WHITE PAPER

Boston Dynamics Spot and Site Hub Security

Boston Dynamics

This document describes how Boston Dynamics maximizes the security of the Spot and Site Hub products. We describe the features and design considerations which let these platforms be trusted parts of customer IT integrations.

The material in this document is up to date as of the Spot 4.0 and Orbit 4.0 release.

Our Product Security group is dedicated to protecting customers and creating the world's most secure mobile robot products. We encourage you to reach out with any questions or comments about the material in this document. Thank you for working with Boston Dynamics.

Introduction

At Boston Dynamics, we imagine a world where robots help humans in real day-to-day environments, including in the workplace. For robots to make the transition into real world applications, they will need to do a lot more than just robotics. Robots will need to satisfy the many requirements of their new jobs. A key requirement is cybersecurity. Robot systems must protect their owners -- allowing only authorized use and preventing access to data, networks, and systems.

This documentation lays out how Boston Dynamics thinks about cybersecurity for the Spot product line. It details the security architecture of these products and the implementation of key protective features. The information in this document is intended to let you understand how Spot and Site Hub are designed to protect you and your organization. With the background from this document, you should be able to securely integrate Boston Dynamics products into solutions deployed at your facilities and in your operations.

Thinking about security

The security of an application is the sum of its parts. The components, mechanisms, and processes which make up that system need to be designed to ensure that properties like confidentiality, integrity, availability, and access control are preserved throughout the life of that system.

Boston Dynamics has designed our products to be easily integrated into a secure application. We have made engineering decisions that support your ability to both reason about the application's overall security as well as configure the product to meet your environment's specific security requirements. The integrity mechanisms integrated into our products are intended to guarantee the products' security properties that we describe in this document.

Products like Spot are only one part of the overall solution. Third-party payloads, other software, and the relationship of the robot to your business and IT infrastructure ultimately contribute to the security of the overall application which involves robots. The many security controls implemented as part of Spot or Site Hub provide a strong basis for protecting your business. Physical security controls are an example of a risk mitigation step where the implementation needs to be considered at the point of system design.

Security objectives

Boston Dynamics products are designed to meet three broad security objectives:

Prevent unauthorized operation or disruption of a robot or system.
Any user who can operate a Boston Dynamics robot or access a system is required to have an account you provide and control. These accounts prevent unauthorized users from being able to access the API to power on, drive, or otherwise take control of the robot. Unauthorized users also cannot see sensor or robot state information. Where possible, they should be prevented from disruption to the operation of the robot inside an application.

Prevent unauthorized access to data stored on the device.
An unauthorized user must not be able to obtain customer data from the robot or software service. This restriction includes live or logged images, sensor readings, commands, etc.

Minimize cybersecurity risk to customer's operations and technology assets.
Spot and Site Hub are designed to defend their system integrity against cyber attackers. Both systems contain security features designed to prevent attackers from gaining unauthorized access or use as a launching point against other networks.

Threat model

In order to contextualize the security objectives described above, we need to discuss the threat models faced by Spot and the Site Hub. Broadly speaking, these products have been designed and implemented to resist these threat models:

- Attacks originating from attackers with solely network-level (remote) access, including attacks originating from compromised devices carried on Spot's payload network or otherwise attached to one of Spot's or the Site Hub's onboard network interfaces

- Most attacks originating from attackers with physical access to the device, especially attackers with only fleeting physical access to the device or only physical access to the exterior of the device

Physical attacks represent a specific challenge for mobile robots, as well as server appliances. We have focused both Spot's and the SIte Hub's physical security on limited duration physical access.

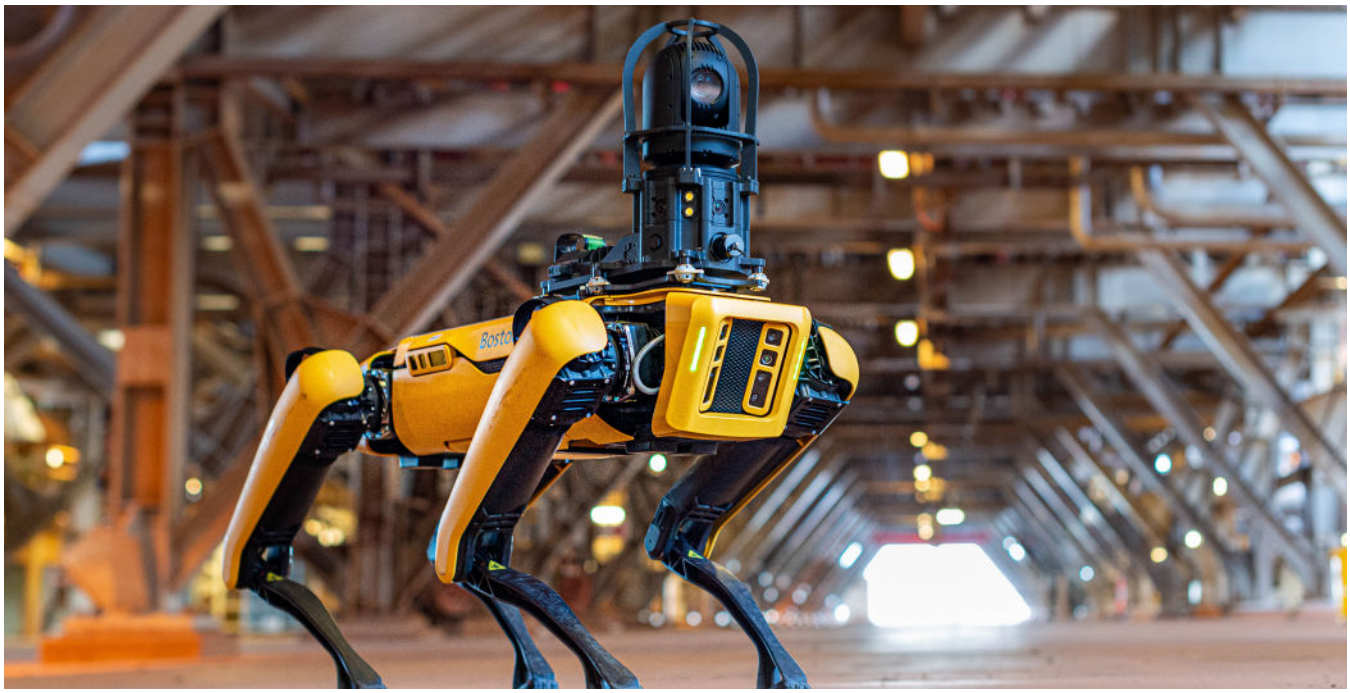
Due to its terms of use, Spot on its own cannot prevent a human from stealing the robot. Given indefinite access to a stolen robot, new physical access exploits to onboard data could be identifiable. We recommend application designers consider physical security as part of their holistic application.

