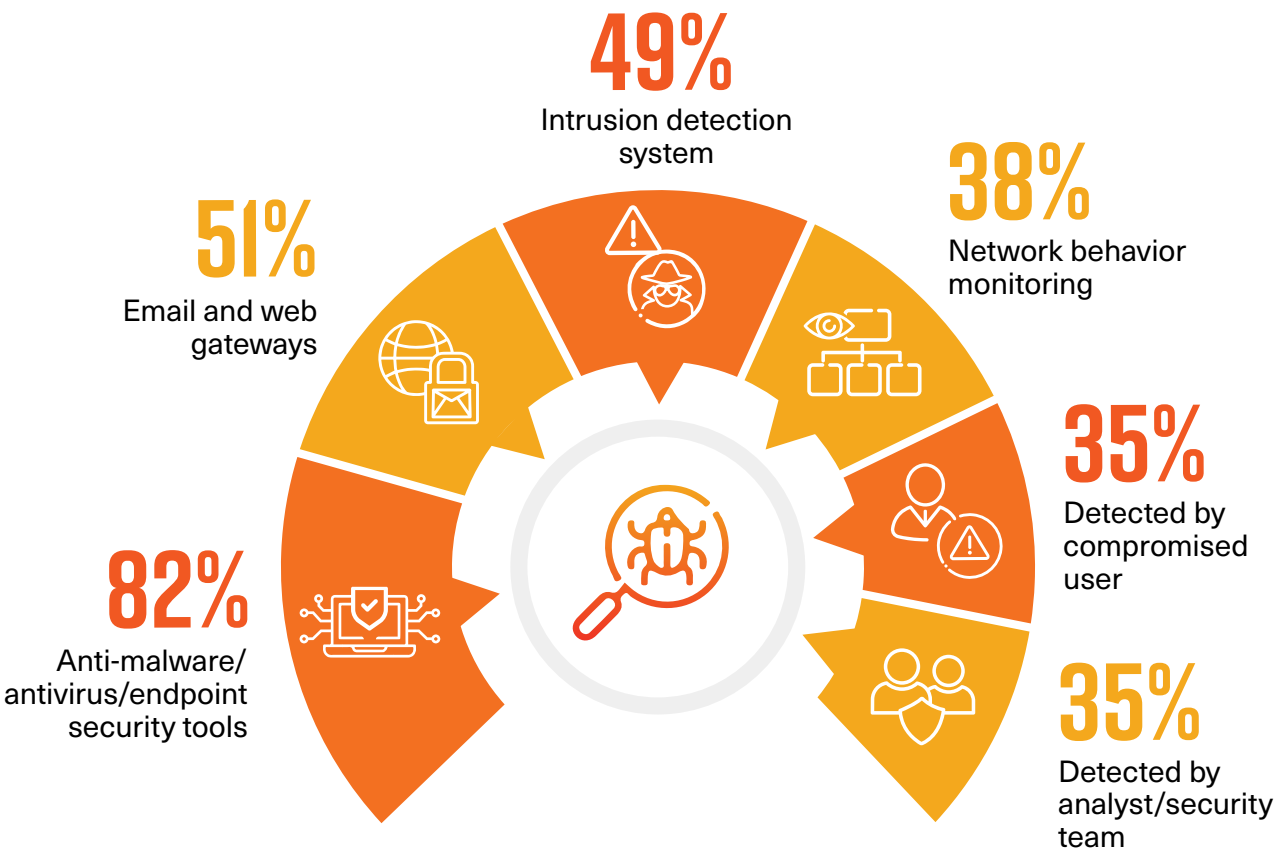


DETECTING RANSOMWARE

Effective ransomware detection is critical for preventing successful attacks and minimizing damage. The survey shows that 82% of respondents rely on anti-malware, anti-virus, and endpoint security tools as their primary detection method. This is followed by security controls including email and web gateways (51%), intrusion detection systems (49%), and network behavior monitoring (38%).

