2022

Cybersecurity INSIDERS

RANSOMWARE & MALWARE REPORT

bitglass

A Forcepoint Company

INTRODUCTION

Malware and ransomware continue to wreak havoc as some 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.

This 2022 Ransomware & Malware Report was produced by Cybersecurity Insiders and Bitglass, a Forcepoint company, to reveal the latest malware security trends, challenges, and investment priorities.

Key findings include:

- A majority of cyber professionals (55%) see malware and ransomware as an “extreme” threat that is not expected to diminish anytime soon. In the next 12 months, 75% of respondents believe malware and ransomware will become a larger threat to their organization.
- Three of the top five ramifications of a malware or ransomware attack negatively affect the bottom line: Productivity loss (52%), system downtime (38%) and revenue loss (27%).
- In response to ransomware attacks, organizations either take an isolation approach (72%) or proactively shut down systems (50%) to thwart an ongoing attack.
- We asked organizations how they are currently protecting against ransomware attacks. Over half (55%) of respondents back up critical files and data. Only about a third (29%) have implemented a zero trust architecture.

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

Thank you,

Holger Schulze

Holger Schulze

CEO and Founder
Cybersecurity Insiders

Cybersecurity INSIDERS

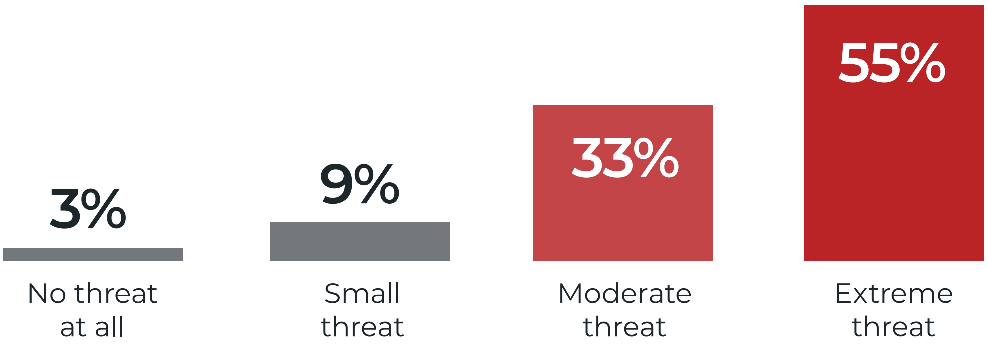
RANSOMWARE HAS BECOME PRIORITY #1

Today, ransomware is on top of organizations' minds. A majority of cyber professionals (55%) even see malware and ransomware as an "extreme" threat. And that threat is not expected to diminish anytime soon. In the next 12 months, 75% percent of respondents believe malware and ransomware will become a larger threat to their organization.

