2022

Cybersecurity INSIDERS

RANSOMWARE/ MALWARE REPORT

Resecurity

INTRODUCTION

Malware, including viruses, ransomware, and spyware, is becoming an increasingly destructive security threat affecting organizations of all sizes and across all industries.

The Ransomware/Malware Report was produced by Cybersecurity Insiders and Resecurity to reveal the state of the threat landscape and explore key challenges and solutions to protect against rising malware and ransomware threats.

Key findings include:

- A majority of 60% of cybersecurity professionals see malware and ransomware as an extreme threat to their organizations.
- Organized cyber-criminals (77%) top the list of malicious actors, followed by opportunistic hackers (67%) and nation-state sponsored hackers (50%).
- Spear-phishing emails remain the single most dangerous malware attack vector (82%), followed by domain spoofing (45%) and man-in-the-middle attacks (43%).
- The majority of respondents (72%) claim they can detect an attack within hours. Fifty percent of organizations report that detection is near real time or within minutes. Despite this quick response, most professionals lack confidence in their organization's capacity to detect and block an attack before it spreads to critical IT systems and files.

We hope you find this report informative and helpful as you continue your efforts in protecting your organization against evolving threats and during challenging times.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

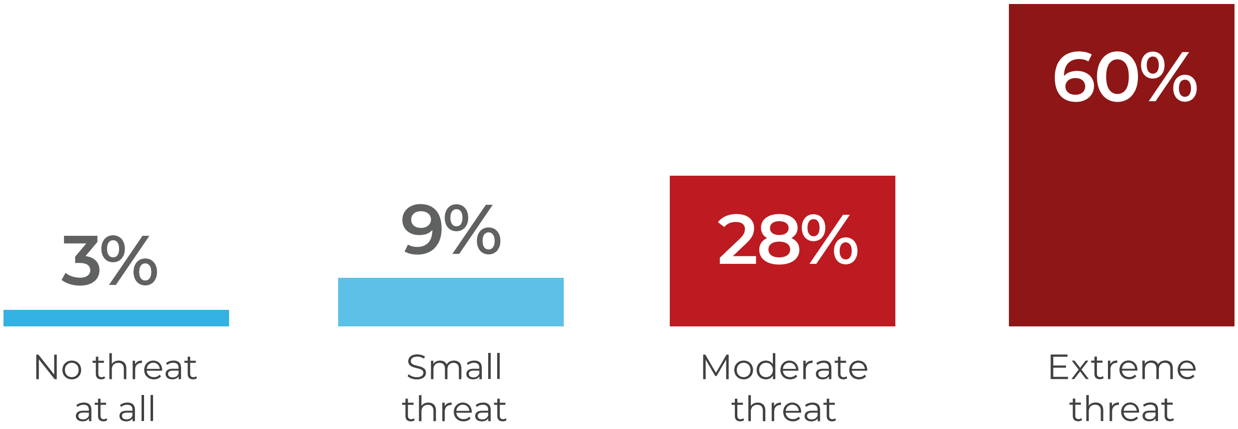
RISING THREAT LEVEL

Malware and ransomware are significant threats and can significantly harm businesses. A majority of 60% of cybersecurity professionals see malware and ransomware as an extreme threat to their organizations.

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

88%

of respondents see malware as an extreme or moderate threat

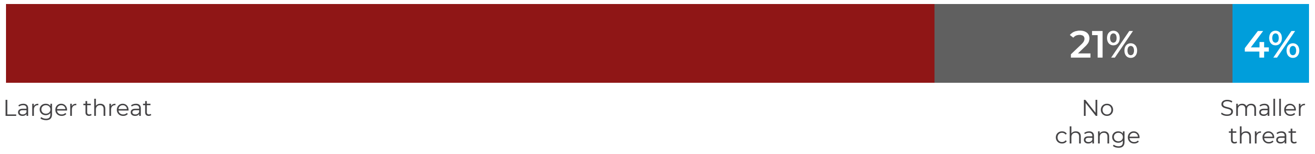


WORSENING ATTACK OUTLOOK

A significant majority of IT security professionals (75%) predict ransomware/malware will become a larger threat in the next 12 months. Eighty-two percent believe attacks are going to become more frequent and 86% said an attack on their business is moderately to extremely likely within the next 12 months.

