2019

Cybersecurity
RESEARCH

MALWARE REPORT

helpsystems

INTRODUCTION

The 2019 Malware Report was produced by Cybersecurity Insiders and HelpSystems to reveal the latest malware security trends, challenges, and investment priorities.

Key findings include:

- Malware and ransomware is still one of the most destructive security threats affecting organizations of all sizes, from SMBs to large enterprises and government agencies. Eighty-six percent of respondents perceive them either as an extreme threat (49%) or moderate threat (37%).
- Seven out of 10 organizations believe malware and ransomware will become a larger threat to their organizations in the next 12 months.
- 76% consider a malware attack in the next 12 months moderately to extremely likely. However, 55% of organizations are not confident in their ability to detect and block an attack.
- 54% consider phishing emails the most dangerous attack vector, followed by trojans with 13%.
- The most significant business impact of malware attacks is the resulting productivity loss (58%) and system downtime (50%).
- Organizations prioritize user awareness training (75%) and anti-malware solutions (74%) as most effective in preventing malware attacks.

We would like to thank HelpSystems for supporting this unique research.

We hope you will enjoy the report.

Thank you,

Holger Schulze

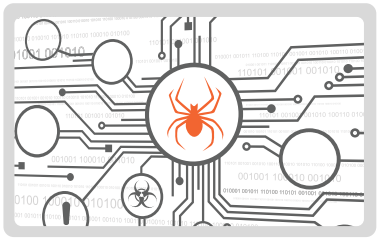
Holger Schulze
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

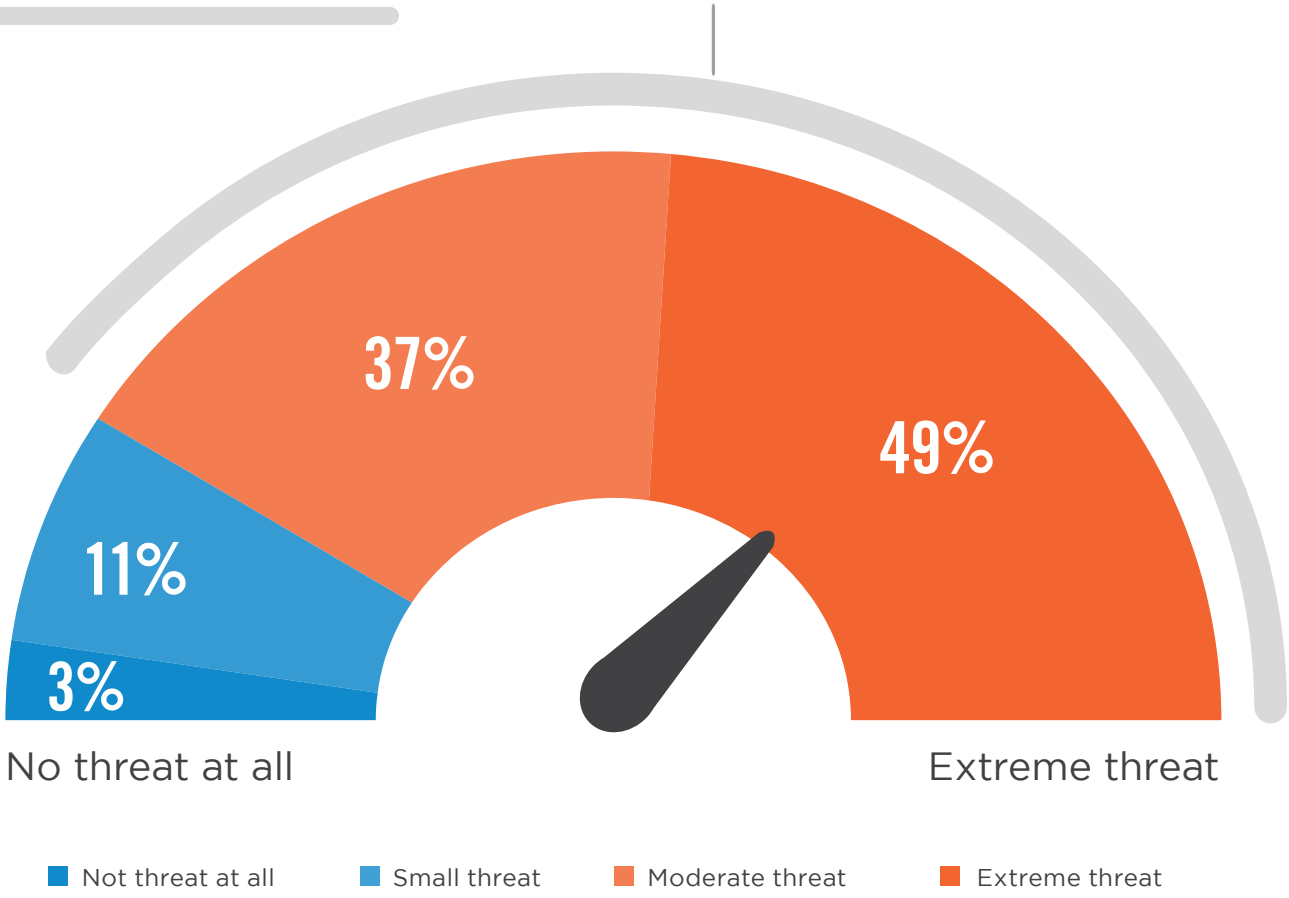
MALWARE AND RANSOMWARE THREAT

Malware and ransomware is still one of the most destructive security threats affecting organizations of all sizes, from SMBs to large enterprises and government agencies. Eighty-six percent of respondents perceive them either as an extreme threat (49%) or moderate threat (37%). Very few respondents (3%) see both as no threat at all.

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



86% of respondents see malware as an extreme or moderate threat.



FUTURE ATTACKS

A significant majority (71%) of IT security professionals predict malware and ransomware to become a larger threat in the future. 68% expect an increase in attack frequency over the next 12 months.

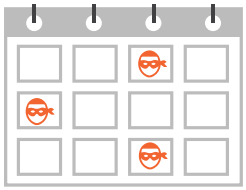
In the next 12 months, do you believe malware and ransomware will be a larger or smaller business threat to organizations?

71%

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?

68%

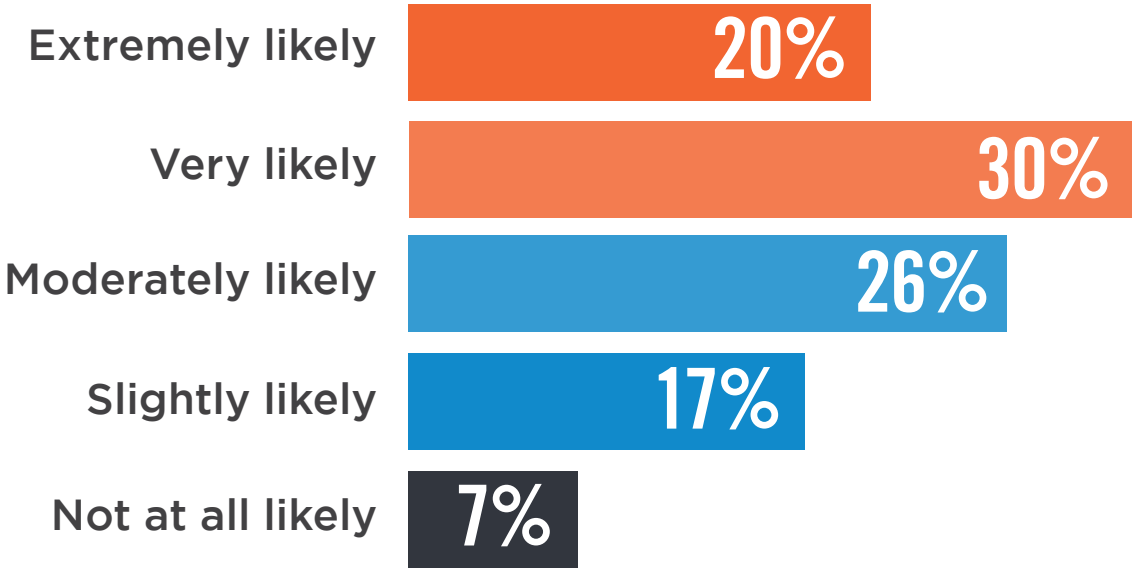


believe malware and ransomware attacks will be more frequent

MALWARE OUTLOOK

When asked about their risk of being affected by malware in the next 12 months, a majority of 76% estimate the probability at least moderately likely.