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

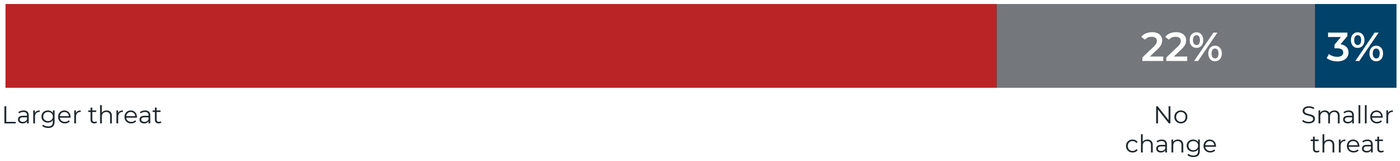
88%

of respondents see malware as an extreme or moderate threat



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

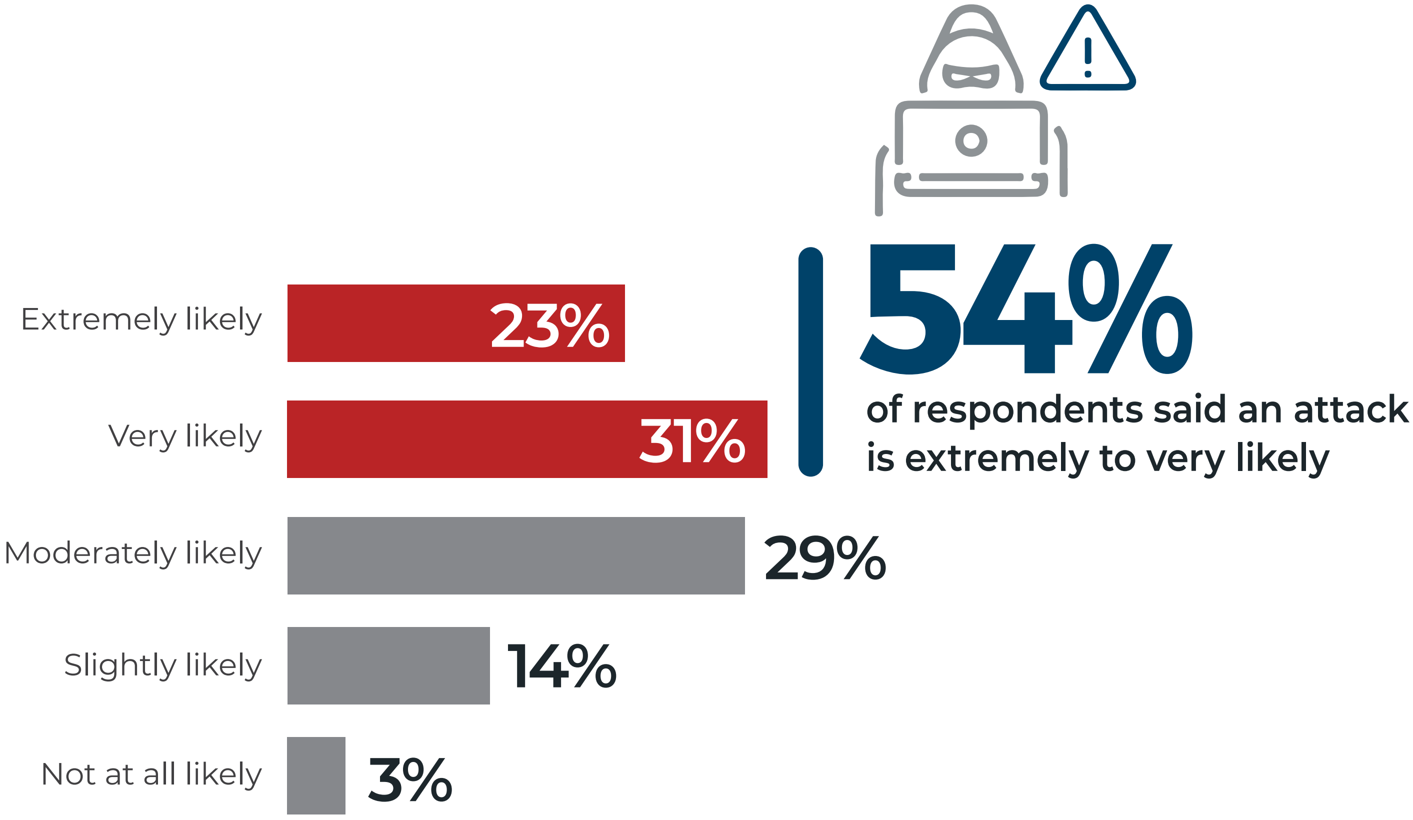
75% **believe malware and ransomware will be a larger threat to organizations in the next 12 months**



RANSOMWARE THREAT RISING

In light of a worsening threat landscape, organizations are quite pragmatic when it comes to ransomware and realize they are likely being targeted for an attack. Over half of respondents believe a malware/ransomware attack is very (31%) to extremely (23%) likely to happen in the next 12 months.

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



54% of respondents said an attack is extremely to very likely

IMPACT OF RANSOMWARE ATTACKS

The impact of an attack directly affects the business. Three of the top five ramifications of a malware/ ransomware attack negatively affect the bottom line: productivity loss (52%), system downtime (38%), and revenue loss (27%). Organizations are tackling the malware and ransomware problem head-on with increased spending (50%) and changing their IT security strategy (40%).

