2019

# The Growing Threat of Ransomware

Cybersecurity Insiders and HelpSystems provided the majority of the data in this report which includes the latest malware and information security trends from an IT security leader's perspective.

secure OPS

# INTRODUCTION

**Key findings include:**

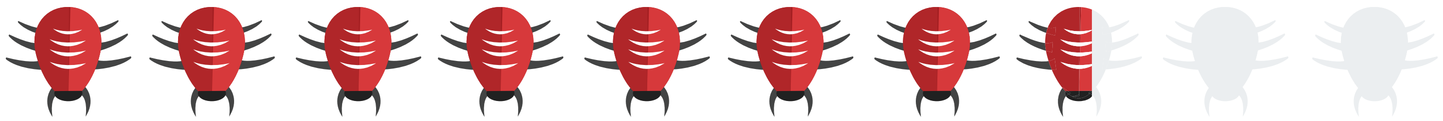
- The World Economic Forum Report listed cyber threats as the fourth greatest risk to world economies and the Cybersecurity Insider and HelpSystems survey confirm the perceived threat among security leaders.
- Malware, particularly ransomware has become one of the most destructive security threats affecting all types of organizations – the Verizon Data Breach Report supports this research and suggested 43% of all breaches affected small businesses.
- 70% of organizations believe malware and ransomware will become a larger threat to their organizations in the next year.
- Only 5% of survey respondents DID NOT experience a ransomware attack.
- 76% consider a malware attack in the next 12 months moderately to extremely likely.
- 86% percent of the survey respondents view malware and ransomware either as an extreme threat (49%) or moderate threat (37%).
- 54% consider phishing emails the most dangerous attack vector, followed by trojans with 13%.

The Verizon Data Breach Report suggested that approximately 70% of the attacks come from outsiders, 30% from insiders, 39% from criminal groups and 23% from state-affiliated actors which you will find is in line with the view of the survey respondents in the HelpSystems/Cybersecurity Insiders report

# MALWARE AND RANSOMWARE THREAT

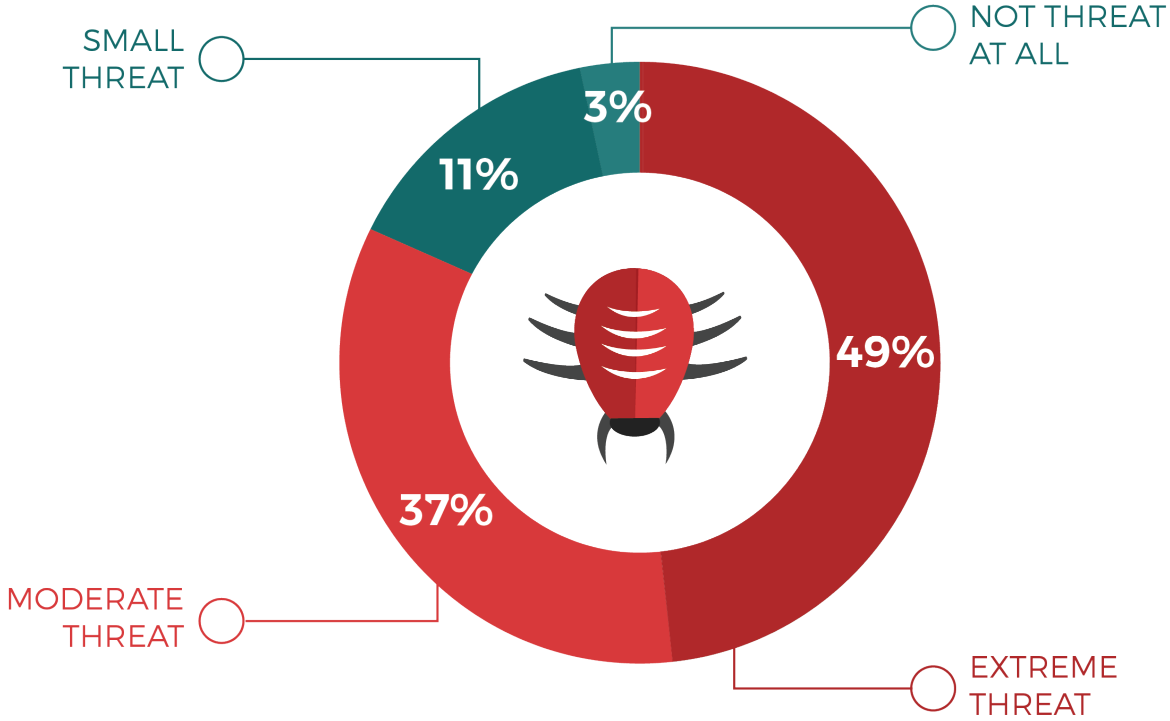
Only 3% of survey respondents thought malware and ransomware was no threat at all while 86% percent of respondents perceive them either as an extreme threat (49%) or moderate threat (37%)

**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

Because ransomware no longer requires technical knowledge to distribute, “script kiddies” are able to threaten organizations. Thus, A majority (71%) of IT security professionals predict malware and ransomware will 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.

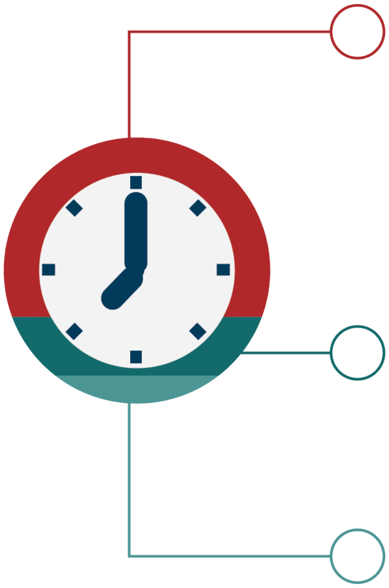
**24%**

No change

**5%**

Smaller threat

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



**68%**

believe malware and ransomware attacks will be more frequent

**22%**

No change

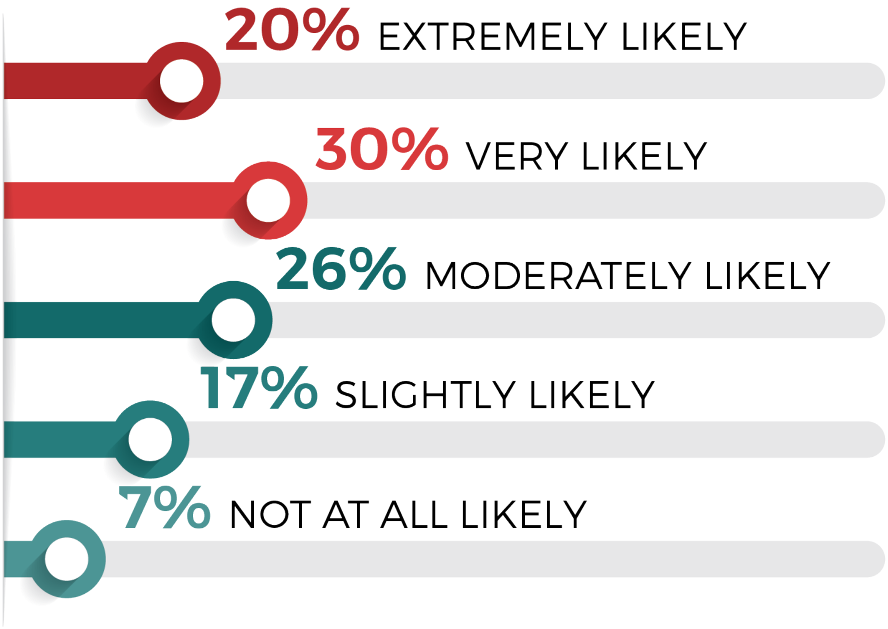
**10%**

Less 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.

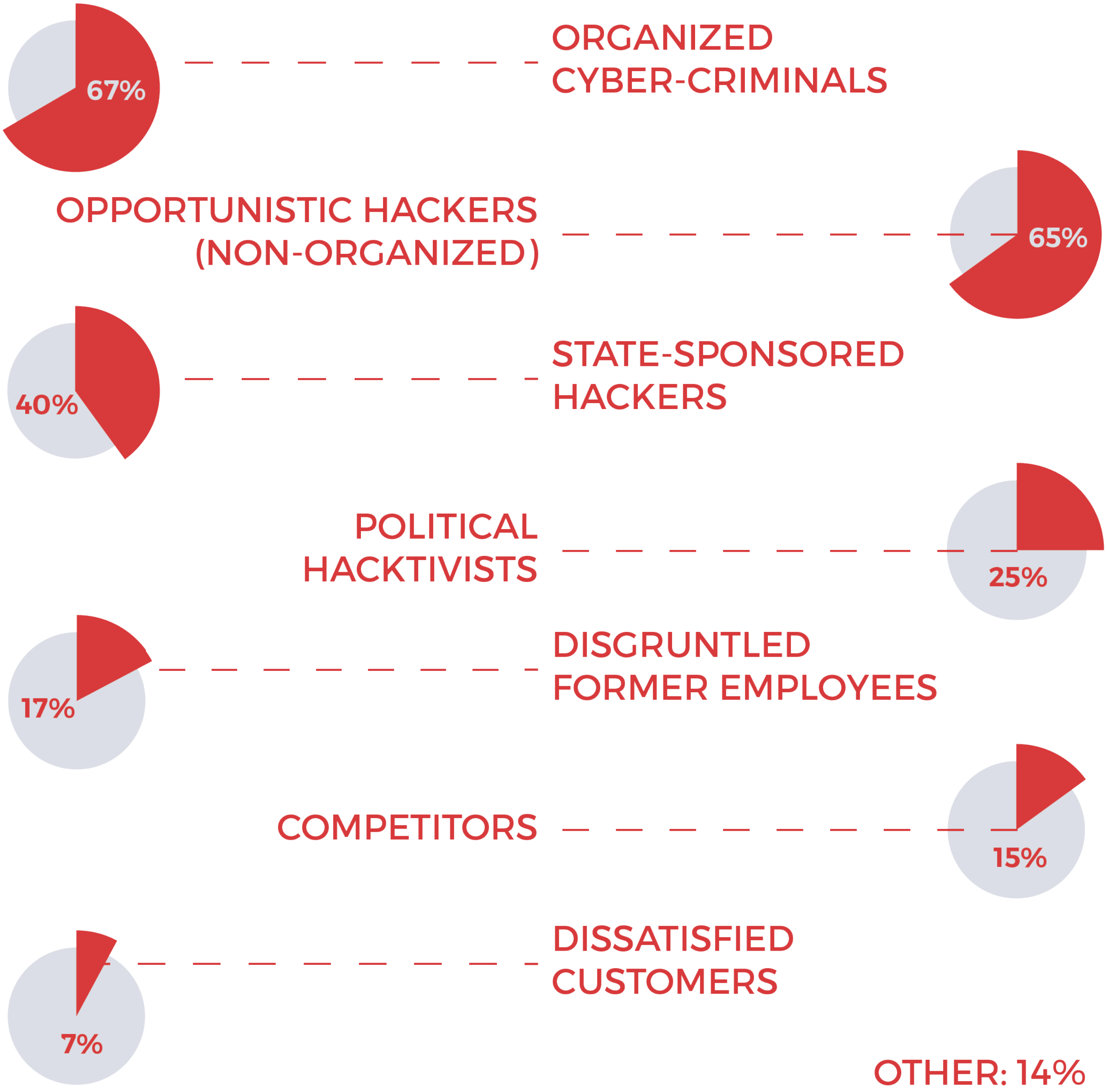
**What is the likelihood that your organization will be a target of a malware/ ransomware attack in the next 12 months?**



# CYBERCRIMINALS BEHIND ATTACKS

Organized cyber-criminal gangs, financially motivated hackers, and an increasing number of state sponsored organizations are responsible for attacks according to this survey group as well as the Verizon Data Breach respondents.

