2018
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 around the world. The report did not disappoint and provided a window into where businesses were on their cloud journey and what security pitfalls kept them up at night.

This year, Armor fielded thousands of responses, which taken together, painted a picture of a corporate environment where organizations feel ready to put highly sensitive data into the cloud, yet challenges remain. Despite their willingness to embrace cloud computing, there is an air of skepticism about their organizations' security postures.

What is clear is that companies want to reduce the cost of managing security—but not at the price of sacrificing compliance, visibility, and incident response.

METHODOLOGY:

To gather information, Armor conducted an online poll series over a 13-week period, from May to August 2018. The series, which was conducted via Twitter, consisted of 13 questions and was open to all social media users interested in the topics of cybersecurity, cloud computing, information security, and information technology. All totaled, Armor received more than 37,000 votes, averaging about 2,859 votes per question. The number of participants is significantly higher than last year's poll (a total of 869 votes), which should be considered when making direct comparisons.

KEY TAKEAWAYS:

Companies are comfortable with the cloud. Forty-six percent of respondents said they store sensitive data in private clouds, and 41% are planning to move their most sensitive information to a cloud during the next two years.

Shared responsibility is still misunderstood. Compared to the 2017 report, there has been virtually no change in the percentages of respondents who do not know what shared responsibility is (50% in 2017 vs. 47% in 2018) and those that define it as part of their core strategy (24% in 2017 vs. 21% in 2018).

Organizations want to reduce the cost of security. Just like last year, managing security costs is top-of-mind for poll participants. However, organizations also want to balance that with the need for user monitoring, access management, and configuration management. Choosing a third-party vendor that can offer a portfolio with an integrated set of these capabilities may provide significant cost savings for businesses.

Overall, cybersecurity confidence is not particularly high. Seventy-four percent of respondents admitted having either moderate (34%) or low confidence (40%) in their cybersecurity posture. When asked about the maturity of their threat remediation process, 46% said it is not a focus.

Incident response capabilities will influence adoption of cloud services. Forty-one percent of respondents called the availability and integration of incident response services into vendors' overall solutions a top priority when choosing a third-party vendor.

CLOUD ADOPTION

We saw a significant change in cloud adoption since our first report, when 58% of participants said they had not yet deployed workloads in the cloud. As shown in Figure 1, that number dropped down to 43% in this year's poll.

When asked how they classified their cloud maturity, more than a third identified themselves as either beginner (20%) or focused (16%) users. This represents a marked increase from 2017, when just 8% of respondents placed themselves in the beginner category. Other research has captured this growth as well. In RightScale's seventh annual 2018 State of the Cloud Report, researchers found that 71% of respondents from the enterprise segment (companies with more than 1,000 employees) said their organizations plan to increase spending on public cloud solutions by more than 20%. In addition, respondents in the RightScale survey said they are running applications in roughly three clouds on average and are experimenting with approximately two more.