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

BUSINESS IMPACT

52%
Productivity loss

50%
Increased spending on IT security

27% Revenue loss

17% Negative press/ bad publicity

15% Damage to company reputation

IT OPERATIONS/SECURITY IMPACT

40%
Change of IT security strategy

38%
System downtime

23% Data loss

17% Loss of confidence from customers and/or partners in our cybersecurity capabilities

12% Senior IT staff (CIO, CISO) lost their jobs

We did not experience any ransomware attacks 19% | Loss of confidence in existing cybersecurity solutions 2% | Other 2%

RANSOMWARE ATTACK VECTORS

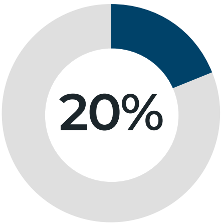
Cybercriminals continue to use classic social engineering techniques, including phishing emails (61%), email attachments (47%), and users visiting malicious websites (39%) to get their ransomware payload into the organization.

How has ransomware entered your organization?

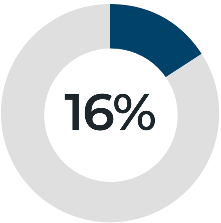
61%
Phishing emails

47%
Email attachments

39%
Users visiting malicious or compromised websites



Exploits targeting vulnerable systems



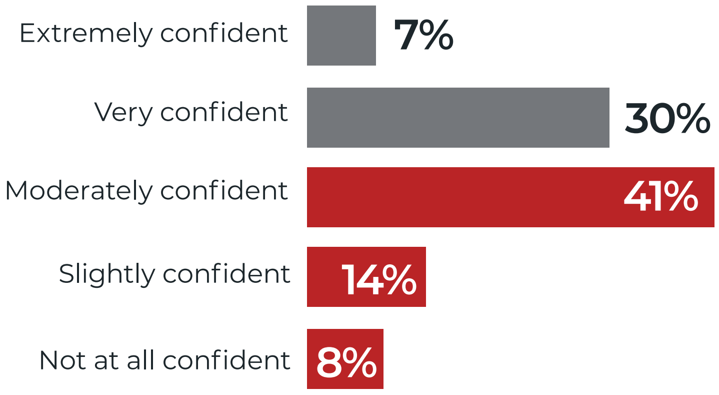
Scan and exploit

Not sure/other 6%

DETECTING RANSOMWARE

Confidence in the ability to detect ransomware remains relatively low. A majority of respondents (63%) are at best only moderately confident in their ability to detect and block malware/ransomware before it spreads to critical systems. To detect potential ransomware threats, IT and security teams are predominantly relying on endpoint tools (82%).

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?



63% are at best only moderately confident in their ability to detect and block an attack

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

82% Anti-malware/ antivirus/endpoint security tools

60% Email and web gateways

47% Intrusion detection system

41% Network behavior monitoring

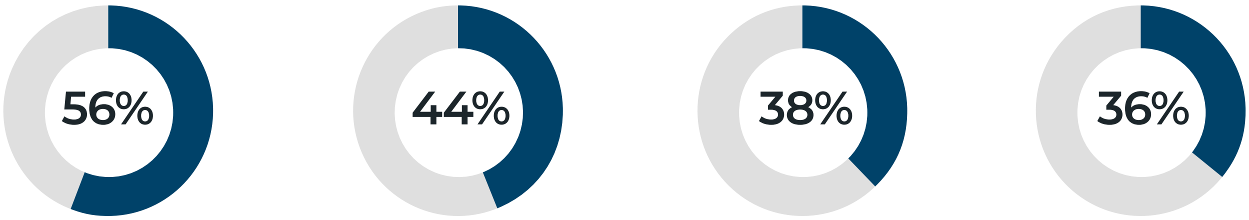
Detected by compromised user 33% | User behavior monitoring 26% | File monitoring 23% | Detected by analyst/security team 21% | Third-party threat intelligence 13% | Detected by a third-party 13% | We cannot detect malware/ransomware 1% | Don't know/other 8%

RESPONDING TO RANSOMWARE

In response to a ransomware attack, organizations are either taking an isolation approach (72%) or proactively shutting down systems (56%) to thwart an ongoing attack.

