Stairwell Forwarder

Everything you need to know

The Stairwell platform offers advanced capabilities that are able to interrogate and analyze all of your executable or executable-like files in order to detect and prevent cyber attacks.

To conduct static and dynamic analysis at the binary level, Stairwell ingests and stores every executable or executable-like file written to disk via a file Forwarder. This allows Stairwell to provide our customers with a comprehensive dataset for identifying current threats as well as attacks which have taken place in the past as all of the file information is retained in each customer's own data lake without retention limitations.

Using advanced and ground breaking techniques, Stairwell is able to quickly identify the presence of malware and variants of malware in your environment by analyzing files in the Stairwell platform rather than directly on an endpoint. By focusing on files as the true source of a threat, Stairwell enables our customers to quickly detect and respond to APTs, supply chain attacks, and other sophisticated threats.

What is the Stairwell Forwarder?
The file Forwarder used by the Stairwell platform is an extremely lightweight process and is analogous to a log shipper used by other security tools. The Forwarder's sole job is file ingestion of new and unique file types your organization is looking to have Stairwell conduct advanced threat analysis on.

The Stairwell Forwarder automatically de-dupes files. As you add more machines, you aren't necessarily adding more files; in practice you are actually adding less files, on a per machine basis, and with additional machines using the Forwarder you will only be sending new or previously unseen files to Stairwell.

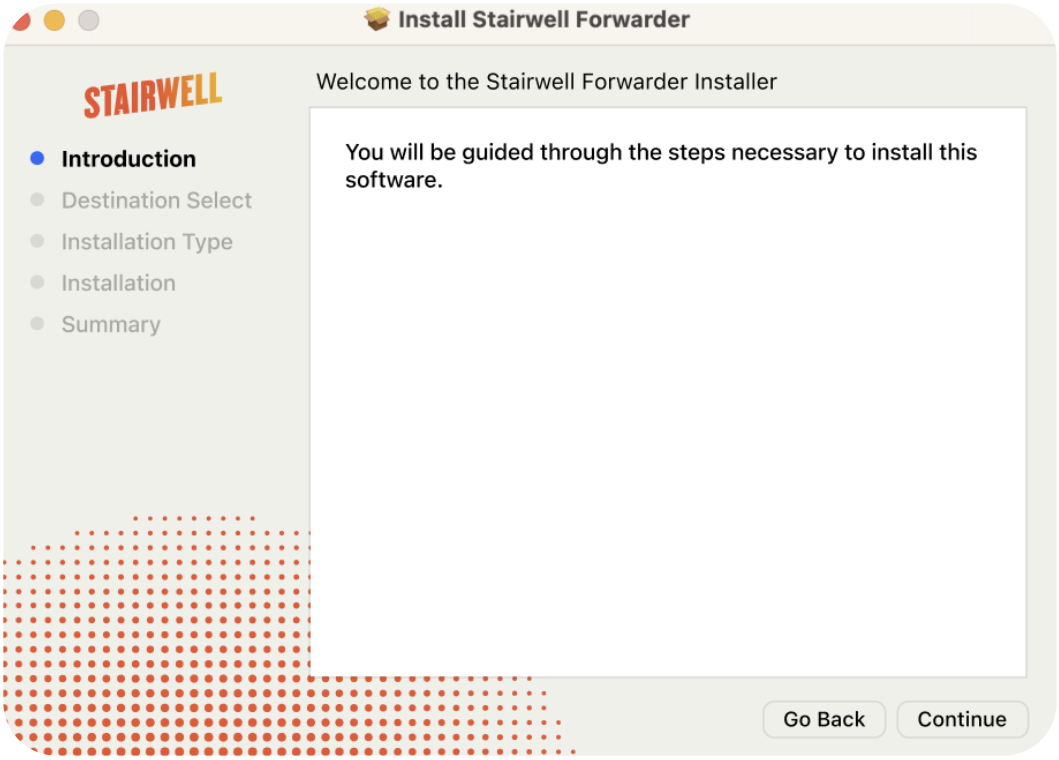
When does the Forwarder engage?
The primary function of the Forwarder is to identify in real-time when a new file is written to disk or a process has been created and has not been observed by the Stairwell platform previously. It is at this point the Forwarder determines whether a file is eligible for upload. Which files are to be included in the upload by the Forwarder is determined by your IT and security teams and is defined in the policy for your organization within the Stairwell platform.

Stairwell Forwarder

How much CPU is needed for the Forwarder?
The Stairwell Forwarder utilizes minimal resources. On average, the amount of system usage is ~25MB of RAM and less than 1% of CPU. Our customers have confirmed the Forwarder has negligible performance impact on the machines where the Forwarder has been installed.

What the Stairwell Forwarder is NOT?
The Stairwell Forwarder is not an agent and it will not hook usermode programs, and it will not perform any remediation.

The Stairwell Forwarder's primary function is to briefly analyze a file and determine if it's eligible for upload to the Stairwell platform. All major file analysis is done in the cloud, on the Stairwell platform, for both current and historical threat analysis. The files uploaded from your environment is based upon your defined policies within the Stairwell platform.

