ALTITUDE NETWORKS

5 Keys to Working Securely in the Cloud

Businesses shifted their workloads to the cloud in 2020 at record-breaking rates. The pandemic left many organizations with few choices other than remote work, and cloud services and applications gave their employees the ability to keep operations moving, customers engaged, and teams collaborating.

91%
increased on the cloud in 2020

60%
add more cloud services

Research for Veeam's 2021 Data Protection Trends report found 91% of organizations increased their reliance on the cloud in 2020, and nearly half have increased Software as a Service (SaaS) use. Moreover, 60% now plan to add more cloud services.

The reasons are clear. The cloud gives teams greater flexibility and mobility. Employees can access their desktops from PCs in their homes and from mobile devices when working on the road or in different locations. Cloud solutions and services also make it easier to backup and recover data, and they make life easier for in-house IT because software patches and updates are automatic and employees are always using the most updated version of the software.

Along with all of the cloud's benefits, however, come some challenges – particularly with security. Cloud services providers invest heavily in technology that protects their services and infrastructure and detects and stops intrusions. Unfortunately, those preventative and mitigation measures often don't address one significant threat: People.

The 2020 Verizon Data Breach Report states that second only to hacking, "miscellaneous errors" are a common reason for data breaches, accounting for nearly one-fourth of all security events.

Businesses and organizations often deploy multi-factor authentication and a centralized single sign-on solution to decrease the chances of human error that results in unauthorized people on the network. It is a positive first step. If an employee's login credentials fall into the wrong hands, a hacker wouldn't be able to complete the steps necessary to gain access as an authorized user. However, solutions such as single sign-on and multifactor authentication are only the tip of the iceberg for comprehensive data protection. Stopping after just adding strong authentication would leave organizations vulnerable to a myriad of security missteps that place critical company data at risk everyday.

5

Factors Necessary to Protect Data in the Cloud

There are five elements that businesses must build into their security strategies to protect data from loss, hacking, and employee errors.

1. Access Control

Many SaaS solutions and cloud services have built-in access control features. Employees can use them to add specific internal and external collaborators to a document or to share the document to a broad audience like the entire company, or entire world, by link. While these settings will prevent access based on the configuration, they are only effective when employees remember to use them—and use them correctly.

Additionally, visibility into employee behaviors is limited with these systems. Often, the IT team, security resources, or managers can't see if employees are following policies to protect sensitive data.

Businesses may deploy data loss prevention (DLP) solutions, but traditional solutions have developed a poor reputation. Legacy DLP solutions often require extra time to set up and deploy and add steps to an employee's workflows before they can safely share a document. Legacy DLP is also notorious for a high volume of false positives, which can monopolize an IT department's time and create alert fatigue. IT may begin to ignore alerts, even if they are critical.

Additionally, legacy DLP solutions may require an agent to be installed on the employee's computer or device, which can contradict some of the mobility and flexible access that the cloud was meant to provide.

The drawbacks and limitations with legacy DLP have inspired modern DLP solutions that are easy to use and cause minimal friction in existing workflows and are designed to work specifically with the needs of cloud collaboration SaaS applications. Today's innovative solutions can differentiate between different types of data, which not only guards access when necessary but also minimizes false positives. The best solutions are also agentless so that employees can use them on all devices through API integration enabling them to work remotely.

2. Employee Education

Whether your employees are just beginning to work in the cloud or they have been using cloud solutions for years, it's smart to educate them about company policies designed to protect sensitive data. New users may not realize the risks that using cloud applications and services can create if they aren't doing their part to protect data, and veteran cloud users may become overconfident and become lax with security.

Create a security training program for your team that includes awareness and instructions on how to avoid data loss related to:

Link sharing permissions

Employees using tools such as Microsoft Office 365 or Google Workspace commonly create documents to share with collaborators. However, when an employee configures a file in "link sharing mode" instead of individually adding specific collaborators, then the file is at risk for access by unintended individuals. In this situation the link could be unintentionally forwarded in an instant message, appended to a group email, or forwarded in a document. In all of these situations, anyone receiving that link could access the file including competitors or anyone from the internet!

The best practice is to follow the principle of least privilege, granting only enough permission for specifically named employees or collaborators to do their jobs – and no more.The difficulty of securing cloud data is that the business naturally shares a variety of data types with many internal and external collaborators. The solution is not to simply block external sharing, but rather ensure only the correct people are able to access sensitive data. Optimally, you should deploy a solution that automatically understands when sensitive data is shared to the wrong audiences or put at risk by incorrect security settings.

Link sharing mistakes

Risks aren't only the result of uninformed or rash decisions about sharing documents and permissions. Sometimes they're simply the results of mistakes. For example, an autocomplete feature meant to save the user from having to type in a collaborators' complete email address may display the wrong person, and the user may click. Suddenly, someone with the same first name as a collaborator has access and possibly the ability to edit and share a document containing sensitive data. Or, your employee may share a document with a collaborator's personal email account, thereby granting access to the employee long after they've left the company.

Training your team is essential to reducing risks from employee mistakes, but technology that can detect instances of unintended sharing to personal accounts can proactively protect against potential data loss.

Permissions for third-party applications

Third-party applications, mobile apps, and plug-ins that integrate with Microsoft Office 365 or Google Workspace environments may ask for the ability to upload, delete, or store data. It may be easiest for your employee to grant the highest permission level so that the integration works seamlessly, but it's not the safest thing to do. If the third-party solution's servers are hacked, your data may also be vulnerable. Furthermore, cybercriminals may use an app or plug-in as a part of an exploit to gain access to your network and your data.

