3D SYSTEMS

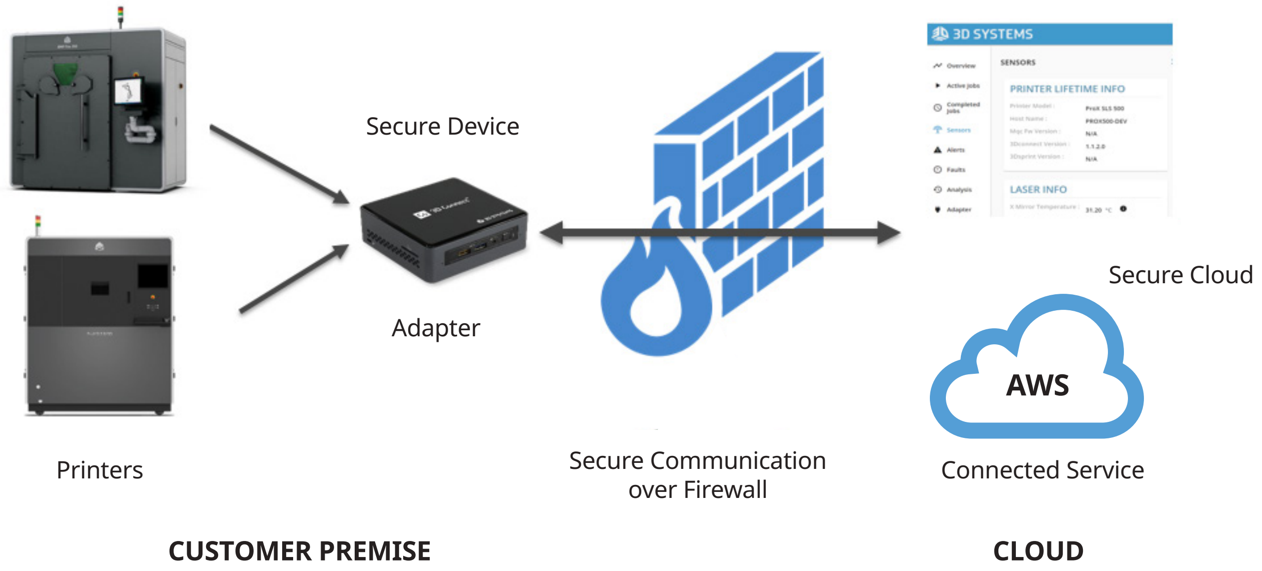
Co 3D Connect™

Architecture and Security

Overview

3D Connect Service provides a secure, cloud-based connection to 3D Systems service teams for proactive and preventative support, enabling better service to improve uptime and deliver production assurance for your system.

The 3D Connect system is comprised of a data collection, transmission, and storage technology stack.
The high-level architecture is displayed in Figure 1 below:



Printer Model : ProX SLS 500
Host Name : PROX500-DEV
Mpc Fw Version : N/A
3Dconnect Version : 1.1.2.0
3Dsprint Version : N/A
X Mirror Temperature : 31.20 °C

Printer data is collected by the adapter, converted to an internal representation, and securely transmitted to 3D Systems alert monitoring and data storage system hosted in Amazon Web Services (AWS). 3D Systems controls and administers the AWS services. Only authorized 3D Systems employees have access to the AWS server.

The hardware adapter is deployed on premise at the customer site and can simultaneously connect up to 20 printers on the customer LAN. For printers utilizing a hardware adapter, no connection to the internet is required from the printer(s).

The alert system in the cloud monitors printer data collected in near-real time and generates alerts to authorized 3D Systems service employees when predefined operating limits are exceeded. The authorized 3D Systems employees have the ability to observe the historical printer data collected in order to help determine whether servicing of the affected printer is required.

Printer Data

WHAT DATA IS COLLECTED?

The printer data consists of low-level operational sensor data, along with metadata regarding builds, such as estimated build time. A complete list of data items collected for the specific printer model is available upon request.

WHAT DATA IS NOT COLLECTED?

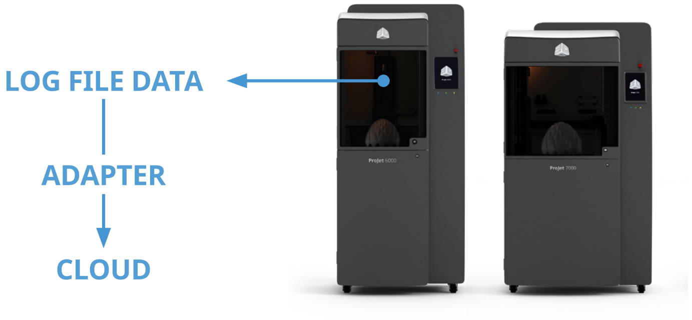
No build-file or proprietary data is collected; i.e., 3D Systems does not collect any information that would allow duplication or visibility of any parts built on the printer.

