#ARMORU

2020

SOCIAL MEDIA POLL SERIES REPORT

Opinions and experiences regarding
cloud usage and cybersecurity by social media users.

INTRODUCTION:

Armor established the first #ArmorU poll series in 2017 to gain insight into the opinions, challenges, and security posture of social users who are interested in IT, cybersecurity, and cloud computing. This report provides a window into where businesses are on their cloud journey and what security pitfalls keep them up at night. This third iteration of the #ArmorU polls showed that businesses are relying more heavily on cloud providers yet are also concerned about protecting the data they have stored, especially given the current COVID-19 landscape.

METHODOLOGY:

To gather information, Armor conducted an online poll series over a 15-week period, from May to August 2020. The series, which was conducted via Twitter, consisted of 15 questions and was open to all social media users interested in the topics of cybersecurity, cloud, information security, and information technology. All totaled, Armor received more than **42,500** votes to the poll, averaging about 2,834 votes per question. The number of participants has continued to grow each year (starting with only 869 votes in 2017), which should be a consideration when comparing year-over-year results.

KEY TAKEAWAYS:

- **Businesses are worried about the security implications of employees working from home.**
  Nearly 55% of respondents reported that they fear that new vulnerabilities will be likely introduced to their company's public cloud – moderately likely (24%) or very likely (30%). Furthermore, 36% of respondents said they feel their company is not prepared to deal with new security issues brought on by employees working from home.

- **Shared responsibility is still largely misunderstood.**
  While this statistic seems to be improving slightly, many respondents still do not know what shared responsibility means for cloud computing (45% in 2020 compared to 50% in 2017). The percentage of respondents who asserted that this knowledge is part of their company's core strategy has remained largely unchanged over the past four years (23% in 2020 compared 24% in 2017).

- **Confidence in third-party vendors' security posture is shaky.**
  A staggering 46% of respondents reported that they have low confidence in the cybersecurity posture of their third-party vendors. However, it appears that respondents are more confident in their own company's security posture – 38% reporting moderate confidence and nearly 27% reporting high confidence.

- **Companies may have a blind spot when it comes to addressing incidents in the public cloud.**
  Only 28% of respondents reported that their company has an incident response plan for security issues in the public cloud. Of the remaining 72% of respondents, 45% said they do not have one and are not in the process of adopting one either.

CLOUD ADOPTION

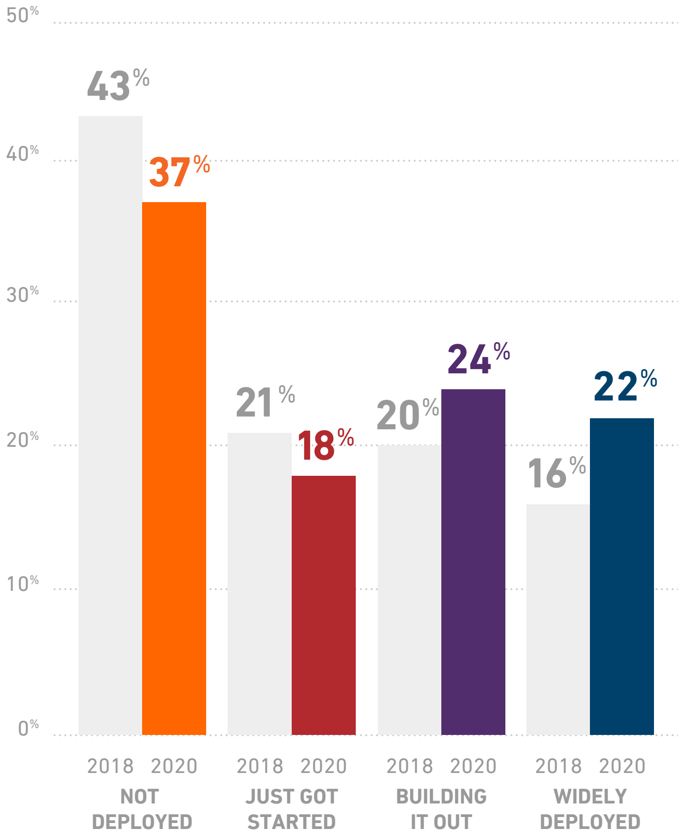
We have seen a significant change in cloud adoption since our first report in 2017, when 58% of participants said they had not yet deployed workloads in the cloud. That number dropped to 43% in 2018 and dropped further to 37% in 2020, a positive sign for the cloud computing industry.