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



# RANSOMWARE STRAINS

Because Ransomware is so easily distributed among cybercriminals it has become the largest threat over the past couple of years. The ransomware strains recognized by security professionals in the survey are WannaCry (80%), CryptoLocker (73%), and Petya (55%).

**What ransomware strains are you generally most aware of?**

**80%**
WannaCry

**73%**
CryptoLocker

**55%**
Petya

**46%**
CryptoWall

**34%**
Locky

**32%**
TorrentLocker

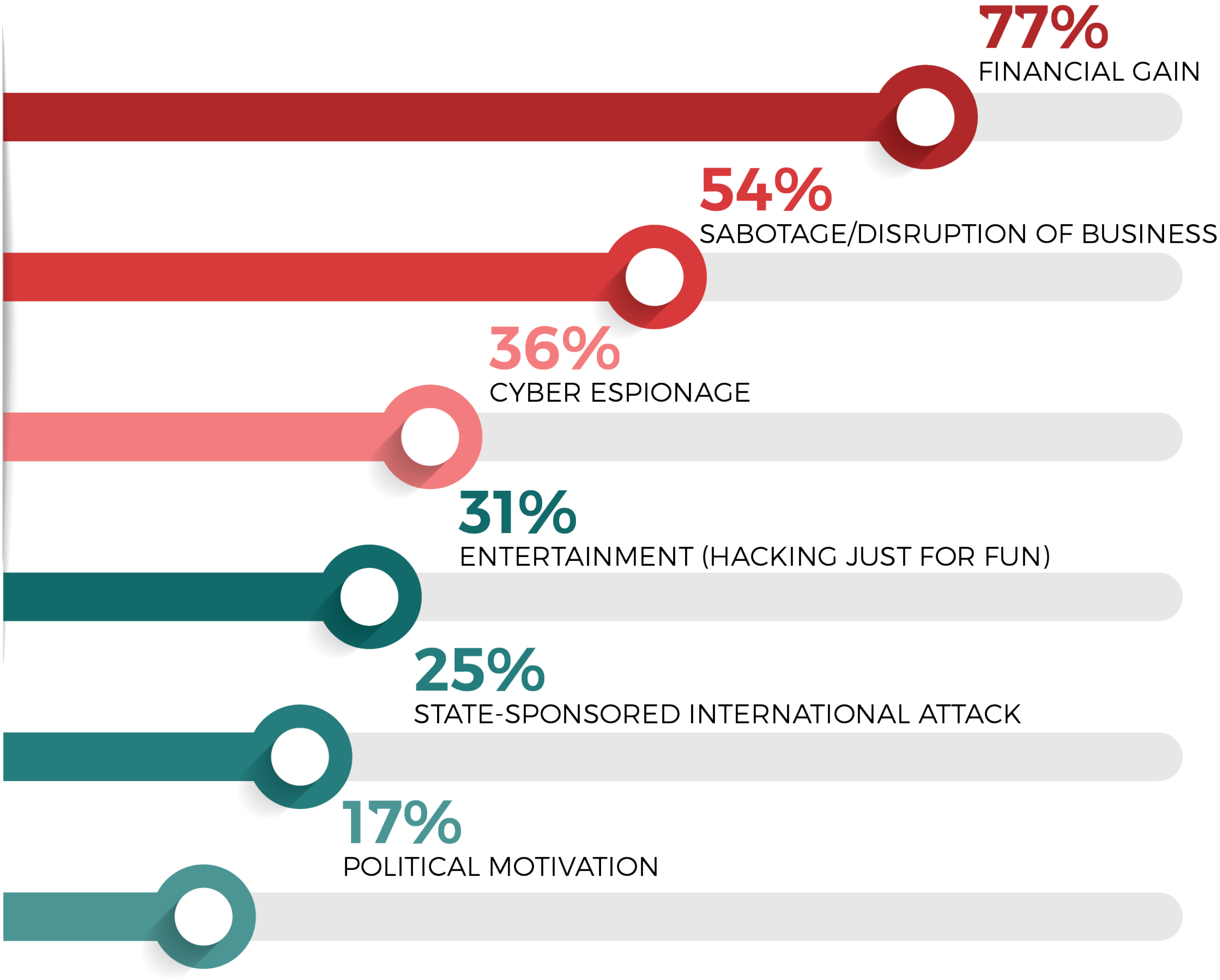
**30%**
BadRabbit

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 incentive is over 75% of what motivates cybercriminals to conduct attacks, followed by a desire to sabotage and disrupt business activities (54%).

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

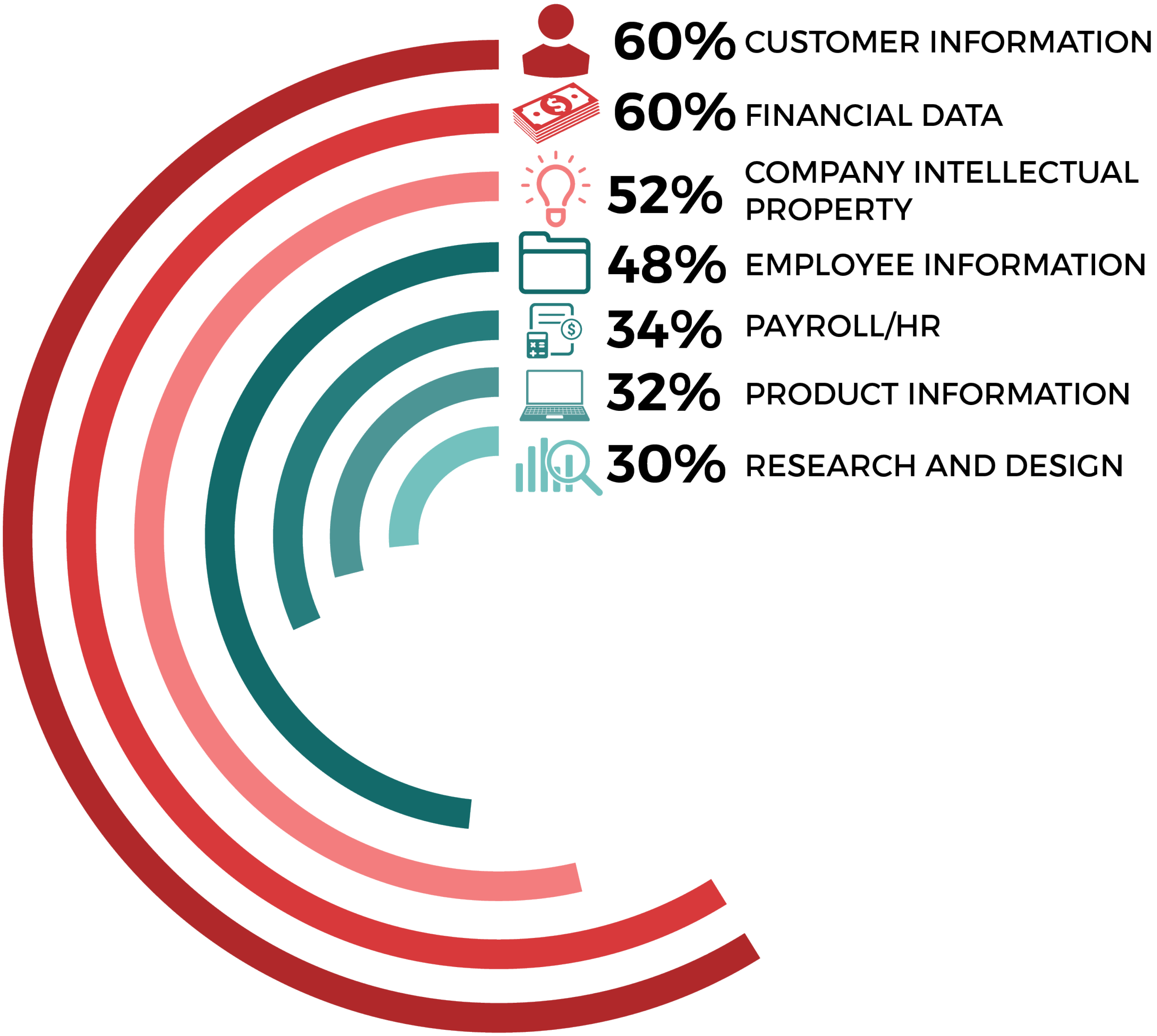


Revenge for a bad experience with organization 13%
Don’t know/other 6%

# DATA AT RISK

Customer information, financial data and organizational intellectual property tops the list of cybercriminal targets. Essentially, whatever sensitive information a company houses has become a commodity that can be exchanged for cash on the dark web.

