2021

Cybersecurity
INSIDERS

# MALWARE REPORT

FORTRA

# INTRODUCTION

Malware and ransomware are one of the most destructive security threats affecting organizations of all sizes, from SMBs to large enterprises and government agencies. Malware is continuously evolving and organizations are facing significant challenges in responding to the threat and protecting their IT environments against new types of viruses, worms, spyware, ransomware, and crypto-jacking malware.

The 2021 Malware Report was produced by Cybersecurity Insiders and Fortra to reveal the latest malware security trends, challenges, and investment priorities.

**Key findings include:**

- Eighty-eight percent of respondents see malware and ransomware either as an extreme threat (60%, up five points since last year) or moderate threat (28%).
- A significant majority (75%) of IT security professionals predict malware and ransomware to become a larger threat in the future.
- Spear-phishing emails remain the single most dangerous malware attack vector at 82%, followed by domain spoofing (45%) and man-in-the-middle attacks (43%).
- Ransomware 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 an increase in IT security-related spending (61%, up two points from last year's survey) and productivity loss (55%). At the IT operations level, ransomware is forcing cybersecurity professionals to update IT security strategies to focus on mitigation (45%), as well as causing system downtime (42%).
- When asked about the most effective security solutions to combat malware/ransomware, security professionals rank anti-malware/antivirus/endpoint security solutions the highest at 78%. This is closely followed by user awareness and training at 70%.

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

We hope you find this report informative and helpful as you continue your efforts in securing your organizations against evolving threats.

Thank you,

Holger Schulze

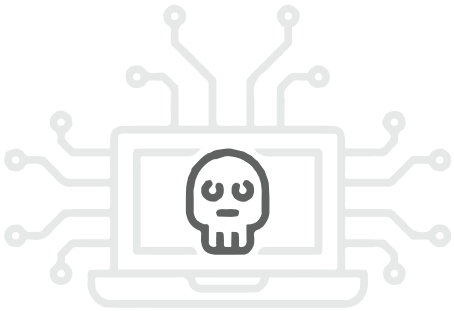
**Holger Schulze**
CEO and Founder
Cybersecurity Insiders

Cybersecurity
INSIDERS

# RISING THREAT LEVEL

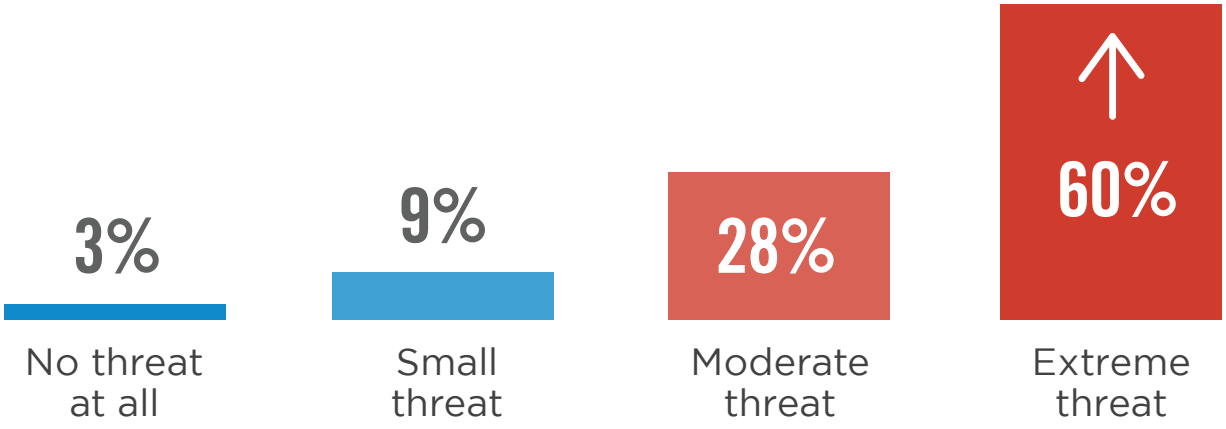
The malware and ransomware threat is growing and continues to be among the most destructive security threats affecting organizations of all sizes. Eighty-eight percent of respondents see malware and ransomware either as an extreme threat (60%, up five points since last year) or moderate threat (28%).

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



**88%**

**Of respondents see malware as an extreme or moderate threat**




A significant change from 2020, with a 5% shift from moderate to more extreme responses.

# FUTURE ATTACKS

A significant majority (75%) of IT security professionals predict malware and ransomware to become a larger threat in the future. Similarly, 82% expect an increase in attack frequency over the next 12 months — an increase of eight percentage points since last year.

