Cybercriminals in the Cloud: Rise of Cloud Security Issues

In the wake of the COVID-19 pandemic, organizations and IT leaders had to shift to work from home. To empower the remote workforce, business leaders opted for tech solutions that were buoyant and agile.
To maintain the seamless model of the business, workload, and continuity of plans, organizations in the remote work culture companies had to adopt the cloud. As per Gartner, organizations spending money on cloud services will grow from 21.7% and hit the whopping amount of $482 billion in 2022. This means that enterprises rely on cloud infrastructure to accelerate the business game.

Why is cloud security important in 2022?

No matter how flexible and productive cloud adoption seems, it has made businesses vulnerable to data breaches and cyber threats. According to a recent survey by IDC, 79% of the organizations have experienced at least one cloud data breach in the course of the past 18 months. A recent study by a credible source bears that data breaches in work from home culture have cost the companies an average of $3.61 million.
According to one of the other credible sources, 28% of the vital spending in IT organizations will migrate to the cloud in 2022, which will affect $1.3 trillion IT spending. In response to the forecasts mentioned above, business leaders need to pay attention to securing cloud-based services. However, cloud consulting services are one of the best ways to prevent cloud attacks.
All the speculations raise a pressing question. What will be the strategies the business and agency leaders need to commit their cyber security expenditure to 2022? To create effective cloud security strategies, business leaders need to watch over these three trends over the coming year.

- **Include cyber security mesh in your new approach**

Cybersecurity Mesh is a modern approach to secure the security architecture that allows the companies to deploy and extend the security where it is most needed. Cybersecurity mesh will be one of the most brilliant defensive approaches to secure the encapsulated data.

- **Zero trust will pick up the speed**

Zero trust is jargon that has become a threat to business leaders. An uninterrupted and consistent security policy guards the resources and data become a fundamental principle to protect the cloud infrastructure. So take initiatives that leverage the zero trust architecture to keep catching on with the organizations.

Read More: Cybercriminals in the Cloud: Rise of Cloud Security Issues