The increasing sophistication of ransomware renders many prevention solutions inadequate in defending against it. To improve detection capabilities, organizations should consider incorporating multiple layers of security, including user behavior monitoring and file monitoring, to strengthen their defenses. Assuming innovative ransomware will enter an organization's network and systems, companies need to focus on mitigation and rapid containment of active attacks. Additionally, leveraging third-party threat intelligence can provide valuable insights into emerging threats and help organizations stay ahead of potential attacks.

How is malware/ransomware typically detected when it attempts to enter your organization?



User behavior monitoring 26% | Third party threat intelligence 22% | File monitoring 22% | Detected by a third party 21% | Don't know/other 7% | We cannot detect malware/ransomware 1%

CONFIDENCE VS. RANSOMWARE REALITY

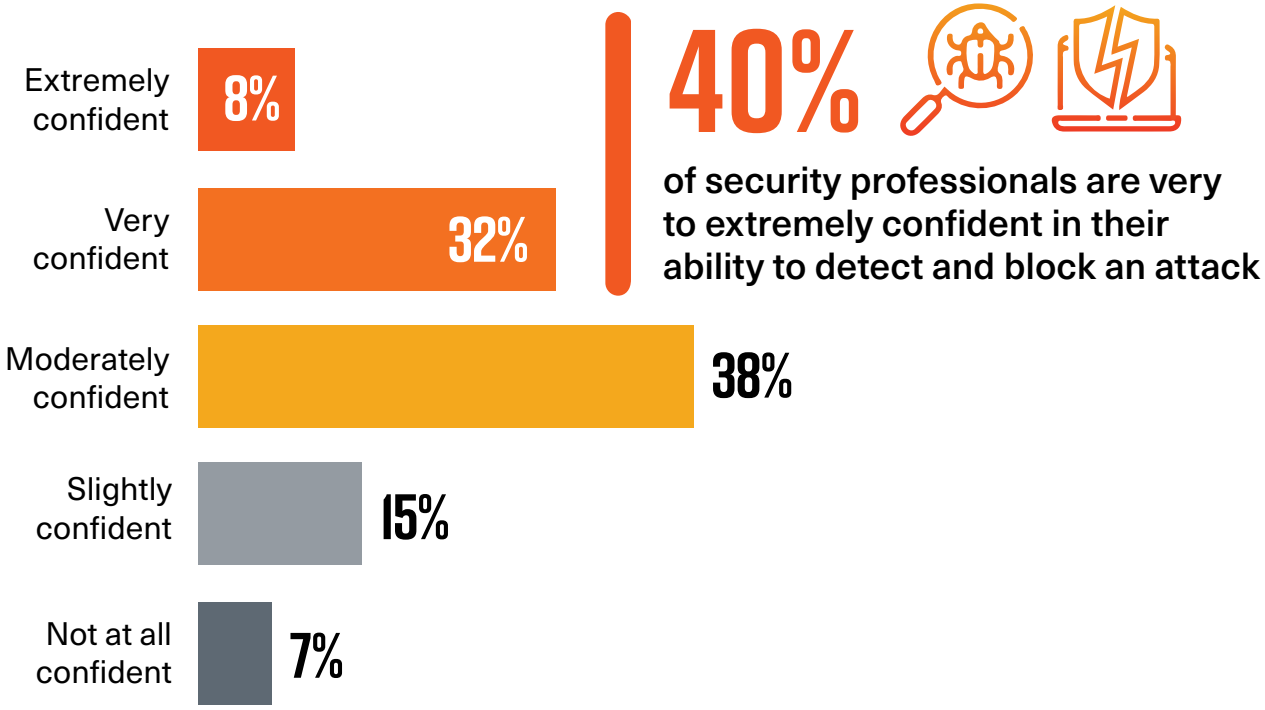
Despite the high levels of successful ransomware attacks, the survey shows that many organizations remain highly confident in their defensive abilities: 40% of respondents are very or extremely confident in their organization's ability to detect and block threats, while 38% are moderately confident.

