



Stratasys IoT Platform Cybersecurity

August 2024

Stratasys Cybersecurity

Stratasys is leading the Additive Manufacturing industry in producing solutions that address today's critical and ever-changing cybersecurity threats. The Stratasys IT organization is ISO 27001 certified, and we continue to invest to insure the most secure solutions in the 3D printing market for the future.

Stratasys has implemented reasonable administrative, technical, and physical safeguards to help protect against security incidents and privacy breaches involving a Stratasys product, provided those products are used in accordance with Stratasys instructions for use. However, as systems and threats evolve, no system can be protected against all vulnerabilities, and we consider our customers the most important partner in maintaining security and privacy safeguards. If you have any concerns, we ask that you bring them to our attention, and we will investigate. Where appropriate, we will address the issue of product changes, technical bulletins and/or responsible disclosures to customers and regulators.

Secure Software Development Lifecycle for IoT Platform Software

Stratasys Software implements security measures across: Software development, Infrastructure setup, Identity Management, and Security Operations.

Our security practices also include an S-SDLC which utilizes a wide range of policies and tools involving secure architecture assessments, Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Supply Chain vulnerability checks (SCA) Penetration testing and participation in the HackerOne bug bounty program.



GrabCAD IoT Platform

Overview

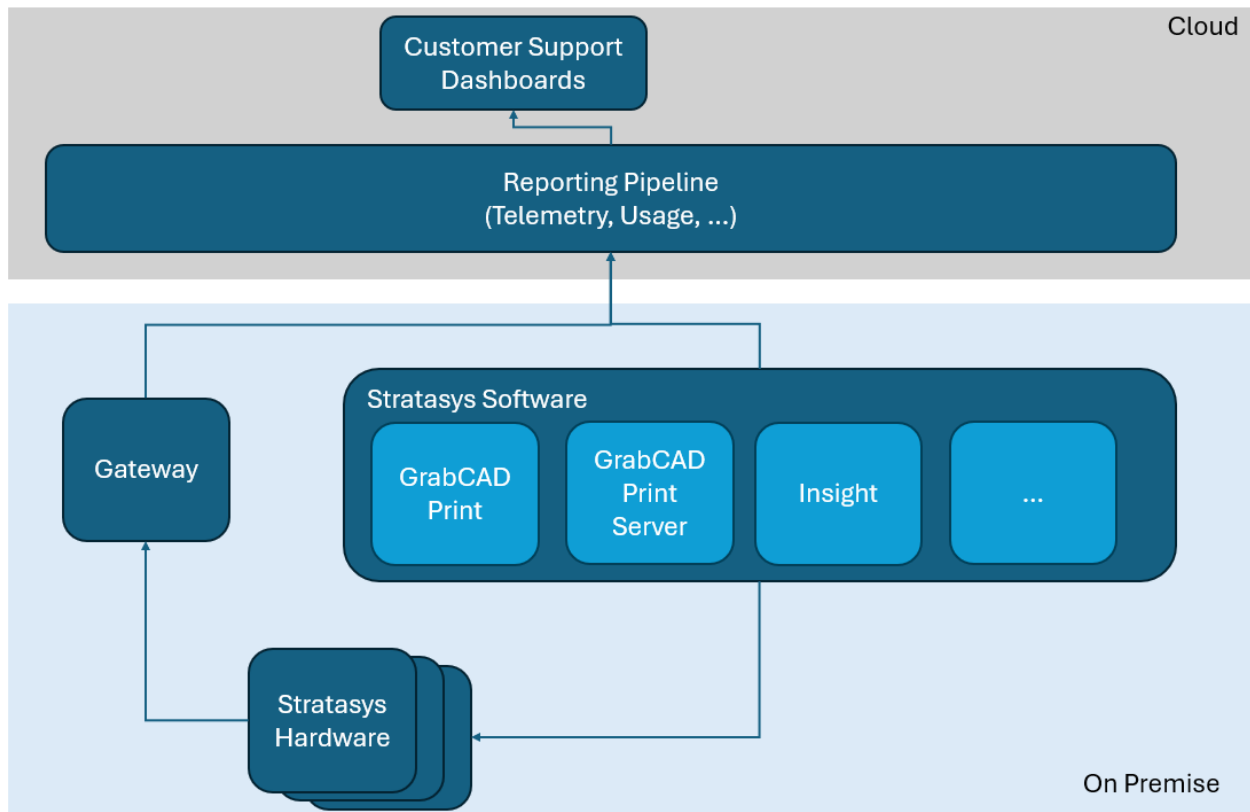
To enable digital workflows and integration with industrial production systems, the GrabCAD IoT Platform is a unified framework to connect all printer data to a single source of truth:

- Collect machine data directly from printers.
- Use industry standard MTConnect – enhanced with Stratasys Machine Language (SML).
- Simple, secure certificate-based communication and reliable data flow with robustness against connectivity loss.
- All data encrypted at rest and in-transit.
- Planned support for both connected and air-gapped solutions.
- High degree of compatibility with industry software and standards.

Features

- High availability & reliability through an architecture that supports near real-time data collection.
- Data collection using industry standards: MTConnect (enhanced by Stratasys Machine Language - SML).
- Consistent and reliable data pipeline: Data Hub as a single source of truth.
- Secured integration with Stratasys Backoffice systems.
- Verification of printers' identity through a strict commissioning flow.
- Providing analysis, dashboard & notification mechanisms for faster time to resolution (TTR).

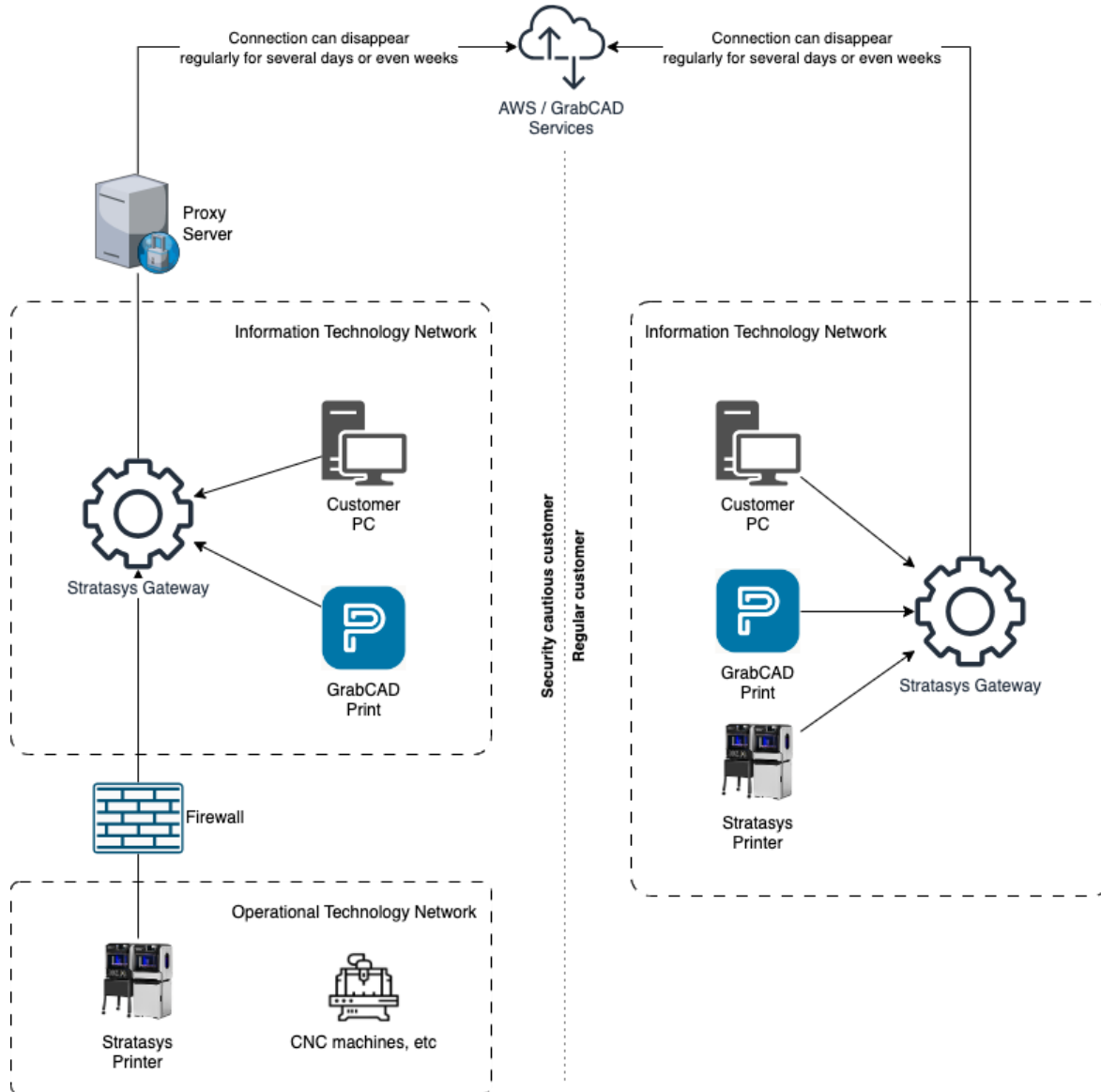
System Diagram



Data Storage and Data Access

All data is encrypted in rest (AWS services) and in transit (TLS).

Network Diagram





Data Collection

- **Printer:**
 - IoT Platform ready machines (Grade 1, G1) send MTConnect/SML data.
 - MTConnect data can be used to coordinate machine data through an MQTT broker.
 - This includes telemetry from the machine but does not include CAD or printable files.
 - Printer commissioning is done via a secure controlled process. This includes issuing a special IoT device certificate for authorizing future communications.
- **Data Hub:**
 - Centralize all data for all printers.
 - Data structure is based on MTConnect vocabulary.
 - Data Hub implements industry standard solutions such as Kinesis Firehose, S3 for data lake, S3/DynamoDB/Redshift for processed data, SQS.
- **Gateway:**
 - Based on AWS IoT Green grass software.
 - Secured data pipes both local and to/from cloud.
 - Authentication and authorization of devices.
 - Manages deployments and configurations (including Stratasys applications).
 - Persistency and robustness through data buffering during connectivity issues.