System security

Spot and the Site Hub implement multiple system security mechanisms with one primary goal: ensure the integrity of those devices' software components at all times. System integrity is the property that only intended software can run on a system and only in the configuration it is intended to run. It prevents attackers from introducing malware or modifying how the system works. System integrity underpins every other security mechanism implemented on the device. For example, it allows us to implement filesystem encryption to protect customer data residing on the device.

All executable software that runs on Spot is cryptographically authenticated prior to execution. This property is also true for all Boston Dynamics software running on the Site Hub. Executable software cannot be modified without failing the cryptographic check. If this check fails for a given executable, the system will have detected that integrity is compromised and prevent further operation. The keys used to perform the executable cryptographic authentication are controlled by Boston Dynamics. Modification of this software can only be performed through a released update; this update is signed with a key controlled by Boston Dynamics and the device verifies this cryptographic signature before installing the update. This control ensures all software running on the robot or the server originates from us. All configurations processed by these executables are also encrypted in order to prevent tampering.

The Site Hub allows customer administrators to install their own Extensions. The software for Extensions is not included in the cryptographic authentication, but is stored encrypted on disk.



Secure Boot

Spot and the Site Hub implement Secure Boot to ensure that only Boston Dynamics-approved software will boot on the device. This mechanism further ensures the system integrity of the robot or server. Secure Boot starts this validation from the moment the robot turns on. At every stage of boot, software components like kernels, boot loaders, and executable programs and scripts are verified to originate from Boston Dynamics using cryptographic signatures before that software is executed. Secure Boot ensures that Spot's safety, command and control, and operating functions all work as intended on any Spot robot.

Secure Boot prevents various types of persistent tampering with either Spot or Site Hub's internal software. Our intention is to make it as difficult as possible for a purely remote attacker to potentially modify the system to obtain access. If an attacker found a means to make a temporary modification, that modification would be removed when Spot was rebooted. If the attacker were able to find some way to persistently change the software on the robot or server, the robot would prevent further operation.

To implement Secure Boot, both Spot and Site Hub use industry-standard UEFI Secure Boot mechanisms. The standard computer boot process involves a number of phases known as platform initialization. Platform initialization is performed by platform firmware, which is trusted code originating from Intel and the motherboard manufacturer. Once platform firmware finishes its start up, it finds and loads a bootloader or operating system kernel, which it validates prior to execution.

The bootloader and operating system kernel originate from Boston Dynamics. The UEFI Secure Boot specification defines how this software will be validated by verifying a cryptographic signature. The signature is created by a special Secure Boot Key as part of our release process. Boston Dynamics controls the Secure Boot keys, and we use them only to sign bootloaders and operating system kernels that we have developed and validated for Spot or the Site Hub. This key ensures that both kernel and bootloader come from us.

Inside Boston Dynamics, the Spot and Site Hub Secure Boot keys are stored in a commercial Hardware Security Module (HSM). These keys are only used for the Spot and Site Hub product lines. At no point Boston Dynamics' allow any external supply chain process to possess these keys. They are only used as part of internally controlled processes, which ensures that no third party can change or tamper with the bootloader or kernel on a customer device, during or after manufacture.

Once the kernel is verified by the Secure Boot process, it loads a disk partition that contains the rest of the binaries executed at runtime. This partition is encrypted with a per-device key protected by the onboard Trusted Platform Module or TPM. Per-device keys ensure that were an attacker to gain access to one Spot robot or Site Hub server's data, that attacker would not be able to then access data on other robots or servers. Data-at-rest encryption is discussed in more detail in a later section.

The integrity of executables on the disk partition are ensured in the following way. The disk partition itself contains a read-only volume. This volume holds all executable code used after boot. Whenever the kernel reads from this read-only volume, the data's integrity is verified using a cryptographically-signed hash tree. The cryptographic signature is created using a key controlled by Boston Dynamics and managed with similar security processes as our other keys. If the read-only data's signature does not match, the data will not be used and the robot will prevent operation.