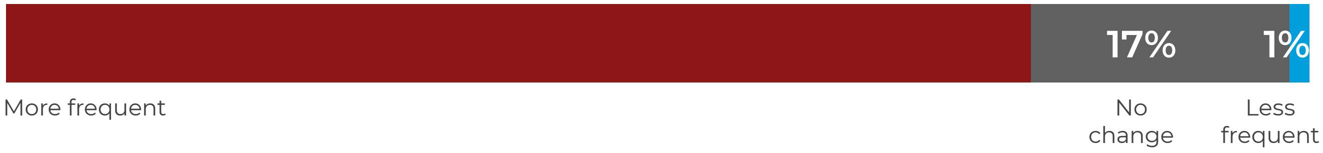
In the next 12 months, do you believe malware and ransomware will be a larger or smaller business threat to organizations?

75% believe malware and ransomware will be a larger threat to organizations in the next 12 months



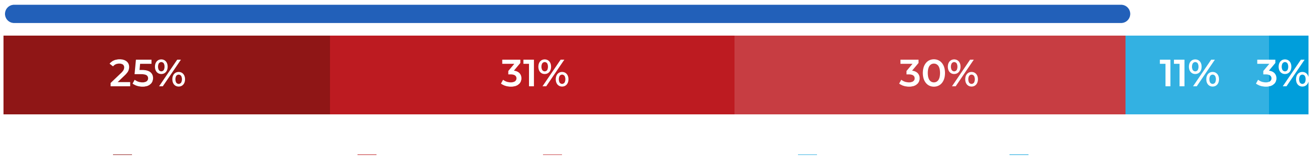
Are malware/ransomware attacks becoming more or less frequent overall?

82% believe malware and ransomware attacks will be more frequent



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

86% of respondents said an attack is at least moderately likely



MOST DANGEROUS THREATS

We asked which types of attackers cybersecurity professionals find most concerning. Organized cyber-criminals (77%) top the list, followed by opportunistic hackers (67%) and nation-state sponsored hackers (50%). Spear-phishing emails remain the single most dangerous malware attack vector (82%), followed by domain spoofing (45%) and man-in-the-middle attacks (43%).

Which of these attackers concern you most?

77% Organized cyber-criminals

67% Opportunistic hackers (non-organized)

50% Nation-state sponsored hackers

Disgruntled/former employees 26% | Politicalhacktivists 22% | Competitors 15% | Dissatisfied customers 14% | Inadvertent/accidental attacks 12% | Don't know/other 6%

What malware attack vectors do you consider most dangerous?

82% Spear-phishing emails

45% Domain spoofing

43% Man-in-the-middle attacks

Trojanized software 42% | Web server exploits 42% | SQL injection 37% | Cross-site scripting 28% | Watering hole websites 24% | Other 3%

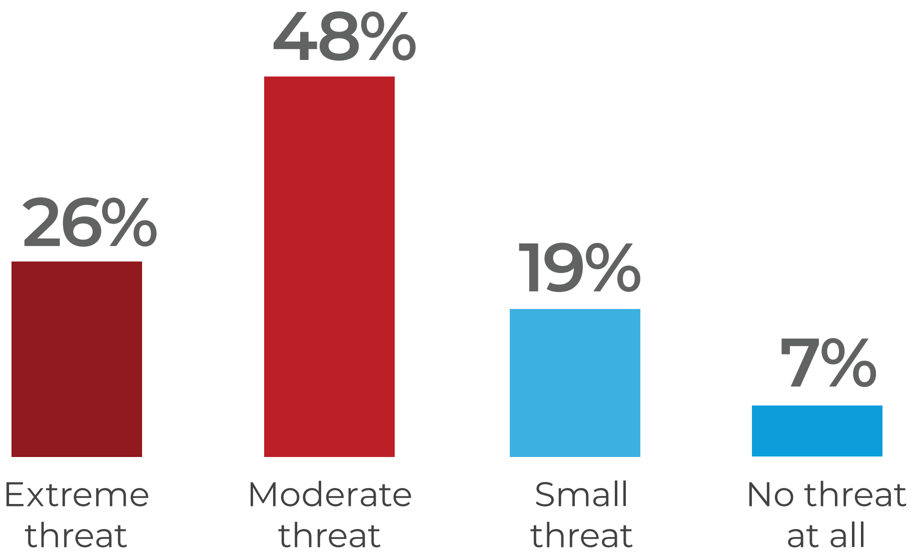
REMOTE WORK RISK

The recent, massive shift to remote work resulted in a significant deterioration for many organizations’ risk exposure. A majority (74%) see remote work as a moderate to extreme risk to their organization.

How significant of a business risk are remote workers to your business?

