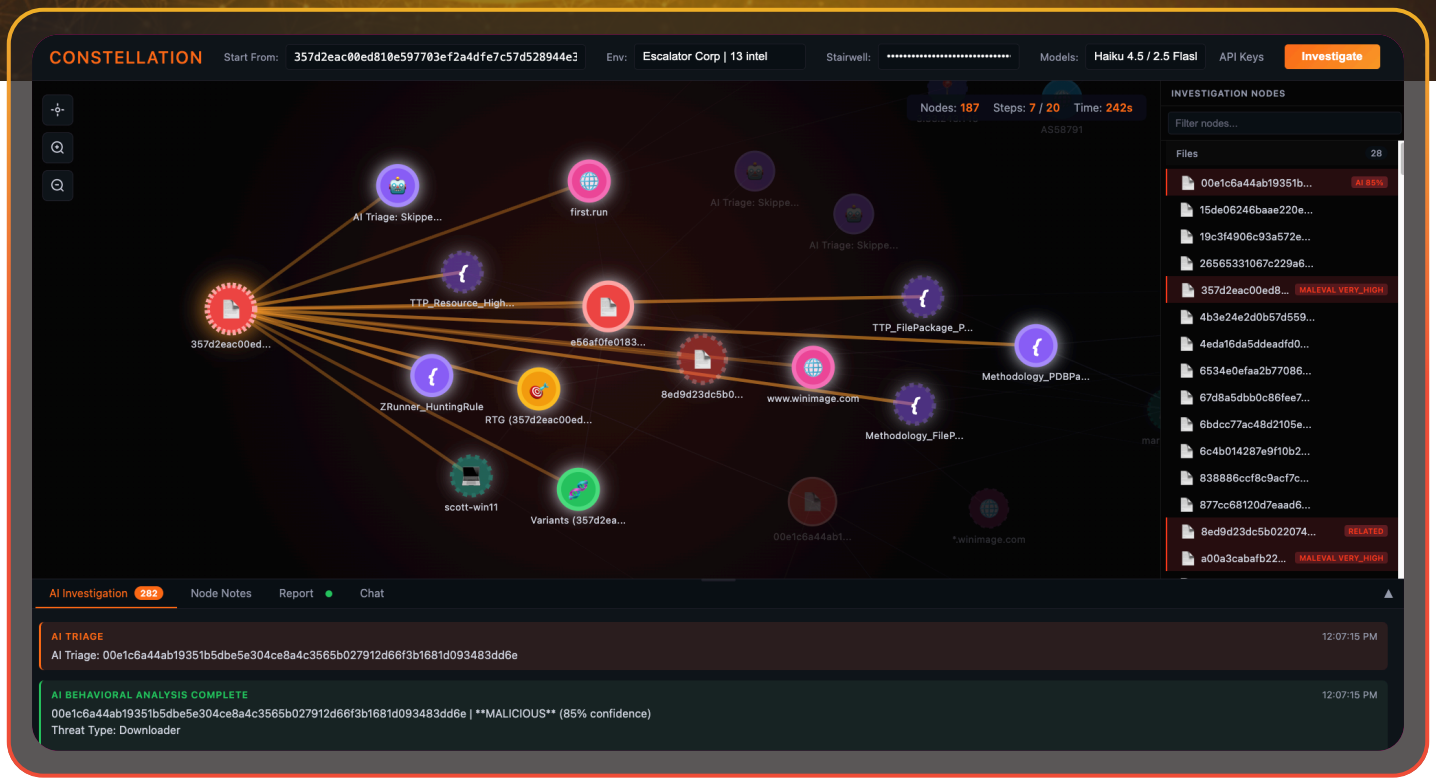
DEFINITIVE AI THREAT INVESTIGATION

Outpace AI-generated threats with agentic investigations
your AI SOC wasn't built to detect