This year, nearly 22% of respondents identified that they have widely deployed a cloud solution for their business environment, up from 16% in both 2017 and 2018. Additionally, about 43% of respondents are in process of adopting cloud usage, with 18% just starting out and about 24% in the process of building out their cloud usage.

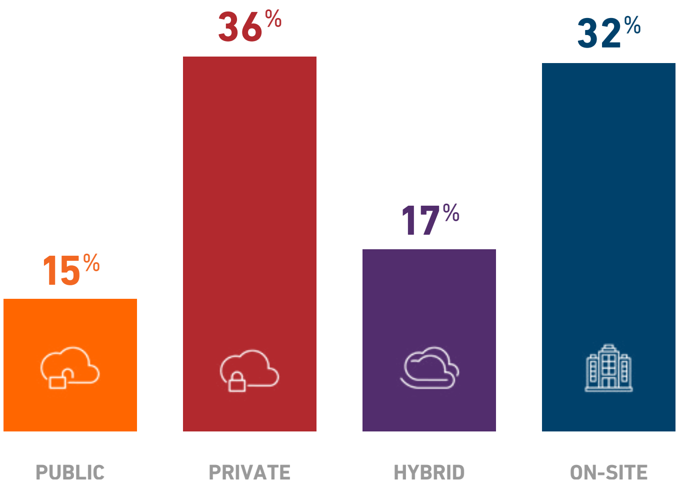
The rising confidence in cloud adoption seems to be contrasted with a growing concern over the security of the cloud environment, as evidenced by a reluctance to place highly sensitive data onto the cloud. This year 32% of respondents said their company stores its most highly sensitive data on-site, a significant increase from 26% just two years ago. On the other hand, the percentage of respondents whose companies are planning to move highly sensitive data onto the cloud within the next two years has dropped from 41% in 2018 to 25% in 2020.

While cloud usage is increasing, it seems to be more frequently utilized for not sensitive (46%) and moderately sensitive data (29%).

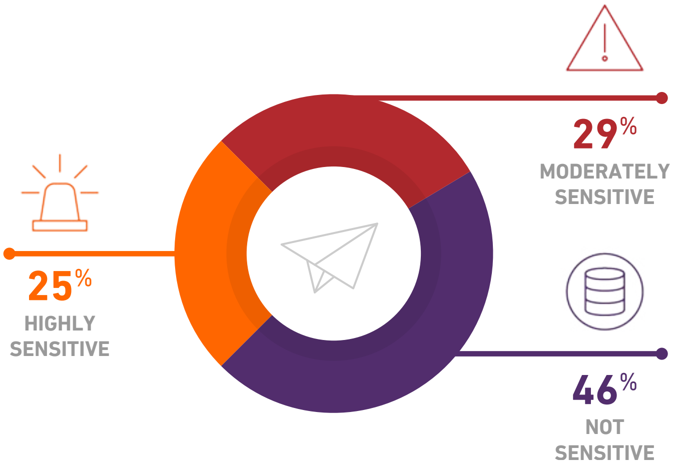
WHERE ON THE CLOUD MATURITY MODEL DOES YOUR BUSINESS CURRENTLY RESIDE?



WHERE DOES YOUR COMPANY STORE ITS MOST SENSITIVE DATA?



WHAT TYPE OF DATA ARE YOU PLANNING ON MOVING TO THE CLOUD IN THE NEXT 2 YEARS?