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

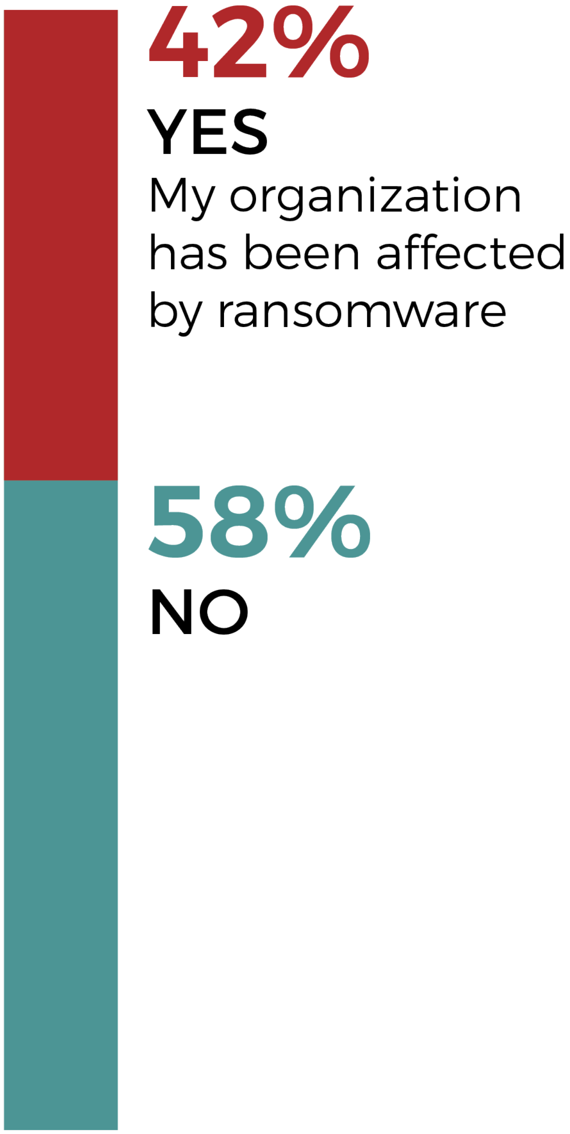


Other 8%

# 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.

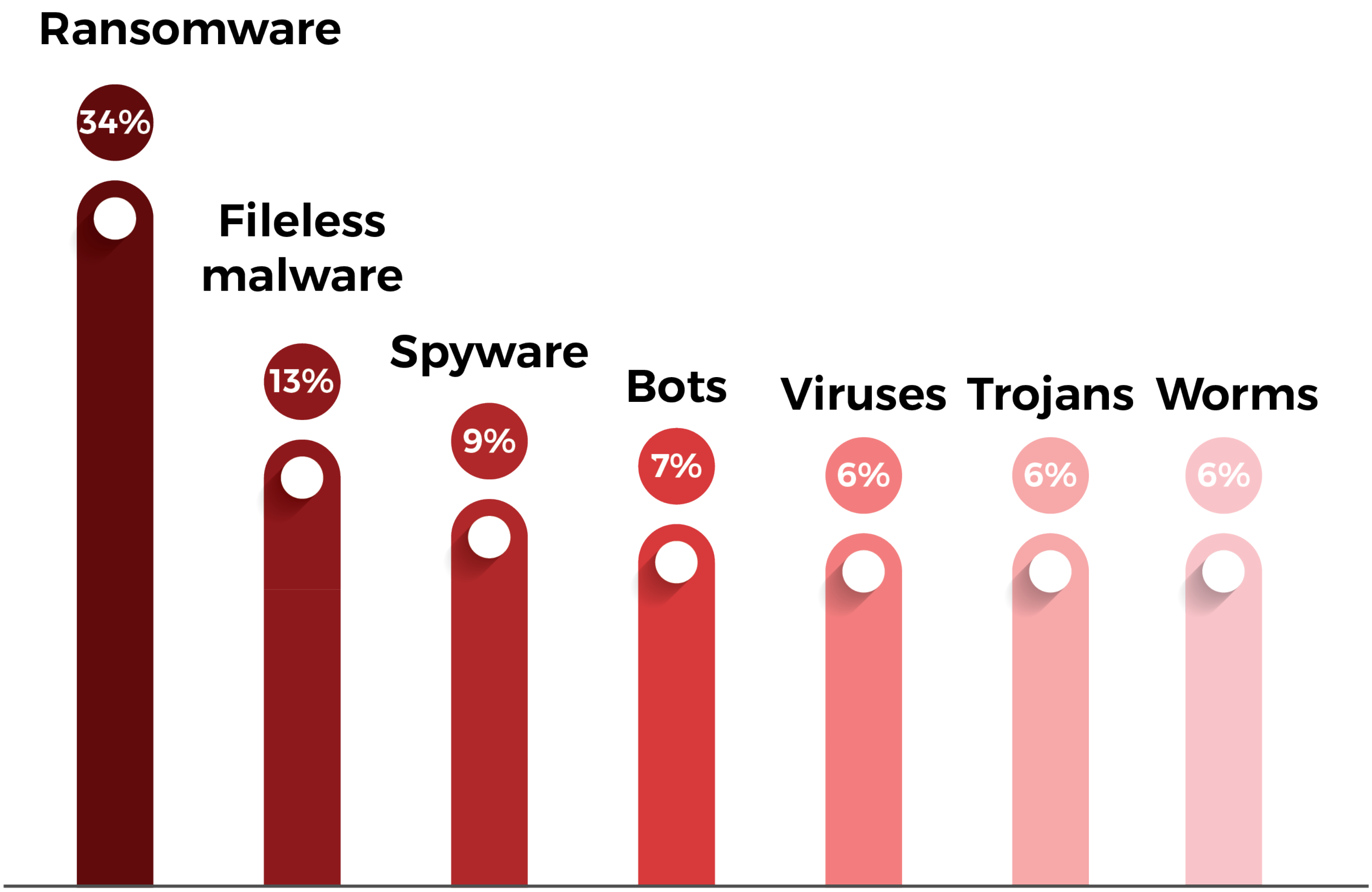
**Has your organization suffered from ransomware attacks in the past?**



# MALWARE TYPES

Ransomware and all the varieties of crypto-malware tops the concerns of IT security professionals and appears to be growing its lead over the past couple of years. Fileless malware which had been a top concern because of its ability to evade signature-based defenses is fading.

**What types of malware are you most concerned about?**



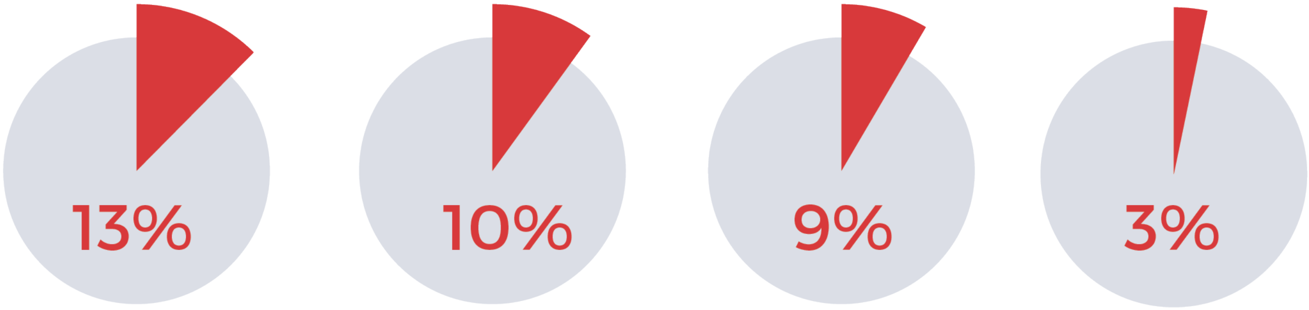
Rootkits 6% | Cryptojacking 5% | Adware 2% | Other 6%

# 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



13%
Trojanized Software

10%
Man-in-the-middle attacks

9%
Web server exploits

3%
Cross-site scripting

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

# RANSOMWARE TYPES

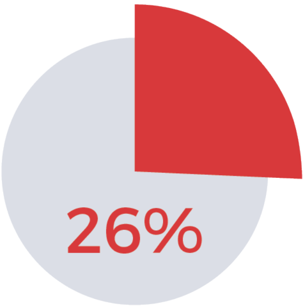
There is a wide array of ransomware types and new variants are created every day within each category. The organizations affected by ransomware overwhelmingly confirm that they encountered encrypting ransomware (or cryptoware that encrypts files and makes them inaccessible) as the top offender at 77%.

**What type of ransomware infected your organization?**

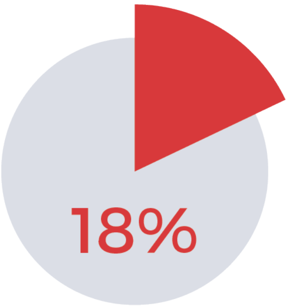
**77%**

**Encrypting ransomware or Cryptoware**

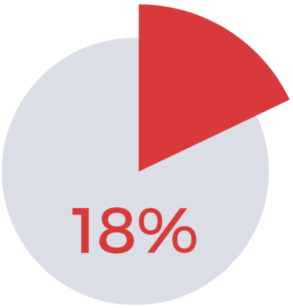
(encrypts files and makes them inaccessible)



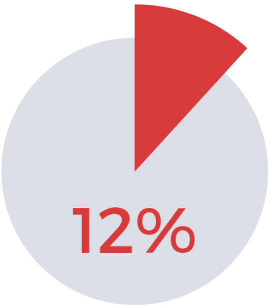
Ransomware that encrypts MBR or NTFS (prevents victims' computers from being booted up in a live OS environment)



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)



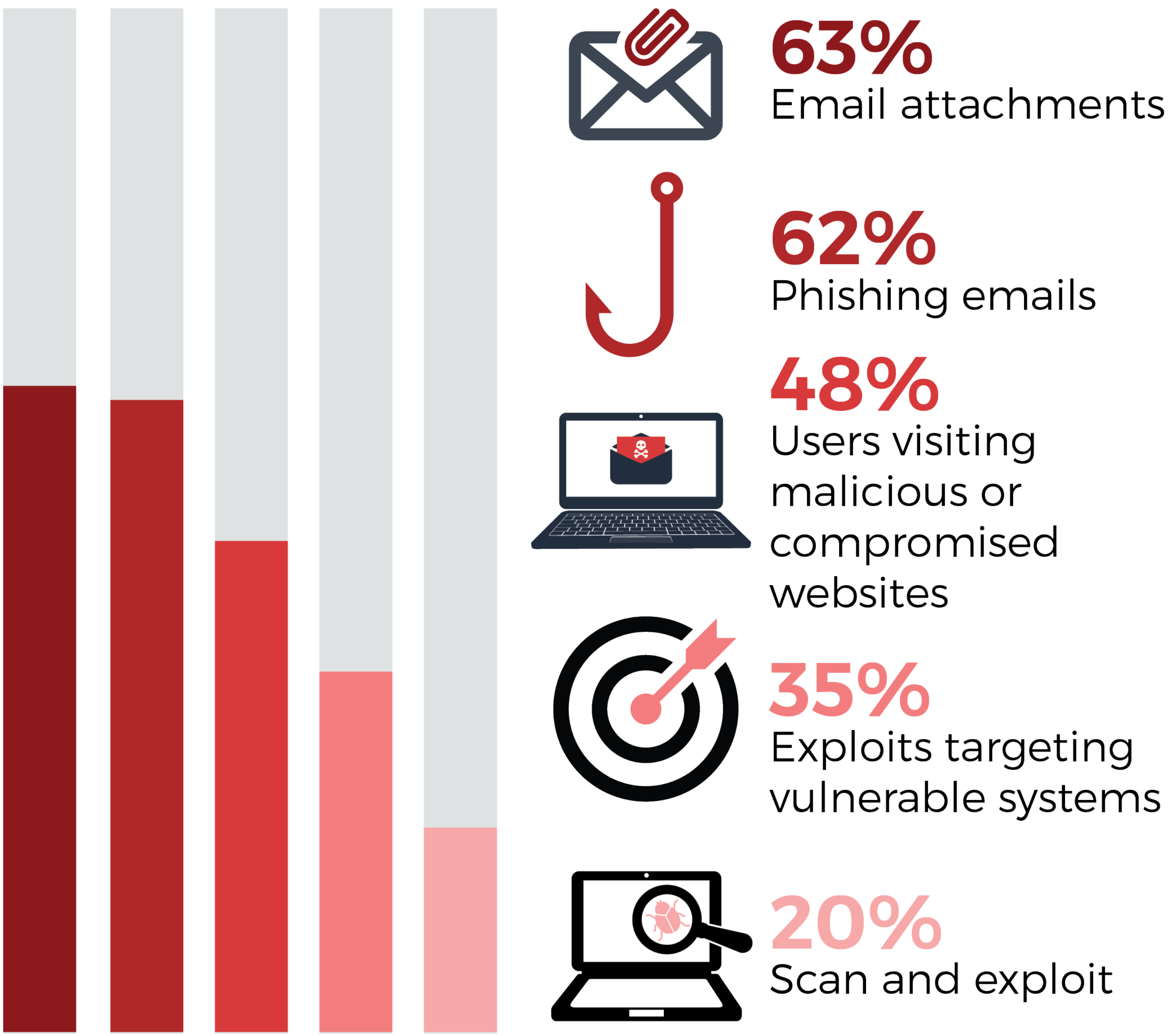
Leakware or extortionware (exfiltrates data that the attackers threaten to release if ransom is not paid)

Not sure/other 13%

# HOW RANSOMWARE ENTERS

Datto's Ransomware Report lists how various types of Ransomware are distributed and the effects of the malware when it locks data or files. Screen locks, file locks and boot record locks typically result in the same predicament for the victim – no access to their data.