This signature mechanism ensures that all executables run after boot originate from Boston Dynamics.

The integrity properties discussed in this section allow us to implement the many other strong security features of Spot and Site Hub. System integrity protects customers against attackers physically accessing storage, replacing software components, or running non-Boston Dynamics software on robots or servers. If a product lacked this property, then other security features could be compromised by for example directly modifying storage or removing software components.

Site Hub extensions and integrity

When configuring the Site Hub, administrators have the option of installing Extensions. These Extensions can contain executable code. The Extensions are not stored on the read-only volume, since administrators need to be able to install and modify them. They are stored however on an encrypted disk partition, which provides both integrity and confidentiality properties to those Extensions. Like all other data on the Site Hub's disks, the encryption key for this partition is protected by the onboard TPM.

Apart from the Extensions, all other executable code on the Site Hub is provided by Boston Dynamics and resides on the read-only volume.

Data-at-rest encryption

All customer data and internal configuration data residing on both Spot's and Site Hub's internal storage is encrypted. Encrypted storage, along with a secure way to manage decryption keys onboard a device, is a primary requirement for security of any system with a physical presence. Without this capability, a robot could be disassembled and its storage removed and modified. Such physical attacks can include attempts to boot the robot off of other media or to inject malware into the robot.

Note that although we refer to storage built into the robot or servers as "disks", we typically use solid state storage inside our machines. In the case that a product contains multiple storage devices, we apply this disk encryption to all of them.

The disk encryption on Spot and the Site Hub uses AES-XTS encryption with a key size of at least 256-bits. The encryption itself is performed by a filesystem filter driver in the kernel. By using a kernel-level filter driver to implement encryption, we ensure that the disk encryption is non-bypassable; all data written to the filesystem is guaranteed to be encrypted.

Key files are used to unlock the master keys used for the filesystem decryption. Each individual robot or server contains its own unique filesystem encryption keys only available on that piece of hardware. Unique encryption keys ensure that were an attacker to compromise a device, data on all other devices would be safe. It also prevents swapping storage media between robots as a mechanism to access customer data. Further, Boston Dynamics does not retain a copy of the key, and we have no means to decrypt data on these disks outside of the robot. The unique key files are generated on the device during manufacturing as part of a controlled Boston Dynamics on-premises imaging process.

Spot and the Site Hub manage the decryption keys for data using the platform's Trusted Platform Module (TPM). Enterprise Spots contain a TPM compatible with the TPM 2.0 specification. Earlier Explorer models, no longer in production, contain a TPM compatible with the TPM 1.2 specification. The key file is encrypted using the TPM using a process known as sealing. During sealing, data such as the key file can be encrypted by the TPM with a key known only to the TPM. The TPM will only decrypt the data, called "unsealing", when certain platform measurements, known as Platform Configuration Registers or PCRs, match the measurements at the time when the key was first sealed.

These PCR measurements are a means to determine if key parts of the system match the shipped configuration of the robot. As implemented on Spot and Site Hub, the PCRs allow the filesystem encryption keys to be unsealed only if all of the following components are free of tampering:

- platform firmware, such as the onboard UEFI firmware and BIOS.
- embedded option ROMs
- UEFI drivers and configuration
- the Secure Boot policy described in the Secure Boot section

This TPM mechanism allows Spot (or the Site Hub) to decrypt its onboard storage only if guarantees about the identity and integrity of the robot are met. Any mobile robot which provides disk encryption needs to implement a system like this in order to allow the robot to self-decrypt. TPM and self-decryption also allow a robot to operate away from humans by eliminating the need for boot passwords or secret control.

Secure software updates

Boston Dynamics continues to release new software for Spot and the Site Hub units owned by customers. These new releases contain new features which add new capabilities to both platforms and issue fixes in response to customer problems. We also ship security updates and improvements as part of these releases. Keeping your Spot robot up to date with new releases will ensure that software onboard contains the latest set of security features and patches.

Boston Dynamics ships these releases as a monolithic single release file which controls the complete set of software on a given Spot or Site Hub unit. These release files completely configure all software on the platform and ensure that system integrity protections work. We've additionally built a number of features into our releases system to protect customers' security.

A customer administrator is always allowed to choose an appropriate time to install an update to Spot or Site Hub's onboard software. This process ensures that administrators control and understand when updates are taken, and exactly what version of software is running -- an important part of their larger IT security picture. Since no network infrastructure is used to perform the update, there are no security concerns around "over the air" update services.

Once a new release is uploaded to the robot, the onboard software update system will verify the uploaded binary contains a valid release. It ensures the complete contents of the release file are signed by Boston Dynamics, using an asymmetric product-specific key held within Boston Dynamics and used only for releases. The software update system contains a public key used to verify the digital signature over any release file. This signature proves that the release originates with Boston Dynamics. It also proves that the contents of the release match what was packaged by us and that the release has not been altered. The release is also encrypted using a separate key, limiting attackers ability to examine its contents.

Customer data and persistent settings stored on the encrypted partition are preserved through a release installation. Before the device reboots to apply an update, persistent settings are backed up on a different encrypted partition to ensure that the device can recover from a failed update. If the release update is interrupted, the device will restore to its last successful release. These protections ensure that a robot or server cannot be damaged by an unintentional or intentional interrupt of the release upgrade process.