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

**75%**

**Believe malware and ransomware will be a larger threat to organizations in the next 12 months**


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

**82%**

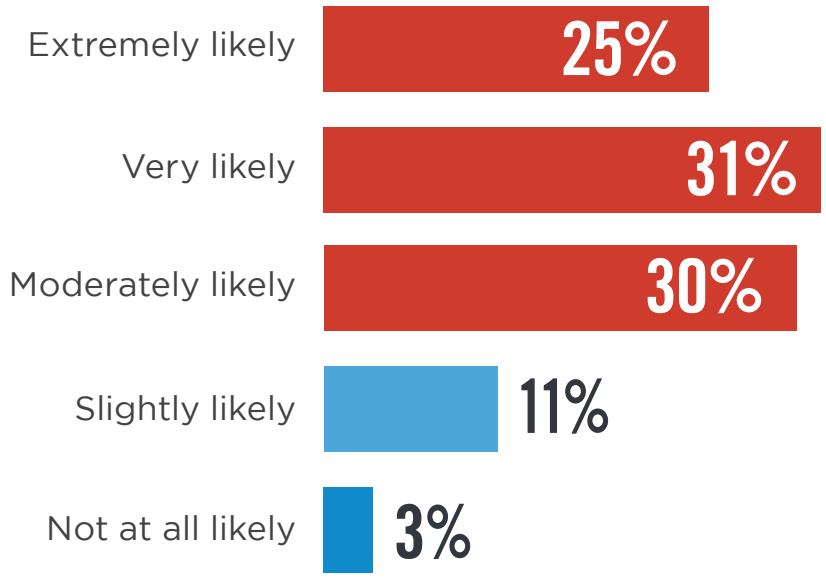
**Believe malware and ransomware attacks will be more frequent**


An increase of 8% from last year.

# WORSENING ATTACK OUTLOOK

We asked organizations how they perceive their risk of becoming a target of malware or ransomware attacks in the next 12 months. A growing majority (86%, up seven percentage points since last year) said an attack is 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?**




An increase of 7% from last year

**86%**

**Of respondents said an attack is at least moderately likely**

# REMOTE WORK RISK

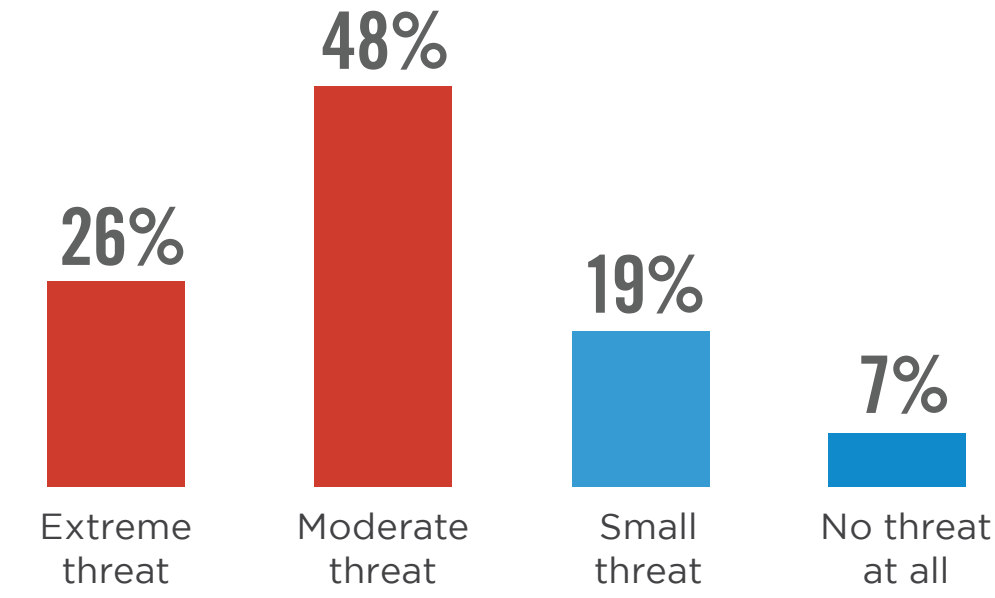
The recent Covid-19 pandemic triggered a massive shift toward remote work, resulting in a significant deterioration in organizations' risk exposure. A majority (74%) see remote work as a moderate threat to extreme threat to their organization. This represents a slight recovery from the risk perception we saw last year.

**How significant of a business threat are remote workers to your business?**

A decrease of 8% from last year

**74%**

**View remote workers as at least a moderate threat to the business**

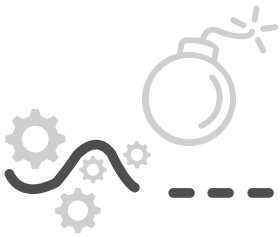


# WHAT MOTIVATES ATTACKERS

We asked organizations what they believe is the main motivation for malware/ransomware attacks. As in previous years, financial gain (80%, up by two points) tops the list of motivators, followed by a desire to sabotage and disrupt business activities (52%, down by three points), and entertainment or hacking for fun (34%, up three points).