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

72% Isolate and shut down offending systems and accounts, recover encrypted files from back-ups, and mitigate the initial attack vector if possible



56% Proactively shut down core systems to prevent spread

44% Engage a third-party incident response service

38% Contact cyber insurance provider

36% Contact cybersecurity technology vendor

Immediately call law enforcement 34% | Attempt to decrypt files ourselves 30% | Notify customers 28% | Attempt to negotiate with the attackers 8% | Pay the ransom 4%

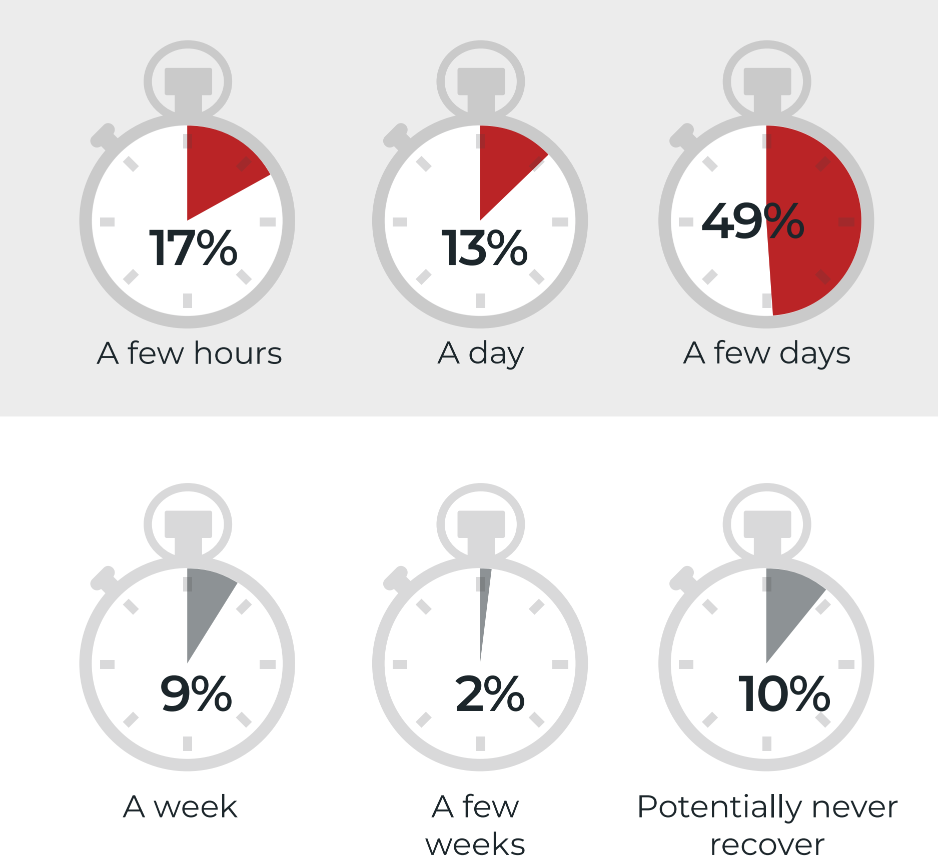
RECOVERING FROM RANSOMWARE ATTACKS

Speed of recovery from an attack is absolutely critical as business costs escalate with every hour the business cannot fully operate. Over 40% of respondents said they are moderately confident in their ability to remediate ransomware after it locks or encrypts data. Nearly half (49%) of respondents believe they can recover from an attack in a few days.