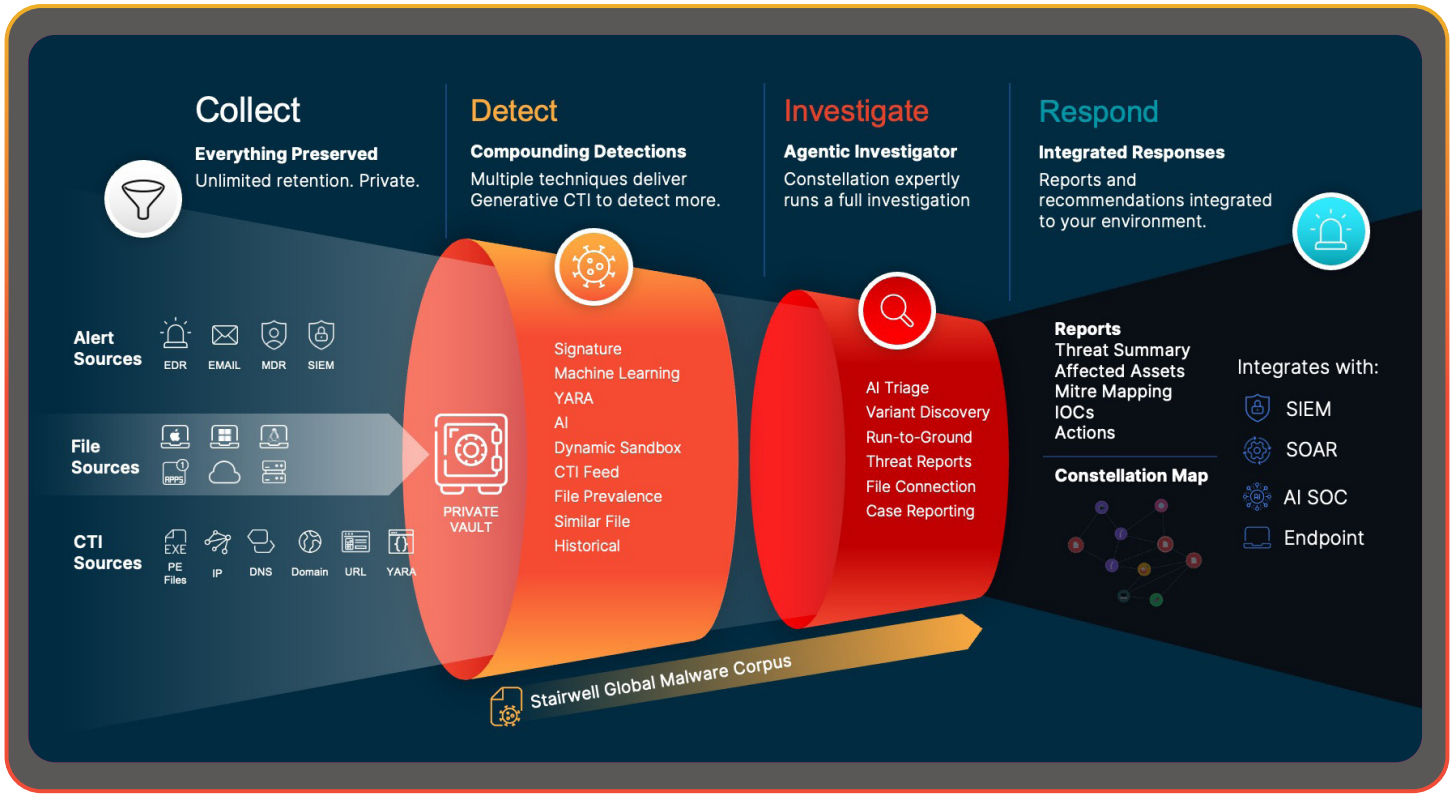
AI is changing the threat landscape by enabling attackers to make threats faster, adapt them easily, and evade detection more effectively. Within this environment, security teams are overwhelmed, drowning in alerts from fragmented tools, and struggling with slow workflows that often end with inconclusive answers.

An alert fires and SOC analysts pivot across reputation lookups, sandboxes, threat feeds, SIEM searches, endpoint tools, and peer research just to answer three basic questions:

1. **Is this file bad?**
2. **Where else is it?**
3. **Did we get everything?**

Stairwell Constellation delivers verified closure in minutes.
It runs an agentic investigation across Stairwell's platform to determine whether a threat is present, its blast radius, and what the team should do next.

HOW STAIRWELL WORKS



COLLECT:

PRESERVE THE EVIDENCE THAT MATTERS

Stairwell is built on a simple belief: files are the ground truth. Logs are incomplete. Telemetry expires. Alerts are filtered. But files reveal what actually exists in your environment. Stairwell gathers and preserves enterprise files in a private vault and connects them with alert sources, threat intelligence, malware feeds, YARA, DNS, domains, URLs, IPs, and Stairwell's global malware corpus.

Result: Stairwell Constellation investigates with high-fidelity evidence which is stronger than incomplete telemetry.

DETECT:

COMPOUND DETECTIONS FIND WHAT SINGLE TOOLS MISS

Stairwell combines multiple detection techniques including signatures, machine learning, YARA, AI Triage, threat feeds, file prevalence, similarity analysis, and historical context to detect threats more definitively. These techniques compound on one another, helping Stairwell identify repacked malware, generate new threat intelligence, and detect new variants at scale across your environment.

Result: Teams move from a single alert or IOC to a broader constellation of connected threats that other tools and AI SOCs miss.

DEFINITIVE AI THREAT INVESTIGATION

INVESTIGATE:

AN AGENTIC INVESTIGATOR TO UNDERSTAND THE BLAST RADIUS

Stairwell Constellation expertly runs the investigation for any analyst removing the technical barriers of expertise to reach understanding. It triages the alert, analyzes the file, discovers variants, checks prevalence, connects related intelligence, identifies affected assets, and determines whether the organization is impacted. Instead of manually pivoting across disconnected tools, analysts get a complete, explainable investigation with a clear outcome: confirmed found or confirmed all clear.

Result: Investigations that once required specialist knowledge and took hours, days, or weeks now reach verified closure and containment in minutes. Most constellation investigations take 200 seconds. This allows your team to focus on more important projects rather than wasting time manually pivoting between tools.

