ignitec

CLOUD SECURITY

Organizations need to prioritize a “cloud first” approach to enable them to transform with agility at scale. But, as its name suggests, every new instance of public cloud has the potential to brew up a security storm. The native/default settings for a new cloud instance are unlikely to satisfy even the basic security requirements of any business operation.

While cloud offers new opportunities to modernize services and transform operations, Security and compliance risk remains the greatest barrier to cloud adoption. Combined with the difficulties in proactively addressing the complexity of secure configuration and a shortage of skills, these challenges can be major roadblocks to a cloud-first journey.

Security is often seen as the biggest inhibitor to a cloud-first journey—but we enable it to be its biggest accelerator.

Traditional Security Tools & Solutions Don’t Work In The Cloud

- Lack of Perimeter to protect
- Traditional security needs to move & adapt at the ever-increasing speed of Cloud.
- Unable to provide visibility adding to confusion & misconfigurations.
- No adherence to Industry regulations while organization constantly evolves & adopts first-to-market approach.

While cloud-based computing delivers overall cost benefits, the security piece of that puzzle can eat into the ROI, as there are so many pieces that need to be managed – microservices, containers, Kubernetes, serverless functions, etc. The infamous cybersecurity skills gap is highly relevant here, as new technologies are rolling out faster than enterprises can find security professionals who have experience working for them.

A Cloud first security architecture can help organisations to achieve the following:

- Fast: With cloud service provider (CSP)-native accelerators that enable security capabilities and controls to be deployed in minutes or hours, rather than months.
- Frictionless: With security embedded in existing solutions, business processes, and operational teams.
- Scalable: With automation and self-healing processes applied to reduce manual steps and break the resourcing model of adding headcount to enable organizations to scale.
- Proactive: With pre-emptive controls established to block accidental or malicious security incidents from happening in the first place.
- Cost effective: Bake-in security from the outset to avoid the additional costs incurred by having to re-do work.

How Ignitec can help:

- ✓ **Continuously monitor and assess Industry regulatory compliances**
- ✓ **Continuous compliance validation will help in detecting and resolving compliance violations by utilizing Cloudbots**
- ✓ **Automate Cloud Native Security**
- ✓ **Visualize cloud Infrastructure**
- ✓ **Identify how new assets are inter-connected and what policies or traffic routes to deploy**
- ✓ **Manage incident response**
- ✓ **Centrally review how threats are being detected, quarantined, and remediated.**
- ✓ **Employ Identity Access Management**
- ✓ **On-time access helps avoid misuse of privileges by conjoining authentication with authorization.**
- ✓ **Deployment to cloud assets in designated region to ensure adherence to compliance and local data residency laws.**

www.ignitecinc.com **sales@ignitecinc.com** **+1 (571) 429-4300**