**How has ransomware entered your organization?**



Not sure/other 3%

# SECURITY IMPACT ON IT

The Ponemon Institute's annual study analyzes the cost of a data breach on organizations. Their research like the research used in this report suggests that organizations are being impacted financially increasingly year over year. While the direct cost of paying a ransom is clear other costs like productivity loss (58%), increased spending on IT security (52%), system downtime (50%) and forcing cybersecurity professionals to change IT strategy, particularly patching routines (45%).

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

## BUSINESS IMPACT

52%
INCREASED SPENDING ON IT SECURITY

16%
DAMAGE TO COMPANY REPUTATION

58%
PRODUCTIVITY LOSS

17%
REVENUE LOSS

14%
NEGATIVE PRESS/BAD PUBLICITY

## IT OPERATIONS/SECURITY IMPACT

50%
SYSTEM DOWNTIME

26%
DATA LOSS

9%
SENIOR IT STAFF (CIO, CISO) LOST THEIR JOBS

45%
CHANGE OF IT SECURITY STRATEGY

20%
LOSS OF CONFIDENCE IN EXISTING CYBERSECURITY SOLUTIONS

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

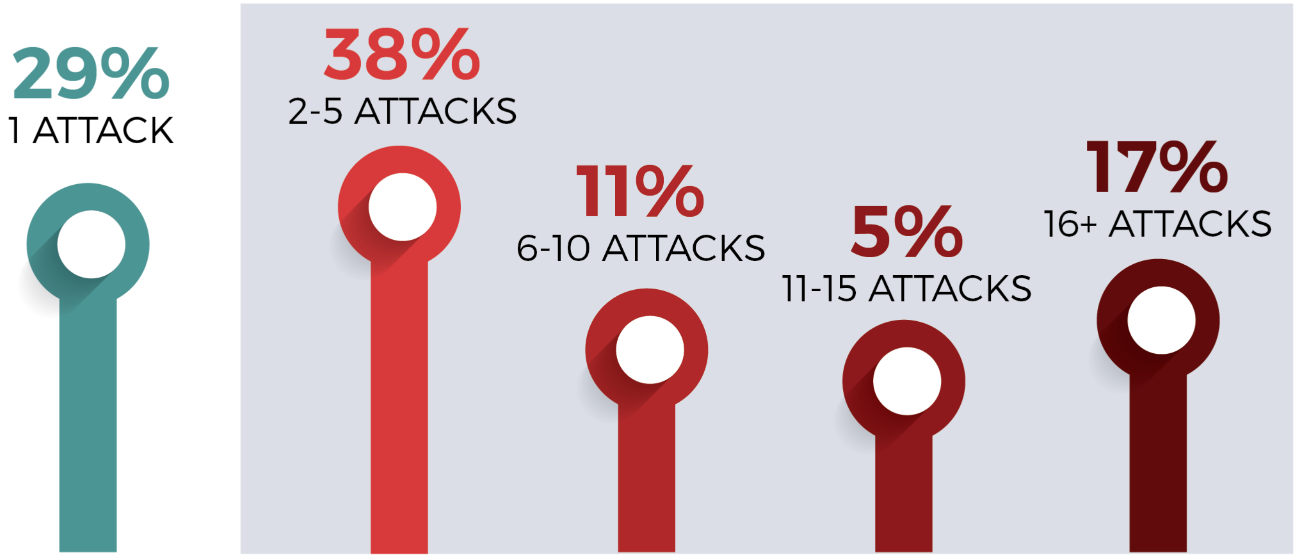
# RANSOMWARE ATTACK FREQUENCY

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%

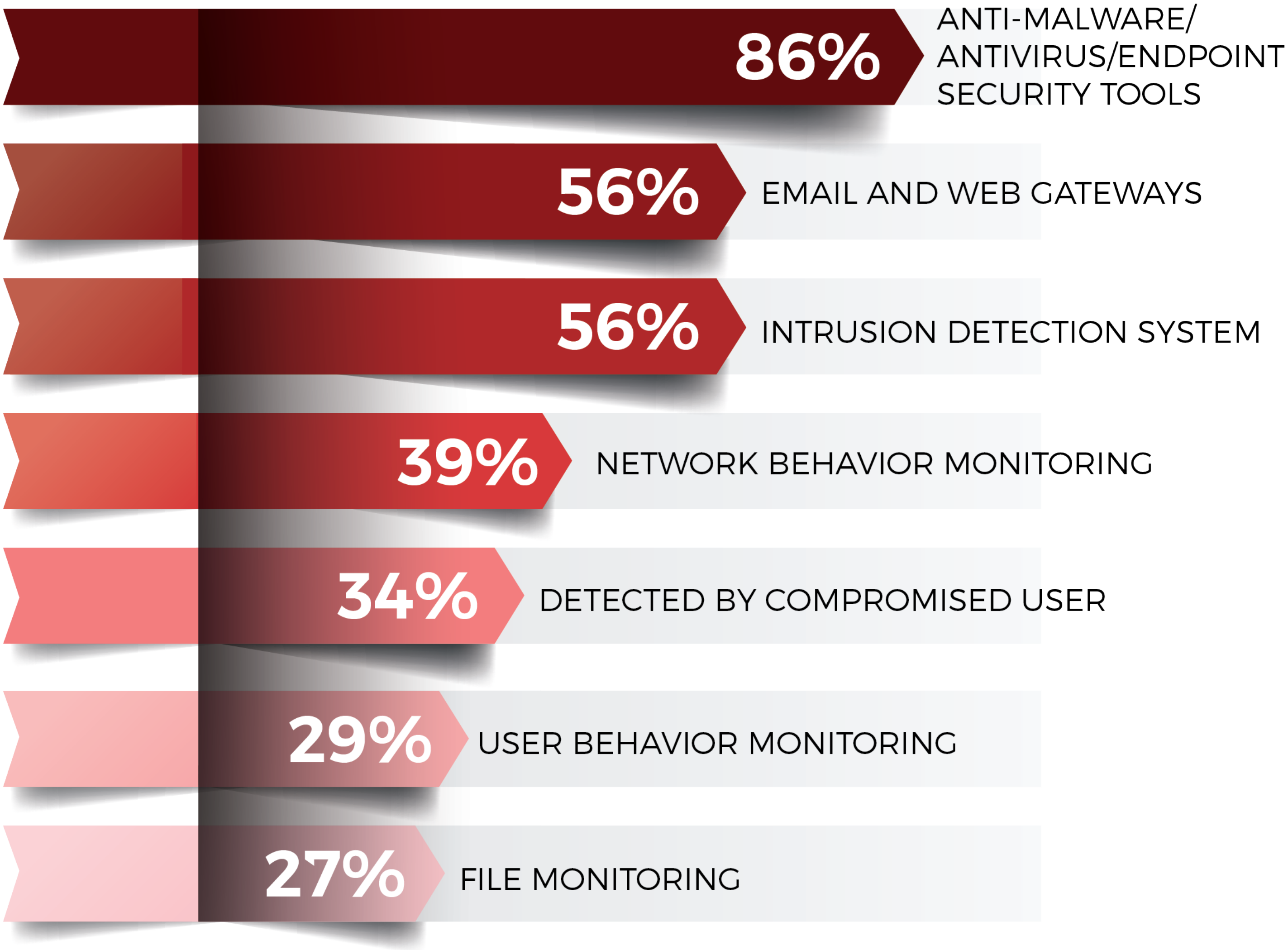
of organizations have experienced
2 or more attacks in the last 12 months.



# DETECTION OF THREATS

Anti-virus, firewalls, Next Gen Firewalls, IDS/IPS, SIEMs are effective at blocking the vast majority of attacks, however as the saying goes, "it only takes one." Whether it's a zero-day or another type of unrecognized piece of code, technology isn't perfect, and neither are people. Phishing attacks have been the method of choice for distributing ransomware.

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



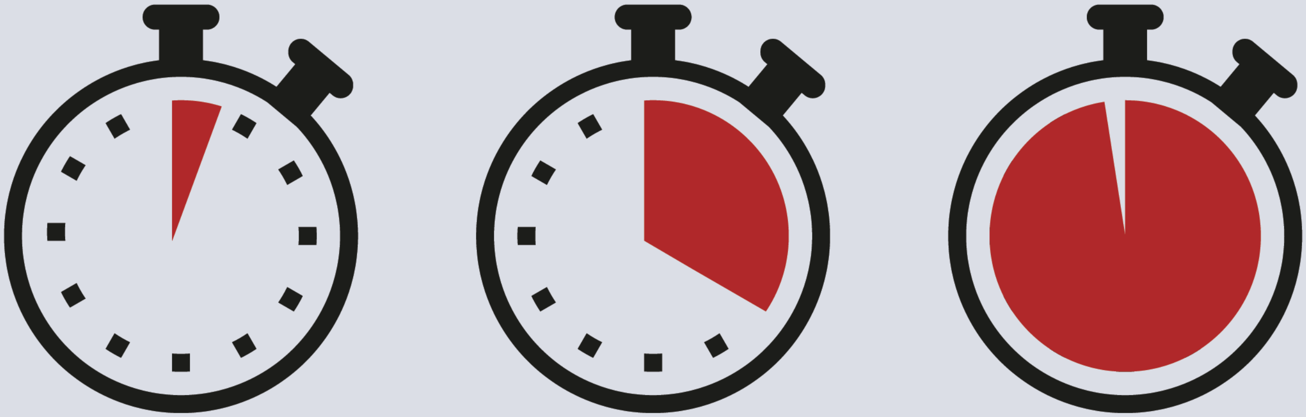
We cannot detect ransomware 4% | Not sure/other 6%

# SPEED OF DETECTION

The Verizon Data Breach report famously documents “dwell time” in its survey which is the time from breach to discovery. In this survey, most attacks or incidents and not breaches, are typically detected within hours (78%). 29% percent of organizations even suggest the malware is found near instantly.

