As Cloud Adoption Surges, Can Security Keep Pace?

Security teams struggle amid the rapid shift to cloud-based operations

May 2022

Sponsored by BISHOPFOX
As Cloud Adoption Surges, Can Security Keep Pace?

RESULTS OF AN APRIL 2022 CYBERRISK ALLIANCE BUSINESS INTELLIGENCE STUDY

BACKGROUND

It’s hard to believe, but Amazon initiated the modern cloud computing era in 2002 when it created its Amazon Web Services subsidiary. And it wasn’t until 2006 that Amazon introduced Simple Storage Service and Elastic Compute Cloud, and most enterprises considered such offerings an interesting novelty back then. Today, cloud computing is everywhere. Yet, many organizations still find themselves grappling with how to deploy, manage, and secure their cloud systems.

Because of its perceived lower costs, greater agility and ability to increase computing power with increased demand; and the ability to continuously deploy new applications and software features, use of the cloud is expected to keep growing. Cloud investments are driven by the need to fuel digital transformation efforts. The research firm IDC expects more than half of the global economy will be based on, or at least influenced by, digital transformation investments this year, accounting for 55% of all information and communication investments within the next two years. That growth has also been fueled in the last two years by the Coronavirus pandemic, which forced companies to pivot operations to the cloud to accommodate remote work.

With cloud use on the rise, criminals and other threat actors have shifted their tactics to cloud data and systems. If organizations are going to successfully adopt cloud or continue their transition, they must ensure security is part of their program.
The CRA Business Intelligence “Cloud Security Survey” (April 2022) shows just how difficult that is for many organizations, especially when it comes to staff and security technology maturity. As one security executive put it:

“Services are being adopted that require multi-cloud support. The platforms differ greatly and are causing a strain on internal expertise, while reliable and knowledgeable external consultants are also difficult to find at reasonable costs.”

RESEARCH METHODOLOGY

The data and insights in this report are based on an online survey conducted by CRA Business Intelligence in April 2022 among 303 security leaders and practitioners in the U.S.

Specific roles included:

- Chief Security Officers/CIOs/CTOs (10%)
- VPs, SVPs, and EVPs of IT/IT security/audit, risk and compliance (7%)
- Directors of IT, IT security, and audit, risk, compliance (55%)
- Managers of IT, IT security, and audit, risk, compliance (24%)
- IT or IT security administrators (2%)
- Analysts, consultants or equivalent (2%)

Organizational size:

- Small (1–99): 5%
- Medium (100–999): 18%
- Large (1,000–1,999): 66%
- Enterprise (10,000 or more): 11%

Study participants worked primarily in the following industries:

- High-tech/IT (32%)
- Retail or e-commerce (20%)
- Manufacturing (10%)
- Financial services and insurance (9%)
- Business or professional services (5%)
- Healthcare (8%)
- Education, transportation, government, non-profits, media, energy, and utilities (16%)
EXECUTIVE SUMMARY

This survey makes it clear that the majority of organizations know that cloud will comprise the majority of their business-technology systems, but they're not quite sure what that looks like yet. And while many organizations are a decade into getting their feet wet with cloud, they aren't quite sure how to manage and secure these systems. Even as some organizations have learned how to flex their “cloud-first” muscles, others are still simply lifting and shifting their current applications to the cloud with no, or very little, customization. When it comes to security, the majority of respondents cite similar concerns.

The federal government grew more concerned about cloud security last year, too. In December, the Senate Homeland Security and Government Affairs committee passed a version of the Federal Secure Cloud and Jobs Improvement Act, which (if passed) would help improve FedRAMP (the Federal Risk and Authorization Management Program) security. FedRAMP itself aims to provide a standardized way to assess and continuously monitor cloud systems used by federal agencies. For its part, the executive branch issued an executive order designed to help improve the nation’s overall security posture, including software supply chain and threat sharing among the government and private sector.

This study highlights the current struggle faced by many organizations: cloud computing is the future, yet the tools, processes, and even internal skillsets aren’t quite in place yet when it comes to successfully securing the cloud. The survey also finds that most organizations plan to increase their budgets and cloud security spending, but time will tell how well these anticipated investments pay off in reduced risk.

Among the survey’s key findings:

- Thirty-seven percent of respondents reported their organization experienced one or more cloud-based attacks or breaches in the last two years. On average, victims experienced an average of four cloud-based attacks since 2020.
- The number of cloud assets/workloads is growing among companies, with 55% of respondents running up to 50 assets/workloads in the public cloud and 56% putting up to 50 assets on hosted clouds, or about an average of 66 assets in either public or hosted clouds.
- As cloud-based assets/workloads increase, 50% of respondents are very concerned about their ability to secure their cloud systems, with 72% “extremely” or “very” concerned.
When it comes to the top data security concerns in the cloud, respondents cite the following: Lack of detection/response, compromised users, misconfiguration, and inability to monitor changes within cloud environments.

