




TLS
We use TLS for our network security, which is a cryptographic protocol that provides privacy, authentication and data integrity.



HTTP HTTPS
We use Extended Validation SSL certificates, which protect users from providing their details to fake websites.

ENCRYPTION AND AUTHENTICATION



We use the JWT authentication for securely transmitting, SHA-256 algorithm, a symmetric signing method for password security


SECURE PAYMENTS

DaySchedule uses Stripe for payment processing.

- Encrypted Data and Communication
- Money Transmitter Licenses



DDOS MITIGATION



We make sure that our sites are secure and customers' data is protected from DDOS.

We use rate limitation on all our API to prevent DDOS attacks.




DaySchedule utilizes AWS infrastructure for hosting, database and load-balancing across multiple regions. The AWS data center operations are certified by ISO 27001 and PCI, GDPR, and HIPAA

GDPR

We are fully compliant since the day we are operating. Our privacy, security policies are also streamlined with the GDPR goals.



FIREWALL PROTECTION



For network security, DaySchedule uses Security Groups which are the premier way to secure AWS EC2 instances, database and network

DaySchedule security is audited and approved by some of the major companies including Google, Microsoft, Zoom etc. in app approval process