74%

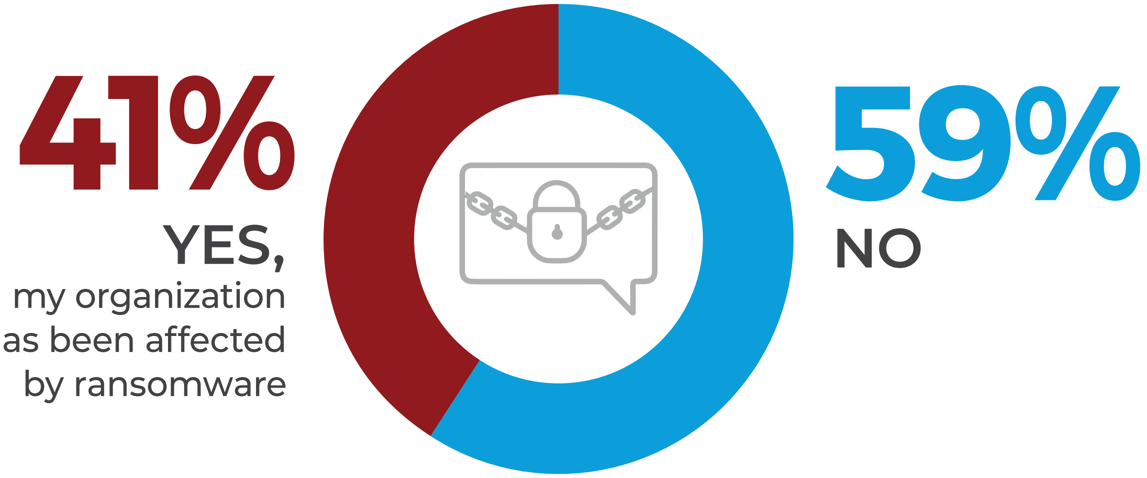
view remote workers as at least a moderate risk to the business



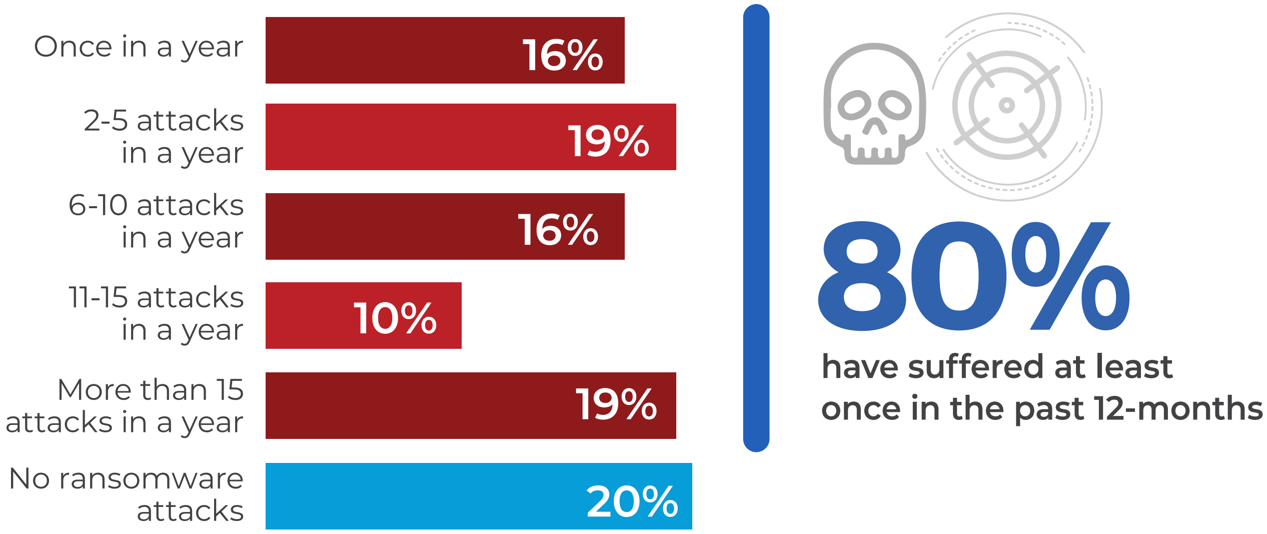
ATTACK FREQUENCY

Less than half of security professionals (41%) say their organization has experienced ransomware attacks. Professionals who are aware of an attack indicate their organizations (80%) have suffered at least once in the past 12-months. An alarming 29% of organizations are even experiencing 11 or more attacks per year.

Has your organization suffered from ransomware attacks in the past?