**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



30%
NEAR REAL TIME

29%
WITHIN MINUTES

19%
WITHIN HOURS

11%
WITHIN 1
BUSINESS DAY

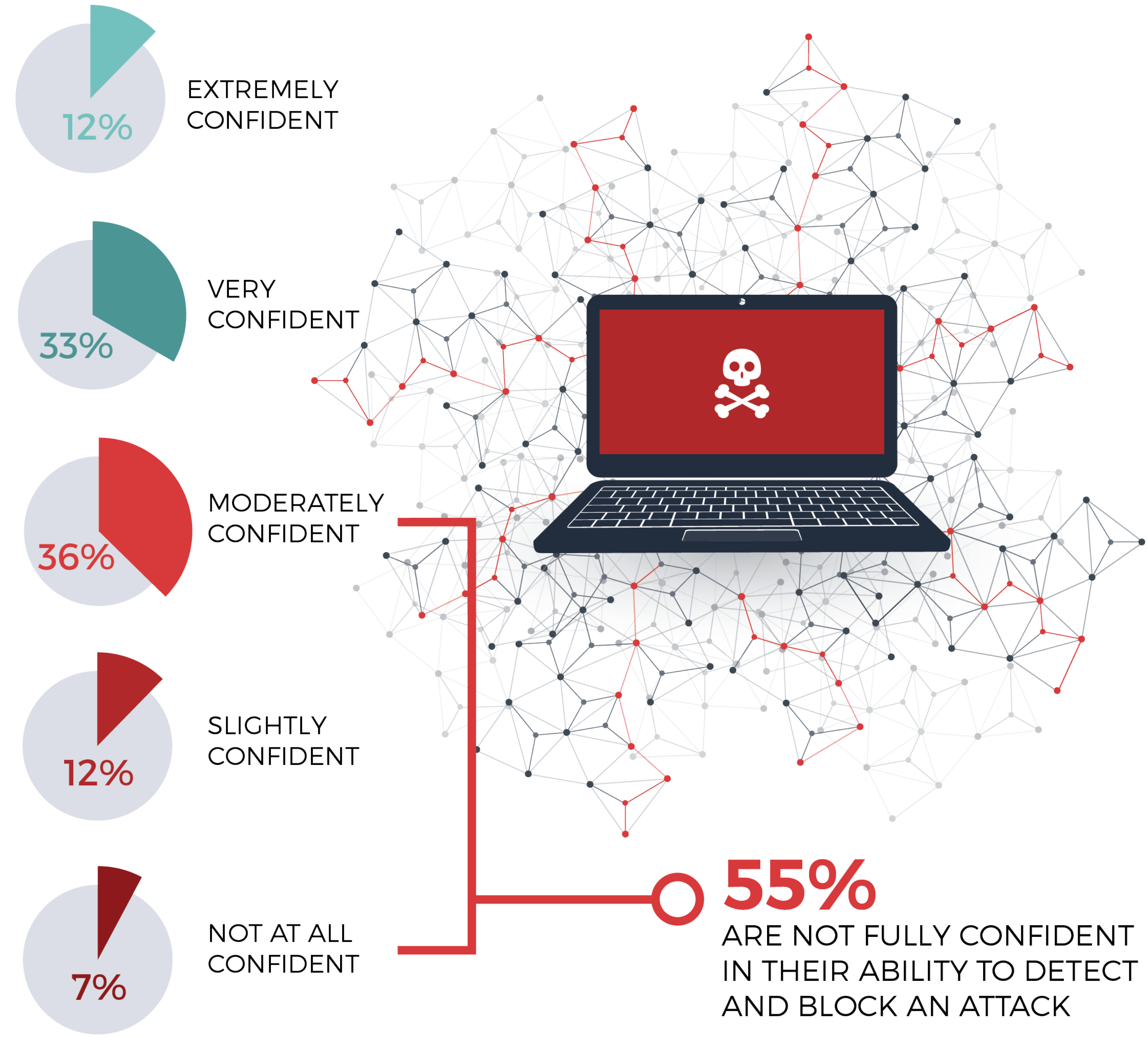
6%
LONGER THAN 1
BUSINESS DAY

5%
MULTIPLE
DAYS

# 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?**

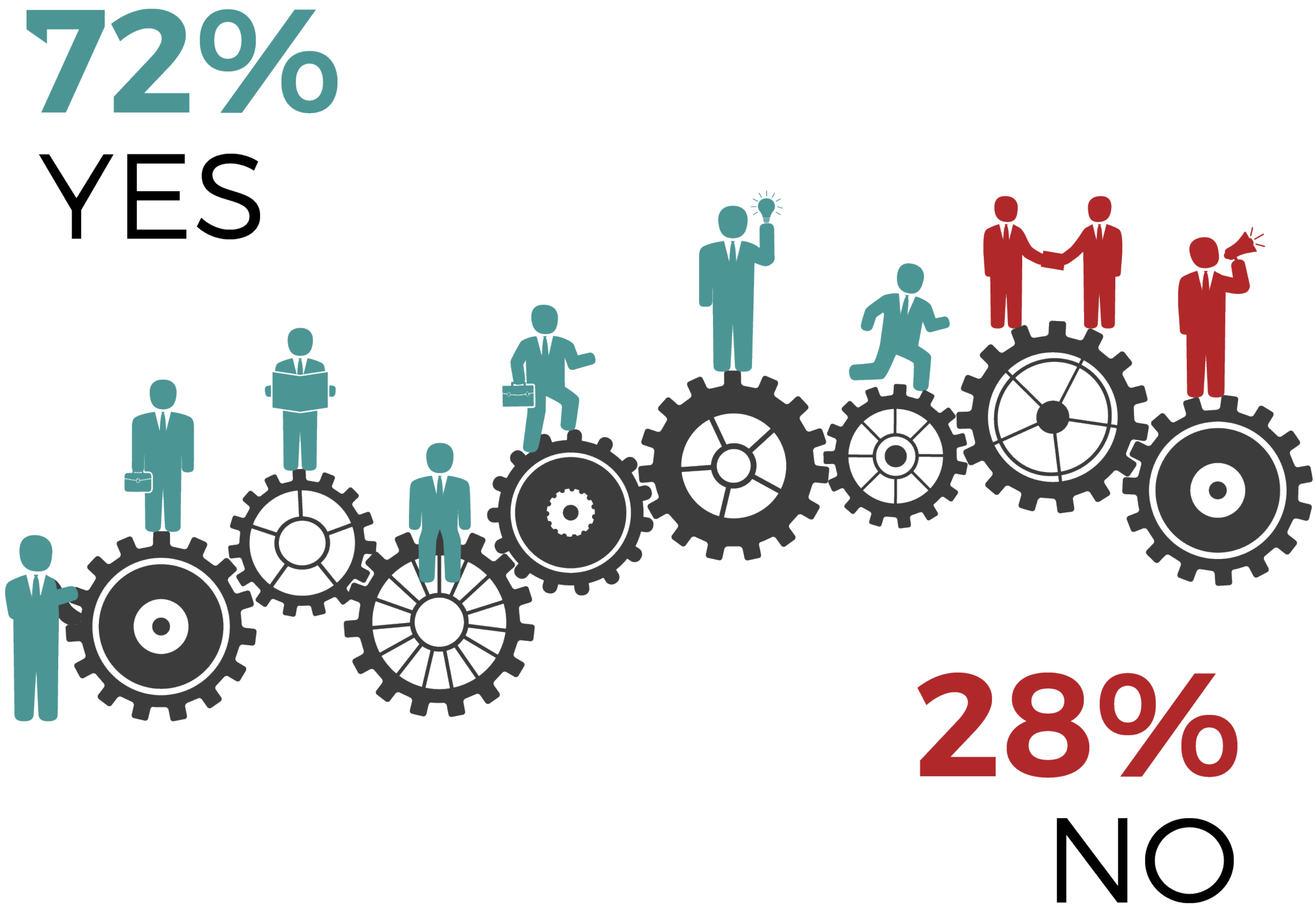


**55%**
ARE NOT FULLY CONFIDENT IN THEIR ABILITY TO DETECT AND BLOCK AN ATTACK

# RESPONSE TEAM READINESS

Organizations have transitioned from contacting outside firms in the event of a breach to creating their own incident response capabilities. Now, only 30% of organizations do not have an IR team to respond to a malware attack.

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



# CONTAINING ACTIVE INFECTIONS

Organizations continue to struggle when malware has entered the network. Encrypted traffic and advance malware code has contributed to this problem, however, Next Gen firewalls and improved response tactics are helping to decrypt traffic and respond to the malware's lateral movement on the network.

**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

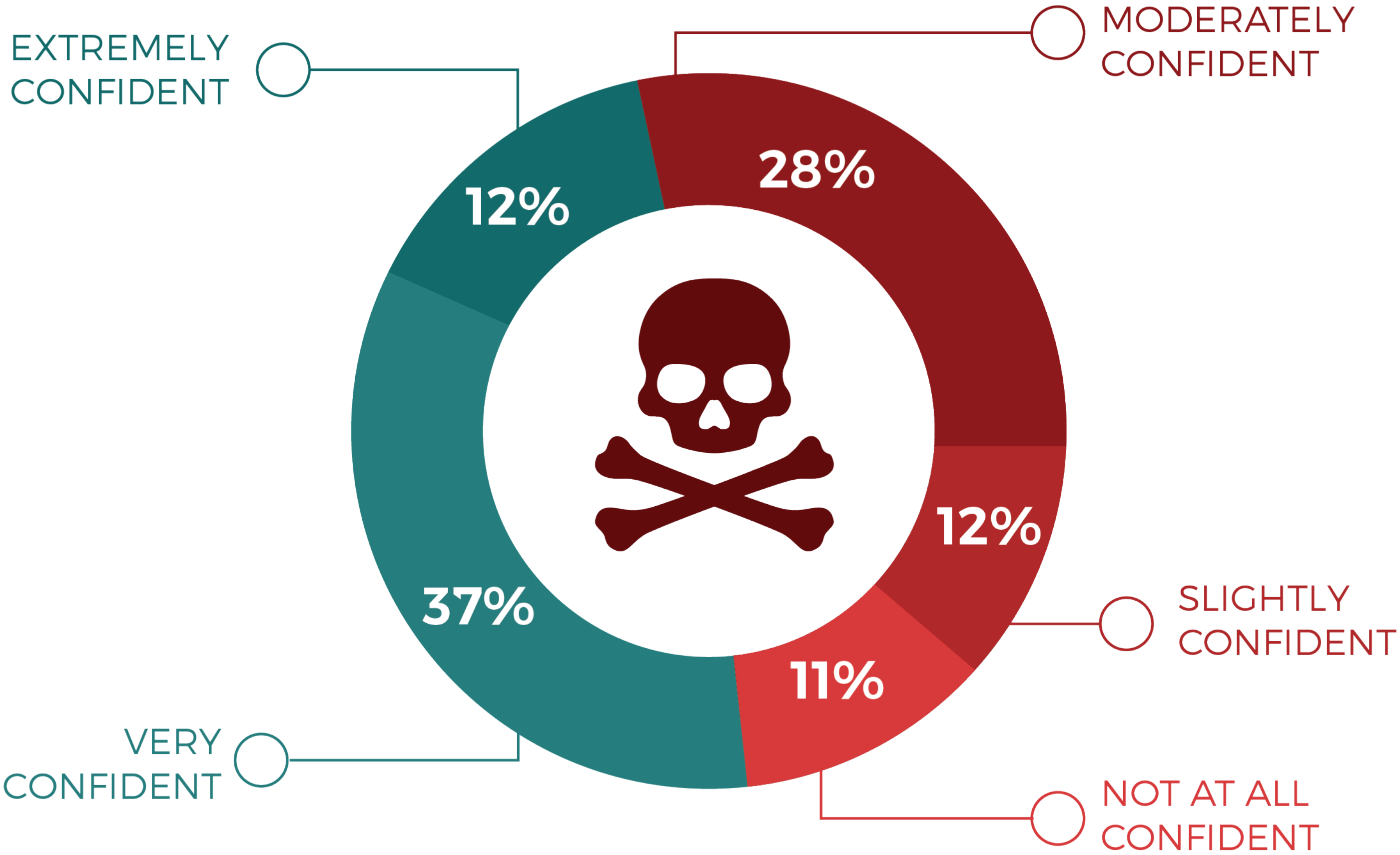
**40%** Advanced, behavior-based malware solution that protect endpoints and has the ability to detect with automated mitigation/remediation capability

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

# CONFIDENCE IN REMEDIATION

After Ransomware locks files a mere 12% of respondents in the survey are extremely confident in their organization's abilities to restore affected files and systems. 37% percent are very confident, however we have to assume that they may be restoring from back-up files and not discovering or creating decryption keys.