This over-confidence could stem from a false sense of security or an underestimation of the evolving sophistication of cyber threats. It's crucial for organizations to recognize that even the most robust defenses may not always be sufficient to fend off advanced ransomware attacks.

The disconnect between high confidence levels in organizations' defenses and the high rates of ransomware attacks can be partly attributed to the fact that cybercriminals are continually innovating and staying one step ahead of preventative measures. This situation is similar to the transition from traditional antivirus solutions to EDRs: Just as antivirus solutions became insufficient, prevention alone will never be enough in the current threat landscape. Containment of active attacks is now necessary to effectively combat ransomware.

A stark example of this reality is that, in a significant number of pentests conducted with existing security tools in place, 100% fail to prevent all ransomware. This further highlights the need for a multi-layered approach to security, including detection, prevention, response, and recovery. By incorporating containment strategies alongside regular employee training, network segmentation, and frequent backups of critical data, organizations can better protect themselves from the growing and evolving threat of ransomware.

How confident are you that your organization's defenses are capable of detecting and blocking malware/ransomware before it spreads and infects critical systems and files?



POST-ATTACK RESPONSE

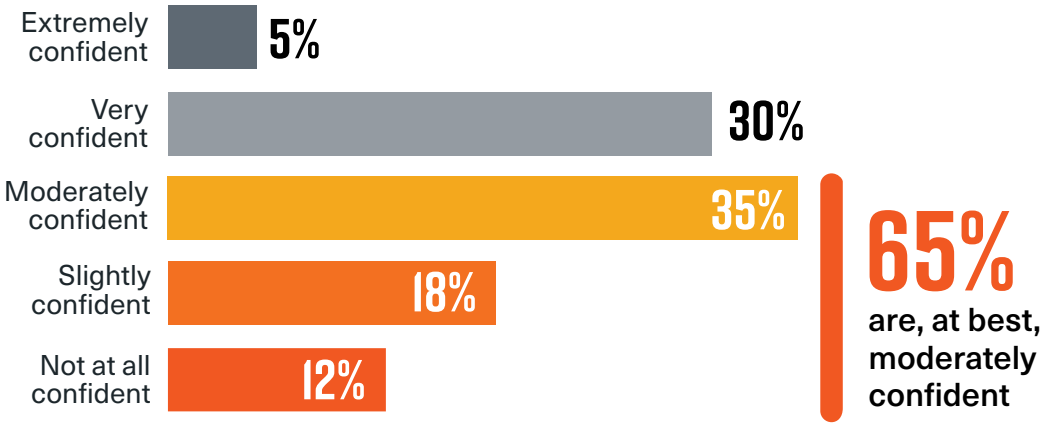
The ability to remediate ransomware after it has locked or encrypted company data is essential for minimizing damage and restoring operations. Having an incident response team is crucial to efficiently detect, investigate, and contain ransomware attacks within an organization. The survey results show that 71% of organizations have such a team in place, while 29% do not. This indicates that a significant number of organizations may be unprepared to handle cyber incidents effectively.

The survey further reveals that only 5% of respondents are extremely confident in their organization's ability to remediate ransomware after an attack, while 30% are very confident. This significant difference in confidence levels between preventing attacks and dealing with post-attack ransomware containment highlights a potential gap in organizations' cybersecurity strategies. High confidence in prevention could be attributed to organizations investing heavily in endpoint security tools, email and web gateways, and other proactive measures, which might offer a false sense of security against incoming threats.

However, the lower confidence in post-attack ransomware remediation suggests that organizations might be underestimating the need for robust response and recovery plans. As ransomware attacks continue to evolve and become more sophisticated, including the potential growth of AI-generated malware, relying solely on prevention measures will prove insufficient. To address this gap and prepare for future threats, organizations should adopt automated containment solutions that complement their existing resources. These tools can enhance their ability to respond to and remediate ransomware attacks, allowing stretched cybersecurity teams to focus on more strategic tasks.