The contents of releases are described in release notes on the Boston Dynamics Support Center. Both Spot and Site Hub incorporate a number of third-party and open-source software packages. We regularly update this third-party software to versions that receive support. As part of our vulnerability management process, we maintain awareness of disclosed vulnerabilities filed against third-party software packages we incorporate. When we become aware of such a vulnerability, we assess its exploitability on our products. If the vulnerability is exploitable in such a way that it exposes customer data or affects the integrity of system software, we work to issue a patch release as quickly as possible.

The release establishes a new verified read-only image. Combined with the features described in the Secure Boot and Data-at-Rest Encryption sections of this document, Spot and Site Hub ensure your device's system software is identical to the intended shipped configuration. These features create a solid foundation of system integrity which allows us to build additional security protections and capabilities. This system integrity is a key security requirement for robots fielded in real world applications.

Executable hardening

The Spot release contains a variety of executable software used to implement the robot's features. When software components are compiled by Boston Dynamics, we enable anti-exploitation features where possible. Typical protections include:

- Stack canaries
- Address space layout randomization (ASLR)
- Executable space protection
- Read-only relocations
- FORTIFY_SOURCE definition.

PCIe bus security

To enable performant communication between hardware peripherals and Spot's software, the Spot hardware platform implements a high-speed bus known as PCI Express or PCIe. Hardware peripherals installed on this bus may in some cases have access to the processor's main memory where software execution resides to enable high speed data transfer. The Spot kernel enables an Input-Output Memory Management Unit (IOMMU) to limit the direct memory access available to these peripherals. The Site Hub kernel also implements an IOMMU.

Firmware security

Both the Spot and Site Hub platforms contain UEFI firmware. This firmware implements the Secure Boot chain that underpins system integrity through the end of the boot process. Our products use automated processes to program standard settings for the UEFI firmware on each unit.

Additionally, certain security-relevant UEFI firmware settings are measured into the TPM's PCRs. Boston Dynamics products will not boot fully and the data filesystems will not decrypt if any unauthorized modification of these settings is detected.

Finally, passwords are set to deter access to the UEFI firmware settings in an environment outside of our manufacturing and service facilities. These passwords are complex, long, and unique for each device.

Spot contains other hardware peripherals, including one or more Field Programmable Gate Arrays (FPGAs), which contain programmable firmware. Firmware for any FPGAs in Spot is encrypted with a key that is burned into the FPGA's eFuse registers. The FPGAs will only load firmware encrypted with this key. This key was generated by Boston Dynamics and we maintain full control over it.

Network security

A key use for mobile robots is for those robots to move and work in areas away from their human operators. Use cases like teleoperation, autonomy, and even remote controlling all require the operator to send commands to and from the robot. Network communication, on existing local area networks or across the internet, uses an existing widely available infrastructure to enable potentially global command and control of a robot fleet. Network security is a key requirement for a mobile robot system, particularly if used as part of a larger IT installation. Boston Dynamics has invested in implementing strong security features to protect customers using our robots on their networks.

Boston Dynamics products implement network security mechanisms with the following goals:

- Minimize the network attack surface of the device.
- Protect all data being transmitted over the network.
- Prevent unauthorized access to network resources.

All products present a minimal set of required services to the external network. Internal systems of the Spot robot and Site Hub server are not exposed.

Both Spot and the Site Hub server can operate in a fully isolated environment without any access to external networks. If a customer chooses, they can integrate the robot and Site Hub into an "island" inside their IT infrastructure.

On each Boston Dynamics product, an onboard firewall filters incoming IPv4 and IPv6 traffic on all interfaces. On Spot the following communication ports are cleared for use.

Port	Protocol	Application	Purpose
22	TCP	ssh	Boston Dynamics service port
443	TCP	https	API and Web access
123	UDP	ntpd	Time synchronize payload computers
8087	UDP	echo	Network debug echo service
51820	UDP	Orbit	Auto-Connect service

The Spot robot also forwards the following port ranges to the payload to allow transparent communication over TCP and UDP.

- 3478-3479
- 8554
- 20022
- 20080
- 20443
- 21000-22000
- 23100-23199
- 24100-24199
- 25100-25199
- 30022
- 30080
- 30443
- 31000-32000
- 35057
- 42630-42632
- 50000-50100

When Spot is connected to a cellular network via the Core I/O or EAP2 payloads, those payloads act as another firewall layer. This firewall acts between the external cellular network and the robot. It allows the following ports to pass through.

Port	Protocol	Application	Purpose
443	TCP	https	Spot API access
31000 -32000	TCP	-	Spot Payload access
31000 -32000	UDP	-	Spot Payload access

All other traffic from the cellular interface is dropped by the Core I/O or EAP2 device. Additionally, all IPv6 traffic is dropped. Additionally, Spot's firewall filter rules remain in place.

On the Site Hub, all interfaces are filtered by its firewall in a similar fashion. The firewall allows access to the following services:

Port	Protocol	Application	Purpose
22	TCP	ssh	Boston Dynamics service port
443	TCP	https	Website and API access
21000 -22000	TCP, UDP	-	Available to applications deployed as Extensions.
31000 -35200	UDP	-	WebRTC over DTLS
51820	UDP	Auto Connect	Auto-connect service for Spots and Site Hubs.

Wi-Fi security (Spot-only)

Spot contains Wi-Fi capabilities. The capabilities allow Spot to be driven using its tablet interface and also to integrate to existing networks installed in a facility. Spot can either act as an Access Point or join an existing Wi-Fi network as a client. The Site Hub does not contain any Wi-Fi capabilities.

