Mar 24, 22 8:43 am

Security in Cloud Applications: Seven Years Ago vs. Now

Mar 24, 2022 | by: Rodika Tollefson

Cloud applications are ubiquitous. Even before many businesses had to accelerate cloud implementation due to the COVID-19 pandemic, the average employee used eight cloud apps, while a midsize company had an average of 121 apps. Despite this robust adoption, security in cloud applications remains a concern for many organizations.

As a result, cloud security investments are becoming a higher priority. Among cybersecurity professionals surveyed in 2021 by Cybersecurity Insiders, more than half said that their cloud security budget would increase in the next 12 months.

But before you invest resources into security for cloud applications, you need to understand the changes in the threat landscape in recent years — and how they impact security best practices.

Main Changes in Security for Cloud Applications

Back in 2015, 90% of information security professionals said they were concerned about cloud security, according to a CloudPassage survey. Since then, cloud service providers have poured billions of dollars into improving security. As one example, popular customer relationship management (CRM) platform Salesforce reportedly spent $2.8 million in 2021 alone to pay ethical hackers who found vulnerabilities in its software.

But the mixed sentiments about security remain. Today, 72% of cybersecurity leaders are still concerned about cloud security, a Check Point report found.

Some of the challenges driving this uncertainty include:

- The complexities of cloud services
- Lack of visibility into cloud applications and data
- The expansion of remote and hybrid work
- A drastic increase in cybercrime
- Lack of consistent controls

The threats in the cloud are evolving, too — adding further challenges.

How Cloud Risks and Threats Have Changed

Seven years ago, cloud computing was cited as the second largest vulnerability that increased organizations' exposure the most, according to "EY's Global Information Security Survey 2015." Fast-forward to 2022, and organizations are still feeling exposed — only about half of leaders in the Check Point survey felt confident about their cloud security posture.

The lack of confidence is not surprising, considering that 40% of 2,600 surveyed security professionals report experiencing a cloud data breach. And among 200 security decision-makers in another survey, 100% reported the same.

For security in cloud applications specifically, some of the top threats include:

Misconfigurations

Gartner forecast that 99% of cloud security failures through 2025 will be "the customer's fault." Misconfigurations, the result of human error or lack of oversight, are the cause of an overwhelming number of cloud data breaches.

One of the many examples was the 2019 exposure of personal data such as email addresses and country of origin for 7.5 million Adobe Creative Cloud customers due to an unsecured internet-facing database.

Unsecured APIs

In recent years, application programming interfaces, or APIs, have taken off as a tool for creating application integrations and interoperability. However, many APIs have exploitable vulnerabilities. The Cloud Security Alliance (CSA) calls APIs the "front door" that may be "the only asset with a public IP address available outside the trusted organizational boundary" — which means they're likely to be continuously attacked.

An example of an API-related data breach was the exposure of 390,000 taxpayer accounts through the IRS "Get Transcript" API.

Account Hijacking or Takeover

Threat actors can gain access into employee or customer accounts through compromised credentials, cloud system vulnerabilities, and phishing attacks. One cybercriminal group, for example, is known for stealing AWS credentials from cloud systems as part of a cryptomining campaign. Most recently, this group has expanded its tactics to target systems that use Kubernetes containers.

The risk of a cloud account takeover has been growing due to the massive number of stolen credentials available on the dark web and even on the public internet. Cybercriminals use these compromised logins to launch credential-stuffing attacks or even targeted ones (as security researchers suspect was the case with the SolarWinds attack).

Best Practices for Better Cloud Security Today

Cloud security best practices are evolving with the growth of cloud-native applications. Many organizations are moving to cloud-native security solutions, which are designed to work seamlessly with cloud applications and scale with them. These solutions take advantage of automation, artificial intelligence, and other technologies, providing benefits such as lower cost, ease of use, and decreased complexity.

Best practices for security in cloud applications include:

- **Identity access management** — ensure your identity access management extends to the cloud so you can enforce your policies consistently across your environment.
- **Access controls** — adopt the principle of "least privilege access," which gives employees access only to what they absolutely need for performing their daily tasks. This approach also supports the zero-trust security model, which is increasingly being recommended by security experts and government entities alike.
- **Encryption** — data needs to be encrypted at rest, in transit, and in use. If your cloud service provider doesn't offer end-to-end encryption, consider either finding an alternative provider or using a third-party encryption solution.
- **Malware prevention** — cloud applications are a growing attack vector for malware infections, with threat actors using malware for attacks such as man-in-the-middle (intercepting data in transit) and distributed denial of service (DDoS).
- **Data loss prevention (DLP)** — to prevent data leakage and unauthorized access, DLP policies or solutions should cover aspects such as data classification, application controls, and use behavior anomalies.

If you're developing applications in-house, there's a host of other best practices recommended across the application lifecycle. Consider advice from experts such as the Cloud Native Computing Foundation and the Cloud Security Alliance.

Final Thoughts

Changes in technology, including emerging technologies such as the Internet of Things, will further expand the reliance on cloud computing — and with it, security risks. Security in cloud applications will likely become even more complex as additional risks emerge.

To improve your confidence about cloud security, start by understanding those risks that will have the highest impact on your organization, evaluate your current posture, and invest resources in closing the gaps