RANSOMWARE

2017 REPORT

LinkedIn Group Partner

Information Security

Cybersecurity Insiders

ALIEN VAULT

RANSOMWARE 2017 REPORT

TABLE OF CONTENTS

INTRODUCTION

Ransomware attacks, in which hackers encrypt an organization's vital data until a ransom is paid, have become a billion dollar cybercrime industry according to the FBI. Ransomware is now widely seen as the single biggest cybersecurity threat to both business and government organizations.

In many respects, ransomware is a game changer: It is incredibly easy and inexpensive for criminals to execute global attacks. At the same time, ransomware is extremely profitable as many businesses will simply pay the ransom to get their mission-critical systems and data up and running again. And even if they don't pay out, the cost of downtime, cleaning up IT systems, and restoring backup data can significantly impact an organization's bottom line.

Cybersecurity Insiders, in partnership with the 370,000+ member Information Security Community on LinkedIn, commissioned Crowd Research Partners to conduct an in-depth study to gather insights, reveal the latest ransomware trends, and provide valuable guidance on effectively addressing the ransomware threat.

The resulting 2017 Ransomware Report is the most comprehensive research to date, revealing how corporate IT and security professionals are dealing with the evolving ransomware threat and how organizations are preparing to better protect their critical data and IT infrastructure.

We would like to thank the study sponsor AlienVault® for supporting this research.

In addition, we want to thank all survey participants who provided their time and input in completing the study.
We hope you will enjoy reading this report and gain insight from its findings and best practice recommendations.

Thank you,

Holger Schulze

Holger Schulze
CEO and Founder
Cybersecurity Insiders

Holger.Schulze@Cybersecurity-Insiders.com

Cybersecurity Insiders

KEY SURVEY FINDINGS

1. Ransomware is the fastest growing security threat, perceived as a moderate or extreme threat by 80% of cybersecurity professionals. 75% of organizations affected by ransomware experienced up to five attacks in the last 12 months alone, 25% experienced 6 or more attacks. 79% predict ransomware to become a larger threat over the next 12 months. Only a small fraction of respondents say they would pay the ransom or negotiate with the attackers. 59% of organizations are either not confident at all or only slightly to moderately confident in their ransomware defense.

2. Email and web use represent the most common ransomware infection vectors with employees opening malicious email attachments (73%), responding to a phishing email (54%) or visiting a compromised website (28%). The information most at risk from ransomware attacks is financial data (62%) followed by customer information (61%). From a solution perspective, the majority of identified ransomware attacks were detected through endpoint security tools (83%), email and web gateways (64%), and intrusion detection systems (46%).

3. Security professionals rank user awareness training the most effective tactic to prevent and block ransomware (77%) followed by endpoint security solutions (73%), and patching of operating systems (72%) as preventive approaches to ransomware threats. Data backup and recovery (74%) is by far as the most effective solution to respond to a successful ransomware attack. 96% of respondents confirm they have a data backup and recovery strategy in place.

4. A majority of 54% say they could recover from a successful ransomware attack within a day, while 39% estimate it will take more than one day to a few weeks to recover. Speed of recovery is absolutely mission-critical as business cost escalates with every hour the business cannot fully operate, causing system downtime (41%) and productivity loss (39%).

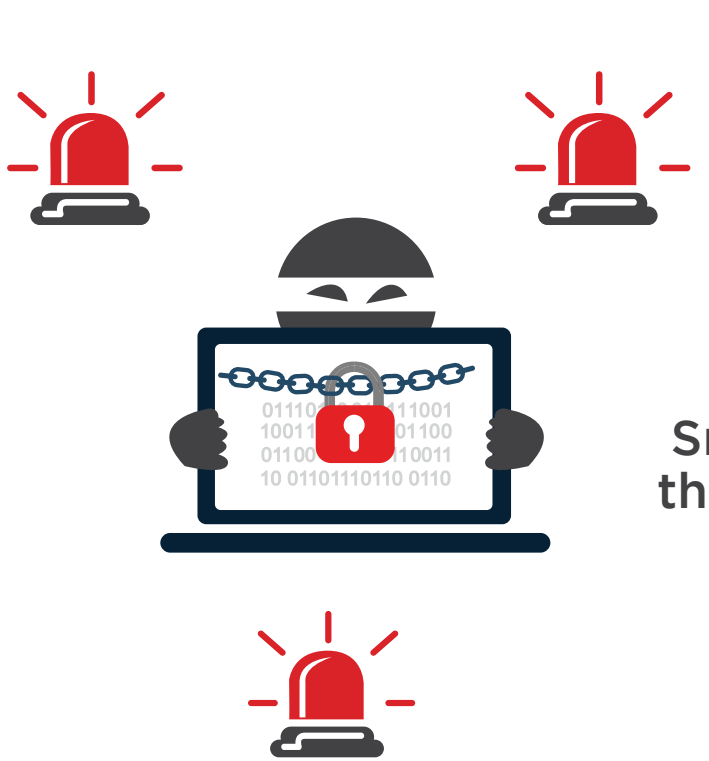
5. Today's main obstacles to stronger ransomware defense are all about resources and staying current on the latest ransomware exploits: lack of budget (52%), dealing with evolving sophistication of attacks (42%), and lack of human resources (33%). The silver lining: 60% of organizations expect their budget for ransomware security to increase.

RANSOMWARE THREAT

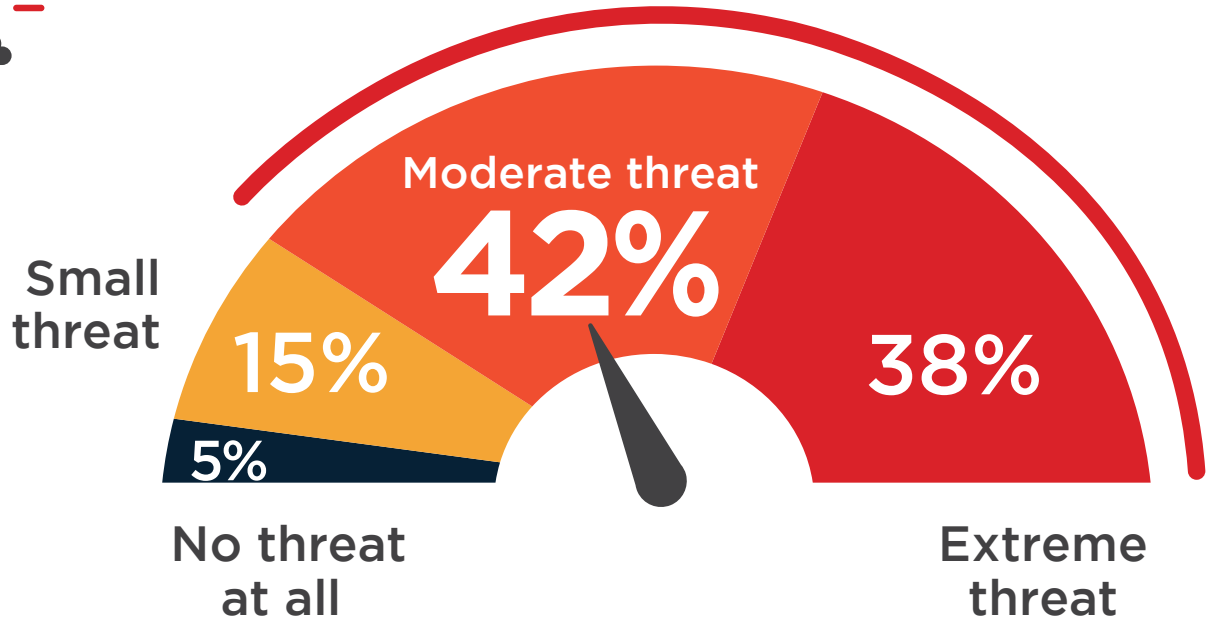
RANSOMWARE THREAT

Ransomware is one of the fastest growing security threats affecting organizations of all sizes, from SMBs to large enterprises and government agencies. IT and cybersecurity professionals are quickly recognizing ransomware attacks as a significant threat. Eighty percent of respondents perceive ransomware either as an extreme threat (38%) or moderate threat (42%). Very few respondents (5%) see ransomware as no threat at all.

How significant of a business threat is ransomware to your business?



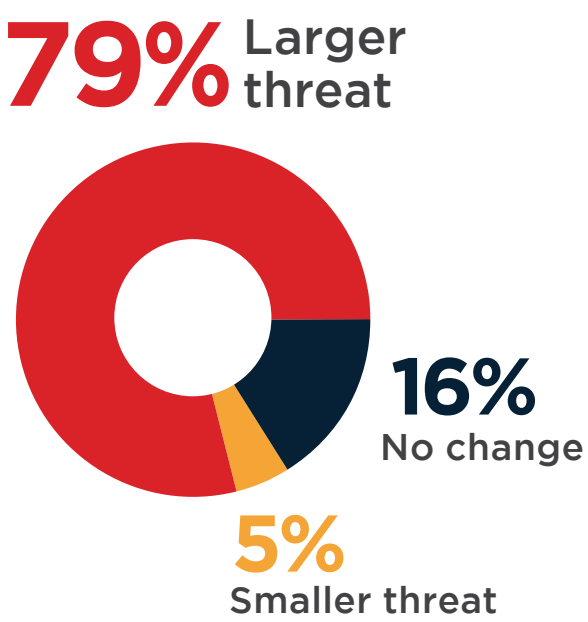
80% of respondents see ransomware as an extreme or moderate threat.



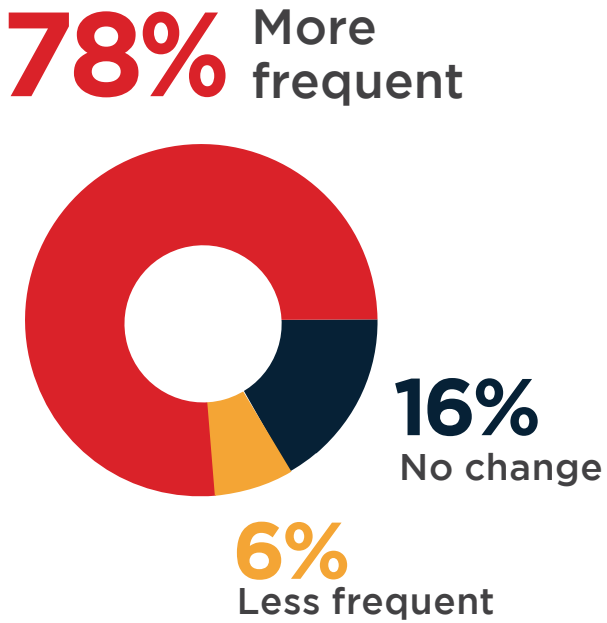
FUTURE ATTACKS

The number of ransomware-related news headlines continues to grow, increasing awareness for ransomware attacks. A significant majority (79%) of IT security professionals predict ransomware to become a larger threat. 78% expect an increase in attack frequency over the next 12 months."

