Orbit Security

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

Network Architecture

Orbit is a web-based software that is hosted by Boston Dynamics using Amazon Web Services. Outbound from robot 443/TCP is required. Outbound from robot UDP/51820 is recommended for improved connection reliability, depending on the site.

Data and Transport Security

Storage: All user and mission data encrypted at-rest with AES-256 encryption.
Web Traffic: TLS1.3 or TLS1.2 only with modern cipher suites. HSTS to enforce HTTPS. Additionally, optional encryption with ChaCha20-Poly1305 if using Auto-Connect feature.
Video Traffic: WebRTC with DTLS encryption.

Authentication and Authorization

All access to Orbit is restricted to authenticated users.
API and Web Interface: Unique domain and AWS CA TLS certificate per customer.
Authentication: SAML SSO integration is available. Local username/passwords are available if SSO not enabled.
Account management: Customer administrators control user accounts through Orbit or their SSO provider. Administrators can add, remove, and manage multiple users.
Account roles: Accounts can be assigned one of two roles, administrator or restricted operator.
Passwords: Customers are provided temporary random passwords if SSO is not enabled. All account passwords must meet complexity requirements.
Web Application Security: Web interface and API requires HTTPS. Defended against CSRF and XSS.

Software Updates

Authenticity: All software associated with Orbit is loaded from software repositories hosted on AWS and fully controlled by approved Boston Dynamics personnel.
Update Schedule: Customers control timing of application software updates.
Security Fixes: Dot-fix releases made available when necessary.

Audit and Compliance

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

Contact