Cybersecurity for Smart Building IOT Platforms

Keeping customer data safe and secure is a huge responsibility and a top priority for Buildings IOT. This document contains the full text of our Security Overview and Privacy Policies.

Last updated: February 15, 2021

Contents

Privately Hosted Data Center Facilities

In our privately hosted data center facilities, there are fully redundant paths from the Internet to each private VLAN that we have built for each customer. In those private VLANs, no interfaces or configuration is shared by any customer system or internal system. Each of the multi-tiered

pathways are fully redundant and no single point of failure exists between the core of the network and the internet. All pathways are secured by a combination of access lists and firewall rules, no routing protocols are used internally, and all configurations are hardened and follow the NIST standards for the configuration of security devices.

Access Control and Organizational Security

Personnel

All employees and contractors (workers) sign confidentiality agreements before gaining access to our code and data. Background checks are performed on our workers prior to their first day of work. Everyone at BIOT is trained and made aware of security concerns and best practices for our systems. Remote access to servers is via our VPN using two factor authentication and limited to only those workers who absolutely need remote access in order to complete their daily work. We log all access to all accounts by IP address.

Dedicated teams

Our IT and Security Team is in charge of access/identity management, network connectivity, firewalls and log file management. Their responsibilities include:

- Maintain and support our automated test suite for development machines.
- Review all changes to the code and infrastructure to ensure we follow best practices and security guidelines (such as OWASP).
- Build and operate BIOT's infrastructure, including logs, monitoring and authentication.
- Review, test and design incident response processes.
- Respond to alerts triggered by any security events.
- Coordinate external audits and security and privacy certifications.
- Monitor and alert on anomalous activity.
- Coordinate vulnerability testing with external security researchers.

Audits, security policies and standards

We have an internally built system that monitors and automatically blocks suspicious activity (including vulnerability scanning, failed logins, and a host of other suspicious activity). We also have alerts in place for excessive resource use that escalates to our Ops team for manual investigation. Our products run on a dedicated network secured with firewalls and carefully monitored.

Data Protection and Privacy

Data location

Our private data centers are in the United States, in Oakland, California, and Hillsboro, Oregon. We also use Amazon AWS for other customers. All data is written to multiple disks instantly, backed up on a rotating cycle from 2 to 6 hours, and stored in multiple locations. Our software infrastructure is updated regularly with the latest security patches.

Encryption

Over public networks, we send data using strong encryption. We use SSL certificates issued by GoDaddy Inc. The connection uses AES_256_CBC for encryption, with SHA2 for message authentication and ECDHE_RSA as the key exchange mechanism.

Our storage system uses AES-256/ SHA-256 encryption. Files are encrypted with AES-256, sliced, replicated, and geographically dispersed to separate data centers on private, end-to-end encrypted network connections. Device, system and controls data isn't encrypted at rest — they are active in our database and subject to the same protection and monitoring as the rest of our systems.

Physical security

Our state-of-the-art servers are protected by biometric locks and round-the-clock interior and exterior surveillance monitoring. Only authorized personnel have access to the data center. 24/7/365 onsite staff provides extra protection against unauthorized entry and security breaches.

Law enforcement

In the unlikely event that law enforcement is interested in the level of information we collect in performing our Service, we would never share your data with law enforcement unless a court order mandates such action. We reject requests from local and federal law enforcement when they seek data without a court order. And unless we're legally prevented from it, we'll always inform you when such requests are made.

Data deletion

All your content will be inaccessible immediately upon cancellation. Within 30 days all content will be permanently deleted from all servers and logs. This information cannot be recovered once it has been permanently deleted.

Incident management and disaster recovery

We practice regular recovery drills. Our backups are tested on a regular basis and are stored off-site for a maximum of 30 days. We have procedures for responding to incidents managed

by our dedicated IT and Security team. A third data center holds a complete data recovery engine, housing offsite disk-to-disk to offsite disks backups of each customer's virtual servers. Those backups are encrypted in transit and also encrypted at rest. Each is stored in a separate and private container. In that facility, we maintain a 2 to 10 ratio of preparedness for hosting customers, with the ability to launch a full working copy of any customers Virtual Server within a two-hour period if required.

Want to know more?

If your IT teams have specific concerns not addressed here, work through your primary account manager to have more details explained and/or set up a meeting with your IT leaders. For more information, you can email us at info@buildingsiot.com.