Does your organization have an Incident Response team in place to detect, investigate, and contain malware/ransomware attacks?

How confident are you in your organization's current ability to remediate ransomware AFTER it locks or encrypts data within your systems?



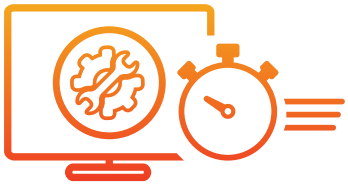
SPEED OF RECOVERY

The speed of ransomware recovery is crucial, as it directly affects an organization's downtime, productivity, and potential revenue loss.

According to the survey, 38% of respondents believe they can recover from a ransomware attack within a day, while 35% think they can do so within a few days. This seems to reflect a high degree of optimism among cybersecurity professionals as real-world ransomware cases show recovery times often measured in weeks and months, not days.

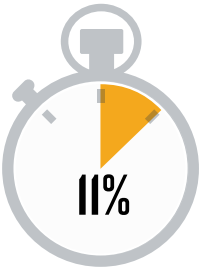
To address this issue, organizations should adopt solutions that can shut down attacks in progress before ransomware can spread through the organization, thereby significantly reducing damage and recovery time.

How fast do you believe you can recover from a ransomware attack?



73%

of customers need at most a few days to recover after a ransomware attack



Potentially never recover

A few hours | A day | A few days | A week | A few weeks

Ransomware Recovery Time

RESPONDING TO RANSOMWARE

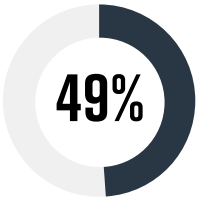
Effective ransomware response strategies are essential in limiting the impact of an attack and restoring normal operations. We asked cybersecurity professionals how their organization would respond after an active ransomware attack is detected. By far the most common response is to isolate and shut down the affected systems, recover files from backups, and mitigate the initial attack vector (68%). This is followed by 49% proactively shutting down core systems to prevent spread and 39% engaging a third-party incident response service.

Interestingly, only 2% would choose to pay the ransom, indicating that organizations are increasingly aware of the risks involved in engaging with attackers.

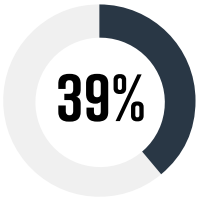
To tackle ransomware, organizations should focus on developing a robust incident response plan that outlines clear procedures to be followed during an attack. This plan should include regular backups, network segmentation, employee training, and effective communication with stakeholders. Implementing such a strategy can help minimize the attack's impact and ensure faster recovery.

How would your organization respond after a ransomware attack is detected on your systems?

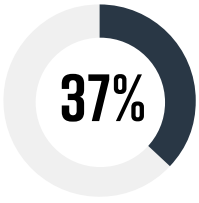
68% **Isolate and shut down offending systems and accounts, recover encrypted files from backups, and mitigate the initial attack vector if possible**



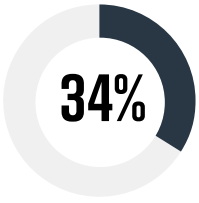
Proactively shut down core systems to prevent spread