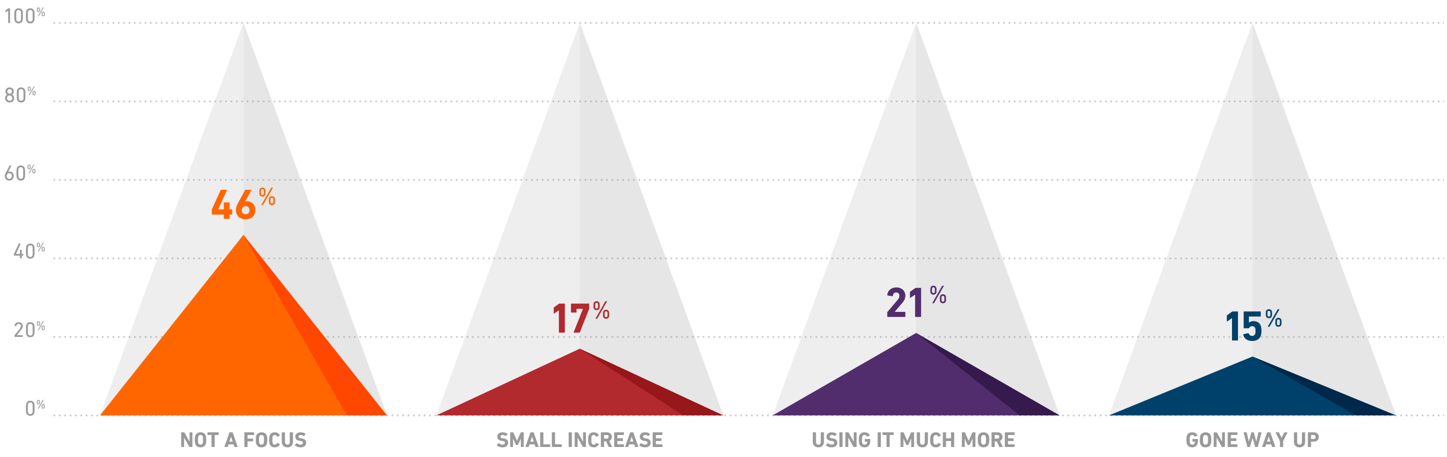


CYBERSECURITY IN THE NEW COVID-19 LANDSCAPE

COVID-19 has brought many operational challenges and changes to businesses. More than half of respondents (54%) reported that their company has increased its reliance on the cloud. Twenty-one percent of respondents reported using the cloud more frequently while 15% said their cloud usage has gone way up.

This may be partially due to many traditional brick-and-mortar businesses that have had to bolster their online presence and virtual offerings given mandated health restrictions. Also, companies across the board have become more reliant on using software-as-a-service, such as collaboration tools, video conferencing, team sharing, and many others to ensure their businesses can continue to operate, while their physical locations are inaccessible.

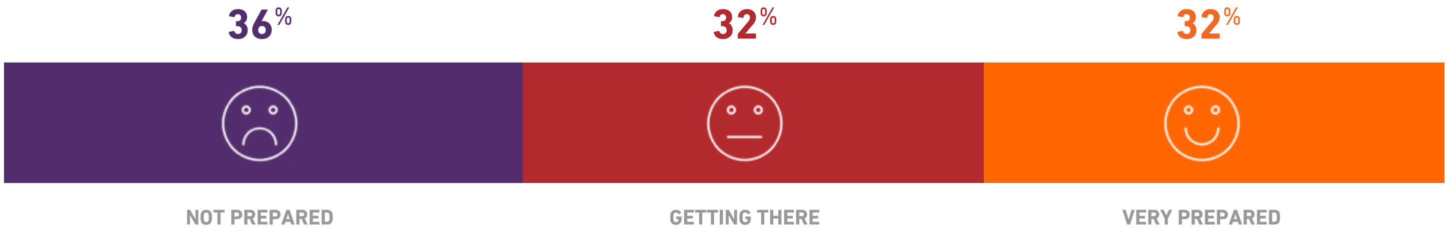
HOW RELIANT ARE YOU ON CLOUD WORKLOADS WITH THE RECENT COVID-19 EVENTS?



However, with many employees working remote to prevent the spread of the virus, companies are worried about the security implications. Nearly 55% of respondents reported they fear that new vulnerabilities being introduced to their company's public cloud are now either moderately likely (24%) or very likely (30%). What's more, nearly 10% of respondents said they actually experienced a cloud security issue due to the new work-from-home environment.

Furthermore, more than one-third of respondents (36%) reported that they feel their company is not prepared to deal with new security issues brought on by a remote workforce. Only 32% of respondents said that their company was "very prepared" and the remaining 32% said that their company is "getting there."

IS YOUR COMPANY PREPARED TO DEAL WITH NEW SECURITY ISSUES BROUGHT ON BY EMPLOYEES WORKING FROM HOME?