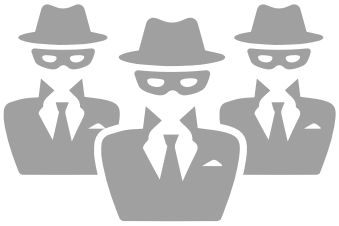
What is the likelihood that your organization will be a target of a malware/ransomware attack in the next 12 months?



CYBERCRIMINALS BEHIND ATTACKS

Survey participants believe that organized cyber criminals (67%), opportunistic hackers (65%) and state-sponsored hackers (40%) are the biggest groups behind malware and ransomware attacks.

Who do you believe is behind malware / ransomware attacks on your organization?



67%

Organized cyber-criminals

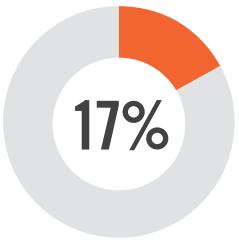
65%

Opportunistic hackers (non-organized)

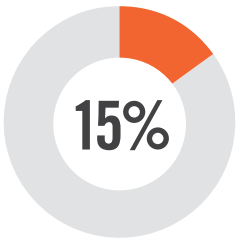
40%

State-sponsored hackers

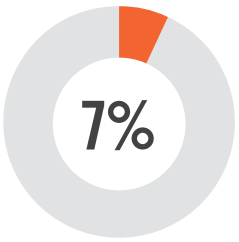
Political hacktivists



Disgruntled/ former employees



Competitors



Dissatisfied customers

Other 14%

RANSOMWARE STRAINS

Ransomware has quickly emerged as a lucrative venture for cybercriminals, in part due to more sophisticated tools for creation and deployment. Most notable ransomware strains recognized by security professionals are WannaCry (80%), CryptoLocker (73%), and Petya (55%). However, it is important to note that lesser known ransomware strains should not be dismissed as less powerful as the results can be just as damaging to any organization.

What ransomware strains are you generally most aware of?

80%

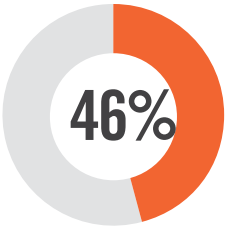
WannaCry

73%

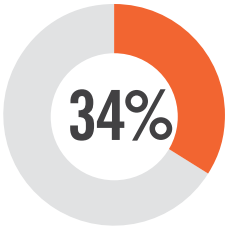
CryptoLocker

55%

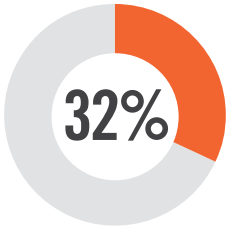
Petya



CryptoWall



Locky



TorrentLocker

BadRabbit

ZCryptor 28% | TeslaCrypt 28% | Jigsaw 23% | CTB Locker 21% | Cerber 18% | Crysis 16% | Spider 15% | GoldenEye 14% | Bit payment 11% | KeRanger 7% | LeChiffre 5% | Jaff 5% | Other 7%

WHAT MOTIVATES ATTACKERS

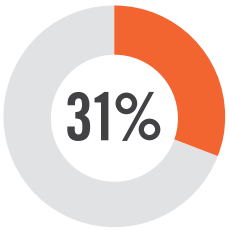
Financial gain (77%) tops the list of motivators for malware and ransomware attacks, followed by a desire to sabotage and disrupt business activities (54%). But while money extortion is the most common motivation for cybercriminals, in some cases attackers are hacking for fun (31%), state-sponsored attacks (25%) and political beliefs (17%).

What do you believe is the main motivation for malware / ransomware attacks against your organization?

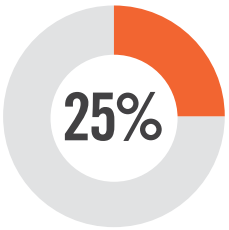
77%
Financial gain

54%
Sabotage/ disruption of business

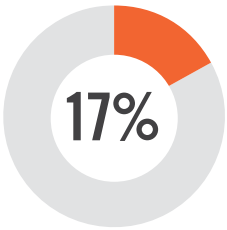
Cyber espionage



Entertainment (hacking just for fun)



State-sponsored international attack



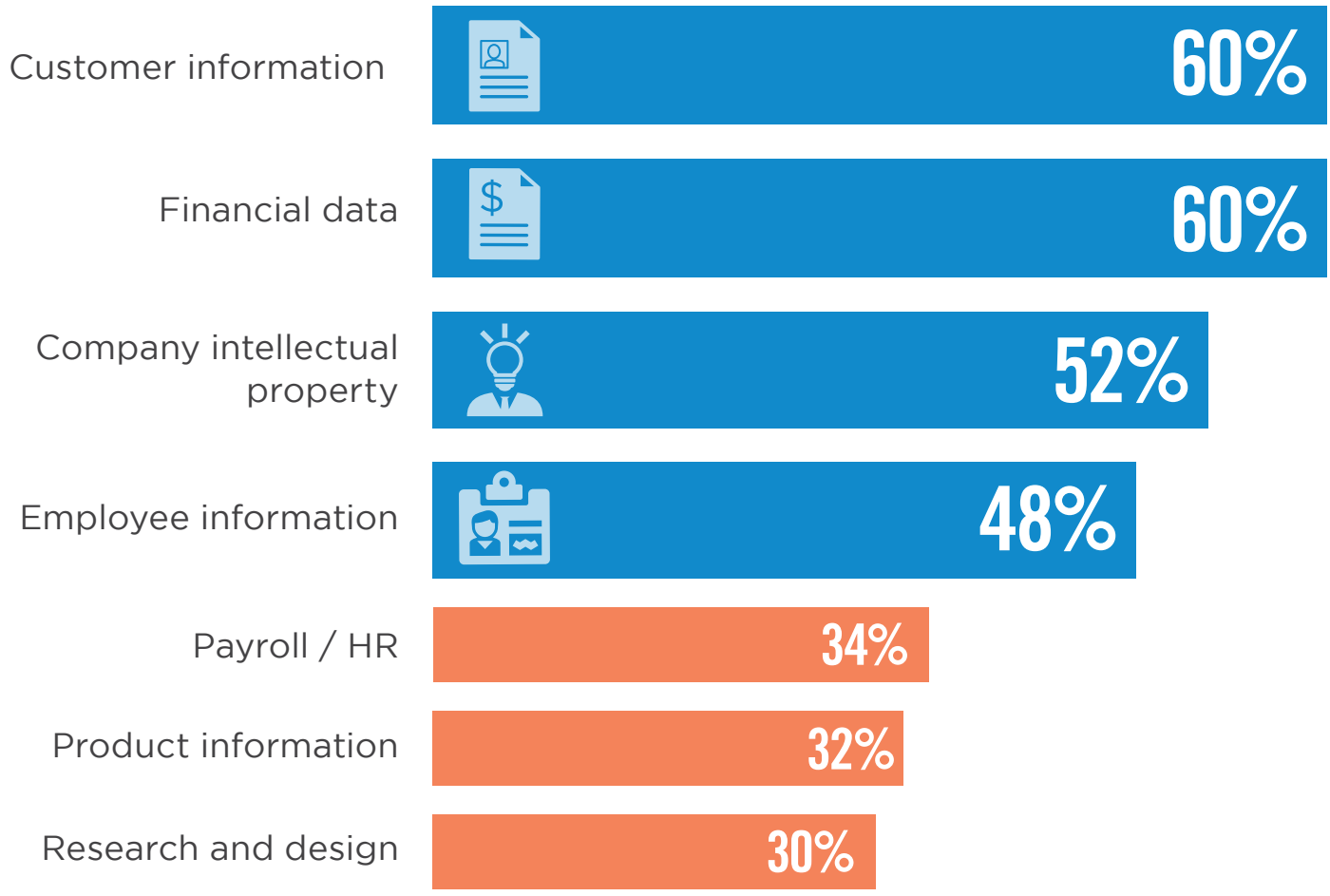
Political motivation

Revenge for a bad experience with organization 13% | Don't know/other 6%

DATA AT RISK

Data has become a strategic asset to virtually every organization and a high value target for cybercriminals. Our research reveals that the information most at risk from ransomware attacks is customer information (60%), tied with financial data (60%), followed by company intellectual property (52%).

