LTIMindtree

ARTICLE

5 Cloud security trends to watch out for in 2023

Modern-day organizations are harnessing the cloud to stay relevant, manage the business better, and offer better services. This has also enabled remote work, hybrid work culture, and multiple-device access, which requires organizations to allow access to employees working away from offices. The rise in the number of businesses adopting cloud platforms and such a work culture has led to the need for security tools and services. Take a look at some cloud security trends which are likely dominate this and possibly shape this market.

1. Zero Trust Network Access

Zero Trust is a security model that constantly validates all users, inside or outside the organization's network, each time they are given access to applications and data. It uses robust authentication methods before allowing access to users, whether on a local network or cloud. This kind of secure access reduces the use of VPN by remote workers, and with its growing popularity, it is being used in case of those working from the office. It is suitable for securing modern-day cloud-based work environment against unauthorized access and ransomware threats. **Gartner** predicts that by 2023, 31% of organizations will invest in Zero Trust protection.

2. Security through DevSecOps

Development, security, and operations, or DevSecOps, is a practice that incorporates security at every stage of software development, right from design through delivery. Using DevSecOps solutions during cloud deployment enhances scalability, speed, round-the-clock service, speed, and security. It also cuts the costs and time spent on fixes post the delivery. A DevSecOps **market report** predicts a CAGR of 31.2% during the period 2018 to 2023, which would amount to $5.9 million USD by 2023.

3. Multi-cloud security

Organizations employ workloads across multiple cloud platforms, including private and public ones, to expand capabilities, enhance productivity, and make operations more efficient. This strategy reduces the organizations' dependency on a single ecosystem, manages costs, and makes the systems more resilient. Distributing workloads across multiple cloud environments calls for multi-cloud security to protect data, assets, and applications from potential security threats or attacks. The growth of the multi-cloud security market will go hand in hand with the **multi-cloud management market,** which is expected to grow up to 49,894 million USD by 2030.

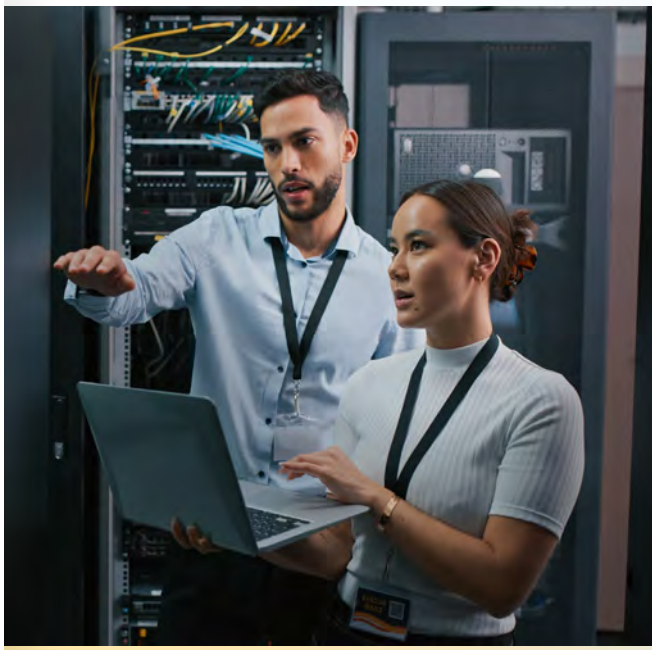
4. AI/ML for cloud security

The surge in the adoption of cloud platforms has led to increasing investments in cloud security. With artificial intelligence and machine learning, organizations can conduct real-time analysis and detect threats, greatly enhancing security initiatives and even limiting or eliminating human intervention. As observed by the Ponemon Institute, employing AI and automation reduced spending on breaches by USD 3.05 million, which was 62.5% lower and by far the largest amount saved.

The systems used for monitoring and security usually produce huge amounts of data, which can be analyzed to detect and predict threats. However, going through all the data may be a daunting task for humans, but it can be done easily with AI and ML. The learning may even help predict incidents early, which may help take steps to block potential threats. AI and ML cannot replace humans entirely. Still, these tools carry out base-level tasks of identifying threats, reduce a lot of manual labor and enable security professionals to work on more critical threats and solutions for identifying and mitigating cyber threats.

5. Evolution of CISO

A Chief Information Security Officer (CISO) is responsible for developing an organization's security policies and ensuring appropriate implementation and enforcement. The responsibilities of a CISO include handling security operations, evaluating cyber risks and helping the board understand the potential threats. They are also responsible for formulating policies and processes for preventing data loss/fraud, creating a security architecture, implementing programs to minimize risks, and ensuring all the security initiatives run smoothly. In case of a breach, a CISO is involved in investigating incidents, Businesses undergoing a digital transformation require the expertise of a CISO to accelerate the process and secure their supply chains and access by remote and hybrid workforces.



In a nutshell

Gartner forecasts an 11.3% growth in cloud security, which means a total spending of USD 188.3 billion in the year 2023. In this context, organizations will adopt and adapt to multiple cloud security trends to secure their businesses from an ever expanding cyber security threat surface.

About LTIMindtree

LTIMindtree is a global technology consulting and digital solutions company that enables enterprises across industries to reimagine business models, accelerate innovation, and maximize growth by harnessing digital technologies. As a digital transformation partner to more than 750 clients, LTIMindtree brings extensive domain and technology expertise to help drive superior competitive differentiation, customer experiences, and business outcomes in a converging world. Powered by nearly 90,000 talented and entrepreneurial professionals across more than 30 countries, LTIMindtree — a Larsen & Toubro Group company — combines the industry-acclaimed strengths of erstwhile Larsen and Toubro Infotech and Mindtree in solving the most complex business challenges and delivering transformation at scale. For more information, please visit www.ltimindtree.com.