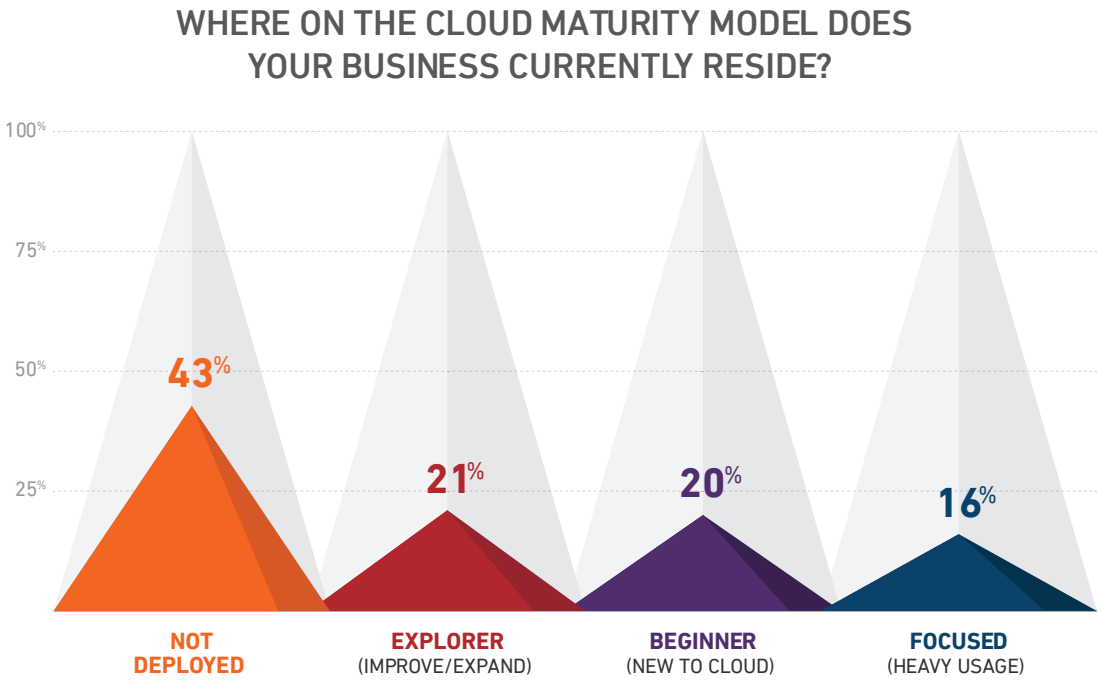


FIGURE 1

The growing confidence in cloud computing is also reflected in the willingness of companies to place their most sensitive data in a cloud. Forty-six percent of respondents said they store their most sensitive data in a private cloud environment, compared with 26% who said they stored the information on-site. Meanwhile, 14% said they stored it in public clouds, and another 14% said they stored it in hybrid environments.

This increased willingness to put sensitive data in hybrid or public cloud environments means organizations will have to adopt security solutions that enable unified visibility and management across different architectures.

WHICH BEST DESCRIBES THE TYPE OF DATA SENSITIVITY YOU INTEND TO MOVE TO A PUBLIC, HYBRID AND/OR PRIVATE CLOUD IN THE NEXT TWO YEARS?

41%
HIGH
CUSTOMER DATA

33%
MEDIUM
MARKETING PLANS

26%
LOW
PUBLICLY AVAILABLE

WHERE DO YOU STORE YOUR MOST SENSITIVE DATA?

14%
PUBLIC CLOUD

46%
PRIVATE CLOUD

14%
HYBRID ENVIRONMENT

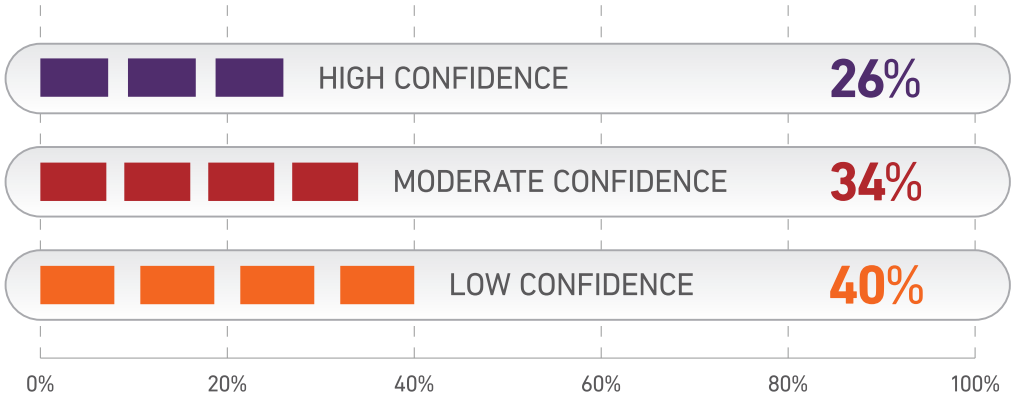
26%
ON-SITE

CLOUD SECURITY CONCERNS

Digging deeper, respondents reported that their biggest cloud-related security concern was monitoring user activity. This demonstrates a clear concern with insider threats and is an acknowledgement that keeping track of user activity not only has an impact on compliance, but also provides more challenges for security teams as they seek to identify anomalous behavior that can be easily disguised as legitimate. The strong interest in access management and configuration issues underscores an awareness that activities like account hijacking and inadvertent data leaks caused by misconfiguration pose serious security risks. In fact, Gartner has predicted that by 2020, 95% of cloud data breaches will be the result of internal client errors, not that of their security vendors.