Engage a third-party incident response service



Immediately call law enforcement



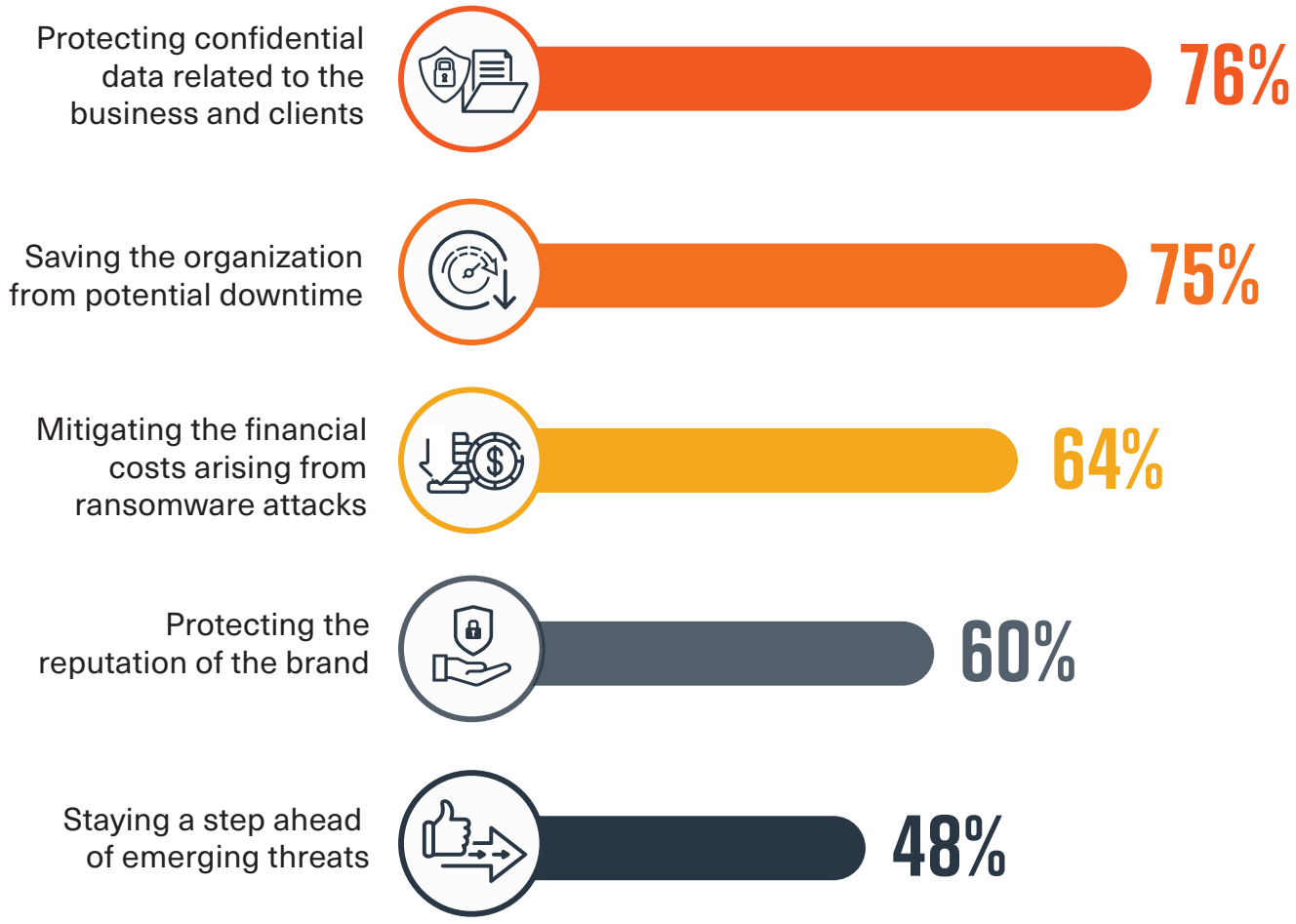
Contact cybersecurity technology vendor

Attempt to decrypt files ourselves 27% | Contact cybersecurity technology vendor 27% | Notify customers 20%
Attempt to negotiate with the attackers 10% | Pay the ransom 2%

DEFENSE PRIORITIES

Understanding an organization's primary drivers for improving ransomware defense helps shape targeted and effective strategies. The top two drivers are protecting confidential data (76%) and preventing potential downtime (75%), followed by mitigating the negative financial impact from ransomware attacks (64%).