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

49%

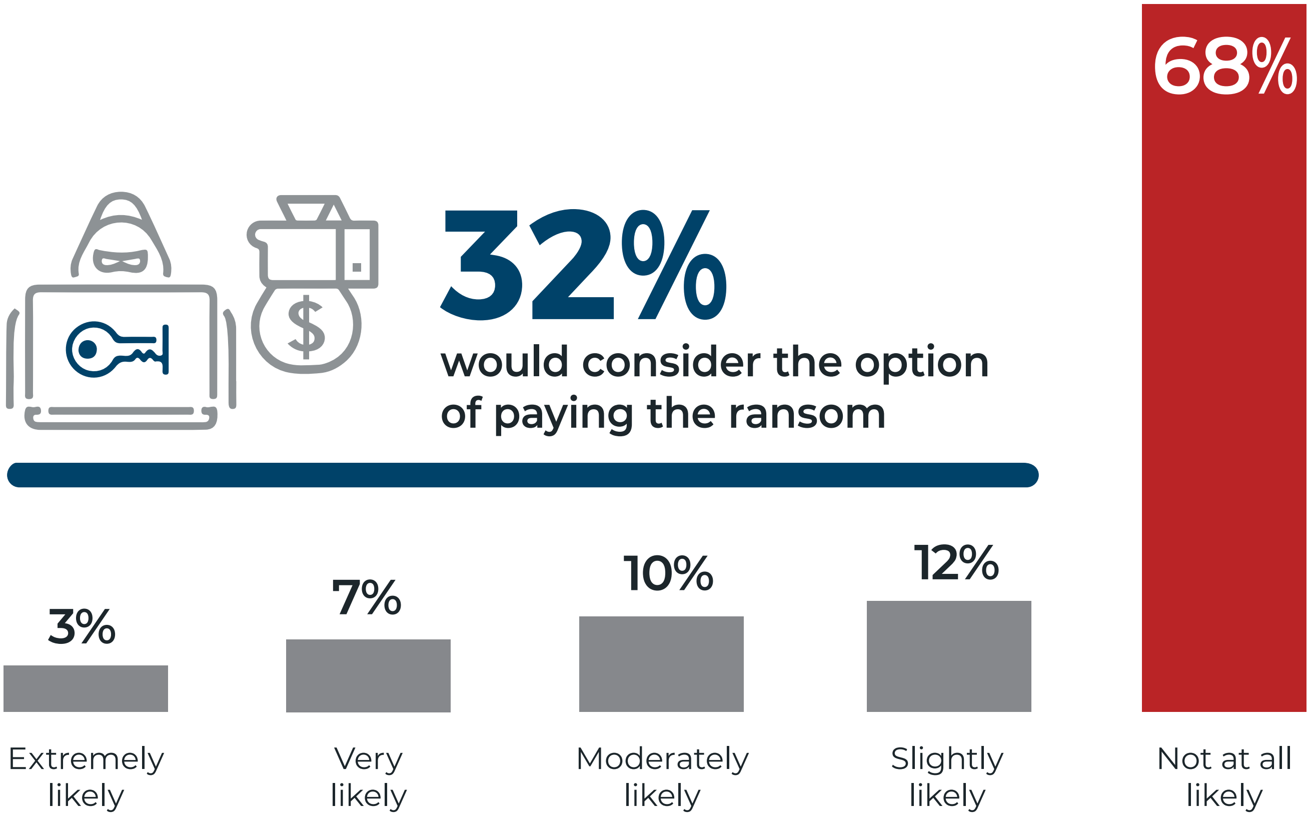
need a few days to recover from a ransomware attack



PAYING RANSOM

The purpose of ransomware is to extract ransom, a payment from the victims of the attack with the implied promise by the cybercriminal of removing the threat. A majority of respondents (68%) say they would not pay the ransom to recover data and systems affected by a ransomware attack. Interestingly, about a third of respondents (32%) would consider the option of paying the ransom.

▶ **How likely is your organization to pay ransom to recover data affected by a ransomware attack?**



PREVENTING RANSOMWARE ATTACKS

We asked organizations how they are currently protecting against ransomware attacks. Over half (55%) of respondents back up critical files and data. About a third (29%) have implemented a zero trust architecture.

How do you currently protect against ransomware attacks?