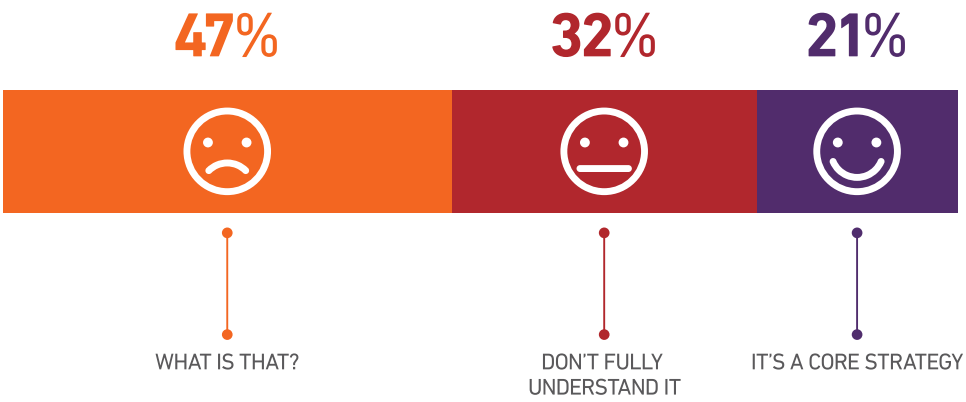
WHAT IS THE BIGGEST SECURITY CONCERN RELATED TO YOUR CLOUD ENVIRONMENT?

HOW CONFIDENT ARE YOU IN YOUR BUSINESS' CURRENT CYBERSECURITY POSTURE?



The focus on security comes with surprising levels of uncertainty. Seventy-four percent of respondents admitted having either moderate confidence (34%) or low confidence (40%) in their cybersecurity posture.

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



Despite the widespread availability of information on best practices for cloud security, many organizations remain confused about the concept of shared responsibility. The shared responsibility model outlines the security obligations of the cloud provider and the client. The responsibilites that lie with each party depend on the service model being used.

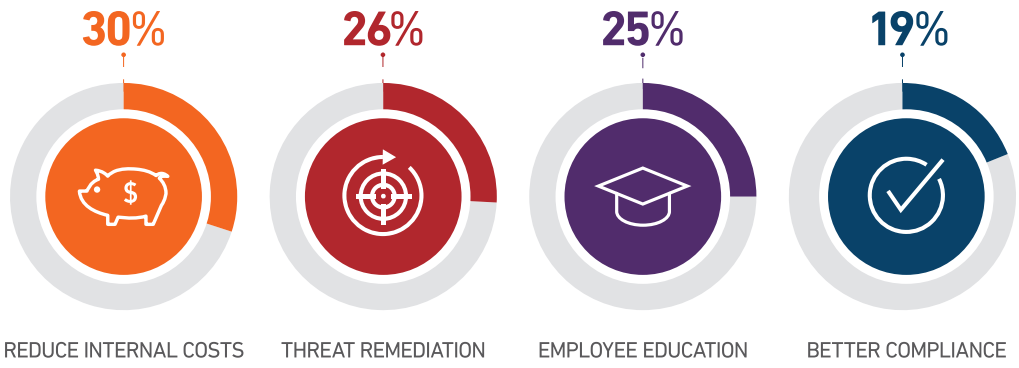
We found that there has been virtually no change in the percentage of individuals who understand the shared responsibility model, or who consider it part of their strategy. Fifty percent reported in 2017 that they don't know what the model is vs. 47% in 2018, while conversely 24% in 2017 state it's part of their core strategy vs. 21% in 2018.

Since the poll cannot 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 their responsibility in securely configuring their cloud environment.