What are your organization's primary drivers for improving malware/ransomware defense?



ENDPOINT SECURITY LIMITATIONS

The survey results reveal a concerning overconfidence in endpoint security / EDR solutions, with 77% of respondents believing their EDR can protect their organization against ransomware attacks. However, EDR's effectiveness against ransomware has limits in the face of rapidly evolving ransomware, especially considering that not all ransomware attacks enter through endpoints.

Organizations should recognize that EDR alone is not enough to prevent all ransomware attacks, particularly considering the constantly evolving tactics and techniques used by cybercriminals. To enhance their defense, companies should adopt a comprehensive approach that includes solutions designed to shut down active ransomware attacks before they spread too far and cause significant damage.

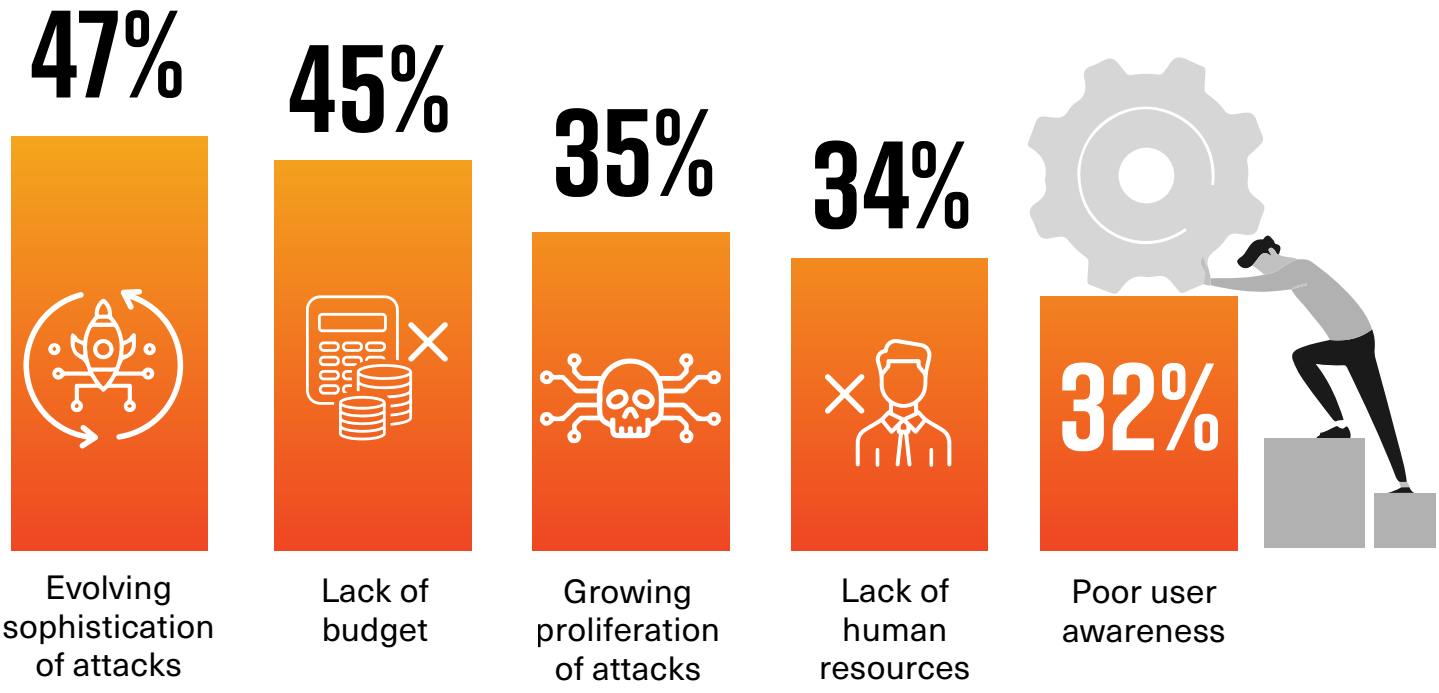
Can your endpoint security solution(s) protect your servers against malware attacks?

