As more **organizations adopt cloud** to leverage advantages like better scalability, more efficiency, and faster deployments, the cybersecurity pros remain concerned about security of data, systems and services. The cybersecurity teams are looking for new strategies as traditional security tools don't fit for cloud environments.

According to 2018 Cloud Security Spotlight report, 90% of cybersecurity professionals are concerned about cloud security, up 11% from a year before.

Alert Logic and Cybersecurity Insiders surveyed 400,000-member Information Security Community on LinkedIn to explore how organizations are responding to cloud security challenges, what are their biggest cloud security challenges, etc.

Below are some of the key findings of Cloud Security Spotlight report:

- **Top cloud security concerns**

18% of the respondents indicated at least one security incident in last 12 months, representing a significant rise in one year.

Protecting cloud against data loss and leakage (67%) is the biggest concern for cybersecurity pros, followed by threats to data privacy (61%), and breaches of confidentiality (53%).

- **Top challenges to cloud security**

Organizations are migrating more of their workloads to cloud, which is increasing the **challenges for security pros** to protect workloads.

As per the report, the top four cloud security challenges included visibility into infrastructure security (43%), compliance (38%), setting security policies (35%), and security not keeping up with the pace of change in applications (35%)

- **Top threats to cloud security**

Misconfiguration of cloud platform (62%) is the biggest threat to cloud security, followed by unauthorized access using employee credentials (55%), insecure interfaces or APIs (50%), and hacking of accounts, services or traffic (47%).

- **Security risk: Cloud vs On-premises**

Almost half of the respondents said that **public clouds** are at higher risk to cyberattacks as compared to traditional on-premises environments.

On the other hand, only 17% indicated that public clouds are less risky to security breaches than the on-premises environments.

- **Solutions to boost the security of cloud**

The organizations need to understand that the same traditional network security tools are not going to work when adopting cloud and hosting applications there.

Majority of organizations (84%) believed that traditional security services and tools either have limited functionality or don’t even work in cloud environments.

On the other hand, only 16% respondents believed that traditional security tools can be used to manage cloud security.

- **Advantages of cloud-based security solutions**

According to report, faster time to deployment (47%) and cost savings (47%) are the biggest advantages of cloud-based security solutions.

The other advantages of these solutions included secure access to apps from anywhere, reduced efforts to patch and upgrade software, better compliance, and better insights into user activity.

- **Barriers to adoption of cloud-based security solutions**

The **report** found that the biggest barriers to cloud-based security solutions are people and processes, rather than the technology.

Respondents cited staff expertise and training (56%), data privacy concerns (41%), and lack of integration with on-premises technology (37%) as the top roadblocks to cloud-based security adoption.

- **Most effective technologies to secure data in cloud**

Respondents said that data encryption (64%) and network encryption (54%) technologies are that most effective security technologies, followed by security information and event management (52%).

More than half of the organizations believed that trained cloud security professionals can also help in securing the cloud.

Also read: Cryptojacking becoming a serious emerging threat to businesses: Cloud Security Trends report

.