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

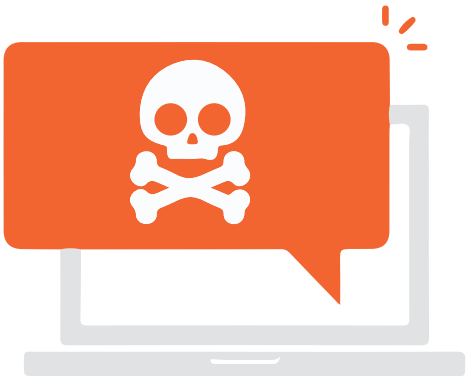


Other 8%

RANSOMWARE EXPERIENCE

More than 4 out of 10 organizations surveyed (42%) said they experienced ransomware attacks, up from 37% in last year's survey. Fifty-eight percent of respondents have not been affected by ransomware yet or aren't aware of a previous or ongoing attack.

Has your organization suffered from ransomware attacks in the past?



42%
YES
My organization has been affected by ransomware

58%
NO

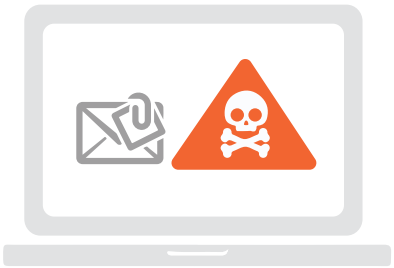
MALWARE TYPES

There is a wide and quickly evolving array of malware types, and new variants are created virtually every day. Ransomware is the top offender at 34%, followed by fileless malware (13%) and spyware (9%).

What types of malware are you most concerned about?

34%

Ransomware

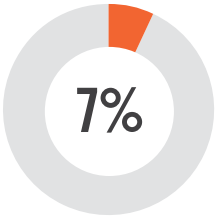


13%

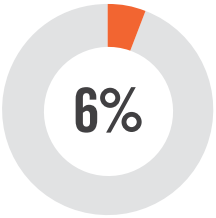
Fileless malware

9%

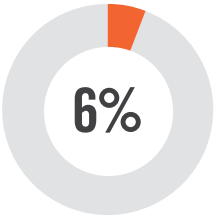
Spyware



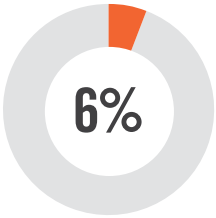
Bots



Viruses



Trojans



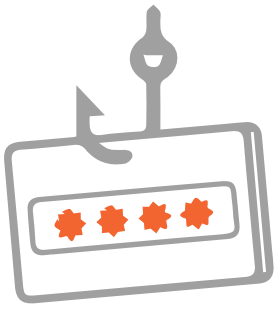
Worms

Rootkits 6% | Cryptojacking 5% | Adware 2% | Other 6%

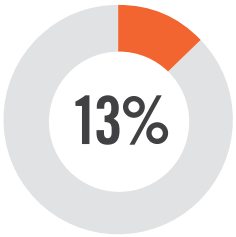
MOST DANGEROUS MALWARE ATTACK

Cybersecurity professionals in our survey consider spear-phishing emails the single most dangerous malware attack vector at 54%, followed by trojans (13%), and man-in-the-middle attacks (10%).

What malware attack vectors do you consider most dangerous?

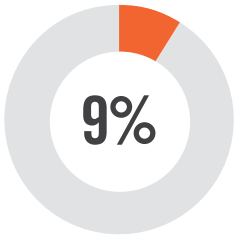


54% Spear-phishing emails

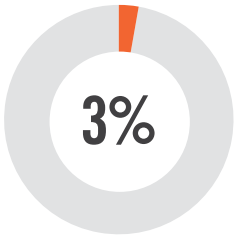


Trojanized Software

Man-in-the-middle attacks



Web server exploits



Cross-site scripting

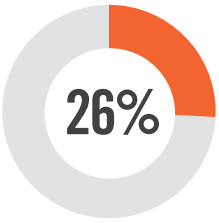
SQL injection 3% | Domain spoofing 3% | Watering hole websites 2% | Other 3%

RANSOMWARE TYPES

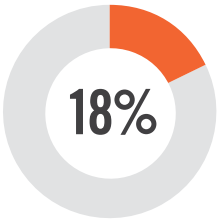
There is a wide array of ransomware types and new variants are created every day within each category. The organizations affected by ransomware overwhelmingly confirm that they encountered encrypting ransomware (or cryptoware that encrypts files and makes them inaccessible) as the top offender at 77%.

What type of ransomware infected your organization?

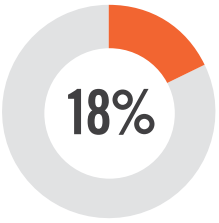
77% **Encrypting ransomware or Cryptoware**
(encrypts files and makes them inaccessible)



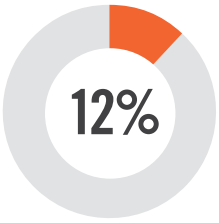
Ransomware that encrypts MBR or NTFS (prevents victims' computers from being booted up in a live OS environment)



Non-encrypting ransomware or lock screens (restricts access to files and data, but does not encrypt them)



Mobile device ransomware (infects cell-phones through "drive-by downloads" or fake apps)



Leakware or extortionware (exfiltrates data that the attackers threaten to release if ransom is not paid)

Not sure/other 13%

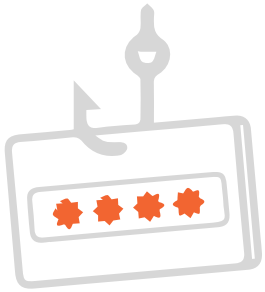
HOW RANSOMWARE ENTERS

Email and web use represent the most common infection methods used to gain organizational access. It's only a matter of time until an employee opens an email attachment (63%), answers a phishing email (62%) or visits a compromised websites (48%).

How has ransomware entered your organization?

63%

Email attachments



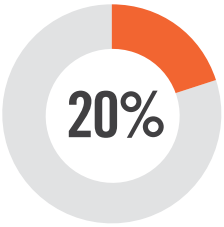
62%

Phishing emails

48%

Users visiting malicious or compromised websites

Exploits targeting vulnerable systems



Scan and exploit

Not sure/other 3%

SECURITY IMPACT ON IT

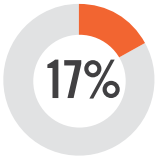
Malware is impacting organizations at the business level as well as from an IT security policy and control perspective. On the business side, malware attacks caused productivity loss (58%) and increased spending on IT security (52%). At the IT operations level, malware is causing system downtime (50%) and forcing cybersecurity professionals to update IT security strategy to focus on mitigation (45%).