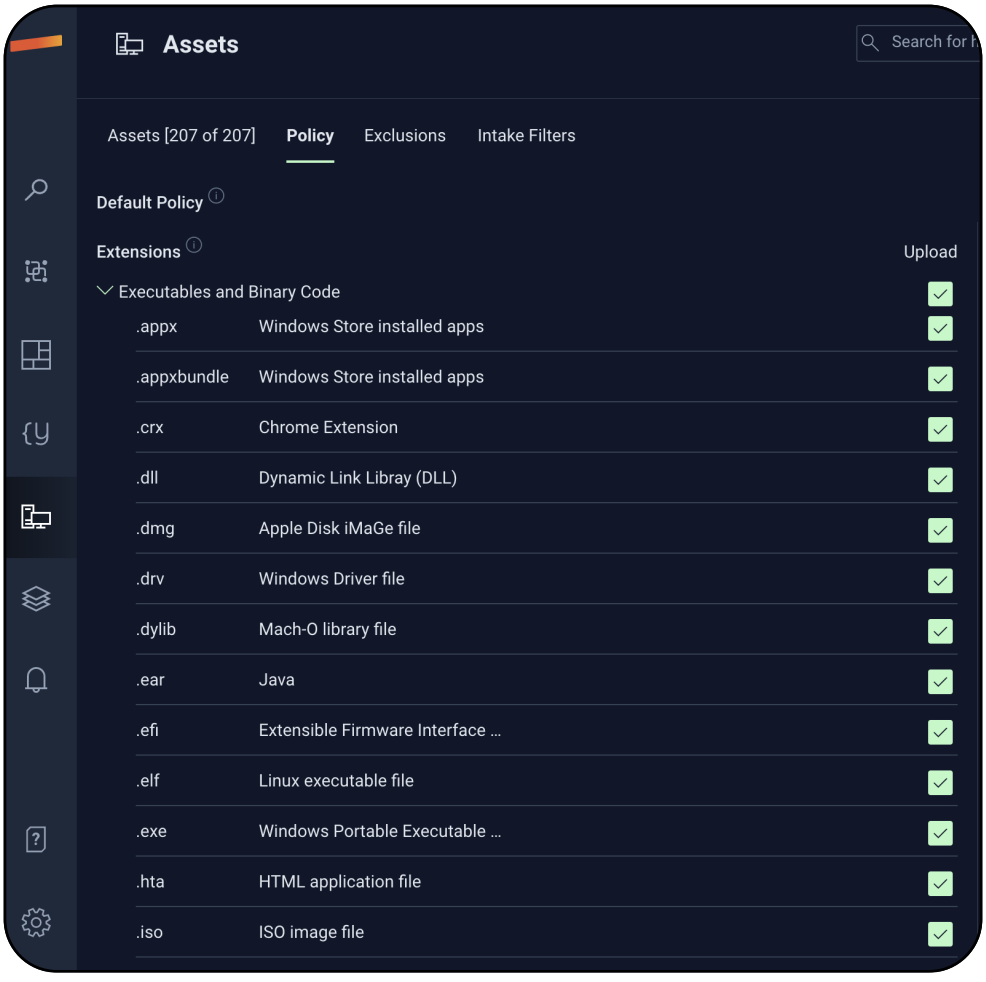


How is the Forwarder installed?
The Stairwell Forwarder is installed via an install package designed for different operating systems (Windows, Linux, MacOS, etc) and can be deployed by all common system management platforms.

Stairwell Forwarder

Although not required, it is common practice to install the Forwarder on a "golden image machine" and then roll out the Forwarder to additional user groups/departments from there.

Please note: Stairwell ingests the most common executable or executable-like files in your environment based upon your organization's policies. Your security and IT teams can customize and manage which file extensions are ingested via the defined policies for your organization.



Are there additional ways to get files to the Stairwell platform?

Yes, although the Forwarded is preferred, we understand everyone's circumstances are different and depending on the infrastructure and the systems used, there are additional ways you can send file information to Stairwell for analysis. The level of file detail and information provided by these alternatives varies and should be fully assessed to understand if they meet your security team's needs:

Stairwell Forwarder

- Your endpoint solution already supports the sharing of file information for analysis by Stairwell
  - Endpoint providers who are integrated with Stairwell: SentinelOne, CarbonBlack, Crowdstrike, MS Defender, or Tanium,
    - Please inquire with your Stairwell team to understand the level of file information and support provided by your endpoint provider
- Your systems do not support the Forwarder but still need to send the files to Stairwell
  - Stairwell provides support via our Swell CLI that includes Linux or systems such as Citrix which are supporting OT environments.

Address security gaps and stay ahead of attackers!
Today, security solutions such as antivirus and EDR solutions are focused on detecting and preventing malicious software, based on IOCs or behavioral patterns that are known ahead of time. This presents a large gap as security teams need to be able to continuously analyze all files in an environment without retention limitations, negatively impacting an endpoint, or being restricted by an OS that isn't supported.

Stairwell's solution fills the security gap where it is now possible to identify malware and its variants at any point across a given time horizon. Stairwell is able to constantly run detections and advanced queries at the binary level over your entire file corpus using neural-net and machine learning.

Now your SOC, threat hunters, and incident responders can quickly stay ahead of even the most advanced attackers by identifying both known and unknown threats!

Learn more at www.stairwell.com.