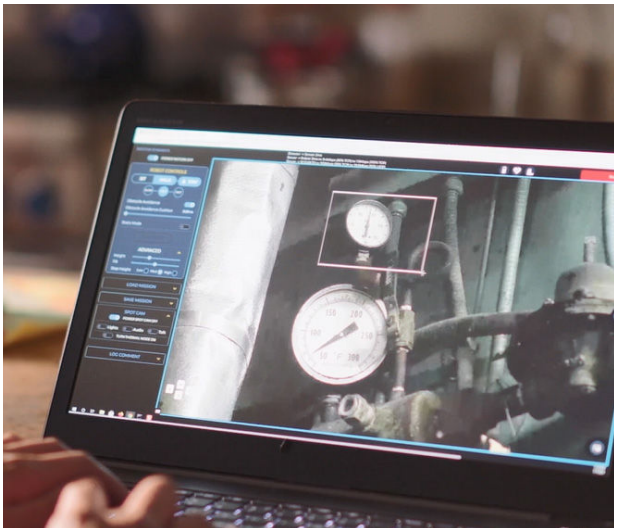
When Spot is operating as an Access Point (AP), WPA2 security must be enabled and a password must be set. This configuration ensures that communication with the robot is encrypted and access to its network restricted. Spot ships already configured to operate as a Wi-Fi AP out of the box, so customers can immediately drive it using the enclosed tablet controller. Each Spot unit's AP has a unique Wi-Fi WPA2 AP passphrase already configured. Customers are encouraged to replace the factory-set password with a new password.

When configured as a Wi-Fi client, Spot supports Enterprise-based Wi-Fi security mechanisms typically known as 802.1x. These 802.1x features include:

- TLS and PWD based authentication
- PEAP authentication including MSCHAPV2, MD5, and GTC
- TTLS based authentication including PAP, MSCHAP, MSCHAPV2, CHAP, MD5, and GTC
- Optional TLS version restriction to 1.0, 1.1, or 1.2

Application security

Spot and the Site Hub implement a wide variety of application features intended to provide value to you, our customers. Each of these application features is designed to ensure that they preserve the security and protections of the Spot robot. The application security mechanisms of Spot and Site Hub defend the integrity of the device as well as prevent unauthorized access.



We require all applications hosting network services to require authentication and encryption, where possible. We document any necessary exceptions.

This section describes the authentication and encryption implemented by each network service. Where relevant, it also discusses application-specific security considerations, specifically those with the potential to compromise data or send unauthorized commands to the device, and additional defensive mechanisms.

Web applications

Spot and the Site Hub's software provide a combination of API and website application features to customers. These features allow you to configure, control, access data from, and perform many other valuable capabilities. These services are built on industry standard best practices around common HTTP communication. This model of communication, and how to secure it, is well understood by IT departments.

We additionally use libraries like Google's gRPC remote procedure call library to implement APIs on top of HTTP communication. These libraries are under active development, maintained, and used in high trust environments. We also use well-known tools, commonly employed at scale on the Internet in web applications, to implement the internals of our system.

All web traffic on both Spot and the Site Hub, including the website frontend, REST APIs, and gRPC APIs, is protected by standard Transport Layer Security or TLS.

On Spot, web endpoints always present a TLS certificate issued by a certificate authority operated by Boston Dynamics.

The Site Hub can be optionally configured to use a custom TLS key and present a custom TLS certificate, provided by the customer.

Spot web application

All clients of the Spot API need to check the validity of the certificate and the certificate chain, and all API clients provided by Boston Dynamics (e.g., the Python SDK) correctly perform this validation. From the perspective of Spot, Orbit, and all Spot payloads act like API clients.

Additionally, all web application endpoints on Spot and Orbit require authentication to access, unless those endpoints intentionally provide an unauthenticated service. The web endpoints use the following authentication mechanisms.

- Session cookies
- JSON Web Tokens (JWT)

The JWT implementation uses the ES256 algorithm and per-device keys. Each JWT is valid only for the Spot robot which issued it.

The Spot web user interface uses session-specific tokens and the double submit pattern to defend against cross-site request forgery (CSRF) attacks. When developing web application and REST API software at Boston Dynamics, code reviews include audits for SQL injection and XSS vulnerabilities. The web application also uses the X-Frame-Options header to mitigate certain clickjacking attacks.

The following REST endpoints intentionally do not require authentication.

Path	Use
/healthz	Health-check endpoint for web server liveness, which will always return HTTP 204.
/static/	Contains a number of static files (images, fonts, scripts, etc.) used to render the web application's user interface. No live data is ever rendered into these static files.
/auth	Must be unauthenticated in order to support cookie-based authentication to the Spot web application. This endpoint cannot itself be authenticated because it must be reachable by unauthenticated users.
/accounts/login/	Required to allow users to authenticate to the Spot web application
/accounts/logout/	Unauthenticated users will redirect to the login page
/accounts/jwt/generate/	Required to allow Spot API clients to authenticate
/logs/log-experiment	Enables all users to generate an encrypted service log when the robot has a fault.
/payload-config/encrypt_secret	Supports payload registration
/bos.bundler.BundlerService	Used to generate and download encrypted service log files even if the web application is non-functional
/bosdyn.api.AuthService	Used by Spot API clients for authentication to obtain a JWT token. This endpoint cannot itself be authenticated because it must be reachable by unauthenticated endpoints.
/bosdyn.api.RobotIdService	Used by Spot API clients to obtain the identity of a robot. No sensitive data is exposed through this endpoint.
/bosdyn.api.PayloadRegistrationService	Used by payloads to register with Spot. An authenticated user must authorize the payload in the Spot administration interface.