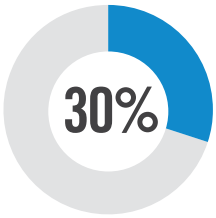
**What do you believe is the main motivation for malware/ransomware attacks against your organization?**

**80%**
Financial gain

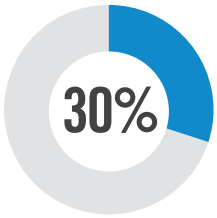


**52%**
Sabotage/disruption of business

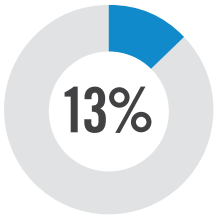
**34%**
Entertainment
(hacking just for fun)



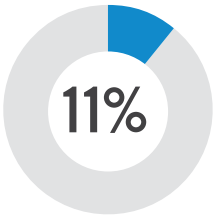

Cyber espionage




State-sponsored international attack




Political motivation




Revenge for a bad experience with organization

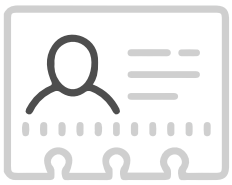
Don't know/other 9%

* Respondents could select all options that applied to their organization.

# DATA AT RISK

When asked what types of data organizations consider to be most at risk from ransomware attacks, cyber professionals prioritize customer information (63%), followed by financial data (53%) and employee information (51%).

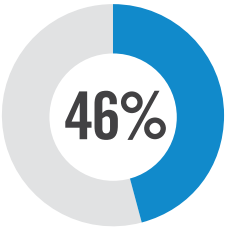
**What type of data in your organization is most at risk from malware/ransomware attacks?**



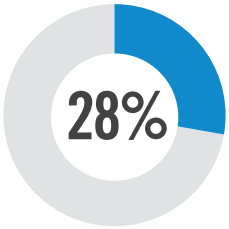
**63%**
Customer information

**53%**
Financial data

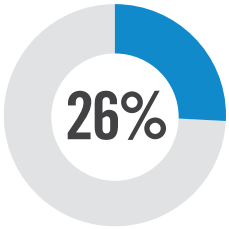
**51%**
Employee information



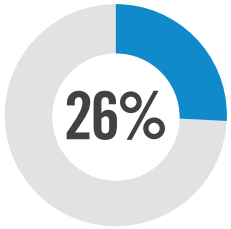

Company intellectual property




Payroll/HR




Product information




Research and design

Other 8%

* Respondents could select all options that applied to their organization.

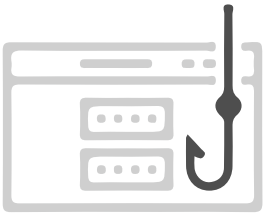
# MALWARE TYPES

The ever-evolving types of malware can be confusing — and new variants are created virtually every day. We asked what types of malware organizations find particularly concerning. Ransomware remains the top offender at 82% of responses, followed by phishing attacks (63%) and viruses (53%).

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

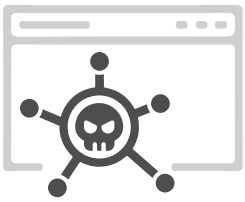
**82%**

Ransomware



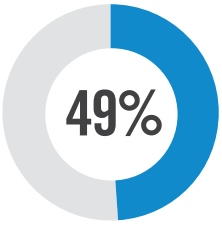
**63%**

Phishing attacks

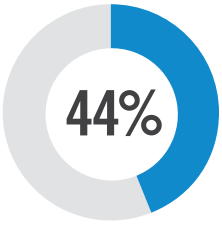


**53%**

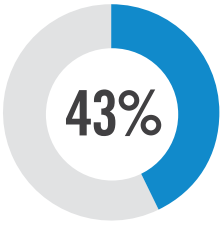
Viruses



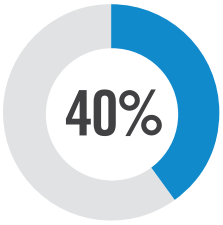

Spyware




Trojans




Cryptojacking




Bots

Rootkits 37% | Worms 35% | Fileless malware 34% | Polymorphic malware 34% | Attacks that use artificial intelligence 33% | Multi-vector malware 32% | Adware 22% | Other 2%

* Respondents could select all options that applied to their organization.

# MALWARE ATTACK VECTORS

We asked cybersecurity professionals what malware attack vectors they find most dangerous. Spear-phishing emails remain the single most dangerous malware attack vector at 82%, followed by domain spoofing (45%) and man-in-the-middle attacks (43%).

