Cloud vs On-premise Security

Have you ever wondered if public clouds are as secure as on-premise IT? Or, have you wondered if you could even use the public cloud for your compliant workloads?

It is understandable that there is a lot of uncertainty when you're considering a move to the cloud. This blog looks at some common concerns and myths that we hear on a regular basis and explores the truth behind those concerns.

MYTH: Public clouds aren't as secure as on-premise IT.

FACT: BIOS's Cloud offering, CloudHPT, takes a multi-layered approach to cloud security. Our approach tackles foundational, physical, logical and application and data security.

Any cloud provider who tells you to simply buy a product in order to achieve security in your environment probably doesn't understand security or have a business unit specifically focused on it.

We understand that security is an ongoing process that requires a true partnership between the client and provider. There are four broad levels of security controls that our highly skilled team supports to reduce your risks and vulnerabilities.

We focus on:

- **Foundational Security** with security policies, ISO 27001, contractual agreements, external penetration testing, security controls governance, awareness training and background checks
- **Physical Security** with datacenter security, physical access control and site audits
- **Logical Security** with advanced firewalls, Malware detection, Security Incident & event Monitoring (SEIM), CISCO ACI network security, Hypervisor-level security and patch management.
- **Application and Data Security** with solutions for end user management and individual application and database security.

CloudHPT is housed in some of the most secure datacenters in the Middle East. We are located in Tier 3 and Tier X Datacenters in geographically separated, redundant locations and are SSAE Type II SOC 2 certified.

MYTH: "My data is comingled with other users' data in a public cloud"

FACT: CloudHPT does not comingle any data or environments between users.

This is one of the most common concerns we hear about public cloud, and it's one we take seriously. While some Software-as-a-Service applications do comingle data from all providers in order to pull business analytics from data, CloudHPT does not. All clients are containerized. This container extends from the Firewalls, down through the network, into compute and down into storage. We do this using Cisco ACI, it is not the cheapest way to do this but it is the best and most secure. This is why CloudHPT is a premium service. In addition, your data can be encrypted at-rest, and in-flight, and resides in your own personal, protected virtual datacenter.

MYTH: "I can't use the public cloud for my compliant workload"

FACT: CloudHPT can be used as a secure, compliant hosting and recovery environment for medical companies, hospitals, labs, financial institutions, universities and ecommerce applications, all of which have strict compliance requirements in terms of security, protection and reliability. We have house hold brands running on all these services.

We work with each client individually to ensure compliance needs are met through architecture and with the addition of managed services. We also focus on collaboration to ensure each side knows its roles, responsibilities as it relates to achieving your compliance objectives.

In case your applications have specific requirements that means they must have a dedicated infrastructure, BIOS can tailor a private cloud to your needs that will still help you achieve the benefits of cloud. We call this solution Datacenter 3.0