IndustryWeek

ASK THE EXPERT

Time to Clear the Air on Cloud Security

MICHELE BARLETTA
Security Product Manager
Siemens MindSphere

The trend is clear. Organizations are moving their data to the cloud. So much so, it's estimated that 83 percent of enterprise workloads will be in the cloud in 2020. The growth of the Internet of Things (IoT) is understandably playing a key a role in this shift. After all, IoT is allowing companies to collect and analyze unprecedented amounts of data.

However, the ongoing migration is resulting in a shift in the balance of power as organizations grapple with the security differences between the two paradigms. Unfortunately, the result is a trust issue. According to a survey of IT security decision makers, 62 percent of respondents working for enterprises with more than 5,000 employees believe their on-premise security is superior to cloud security. In large enterprises, 22 percent of IT leaders said that security strength was no different between the two environments, and 16 percent said that cloud security was stronger.

Below, Michele Barletta, security product manager for MindSphere, part of Siemens Digital Industries Software, shares his insights on cloud security. With more than 15 years of experience in theoretical and practical aspects of applied security, Barletta has held roles including security consultant, senior security key expert and ethical hacker.

Q: How does cloud security differ from on-premise?

A: The main difference between the two is the ownership of the security environment. For most organizations, IT has the control when storing data on-premise. In the cloud environment, security control adheres to a shared responsibility concept. Despite some companies feeling that they are losing some control, there are big advantages when considering how security is actually handled on the cloud side.

When managing data on-premise, the security tooling (web application firewalls, next-gen firewalls, etc.) are all working on a standalone basis with mostly manual controls.

Cloud security leverages dynamic resources including APIs, which play an essential role in providing automation and orchestration to enable some of the features such as scaling with services common in today's business environment.

Q: Is there data that should never be stored in the cloud?

A: All kinds of data can be uploaded to the cloud. The real question is how much we trust the provider. Organizations need to take the time to analyze what controls and measures the cloud provider has implemented. There are differences between cloud providers and the level of security they provide. Companies need to do the work to find the best provider for their needs, especially when uploading sensitive data. The certifications do not apply to each cloud service and not every cloud service can be used in every region. The configuration of each cloud service also strongly influence which security level can be achieved or which local regulation might apply.

For example, the decision if it is enough to store the backup in the same datacenter, in different datacenters or even over different continents depends on the criticality of the data and the individual use case.

Certain industries (healthcare, legal or financial) need to follow compliance-based regulations. Most IoT data is not so sensitive. Going back to the concept of shared responsibility, it's the company's responsibility to check capabilities of their selected provider.

Q: What questions should companies ask to ensure that the cloud provider is keeping their data safe?

A: The goal is to select a provider who aligns with your business needs. Some important questions to ask are:

Is the provider following security standards and certified to those standards? Whether it's ISO 27001 or an industry-specific requirement, this is the best route to take to ensure that the provider is following the best practices for your individual needs.

What are their storage and computing capabilities? You do not want to find yourself tied to a system that is not scalable enough to react as your organization grows and evolves.

Is data encrypted (in motion and at rest)? Who handles the encryption keys? When you have a connection to the cloud environment, you always make sure the data is encrypted. When it comes to keys, some providers offer full managed service, while others allow organizations to manage their own. This is a crucial question to ask to make sure a cloud provider keeps your data safe.

What is the mechanism for sharing? How the provider handles sharing tells you about their authentication process. You can actually have full control of data on the cloud, but you need to know how they work.

How is disaster recovery handled? This is crucial because you need to know what happens if the provider gets hacked or there is a flood or fire. Are you losing data or is there data redundancy built in with copies stored in different geographical locations? Also, this lets you know what your responsibilities are in terms of preventing data loss.

Of course, no one should blindly trust information from a provider. Always go back to the certifications and make sure they are handled by third parties.

Q: What level of security should companies aim for?

A: Every customer should aim for the level of security that meets their organizational needs and industry regulations. Make a plan and categorize the data you put in the cloud. Is it restricted or confidential? How is it classified in terms of business value? Understand which mechanisms and controls exist and make sure the provider properly configures the services to meet your requirements.

Q: How do companies continue to stay safe in the cloud over time?

A: Security is always a journey. And, the shared responsibility model means companies are working together with the cloud provider to ensure that data remains safe over time. Resources are always changing. Systems are constantly changing. It's important to track those changes when adding more data to the cloud. The security controls need to stay up to date to maintain security expectations. Keep an eye on the provider's certifications as well to ensure that they are updating them as new requirements arise. No organization wants to find out that it is no longer compliant with industry regulations.