

INTERSTACKS

Data Security

Data encrypted everywhere, from sensor to storage

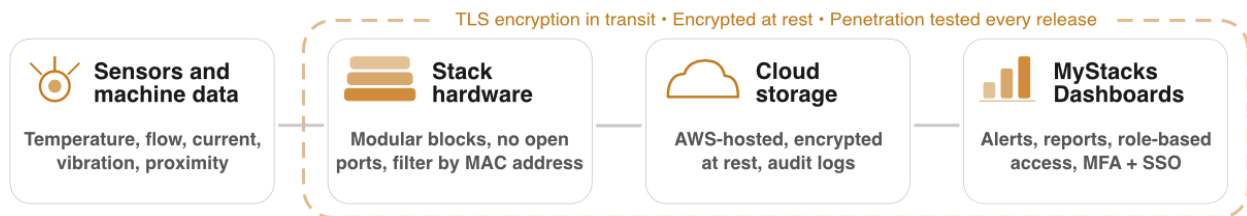
Doc Ref: 2026-MM002-02



Interstacks collects data from physical sensors, and sends it to easy-to-use customizable dashboards. It can be deployed in a few minutes, and includes powerful features such as real-time alerts and automatically generated reports sent to your inbox.

Security is built into the Interstacks data chain at every step, from the hardware that collects sensor data to the cloud infrastructure that stores and serves it. Because Interstacks is a tightly integrated hardware-dashboard system, it is more secure than systems built from disparate pieces. This document outlines specific measures that protect your data, your network, and your users throughout the system.

Secure data chain, from sensor to dashboard



Encryption in transit and at rest

All data captured and sent from a stack is encrypted using TLS (Transport Layer Security). Once received, all data at rest in the MyStacks database— every timestamped sensor reading— is encrypted. There is no point in the data chain where your operational data is exposed in plain-text.

Encrypted longitudinal data is stored indefinitely, and multiple audit logs are maintained at the cloud level for compliance and review purposes.



Hardware and network security

Interstacks hardware does not use any open source operating system, such as Linux. As a result, we have complete control over all network transactions and there are no hidden open network ports that could serve as an attack surface.

Ethernet, Wifi, or Cell data blocks can be used to transmit data from a stack, depending on your network requirements:

- Networks can optionally filter by hardware MAC addresses.
- For Ethernet and Wifi connections, only a single URL needs to be allowed through a network firewall
- For cellular data, no connection to the local network is required.

Cloud infrastructure

The MyStacks IoT platform is hosted on Amazon Web Services (AWS), the world's leading cloud infrastructure provider. Approximately 45% of global web applications run on AWS, including systems used by healthcare organizations and government agencies.

Running on AWS means that your data benefits from continuous enterprise-grade security updates, firewall management, and cybersecurity monitoring, exceeding what on-prem servers can sustain. These security updates are applied continuously without any action required from you. No software is downloaded or installed locally on your devices.

User access and authentication

Every Interstacks user has a unique login and role-based permissions: Read-only, Read/Write, and Administrative. MyStacks supports multi-factor authentication (MFA) and single sign-on (SSO) to enable integration with your existing identity management infrastructure.



Data access and ownership

You own your data at all times. It is never shared, sold, or used for any purpose other than powering your dashboard and reports. Interstacks logs sensor and machine data exclusively; No personal, financial, internal communications, or payment information is ever collected.

You can access your data via several channels, depending on your workflow:

- Live dashboards accessed in any web browser
- Automated daily/weekly/monthly reports, sent to your email inbox
- Exportable CSV files and raw data downloads
- API access for integration with other business systems

Ongoing security validation

Penetration testing is performed for every platform release. Interstacks supports large-scale continuous deployments, streaming data every second of every day from operations all over the world. Customers include large international enterprises, OEMS, and smaller manufacturers alike. Contact us to discuss your process, challenges, and how better data visibility could improve your operations.

To discuss your security requirements or infrastructure setup, visit www.interstacks.com or contact our team directly at info@interstacks.com.