Don't **Rule** Out the **Cloud**.

We break down the layers of security your cloud provider should be using.

BriteSky.ca

CLOUD SECURITY MYTHS

BriteSky.ca

BriteSky Enterprise Cloud Provider™

The cloud has been getting a lot of heat lately, and the recent hacks on celebrity mobile clouds have only been adding fuel to the cloud security debate. Headlines read something like this: More Than 100 Celebrities Hacked, Nude Photos Leaked and Apple Boosts iCloud Security Measures after Celebrity Photo Hacks. But how much was Apple and their iCloud service at fault?

In reality, the so-called "breakdown of the cloud" was actually a phishing attack that involved users clicking on fraudulent messages that masqueraded as trustworthy, legitimate sources.

These hoax messages tricked users into disclosing personal information, such as Apple IDs, passwords, and security questions, in order to steal identities or – in the case of the unfortunate celebrities – sensitive data stored on their personal iClouds. In the end, the cloud wasn't hacked, but the users' personal account information was compromised by their own actions.

From this debacle, a question arose: Is the cloud safe? The answer is simple: It all depends on the cloud provider you choose to store and safeguard your data.

Let's dive into the characteristics that make up a secure cloud.

THE TRUTH ABOUT CLOUD SECURITY

BriteSky.ca

BriteSky Enterprise Cloud Provider™

Clouds can be vulnerable in many ways – just like there are ways a house can be vulnerable to attacks. If the walls of a house are flimsy, then it's easy for a burglar to enter. The same can be said about cloud architectures.

Cloud data centers that are built from the ground up with security in mind are going to be more secure than companies that layer software to protect against the risks caused by allowing routing between services. Secure cloud data centers don't need to rely on software as their main protection. Instead, security is built directly into the architecture. The key is separation of data.

IBM, Microsoft, and the top 50 organizations in the U.S. and Canada have built some of the most secure cloud infrastructures using security zones to store data. This separation helps to migrate the effects of denial of service attacks, which can easily take down or infect large data pools and – in extreme cases – an entire infrastructure. Downtime, data loss, malicious infections, and other vulnerabilities can arise from denial of service attacks.

Large cloud providers are most at risk for denial of service attacks, but with the separation that security zones offer, these attacks are limited to affecting only small areas of an infrastructure. As a result, these threats can easily be quarantined and mitigated. It is also a better, more scalable, and more private approach to cloud architectures.

SECURITY YOU SHOULD LOOK FOR IN A CLOUD PROVIDER

BriteSky.ca

BriteSky Enterprise Cloud Provider™

Here are a few things your next cloud provider should have to ensure the security of your applications and data:

Up-to-date, top-of-the-line, enterprise-grade equipment – Technology is always improving and crafting answers to new problems that sprout every day. Working with a cloud provider that is dedicated to keeping pace with these innovations helps your company ensure security and competitiveness in the marketplace.

A layered architecture – Layered cloud architectures offer more customization options for companies looking to build a unique solution. Layers allow companies to add additional firewalls, encryption, load-balancing applications, rule-based traffic restrictions, and more.

Separation of data – Sectioned security zones control data separation and prevent against denial of service attacks, as well as the spreading of other malicious programs. The ability of a cloud provider to quarantine and mitigate risks without suffering downtime is critical to maintaining your organization's operations and data security.

Same portal access – When it comes to virtualizing in the cloud, working with a service provider that is hypervisor-agnostic may seem like the ultimate goal for man companies. Although hypervisor-agnostic abilities helps organizations streamline applications into the cloud and avoid additional migrations, companies should still expect cloud providers to go a step further. With same portal access, it doesn't matter how many hypervisors your company uses. Your business will still access the cloud from the same point. This limits the number of access points to your cloud environment, which bolsters security.

THE BRITESKY CLOUD DIFFERENCE

BriteSky
Enterprise Cloud Provider™

Built with a ground-up approach and enterprise-grade security, the BriteSky cloud data center has a number of unique components that stand out against competing cloud providers. First, the physical infrastructure is consistently updated and altered to utilize best-of-breed technologies. As a result, the cloud architecture is only going to be bigger, better, and stronger a year from now.

With a purpose-built architecture that functions like a private cloud, BriteSky's layered architecture makes it a very unique cloud environment compared to other cloud providers.

These separate layers include:

- Virtual storage
- Virtual networking
- Compute (the latest IBM servers)
- Virtualization (virtual data center)
- Security (virtual firewall)

All of those encapsulated layers form a virtual vault (or security zone) called a PODD – or Portable On-Demand Data Center. This architecture gives every company a separate, secure cloud environment and prevents denial of service attacks and other malicious threats.

With capacity for Exabytes of storage and up to 30,000 virtual machines, the BriteSky cloud also has the unique ability to morph itself into an environment that can meet specific client needs. With enhanced option layers, companies can customize their own cloud environments by adding extra security, encryption, access rules, and even added products.

With a collaborative mindset, the BriteSky team works with clients to ensure that the cloud solution chosen will meet their business goals and needs.

At the end of the day, companies need a reliable cloud provider that can lay out the specifics on how they protect their cloud environments – and your data.

To learn more about BriteSky's enterprise-grade cloud services and secure, home-built data center, reach out to one of our experts today.

BriteSky
Enterprise Cloud Provider™

120 Iber Road Suite 106 Ottawa, ON K2S 1E9
855.336.3700

BriteSky.ca