What is the frequency of ransomware attacks targeting your organization in the last 12 months?

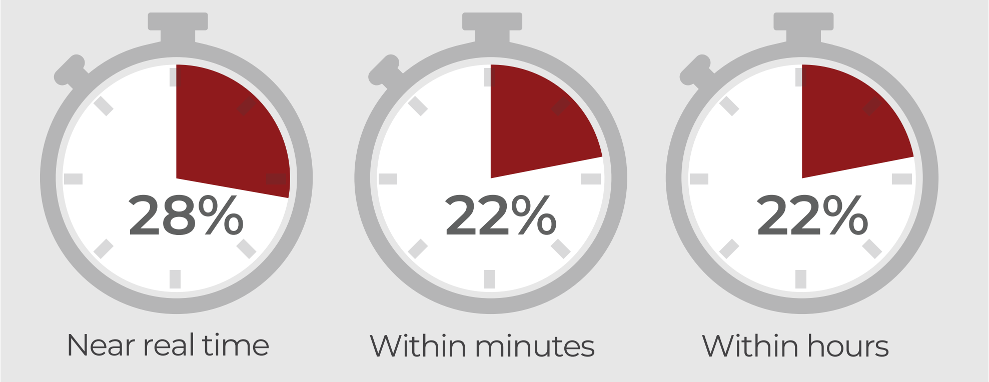


SPEED OF DETECTION

The speed of detecting malware/ransomware infiltrations is most critical in responding to fast-moving attacks before they succeed in spreading across the network. The majority of respondents (72%) claim they can detect an attack within hours. Fifty percent of organizations report that detection in near real-time or within minutes. Despite this quick response, most professionals lack confidence in their organization's capacity to detect and block an attack before it spreads to critical IT systems and files.

How quickly is malware/ransomware typically detected by IT security when it attempts to enter your organization?

72% of attacks are detected within hours

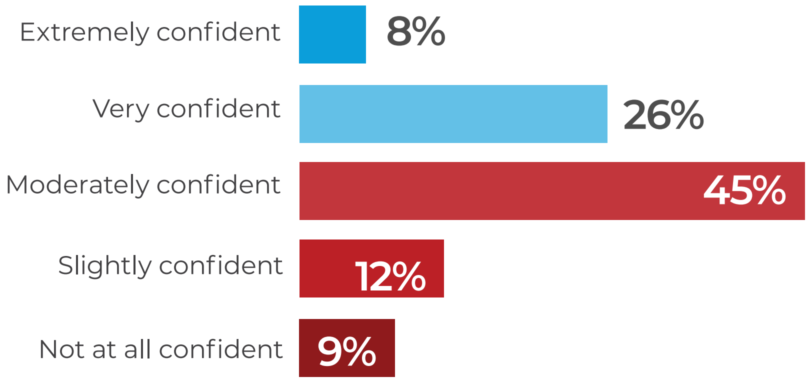


10% Within one business day

10% Longer than one business day

8% Multiple days

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?