FACTORS CONTRIBUTING TO VULNERABILITIES

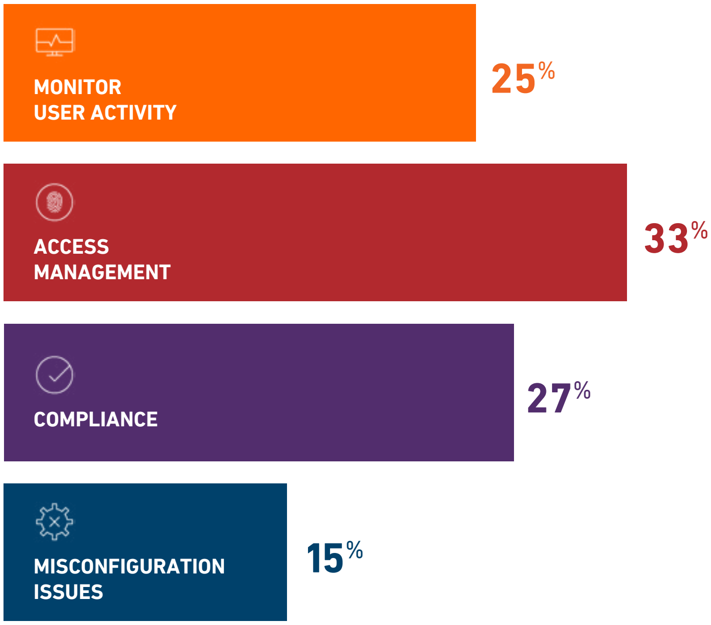
- The use of the open internet for data sharing.
- Employees using personal computers for work.
- Employers loosening some of their cybersecurity policies to ensure employees have access to the corporate network.
- Increase in phishing attacks in the form of news about COVID-19 and impersonating trusted conferencing platforms.
- Employees not using the same rigorous compliance practices that they would employ at work.

CLOUD SECURITY CONCERNS

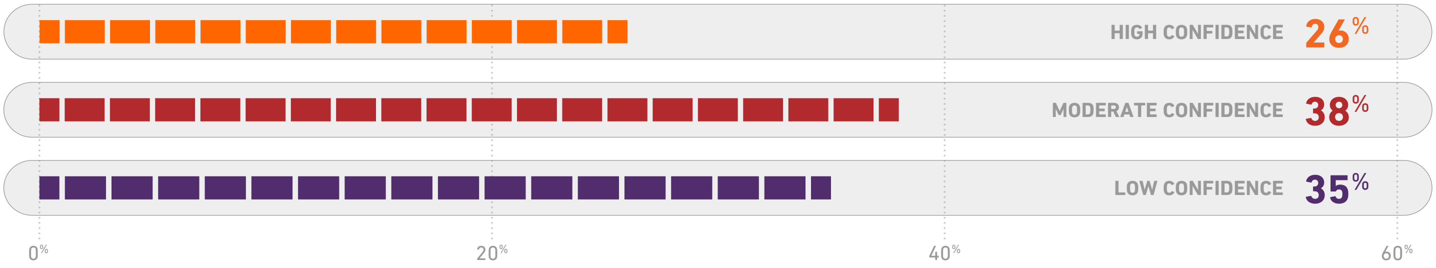
Digging deeper, respondents reported that their biggest cloud-related security concern this year was access management. In transitioning to a work-from-home model, companies quickly implemented changes overnight to accommodate health guidelines, which meant granting nearly all employees VPN and remote access to the company network. Many vulnerabilities may have been introduced in this process as companies have had to quickly accommodate to address and ensure their employees continue to be productive. Also, in their haste, companies might have overlooked compliance requirements applicable to their respective verticals.

This concern underscores a larger concern for businesses' security posture overall. Seventy-three percent of respondents admitted having either moderate confidence (38%) or low confidence (35%) in their cybersecurity posture, a statistic that has only slightly improved from two years ago.

WHAT'S THE MOST IMPORTANT SECURITY CONCERN FOR YOUR CLOUD ENVIRONMENT?



ARE YOU CONFIDENT IN YOUR BUSINESS'S CYBERSECURITY POSTURE?