Orbit application

The Site Hub hosts a version of the Orbit application that is largely the same as our cloud offering. The Orbit web application (frontend) uses session-specific tokens for session authentication and the double submit pattern to defend against cross-site request forgery (CSRF) attacks. When developing web application and REST API code, our code reviews include audits for SQL injection and XSS vulnerabilities. Additionally, the web application uses the X-Frame-Options header to mitigate certain clickjacking attacks.

Unauthenticated endpoints are documented below.

Path	Use
/api/v0/login	Used by users to log in
/api/v0/login-temp	Used by temporary users to log in
/api/v0/version	Returns information about the Site Hub software version
/ws/v0/bandwidth-test/.websocket	Supports network debugging features
/ws/v0/ping/.websocket	Supports network debugging features
/api/v0/webrtc-test/	Supports network debugging features

WebRTC

WebRTC is used to stream video content between a SpotCAM payload and clients, including browsers, tablets, Site Hubs, Orbit, or other API clients. WebRTC is also used to stream between a browser client and an Orbit instance.

The product implementation of video streaming relies on TLS to protect the initial exchange of trusted identities needed for WebRTC. The WebRTC standard mandates the use of DTLS-SRTP to protect video data.

If a Spot is not equipped with a SpotCAM, streaming of images from Spot's body cameras uses a connection protected by TLS.

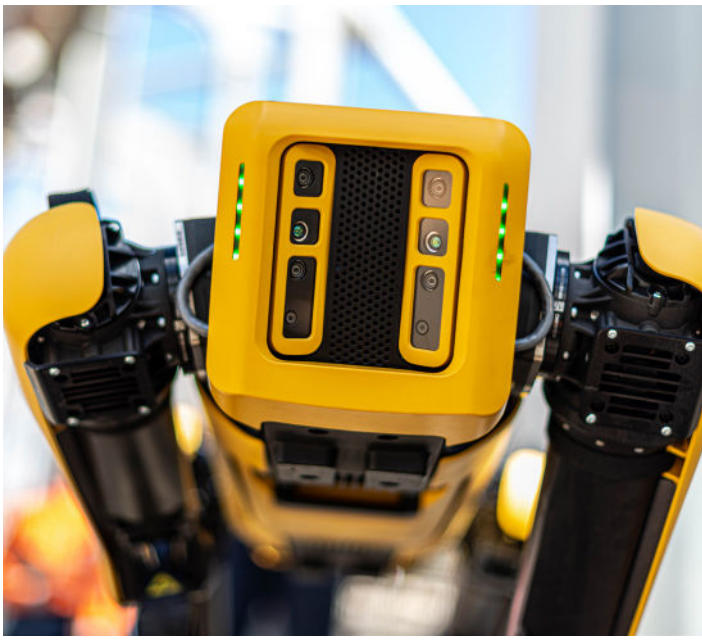
On the Site Hub, a TURN relay is hosted at 443/tcp. This relay does not use (D)TLS. The endpoint is authenticated using a shared secret between the client and server that is retrieved through the Site Hub's REST API over TLS.

Auto-Connect

Auto-Connect is implemented using the WireGuard network tunnel protocol. The initial exchange of trusted identities is performed manually during the setup of the Auto-Connect feature. The rest of the setup for the WireGuard tunnel is performed over TLS using an ephemeral self-signed certificate. Once setup is finished, data is transmitted over the WireGuard tunnel.

Boston Dynamics service access via SSH

Boston Dynamics maintains the ability to perform service remotely via the Secure Shell Protocol (SSH). This service is only used during support and service incidents, with advance notification and customer consent.



Authorized Boston Dynamics personnel are authenticated to SSH using only SSH certificates or keys. Access to these device-specific SSH credentials is governed by our Hardware Security Module (HSM), which has been programmed to limit access to the relevant personnel. When the HSM grants access, it emits audit logs noting the employee being granted access and the specific device to which access is being granted. The SSH certificate is set to expire after a short period of time.

During normal operation, customers can block access to this port at the network layer and device operation will remain unaffected.

User profile and privilege management

The previous section described the scope of authentication on Spot and the Site Hub and documented the authentication mechanisms used on Spot and the Site Hub. In this section, we will describe the authentication requirements for users and associated privilege management features on each device.

Spot

Spot has the capability to set up user accounts intended to enable privilege separation. User accounts are named identities that bind to either a Spot administrator or Spot user role. The administrator role has the ability to configure a Spot robot. The user role has privileges to only operate the robot, for example driving it or commanding it to go to a location.

Each user account is associated with a password, which must meet these complexity requirements:

- Minimum of 12 characters
- Must not be entirely numeric
- Cannot be a common password
- Cannot be too similar to the username

When stored on-robot, these passwords are salted with a unique salt and hashed with PBKDF2-HMAC-SHA256 using 150,000 iterations.

All login attempts to Spot are rate-limited to 6 attempts per 60 seconds per account.