HOW DATA IS COLLECTED:

ProJet 6000 and 7000

The Projet 6000 and 7000 when operating write data to a set of log files during builds. These log files are monitored by Filebeat, a commercial open source product from Elastic. Filebeat runs natively on the printer; the data from the log files are transmitted to the adapter where the data is parsed, converted to our internal representation, and then securely transmitted to the cloud. We also collect CPU, file system, and DRAM utilization with Metricbeat, another product from Elastic. Like Filebeat, Metricbeat runs natively on the printer. Metricbeat and Filebeat are extremely efficient, small-footprint services and do not affect build times or quality.

The adapter periodically queries the printer using the 3D Systems proprietary printer-interface protocol for additional data items. This proprietary protocol is the same method by which print jobs are submitted and monitored by our client software 3D Sprint®.



With the combination of Filebeat, Metricbeat, and programmatic queries, we gather a complete set of data that indicates the operational health of the printer.

Other Printer Families

Other 3D Systems printer families proactively send data directly to the adapter when configured for 3D Connect utilization.

Secure Adapter Device

The hardware adapter is designed using an Intel NUC (Next Unit of Computing) hardware platform. The software stack on the adapter consists of the Ubuntu 16.04 LTS Linux operating system, with the internal components of the adapter running as microservices. The adapter contains only the services and ports required for connecting to the printer and operation of the 3D Connect AWS database. The adapter is preconfigured to securely communicate with the 3D Systems AWS platform and is the device that initiates outbound communication with the AWS platform through any localized firewalls.

Secure Cloud

3D Connect Service features best-in-class security structure through a partnership between 3D Systems and AWS (Amazon Web Services). Cloud Security and Compliance is a shared responsibility between AWS and 3D Systems.

AWS RESPONSIBILITY “SECURITY OF THE CLOUD”

AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

3D SYSTEMS RESPONSIBILITY “SECURITY TO/IN THE CLOUD”

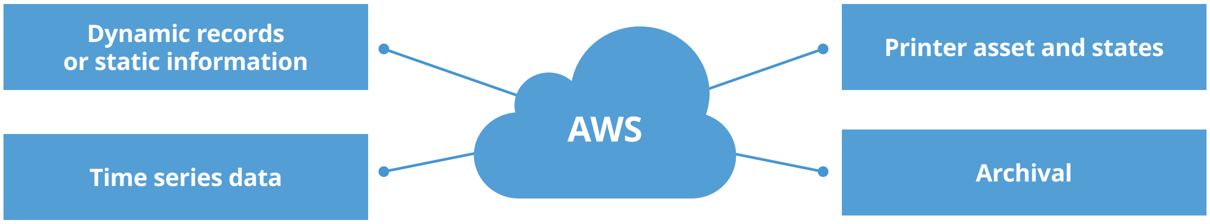
3D Systems is responsible for properly sending data to the AWS Cloud and config the AWS Cloud services based on AWS security best practices.

The primary cloud security applied by 3D Systems are listed below:

- X.509 certificate backed data transmission over a secure TLS connection
- Data at rest encrypted using AWS managed AES-256 keys
- AWS Virtual Private Cloud deployed to host key databases
- Fine-grained user authentication and authorization

DATA TRANSMISSION TO THE AWS PLATFORM SERVER

Within the adapter, 3D Systems has configured AWS Greengrass software to provide secure, X.509 certificate backed messaging over a secure TLS connection to transmit telemetry data over to the cloud. Within the cloud, an AWS IoT Core endpoint receives, decrypts, and routes messages to a variety of server-less microservices.


Dynamic records or static information

Time series data

AWS

Printer asset and states

Archival

DATA STORAGE

Data collected is stored into four different databases on the platform depending on its type:

- Dynamic records or static information
- Time series data
- Printer asset and states
- Archival

DATA ACCESSIBILITY

Data is accessed via a web portal to view information collected by the platform. Only authorized 3D Systems employees have login credentials.

Summary

3D Systems has chosen to work with AWS to ensure the highest security possible is provided to users of the 3D Connect platform. From edge to the cloud, customer security has been prioritized to deliver the best experience possible.