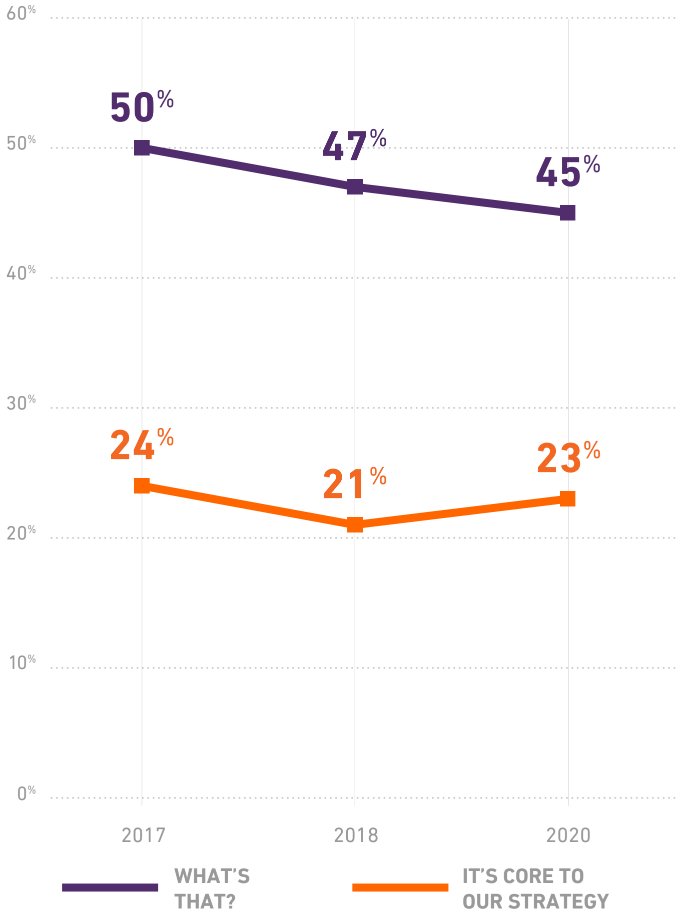
Despite these very real concerns, many organizations remain confused about the concept of shared responsibility. Shared responsibility refers to the mutual ownership of security by the cloud provider and the customer. What responsibility each side has depends on the service model being used.

While this statistic seems to be improving slightly, many respondents still do not understand what shared responsibility means for cloud computing (45% in 2020 compared to 50% in 2017). Furthermore, the percentage of respondents who asserted that this knowledge is part of their company's core strategy has remained largely unchanged over the past four years (23% in 2020 versus 21% in 2018 and 24% in 2017).

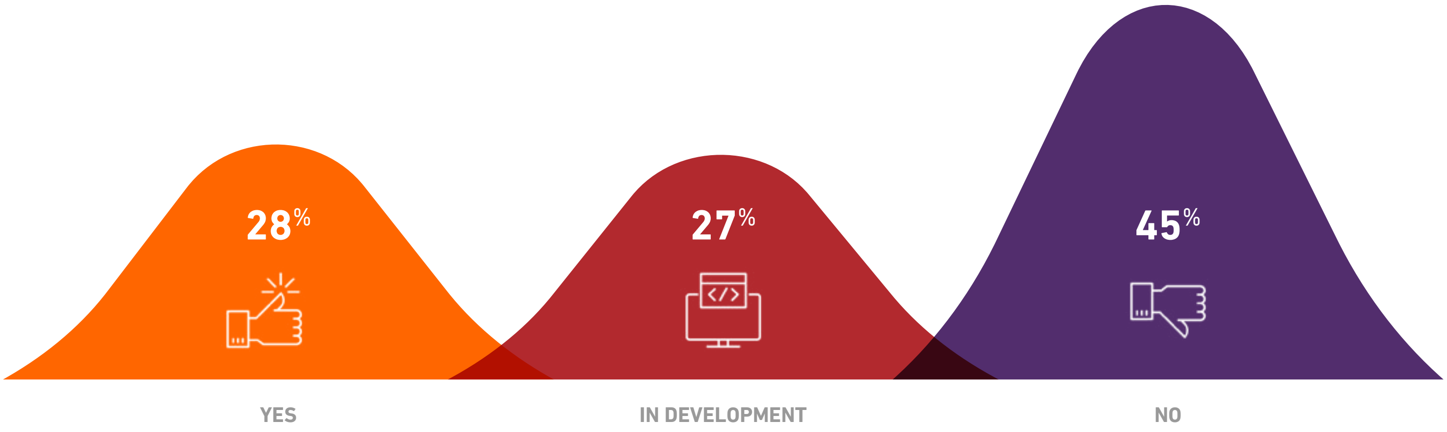
Companies may also have a blind spot when it comes to addressing incidents in the public cloud. Only 28% of respondents reported that their company has an incident response plan for security issues in the public cloud. Of the remaining 72% of respondents, 45% said they do not have one and are not in the process of adopting one either. This is another troubling fact that underscores the misunderstanding of the shared responsibility model.