Your IT team should vet each application or tool that your team uses to ensure it meets your security and data protection standards. Furthermore, your team should monitor app use so that only approved tools are used in your IT environment. Your business will also benefit from using a solution that continually monitors applications connected to your cloud collaboration application alerts you when new apps or plug-ins are used, and if they have a high level of permissions.

Documents created in personal accounts

With more people using cloud applications and services, it's possible that employees can shift between their personal and work accounts, especially when working from home or using mobile devices when away from the office. This may not be deliberate. For example, when an employee uses a personal laptop at home, their computer may save a document to their personal Google Drive rather than the business'.

Documents created in personal accounts can put data at risk, but there is an additional problem. If your employees make it a habit, you will eventually have a volume of data that's stored and used outside of your IT environment. You lose control of where your data is, how it's used, and who can see it.

Malicious employees

Accepting the fact that some employees have malicious intentions is also essential. An employee may be ready to change jobs – and take client lists or other data before resigning. Others may have even more nefarious intent, such as an employee involved in corporate espionage or a disgruntled employee set on corrupting data. In these cases, it's critical that you identify how documents are created and how they are shared. Education can be helpful here to inform managers and HR teams of the resources to detect and respond to disgruntled or exiting employees that may be attempting to exfiltrate company data.

A solution that identifies and alerts IT and security that a document is coming from outside your organization is crucial to spot these issues, retrain the employee, and move the document within your cloud environment.

3. Maintaining Control of Partner Documents

Most business leaders are aware that data is at risk from cyberattacks, human error, and theft, but they don't always see working with partners as a potential cause of data loss. If a contractor, consultant, or other business partner creates a document, the policies they follow may differ from yours, putting data at risk. Furthermore, if the partner is the document owner and then deletes it, you can lose critical data.

On the other hand, if you are the document's owner but don't change permissions after the project is complete, your partner may still have the ability to enter the file and view or even copy data.

Tracking documents that you share with a partner can be difficult. You may need to require collaborators from your organization to report on shared documents and keep a permanent copy for your business. Performing this task manually can be time-consuming, and records can be incomplete. Leveraging technology to track partner-generated shared files will streamline the process, generate a complete list of files, and give you visibility when your partner moves a document. Of course, the best strategy is for your business to own all vital documents, maintain control of them, and ensure that users follow company policies for data protection.

4. Simplicity

Complex DLP solutions won't provide your business with benefits if none of your employees use them, or worse, they cause such friction throughout the company that business can't be accomplished. Historically, DLP solutions used in complex IT environments have slowed employees down, adding steps before they could share documents and possibly interrupting a collaborative team's synergy and workflow. In some cases, DLP solutions require the user to tag or encrypt sensitive data manually. The unfortunate result of clunky workflows required to prevent data loss is that users will disable DLP features or find workarounds so they can share data more quickly.

To simplify data protection policies for your employees, start with centralizing cloud collaboration platforms and avoiding supporting multiple similar SaaS applications. In many cases the desire to have two, or more, different cloud collaboration platforms is an unfortunate byproduct of the desired platform not having sufficient security controls and options to protect critical data. By streamlining the environment to a small number of SaaS cloud collaboration applications, the proper security controls and settings can be applied leading to easier management and fewer demands on employees to apply security controls.

The optimal scenario is a streamlined IT environment protected by a security solution that automates data protection policy enforcement and doesn't require users to tag documents containing sensitive data manually or turn on features. It is also beneficial for the solution to notify IT/Security when it detects files at risk so that they can intervene to protect the data and provide employee training, if necessary.

5. Intelligent Technology

As your employees work, security isn't always top of mind. They're focused on customer service, closing deals, meeting goals, and building revenues. However, an intelligent data loss prevention solution is always focused on securing all the sensitive data your team is using and sharing.

DLP solutions that leverage natural language processing (NLP) search files for protected data and alert your security team when files are shared outside your company or an employee is downloading large volumes of sensitive data. Intelligent DLP technology also learns as you use it to understand what typical business processes look like and how your team works, then pinpoints and flags unusual or risky behaviors using behavioral analysis.

Along with making it easier for your team to comply with data protection policies and for your security team to monitor and address issues, an intelligent DLP solution also gives you the advantage of stopping data loss before it occurs. A proactive approach eliminates the need to deal with the outfall after a team member accidentally (or intentionally) shares sensitive data with the wrong people.

Give Your Business the Full Advantages of Cloud Without the Risks

Transitioning workflows to the cloud has been necessary for many businesses to maintain operations during the pandemic. Moreover, cloud IT environments will give companies the flexibility to adapt if crisis circumstances arise in the future. However, it's crucial to remember that along with the convenience and flexibility that the cloud provides is a greater chance for protected data to become visible, fall into the wrong hands, or be lost.

Perhaps the biggest risk is adopting cloud solutions without taking the need for new security policies and procedures into account.

Embrace the cloud for all the good things it will provide to your business, but proceed with caution, building a strong, comprehensive security strategy that will protect your data and your business.

Altitude Networks is at the forefront of enterprise cloud security and data loss prevention — protecting your company's cloud data against unauthorized access, accidental or malicious sharing, and theft.

With our cloud-native DLP solution, you can quickly identify, remediate, and prevent data loss in the cloud with one click.

For a free Rapid Security Assessment, visit us at AltitudeNetworks.com.