Can cloud compete with on-premises when it comes to cybersecurity?

Cloud computing represents a seismic shift from traditional computing, one that enables users, whether businesses or government agencies, to do more, faster. In part, this shift is due to the way in which cloud services are provisioned and maintained, allowing customers to tap into the power of cloud datacenters and services without having to build, manage, or maintain them. However, this technological transformation has been plagued by security concerns - driven, in part, by both increased understanding of the general online risk environment and by persistent media coverage of cyberattacks, whether related to cloud computing or not. Additionally, cloud computing requires a change in attitude when it comes to control, which can be uncomfortable for those used to older, traditional technologies. The cloud approach itself can *feel* more insecure because data is stored on servers outside an organization's direct control. However, as when we compare car and air travel safety, *direct control does not always equal greater safety or, in the case of computing, security*.

Data hosted on-premises is not free from cybersecurity risk. It is subject to many of the same cyberattacks as cloud solutions but with the disadvantage of lacking the immediate access to cloud providers' multinational resources and security measures, which are a major focus for those providers. Examples of security benefits cloud usage can bring are given below.

Security as a core business function

Cloud providers recognize that trust is a fundamental part of their business model and do their upmost to keep it. At the same time, they operate on a scale that requires them to architect their systems based on the assumption that anything that can go wrong will go wrong, e.g. nefarious users will exist, customer workloads will sometimes be infected with malware, or physical machines, network devices, and storage arrays will fail. Providers therefore need to maintain complete control of the environment and enforce best practices and secure defaults for tenants. Moreover, cloud providers also use security to differentiate themselves, hiring the best talent in this space and dedicating significant resources to its development. For example, Microsoft in 2015 invested more than $1 billion in security.

Physical access to data

Cloud solutions have a physical infrastructure component, which includes data center facilities and, components that support the services and network. However, the security measures that can be applied at large data centers are substantive. Designed to meet the requirements of multiple stakeholders, they are often at higher level than those imposed or realized by any single company. Examples include restricting access to only personnel with completed background checks, requiring biometrics to gain physical access, and applying a least privilege policy.

A better understanding of the threat environment

The large pool of clients can work to the benefit of security, as it allows cloud providers to look for security intelligence across their whole environment, which is much larger than an average corporation's traditional on-premises infrastructure. This data can be used by big data security-intelligence systems to discover malware and network intrusion attempts around the globe. The faster such threats are identified, the better chance there is of stopping malware before it infects a cloud provider's client. For instance, Microsoft detonates email attachments blocked by our advanced threat protection service, and if malware is found, then we can search our entire cloud environment for that attachment and protect all of our customers from that malware.

Outsourcing security maintenance

Depending on the cloud service model, cloud providers may not manage just datacenter security but also network controls, identity and access controls, and patching. For example, the cloud provider can take care of some tasks that in traditional environments are time-consuming, such as automatically applied patch management, regular vulnerability and system security configuration scanning and privilege management. All of these actions help to reinforce the cybersecurity of the cloud environment

Scale as a shock absorber for security

The rapid, smart scaling of distributed cloud resources enables cloud providers to thwart emergencies and distributed denial of service (DDoS) attacks more effectively than on-premises solutions. The growing sophistication of large-scale DDoS attacks means that the perpetrators are often able to overload the network connection faster than mitigations can be put in place. Cloud providers can bring scale and power of computing to thwart those attacks. Moreover, cloud providers that utilize geographic replication are able to host data and services in several regions so can not only absorb the impact of an online event, but also ensure that data is safeguarded. Indeed, in an environmental disaster or another unforeseen emergency event, distributed data centers are a key way of ensuring data is preserved, something that a traditional on-premises computing environment cannot ensure.

Security as a function of greater awareness

The very process of migrating data and services to the cloud can increase the security and resilience of an organization's computing infrastructure. This is because migration can act as a forcing function for robust data governance, making organizations not only more aware of the data that they retain but also more purposeful about how they treat it.

Security innovation comes first in the cloud

Finally, it is important to acknowledge that most technology providers have adopted a "cloud first" approach. As a result, the majority of their innovation is delivered in the cloud and only later translated into on-premises solutions. Given the comparative speed of updates in the two environments, that represents a significant advantage for cloud over traditional implementations; many of these developments are in security.

The above points go some way showing that cloud security can not only compete with security delivered on-premises but that cloud computing has several distinct advantages. This has also been the conclusion of an increasing number of government agencies around the world, underpinned by the decision of the United States General Series Administration to certify a small number of cloud providers to store even the most highly sensitive government data in the cloud[1]. However, it is important to remember that *no two organizations are exactly the same*, and that when it comes to cloud, no single solution fits all models. While many organizations might benefit from a complete immersion in the cloud, others may need an in-house solution and some might benefit from a hybrid of both. As a consequence, cloud adoption strategies need to involve nuanced risk management decisions that take place within a framework of security assurance to ensure the most appropriate approach is taken.

[1] FedRAMP High Baseline: https://blogs.microsoft.com/firehose/2016/06/23/microsoft-cloud-for-government-achieves-fedramp-high-compliance-status/#sm.0001qncafoiz5cp0sd71wzk0s6lji