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



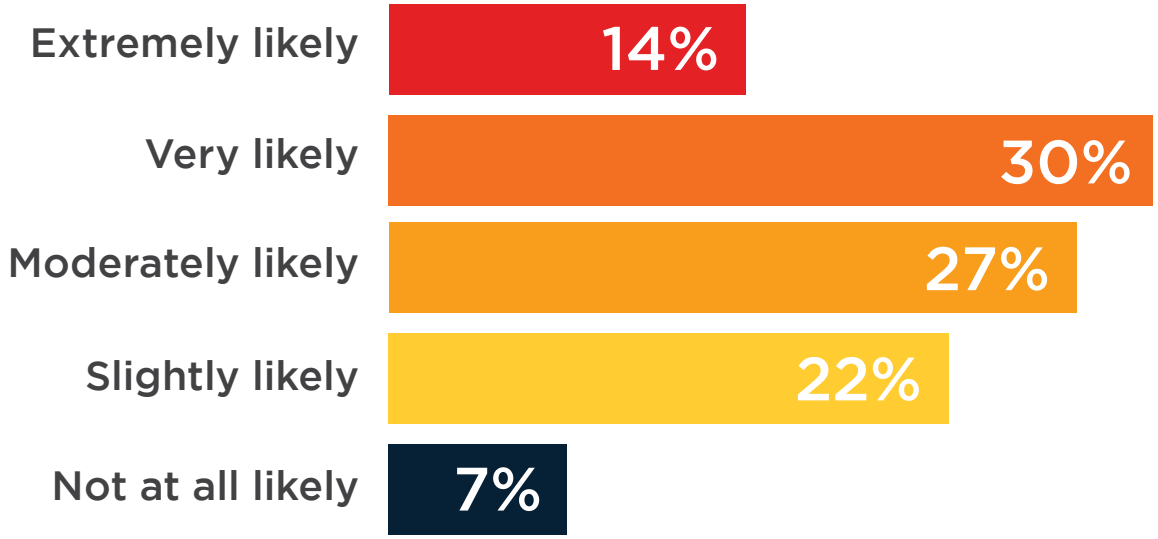
Are ransomware attacks becoming more or less frequent overall?



RANSOMWARE OUTLOOK

Looking ahead, we surveyed organizations regarding their outlook as a future target of ransomware. Nearly half of the respondents (44%) assess their probability as a target as very or extremely likely. Twenty-seven percent say an attack is moderately likely.

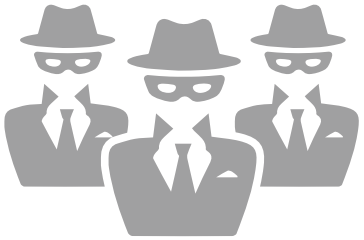
What is the likelihood that your organization will be a target of ransomware in the next 12 months?



CYBERCRIMINALS BEHIND RANSOMWARE

The survey reveals cybersecurity professionals perceive organized cybercriminals (69%), non-organized opportunistic hackers (58%) and state sponsored hackers (28%) as the top three culprits behind ransomware attacks.

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



69%

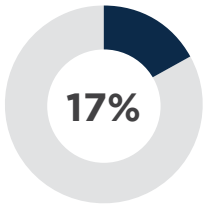
Organized cybercriminals

58%

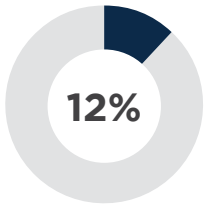
Opportunistic hackers (non-organized)

28%

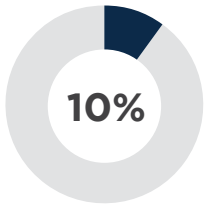
State-sponsored hackers



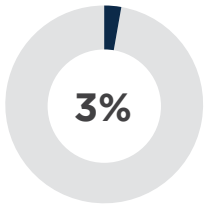
Political hacktivists



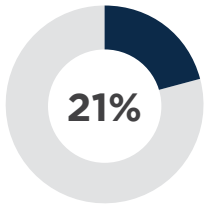
Competitors



Disgruntled/former employees



Dissatisfied customers



Don't know/others

WORST RANSOMWARE STRAINS

Ransomware has quickly emerged as a lucrative venture for cybercriminals. New ransomware delivery platforms and authoring tools are spurring an increase in ransomware variants and their sophistication. Most notable ransomware strains recognized by security professionals are WannaCry, (83%), CryptoLocker (77%) and Petya (67%). 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?

83%

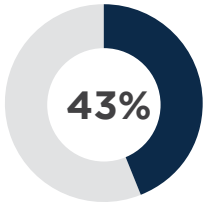
WannaCry

77%

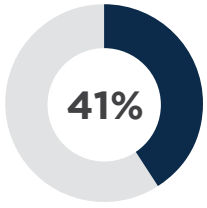
CryptoLocker

67%

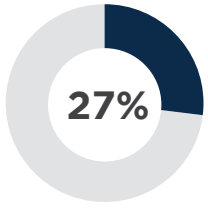
Petya



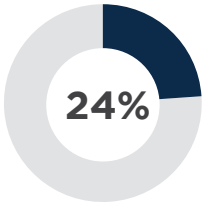
CryptoWall



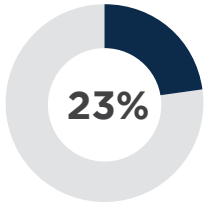
Locky



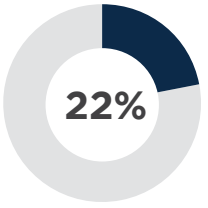
TeslaCrypt



TorrentLocker



Cerber



ZCryptor

Jigsaw 19% | CTB Locker 19% | Crysis 13% | KeRanger 7% | LeChiffre 5% | Other 5%

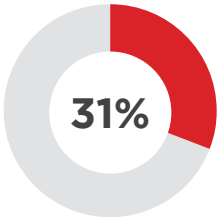
WHAT MOTIVATES ATTACKERS

Financial gain (86%) tops the list of motivators for ransomware attacks, followed by a desire to sabotage and disrupt business activities (58%). But while money extortion is the most common motivation for cybercriminals, in some cases attackers are motivated by personal revenge (8%), political beliefs (17%), hacking for fun (25%) and state-sponsored attacks (29%).

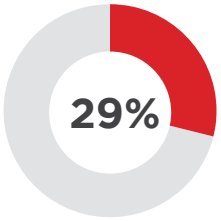
What do you believe is the main motivation for ransomware attacks against your organization?

86%
Financial gain

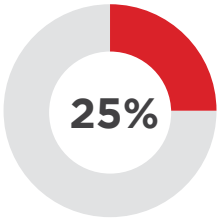
58%
Sabotage/disruption of business



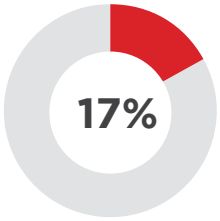
Cyber espionage



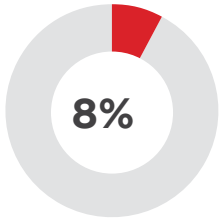
State-sponsored international attack



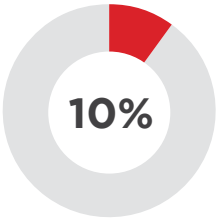
Entertainment (hacking just for fun)



Political motivation



Revenge for a bad experience with organization



Don't know/ other

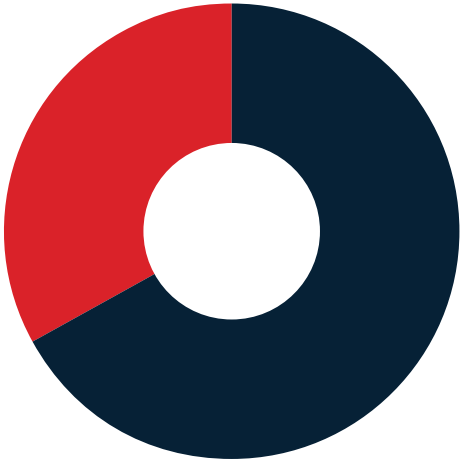
RANSOMWARE ATTACKS AND IMPACT

RANSOMWARE EXPERIENCE

A third of organizations surveyed (33%) said they experienced ransomware attacks. Sixty-seven 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?

33%
YES
My organization has been affected by ransomware.



67%
NO

RANSOMWARE TYPES

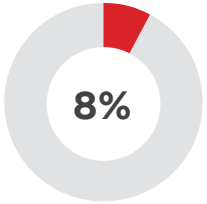
There is a wide array of ransomware types and new variants are created every day within each category. The organizations affected by ransomware overwhelmingly confirm that they encountered encrypting ransomware (or cryptoware that encrypts files and makes them inaccessible) as the top offender at 88%.

What type of ransomware infected your organization?

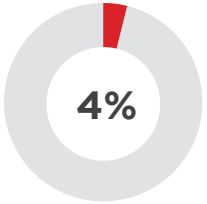
88%

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

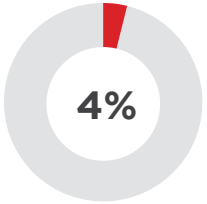
Non-encrypting ransomware or lock screens (restricts access to files and data, but does not encrypt them)



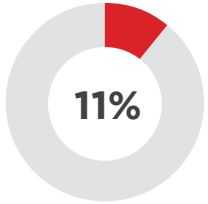
Ransomware that encrypts MBR or NTFS (prevents victims' computers from being booted up in a live OS environment)



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



Mobile Device Ransomware (infects cell-phones through "drive-by downloads" or fake apps)



Don't know/ other

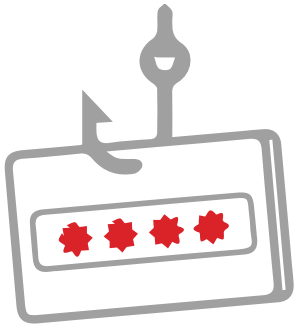
HOW RANSOMWARE ENTERS

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 (73%), answers a phishing email (54%) or visits a compromised website (28%).

How has ransomware entered your organization?

