Security implications of logical separation in the cloud

Microsoft Policy Papers

Security of a multitenant environment

In recent years there has been increasing pressure on organizations of all types to deliver cost-effective and efficient services that are responsive to current and future needs. Information and communication technology (ICT) has played an important role in reaching these goals. Along the way ICT has transformed, moving from traditional on-premises data center environments to virtualized ones, or to cloud computing. Today's data centers and clouds host different users, sharing physical servers and network infrastructure in order to efficiently and cost-effectively pool computing resources and/or applications. This is called multitenancy.

Cloud computing is a fundamentally different ICT paradigm and security approaches must adapt. Modern cloud providers operate at a scale that requires them to architect based on the assumption that what can go wrong will go wrong: nefarious tenants; malware-infected customer workloads; failures in physical machines, network devices, and storage arrays. Providers must maintain complete control of the environment and enforce best practices and secure defaults for tenants. On-premises environments are often smaller and so are challenged to match the sophistication, expertise and resourcing available to hyper scale providers. Indeed, best-in-class procurement requirements and controls recognize that multitenant environments meet the same standards as physically separated ones.

They do so by using a hypervisor, which allows workloads from different tenants to run in isolation on shared physical servers. Hypervisors are designed to be as small as possible and undergo rigorous security reviews to stop a workload from being able to detect other workloads. Each workload sees a virtual storage device containing only the files associated with its own data. Moreover, the hypervisor has complete control to start, stop and pause workloads. It also controls the physical network cards, so it can filter all the network packets based on the workload identity and tenant. The physical storage media contents are tagged with the tenant owner and associated virtual machine. Moreover, tenants can control their network connectivity between servers and the Internet, as well as create separate virtual networks for different purposes like production, development and testing. The hosting provider's fabric controller coordinates with hypervisors hosting workloads for each tenant to make sure only workloads on the same virtual networks of a tenant see each other's traffic or have connectivity to the Internet.

The fact that in a public cloud environment different customers are separated logically (by software) rather than physically, has been cited as one reason for organizations not moving to the cloud. Such concerns should, however, be considered in a larger context of balancing benefits and risks, e.g. comparing the competitiveness impact of not moving to the cloud with the risk of downtime should a cloud provider suffer an outage. Focusing on security alone, physical infrastructure needs is just one of many factors within a holistic view of an organization's risk environment. Access management, software development and incident response capabilities, etc. must also be considered (as below). There are seven common concerns relating to security implications of logical separation in the cloud. They are:

- Concern 1: Physical security

As with on-premises solutions, cloud relies on physical infrastructure, e.g. data center facilities and hardware. However, because of their scale, cloud providers use built-to-order data centers with physical protections and continuous monitoring that are not realistic for smaller solutions. Larger providers also have significant influence over supply chain security practices and can review hardware and firmware implementations in depth with their vendors.

- Concern 2: Data leakage

Multitenant environments may use the same physical infrastructure for workload compute, but architecture design can provide strong isolation between tenants. Moreover, most cloud providers provide encryption for data-at-rest and data-in-transit and are working on end-to-end encryption. This defense-in-depth strategy ensures that failures in one area can be covered by protections in another. Finally, tenant specific solutions, e.g. Active Directory, give extra layers of defense easily combined with hosting provider technologies.

- Concern 3: Malicious or ignorant tenants

Infrastructure hosting providers can pose serious issues if their extensive resources are used for external attacks, spam, etc. To prevent such misuse, providers implement best practices in secure defaults and least privilege,

greatly lowering the risk that new workloads will be infected in setup and configuration, and mitigating the risk that one tenant could interfere another except via usual Internet traffic.

- Concern 4: Co-mingled tenant data

Co-mingling of data, e.g. multiple tenants sharing an application stack, or cloud providers storing data from multiple tenants in same database table-spaces and backup tapes, both drive fear of data corruption or destruction. A solution is to fix providers' behavior via service level agreements and third party audits. Azure is a best practice example, with network access control and segregation, network filtering to prevent spoofed traffic, traffic flow policies on edge devices, restriction of inbound/outbound traffic through ports and protocols defined by the customer.

- Concern 5: Greater attack surface

Cloud environments may be seen to present a larger "attack surface", as a compromised physical machine usually has only one way to get at other machines, i.e. via the network, whilst a virtual machine might allow access to others in the same shared environment. However, virtual machines can match the physical machines by limiting their "channels out" and narrowing the attack surface of their virtualization software. Providers need to follow best practices, e.g. security by design. Indeed many providers create different tenants for development and production, giving additional network and storage isolation for customers.

- Concern 6: Access controls

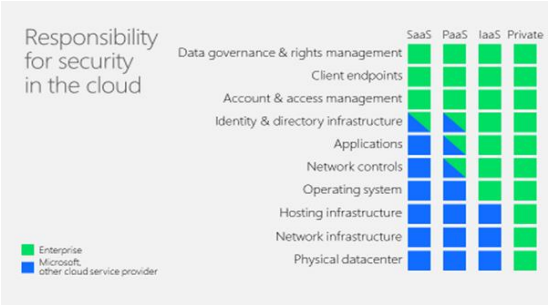
Data access and access policies in a distributed, virtualized, multitenant environment, are concerns, especially for the hypervisor. As with co-mingled data, service level agreements and third party audits can ensure transparency of access and clear separation of duties, e.g. via a least privilege and "just in time" policies, which are logged and which minimize access to just the resources and information needed for a specific task.

- Concern 7: Immaturity of monitoring solutions

Traditional monitoring tools focus on specific events within intra-host communications but this may not be applicable to cloud computing. Cloud computing empowers the tenant to monitor and log activities at the application layer, e.g. via Active Directory sign in and audit report, which can help catch unusual or suspicious sign-in activity.

While the techniques above mitigate risks inherent to a shared virtual environment, organizations should realize that virtualized solutions can be as secure as traditional on-premises options. Indeed, cloud can have significant security advantages. Physical proximity for maintenance (essentially on-site privileged access) can be minimized by remote system maintenance and incident handling. Moreover, cloud reimaging, a routine part of operations, can help clean out persistent and subtle compromises, e.g. malware infections, that might otherwise be hard to spot and address.

There is, however, no silver bullet for cloud security. The security controls appropriate for one implementation may not suit another, even within the same delivery model, and, as the graphic indicates, roles and responsibilities for security across implementations vary. Therefore, to realize cloud's enhanced security, organizations need to better understand how to operate security features and manage risks in their cloud solutions.



In conclusion, the cost-effectiveness and efficiency of virtualized and cloud solutions is real, and security concerns can be readily addressed. Organizations planning to harness the cloud must understand the environments they are creating and using, evaluating not only the security risks but the benefits of moving away from the traditional on-premise data center environment that until now they may have been used to.