Meghan S. Everard

From: Kurt Danilson from Streamline <support@getstreamline.com>
Sent: Monday, October 14, 2024 12:35 PM
To: Meghan S. Everard
Subject: Cyber Security

Follow Up Flag: Follow up
Flag Status: Flagged

Hello Meghan,

We use AWS to store our website data. Below is an overview of the protection AWS provides:

AWS (Amazon Web Services) is considered highly secure, offering world-class cybersecurity features. Here's a quick overview of how AWS maintains strong security:

1. **Global Infrastructure and Data Centers**
AWS data centers are monitored 24/7 with physical access controls like biometric scanners and video surveillance.
Redundancy is built into its infrastructure to ensure availability and disaster recovery.

2. **Compliance and Certifications**
AWS complies with major security frameworks like ISO 27001, SOC 1/2/3, HIPAA, FedRAMP, and GDPR, proving that it meets strict security and data privacy requirements.

3. **Encryption and Access Control**
Encryption: Data can be encrypted in transit (using TLS) and at rest with AWS KMS (Key Management Service).
Identity and Access Management (IAM): Allows organizations to enforce fine-grained access policies, ensuring users only access the resources they need.

4. **Network Security**
AWS offers tools like VPC (Virtual Private Cloud) and firewalls for segmenting networks and controlling traffic.
DDoS Protection: Services like AWS Shield defend against Distributed Denial-of-Service (DDoS) attacks.

5. **Monitoring and Threat Detection**
Tools like Amazon GuardDuty and CloudTrail provide continuous monitoring for malicious activities and logging of events.
AWS Security Hub consolidates security alerts from multiple services for proactive monitoring.

Does this help? Let us know if you have any additional questions or concerns!

Your Ticket #4126881589

Kurt Danilson
Streamline Support

(916) 238-1811