**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.

# SPEED OF RECOVERY

48% of the respondents suggested that 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. We do wonder what "recover" means as the type of attack, the response to the attack, and the method of "recovery" are all variables that need to be considered.

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

29%
A few hours

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

19%
A DAY

31%
A FEW DAYS

5%
A WEEK

5%
A FEW WEEKS

11%
POTENTIALLY NEVER RECOVER

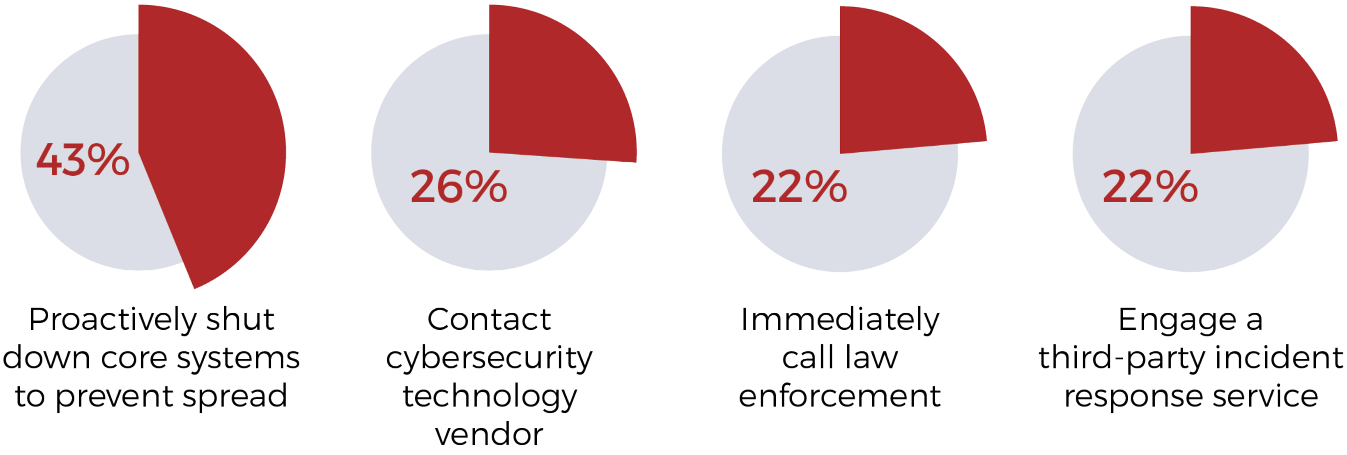
# ATTACK RESPONSE TACTICS

“Pulling the plug” and containing the Ransomware to as limited a number of systems as possible is the most consistent answer in the survey when respondents were asked how they would deal with a “detection” of Ransomware.

**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



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

Consistent with most attacks, the most significant reason for enhancing their organization's ransomware defense is to protect 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

**71%**
Saving the organization from potential downtime

**60%**
Mitigating the financial costs arising from ransomware attacks

**57%**
Protecting the reputation of the brand

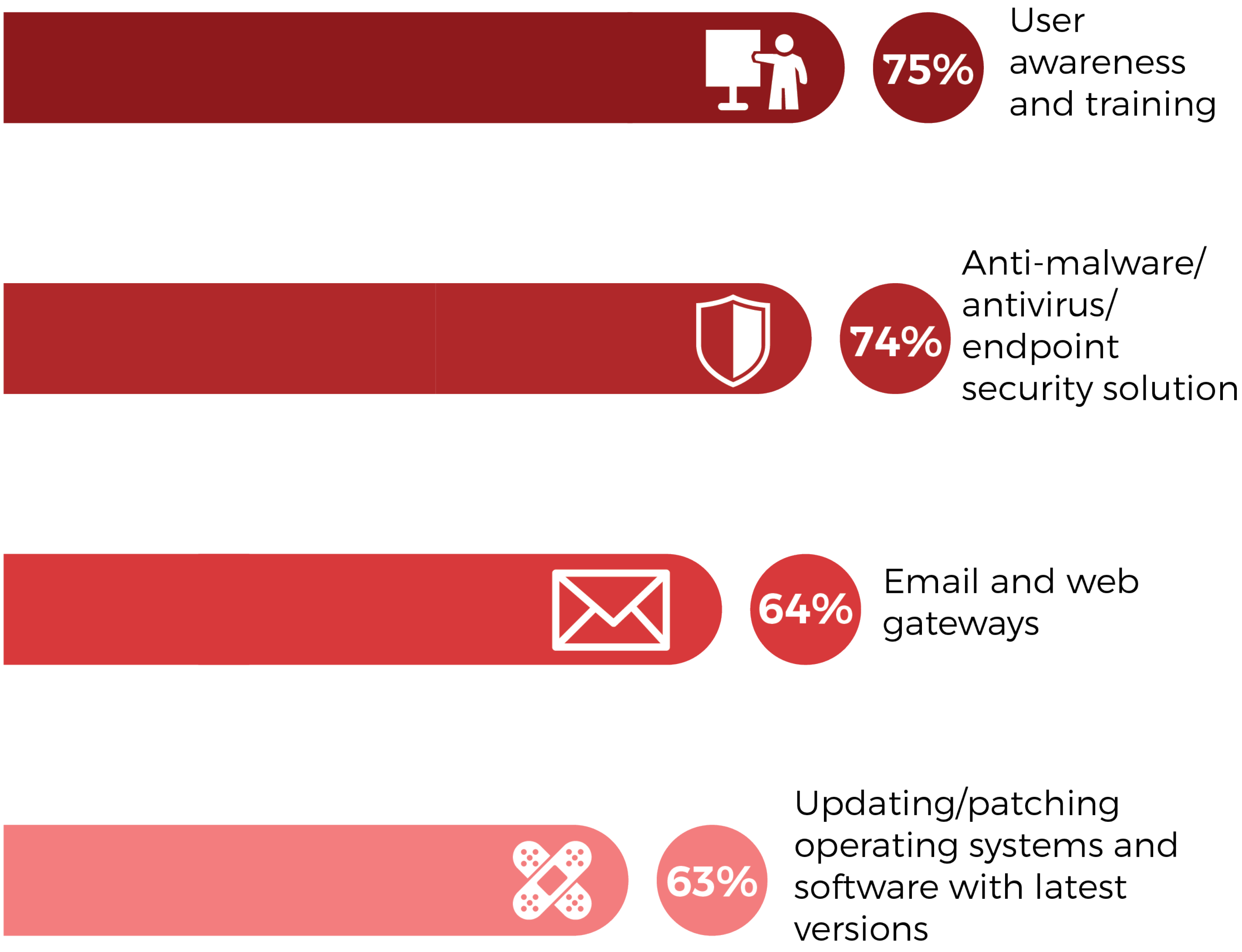
**51%**
Staying a step ahead of emerging threats

Other 1%

# EFFECTIVE PREVENTION

Ransomware is consistently and most successfully delivered through phishing attacks. Users typically untrained in social engineering and other types of training that would educate them concerning clicking on links or opening attachments from senders they don't know often initiate the attack. User awareness according to survey respondents would reduce the success of phishing attacks.

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

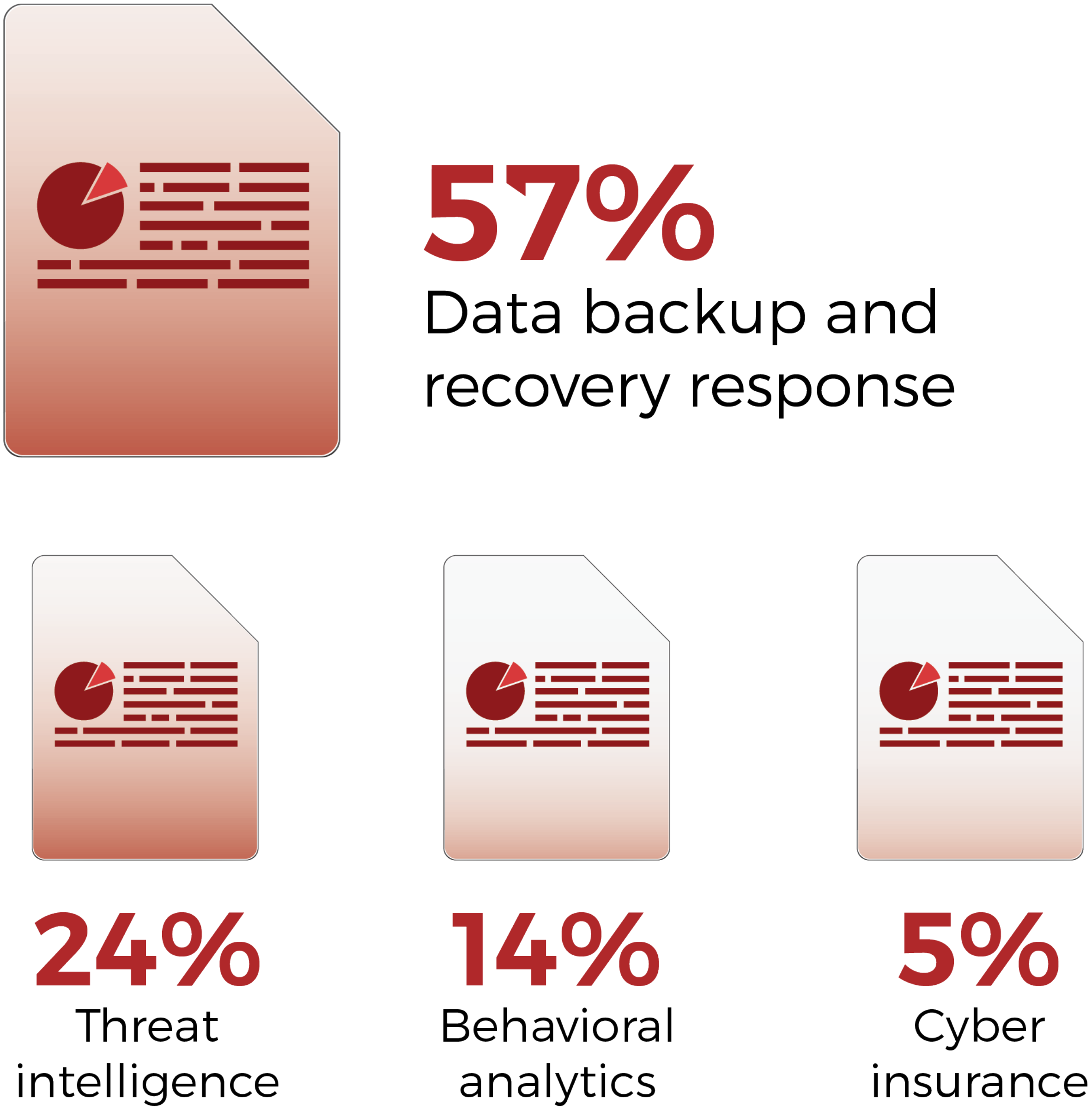


Network IDS/Traffic Monitoring 56% | Spam filters 53% | Internal access controls and authentication 53% | Behavior based/machine learning endpoint protection 51% | Infrastructure security monitoring 51% | Endpoint Detection and Response (EDR) 43% | File monitoring 39% | Application whitelisting 38% |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