55%
Back up critical data and assets

29%
Implement a zero trust architecture

7%
Purchase cyber security insurance

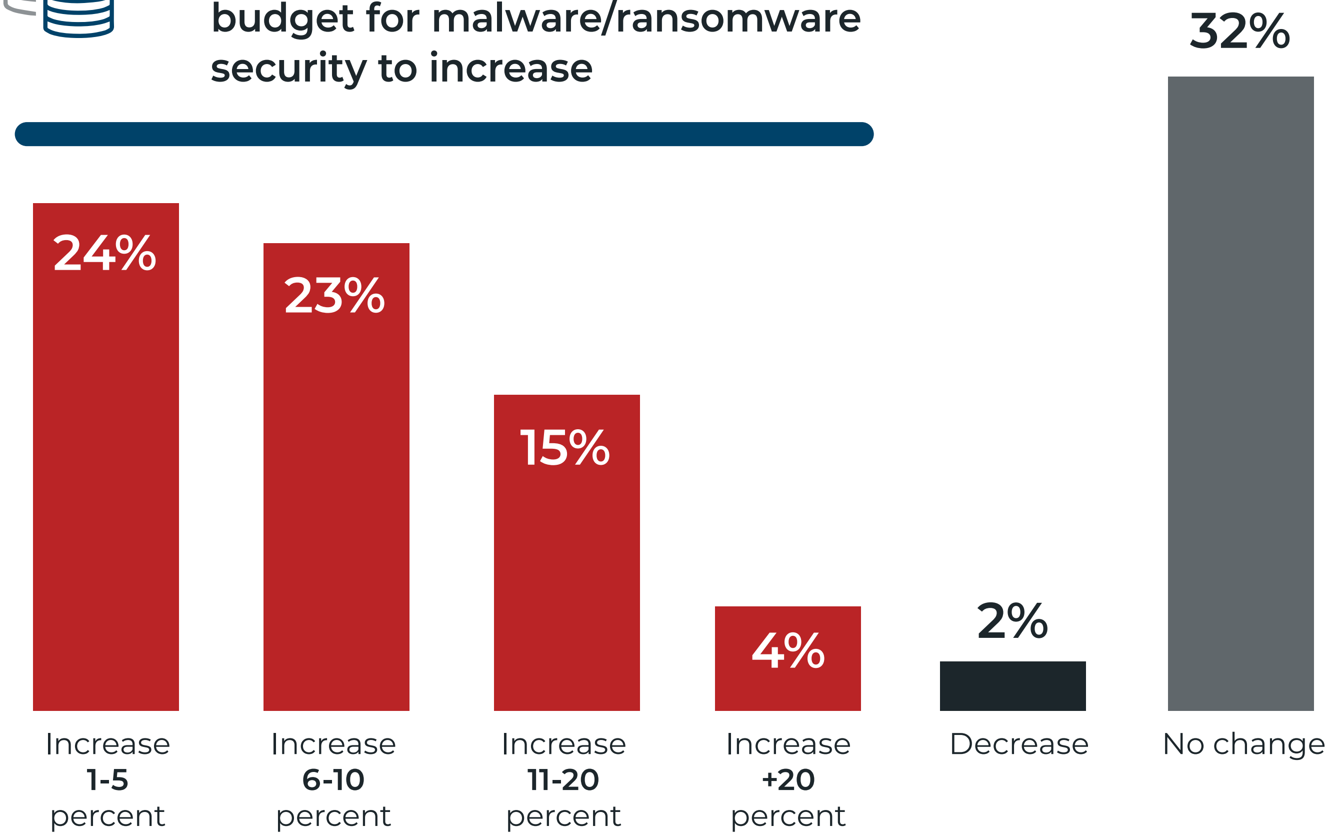
None of the above 9%

BUDGET TREND

When asked about future budgets for malware/ransomware security, a majority of respondents (66%) are expecting minor to moderate increases to their budget.

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

66% expect the organization's budget for malware/ransomware security to increase



CHALLENGES

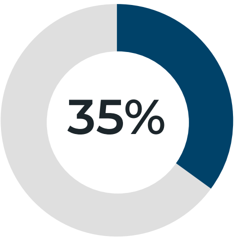
Security teams are facing challenges both internally and externally in their effort to protect IT environments against threats. Most organizations identify the lack of budget (50%), evolving and sophisticated attacks (49%), and growing proliferation of attacks (36%) as the main obstacles to better malware protection.