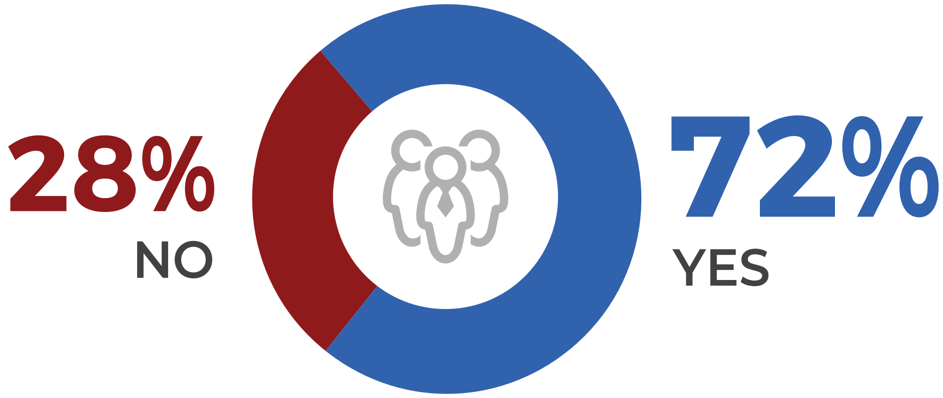


66% are not fully confident in their ability to detect and block an attack

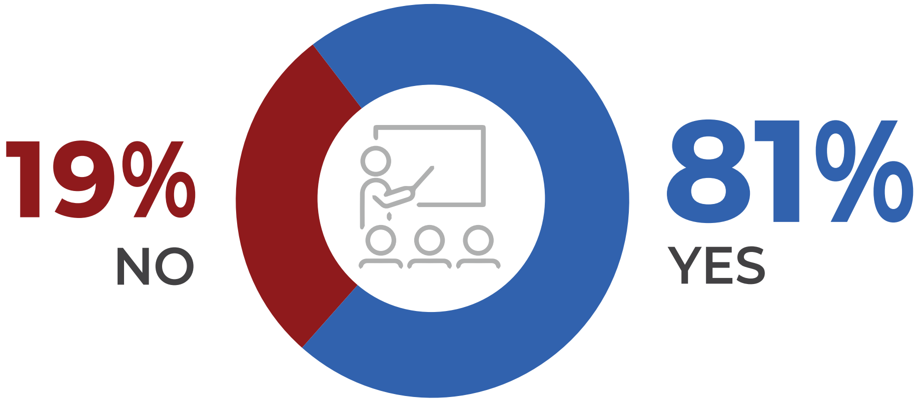
RESPONSE TEAM READINESS

Incident response teams are a critical component in defending against an attack. Seventy-two percent of organizations responding to this survey have response teams in place to detect, investigate, and remediate an attack. Eighty-one percent have a formal training program in place to educate employees and raise awareness for defense against malware/ransomware attacks.

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



Does your organization have a training program in place to educate employees and raise awareness for defense against malware/ransomware attacks?

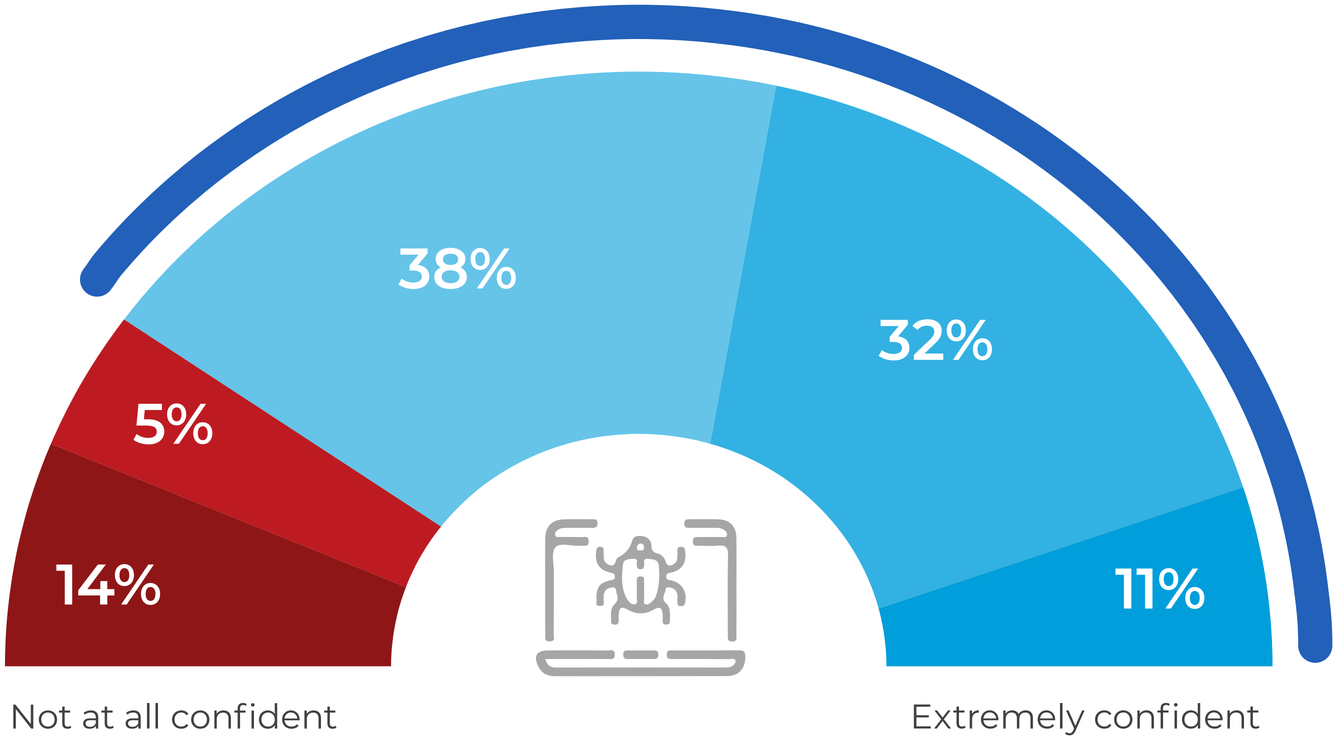


CONFIDENCE IN REMEDIATION

We asked cybersecurity professionals about their confidence in their organization's ability to remediate ransomware after it locks or encrypts data within their systems. A surprising eight out of ten organizations are extremely to moderately confident in their organization's ability to remediate an attack. However, 14% are not confident at all.