**What malware attack vectors do you consider most dangerous?**

**82%**

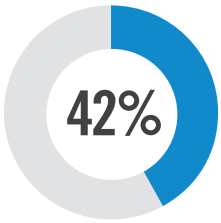
Spear-phishing emails


**45%**

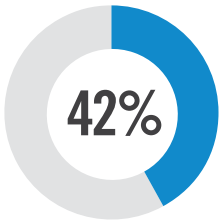
Domain spoofing

**43%**

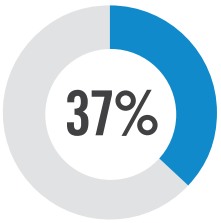
Man-in-the-middle attacks



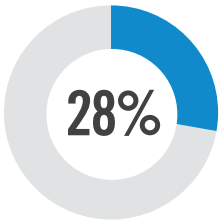

Trojanized software




Web server exploits




SQL injection




Cross-site scripting

Watering hole websites 24% | Other 3%

* Respondents could select all options that applied to their organization.

# EXPERIENCED ATTACKS

More than four out of ten organizations (41%) say they have experienced ransomware attacks. Fifty-nine 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?**

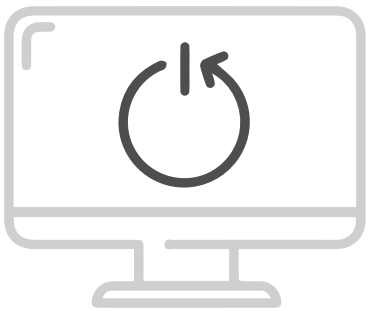
**41%**
**YES**
My organization has been affected by ransomware.

**59%**
**NO**

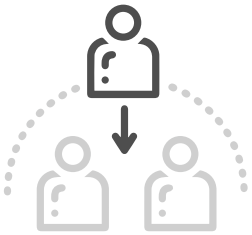
# RECOVERY TACTICS

We asked organizations how they recovered from the ransomware attacks they experienced. A majority (54%) re-installed or restored backups. Eighteen percent brought in third-party experts for help and 13% managed to decrypt locked files. Only 5% paid the ransom.

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



**54%** Re-installed/ restored



**18%** Brought in third-party

**13%** Decrypted files ourselves

**5%** Paid the ransom

Not sure/other 38%

* Respondents could select all options that applied to their organization.

# HOW RANSOMWARE ENTERS

When asked how ransomware found its way into the corporate network, survey participants report that phishing emails are the number one path of entry (70%, up two points from last year). Email attachments (54%) and malicious websites (41%) round out the three most common infection methods for ransomware to gain access.

**How has ransomware entered your organization?**

**70%**

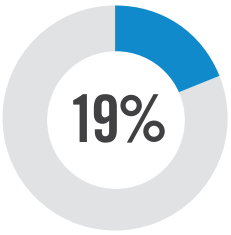
Phishing emails

**54%**

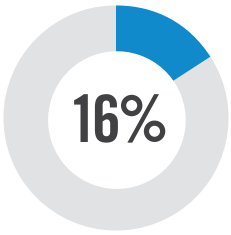
Email attachments


**41%**

Users visiting malicious or compromised websites




Exploits targeting vulnerable systems




Scan and exploit

Not sure/other 6%

* Respondents could select all options that applied to their organization.

# IMPACT OF MALWARE ATTACKS

Ransomware 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 an increase in IT security related spending (61%, up two points from last year's survey) and productivity loss (55%). At the IT operations level, ransomware is forcing cybersecurity professionals to update IT security strategies to focus on mitigation (45%), as well as causing system downtime (42%).

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

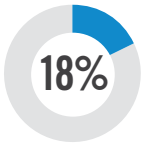
## BUSINESS IMPACT

**61%**
Increased spending on IT security

**55%**
Productivity loss

Revenue loss

Damage to company reputation

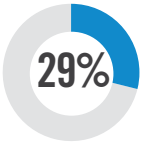


Negative press/ bad publicity

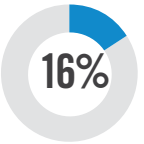
## IT OPERATIONS/SECURITY IMPACT

**45%**
Change of IT security strategy

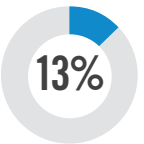
**42%**
System downtime



Data loss



Senior IT staff (CIO, CISO) lost their jobs



Loss of confidence in existing cybersecurity solutions

We did not experience any ransomware attacks 24%

* Respondents could select all options that applied to their organization.

