aws small and medium business

AMAZON WEB SERVICES

How AWS cloud provides data security for companies of all sizes

The imperative to protect data and maintain compliance

An essential part of operating a thriving business is mitigating existing and emerging security threats. By identifying and addressing potential gaps in data security, companies of all sizes can take steps to protect customer data, safeguard intellectual property (IP), and maintain compliance. Business data breaches increased by almost 20%[1] in 2021, so a focus on data security is a business imperative.

Adopting cloud-based tools with Amazon Web Services gives companies automated and built-in solutions for network and data security, configuration management, access controls, monitoring, and visibility. And, AWS is designed to be secure without the capital outlay and the operational overhead of a traditional data center. As your business grows, AWS cloud can provide secure scalability. AWS capacity can increase when you need it and decrease when you don’t. Your company pays only for what you use.

Here are three real-world examples of businesses that migrated to AWS cloud to better protect their companies and reach business objectives.

AWS Customer: TNEX

Mobile bank improves security as it grows

TNEX launched in late 2020 as Vietnam's first mobile bank for retail consumers and small merchants. Its consumer app has lifestyle functions, like daily step and mood tracking, and chat. The embedded personal financial management features are emoji-driven and easy to use for money transfers, bill payment, and other financial tasks. A separate app and banking system for small and medium-sized business merchants includes free website creation, invoicing, inventory, and campaign management.

The company was on target to register 250,000 retail and 20,000 business customers by the end of 2021 and knew it needed to help verify that sensitive data was segmented, controlled, and encrypted. Strong security is important to protect company and customer data and stay compliant with industry and government standards.

Creating an enhanced technology framework with resilience against cyberthreats is an essential reason TNEX designed its infrastructure on AWS. AWS and its partners helped the company create infrastructure that segregates applications and reduces the risk of a threat to one application impacting another. All customer and company data are also anonymized and tokenized — swapped out for a non-sensitive data placeholder — to help prevent a data breach. In addition, multiple layers of user authentication and encryption of all data, in transit or at rest within the company, provide a safeguard against unauthorized access to data.

AWS helped TNEX achieve its growth objectives with improved security by providing:

- Microservices and container orchestration using Amazon Elastic Container Service (Amazon ECS) to create infrastructure that isolates applications and segregates threats.
- Data monitoring in real time using Amazon CloudWatch and Amazon GuardDuty to detect network deviations that could indicate fraudulent activity.
- Segmenting and tracking of user activity using AWS Key Management Service (AWS KMS) to create and manage cryptographic keys to unlock encrypted data.
- Designation of security groups with AWS Web Application Firewall (AWS WAF) to segment applications and better protect each one from breaches that might occur in another.

AWS Customer: See-Mode

Healthcare company manages compliance in the cloud

See-Mode uses artificial intelligence (AI) and machine learning (ML) to predict risk factors of stroke by automating and improving medical image analysis. The company's software can accurately process 50-100 ultrasound images in seconds, freeing up clinicians to spend more time with patients. See-Mode works with hospitals and imaging centers in multiple international locations, including Australia, Europe, Singapore, and the U.S. Its global success requires the company to manage security and privacy regulations in each location, including HIPAA in the U.S. and the General Data Protection Regulation (GDPR) in the EU.

By migrating to the cloud with AWS, See-Mode adhered to standards set by regulatory agencies around the globe, such as Australia's requirement that patient data be anonymized before leaving the country. A centralized platform for its entire cloud-based infrastructure provided a comprehensive view of its compliance status across all its networks.

AWS helped See-Mode handle its global compliance requirements by providing:

- Nearly continuous monitoring using Amazon GuardDuty to track user activity, and identify and mitigate threats each time the company's servers are accessed.
- Detailed server event histories using AWS CloudTrail to help with reports required for auditing to maintain compliance with global security regulations.

AWS Customer: Altium

Manufacturer provides enhanced security for dispersed global teams

Altium is a developer of a widely used printed circuit board (PCB) that designers, engineers, manufacturers, and suppliers rely on to create electronics. The company's Altium 365 product is cloud-based, so remote teams can collaborate from any device. During the pandemic, a globally distributed team used Altium 365 to quickly produce field emergency ventilators to offset the strain on the medical supply chain.

Security is a top priority for the company, since many different teams share huge amounts of valuable and proprietary IP. By migrating to the cloud with AWS, Altium now has infrastructure that keeps every customer's workstream isolated in the database and routinely backed up.

AWS helped Altium improve the security of global collaboration by providing:

- Infrastructure built with a separate database for each customer using Amazon Relational Database Service (Amazon RDS) to provide a hardened separation of customer data and protection from one application's data impacting another.
- Multiple, automated, daily backups based on the separation created using Amazon RDS to enable the security of customer data.
- Improved security and resizable compute capacity using Amazon Elastic Compute Cloud (Amazon EC2) to maintain high performance and availability from many locations and devices.

After migrating to the cloud, businesses reported a 43% reduction in annual security incidents, according to Nucleus Research.[2] Adopting cloud-based tools with AWS is good for security and for reaching business objectives. Without the distraction of security disruptions, or the investment of a traditional data center, companies can focus their attention and resources on ambitious goals.

Ready to get started?

Contact AWS to find out how migrating to the cloud with AWS can address your company's specific security needs.

[1] Identity Threat Resource Center, "Number of All Data Breaches in 2021 Surpasse All of 2020," www.idtheftcenter.org/identity-theft-resource-center-to-share-latest-data-breach-analysis-with-u-s-senate-commerce-committee-number-of-data-breaches-in-2021-surpasses-all-of-2020/

[2] Nucleus Research, "Deep Learning on AWS," https://pages.awscloud.com/hk-nucleus-deep-learning.html