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

BUSINESS IMPACT

58%
Productivity loss

52%
Increased spending on IT security



Revenue loss

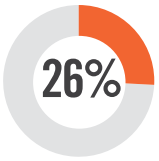
Damage to company reputation

Negative press/ bad publicity

IT OPERATIONS / SECURITY IMPACT

50%
System downtime

45%
Change of IT security strategy



Data loss

Loss of confidence in existing cybersecurity solutions

Senior IT staff (CIO, CISO)lost their jobs

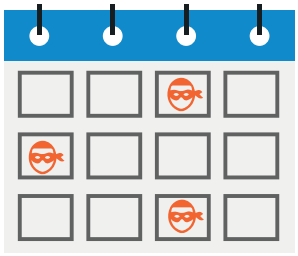
We did not experience any ransomware attacks 5% | Other 3%

RANSOMWARE ATTACK FREQUENCY

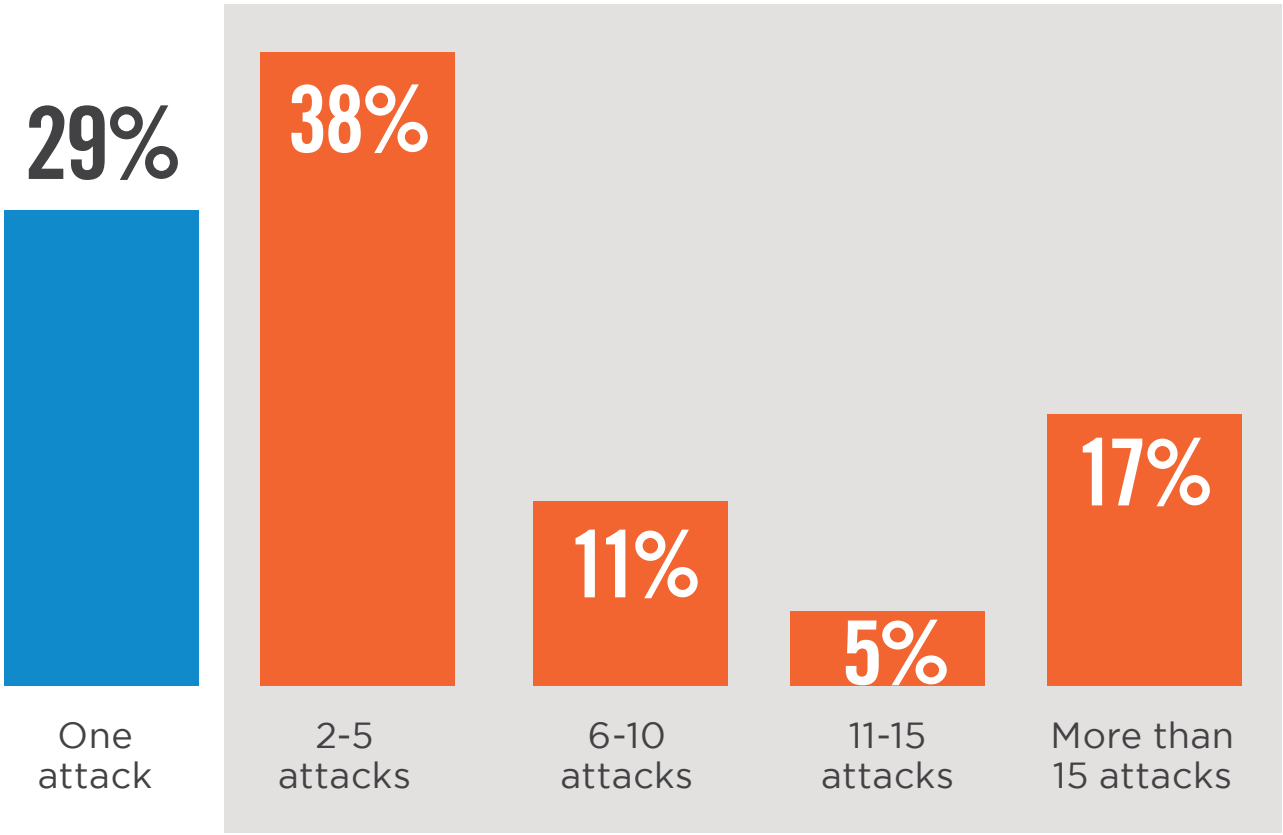
In the past 12 months, the variety and frequency of ransomware incidents directed at organizations have increased dramatically. Of those organizations that experienced ransomware attacks, 67% experienced up to five attacks, while the remaining third of organizations experienced 6 or more attacks.

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

71%



of organizations have experienced
2 more more attacks in the last 12 months.



DETECTION OF THREATS

There are numerous security tools available to help cybersecurity professionals identify and monitor cyber threats. The vast majority of identified malware/ransomware attacks were detected through anti-malware/antivirus/endpoint security tools (86%), email and web gateways (56%), and intrusion detection systems (56%) tied at second place. Unfortunately, many malware attacks succeed in evading detection.

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

86%

Anti-malware/antivirus/ endpoint security tools

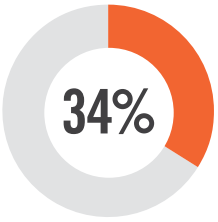
56%

Email and web gateways

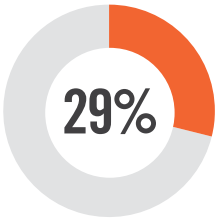
56%

Intrusion detection system

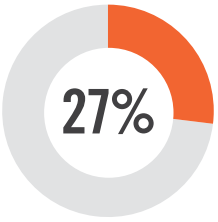
Network behavior monitoring



Detected by compromised user



User behavior monitoring



File monitoring

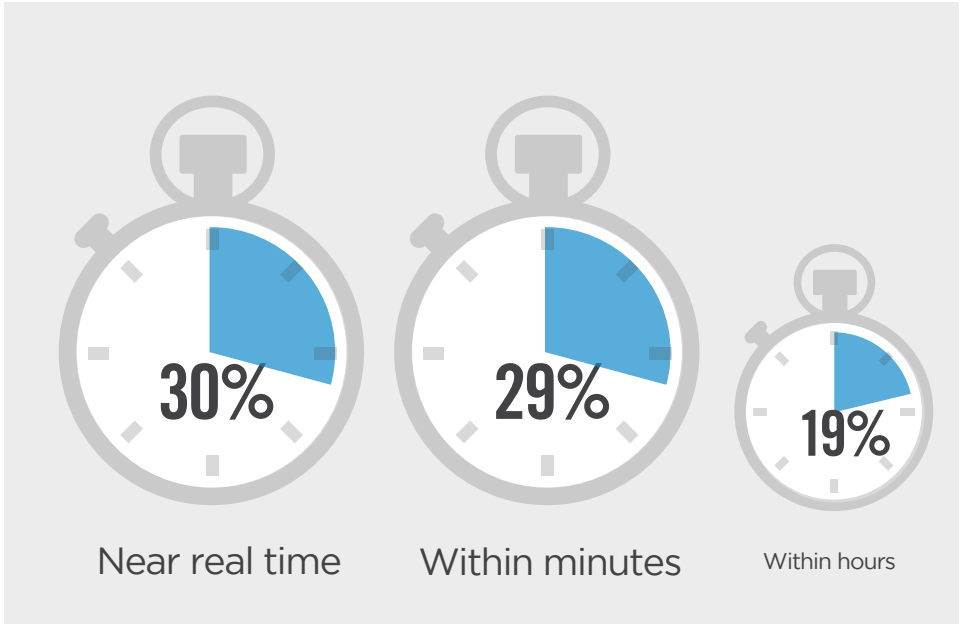
We cannot detect ransomware 4% | Not sure/other 6%

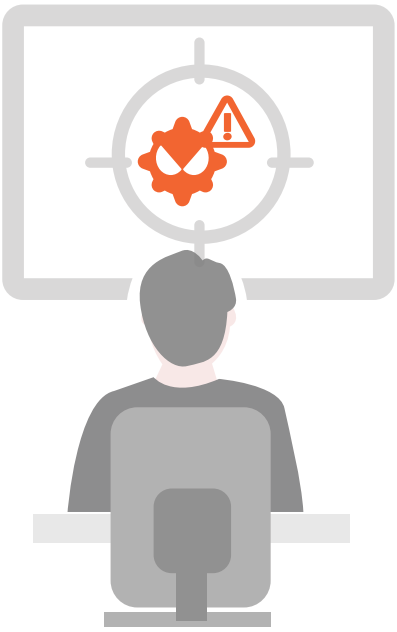
SPEED OF DETECTION

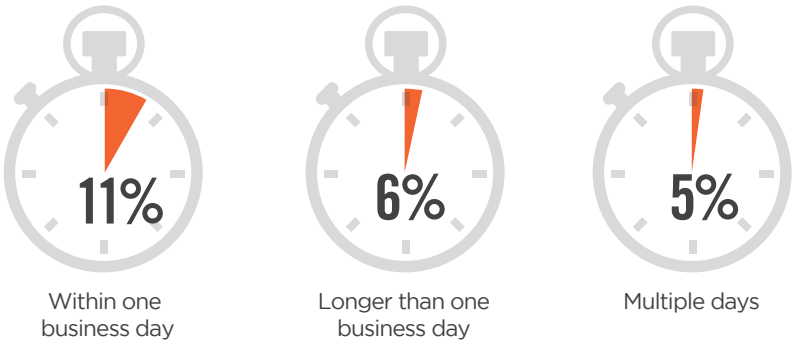
While the speed of malware/ransomware detection varies based on the strain and organizations' detection capabilities, most attacks are typically detected within hours (78%). Twenty-nine percent of organizations claim detection is near real time or within minutes. The rate and speed of malware/ransomware detection is critical in combating fast moving attacks before they succeed in spreading across the network.