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

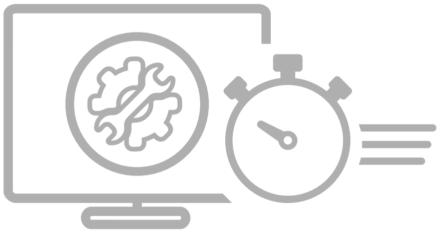
81% are extremely to moderately confident in their organization's ability to remediate a ransomware infection



SPEED OF RECOVERY

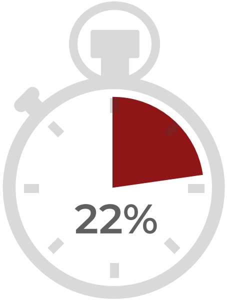
Speed of recovery from an attack is absolutely critical as cost escalates with every hour the business cannot fully operate. Slightly more than half (55%) of organizations can recover from a ransomware attack within a few days, while 34% estimate it will take one day or less to recover. Only 11% of the organizations believe they will never fully recover.

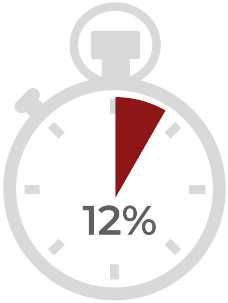
How fast do you believe you can recover from a ransomware attack?

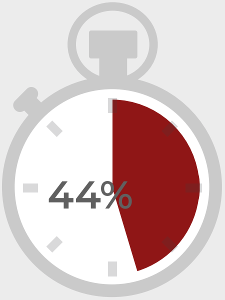


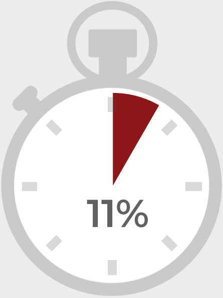
55%

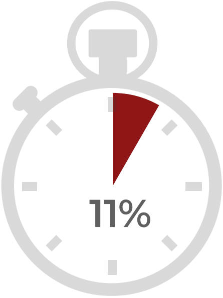
need longer than a few days to recover from a ransomware attack









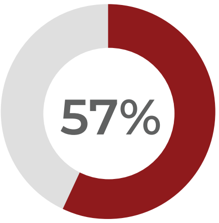


ATTACK RESPONSE TACTICS

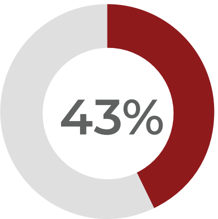
We asked cybersecurity professionals how their organization would respond after a ransomware attack is detected. The most common response (73%) after an attack is detected, is to isolate and shut down all infected systems and accounts, and recover the encrypted files from backups while blocking the initial attack vector.

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

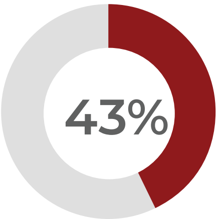
73% **isolate and shut down offending systems and accounts, recover encrypted files from backups, and mitigate the initial attack vector if possible**



Proactively shut down core systems to prevent spread



Engage a third-party incident response service



Contact cyber insurance provider

Immediately call law enforcement 32% | Notify customers 32% | Attempt to decrypt files ourselves 30% | Pay the ransom 5% | Attempt to negotiate with the attackers 5%

EFFECTIVE SOLUTIONS

Cybersecurity professionals continue to view data backup and recovery (86%) as the most effective solution to respond to a successful attack. Threat intelligence is also an effective means of prevention for 77% of security professionals.

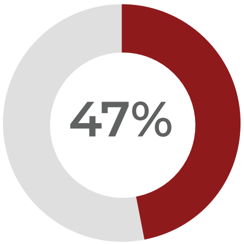
What security solutions would you say are the most effective to respond to malware/ransomware?

86%

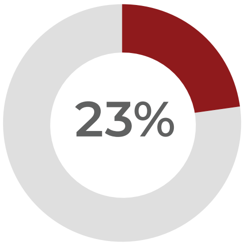
Data backup and recovery response

77%

Threat intelligence



Behavioral analytics



Cyber insurance

SERVER-LEVEL MALWARE PROTECTION

When asked about the features that are most important in server-level malware protection solutions, 76% of security professionals prioritize automatic updating and scanning, followed by heuristic analytics (67%).