# MALWARE DETECTION

Cybersecurity analysts have access to numerous threat detection tools to identify and monitor cyber threats. Most malware/ransomware attacks are detected through anti-malware/antivirus/endpoint security tools (82%). This is followed by email and web gateways (61%) and intrusion detection systems (49%). Unfortunately, an increasing number of innovative malware variants succeed in evading detection.

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

**82%**

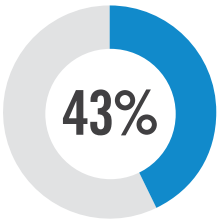
Anti-malware/ antivirus/endpoint security tools

**61%**

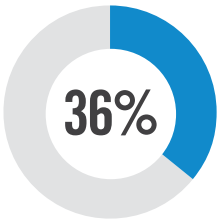
Email and web gateways

**49%**

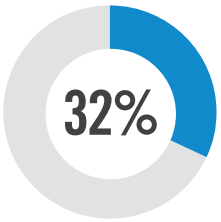
Intrusion detection system



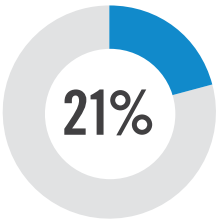

Network behavior monitoring




Compromised user




User behavior monitoring




File monitoring

Analyst 14% | Third-party threat management 9% | We cannot detect ransomware 1% | Not sure/other 9%

* Respondents could select all options that applied to their organization.

# SPEED OF DETECTION

The rate and speed of malware/ransomware detection is critical in responding to fast moving attacks before they succeed in spreading across the network. While the speed of malware/ransomware detection varies based on the specific strain and an organization's detection capabilities, most attacks are typically detected within hours (72%). Fifty percent of organizations report that detection is near real time or within minutes.

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

**72%** Of attacks are detected within hours

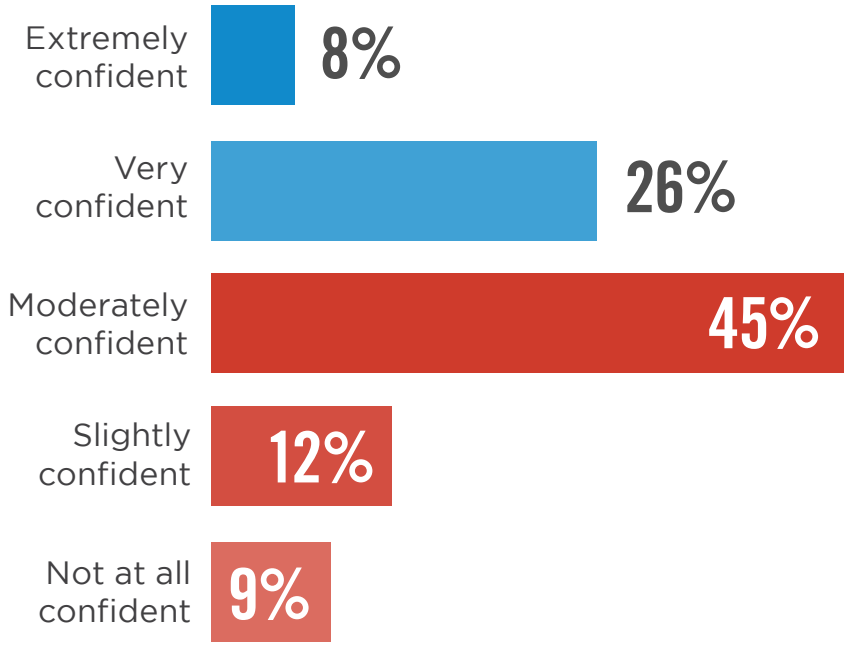





# CONFIDENCE IN DETECTION

A growing majority 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 and files (66%, up 10 points since last year). Only eight percent are extremely confident (four points lower than last year) and 26% are very confident (five point decline).

**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?**




An increase of 10% from last year

**66%**

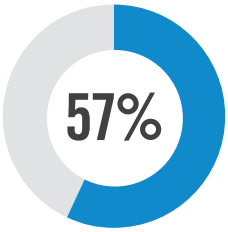
**Are not fully confident in their ability to detect and block an attack**

# ATTACK RESPONSE TACTICS

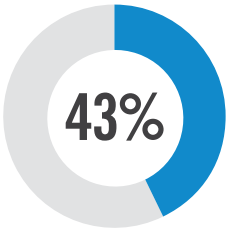
In response to a detected ransomware attack, cybersecurity professionals can take a number of actions. The single most common response (73%) is containing the damage by isolating and shutting down all infected systems and accounts, and recovering the encrypted files from backups while blocking the initial attack vector.