Overall, how concerned are you about securing your cloud assets/workloads over the next 12 months?

<table>
<thead>
<tr>
<th>Concern Level</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all concerned</td>
<td>1%</td>
</tr>
<tr>
<td>A little concerned</td>
<td>7%</td>
</tr>
<tr>
<td>Moderately concerned</td>
<td>21%</td>
</tr>
<tr>
<td>Very concerned</td>
<td>50%</td>
</tr>
<tr>
<td>Extremely concerned</td>
<td>22%</td>
</tr>
</tbody>
</table>

Note: May not sum to 100% due to rounding.

GROWING CLOUDS, GROWING ATTACKS

As cloud use accelerates, not even companies with robust security protocols are immune from attacks.

Recent breaches occurred at organizations that should have the resources to avoid such incidents, including Accenture being hit as a result of unsecured AWS storage, as well as a LockBit ransomware attack that purportedly resulted in 6TB of stolen data. In 2017, telecommunications giant Verizon fell victim to a cloud breach that lead to system infiltrations. The list goes on.

Overall, organizations are running, on average, about 66 cloud assets or workloads in either public or hosted clouds. The bifurcation and the move to hybrid environments is appropriate for organizations moving stable, more predictable workloads to hosted clouds, while workloads in the public cloud are ideal for those that may have unpredictably large bursts, such as spikes in customer demand.
As Cloud Adoption Surges, Can Security Keep Pace?

Security concerns such as lack of detection and response capabilities in the cloud and exposure due to compromised users with cloud access stem from an overall perception of lack of maturity in cloud security tools and organizational ability to respond.

What are your top three security concerns about data stored in your cloud environment(s)?

Please select up to three choices.

- Lack of detection and response capabilities in the cloud: 53%
- Exposure due to compromised user with access to the cloud: 46%
- Inadvertent exposure due to misconfiguration: 45%
- Inability to monitor changes within our cloud environment(s): 41%
- Lack of prevention capabilities within cloud-native services: 39%
- Exposure due to malicious insider with access to the cloud: 37%

Note: May not sum to 100% due to rounding.
While concerns about malicious insiders are top of mind among many — and there is reason to be vigilant — most cloud data breaches continue to stem from careless users, according to security researchers at Group-IB’s Attack Surface Management team, who managed to find 165,600 exposed databases (see The number of public-facing databases increased 16% in the second half of 2021, SC Media).

In Their Own Words

Several survey respondents recounted their experiences with cloud attacks at their organizations:

“While we discovered that no data was leaked, our data sources were infiltrated, and malicious agents did have to be removed and cleaned from the system. Infiltration began with links that were opened up in phishing emails.”

“The infiltration was due to an exploit contained in an email that was opened by one of our employees and that, due to the innocence of said employee, contained the means for the attack. The executed exploit caused a DoS attack.”

“Attackers from outside our organization breached our cloud and tried to steal sensitive information about developing products. We stopped the attack by shutting down the server, reconfiguring the firewall, and replacing all the tokens.”

PUBLIC CLOUDS MOST PRONE TO ATTACKS

While 38% of respondents say their organization suffered a cloud attack or breach in the past two years, many report they were compromised on both their hosted and public cloud environments. The vast majority (84%) experienced attacks on their public cloud and 56% were impacted in their hosted cloud environments.
According to *Top Threats to Cloud Computing*, cloud attacks are largely due to lack of visibility and control into hosted and public clouds, including misconfigurations, poor change control, lack of strategic cloud security architecture, and a weak control plane. Others are tied to identity management problems, such as account highjacking and insufficient identity, credential, and access/key management.

**NO ONE-SIZE-FITS-ALL CLOUD STRATEGY**

While smaller or relatively young organizations might have the luxury of building their business-technology environments entirely within the cloud, most organizations don’t have that ability. Respondents classified their organization’s cloud security strategies as follows:

- Cloud first/cloud-native (29%)
- Lift and shift (moving existing applications “as is” to the cloud) (31%)
- Data center focused hybrid cloud architecture (24%)
- Experimenting with public or hosted clouds (16%)

Still, simpler doesn’t always mean easier. Survey respondents cited the following concerns and challenges in managing their cloud architectures:

- **Cloud first/cloud native.** Concerns from “cloud first” organizations included the ability to identify and respond to security incidents, detect changes in a timely manner within their clouds, the inability to detect malicious attacks in a timely manner, and lack of internal expertise.
Lift and shift. These respondents cited concerns about difficulties in monitoring their cloud environments, compatibility issues that require keeping on-premises capabilities, and data loss through the data migration process.