73%

Email attachments

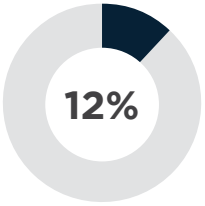


54%

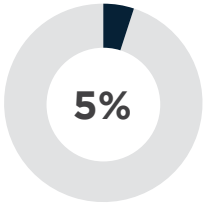
Phishing emails

28%

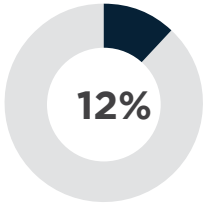
Users visiting malicious or compromised websites



Exploits targeting vulnerable systems



Scan and exploit

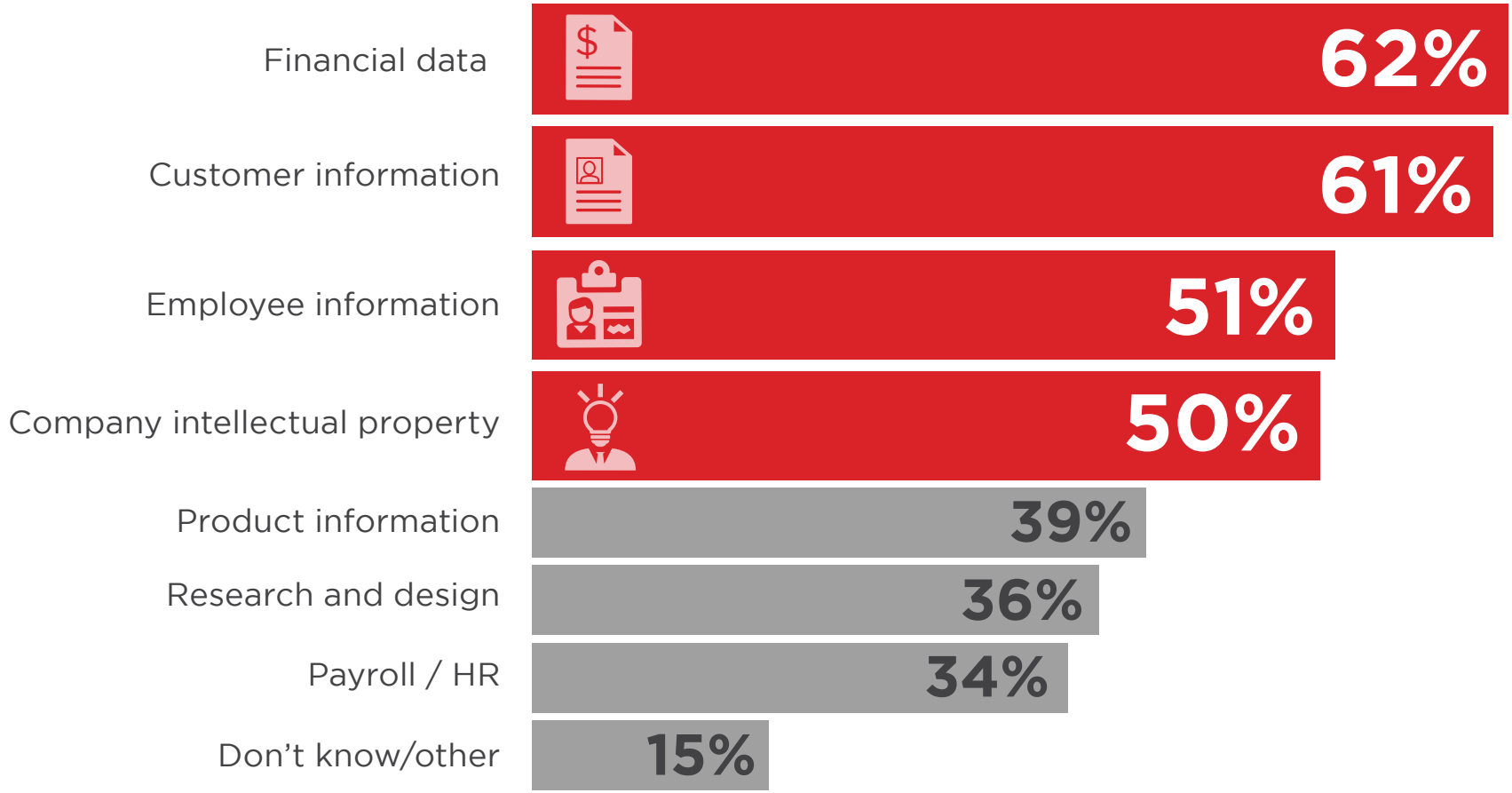


Don't know/ other

DATA AT RISK

Data has become a strategic asset to every organization and equally a high value target for cybercriminals. Our research reveals that the information most at risk from ransomware attacks is financial data (62%), followed by customer information (61%). More than half of the respondents said both employee information (51%) and company IP (50%) were also at significant risk.

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



BUSINESS & IT SECURITY IMPACT

Ransomware is changing the threat landscape and how organizations are impacted at the business level as well as from an IT security policy and control perspective. On the business side, ransomware attacks mostly caused system downtime (41%) and productivity loss (39%), i.e. the exact effect intended by cybercriminals to cause maximum pain and extort money. At the IT governance level, ransomware attacks caused cybersecurity professionals to update IT security strategy to focus on mitigation (49%) and increase spending on IT security (41%).

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

BUSINESS IMPACT

41% System downtime

39% Productivity loss

30% Data loss

IT SECURITY IMPACT

49% Change of IT security strategy, to focus on mitigation

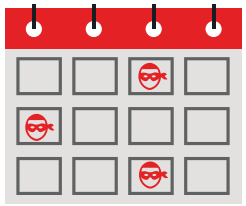
41% Increased spending on IT security

16% Loss of confidence in existing cybersecurity solutions

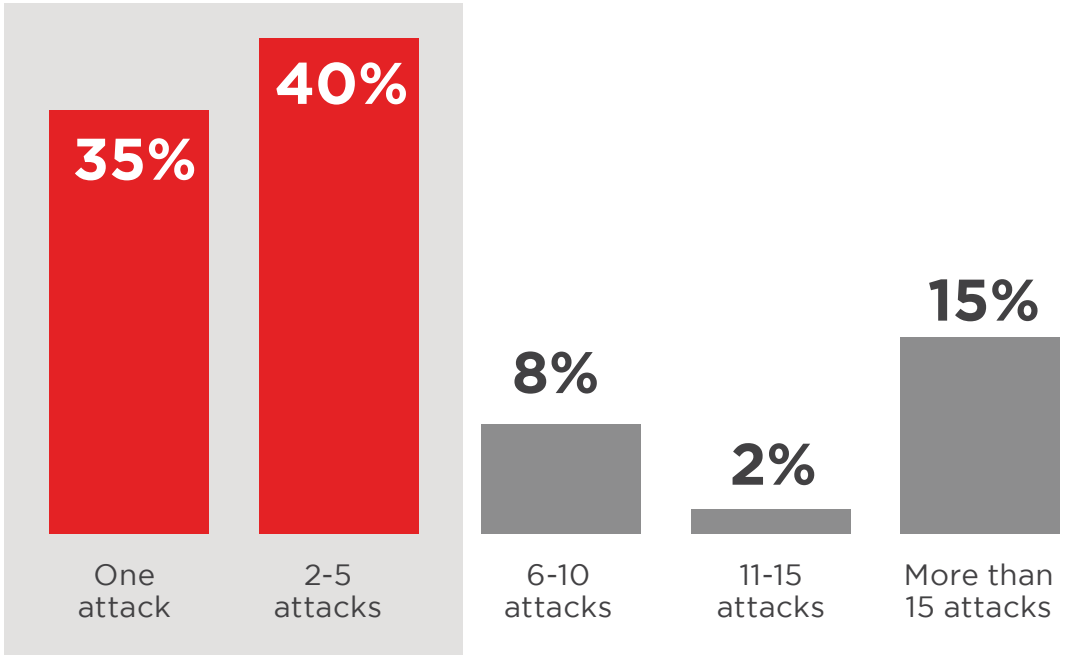
RANSOMWARE ATTACK FREQUENCY

In the past 12 months, the variety and frequency of ransomware incidents directed at organizations have increased dramatically. Of those who experienced ransomware attacks, 75% experienced up to five attacks, while the remaining quarter of organizations experienced 6 or more attacks.

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



75%
of organizations experienced
five or fewer attacks in a year

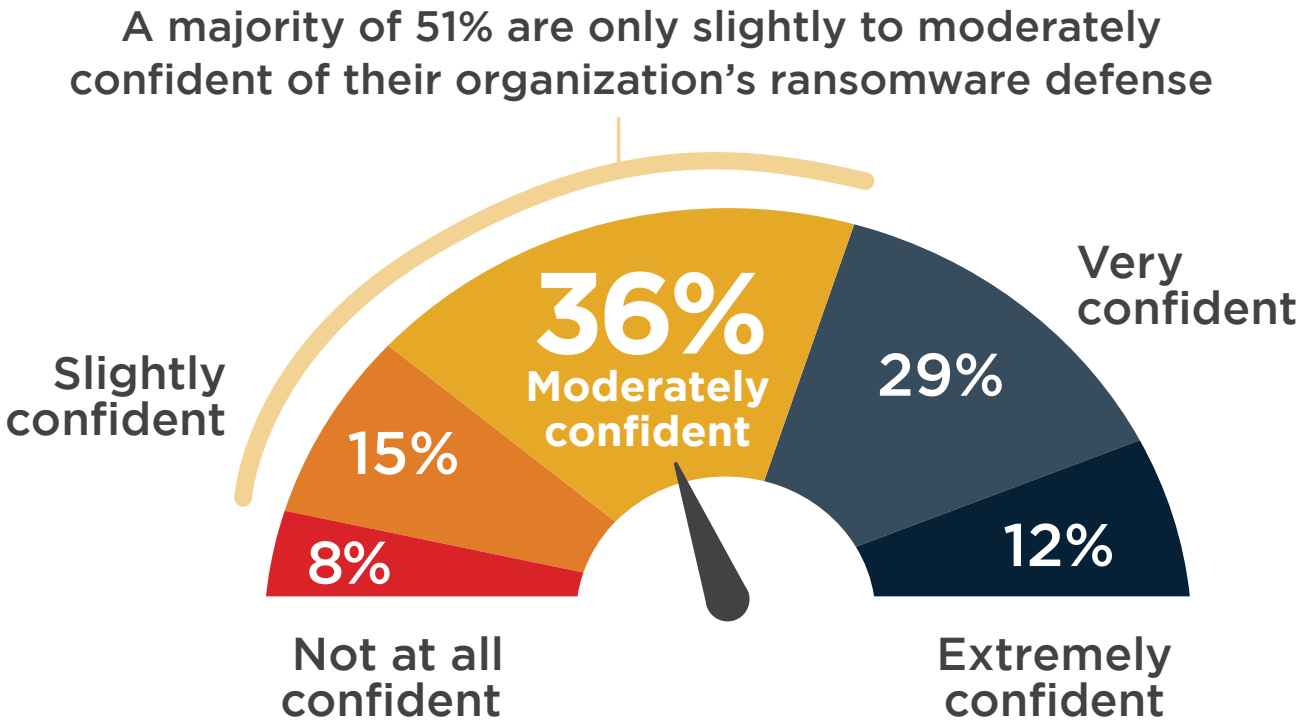


RANSOMWARE READINESS

CONFIDENCE IN DEFENSE

We asked cybersecurity professionals to assess their organization's capacity to detect and block ransomware attacks before they spread to critical IT systems across the organization. Only 12% are extremely confident in their organization's abilities – perhaps overly so given the success rate of innovative ransomware variants. Twenty-eight percent are very confident. Compared to their highly confident peers, a majority of 51% are only slightly to moderately confident of their organization's ransomware defense. An alarming 8% is not confident at all.

