TOP 5 CLOUD SECURITY TRENDS FOR 2021

Cloud computing is often perceived as a convoluted term. There's a classification of public, private, and hybrid clouds, delivery models of software, platform, and infrastructure as-a-Service, and then an ever-growing list of technologies using some variations of cloud classifications and as-a-Service delivery models.

It's often hard to keep up with the opportunities surrounding every different and new innovation that hits the market. It's even more difficult to stay on top of the current challenges—particularly the security issues facing the variety of cloud computing solutions available in the market.

In this article, we will cover the top challenges and trends in cloud security in 2020 and the coming years.

1. Ransomware, cybercrime & cloud security

Cloud computing enables anytime, anywhere access of information from centralized datacenter repositories. The underlying resources are not always controlled by the customers and vendors are responsible for managing vulnerabilities. On the other hand, users of cloud computing are expected to keep data safe against cyber threats such as ransomware that use social engineering ploys to access and control sensitive data stored in data centers.

Two factors have contributed to cloud data centers becoming popular targets of ransomware and crypto-mining:

- Lack of security awareness among users
- Inadequate visibility and control into cloud infrastructure

These damages cost the U.S. $7.5 billion in 2019, compromising government agencies, schools, healthcare institutions, and SMB firms using cloud-based data storage solutions.

Cloud computing exposes data on three fronts:

- **Data at rest**: data stored in data centers
- **Data in transition**: data transfer across the network
- **Data in use**: data processed in servers locally or in the cloud

Prediction: To reduce the risk of data leaks and ransomware attacks, organizations must manage data access and enable end-to-end encryption.

2. Lack of cyber laws, consensus & privacy awareness

Governments around the world have called for stringent measures that guarantee cloud security for business customers and end-users. The 2018 UNESCO Internet Governance Forum event is one example, but a global or regional consensus remains rare. Security, access violations, intellectual property rights, and resilience against cyberthreats is perceived differently across the world, so global companies are forced to comply with diverse regulations accordingly.

Uncertainty and diversity affect cloud security even more, due to the geographic diversity of data center locations and the users accessing them. Furthermore, privacy awareness among users drives demand for transparency, whereas customers of cloud computing resources may have only limited visibility into the underlying security performance of the cloud infrastructure.

From the perspective of business organizations, this trend means that cloud security, government regulations, and end-user privacy will play an important part of the IT strategy and investments. Business organizations in the E.U. have already spent $9 billion to prepare for the GDPR regulation and employed 500,000 data protection officers.

Prediction: Global organizations will likely soon require increasingly stringent cloud security measures in response to

- Upcoming security regulations
- Increasing security and privacy awareness among end users
- The growing cybercrime risk

3. DevSecOps and SDLC in the cloud

DevOps is growing in popularity as an SDLC framework that enables rapid releases of high-quality software products with lower risk and waste processes. DevOps adoption requires automation and infrastructure management solutions delivered as a cloud service. The process itself must be simultaneously fast and secure.

The approach of integrating and automating security tasks within the SDLC process is called DevSecOps, where the people and technology involved in the pipeline actively contribute to the full lifecycle of the software products. Security must be integrated within the process itself, and not as an additional layer of checklist items that can be automated.

Prediction: In terms of cloud computing, security policies must be developed for every stage of the SDLC pipeline to protect the infrastructure environment and data. For SDLC of cloud-based software products, DevSecOps extends to the app functionality and the underlying cloud resources that power the app. Both functionality and security of the app is tested and improved continuously during the SDLC. (Similarly, vulnerabilities, security challenges, and regulatory issues applicable to those cloud resources such as containers and microservices are already a part of the SDLC strategy.)