RESPOND:

INTEGRATED RESPONSES FOR YOUR ENVIRONMENT

Stairwell Constellation packages the investigation into response-ready outputs, including a threat summary, affected assets, MITRE mapping, IOCs, and recommended actions. The Constellation Map visualizes connected threats across files, variants, infrastructure, indicators, and affected assets, helping teams understand the full scope of activity. Stairwell also integrates with existing workflows, including SIEM, SOAR, AI SOC, and endpoint tools.

Result: Teams respond faster, with the evidence and context needed to act confidently. And we integrate into your existing tool stack.

MITRE ATT&CK Mapping

TACTIC	TECHNIQUE	EVIDENCE
Initial Access	T1566.002 Phishing: Phishing with Attachment	Attack chain initiated via batch script delivered to user systems (likely via email or download); no direct evidence of delivery mechanism recovered but temporal placement in user directories and downloader characteristics consistent with email-based delivery
Execution	T1059.003 Command and Scripting Interpreter: Windows Command Shell	Batch script (00e1c6a44ab19351b5dbe5e304ce8a4c3565b027912d66f3b1681d093483dd6e) is a Windows Batch file designed to execute commands; script uses 'start /B' command to execute secondary payload in background; PDB path methodology YARA matches indicate script-based execution layers
	T1106 Native API	Secondary payload executables (357d2eac00ed810e597703ef2a4dfe7c57d528944e337d71780c2d5d3ddd6283, variants 8ed9d23dc5b022074fed6dafb07c85d6620f32c73cd4e4a580e334e69c542c2f, e56afOfe01834fd6c75200ddd87d4f6ef7e1d32a97d6f329bf2dbd25410c65dd) are PE executables with high entropy and VM detection YARA matches, indicating direct native API calls for evasion and execution control
	T1204.002 User Execution: Malicious File	Batch script (001c6a44ab19351b5dbee304ce8a4c3565b027912d66f3b1681d093483dde) relies on user execution or scheduled/automated execution to trigger initial payload download; discovered in user-accessible directories (AppData\Local\Temp\)
Defense Evasion	T1027 Obfuscated Files or Information	Multiple payloads exhibit high Shannon entropy (7.93-7.97) indicating encryption/packing; embedded unsigned PE files within PE containers (TTP_FilePackage_PE_embedded_unsigned YARA match); suspicious PE overlays detected (SUSP_PE_at_Overlay); non-standard tool names (zcurl.exe vs.standard curl.exe) used in downloader
	T1036.005 Masquerading: Match Legitimate Name or Location	Payloads exhibit Methodology_Masquerade_Microsoft_NonStdPDB YARA matches indicating masquerading techniques; some files signed with Microsoft Code Signing signatures despite malicious behavior, suggesting signature spoofing or code signing compromise

WHY SOC TEAMS CHOOSE STAIRWELL?

INVESTIGATE FASTER

Stairwell Constellation automates complex analysis and eliminates repetitive pivots, helping every SOC role investigate faster. A platform for everyone including SOC analysts, threat hunters, incident responders, and threat intelligence analysts.

REDUCE LOG RELIANCE

Because Stairwell preserves and analyzes files as the source of truth, teams can reduce dependency on high-volume expensive log storage for certain investigation workflows helping lower SIEM costs while maintaining durable evidence.

SEE MORE THREATS

By continuously analyzing files and connecting them to threat intelligence, together with compounding detection techniques, Stairwell helps teams find related variants, repacked malware, and threats or infections that traditional tools miss.

REDUCE TOOL SPEND

Stairwell's agentic platform consolidates capabilities typically spread across reputation lookups, sandboxes, threat feeds, threat intelligence platforms, malware analysis tools, and manual investigation workflows. With Stairwell you eliminate many tools from your budget.

FROM ALERT TO VERIFIED CLOSURE

Stairwell Constellation gives SOC teams a faster, more definitive way to investigate AI-era threats.

Gather the evidence. Detect connected threats. Investigate with an agentic expert. Respond with confidence.

About Stairwell

Stairwell helps security teams investigate faster, reduce tool sprawl, and detect AI generated threats that other tools miss. Its private continuous threat intelligence platform gives organizations hindsight across every file they have ever seen while keeping sensitive samples out of public repositories. With Constellation, Stairwell's agentic investigator, teams move from alert to definitive answer without bouncing between EDR, SIEM, sandboxes, threat feeds, and standalone analysis tools. Stairwell connects suspicious files to related variants, historical sightings, infrastructure, and enterprise exposure, giving analysts the context to decide what matters, where it appeared, and what to do next. The result is faster triage, definitive investigations, lower spend on redundant tools, stronger containment proof, and time back for every SOC analyst, threat hunter, and incident responder.

Private by design. Continuous by default. Hindsight in real time.

CONTINUOUS ANALYSIS OF EVERYTHING. IN YOUR OWN PRIVATE VAULT.

STAIRWELL.COM/REQUEST-A-DEMO/

STAIRWELL