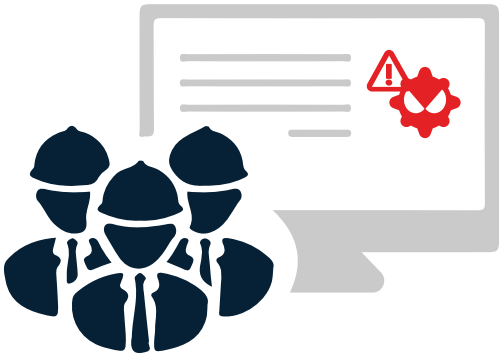
How confident are you that your organization's defenses are capable of detecting and blocking ransomware before it spreads and infects critical systems and files?



RANSOMWARE RESPONSE READINESS

Four out of ten organizations do not have an Incident Response team in place to respond to a ransomware attack. The good news is organizations realize that prevention and awareness are critical pieces of effective, multi-layer defense against ransomware, and the majority (72%) have already implemented employee awareness and security training programs.

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



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

DETECTION AND BLOCKING OF THREATS

There are numerous security tools available to help cybersecurity professionals identify and monitor cyber threats. The vast majority of identified ransomware attacks were detected through anti-malware/antivirus/endpoint security tools (83%), email and web gateways (64%), and intrusion detection systems (46%). Unfortunately, many ransomware attacks succeed in evading detection.

How is ransomware typically detected (and blocked) when it attempts to enter your organization?

83%

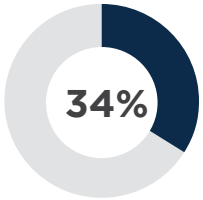
Anti-malware/Antivirus/ Endpoint security tools

64%

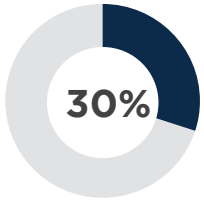
Email and web gateways

46%

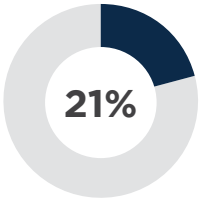
Intrusion detection system



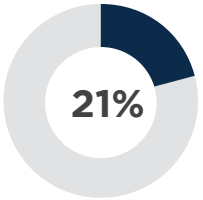
Network behavior monitoring



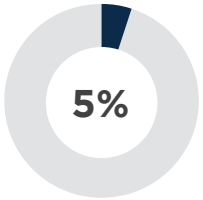
Detected by compromised user



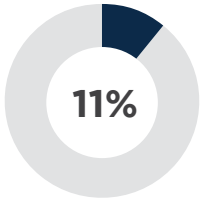
File monitoring



User behavior monitoring



We cannot detect ransomware



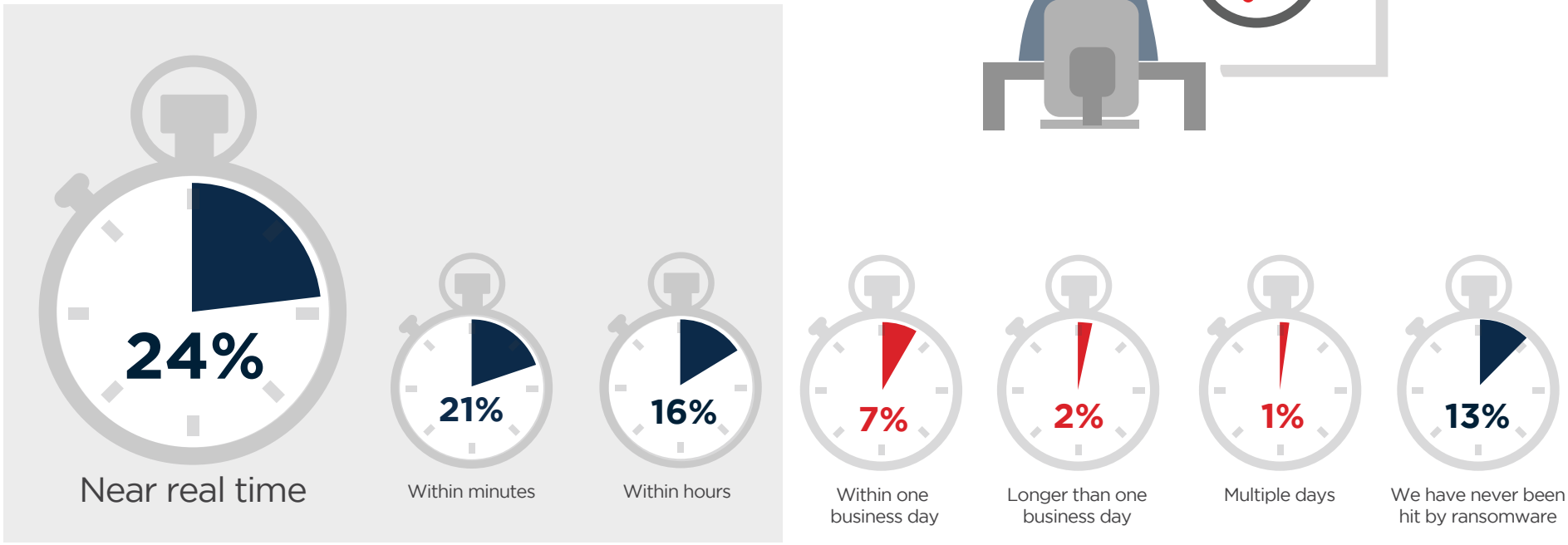
Don't know/ other

SPEED OF DETECTION

While the time it takes organizations to detect ransomware varies, for ransomware attacks identified in their early stages, most attacks are typically detected within hours (61%). Nearly one quarter of organizations claimed detection is near real time (24%), while 21% say they detect ransomware within minutes of an attack. The rate and speed of ransomware detection is critical in combating fast moving attacks before they succeed in spreading across networks and encrypting vital data.

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

61% most attacks are typically detected within hours



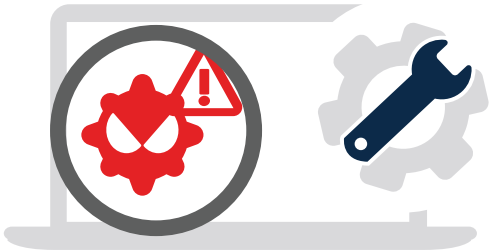
16% Don't know

RANSOMWARE ATTACK RESPONSE & COST

CONFIDENCE IN REMEDIATION

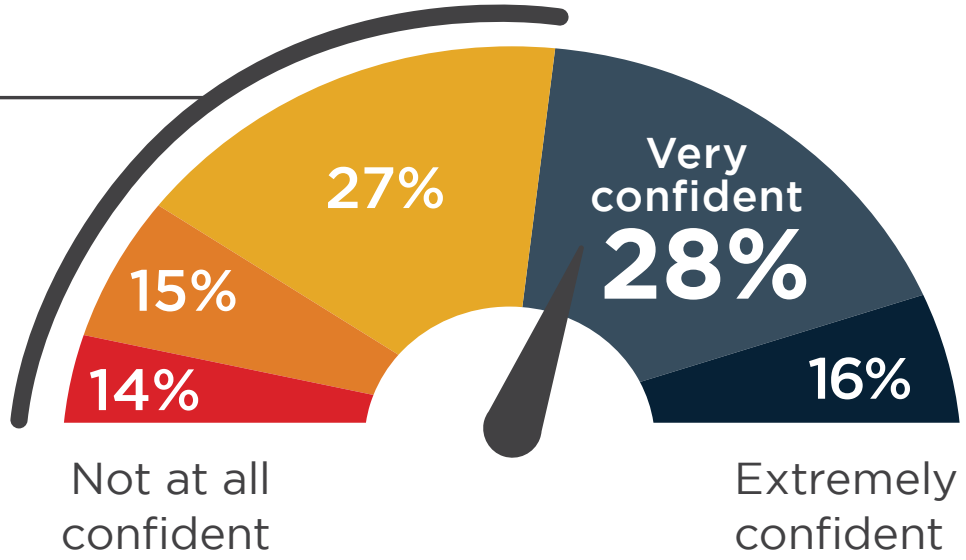
We asked cybersecurity professionals to assess their organization's capacity to remediate a ransomware attack in progress that has already encrypted files and spread to critical IT systems across the organization. Only 16% are extremely confident in their organization's abilities to unlock or restore affected files and systems. Twenty-eight percent are very confident. Confidence appears to correlate with the presence and maturity of incident response teams in the organization. Compared to their highly confident peers, 42% are only slightly to moderately confident of their organization's ransomware cleanup ability. An alarming 14% 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?