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

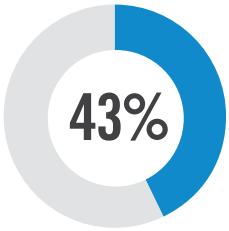
**73%** Isolate and shut down offending systems and accounts, recover encrypted files from backups, and mitigate the initial attack vector if possible




Proactively shut down core systems to prevent spread




Engage a third-party incident response service




Contact cyber insurance provider

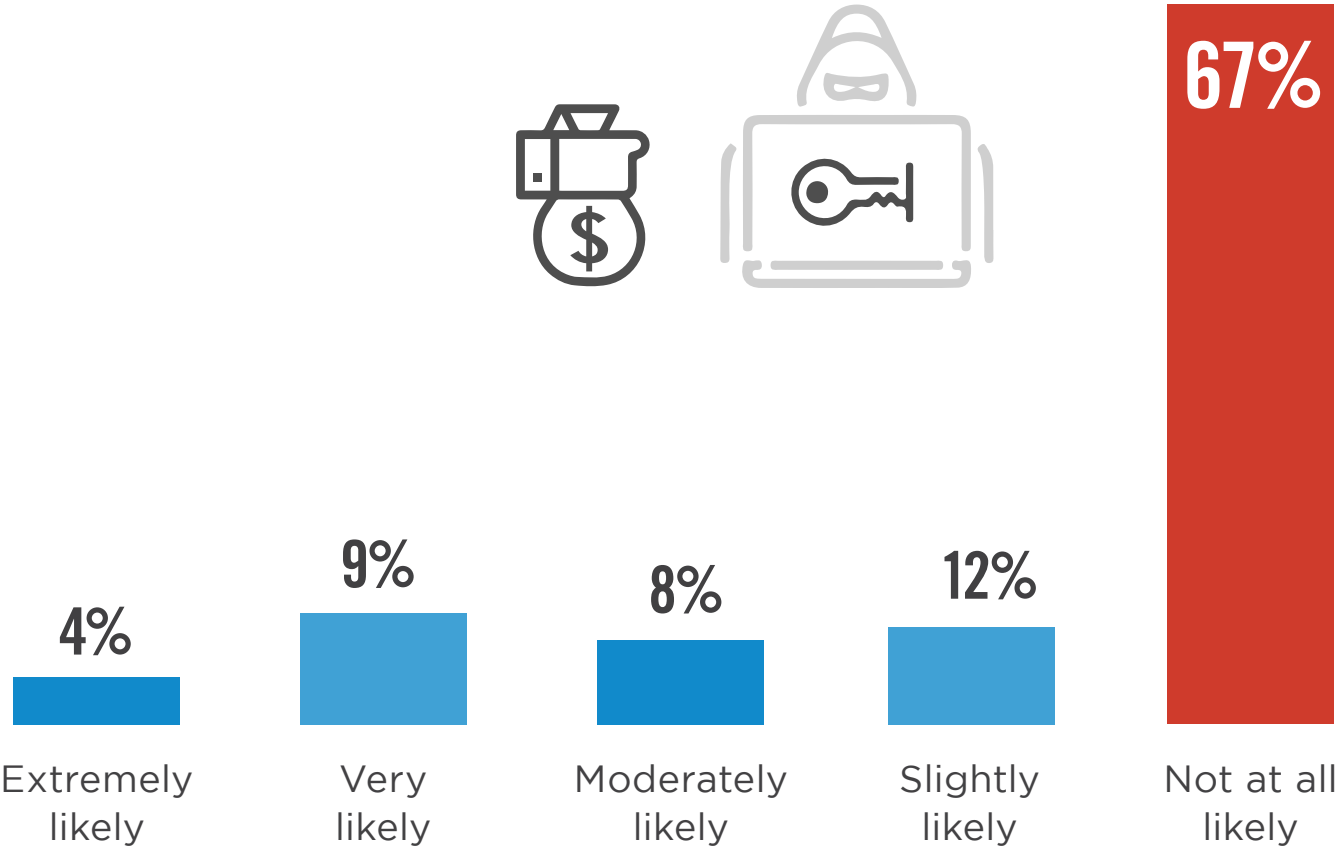
Immediately call law enforcement 32% | Notify customers 32% | Attempt to decrypt files ourselves 30% | Pay the ransom 5% | Attempt to negotiate with the attackers 5%

* Respondents could select all options that applied to their organization.

# NO RANSOM PAYMENT

When asked how likely organizations are to make ransom payments, the vast majority of survey respondents categorically say they will not pay (67%).

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



# EFFECTIVE PREVENTION

When asked about the most effective security solutions to combat malware/ransomware, security professionals rank anti-malware/antivirus/endpoint security solutions highest at 78% (up three points since last year). This is closely followed by user awareness and training as the next most effective strategy to prevent and block ransomware (70%).

