Where public cloud security outperforms non-cloud deployment models

The race is on between cloud and non-cloud service deployment models and cloud service providers have one clear advantage: scale.

PAYMENT CONNECTIVITY CYBERSECURITY ACCESS CONTROL JUSTICE & PUBLIC SAFETY TRAVEL

POSTED ON 01.26.23

Any individual organization has a fixed capacity for investment in security; but in the cloud, the sky's the limit. Cloud service providers pool the resources of every company in their network, making it possible to invest billions to stay ahead in the race.

The cloud deployment evolution

Since the cloud was created over 10 years ago, roughly two-thirds of enterprises have migrated over. For the remaining third, much of their reluctance stems from not being fully aware of how the cloud environment has evolved over the past decade. The last holdouts in the public and private sectors still tend to equate today's cloud with the first ever cloud. But **the cloud has come a long way over the past decade**—especially in terms of security.

Public cloud security is business critical and battle tested

Leading cloud service providers have been around from the beginning, growing in size and expertise with each passing day. As they expanded and became increasingly more critical, they simultaneously encountered a growing number of attacks as well as **heightened scrutiny** from state and industry actors. As a result, they invested massively in public cloud security and in developing their expertise in fending off attacks. After all, any cloud computing security breach puts their reputation and their viability at stake. **Mitigating large scale attacks has become business as usual** for these major players, who have become uniquely capable of securing cloud service at scale.

One clear example of this is their **ability to mitigate DDoS (Distributed Denial of Service) attacks**. Hackers typically use thousands of bots to inject junk traffic and saturate data center networks, bringing service access to a complete standstill. Mitigation requires spreading the attack over a large backbone that is resilient enough to avoid saturation. It is nearly impossible for independent data centers to compete in this type of **asymmetrical war**—one that costs a few thousand dollars a month to execute; meanwhile requiring upwards of 100 thousand dollars a month to defend. On the other hand, major cloud service providers operate at a scale that makes it possible to **spread the investment burden** across a customer base of millions. Both AWS and Azure fended off attacks above 2 terabits per second (Tbps) in 2020 and 2022[1]—something very few companies can claim.

Cloud resilience

The scale of cloud service providers also makes them uniquely apt at ensuring the resilience of their networks. For example, typical data centers have hundreds of pieces of equipment in service at any given moment. They simply do not have the time or resources to test for failures every day. Cloud service providers, on the other hand, have millions of devices in operation, which statistically speaking, means that they are faced with failures on a daily basis. The difference here is that cloud service providers have **teams dedicated solely to avoiding and recovering from failure**—for them, it's just business as usual.

A granular approach to public cloud security

Another key area where public cloud security outperforms traditional data centers is the way they approach security. On-prem data centers and workloads were initially designed around the notion of physical and logical perimeters, or "walls". These walls can be very strong, but once breached can open up a large attack surface.

At the time, the technology for granular security didn't even exist—and building it now would be extremely difficult, time consuming and expensive. This matter, once again, goes back to scale. A single organization doesn't have the resources to integrate highly granular security. Cloud deployment models, however, **have been built from the ground up to provide security at every level**. This means that every unit, every server, application and service can be configured with its own security context and walls. This is called **in-depth security**, meaning that highly sensitive information can be protected by several layers of security. If one layer is compromised, it has a backup, and its backup has a backup.

Who is responsible for public cloud security?

While public cloud security continues to increase, organizations running services on cloud service providers' networks **cannot blindly rely on them** with cloud security. After all, cloud service providers are only responsible for the security of the infrastructure.

These organizations need to **ensure that they are doing their part to secure services and applications** for their clients. This includes explaining the roles and responsibilities with their clients, analyzing the specificities of the services, and sharing and applying best practices accordingly.

Cloud service providers clearly identify the limit of their scope in a "**shared responsibility model**," which lets service providers relying on their network know what they have to implement within the the cloud environment—on top of the solid foundation provided by the public cloud scale. The security provided by major cloud service providers such as AWS, Azure or Google is often referred to as **security *of* the cloud**, whereas additional security that falls under the responsibility of service providers who are managing critical services for governments or highly regulated industries is called **security *in* the cloud**.

Whether by protecting against DDoS attacks, protecting against loss of data or tampering, or allowing themselves to major benefits that the cloud provides, cloud deployment models allow companies to leverage the tools, processes, investment and expertise of major cloud service providers in order to **stay ahead in the ongoing security race**.

---

[1] https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/; https://www.zdnet.com/article/microsoft-heres-how-we-stopped-the-biggest-ever-ddos-attack/