56%

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



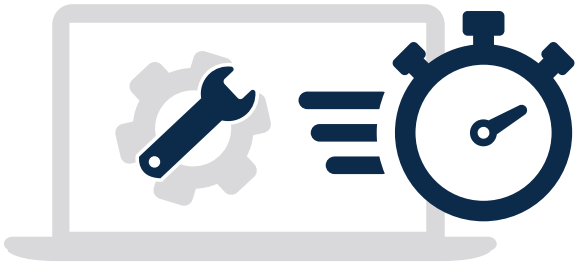
SPEED OF RECOVERY

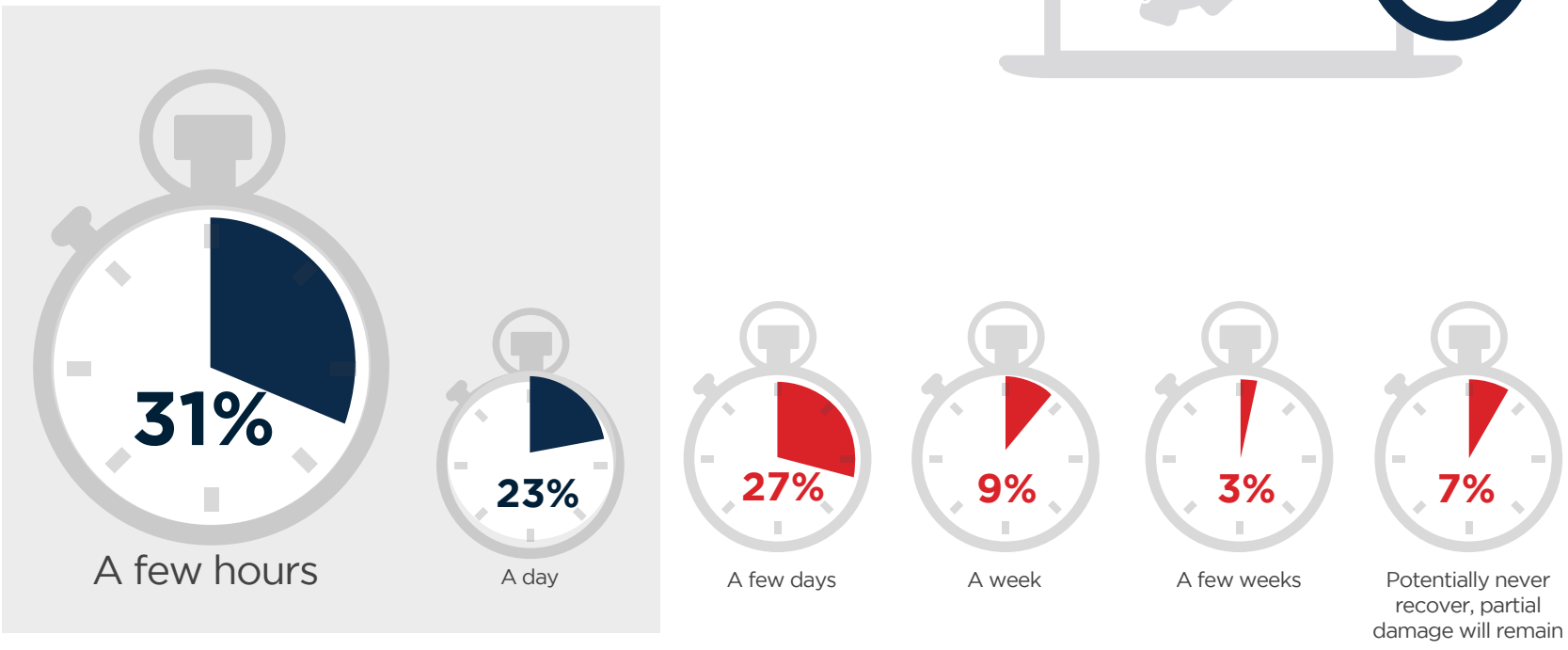
A majority of 54% say they could recover from a ransomware attack within a day, while 39% estimate it will take more than one day to a few weeks to recover. Only 7% of the organizations believe they will never fully recover. Speed of recovery is absolutely mission-critical as business cost escalates with every hour the business cannot fully operate.

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

54%

could recover from a ransomware attack within a day



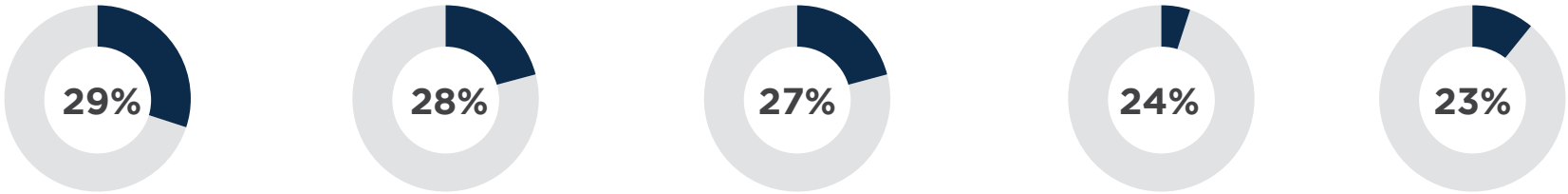


ATTACK RESPONSE TACTICS

Following a ransomware attack, cybersecurity professionals can deploy a number of defensive responses. The single most common response (81%) is identifying the ransomware strain attacking the organization, containing the damage by isolating and shutting down all infected systems and accounts, eradication of malware, followed by recovery from backup files.

How would your organization respond to a ransomware attack?

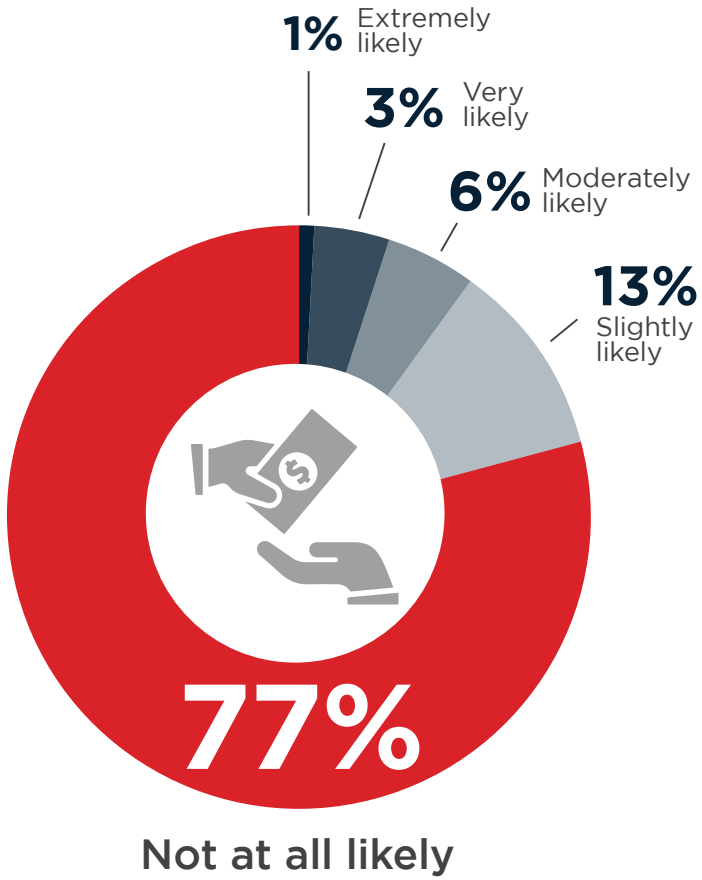
81% Identify the ransomware attacking the organization, contain the damage by isolating and shutting down all infected systems and accounts, eradicate malware, and recover affected files and volumes from backups.



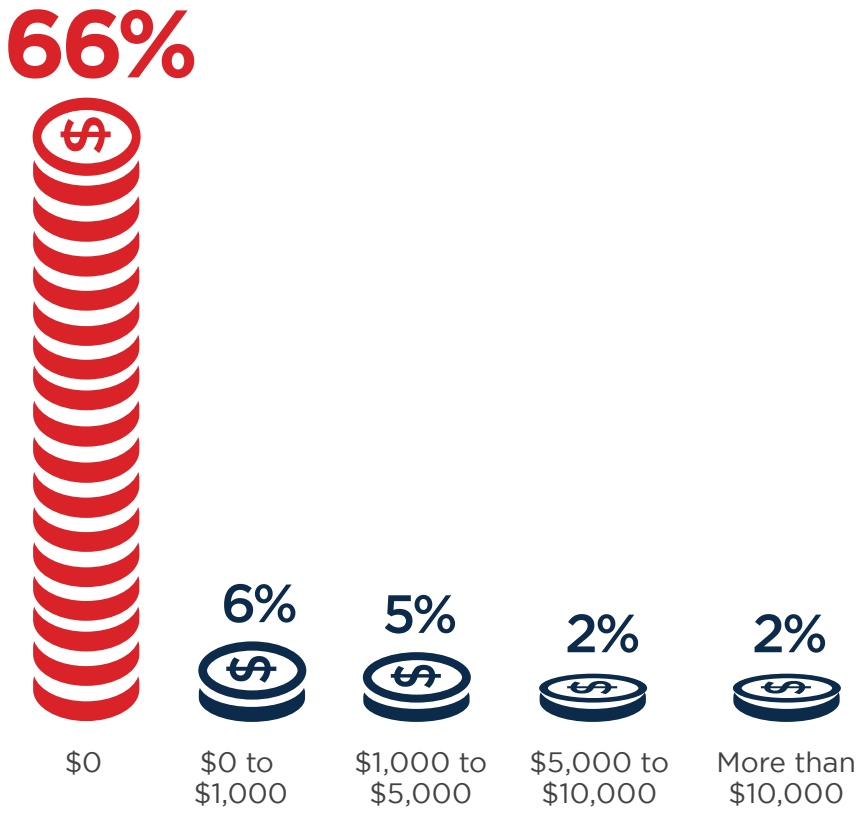
TO PAY OR NOT TO PAY

More than three-quarters of respondents say their organization is not at all likely to pay the ransom in order to recover their data (77%). The position of refusal to pay is admittedly somewhat theoretical as it is much harder to take a principled stand when the survival of a business and jobs are on the line (or when no viable backup is available). Only a small minority confirm they are willing to pay some ransom (3% of companies have already set up a Bitcoin account in preparation).

How likely is your organization willing to pay for recovering data affected from a ransomware attack?



How much money would your organization pay in response to a ransomware attack?



Can't disclose 19%

RANSOMWARE DEFENSE & BUDGET

EFFECTIVE RANSOMWARE PREVENTION

There are a myriad of cybersecurity tools and policy controls available to combat ransomware early on. Security professionals rank user awareness and training as the most effective means to prevent and block ransomware (77%). The survey indicates both Anti-Malware/ Antivirus/ Endpoint security solutions (73%) and updating / patching operating systems and software (72%) were highly effective as preventive approaches to ransomware threats. Successful ransomware prevention relies on a blend of security controls and effective user training.

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

77%

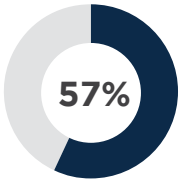
User awareness and training

73%

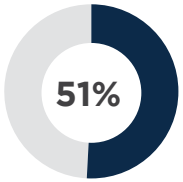
Anti Malware/Antivirus/ Endpoint security solution

72%

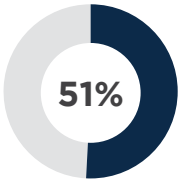
Updating/patching operating systems and software with latest versions



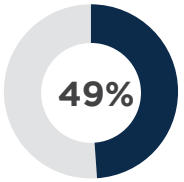
Email and web gateways



Spam filters



Network IDS / Traffic Monitoring



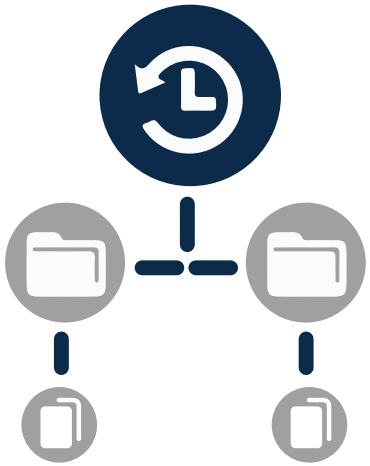
Internal access controls and authentication

Infrastructure security monitoring 46% | Behavior-based / machine learning endpoint protection 45% | File monitoring 41% | Sandbox 35% | Application whitelisting 34% | User monitoring 29% | Behavioral analytics 1% | Other 7%

RANSOMWARE RESPONSE: DATA BACKUP & RECOVERY

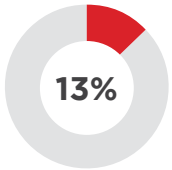
Cybersecurity professionals view data backup and recovery (74%) by far as the most effective solution to respond to a successful ransomware attack. A whopping 96% confirm they have a data backup and recovery strategy in place. This way, organizations can recover their backups and restore data without having to pay cybercriminals.

