



THREE TOP CLOUD SECURITY CHALLENGES FACING COMPANIES



WITH TECHNOLOGY INNOVATION COMES NEW THREATS AND RISKS.

Cloud technology revolutionized the way companies manage their systems and data over the past decade. Where information was previously stored primarily on local devices and servers, it is now commonly stored and remotely accessed via cloud services.

The ever-changing technology landscape, however, may expose an organization to new security risks. Managing those risks can present significant challenges, especially for companies with constrained information security resources and/or limited experience with cloud-based technologies.

HERE ARE THREE OF THE TOP CLOUD SECURITY CHALLENGES COMPANIES FACE:

1.



MANAGING ACCESS AND AUTHENTICATION

Companies need to be diligent about ensuring only authorized users can access their data. Now that data is routinely stored and accessed remotely, it can be an increasingly attractive target to bad actors. No longer are physical barriers a primary means of controlling access to company data.

Companies have several tools at their disposal to protect against unauthorized access, including:

- ▶ **Multifactor authentication**, which requires a user to submit two or more pieces of authentication information to gain access to a system (e.g., password and token, or password and a code sent via email or SMS) rather than a password alone;
- ▶ **Endpoint detection and response (EDR)** solutions to protect users' devices from threats such as viruses, malware ransomware and phishing; and
- ▶ **Zero Trust solutions** that help the organization grant or deny access based on the user's context (e.g., from where and when are they attempting to access the system).

Companies need to determine which methods are appropriate for their organization and users. Stronger authentication is typically required for administrators and those with access to the most sensitive information.

2.



STORING AND ENCRYPTING SENSITIVE INFORMATION

Companies have a number of responsibilities when storing data in the cloud. Chief among these are data security and privacy requirements. Some considerations companies need to keep in mind include:

- ▶ **What data should I keep?** The more data a company stores, the more difficult it is to manage. By storing unnecessary yet sensitive data, companies open themselves up to greater risk in the event of a security incident.
- ▶ **How long do I keep data?** Companies should not keep data longer than necessary. But how long is too long? The answer to that question varies based on the nature of the data, to whom the data belongs, changing regulatory requirements, policies and contractual requirements.
- ▶ **How do I secure the data?** Secure encryption of sensitive data is a strong defense against unauthorized access to data. Companies should take advantage of the encryption functionality provided by cloud services.

A practical approach to data life cycle management and encryption of sensitive data can be a key risk mitigation strategy.

3.



MANAGING SECURITY INCIDENTS

Security incidents are inevitable. Sooner or later, every company will experience a security breach — for example, an employee falling for a phishing scam — that puts the company's data at risk.

Companies need strong processes and tools in place to detect and manage security incidents, including key steps such as:

- ▶ **Identify the incident** — Quickly identify security events that potentially involve access to systems and sensitive data and initiate the incident response process.
- ▶ **Contain the incident** — Ensure the bad actors are unable to access any other data in the system, and work to disable their access as quickly as possible.
- ▶ **Assess the impact** — Determine what data was vulnerable to or accessed by the bad actor, where that data resided and who has been impacted. Is it a specific customer or group of customers? Was it a vendor system that was compromised? Forensic analysis may be required.
- ▶ **Notify impacted parties** — Make sure that anyone whose data was impacted is notified of the security breach and your company's efforts to address it in accordance with breach notification legal requirements.

Companies need to have processes in place before a security incident happens. Otherwise, they will find themselves scrambling to effectively respond when an incident occurs.

WHAT CAN YOU DO?

These are three of the top challenges that companies face as they seek to manage cloud security. How can you make sure that your company has the right controls in place to address these challenges, particularly if you provide services that process and store sensitive customer data?

By seeking third party [attestation services](#), an organization can obtain verification of their security and privacy compliance with industry standards. There are various types of attestation services that you can seek for this purpose. They include:

1. **SOC 2 Report:** This report includes an examination of an organization's internal controls related to security and can also cover availability, processing integrity, confidentiality and privacy. SOC 2 focuses on the company's controls to address a defined set of security and other requirements for services provided to its customers. For more information, read our [summary of SOC reporting](#).
2. **ISO Certification:** ISO security and privacy certifications offer validation that your organization's security or privacy program is operating in accordance with international standards. ISO certification tends to be most applicable to companies with a global customer base. To see recent updates to ISO 27001 and ISO 27002 for 2022, [read here](#).
3. **CSA STAR Assessment:** This is a program developed by the Cloud Security Alliance (CSA) based on requirements defined in the Cloud Controls Matrix (CCM). CSA STAR was developed specifically to address cloud security risks and requirements. It includes options that companies can pursue based on their needs.
 - **Level 1:** Self-Assessment.
 - **Level 2:** Third-Party Audit. This includes STAR Certification which is an expansion of ISO 27001 certification and STAR Attestation which is an expansion of SOC 2 reporting.

More information on CSA STAR can be found on [their website](#).


Each of these third-party attestation processes can help a company to evaluate and improve its cloud security practices, including the areas noted above. The resulting independent auditor's reports can then be shared with customers to address their security concerns.



WHY BDO?

At BDO, we pride ourselves on tailoring our attestation services to your needs, based on a deep understanding of your business. We not only provide fair and balanced assessments, but we also provide the support you need to demonstrate adequate controls and safeguards. We offer a variety of [attestation services](#), including SOC 2 reporting, ISO certification and CSA STAR assessments to give you confidence in your cloud security controls.

READY FOR YOUR ASSESSMENT? SEE WHICH OF OUR ATTESTATION SERVICES IS RIGHT FOR YOU ►



BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, and advisory services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 70 offices and over 800 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of more than 97,000 people working out of more than 1,700 offices across 167 countries and territories.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.

© 2022 BDO USA, LLP. All rights reserved.