CLOUD SECURITY AND DATA PRIVACY ESSENTIALS, AND WHY THEY MATTER

When the rush to the cloud began, the value proposition was a prime attraction. Organizations could save money on capital expenses, because hardware and the people to maintain and support it were furnished by the cloud service provider.

They didn't have to fret about software and hardware upgrades, either, because the cloud provider took care of that, too. They didn't have to worry about storage, because cloud storage was unlimited. And they didn't have to worry about scaling resources up or down, because that could be done quickly in the cloud.

Those benefits of the cloud are still a major draw for organizations, but now data security and privacy—once considered major weaknesses with cloud-based systems—are now considered pluses by many customers. There's more to it. Here's what your organization needs to know about cloud security and privacy, and why.

Security: A cloud bugaboo

Security has always been a problem for the cloud. In the early days of cloud development, security was often raised as a barrier by IT executives reluctant to turn over control of their organization's family jewels—its data—to strangers.

Over time, though, it became apparent that, when it came to securing infrastructure, cloud providers could do a better job than most organizations could do on their own. Cloud service providers could afford to hire the best talent and deploy the best technology to secure their networks.

However, the security model that's evolved for cloud services is a shared one. At its most basic level, shared responsibility means a cloud security provider will be responsible for the security of the cloud, while the customers are responsible for the data they put in it.
But those lines of responsibility aren't strictly drawn. For example, in an infrastructure-as-a-service arrangement, customers are responsible for managing the guest operating system, installing and maintaining applications, and configuring firewalls, as well as overseeing data, classifying assets, and granting permissions for identity and access management.

But in a platform-as-a-service environment, the cloud service provider handles the underlying operating system—and all the maintenance that entails—while the customers take care of deploying, managing, and securing applications, as well as controlling data, assets, and permissions.

Even more responsibility is dumped on the cloud service provider in the software-as-a-service model. There, all the customer needs to worry about is managing data and access.

What's good about cloud security today?

As cloud adoption grew, cloud service providers (CSPs) continuously bolstered their security offerings; today, it is much more likely that any security problems in the cloud will be caused by a customer than a CSP.

In contrast to the past, customers are much more aware that CSPs have far more resources than most companies to secure infrastructure. What's more, because the components of the cloud are running in data centers staffed by experts in the technology, data stored there can be more secure than data stored locally using conventional practices.

Organizations can also expect a cloud service provider to have a full complement of security tools to protect their environment, including the latest anti-malware software, intrusion protection systems, application firewalls, and network monitoring and event analysis solutions powered by machine learning and artificial intelligence.

CSPs are also more capable of handling distributed denial-of-service attacks than most organizations.

That's becoming more of a concern as DDoS barrages have been on the rise lately. According to NextGuard, a DDoS mitigation provider, DDoS attacks increased by 242% year over year in the first quarter of 2020, and by 542% over the previous quarter. Thwarting DDoS attacks requires a robust infrastructure—the kind that large CSPs have with their global reach and multiple points of presence.

Many organizations have also taken to the cloud to develop their apps in a secure environment. Often, the approaches and mechanisms offered to developers and administrators in the public cloud are better than the tools and methods they're using in the enterprise.

Room for improvement

While there are many security benefits to organizations migrating to the cloud, one of the major hangups centers on encryption. Since under the shared responsibility model, cloud customers are ultimately responsible for the security of their data, many have started wanting to use encryption to protect it. CSPs responded by creating encryption tools. Those tools, though, are less than ideal for some organizations.

For example, the encryption model used by some providers uses an encryption key for every data element stored. That can get unwieldy as an enterprise scales up its data requirements and needs to deal with millions of database records.

Organizations have also raised concerns about never having complete control of data encrypted by a CSP because the provider controls the encryption keys. CSPs have tried to address those concerns with something they call "bring your own key." Even that approach is flawed, however, because the master encryption keys are always controlled by the CSP, which can be used to override the customer's key.

For organizations using multiple CSPs, encryption presents another problem. Data encrypted by one provider must be decrypted before it can be used with another provider or by on-premises systems. Decrypting the data, of course, exposes it to security risks.

In addition, encryption services are anchored to regions. There's no guarantee of cross-region integration of encryption services or that keys used to encrypt data in one region will be available to decrypt the data if it's moved to another region.

The variety of CSPs' encryption is also limited. That can hamstring an organization that needs to work with encrypted data without decrypting it or with defined tokenization services, which are needed to meet some compliance requirements.

How do you get started?

When you think about security and privacy in the cloud, you should start with the basics. The four pillars of any security program are authorization, logging, confidentiality, and integrity.

Authorization. Simply put, you have to determine who has access to what. You want to make sure that employees have the authority they need to do their job, but not so much authority that they could become a security risk if their credentials are compromised.

Logging. Keeping tabs on the actions of users creates an audit trail that can be reviewed when something goes wrong. That trail can also help identify patterns that reveal security flaws and gaps, or system compromises.

Confidentiality. Making sure data is viewed or shared with only authorized parties is important, not only for maintaining the confidence of customers and stakeholders, but, in many cases, because it's required by law. Failure to obey those laws can result in stiff fines and penalties.

Integrity. Just as you don't want your data to be seen or shared by unauthorized individuals, you don't want data you're responsible for to be accidentally or maliciously modified. One way to preserve the integrity of data is to encrypt it. Encryption makes it difficult to tamper with data because a set of keys is needed to decrypt it. Those keys are usually stored securely and access to them is limited.

How is the security and privacy space evolving?

Traditional cloud security issues —denial of service, shared technology vulnerabilities, cloud service provider data loss, and system vulnerabilities—are becoming less important to security practitioners. Instead, they're more worried about higher-level issues: control plane weaknesses, metastructure and applistructure failures, and limited cloud service visibility.

Identity management is also gaining importance for protecting data and preserving privacy. In the "data everywhere" world that organizations operate in today, controlling who or what has access to information is essential for securing it.

Through identity and access management (IAM) software, user identities and access can be initiated, captured, and recorded. IAM systems can assure that privileges are granted based on policies set by developers and security administrators. Equally important, they can verify that all individuals and services are properly authenticated, authorized, and audited.

The developer's role in cloud security and privacy is also evolving. The cloud has increasingly become a platform for application development. That has expanded opportunities for threat actors, but it has also created opportunities for developers to improve the security of their applications through DevSecOps, which puts security at the core of the development to infrastructure and operations pipeline.

In addition, the attitude of businesses toward data is evolving. They're realizing that protecting data at different technology layers is not enough. They need a holistic approach to security and privacy and must protect information through its entire lifecycle, from the moment it's captured to the day it's destroyed.

Taken from: https://content.microfocus.com/cloud-security-data-privacy-tb/cloud-security-data-privacy