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

78% Most attacks are typically detected within hours



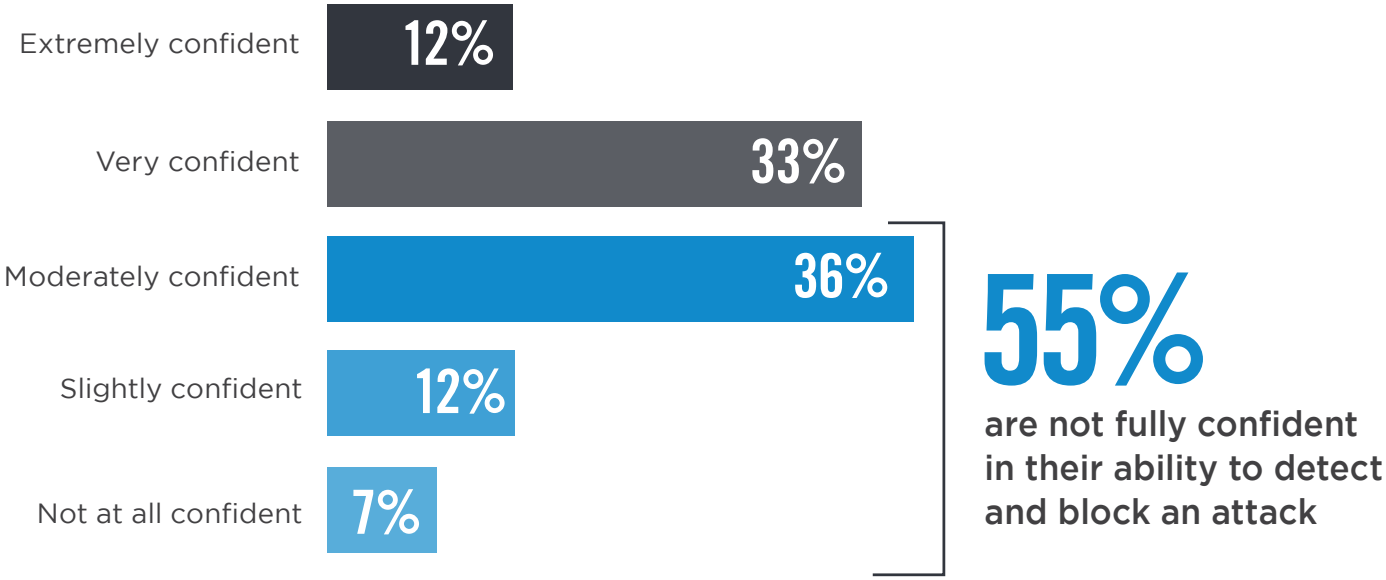




CONFIDENCE IN REMEDIATION

A majority of 55% of cybersecurity professionals are not fully confident in their organization's capacity to detect and block a malware/ransomware attack before it spreads to critical IT systems across the organization. Only 12% are extremely confident, 33% percent are very confident.

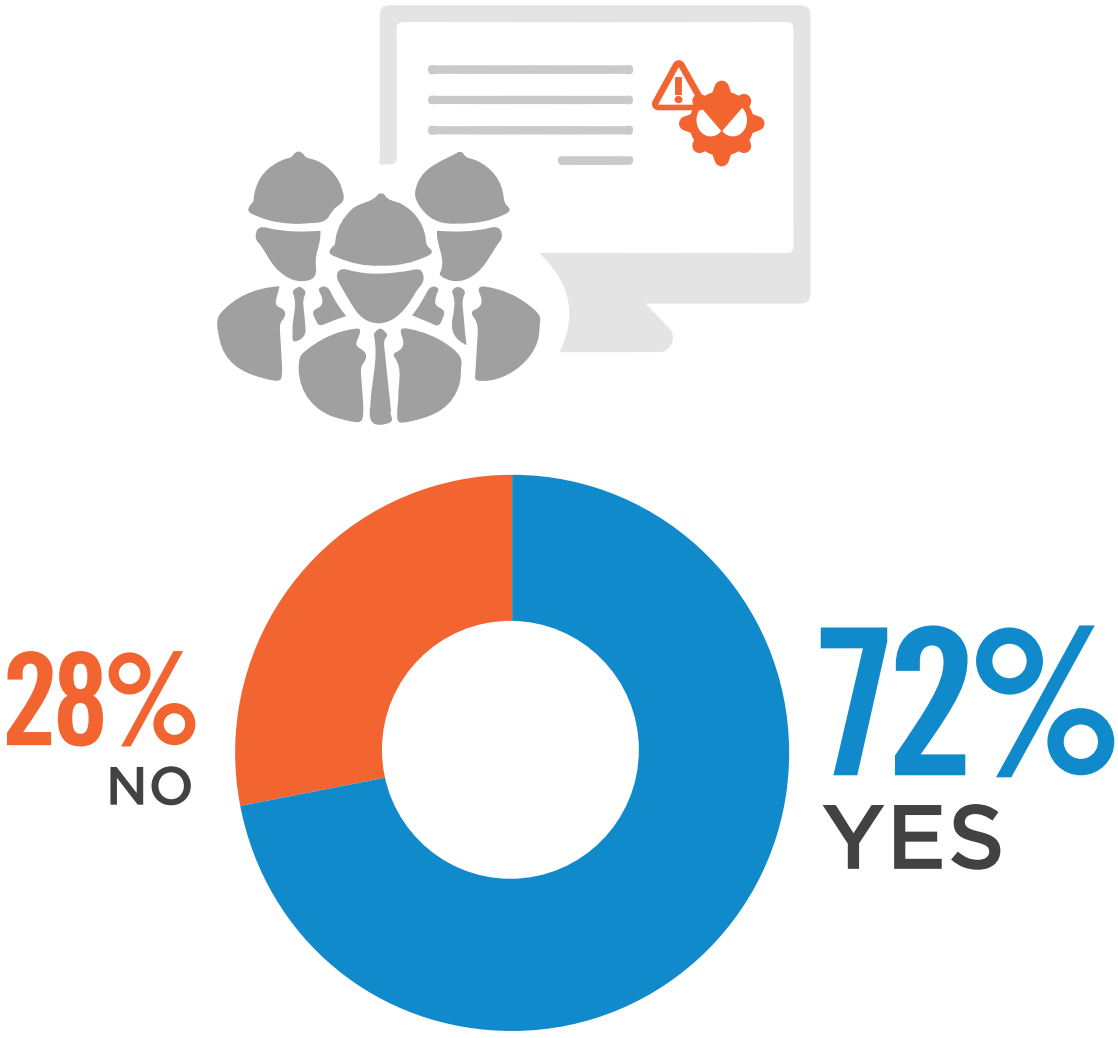
How confident are you that your organization's defenses are capable of detecting and blocking malware /ransomware before it spreads and infects critical systems and files?



RESPONSE TEAM READINESS

Only three out of ten organizations do not have an Incident Response team in place to respond to a malware / ransomware attack. The good news is organizations realize that incident response are critical pieces of effective, multi-layer defense against attacks, and the overwhelming majority (72%) have incident reponse teams in place.