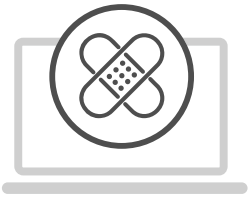
**What security solution(s) would you say is (are) most effective to prevent and block malware/ransomware?**

**78%**

Anti-malware/ antivirus/endpoint security solution

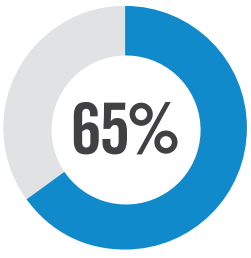
**70%**

User awareness and training

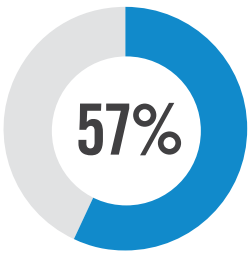


**67%**

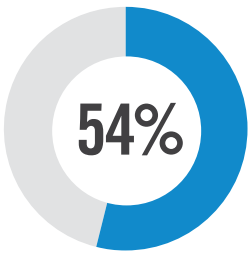
Updating/patching operating systems and software with latest versions



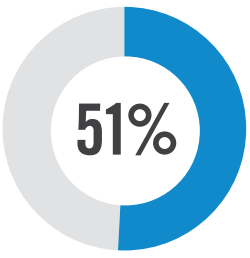

Endpoint Detection and Response (EDR)




Email and web gateway




Spam filters




Infrastructure security monitoring

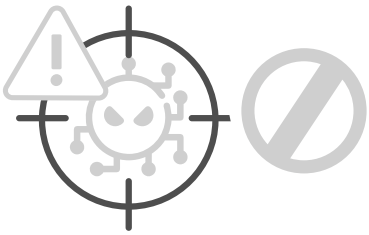
Network IDS/traffic monitoring 50% | Internal access controls and authentication 46% | Behavior-based/machine learning endpoint protection 41%

* Respondents could select all options that applied to their organization.

# ENDPOINT SECURITY

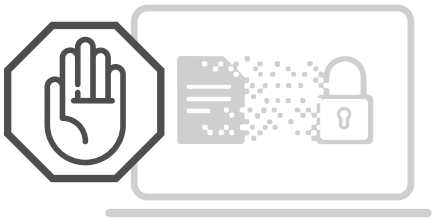
When asked about the most effective endpoint security capabilities to protect against malware, most respondents agree that detecting and blocking malicious behavior (70%, up six points since last year), and blocking ransomware and other attacks pre-execution (60%) rank as the most effective endpoint security capabilities.

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



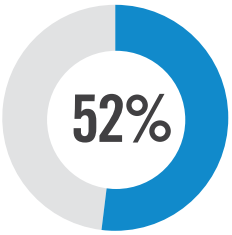
**70%**

Detect and block at the first sign of malicious behavior (i.e., encryption)

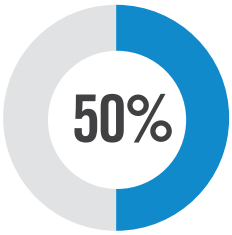


**60%**

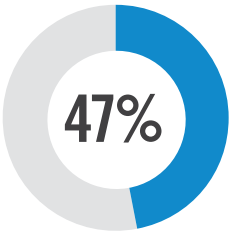
Block ransomware and others at pre-execution to stem the spread



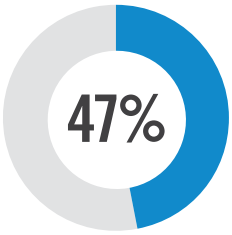

Advanced file analysis (i.e., nextgen antivirus tools)




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




Non-signature based detection and prevention technologies (i.e., machine learning and behavior-based)




Automatic mitigation including the ability to roll back changes

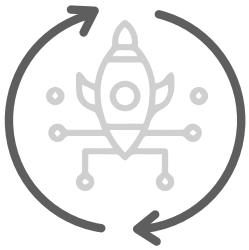
Fileless/exploit prevention through real-time behavior analysis 45% | Endpoint integrated sandbox 44% | File-based detection/signature-based traditional antivirus 36% | Built-in anti-exploit 28% | Other 6%

* Respondents could select all options that applied to their organization.

# OBSTACLES TO DEFENSE

We asked survey participants what they see as the biggest obstacles to better malware defense. Evolving sophistication of malware attacks jumped to the number one spot (51%, up seven points since last year), followed by lack of budget (49%) and the growing proliferation of attacks (37%, up four points).

