

Boston Dynamics values your security. Spot has the following security measures in place which are designed to keep your data and access safe.

## ROBOT SECURITY

### DATA ENCRYPTION

Onboard Storage	All user data encrypted with military-grade encryption. Owner has complete control over data access.
Stored Data	Logs and sensor data encrypted at rest by default.
API and Web Requests	All connections encrypted and authenticated using industry standard techniques (TLS 1.2+) and modern cipher suites.
Certificate Verification	HSM-backed private root.

### AUTHENTICATION AND AUTHORIZATION

API and Web	Access requires an authenticated authorized user.
Login Info	Login attempts rate-limited.
Account Management	Owners can add, remove, and manage multiple user accounts.
Account Types	Accounts can be the administrator or restricted operators.
Default Passwords	Robot ships with unique random passwords. Account password complexity requirements enforced.
Session Tokens	Modern web security practices.
Networking	Robot fully operational without internet access.

### FIRMWARE

Software Updates	Digitally signed by Boston Dynamics. User completely controls upgrade.
Patching	Components updated at all main release points. Security point releases if needed.
Security Audits	Multiple audits with third-party vendor.
Trusted Software	Robot uses well-trusted, well-maintained modern web backend components.

### TABLET

Security Audits	Audited by respected third-party security specialists.
Operating System	Tablet runs Android 8.1 which is maintained by Google.