24%
Threat intelligence

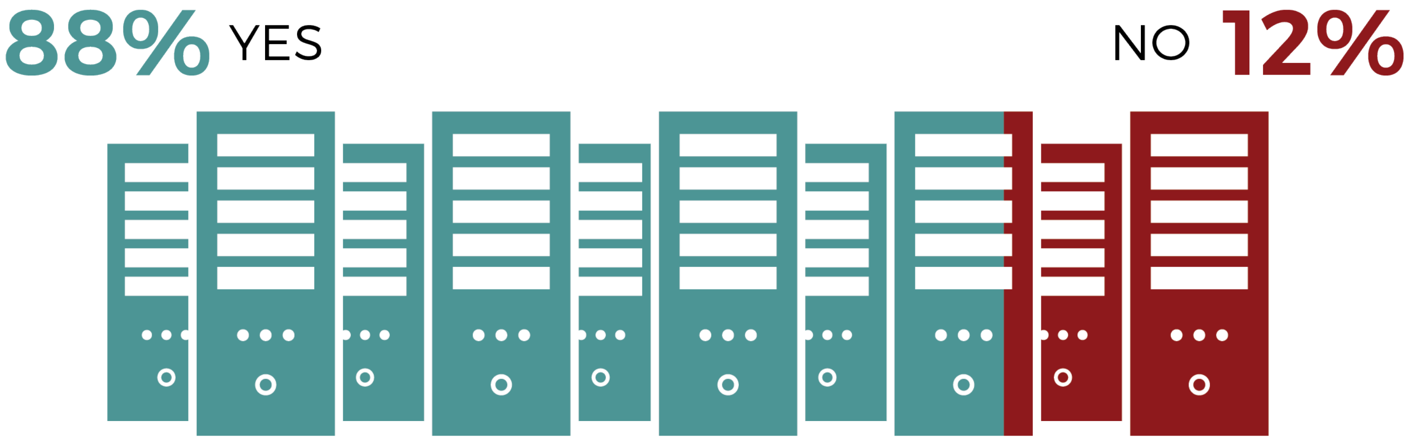
14%
Behavioral analytics

5%
Cyber insurance

# MALWARE SECURITY SOLUTIONS

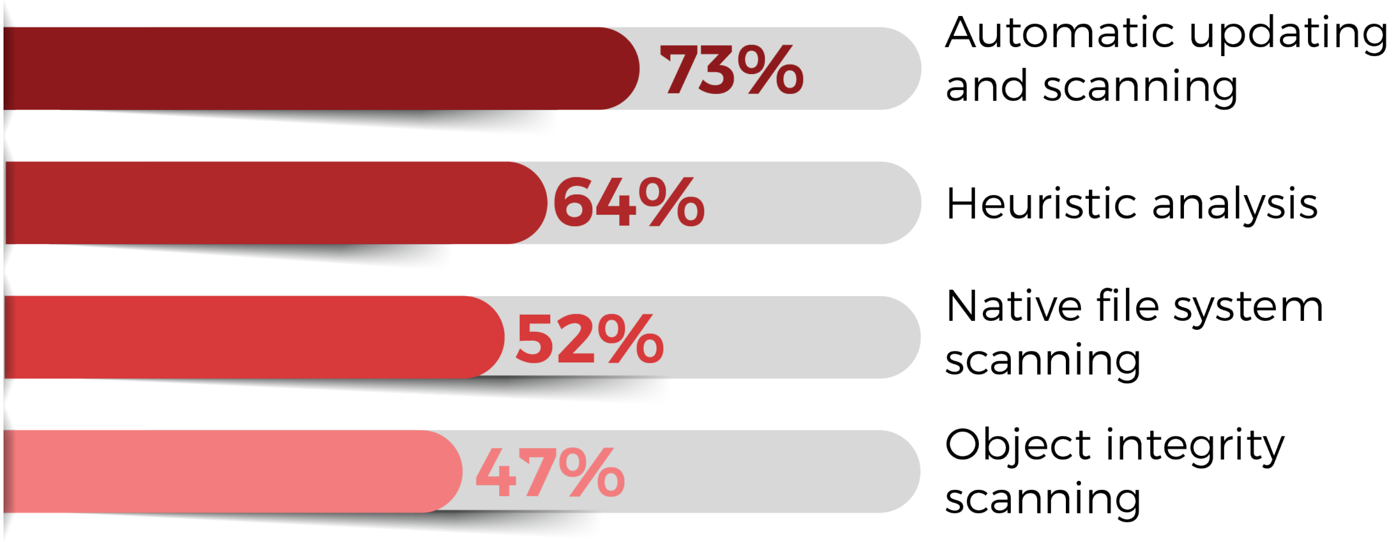
Most organizations (88%) are confident that endpoint security solutions can protect their servers against malware attacks. However, the reality is that endpoint systems struggle identifying and remediating malware prior to damage in many of the post-mortem's conducted by digital forensic teams.

**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?**



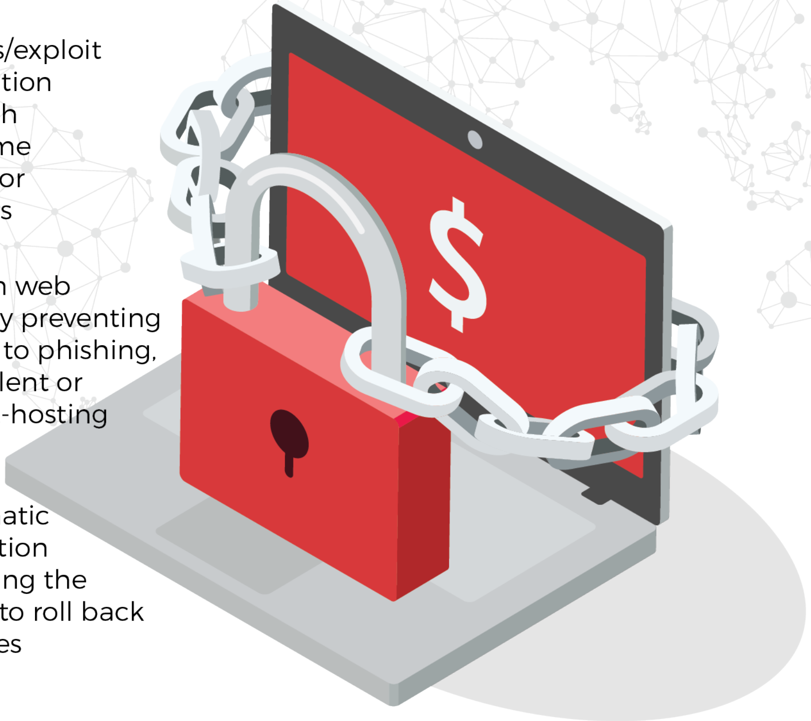
Other 4%

# ENDPOINT SECURITY

When asked about the most effective endpoint security capabilities to protect against malware, survey respondents suggest that detecting and blocking traffic or executables at the first sign of malicious behavior (65%), and blocking attacks pre-execution (63%) are 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) |
| 49% | Advanced file analysis (i.e. nextgen antivirus tools) |
| 43% | Fileless/exploit prevention through real-time behavior analysis |
| 43% | Built-in web security preventing access to phishing, fraudulent or exploit-hosting sites |
| 37% | Automatic mitigation including the ability to roll back changes |



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

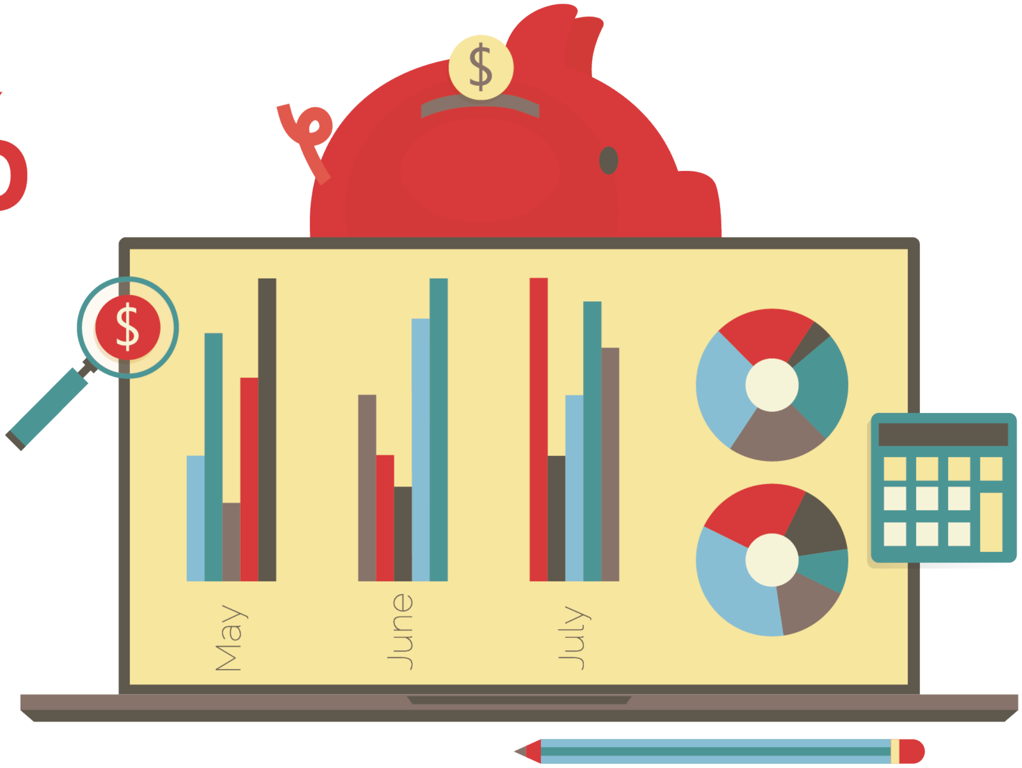
# OBSTACLES TO DEFENSE

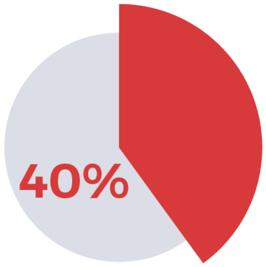
Effective risk management or the balance between protection and cost-effectiveness is an issue in most organizations according to the majority of IT Security leaders. Organization can spend endlessly, however protecting the right data, systems, and spending on the right technology and people are key.  Budget as usual is seen as a key reason companies are seen as vulnerable.