Orbit on Site Hub

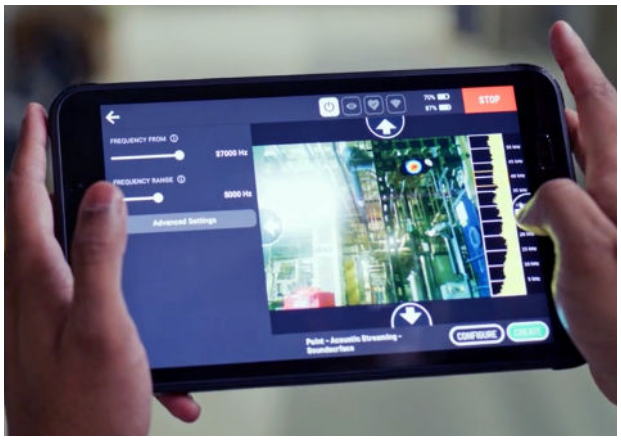
Orbit on Site Hub has the capability to set up user accounts intended to enable privilege separation and to bind named identities to a variety of permission sets. The privileges of each permission set is documented on the Boston Dynamics Support Center. Each user account is associated with a password which must meet a strength requirement determined by zxcvbn, a common password strength measurement library.

These passwords are salted with a unique salt and hashed using bcrypt with a work factor of 8.

Optionally, administrators can create accounts tagged as “temporary”. Temporary accounts expire the account access at a specified time. Users on temporary accounts can log in using their username and password through the normal login interface. Temporary accounts can also log in using a randomly-generated, unique URL linked with each temporary account. These accounts allow administrators to grant certain users a limited time ability to access the Orbit application.

In Orbit on Site Hub, each IP is rate-limited in login attempts to 5 attempts per second.

Security considerations when using third-party integrations



Both Spot and the Site Hub can host custom integrations that make use of data and capabilities hosted by either device. Spot can host Payloads as well as present off-robot services as part of its own API. Orbit on Site Hub can host Extensions that can be used to process data that a robot retrieves, as well as host Custom Web Views to present external data as part of its own interface. Orbit hosted in the cloud cannot host Extensions at this time; we recommend customers self-host any Extensions and use webhooks to push data from Orbit to their Extensions.

This section contains important security considerations to be aware of when implementing any such integrations.

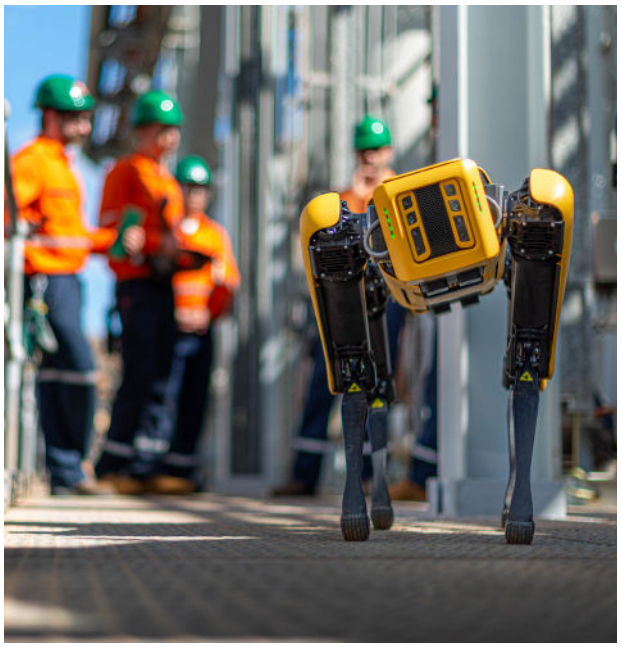
Spot Payloads

Payloads are systems which attach to Spot in order to extend its capabilities. Common payloads include devices which connect to Spot via its payload ports. Payloads produced by Boston Dynamics have specific security features designed to protect the robot and access. We encourage our partner ecosystem to meet the same security standards we have for our products.

Payload networking

When a payload is attached to Spot via Spot's payload ports, the payload gains access to Spot's payload network. Over this network, the payload can send traffic to Spot directly or communicate with other payloads on the network. There is no firewalling between payloads. Spot, however, is firewalled from payloads as described in the "Network security" section.

Spot will forward certain traffic it receives on its shore Ethernet and Wi-Fi interfaces to attached payloads. These forwards are documented here.



Payload network security and authentication

One purpose of Spot's exposure to the payload network is to allow payloads to make requests of Spot's API. Like all other clients, payloads must interact with Spot's API using TLS. When using TLS, payloads must verify the validity of the TLS certificate presented by Spot's gRPC endpoints.

As described in the "Application security" section, most of Spot's API endpoints require authentication. Payloads can authenticate to the Spot API using one of two methods: 1) a Spot user's username and password, or 2) the Payload Registration Service and workflow. In either case, the payload will need to store authentication credentials in a secure manner. Payloads produced by Boston Dynamics meet this standard, and we encourage our partners to meet the same standard.

Of the two authentication methods, we recommend payload partners use the Payload Registration workflow. The mechanics of this workflow is detailed in our SDK documentation and the security mechanisms it uses will be discussed below.

