What is different about cloud security

Article by Red Hat

Cloud security is the protection of data, applications, and infrastructures involved in cloud computing. Many aspects of security for cloud environments (whether it’s a public, private, or hybrid cloud) are the same as for any on-premise IT architecture.

High-level security concerns—like unauthorized data exposure and leaks, weak access controls, susceptibility to attacks, and availability disruptions—affect traditional IT and cloud systems alike. Like any computing environment, cloud security involves maintaining adequate preventative protections so you:

• Know that the data and systems are safe.

• Can see the current state of security.

• Know immediately if anything unusual happens.

• Can trace and respond to unexpected events.

Why cloud security is different

While many people understand the benefits of cloud computing, they’re equally deterred by the security threats. We get it. It’s hard to wrap your head around something that exists somewhere between amorphous resources sent through the internet and a physical server. It’s a dynamic

environment where things are always changing—like security threats. The thing is that, for the most part, cloud security is IT security. And once you understand the specific differences, the word "cloud" doesn't feel as insecure.

Dissolving perimeters

Security has a lot to do with access. Traditional environments usually control access using a perimeter security model. Cloud environments are highly connected, making it easier for traffic to bypass traditional perimeter defenses. Insecure application programming interfaces (APIs), weak identity and credentials management, account hijacks, and malicious insiders may pose threats to the system and data. Preventing unauthorized access in the cloud requires shifting to a data-centric approach. Encrypt the data. Strengthen the authorization process. Require strong passwords and 2 factor authentication. Build security into every level.

Everything is now in software

"Cloud" refers to the hosted resources delivered to a user via software. Cloud computing infrastructures—along with all the data being processed—are dynamic, scalable, and portable. Cloud security controls need to respond to environmental variables and accompany workloads and data while at rest and in transit, either as inherent parts of the workloads (e.g. encryption) or dynamically through a cloud management system and APIs. This helps to protect cloud environments from system corruption and data loss.
Sophisticated threat landscape

Sophisticated threats are anything that negatively impacts modern computing which—of course—includes the cloud. Increasingly sophisticated malware and other attacks like Advanced Persistent Threats (APTs) are designed to evade network defenses by targeting vulnerabilities in the computing stack. Data breaches can result in unauthorized information disclosure and data tampering. There's no clear solution to these threats, except that it's your responsibility to stay on top of the cloud security practices that are evolving to keep up with threats.

Cloud security is a shared responsibility

Regardless of what cloud deployment you're using, you're responsible for securing your own space within that cloud. Using a cloud maintained by someone else doesn't mean you can—or should—sit back and relax. Insufficient due diligence is a major cause of security failures. Cloud security is everyone's responsibility, and that includes:

• Using trusted software
What's inside your cloud matters. As with any code you download from an external source, you need to know where the packages originally came from, who build them, and if there's malicious code inside them. Obtain software from known, trusted sources and ensure that mechanisms are in place to provide and install updates in a timely way.

• Understanding compliance
Personal, financial and other sensitive data may be subject to strict compliance regulations. The laws very depending on where (and with whom) you do business – for example, see the European Union's General Data Protection Regulation (GDPR). Check your compliance requirements before choosing a cloud deployment.

• Managing lifecycles
Cloud-native environments make it easy to spin up new instances-and it's also easy to forget about the old ones. Neglected instances can become cloud zombies-active but unmonitored. These

abandoned instances can become outdate quickly, which means no new security patches. Lifecycle management and governance policies can help.

• Considering portability
Can you easily move your workloads to another cloud? Service-level agreements (SLA) should clearly defined when and how the cloud provider returns the customer's data or applications. Even if you don't foresee moving things soon, it's likely a future scenario. Prevent future lock-in concerns by considering portability now.

• Continuous monitoring
Monitoring what's going on in your workspaces can help you avoid – or at least inhibit the effect of – security breaches. A unified cloud management platform can help you monitor every resource in every environment.

• Choosing the right people
Hire and partner with qualified, trustworthy people who understand the complexities of cloud security. Sometimes, a public cloud's infrastructure may be more secure than a particular organization's private cloud, because the public cloud provider has a better informed and equipped security team.

Are public clouds secure?

Ok. Let's talk about it. We could tell you all about the security differences between the 3 cloud deployments—public, private, and hybrid—but we know what you're really wondering: "Are public clouds secure?" Well, it depends.

Public clouds are appropriately secure for many types of workloads, but aren't right for everything, largely because they lack the isolation of private clouds. Public clouds support multitenancy, meaning you rent computing power (or storage space) from the cloud provider alongside other "tenants". Each tenant signs an SLA with the cloud provider that documents who's responsible and liable for what. It's a lot like leasing a physical space from a landlord. The landlord (cloud provider) promises to maintain the building (cloud infrastructure), hold the keys (access), and generally stay out of the tenant's way (privacy). In return, the tenant promises not to do anything (e.g. run unsecured applications) that would corrupt the integrity of the building or bother other tenants. But you can't choose your neighbors, and it's possible to end up with a neighbor who lets in something harmful. While the cloud provider's infrastructure security team is watching for unusual events, stealthy or aggressive threats—like malicious distributed denial-of-service (DDoS) attacks—can still negatively affect other tenants.

Fortunately, there are some industry-accepted security standards, regulations, and control frameworks like the Cloud Controls Matrix from the Cloud Security Alliance. You can also isolate yourself in a multi-tenant environment by deploying additional security measures (like encryption and DDoS mitigation techniques) that protect workloads from a compromised infrastructure. If that's not enough, you can release cloud access security brokers to monitor activity and enforce security policies for low-risk enterprise functions. Though all this may not be sufficient for industries that operate under strict privacy, security, and compliance regulations.

Mitigate risk with hybrid cloud

Security decisions have much to do with risk tolerance and cost-benefit analysis. How could potential risks and benefits affect the overall health of your organization? What matters most? Not

every workload demands the highest level of encryption and security. Think about it like this: Locking your home keeps all your belongings relatively secure, but you might still lock your valuables in a safe. It’s good to have options.

That’s why more enterprises are turning to hybrid clouds, which give you the best of all the clouds. A hybrid cloud is a combination of 2 or more interconnected cloud environments—public or private.

Hybrid clouds let you choose where to place workloads and data based on compliance, audit, policy, or security requirements—protecting particularly sensitive workloads on a private cloud, while operating less-sensitive workloads in the public cloud. There are some unique hybrid cloud security challenges (like data migration, increased complexity, and a larger attack surface), but the presence of multiple environments can be one of the strongest defenses against security risks.