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

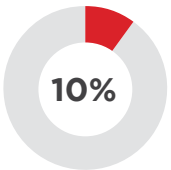


74%

Data backup and recovery response



Threat intelligence

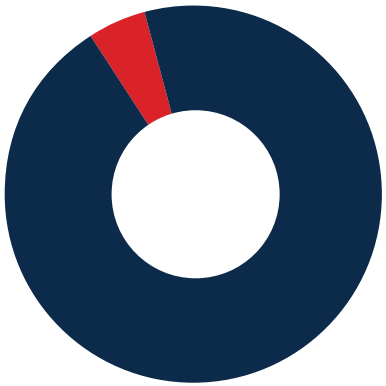


Behavioral analytics

Cyber insurance

Do you have a data backup and recovery strategy?

4%
NO



96%
YES

ENDPOINT SECURITY

To stay ahead of evolving security threats, organizations employ a multi-layered security approach, including strong endpoint security. When asked about the most effective endpoint security capabilities to protect against ransomware, most respondents agree that blocking ransomware attacks at pre-execution (60%), and detecting and blocking traffic at the first sign of malicious behavior (59%) rank as the most valuable endpoint security capabilities. This is followed by technologies that do not rely on signatures but can detect ransomware based on behavior (49%).

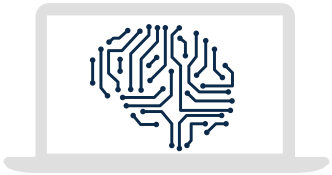
What do you think is the most valuable endpoint security technology to have?

60%

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

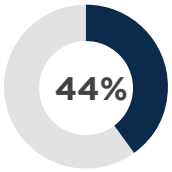
59%

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

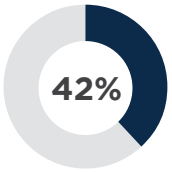


49%

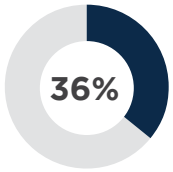
Non-signature based detection and prevention (such as machine learning and behavior-based solutions)



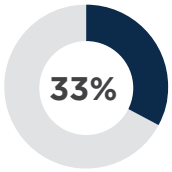
Built-in Web security preventing access to phishing, fraudulent or exploit-hosting sites



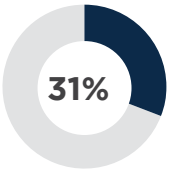
Advanced file analysis - i.e. NextGen Antivirus tools



Fileless/exploit prevention through real-time behavior analysis



Automatic mitigation including the ability to roll back changes



File-based detection - signature-based traditional Antivirus

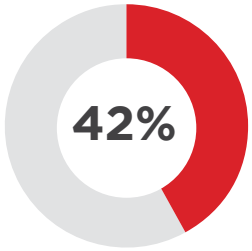
Endpoint integrated sandbox 29% | Built-in anti-exploit 28% | Don't know/other 16%

OBSTACLES TO RANSOMWARE PROTECTION

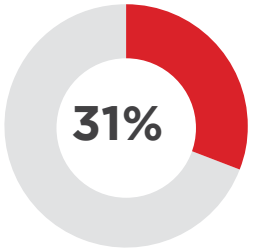
The three biggest obstacles standing in the way of stronger ransomware defense are all about resources and staying current on the latest ransomware exploits: lack of budget (52%), dealing with evolving sophistication of attacks (42%), and lack of human resources (33%).

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

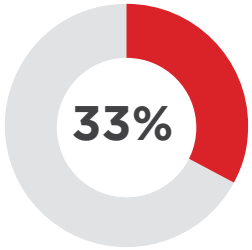
52%
Lack of budget



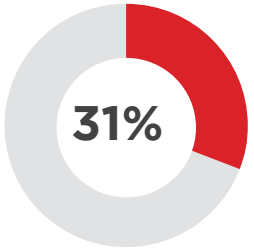
Evolving sophistication of attacks



Poor user awareness



Lack of human resources



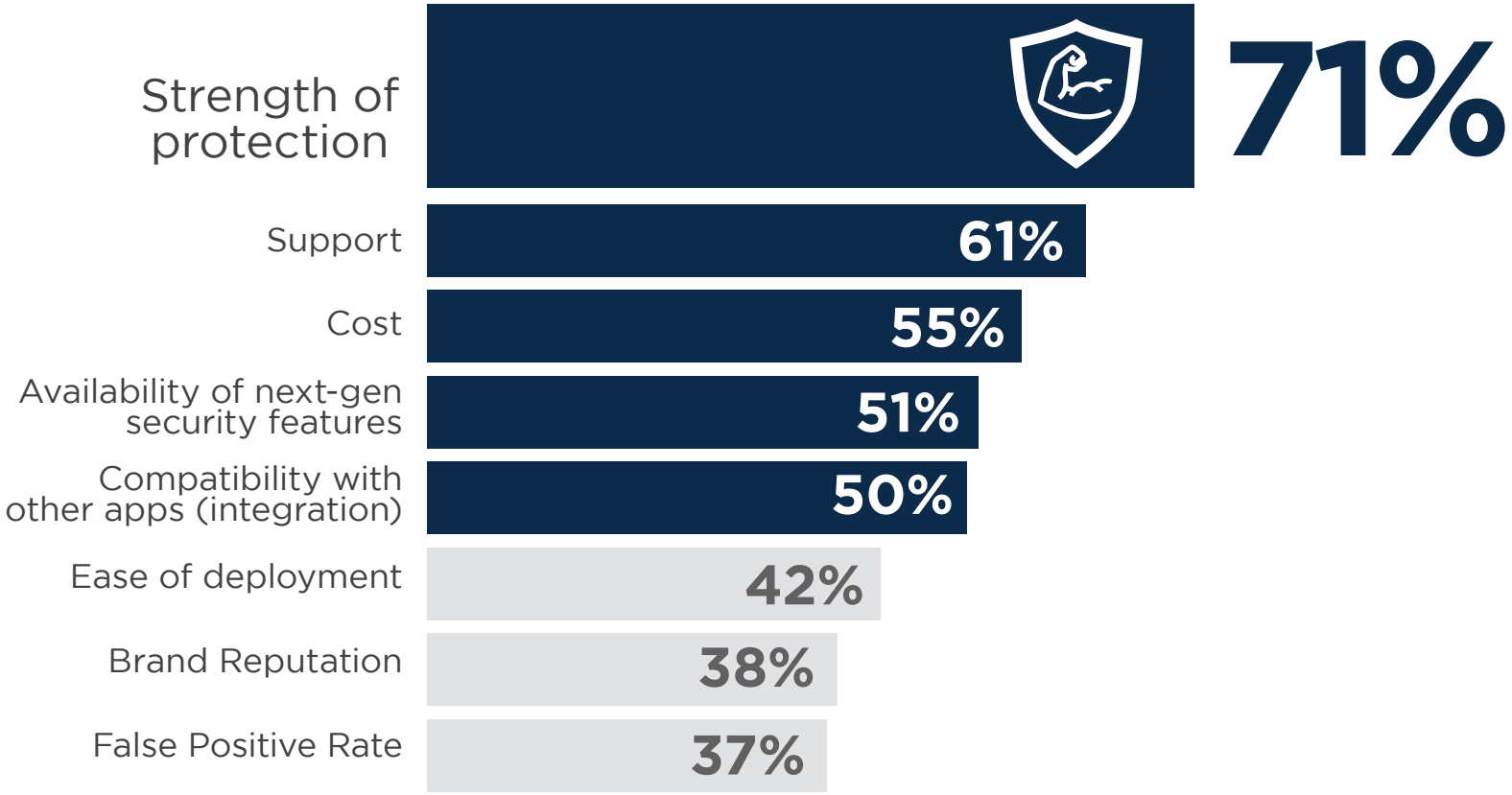
Growing proliferation of attacks

Lack of executive sponsorship 28% | Uncertainty what security solution to use 21% | Our partners' lack of preparedness or response 10% | Don't know/other 8%

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 (71%), followed by support (61%) and cost (55%). Availability of next-gen security features (51%) and integration with other apps (50%) round out the top five selection criteria.