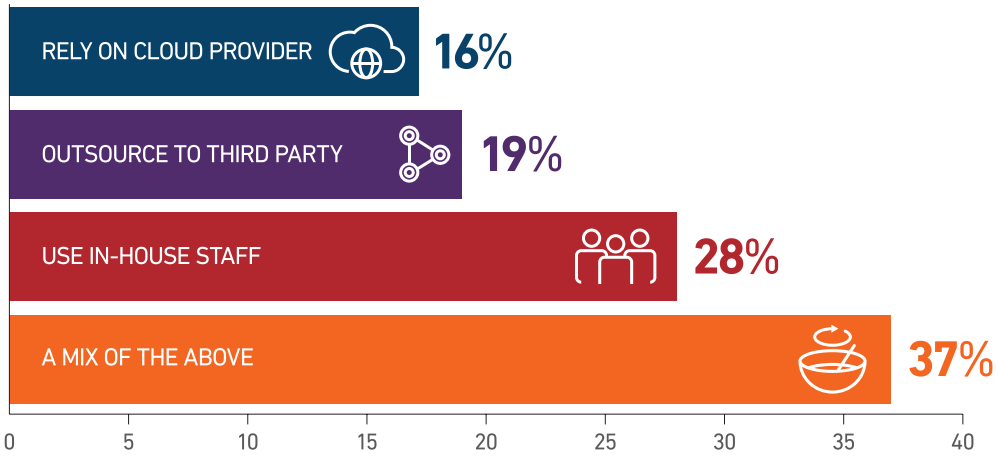
ANSWERING THE CALL FOR SECURITY

With all these challenges before them, respondents still put reducing cost as priority No. 1 when it comes to enhancing their cybersecurity program. This is in line with last year's poll, in which participants cited managing cost as the main challenge of securing cloud environments. The pressure to secure environments cheaply, without compromising compliance efforts, has become a key market driver for cloud service providers.

WHAT ARE YOU LOOKING TO ENHANCE MOST IN YOUR CYBERSECURITY PROGRAM THIS YEAR?



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

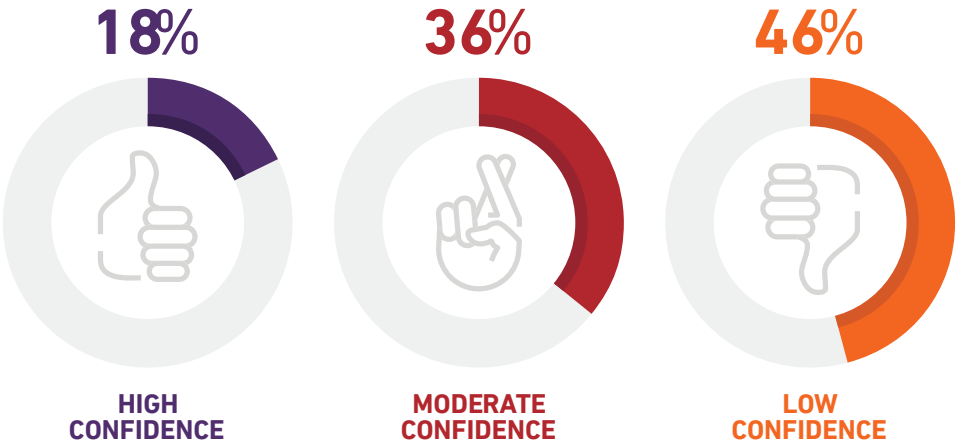


According to a study by Grand View Research, the global market for cloud managed services is projected to grow to $82.51 billion by 2025, and adoption is expected to help enterprises reduce costs and improve productivity. As the #ArmorU poll shows, many organizations are reaching out to third parties or relying on their cloud providers to manage cloud security.

Third-party providers have often relied on their ability to offer secure, less expensive alternatives to handling security in-house. However, the poll demonstrates there is skepticism in the market regarding the security posture of third-party vendors as well. Choosing the right partner requires extensive due diligence. Before selecting a provider, organizations should:

- Check for security certifications from organizations such as the Cloud Security Alliance and (ISC)2
- Understand where their data will reside and any resulting compliance implications
- Assess what security controls the service provider offers, and what gaps, if any, exist
- Examine the vendor's incident response plan.

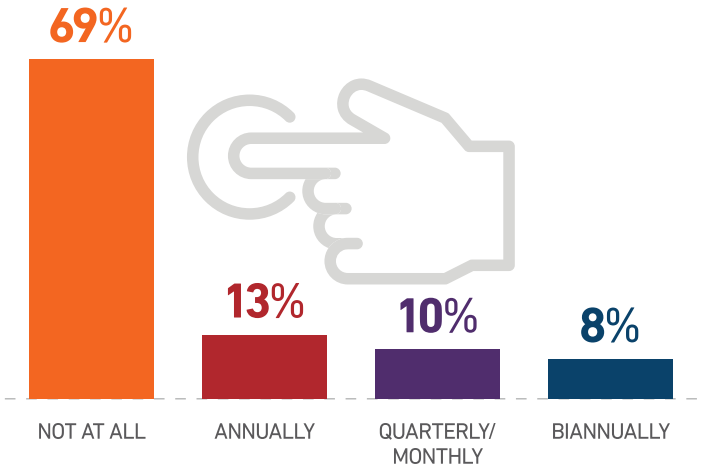
HOW CONFIDENT ARE YOU IN THE CYBERSECURITY POSTURE OF YOUR THIRD-PARTY VENDORS?