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



CONTAINING ACTIVE INFECTIONS

How do organizations contain an active infection? Half (50%) utilizes incident response teams and tools to detect and isolate the malware, followed by the deployment of sophisitcated malware detection and response solutions (40%).

How does your organization detect and respond to lateral movement or infected computers that participate in a botnet?"

50%

Incident response team to detect and isolate

40%

Advanced, behavior-based malware solution that protect endpoints and has the ability to detect with automated mitigation/remediation capability

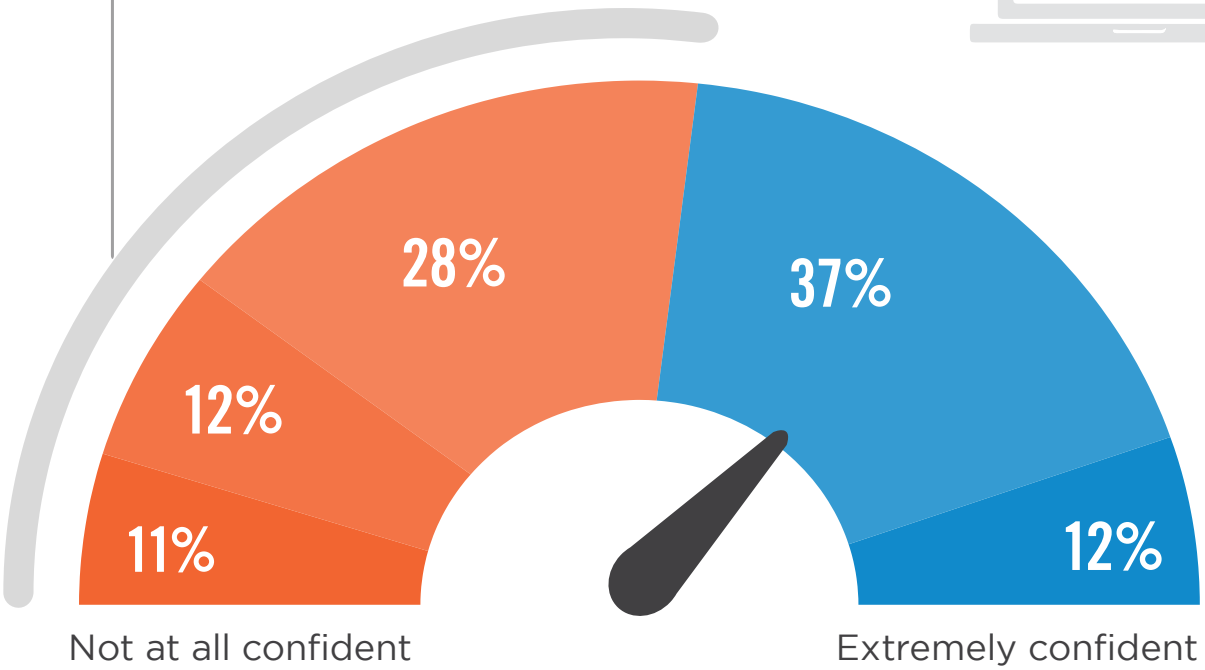
This scenario is unlikely to happen in my organization 19% | Don't know/other 23%

CONFIDENCE IN REMEDIATION

We asked cybersecurity professionals to assess their organization's capacity to remediate a ransomware attack in progress that has already encrypted files and spread to critical IT systems across the organization. Only 12% are extremely confident in their organization's abilities to unlock or restore affected files and systems. Thirty-seven percent are very confident. An alarming 11% is 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?

51% lack confidence in their organization's ability to remediate a ransomware infection.

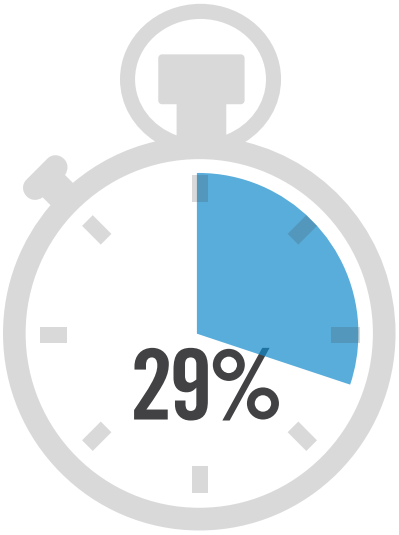


Not at all confident | Slightly confident | Moderately confident | Very confident | Extremely confident

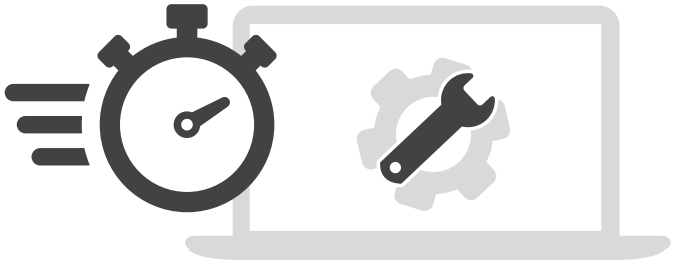
SPEED OF RECOVERY

A majority (48%) say they can recover from a ransomware attack within a day, while 41% estimate it will take more than one day to a few weeks to recover. Only 11% of the organizations believe they will never fully recover. Speed of recovery is absolutely critical as cost escalates with every hour the business cannot fully operate.

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

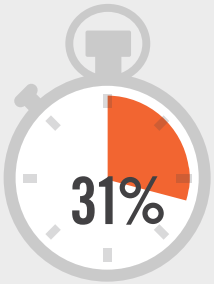


A few hours



52% need longer than a day to recover from a ransomware attack.

A day



A few days

A week

A few weeks

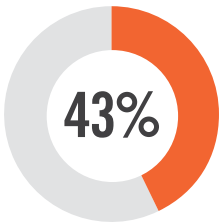
Potentially never recover

ATTACK RESPONSE TACTICS

Following a ransomware attack, cybersecurity professionals can deploy a number of defensive responses. The single most common response motion (77%) is containing the damage by isolating and shutting down all infected systems and accounts, eradicating the malware, followed by recovery from backup files.

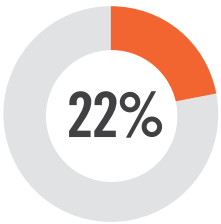
How would your organization respond when it has been detected that ransomware has attacked your systems?

77% Isolate and shut down offending systems and accounts, recover encrypted files from backups, mitigate the initial attack vector if possible

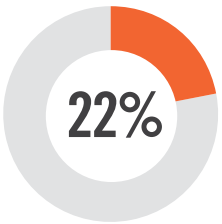


Proactively shut down core systems to prevent spread

Contact cybersecurity technology vendor



Immediately call law enforcement



Engage a third-party incident response service

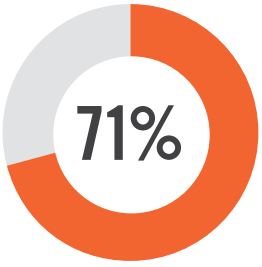
Attempt to decrypt files ourselves 20% | Notify customers 17% | Contact cyber insurance provider 17% | Attempt to negotiate with the attackers 4% | Pay the ransom 4% | Other 4%

RANSOMWARE DEFENSE MOTIVATORS

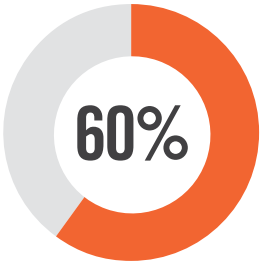
The biggest motivator for improving their organization's ransomware defense is the protection of sensitive business data against attack (77%), followed by preventing system downtime (71%) and mitigating the financial costs arising from ransomware attacks (60%).

What is your organization's primary driver for improving ransomware defense?