 - Gateway commissioning is done via a secure controlled process. This includes issuing a special IoT device certificate for authorizing future communications.



Additional Information:

- We publish "[Your Data on GrabCAD](#)"
- We offer the "[GrabCAD Platform Security Whitepaper](#)"
- End User Agreement www.grabcad.com/terms

For further questions around Stratasys Security:

- For completion of questionnaires and forms please contact us via customerquestionnaires@stratasys.com
- For application and product Security questions relating to Stratasys Products, Software, Cloud development and Cloud production please contact us via sw-security@stratasys.com

Disclaimer

The information contained in this Product Security White Paper is for reference purposes only. Nothing contained in this document or relayed verbally to any customer will be deemed to amend, modify, or supersede the terms and conditions of any written agreement between such customer and Stratasys, or Stratasys subsidiaries or affiliates (collectively, "Stratasys"). Stratasys does not make any promises or guarantees to customer that any of the methods or suggestions described in this Product Security White Paper will restore customer's systems, resolve any issues related to any malicious code or achieve any other stated or intended results. Customer exclusively assumes all risk of utilizing or not utilizing any guidance described in this Product Security White Paper.

Stratasys Headquarters

7665 Commerce Way,
Eden Prairie, MN 55344
+1 800 801 6491 (US Toll Free)
+1 952 937-3000 (Intl)
+1 952 937-0070 (Fax)

stratasys.com
ISO 9001:2015 Certified

1 Holtzman St., Science Park,
PO Box 2496
Rehovot 76124, Israel
+972 74 745 4000
+972 74 745 5000 (Fax)

© 2023 Stratasys. All rights reserved. Stratasys, the Stratasys Signet logo, FDM, F900 and Fortus are registered trademarks of Stratasys Inc. GrabCAD Print, Control Center, Insight, ProtectAM and Fortus 450mc are trademarks of Stratasys, Inc. All other trademarks are the property of their respective owners, and Stratasys assumes no responsibility with regard to the selection, performance, or use of these non-Stratasys products. Product specifications subject to change without notice. RD_FDM_Cybersecurity_1223a