Since the poll did not separate respondents according to the size of their business or cloud maturity, it is possible this represents a disproportionate amount of small businesses still struggling with the security implications of cloud adoption. The worst-case scenario, however, is that businesses are moving too quickly and adopting cloud solutions without fully understanding the role they need to play in securely configuring their cloud environment.

WHEN MANAGING THE SECURITY OF YOUR PUBLIC CLOUD, HOW WELL DOES YOUR BUSINESS UNDERSTAND THE SHARED RESPONSIBILITY MODEL?



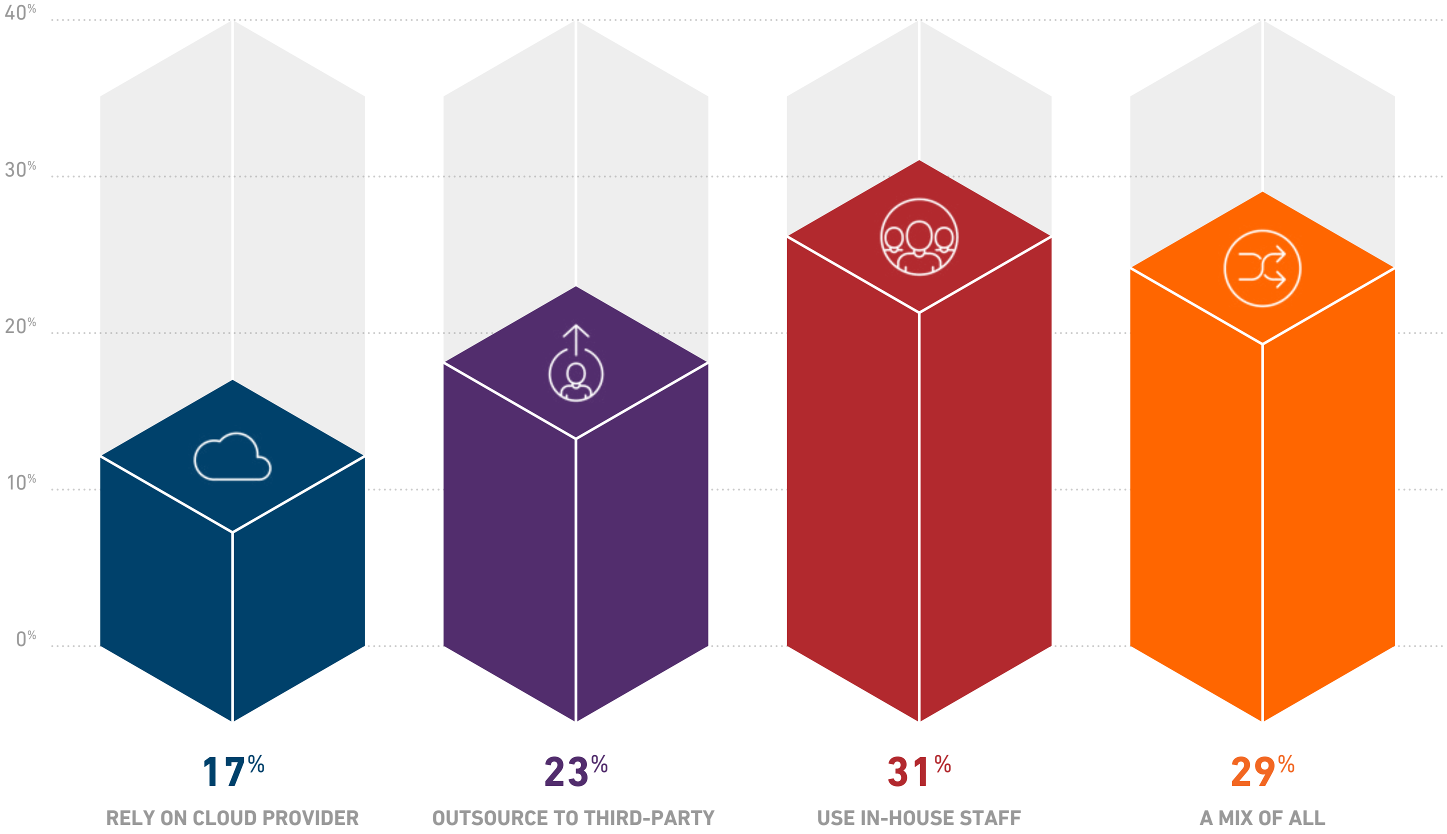
DOES YOUR INCIDENT RESPONSE PLAN ADDRESS YOUR WORKLOADS IN THE PUBLIC CLOUD?