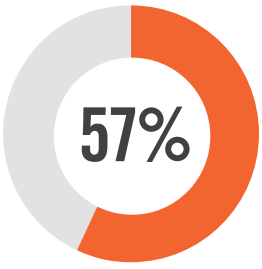
77% Protecting confidential data related to the business and clients



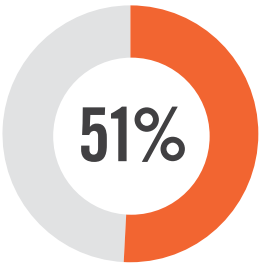
Saving the organization from potential downtime



Mitigating the financial costs arising from ransomware attacks



Protecting the reputation of the brand



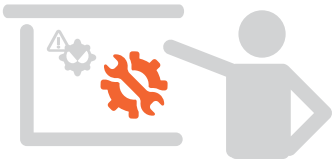
Staying a step ahead of emerging threats

Other 1%

EFFECTIVE PREVENTION

There are a myriad of cybersecurity tools and policy controls available to combat malware/ransomware early on. Security professionals rank user awareness and training as the most effective means to prevent and block ransomware (75%). The survey indicates both Anti-Malware/Antivirus/Endpoint security solutions (74%) and Email and web gateways (64%) were highly effective as preventive approaches to malware/ransomware threats.

What security solution(s) would you say is (are) most effective to prevent and block malware/ransomware?



75%

User awareness and training

74%

Anti-malware/antivirus/endpoint security solution

64%

Email and web gateways

63%

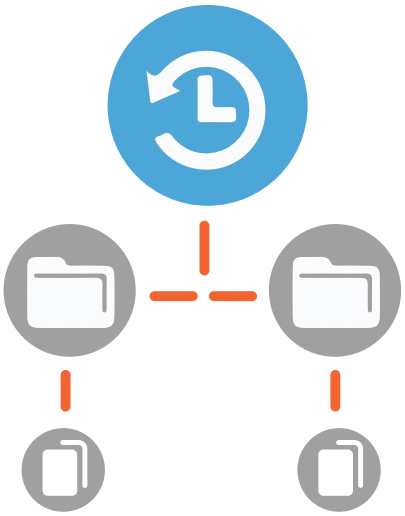
Updating/patching operating systems and software with latest versions

Network IDS/Traffic Monitoring 56% | Spam filters 53% | Internal access controls and authentication 53% | Behavior based/machine learning endpoint protection 51% | Infrastructure security monitoring 51% | Endpoint Detection and Response (EDR) 43% | File monitoring 39% | Application whitelisting 38% | Sandbox 35% | User monitoring 35% | Other 5%

MALWARE/RANSOMWARE RESPONSE

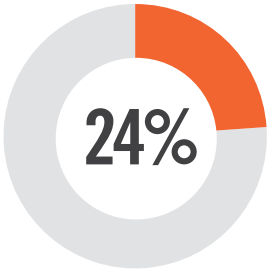
Cybersecurity professionals continue to view data backup and recovery (57%) by far as the most effective solution to respond to a successful ransomware attack. This way, organizations can often restore critical data without having to pay cybercriminals.

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

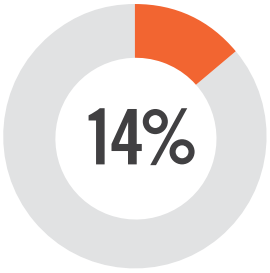


57%

Data backup and recovery response



Threat intelligence



Behavioral analytics

Cyber insurance

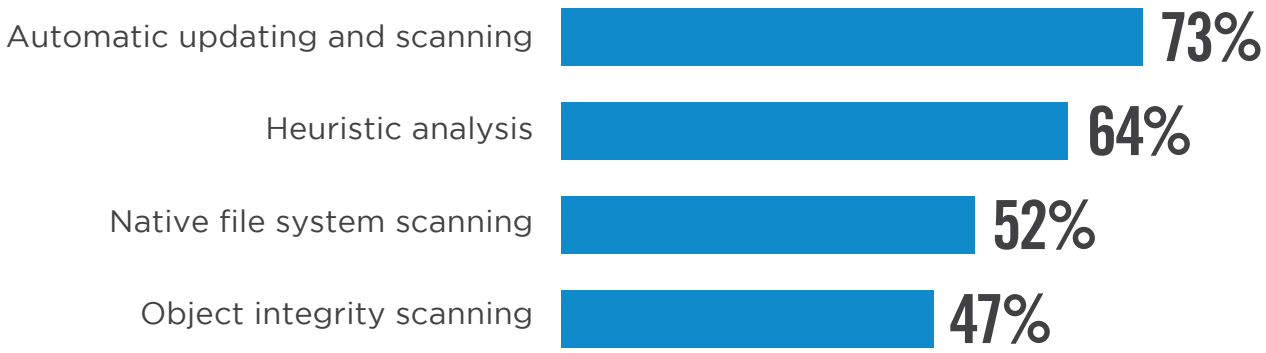
MALWARE SECURITY SOLUTIONS

The vast majority of organizations (88%) is confident that endpoint security solutions can protect their servers against malware attacks - perhaps and overly optimistic stance for those using solutions that aren't native to their operating systems.

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

The most important features for server-level malware security solutions include automatic updating and scanning of systems (73%), heuristic analysis (64%) and scanning of native files (52%) and object integrity (47%).

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



Other 4%

ENDPOINT SECURITY

To stay ahead of evolving security threats, organizations employ a multi-layered security approach, including strong endpoint protection. When asked about the most effective endpoint security capabilities to protect against malware, most respondents agree that detecting and blocking traffic or executables at the first sign of malicious behavior (65%), and blocking attacks pre-execution (63%) rank as the most effective endpoint security capabilities.

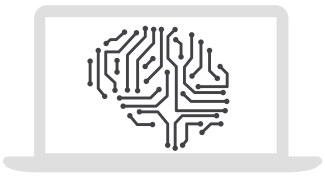
What do you think is the most valuable endpoint security technology to have?

65%

Detect and block at the first sign of malicious behavior such as encryption

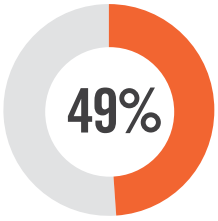
63%

Block ransomware and other at pre-execution to stem the spread

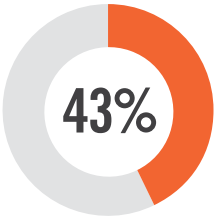


49%

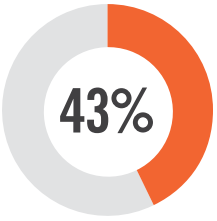
Non-signature based detection and prevention technologies
(such as machine learning and behavior-based)



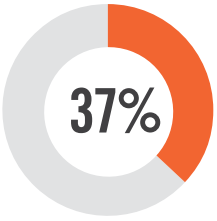
Advanced file analysis (i.e. nextgen antivirus tools)



Fileless/exploit prevention through real-time behavior analysis



Built-in web security preventing access to phishing, fraudulent or exploit-hosting sites



Automatic mitigation including the ability to roll back changes

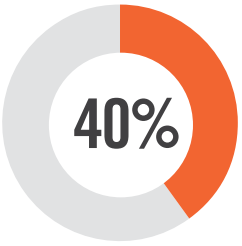
File-based detection - signature-based traditional Antivirus 37% | Endpoint integrated sandbox 36% | Built-in anti-exploit 29% | Other 2%

OBSTACLES TO DEFENSE

The three biggest obstacles standing in the way of stronger malware defense are all about resources and staying current on the latest exploits: lack of budget (51%), dealing with evolving sophistication of attacks (40%), and tied at 36%, poor user awareness and lack of human resources.

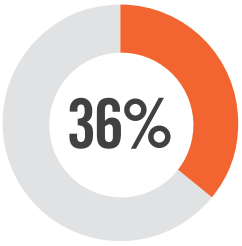
What do you believe to be your organization's biggest obstacles to improving malware/ransomware defense?