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

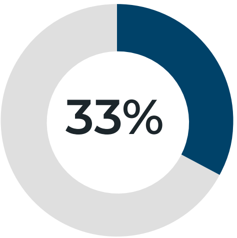
50%
Lack of budget

49%
Evolving sophistication of attacks

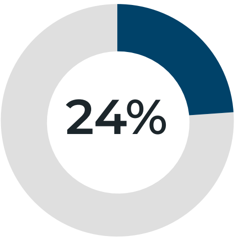
36%
Growing proliferation of attacks



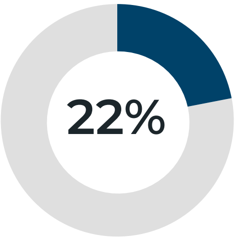
Poor user awareness



Lack of human resources



Uncertainty what security solution to use



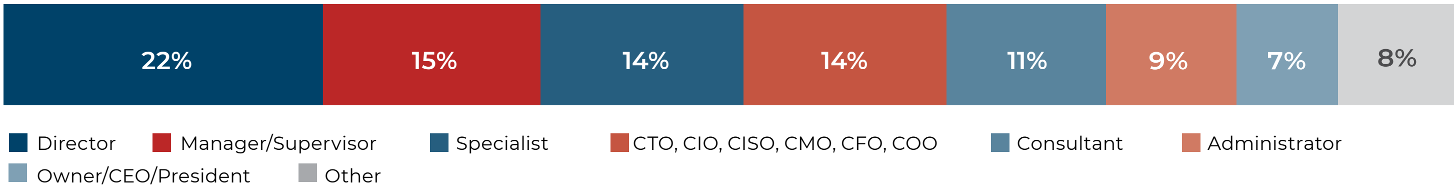
Lack of executive sponsorship

Our partners' lack of preparedness or response 9% | Other 7%

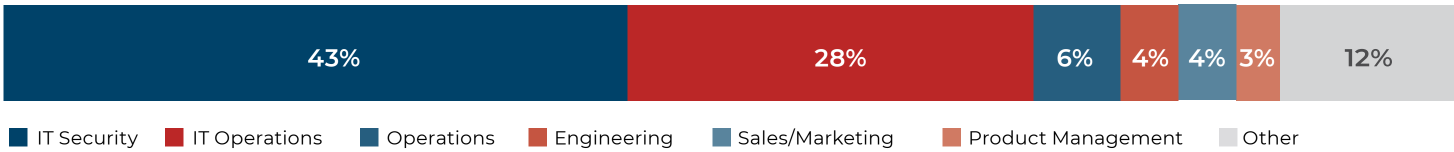
METHODOLOGY & DEMOGRAPHICS

This report is based on the results of a comprehensive online survey of 236 cybersecurity professionals conducted in Fall 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.

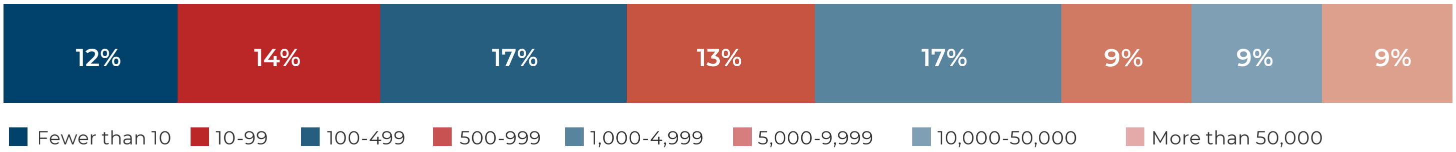
CAREER LEVEL



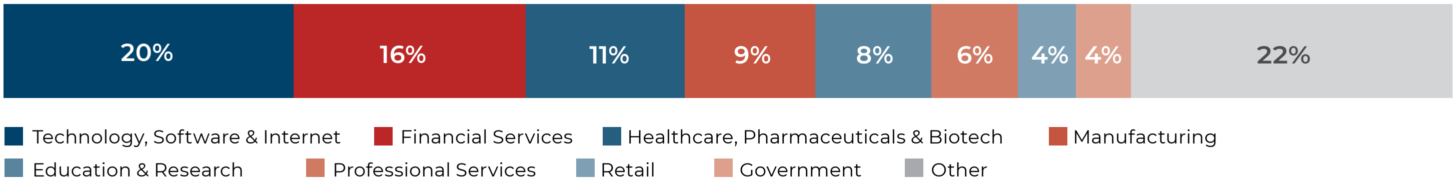
DEPARTMENT



COMPANY SIZE



INDUSTRY



bitglass

A Forcepoint Company

Bitglass, a Forcepoint company, delivers the industry’s only truly integrated cloud-native Secure Service Edge (SSE) platform for securing access to and usage of information as organizations transform to the cloud. The company brings together best-in-class Cloud Access Security Broker (CASB), Secure Web Gateway (SWG), Zero Trust Network Access (ZTNA), and Cloud Security Posture Management (CSPM), combined with Data Loss Prevention (DLP) capabilities to help organizations enable uniform security policies for accessing the web, cloud, and private data centers to be defined and managed through a single console.

The capabilities within Bitglass’ SSE platform complement Forcepoint’s Data-First Secure Access Service Edge (SASE) architecture that dramatically simplify how customers safely and efficiently access, protect and use data anywhere, on any device.