What features do you consider most important in server-level malware protection solutions?

76%
Automatic updating and scanning

67%
Heuristic analysis

66%
Native file system scanning

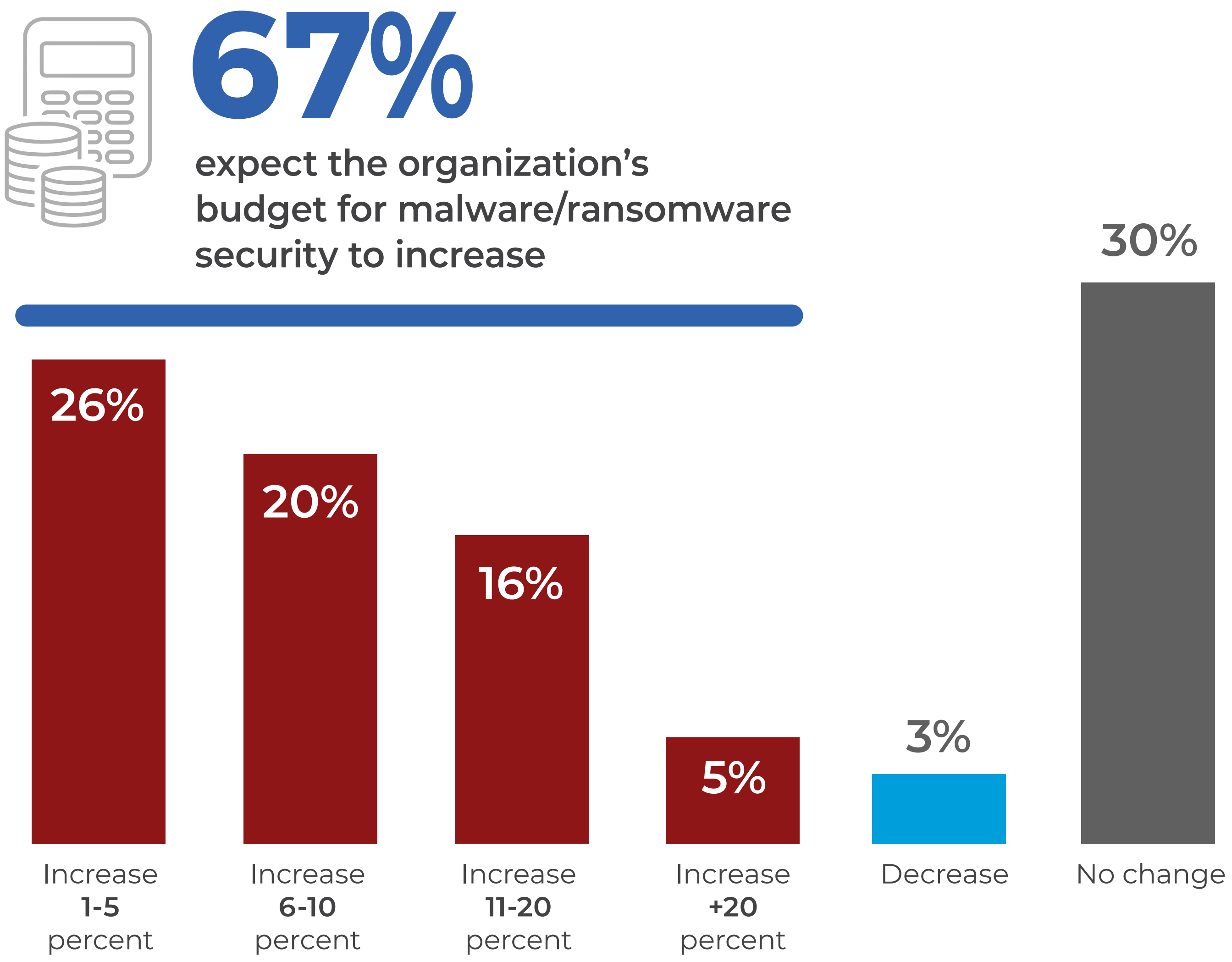
61%
Object integrity scanning

Other 6%

SECURITY BUDGETS

Budgets to protect organizations against malware/ransomware attacks are expected to increase according to 67% of security professionals. Thirty percent do not expect any changes to their budgets.

