Spot Security

Boston Dynamics values your security. The following Spot security measures are designed to keep your data and access safe.

Data Security

Onboard Storage: All user and mission data encrypted at-rest with AES encryption. The disk encryption key is bound to the robot's Trusted Platform Module (TPM) and will not be unsealed if Secure Boot fails.
Secure Boot: Discrete TPM used to detect tampering with on-robot platform software.
Downloadable Logs: Service logs encrypted to Boston Dynamics with XChaCha20-Poly1305.
API and Web Interface: All endpoints require use of TLS 1.2 or later and use of cipher suites offering 128-bits of security or higher.
TLS Public Key Infrastructure: TLS endpoints rooted to an HSM-backed private Certificate Authority.
WiFi Security: WPA2-PSK, with support for some WPA2-Enterprise 802.1x methods. See the Boston Dynamics Support Center for more information.
Network Ports: 443/TCP (additional ports may be required for various Spot payloads).
Air Gap Ready: Robot fully operational without internet access. Even on-board WiFi can be disabled in certain configurations.

Authentication and Authorization

API and Web Interface: All endpoints require authenticating to an authorized user.
Authentication: Attempts are rate-limited.
Account Management: Customer administrators control user accounts. Administrators can add, remove, and manage multiple users.
Account Roles: Accounts can be assigned one of two roles, administrator or restricted operator.
Passwords: Each robot ships with customer-configurable unique random passwords. All account passwords must meet complexity requirements.
Web Application Security: Web interface and API requires HTTPS. Defended against CSRF and XSS. HSTS enabled.

Software Updates

Authenticity: Updates digitally signed with a key controlled by Boston Dynamics. Update contents verified prior to installation.
Update Schedule: Owner controls timing of update installation.
Security Fixes: Dot-fix releases made available when necessary.

Tablet

Operating System: Android 12, with updates available from manufacturer.
Mobile Device Management (MDM): Tablet supports third-party Android MDM.

Audit and Compliance

Security Assessments: Boston Dynamics products are assessed by contracted security consultants.
Internal IT Controls: Boston Dynamics aligns to CIS Security Controls.