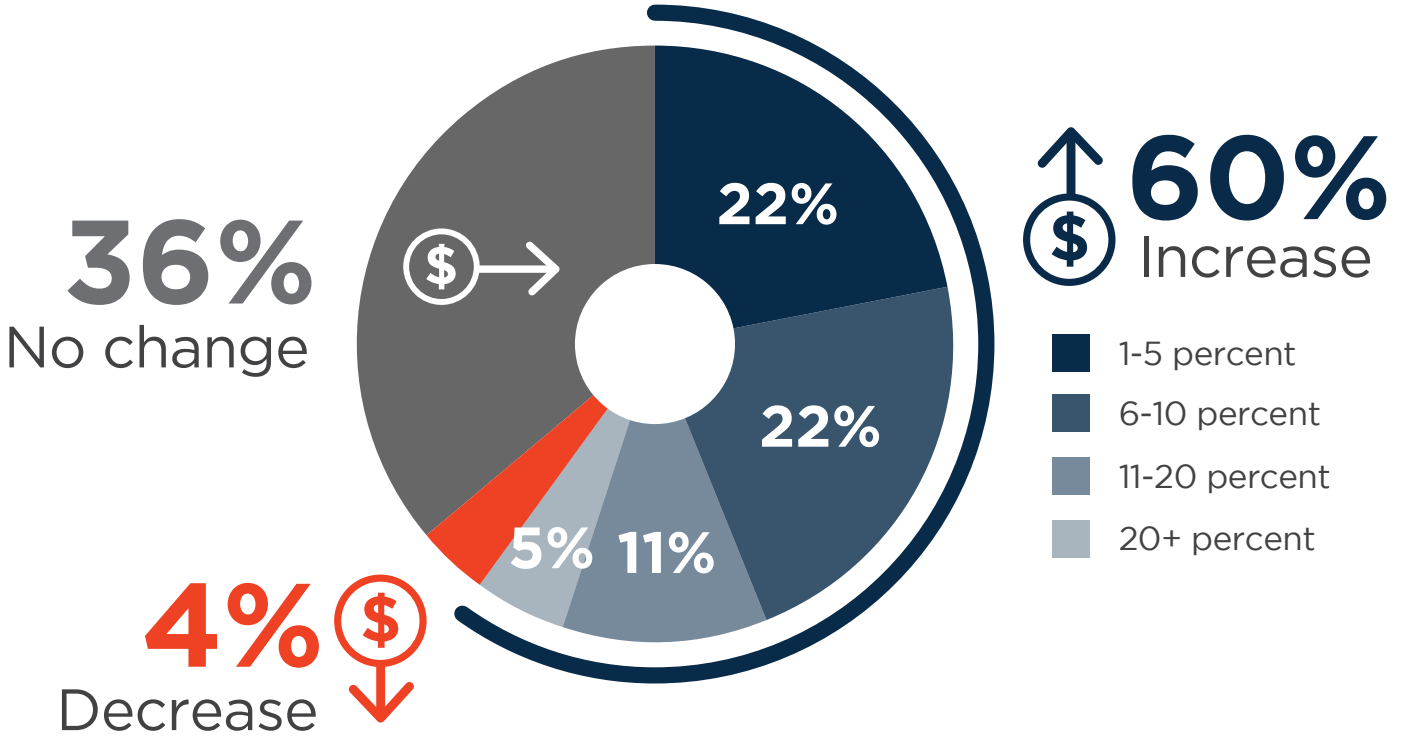
What are the main criteria that you consider when selecting a security provider to protect you from ransomware attacks?



RANSOMWARE PROTECTION BUDGET

Sixty percent of organizations expect their budget for ransomware security to increase over the next 12 months. That is the strongest budget increase intent we have seen in years of cybersecurity research – likely driven by the dramatic rise in ransomware attacks and their devastating impact. Thirty-six percent do not expect a change in their budget, while the remaining 4% foresee a decrease in their ransomware security funding.

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



EMAIL SECURITY

EMAIL THREAT CHALLENGES

Cybercriminals use email as a common entry vector to gain access into organizations; it is a popular medium for the spread of spam, phishing attacks and ransomware. The top two challenges facing Security Operation Centers against evolving email threats are detection time (67%) and mitigation time (50%).

Which of the following do you consider to be top challenges facing your SOC/security team in relation to addressing emerging email threats?

67%

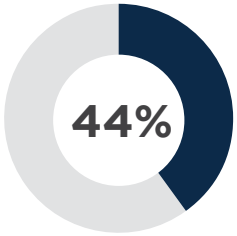
Detection time

50%

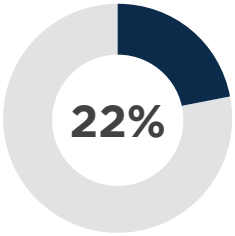
Mitigation time

45%

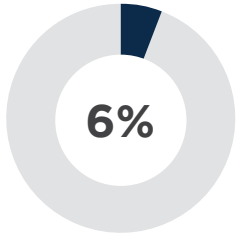
Remediation of infected mailboxes



Forensics



Orchestration

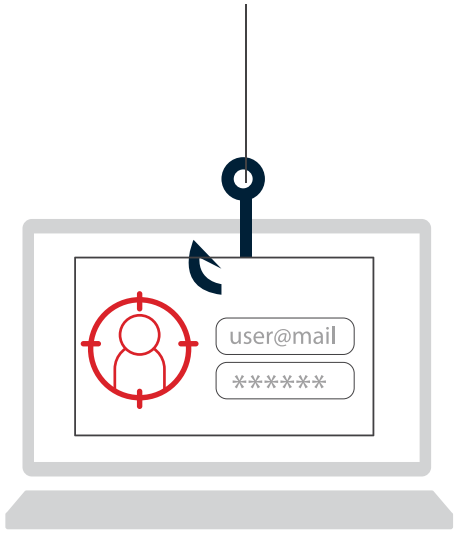


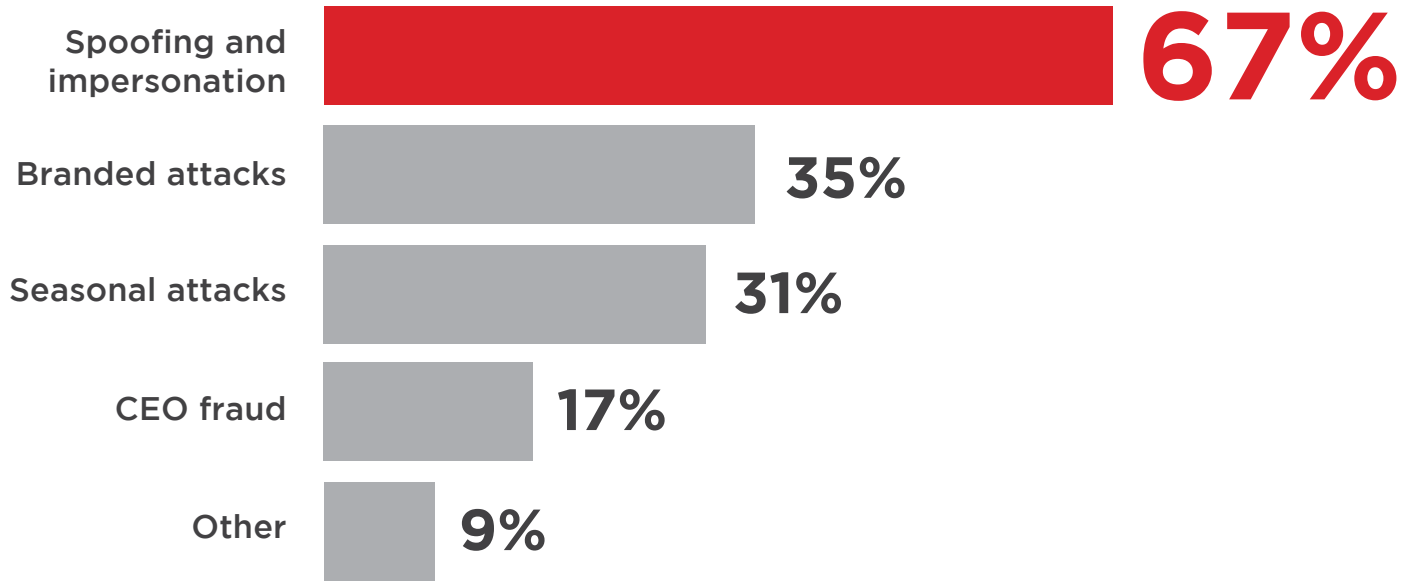
Other

PHISHING ATTACKS

Phishing attacks trick employees into sharing sensitive company information, by posing as legitimate businesses or trusted contacts, often containing malware in attachments or hyperlinks to compromised websites. Security professionals confirmed that their employees are most often victims of spoofing and impersonation (67%), followed by branded (35%) and seasonal attacks (31%). This clearly shows the need for better detection and InMail tools to help employees spot spoofing and impersonation attacks.

What types of phishing attacks are most successful in tricking your employees?

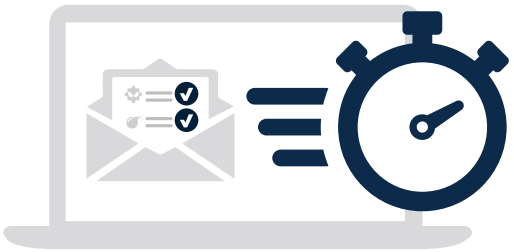




PHISHING RESPONSE SPEED

Remediation of attacks is one of the biggest security challenges. An alarming half of organizations say it takes a day or longer to remove a phishing email from endpoints once a phishing attack has been reported to the SOC/security team (46%).

How long does it take your SOC/security team to remove a phishing email completely from all endpoints in the network?

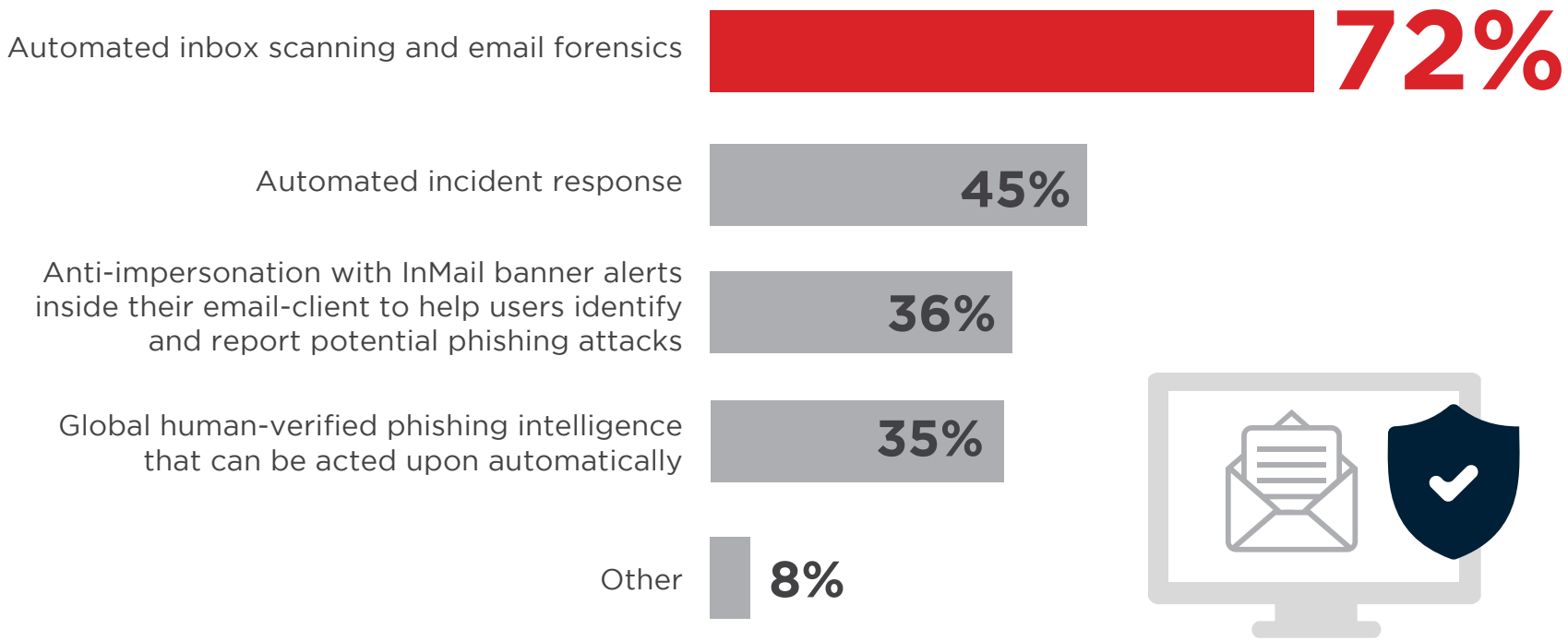


46% take a day or longer to remove a phishing email

EMAIL SECURITY SOLUTIONS

We asked security practitioners what they consider the most effective email security technologies to help thwart email threats. They prioritize automated inbox scanning and email forensics (72%), over automated incident response (45%), followed by anti-impersonation with InMail banner alerts (36%) and global human-verified phishing intelligence (35%).