Hybrid. Data center-focused hybrid cloud respondents mostly cited lack of internal expertise, visibility, detection, and response as their challenges and concerns.

When asked to select the top three drivers for their cloud security strategy, most respondents reported IT/development demands (64%) and business requirements (56%), while regulatory requirements, the shift to a remote workforce, and client demands were cited by a smaller share of respondents.

In Their Own Words

Respondents had this to say about challenges they've encountered when adopting a more aggressive cloud strategy:

“I think one of the key issues is a lack of experience and knowledge for the internal teams. We have to rely on the expertise of consultants and then attempt to build our own skillsets through new hires or on-hand experience.”

“We have less visibility into platforms overall and it is harder to stay on top of all of our security goals. We can only have visibility at a deep level into our applications but not the platform.”

“The integration of the technology with our currently existing systems can sometimes create challenges in our operations.”
FILLING THE GAPS IN CLOUD SECURITY CAPABILITIES

Respondents also identified various technologies and capabilities included in their cloud security strategy. Those most common included the following:

- Vulnerability management (69%)
- Cloud workload protection management platform (56%)
- API security (55%)
- Software composition analysis testing (50%)
- Static analysis security testing (50%)
- Container security (45%)

Additionally, when respondents were asked to rate the importance (using a 7-point scale where 1=Not at all important and 7=Extremely important) of these and other cloud security capabilities as well as their satisfaction with these capabilities using the same rating scale (1=Not at all satisfied and 7=Extremely satisfied), several gaps existed among respondents providing relatively high importance scores and lower satisfaction scores for the same capability. In particular, vulnerability management, with an average importance score of 6.1, received an average satisfaction score of 5.8. Other capabilities with importance/satisfaction gaps include API security and penetration testing, among others, suggesting organizations may need to focus on improvements in this area.
Cloud Security Solution Feature Importance/Satisfaction
(Mean Scores out of 7)

Feature Importance/Satisfaction for Cloud Security Technologies

**Importance**: How important is each of the following technology areas in your organization’s cloud security strategy? Rate on a scale from 1 to 7, where 1 is “Not at all important” and 7 is “Extremely important.”

**Satisfaction**: How satisfied are you/your organization with each of your current capabilities? Rate on a scale from 1 to 7, where 1 is “Not at all satisfied” and 7 is “Extremely satisfied.”

In addition to some of these solution capability gaps, only one in four respondents (26%) say they are “very confident” with their organization’s ability to secure their cloud infrastructure and assets, highlighting the need for organizations to invest in technology/automation, service providers, and/or improved policies and processes to protect their cloud assets. Indeed, virtually all organizations (90%) said their spending on cloud security increased in the past year, but budgets and changing internal processes continue to challenge organizations and demonstrating the ROI to upper management can be difficult.
How will your organization’s spending on cloud security change in 2022 compared to 2021?

<table>
<thead>
<tr>
<th>Change</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decrease 1% to 3%</td>
<td>42%</td>
</tr>
<tr>
<td>Decrease 4% to 5%</td>
<td>22%</td>
</tr>
<tr>
<td>Decrease 6% to 10%</td>
<td>9%</td>
</tr>
<tr>
<td>No change</td>
<td>26%</td>
</tr>
<tr>
<td>Increase 1% to 3%</td>
<td>0%</td>
</tr>
<tr>
<td>Increase 4% to 5%</td>
<td>0%</td>
</tr>
<tr>
<td>Increase 6% to 10%</td>
<td>1%</td>
</tr>
</tbody>
</table>

BEST PRACTICES IN SECURING CLOUD SYSTEMS

To increase their confidence and deploy their security budget properly, organizations must focus on securing their systems in the right way, and not just buying tools and haphazardly throwing money and technology at the challenges. Here are some areas the survey reveals respondents would benefit by improving:

**Continuously monitor and harden cloud assets:** Get to know where all cloud assets reside. New cloud assets are always being added, changed, and dropped. As settings and configurations change, so does security posture. Enterprises must be able to continuously monitor to discover their cloud assets, identify vulnerabilities in those systems, and then remediate those vulnerabilities.

**Consider a cloud security gap assessment:** It’s very difficult for organizations to objectively look at the status of their cloud security programs. Turning to a trusted services provider to conduct a cloud security gap assessment can help to identify the objective state of the program, areas that need to be in place or improved, and then prioritize them for implementation.

**Focus on workload, application configurations:** Most cloud attacks focus on poor configurations, such as loosely configured storage buckets and publicly facing databases. Strictly enforce configuration policies, and whenever possible automate the remediation of any out-of-policy and at-risk workloads or assets.
Review identity and permissions: It’s not just people who have access rights to cloud applications and cloud resources: it’s also other applications and even robotic processes that need access. Constantly scour cloud systems and workloads to make sure that people and systems have only the access they need and that excess privileges are reduced.