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



**51%**

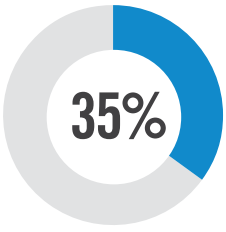
Evolving sophistication of attacks

**49%**

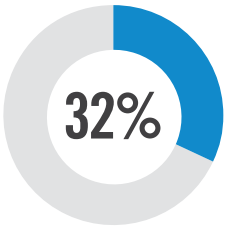
Lack of budget

**37%**

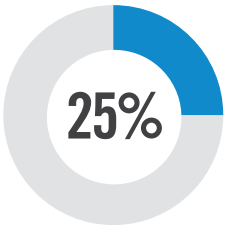
Growing proliferation of attacks



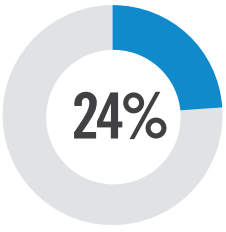

Poor user awareness




Lack of human resources




Uncertainty what security solution to use




Lack of executive sponsorship

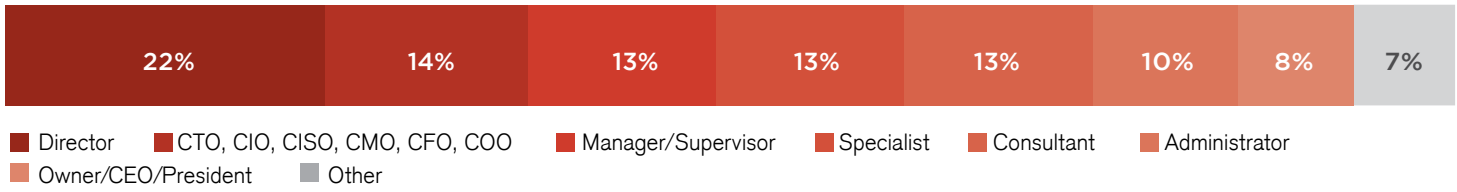
Our partners' lack of preparedness or response 11% | Other 9%

* Respondents could select all options that applied to their organization.

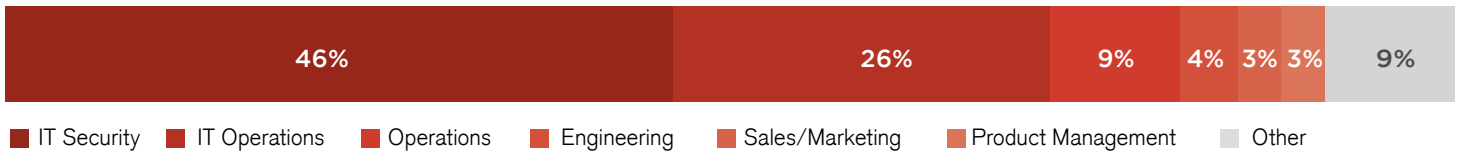
# METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of 367 cybersecurity professionals conducted in May 2021, 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.

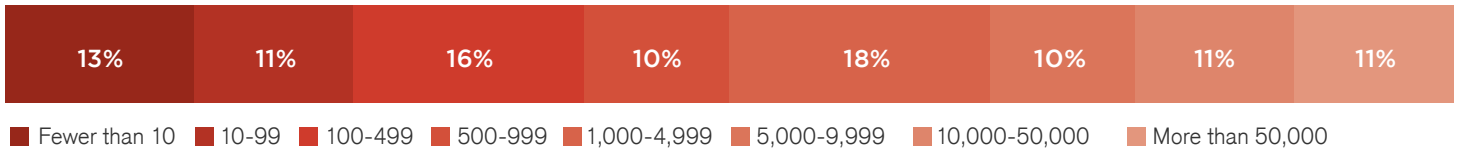
## CAREER LEVEL



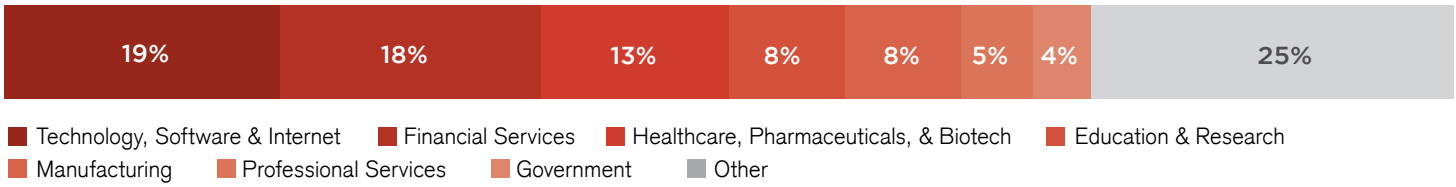

## DEPARTMENT




## COMPANY SIZE




## INDUSTRY



## About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We’re the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.