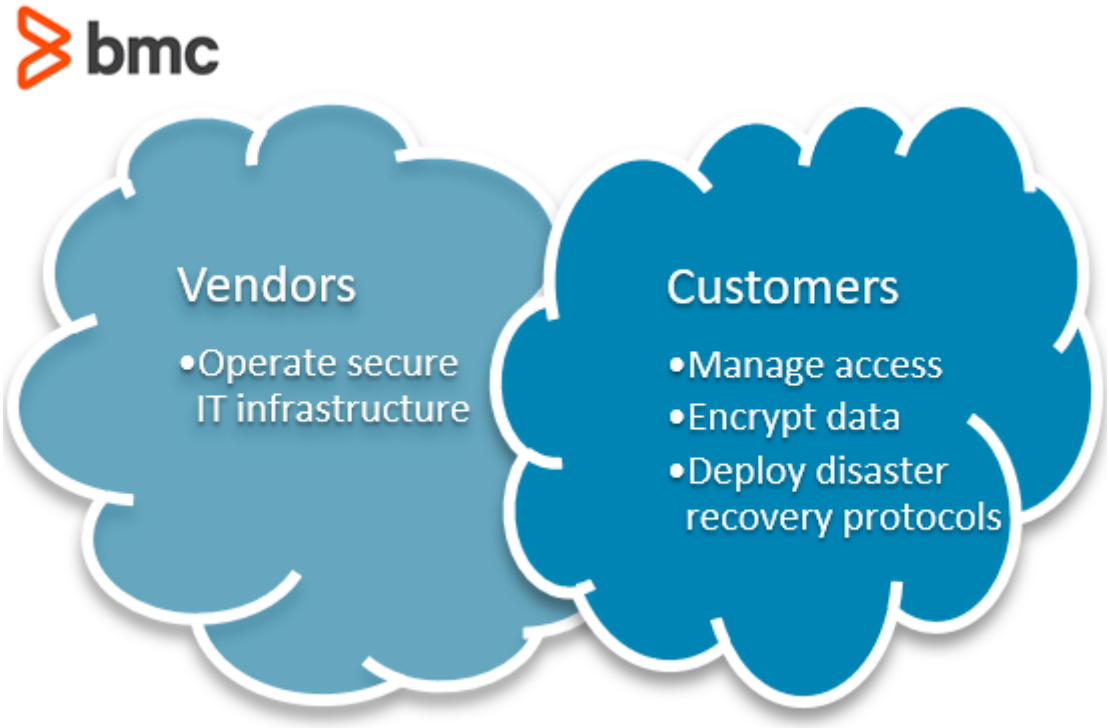
4. Cloud security investments & industry trends

The (public) cloud computing industry is expected to grow by 17% YOY to reach the $266.4 billion mark in 2020, among other cloud trends. The global cloud security industry is following a similar growth trend, increasing by 23.5% CAGR to reach the $8.9 billion mark by the end of this year. Global events have reshaped the way technology companies work, with further increased cloud adoption—and the associated underlying security risks.

According to McAfee, enterprise use of cloud solutions increased by 50% between January and April 2020. At the same time, external threat actors increased by 630%. The report also points to cloud-native security considerations as critical for enterprise workloads operating in the cloud. In response, certain tasks must be automated, such as:

- Cloud security administration
- Configuration management
- Other manual processes

Prediction: Organizations must carefully understand and follow the shared cloud security responsibility model: vendors are responsible for operating a secure IT infrastructure, while customers are responsible for managing access, encryption, and disaster recovery protocols.



Shared cloud responsibility model

5. AI as a Solution?

Of course, automation alone is not sufficient to combat the security risks associated with cloud computing. Business operations in the enterprises and software products operating from the cloud are largely data driven. Automated configuration management and infrastructure operation changes must account for contextual behavior of the IT environment and business requirements. This is where intelligence plays a key role and technologies such as AIOps are becoming increasingly popular in the ITSM space driven by cloud computing and security challenges.

Prediction: Moving forward, security efficiency will be defined by the organization's ability to proactively identify anomalous behavior of workloads and data in the cloud. Real-time decision making will be largely driven by AI technologies. And while the underlying algorithms and technologies will require expensive cloud computing resources to work, the ITSM process and cloud operations from the perspective of IT users will be simplified, well-informed, and driven by insightful metrics instead of raw data.

Additional resources

For more information on clouds and cloud security, explore the BMC Multi-Cloud Blog and these resources:

- How to Secure Your Public Cloud
- 3 Tips for Effective Cloud Security
- How to Prevent Cloud Configuration Security Vulnerabilities
- 5 Ways Multi-Cloud Discovery Can Enhance IT Security

Listen to the podcast:

Run & Reinvent Podcast · Episode 2: Cloud Security and How Self-Driving Remediation Helps Businesses Reduce Vulnerability