Move up the Cloud Security Maturity Model: The Cloud Security Maturity Model is a framework that helps organizations understand the security maturity of their organization. From a high level, increasing cloud security maturing is about moving from manual and decentralized processes to automated, centralized and more integrated cloud security operations.

Trends Impacting “Cloud First” and “Lift and Shift Cloud” Respondents

<table>
<thead>
<tr>
<th>CLOUD FIRST / CLOUD NATIVE ADOPTERS*</th>
<th>LIFT AND SHIFT CLOUD ADOPTERS*</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Average number of cloud assets</strong></td>
<td>Public Cloud: 83</td>
</tr>
<tr>
<td></td>
<td>Hosted Cloud: 70</td>
</tr>
<tr>
<td><strong>Average number of cloud attacks or breaches in past 2 years</strong></td>
<td>3.3</td>
</tr>
<tr>
<td></td>
<td>2.7</td>
</tr>
<tr>
<td><strong>Top 3 security concerns</strong></td>
<td>Inadvertent exposure due to misconfiguration (48%)</td>
</tr>
<tr>
<td></td>
<td>Inability to monitor changes within cloud environment(s) (47%)</td>
</tr>
<tr>
<td></td>
<td>Lack of prevention capabilities within cloud-native services (46%)</td>
</tr>
<tr>
<td></td>
<td>Lack of detection and response capabilities in the cloud (52%)</td>
</tr>
<tr>
<td></td>
<td>Inadvertent exposure due to misconfiguration (47%)</td>
</tr>
<tr>
<td></td>
<td>Exposure due to compromised user with access to the cloud (45%)</td>
</tr>
<tr>
<td><strong>Top 3 drivers of cloud strategy</strong></td>
<td>Business requirements (63%)</td>
</tr>
<tr>
<td></td>
<td>IT/development demands (63%)</td>
</tr>
<tr>
<td></td>
<td>Regulatory requirements (39%)</td>
</tr>
<tr>
<td><strong>Most likely to be included in cloud security strategy</strong>**</td>
<td>API security</td>
</tr>
<tr>
<td></td>
<td>Cloud Workload Protection Platform</td>
</tr>
<tr>
<td></td>
<td>Container Security</td>
</tr>
<tr>
<td></td>
<td>Infrastructure as Code</td>
</tr>
<tr>
<td></td>
<td>Penetration Testing</td>
</tr>
<tr>
<td></td>
<td>Software Composition Analysis</td>
</tr>
<tr>
<td></td>
<td>Static Analysis Security Testing</td>
</tr>
<tr>
<td></td>
<td>Vulnerability Management</td>
</tr>
<tr>
<td><strong>% indicating very high confidence in securing cloud</strong></td>
<td>33%</td>
</tr>
<tr>
<td><strong>% indicating increased spending in 2022 since 2021</strong></td>
<td>89%</td>
</tr>
</tbody>
</table>

* Predominantly large organizations (1,000+ employees); **Cited by at least 50% of respondents
CONCLUSION

Reliance on cloud computing is growing, and criminals and threat actors have taken notice. Organizations are targeting cloud systems with greater ferocity since that’s where the data and systems reside. As this study confirms, they are taking the hits, but at least they’re not taking them lying down.

Many organizations are increasing their investments in security defenses and know they have challenges ahead. For example, some are likely to face significant learning curves and complexities in moving from on-prem to hybrid/cloud. Configuration issues may also become forefront, requiring more training for sys admin roles as well as active automated monitoring, logging, and reporting.

This survey reveals just how much work organizations may have ahead, in not only finding the talent they need to build secure and resilient systems but adopting and implementing the right technologies and processes – from secure coding and development pipelines to mastering cloud security architectures.

While some respondents described the impact of the rapid adoption of cloud in terms of being “so much harder to protect information,” and “vulnerable due to the amount of data being moved and integrated,” others were more optimistic and believed “early-stage hiccups would settle after some time and the cloud would become the best option.”

Ultimately, IT security will need to adapt with more effective tools for cloud security to keep the pace.
ABOUT CYBERRISK ALLIANCE

CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA’s brands include SC Media, SecurityWeekly, ChannelE2E, MSSP Alert, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, its research unit CRA Business Intelligence, and the peer-to-peer CISO membership network, Cybersecurity Collaborative. Click here to learn more.

ABOUT BISHOP FOX

Bishop Fox is the leading authority in offensive security, providing solutions ranging from continuous penetration testing, red teaming, and attack surface management to product, cloud, and application security assessments. Discover why our Cosmos platform was named Best Emerging Technology in the 2021 SC Media Awards and our offerings are consistently ranked as “world-class” by our customers. Visit https://bishopfox.com/.