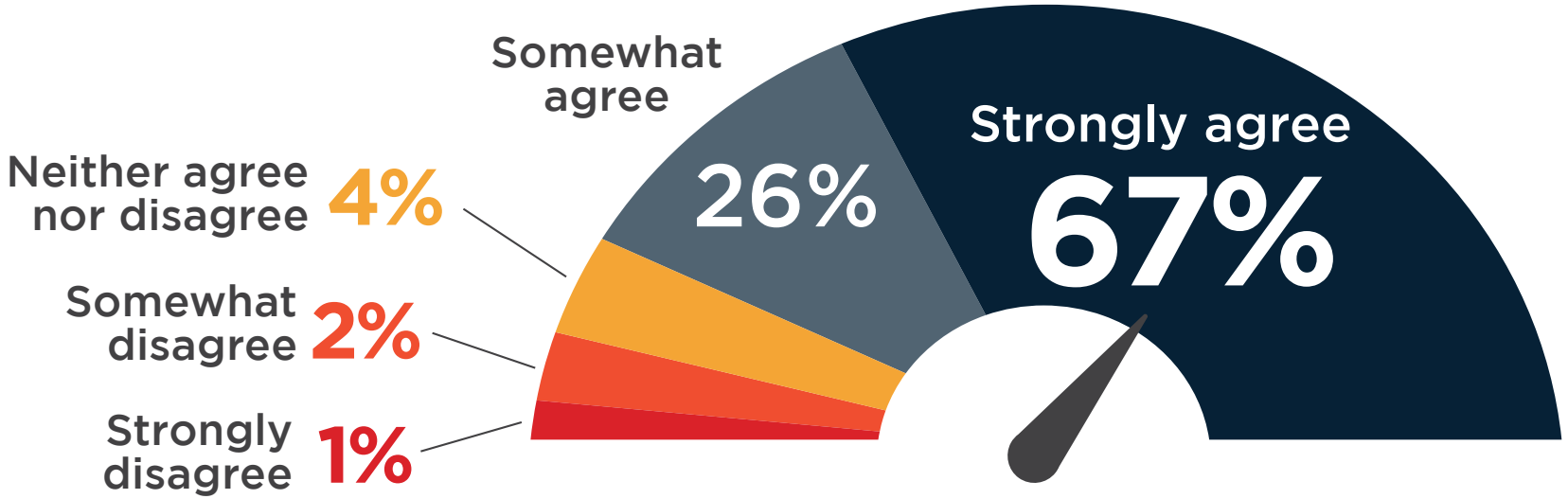
What do you think is the most valuable email security technology to have?



HUMANS & TECHNOLOGY AGAINST PHISHING

Ninety-three percent of respondents agree that humans and technology need to work side by side in order to better detect and respond to sophisticated email phishing attacks.

What is your level of agreement with the statement: "Humans and technology need to work side by side in order to better detect and respond to sophisticated email phishing attacks."



ANATOMY OF A RANSOMWARE ATTACK

Ransomware typically spreads via spam or phishing emails, but also through websites or drive-by downloads, to infect an endpoint and penetrate the network. Once in place, the ransomware then locks all files it can access using strong encryption. Finally, the malware demands a ransom (typically payable in Bitcoins) to decrypt the files and restore full operations to the affected IT systems.

1 INFECTION

After it has been delivered to the system via phishing email, the ransomware installs itself on the endpoint and any network devices it can access.

2 SECURE KEY EXCHANGE

The ransomware contacts the command and control server operated by the cybercriminals behind the attack to generate the cryptographic keys to be used on the local system.

3 ENCRYPTION

The ransomware starts encrypting any files it can find on local machines and the network.

4 EXTORTION

With the encryption work done, the ransomware displays instructions for extortion and ransom payment, threatening destruction of data if payment (typically in Bitcoins) is not made.

5 UNLOCKING

Organizations can either pay the ransom and hope for the cybercriminals to actually decrypt the affected files (which in many cases does not happen). Or they can attempt recovery by removing infected files and systems from the network and restoring data from clean backups.

HOW TO PROTECT AGAINST RANSOMWARE

1. **SEGREGATE NETWORKS**
and turn off network shares to minimize the spread of a ransomware infection

2. **TURN OFF ADMIN RIGHTS**
for users who don't require them and apply least privilege policies

3. **RESTRICT WRITE PERMISSIONS**
on file servers as much as possible

4. **EDUCATE YOUR USERS**
on the most common phishing and ransomware email patterns and how to respond

5. **MAKE FREQUENT, COMPREHENSIVE BACKUPS**
of critical files and keep them offline

6. **PROTECT EMAIL AND WEB ACCESS**
with email and web security gateways with advanced threat protection capabilities

7. **DEPLOY SOPHISTICATED ENDPOINT SECURITY**
with behavioral and intelligent monitoring of suspicious patterns

8. **PATCH EARLY AND OFTEN**
to close known vulnerabilities in operating systems, browsers, and web plugins

GOT AN ACTIVE RANSOMWARE INFECTION?

ISOLATE AND SHUT DOWN NETWORKS AND SYSTEMS
in the event of an active ransomware infection to prevent further spread

IDENTIFY AND ERADICATE THE RANSOMWARE
and follow best practices for dealing with this specific strain, including deploying ransomware removal tools or hiring experts

WIPE INFECTED MACHINES AND RESTORE FROM BACKUPS
to make sure no ransomware remnants remain hidden in your systems

POST MORTEM ANALYSIS AND MONITORING
to understand the anatomy of the attack and prevent similar attacks from occurring again

SPONSOR OVERVIEW

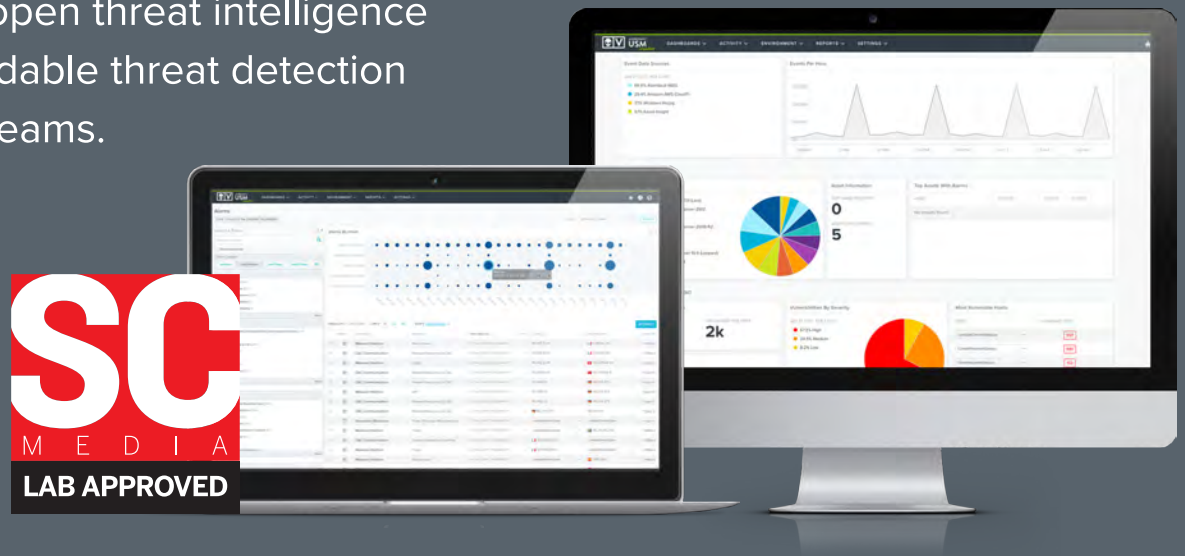
SPONSOR OVERVIEW

AlienVault® | www.alienvault.com

AlienVault® has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our unique and award-winning approach combines our all-in-one platform, AlienVault Unified Security Management™, with the power of AlienVault's Open Threat Exchange®, making effective and affordable threat detection attainable for resource-constrained IT teams.

AlienVault® has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our unique and award-winning approach combines our all-in-one platform, AlienVault Unified Security Management™ (USM™), with the power of the Open Threat Exchange™, the first truly open threat intelligence community, to make effective and affordable threat detection attainable for resource-constrained IT teams.

Learn More and Start a Free Trial >

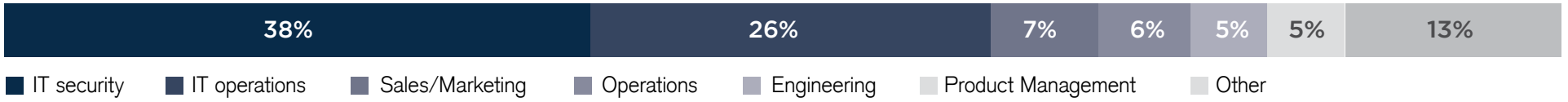


www.alienvault.com

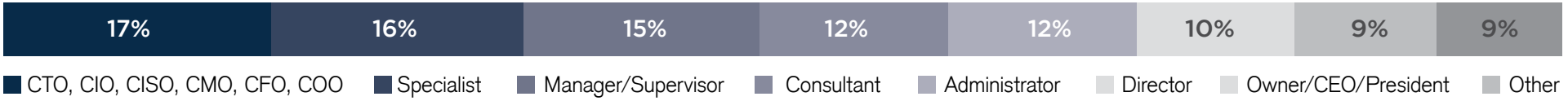
METHODOLOGY & DEMOGRAPHICS

The 2017 Ransomware Report is based on the results of a comprehensive online survey of 516 cybersecurity professionals to gain deep insight into the ransomware threat faced by organizations and the solutions to detect, remediate, and prevent it. The respondents range from technical executives to managers and IT security practitioners, representing organizations of varying sizes across all industries.

DEPARTMENT



JOB LEVEL



IT SECURITY TEAM SIZE

COMPANY SIZE