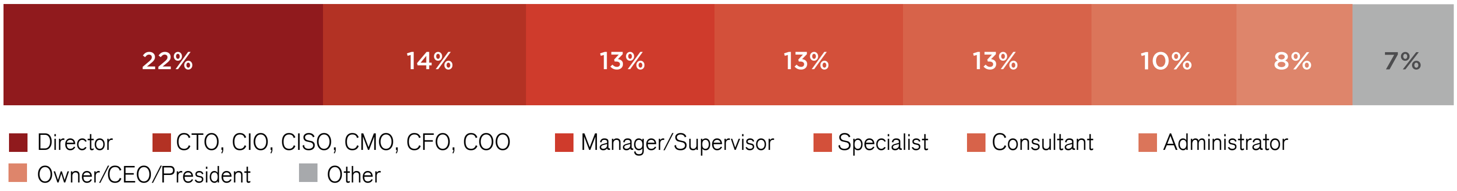
How do you expect your organization's budget for malware/ransomware security to change?



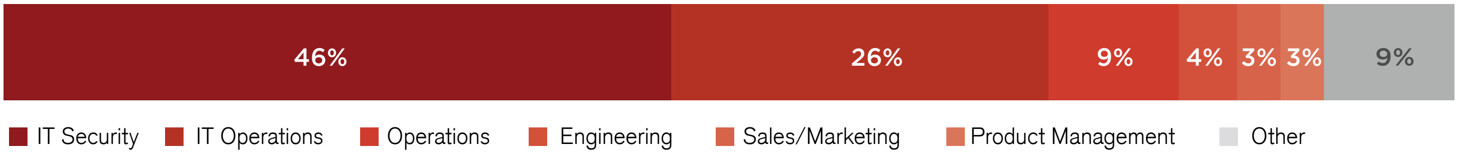
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of 225 cybersecurity professionals, 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.

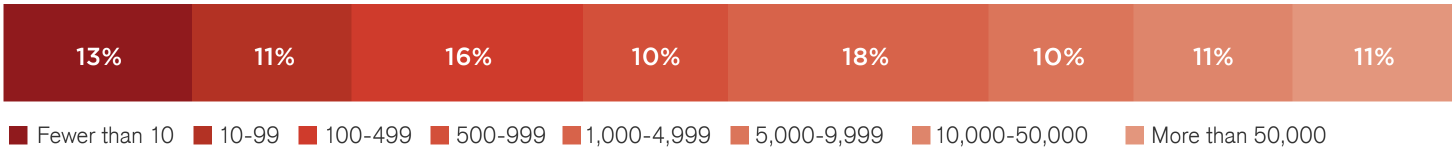
CAREER LEVEL



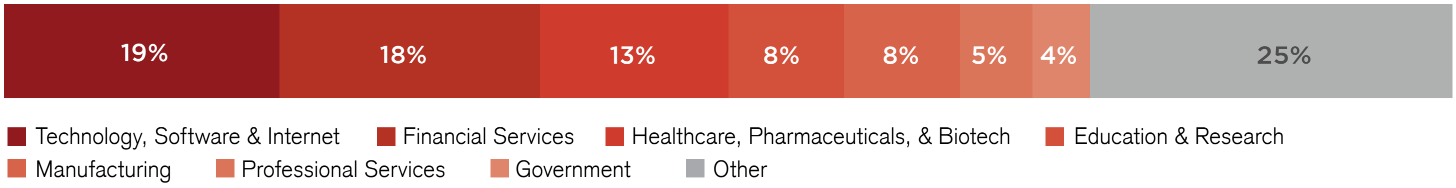
DEPARTMENT



COMPANY SIZE



INDUSTRY



Resecurity

Resecurity is a cybersecurity company that delivers a unified platform for endpoint protection, risk management, and threat intelligence for large enterprises and government agencies worldwide.

Resecurity provides intelligence, risk management, and security capabilities. It's mission is to enable enterprises, national security, and law enforcement agencies to combat cyber threats regardless of how sophisticated they are.

Resecurity is focused on intelligence-driven solutions. The company invests in Big Data, Artificial Intelligence, and Data Science. These bring unique value in complex investigations of cybercrimes, APT campaigns, and threat actors.

A big part of Resecurity's work is R&D. The company researches the latest techniques and tradecrafts of cybercriminals and nation-state actors, and analyzes massive amounts of data in order to improve its products.

The company aims to revolutionize cybersecurity for organizations of all sizes, making them safer. At Resecurity, protecting their customers are the company's commitment and passion.

resecurity.com