DEFENSE OBSTACLES

Security teams are facing many obstacles, both internally and externally, in their effort to protect IT environments against ransomware threats.

The survey highlights that organizations perceive the evolving sophistication of attacks (47%), lack of budget (45%) and growing proliferation of attacks (35%) as their biggest challenges in improving ransomware defense. These factors contribute to the difficulty in maintaining an effective security posture and underscore why organizations need to move beyond prevention and into automated containment.

What do you believe to be your organization's biggest obstacles to improving malware/ransomware defense?

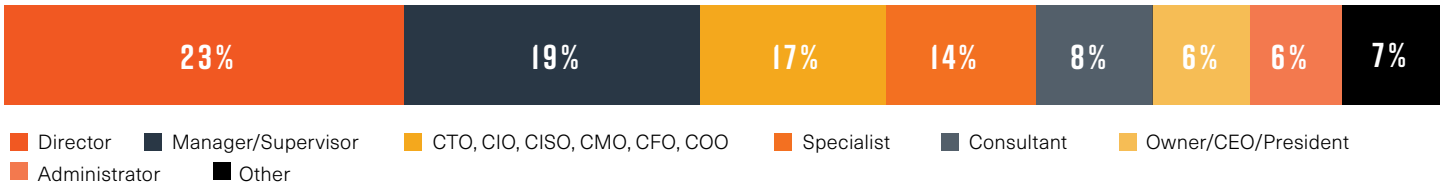


Uncertainty what security solution to use 23% | Lack of executive sponsorship 18% | Our partners' lack of preparedness or response 8% | Other 3%

METHODOLOGY & DEMOGRAPHICS

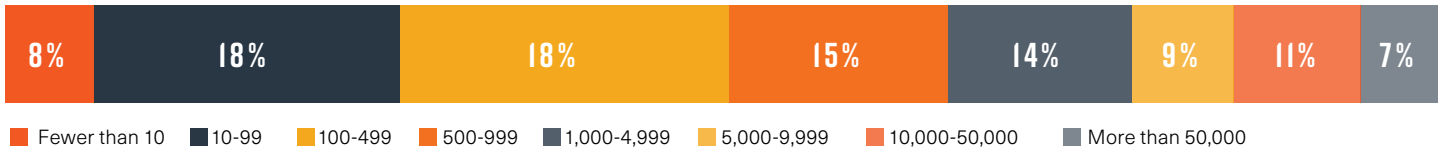
This report is based on the results of a comprehensive online survey of 435 cybersecurity professionals conducted in April 2023 to gain more insight into the latest trends, key challenges, and solutions for malware and ransomware security. The respondents range from technical executives to managers and IT security practitioners, representing a balanced cross-section of organizations of varying sizes across multiple industries.

