The Stairwell platform

The Stairwell platform is revolutionizing the security game by automatically monitoring and analyzing every executable or executable-like file in your organization, collecting crucial intelligence and providing your security team with in-depth analysis and evidence. Stairwell tackles critical gaps in modern security tooling by preventing evolving threats and detecting both known and unknown attacks. Stairwell supercharges your security team's abilities, providing them with the confidence to overcome any attack decisively and quickly.
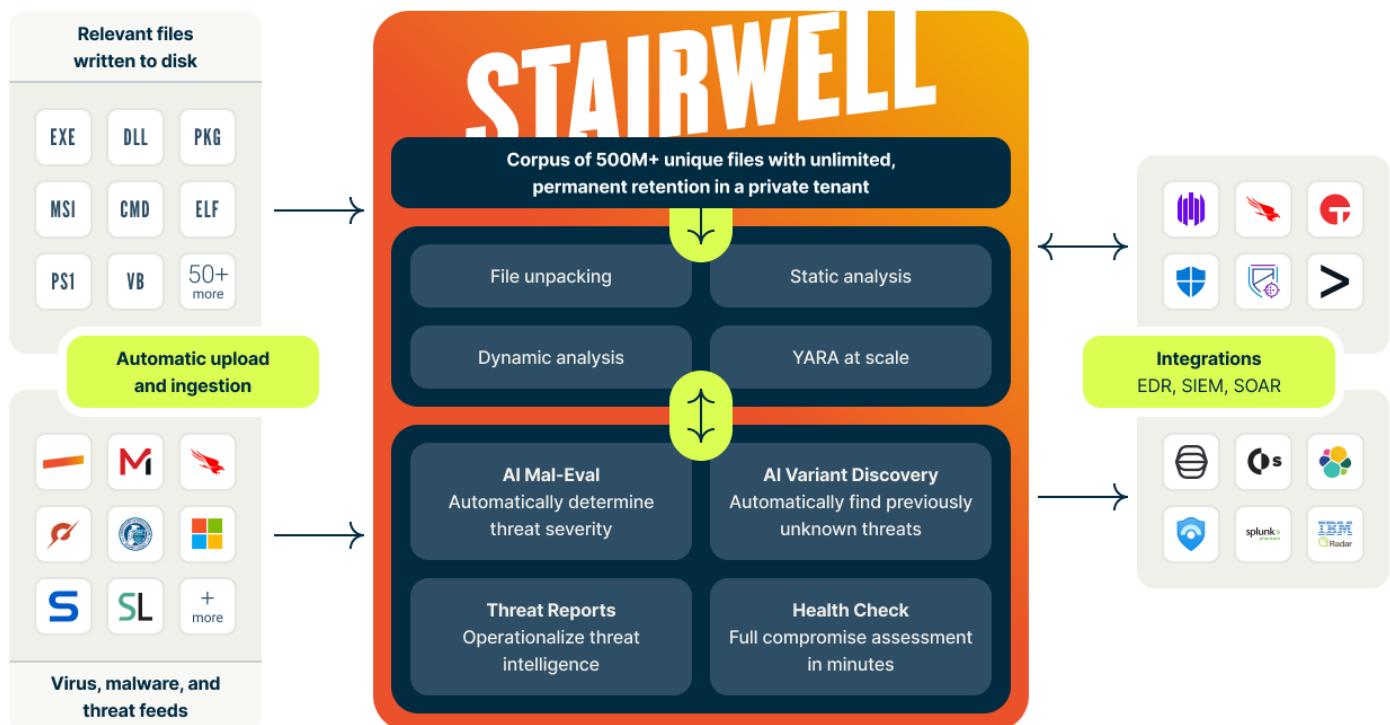
Stairwell helps you stay ahead of attacks

- **Continuous analysis**: Overcome gaps of other security tools with continuous dynamic and static analysis of files at the binary level.
- **Compromise assessment in minutes**: Answer, "Have we been impacted?" with confidence - conduct a full-scale assessment with automatic, examination-based verdicts on all files.
- **Unlimited file retention:** Stairwell automatically ingests all of your executable or executable-like files and stores them indefinitely, overcoming point-in-time limitations and providing instantaneous insights of an attack, from today or from any point since adopting the Stairwell platform.

- **Forensic analysis in seconds:** The platform employs neural-net-based analytics, YARA at scale, and Stairwell's automated Variant Discovery against the latest threat intelligence, helping protect your organization against evolving threats.
- **Confidence with peace of mind:** Whenever there's a new alert, new threat intel, or the CEO wants to know more, know with certainty and in seconds whether your environment is or has ever been compromised by a threat since adopting the Stairwell platform.

Detect & hunt ◈	Respond ◈	Automate & reduce cost ◈
Automatically detect both known and unknown threats across your files with advanced analytics, leaving attackers with no place to hide or the ability to evade. Automatically scan and detect across your environment with the latest threat intelligence.	Leverage advanced analytics and tools like YARA with automated ingestion of IOCs to conduct full-scale, forensic-based assessments in minutes. Know with certainty if a file is malicious with Stairwell Mal-eval.	Get an automated review of risks associated with threats via the Stairwell Health Check report. Conduct advanced, binary-level investigations quickly and respond to advanced threats in minutes. With unlimited file retention, there are no hidden costs.

Next-level threat detection & automation

- **Hindsight, insight, foresight**

Continuous and on-demand scanning of all of your executable files, past or present, to detect threats and create instantaneous insights that help your teams stop an attack.

- **Integrates into your existing workflows**

Use pre-built or custom integrations to connect Stairwell with traditional security tools like EDR, AV, SIEM, and SOAR to provide a forensic-based level of analysis and insights for action.

- **Operationalize threat intelligence**

Automatically ingest and parse IOCs/signatures from all of your threat report feeds and scan your environment (past and present) within minutes – automatically.

Supercharge your security team

Whether a SOC analyst, threat hunter, or incident responder, and regardless of experience, they will be able to easily leverage sophisticated tools like YARA, Stairwell Mal-eval, or Variant Discovery to take quick action with confidence. Visit stairwell.com to learn more.

STAIRWELL