51%
Lack of budget

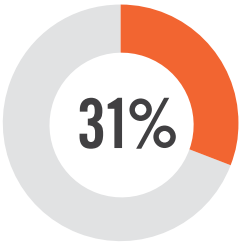


Evolving sophistication of attacks

Poor user awareness



Lack of human resources



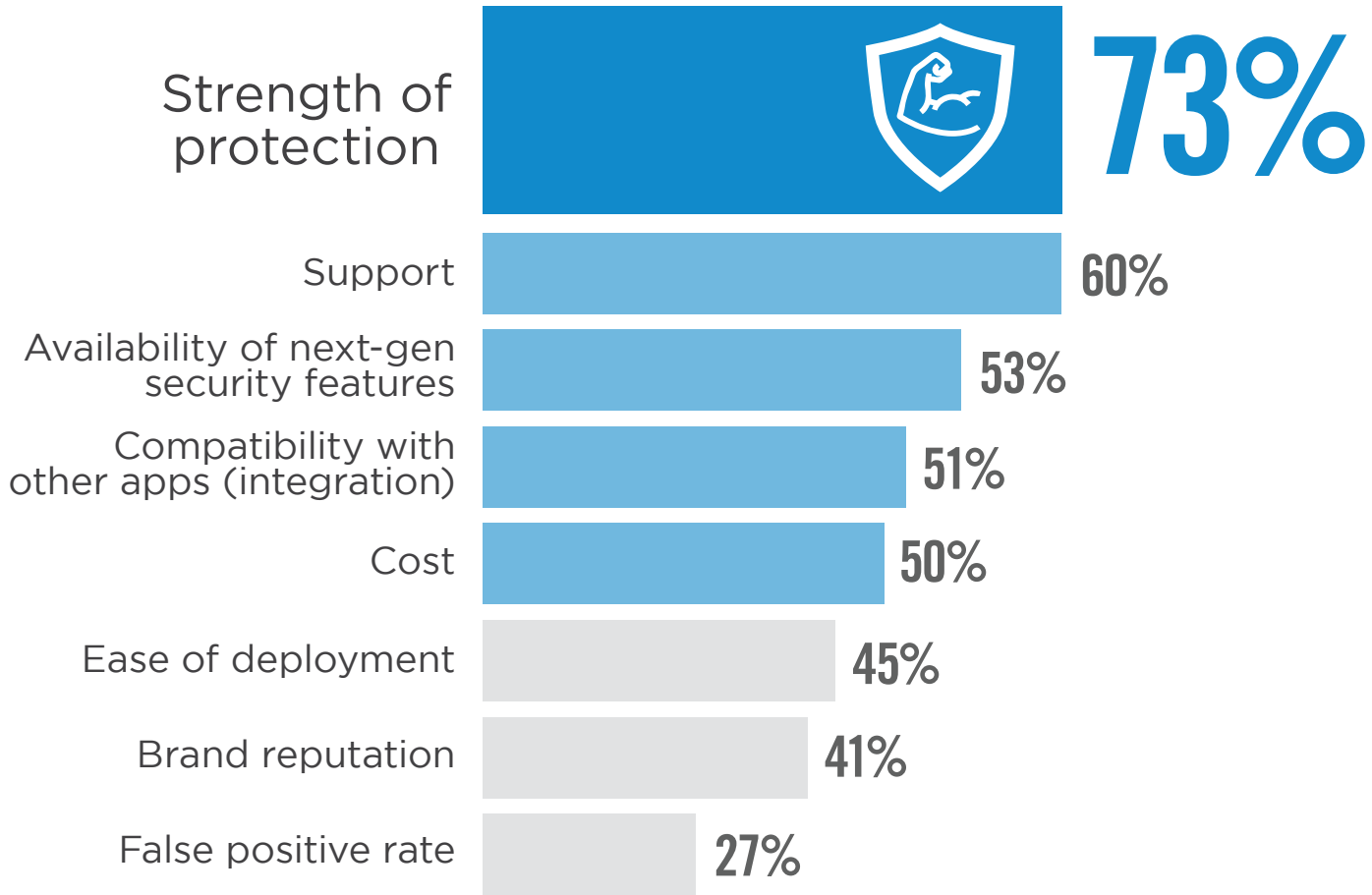
Growing proliferation of attacks

Uncertainty what security solution to use 24% | Lack of executive sponsorship 22% | Our partners' lack of preparedness or response 14% | Other 5%

SOLUTION PROVIDER CRITERIA

Choosing the right security provider is an investment decision that will significantly affect the security posture of your organization. The primary factor that respondents consider when choosing a solution is strength of protection (73%), followed by support (60%). Availability of next-gen security features (53%) compatibility with other apps (51%) and cost (50%) round out the top five selection criteria.

What are the main criteria that you consider when selecting a security provider to protect you from malware/ransomware attacks?

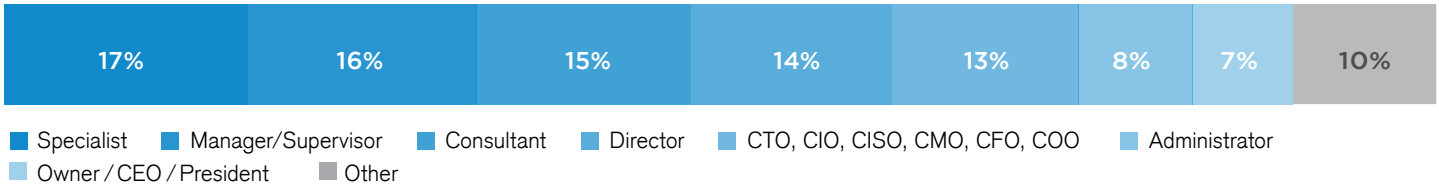


Other 4%

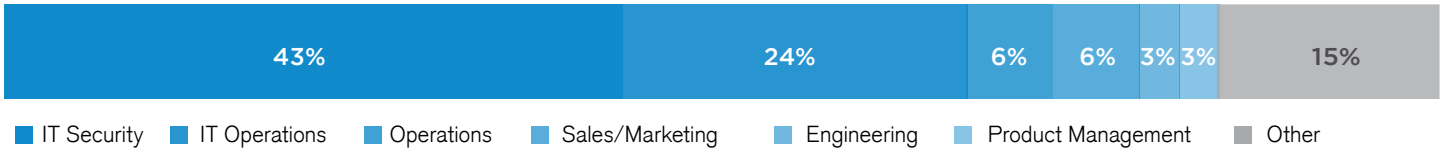
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of 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.

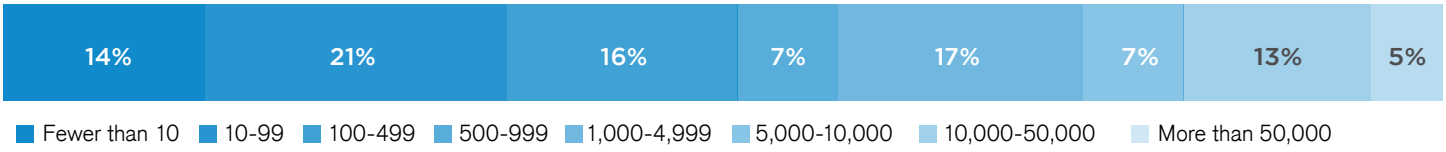
CAREER LEVEL



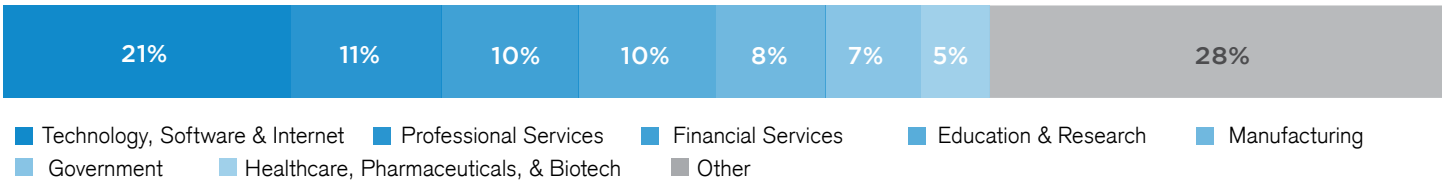
DEPARTMENT



COMPANY SIZE



INDUSTRY



HelpSystems helps you protect business-critical data with a suite of integrated and automated security solutions for defense in depth, comprehensive visibility, and streamlined reporting across your on-prem and cloud environments.

www.helpsystems.com