WORKING WITH THIRD-PARTY VENDORS

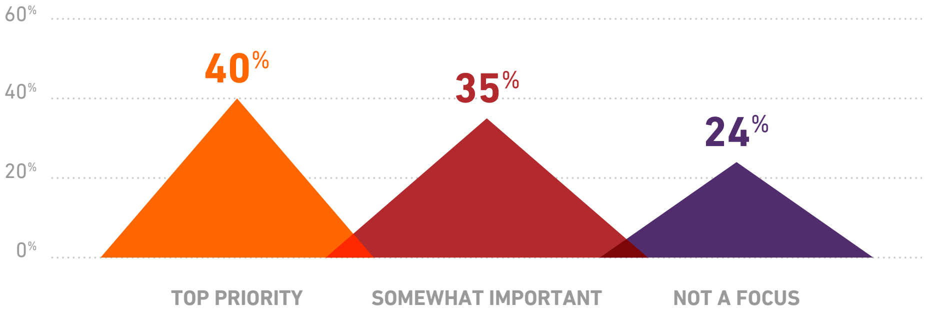
Given the complexity of cybersecurity, many companies take different approaches to managing their cloud security, with less than one-third saying they keep it in house. Other options include outsourcing their security needs to a third-party vendor, relying solely on the protection of a public cloud provider, or a mix of any of these options.

WHICH BEST DESCRIBES YOUR ORGANIZATION'S APPROACH TO MANAGING CLOUD CYBERSECURITY?



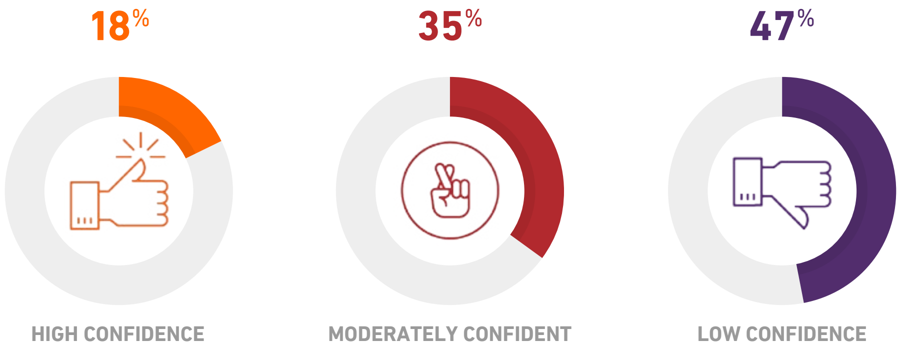
Companies that decide to outsource their cloud security have a number of factors to consider when choosing a vendor. According to our poll, 40% of respondents identified incident response as the top priority during the selection process. This underscores the fact that while detection and prevention are extremely important, being able to contain and respond to a realized threat is critical.

WHEN CHOOSING A CYBERSECURITY VENDOR, WHERE DOES INCIDENT RESPONSE RANK?



However, despite the fact that such a great emphasis is placed on incident response and that more than half of respondents utilize third-party providers for some or all of their cloud security needs, confidence in these vendors is shaky. A staggering 47% of respondents reported that they have low confidence in the cybersecurity posture of their third-party vendors.

HOW CONFIDENT ARE YOU IN THE CYBERSECURITY POSTURE OF YOUR THIRD-PARTY VENDORS?



CONCLUSION

Businesses are facing more challenges and threats than ever before. The global pandemic has forced organizations to adapt quickly and, in many cases, implement massive policy changes overnight that have significant security implications. While businesses are beginning to rely more heavily on the cloud, companies have expressed deep concern that neither they nor their security vendors are providing the full protection and incident response plans that they need to secure their most sensitive data. As cloud adoption continues, businesses should focus on finding robust solutions that provide the full range of threat detection and response capabilities, so they can focus on the work of growing their business.

ARMOR

ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167