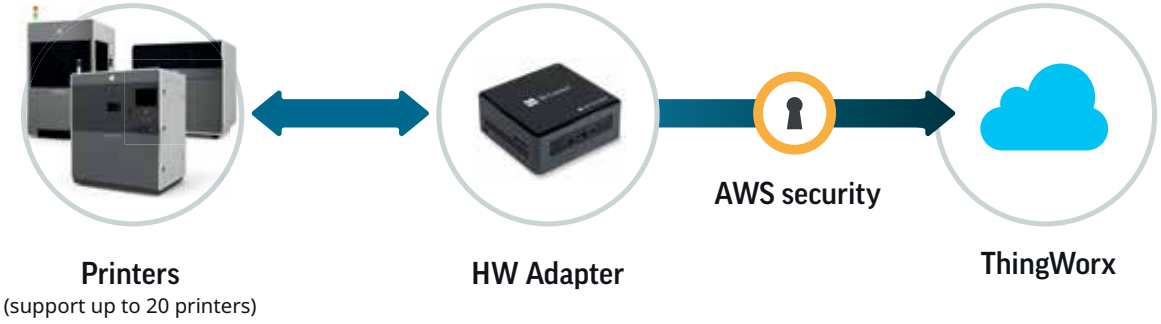
3D SYSTEMS

Co 3D Connect™

Architecture and Security

Overview

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



Data is collected from the printer(s) by the adapter, converted to an internal representation, and securely transmitted to an Amazon Web Services (AWS) hosted instance of the Thingworx platform (from PTC). 3D Systems controls and administers the Thingworx server. Only authorized 3D Systems employees have access to the AWS server.

The HW adapter can simultaneously support up to 20 printers and is the only device that requires internet connectivity; no connection to the internet is required from the printer(s).

The Thingworx platform monitors data collected from the printers 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 data collected in order to help determine whether servicing of the affected printer is required.

The connection is essentially one-way; 3D Systems does not have the ability to affect the operation of the printer in any way. 3D Systems cannot transfer any data to the printer, such as firmware, executable files, job data, etc.

Adapter internal architecture

The HW 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 within Docker containers. The Docker containers provide an isolated, secure environment for the microservices.

No data is persisted on the adapter beyond what is in memory at a given time. The adapter does not contain a webserver or any open ports beyond what is required for connection to the printer.

Data collection from printer

WHAT DATA IS COLLECTED

The data collected from printers generally consists of low-level operational sensor data, along with metadata regarding builds.

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 6K and 7K: The Projet 6K and 7K 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 logfiles are transmitted to the adapter where the data is parsed, converted to our internal representation, and then securely transmitted to the Thingworx platform. We also collect CPU, filesystem, 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.

Other printer families: Other 3D Systems printer families proactively send data directly to the adapter and no logfile-scraping technology is employed.

All printer families: The adapter also periodically queries the printer using our 3DSystems proprietary printer-interface protocol for additional data items. This proprietary protocol is the 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 an essentially complete set of data that indicates the operational health of the printer.

Data transmission to the THINGWORX patform server

Any device that connects to the Thingworx platform must be preconfigured to do so. Our adapters have been constructed such that each adapter is individually authorized and authenticated to the platform.

The Thingworx server has the following security attributes:

- Uses standard PKI infrastructure for certificate validation. Our certificates have been generated and signed by a trusted certificate authority.
- TLS 1.x support for certificate validation
- 128 bit AES encryption
- Fine-grained visibility, access, and permission model for data and services
- HTTP authentication; users must establish a web session with username and password

It is important to note that all interaction with the Thingworx server, either by the adapter or by a user, requires authentication, authorization, and is encrypted.

Data storage

Data is securely stored using an AWS-hosted database-as-a-service DB (Postgresql). The data is encrypted at rest.

Accessing data from THINGWORX

Data is accessed via a web browser using visualization tools provided by the Thingworx platform. Only authorized 3DSystems employees can access the data.

AWS security

The underlying server hosting the Thingworx platform is only accessible from specific IP addresses from the 3D Systems intranet; no public access to the operating system is possible. The Thingworx platform itself is only accessible via the standard HTTPS port 443, and has been previously described, requires a user login, or in the case of the adapter, a secret key. The key used by the adapter to access the platform is unique to each adapter.

The database used by Thingworx is only accessible from the Thingworx platform, and similar to the server, from specific IP addresses within the 3D Systems intranet.