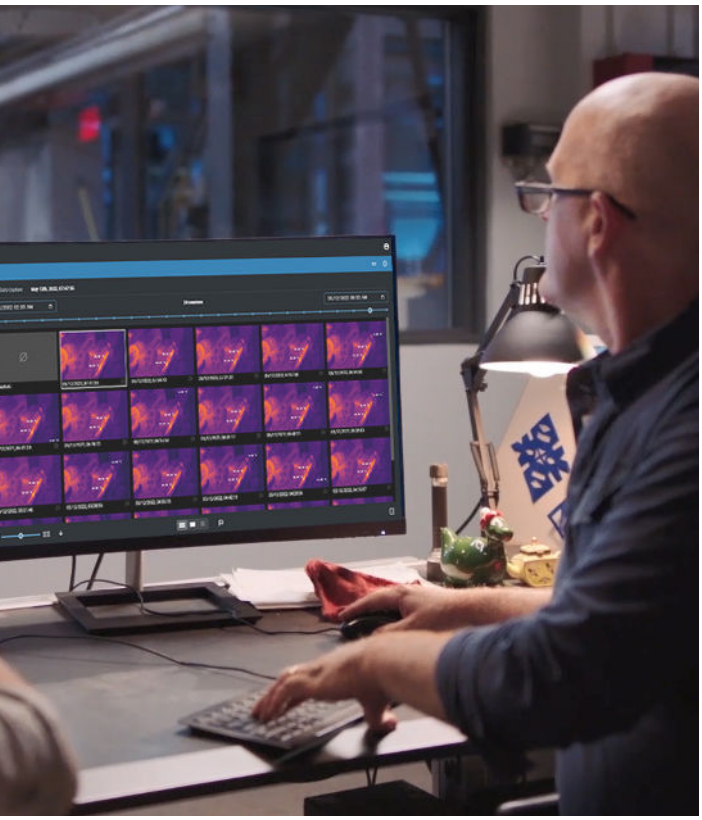
When the payload performs the initial registration request, this is performed as an unauthenticated gRPC call over TLS. At registration time, payloads also send a secret password. We have advised payload partners to use high-entropy randomly generated values unique to a specific device for this password.

If the request is accepted, Spot will create an entry on the Payloads page in the Spot administration web application. At this point, an authenticated user can approve the payload. Approval must take place before the Payload is recognized by the robot system.

The payload will use this password to authenticate to Spot and obtain a 12-hour JWT access token. This token can be refreshed or the payload can re-authenticate to obtain a new token.

Offboard API services (Spot)

Using the Directory Registration Service, off-robot services can be registered on Spot and discovered by Spot API clients. Clients can invoke these services via Spot's API, and these communications will be protected by TLS using Spot's TLS certificate. However, when the client's traffic is forwarded to the off-robot services, that communication is not encrypted. SpotCAM is an exception; in other words, clients' communications with SpotCAM are encrypted.



When the off-robot service is hosted by a payload, this traffic traverses Spot's onboard payload network, which is a wired network only accessible by attached payloads (further details in the "Payload networking" section).

However, if the service is hosted elsewhere, this traffic may traverse wireless networks or the public Internet. The exact types of networks this traffic traverses depends on the configurations of the networks between Spot and the service.

Extensions (Orbit on Site Hub)

Customers can implement Extensions using standard Docker infrastructure. As such, the Extension provides customers with a mechanism to execute arbitrary logic on the Site Hub to process data from one or more robots. This powerful privilege is limited to administrative users. Administrators are advised to carefully evaluate the origin and composition of Extensions for trustworthiness.

Custom Web Views (Orbit and Orbit on Site Hub)

The Orbit web application contains a Custom Web Views feature which will render content and data originating from sources external to the Orbit instance. When using this feature, it is important to evaluate the trustworthiness of those sources of content and keep in mind common web security attacks, such as cross-site scripting, cross-site request forgeries, etc.

Customer data received by Boston Dynamics

Customers can opt to send either Service Logs or Performance Logs to Boston Dynamics. To learn more about the details of the data types in these logs, the transmission and encryption mechanisms, and how this data is handled once it arrives at Boston Dynamics, please refer to the Spot Privacy Notice.

Security and the software development lifecycle

Both Spot and the Site Hub are developed using a single product development lifecycle, run by dedicated product and program management staff. That lifecycle includes four phases:

1. Inception
2. Elaboration
3. Construction
4. Transition

During each phase, relevant personnel perform specific security tasks to ensure that security concerns are carried through all phases of development.

In the **Inception** phase, product managers are focused on development of the business case for any given proposed feature. Security features driven by customer requests can start here.

In the **Elaboration** phase, product managers are focused on developing requirements for a new feature and some engineering staff are involved in early prototyping with the goal of scoping the work. Specific security requirements are identified and documented during this phase. As prototyping proceeds, a software architecture begins to emerge. As the software architecture evolves, it undergoes high-level security reviews with the goal of developing requirements and providing input into the scope of the work.

In the **Construction** phase, engineering staff take requirements and prototypes developed in the previous phase and iterate towards the finalized implementation. During this phase, we implement low-level code reviews, secure coding reviews, and static analysis security testing. The software architecture is not expected to change significantly, but if it does, it undergoes yet another high-level security review.

The final phase is the **Transition** phase, where staff are focused on driving a feature towards release readiness. This always involves qualification testing and field testing. Testing is performed against the requirements identified in the Elaboration phase, which often includes specific security requirements associated with the new feature.

Throughout the development lifecycle, we are continuously performing testing against our newest code. These include full system tests and integration tests that include testing for specific security mechanisms. We also perform dynamic application security testing to identify coding mistakes that escape code review.

Bug fixes also go through an abbreviated version of the software development lifecycle. Simple bug fixes where the requirements and architecture are well-understood might only go through the Construction and Transition phase, including continuous testing, system testing, and qualification testing. Major rework may go through all four phases again.