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

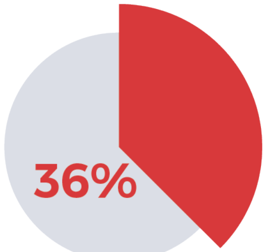
51%

Lack of budget

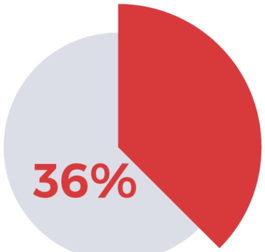




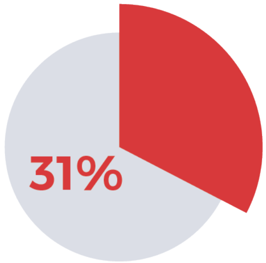
Evolving sophistication of attacks



Poor user awareness



Lack of human resources



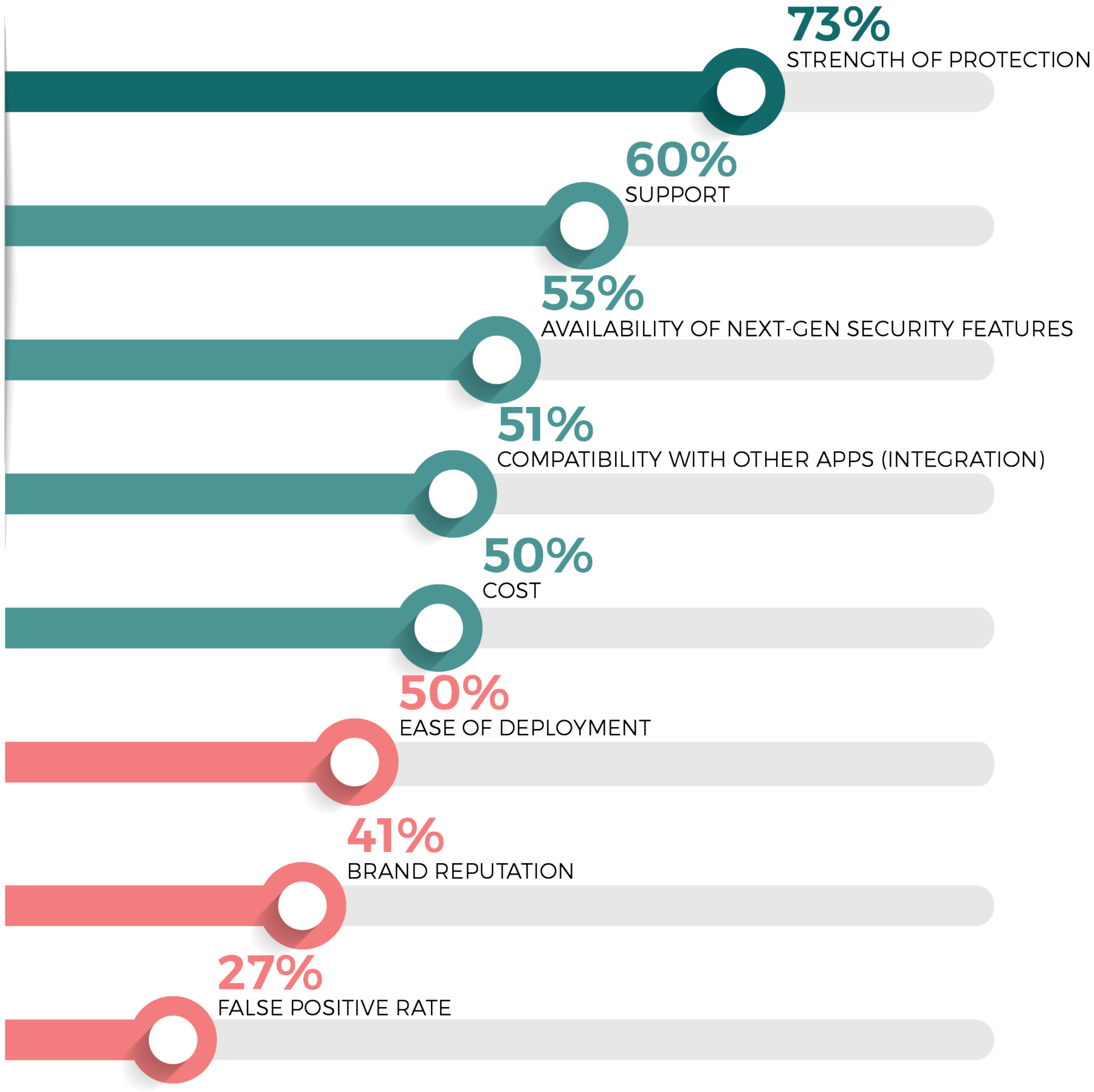
Growing proliferation of attacks

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?**

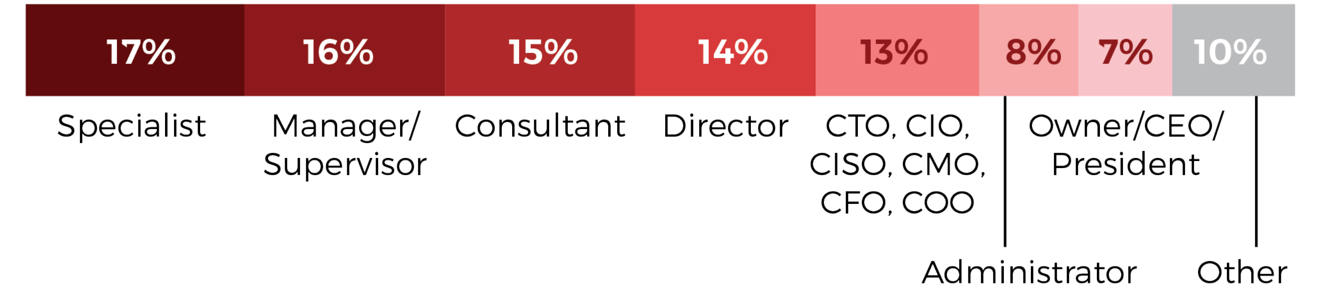


Other 4%

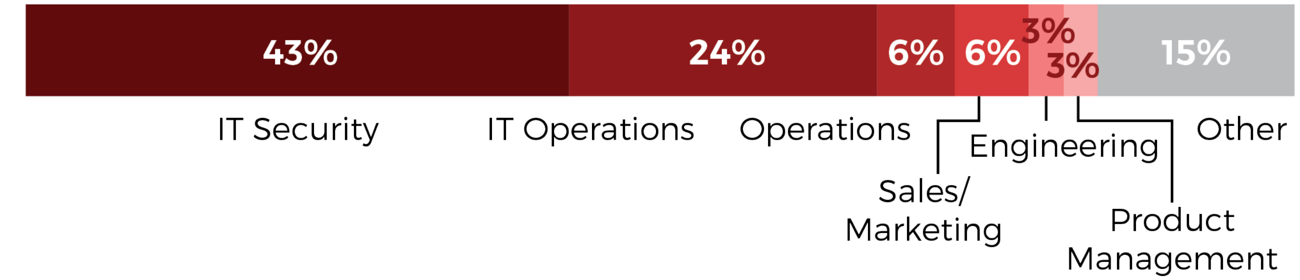
# METHODOLOGY & DEMOGRAPHICS

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.

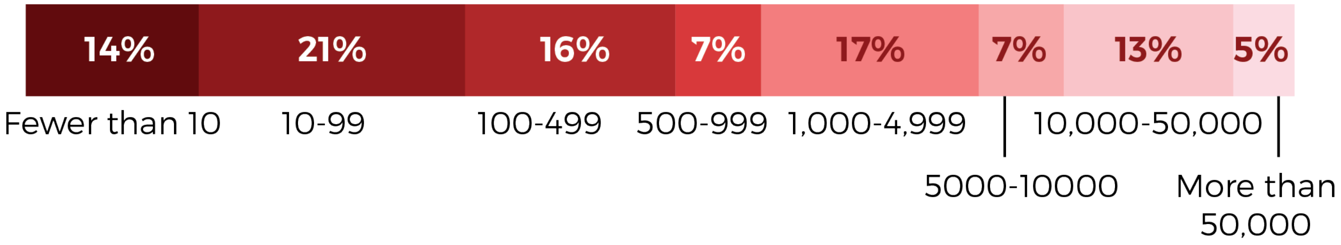
## CAREER LEVEL



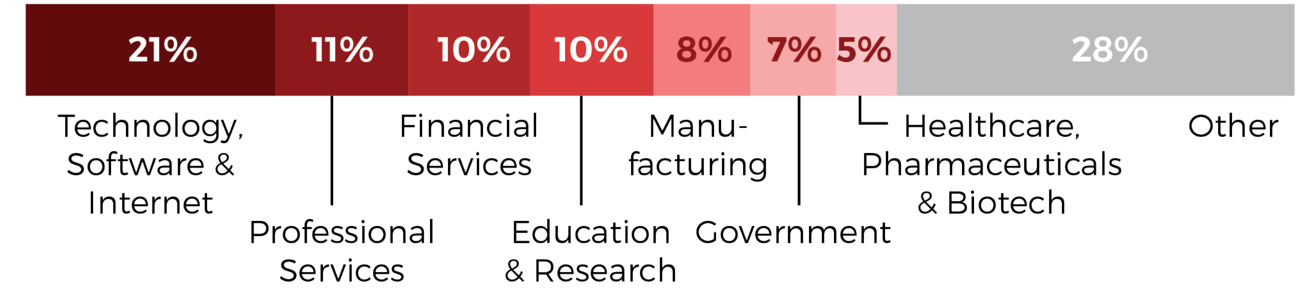
## DEPARTMENT



## COMPANY SIZE



## INDUSTRY



# CONTACT US

**SecureOps Montreal**
1550 Metcalfe Street, Suite 502
Montreal, Quebec, Canada H3A 1X6
Phone: 1-888-982-0678
Phone: 1-514-316-9141
Fax: 1-514-982-0362

**SecureOps Prague**
Meteor Office Park
Sokolovská 100/94,
186 00 Praha 8
Czech Republic
Phone: 1-888-982-0678
Phone: 1-514-316-9141
Fax: 1-514-982-0362

secure OPS