THE SMALLEST FOOTPRINT FOR HINDSIGHT IN REAL TIME.

A minimal, low-overhead forwarder that securely ships selected files and nothing more.

Most security teams don't want to deploy another "agent." Neither do we.

The Stairwell Forwarder doesn't block, scan, hook, inject, or remediate anything. It doesn't interfere with EDR, and it doesn't analyze files on the endpoint.

Think of this simply as like a Splunk Log Forwarder, except for executable files not logs.

It simply watches new files land on your device and sends any new ones to get analyzed.

WHAT WE COLLECT

If it can execute or load into memory, we collect it. This includes:

BINARIES	.appx, .appxbundle, .crx, .drv, .efi, .elf, .exe, .hta, .lnk, .sys, .com, .scr, .xpi
LIBRARIES	.dll, .dylib, .lib, .so
SCRIPTS	.ascx, .ashx, .asmx, .asp, .aspx, .bat, .cfm, .cgi, .cmd, .js, .jsp, .jspx, .php, .pl, .ps1, .py, .rb, .sct, .soap, .sh, .vb, .vba, .vbs, .vbscript, .zsh
JAVA ARCHIVES	.jar, .ear, .war, .nar
INSTALLERS	.dmg, .iso, .msi, .pkg, .sfx

HOW IT WORKS

When a new file appears, the process is surgical:

1 LOCAL HASH

The Forwarder calculates a hash locally.

2 SIGHTING

It sends a tiny REST call (hash, filename, path).

3 DEDUPLICATION

If Stairwell has the file, nothing happens. If it's new, **one copy** is uploaded... only once!

The Power of "Once": Once Stairwell has received a file from an endpoint in your environment, no other endpoint in your environment will ever upload that exact file again. Stairwell gets lighter load the more you use it.

THE INITIAL BASELINE (BACKSCAN)

The first time you deploy, the Forwarder performs a one-time inventory to establish your starting point.

OS SYSTEMS	Windows/Mac/Linux
EFFICIENCY	CPU usage is capped at **5%**.
SPEED	Takes 20 minutes to a few hours depending on volume.
INTELLIGENCE	As you deploy to more machines, backscans get faster because most files have already been seen.

Over time, the system gets lighter, not heavier.

PERFORMANCE & CONTROL

METRIC	IMPACT
RAM USAGE	~25MB
TYPICAL CPU	<1%
CPU HARD CAP	5%

YOUR ENVIRONMENT. YOUR POLICY.

REAL-TIME MODE:
Captures self-deleting malware the moment it hits disk.

SCHEDULED MODE:
Runs only at the times you choose.

FULL CUSTOMIZATION:
Define allow/deny lists, add extensions, or choose kernel vs. kernel-less mode.

FILE SIGHTING SERVICE

This isn't "another agent." It's a **file sighting service**. It is the minimum mechanism required to give you:

- Your own private, continuous malware corpus.
- Hindsight in real time.
- Operationalized threat intelligence tied to your environment.