

Advanced Data Security for Discrete Manufacturers In the Age of AI and the IIoT TOTAL PRODUCTION OPTIMIZATION SUITE



A SECURITY-COMPETENT AI & IIOT SOLUTIONS PARTNER

Plataine is the leading provider of AI-based IIoT optimization solutions for advanced manufacturing. Our Total Production Optimization (TPO) suite uses intelligent, connected Digital Assistants to monitor and analyze the production floor, empowering manufacturers to make optimized decisions in real-time. Easy integration with existing systems offers an end-to-end solution to digitize your manufacturing operations.

Embracing AI and the IIoT delivers radical improvements to the productivity of discrete manufacturers. It also requires constant connectivity, and full integration with the cloud. Advanced data security is therefore crucial. To benefit from cloud-based AI optimization solutions with confidence, discrete manufacturers must ensure they partner with a reliable, security-competent partner.

This datasheet outlines the measures Plataine takes to keep your cloud-based operations safe and protected.

PROTECTING YOUR DATA

Data security is the primary concern of discrete manufacturers considering using cloud-based AI and IIoT solutions. That's why, at Plataine, we've made it our vital concern as well, and we are fully committed to your privacy and security.

TPO is a highly secure AI-based IIoT production optimization solution.

Benefits

- Security compliance
- Interoperability and ease of integration
- SLA (High-Availability, redundancy)
- Scalability
- Localization (multiple languages UI)
- Seamless and continuous delivery of software upgrades

Delivering Advanced Data Security

- Corporate level ISO 27001
- Slash costs by sharing core infrastructure with secure, shared multi-tenant architecture
- Full encryption and cryptographic hashing on secured channels
- Complete control over access levels of individual users
- Total security with virtual private networks, virtual private clouds, virtual firewalls, and secure shell technology

OUR DATA SECURITY CREDENTIALS

ISO 27001 – CORPORATE LEVEL



ISO 27001 is the international standard for information security. It's a holistic approach to creating and maintaining a complete information security management system. It is subject to regular external audits, meaning we're constantly evolving to maintain the highest possible standards.

ITAR COMPLIANCE

Plataine uses Amazon Web Services (AWS) as its preferred public cloud infrastructure provider. Plataine offers an ITAR-compliant option through AWS, which provides specifically ITAR-compliant services in its GovCloud offering.

SECURING DATA IN TRANSIT AND DATA AT REST

Protecting sensitive data both in transit and at rest is imperative for modern enterprises as attackers find increasingly innovative ways to compromise systems and steal data.

Data In Transit data protection in transit is the protection of this data while it's traveling from network to network or being transferred from end point to another. At Plataine Data in Transit is kept safe using secured channels (HTTPS), and SSL certificates.

Data at Rest data protection at rest aims to secure inactive data stored on any device or network.

Plataine invests heavily in the latest encryption technology, to constantly keep our stored data encrypted.

MULTI-FACTOR AUTHENTICATION SUPPORT (MFA)

Enables extra security to be added to the account by granting access to the system only after the user provides additional proof of their identity. This additional proof comes in the form of a code or button from within an authentication app, email, or text.

VIRTUAL PRIVATE CLOUD

Plataine's cloud infrastructure makes use of virtual private clouds (VPCs). Each system component is hosted in the VPC that's relevant to it only, thus providing an additional layer of segregation.

SECURE AUTHENTICATION & AUTHORISATION AND ACCOUNT SEPARATION

Secure authentication and authorization procedures mean more than just having a username and password. Plataine's solutions hold detailed information on each system user, allowing strict access rules depending on the individual. Separate accounts for production and development personnel means different levels of user access to ensure IIoT system users can only access the data they need to perform their own specific roles.

CRYPTOGRAPHIC HASHING

Hashing means converting data into a unique string of text and storing it in this form. This highly secure system ensures that even if the database of hashed information broken into the data cannot be used to access the system. For example, crucial system passwords.

VIRTUAL FIREWALLS

Plataine uses the Security Groups feature. Security Groups keep access to the minimum necessary at the component and port level. By doing so, Plataine follows the Principle of Least Privilege (POLP), which is an important system security concept.

SECURE SERVICE-TO-SERVICE INTEGRATION

Plataine's TPO services use a dedicated authorization module to receive applications to authenticate client credentials. These credentials determine the permissions granted to your organization. APIs seeking access on behalf of an end user use the JWT (JSON web token) standard to authenticate and grant access, which is considered an industry standard.

ABOUT PLATAINE: Plataine is the leading provider of AI-based and Industrial IIoT optimization solutions for advanced manufacturing. Our solutions provide intelligent, connected Digital Assistants for production floor management and staff, empowering manufacturers to make optimized decisions in real-time, every time. Plataine's technologies are used by leading manufacturers worldwide, including Airbus, GE, IAI, Triumph, Stelia North America, Alestis, MRAS, TPI, Kinenco-Kaman, IFS, Light & Strong and Ethan Allen. For more information, visit: www.plataine.com.