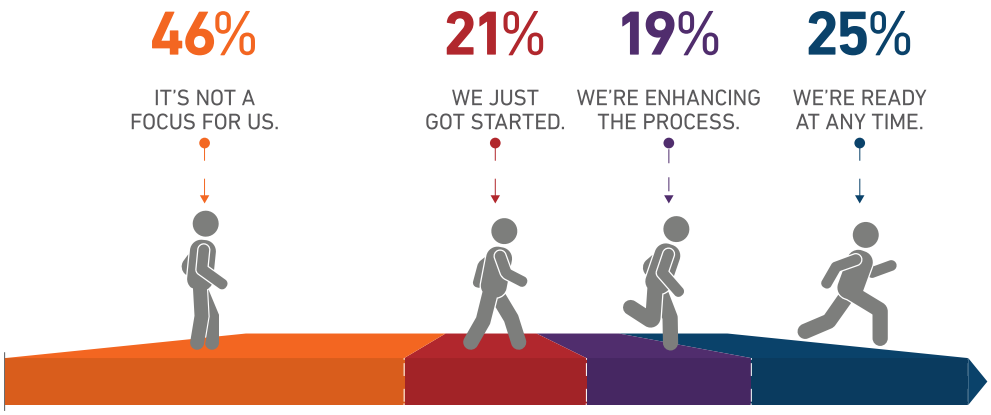
Many respondents expressed little confidence in their organization's threat remediation abilities. Nearly 70% of respondents said they do not test their incident response plan at all. This is potentially a critical blind spot, as reducing dwell time shortens the period in which attackers can steal data or damage a compromised environment. The faster an attack can be identified, quarantined, and eradicated, the sooner businesses can resume normal operations.

When asked about the maturity of their threat remediation process, 46% said it is not a focus. However, the good news is that 41% cited incident response as a top priority when choosing a third-party vendor, meaning that having a provider that can offer that capability will be of growing importance to enterprises.

HOW FREQUENTLY DO YOU TEST YOUR CYBERSECURITY INCIDENT RESPONSE PLAN?



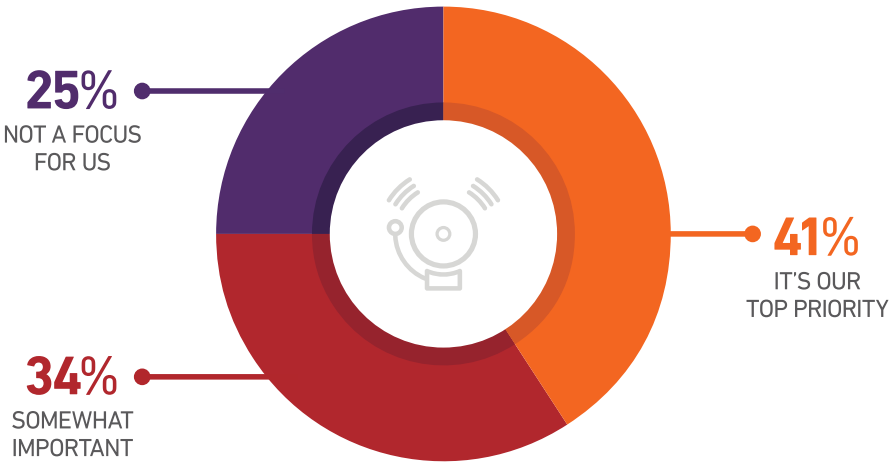
HOW MATURE IS YOUR THREAT REMEDIATION PROCESS?



According to Ponemon Institute's 2018 Cost of a Data Breach Study: Global Overview, companies that contained a breach in under 30 days saved $1 million compared with those who took longer. The lack of focus on threat remediation and testing their own incident response capabilities indicates businesses are looking to vendors to provide this service. This is further supported by the continued growth

of managed detection and response (MDR) solutions and the increasing number of managed security service providers (MSSPs) offering MDR capabilities. As cloud adoption increases, it is likely the subject of incident response will take its place alongside user monitoring, access control, and compliance as a key component of what prospective customers need in their cybersecurity program.

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



CONCLUSION

As businesses move forward on their digital journey, protecting their systems and data should stay front and center. As cloud adoption continues, businesses of all sizes should focus on finding solutions that empower them to transform their business without sacrificing security, compliance, and availability.

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