CAREER LEVEL

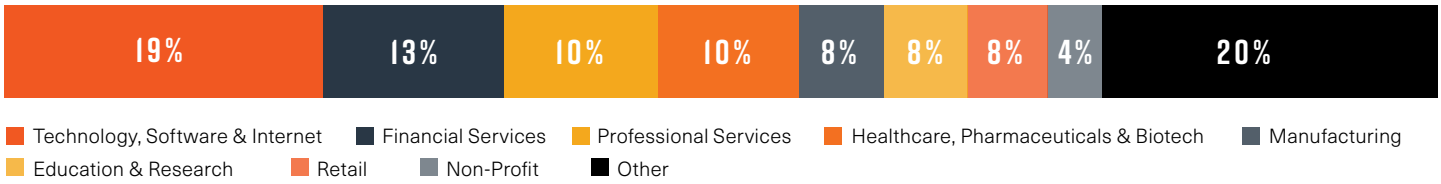


DEPARTMENT

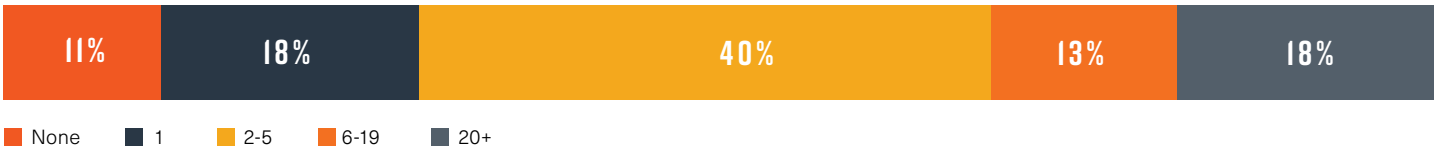
COMPANY SIZE



INDUSTRY



IT SECURITY TEAM



RANSOMWARE BEST PRACTICES

As ransomware threats continue to evolve, organizations must adapt and strengthen their defenses. Here's a list of best practices to consider for a comprehensive ransomware defense strategy:

Employee Education and Awareness: It's important to acknowledge that employees are often the first line of defense against ransomware attacks. Implementing regular cybersecurity training and promoting a security-aware culture will help reduce the risk of successful phishing and social engineering attacks.

Robust Backup and Recovery: Ensuring a robust backup and recovery strategy is crucial because it minimizes downtime and data loss in case of a ransomware attack. Implementing frequent and tested backups, storing them offsite or in the cloud, and having a clear recovery plan will greatly enhance the organization's resilience.

Rapid Containment of Active Attacks: Focusing on solutions that can quickly shut down an ongoing attack is critical for limiting damage. Implementing tools and processes that identify and contain ransomware activity in real-time significantly reduces the impact of an attack.

Regular Vulnerability Assessments and Patch Management: Conducting regular vulnerability assessments and promptly patching discovered vulnerabilities helps prevent exploitation by ransomware. Keeping software and systems up to date reduces the likelihood of successful attacks and maintains a strong security posture.

Multi-Factor Authentication (MFA): MFA adds an extra layer of security by requiring multiple forms of authentication before granting access to sensitive data or systems. Implementing MFA helps protect against unauthorized access, even if an attacker obtains valid credentials.

Threat Intelligence and Information Sharing: Staying informed about emerging threats and sharing information with relevant stakeholders helps organizations proactively prepare for potential attacks. By leveraging threat intelligence and collaborating with other organizations, businesses can identify and respond to threats more effectively.

Incident Response Plan and Team: Having a well-defined incident response plan and a dedicated team ensures a quick and efficient reaction to ransomware attacks. Regularly reviewing and testing the plan keeps the organization prepared for a swift response, minimizing damage and downtime.

Network Segmentation: Segmenting networks limits the attack surface and prevents the spread of ransomware within the organization. By dividing the network into smaller, separate segments and implementing strict access controls, organizations can better protect sensitive data and critical systems.

By following these best practices, organizations can build a more resilient defense against ransomware and reduce the likelihood and impact of successful attacks.

BULLWALL

ABOUT BULLWALL

BullWall is a cybersecurity solution provider with a dedicated focus on protecting data and critical IT infrastructure during active ransomware attacks. We are able to contain both known and zero-day ransomware variants in seconds, preventing both data encryption and exfiltration.

BullWall is your last line of defense for active attacks.

Learn more at www.bullwall.com.

Cybersecurity
INSIDERS

Cybersecurity Insiders is a 600,000+ member online community for information security professionals, bringing together the best minds dedicated to advancing cybersecurity and protecting organizations across all industries, company sizes, and security roles.

We provide cybersecurity marketers with unique marketing opportunities to reach this qualified audience and deliver fact-based, third-party validation thought leadership content, demand-generation programs, and brand visibility in the cybersecurity market.

For more information please visit www.cybersecurity-insiders.com