



Stairwell Platform

Threat Detection and Incident Response Platform

Traditional threat detection and incident response offerings fail to keep up with evolving threats. These offerings miss sophisticated attacks that are designed to evade detection and wipe their tracks. On-device detection engines used by EDRs and other products are vulnerable to these types of attacks and must balance threat detection and user experience, often compromising on both. An over reliance on logs results in incomplete visibility, limited detection opportunities, and less effective incident response.

Stairwell overcomes the limitations of these traditional cybersecurity offerings. Stairwell's threat detection and incident response platform is built on an evasion-resistant architecture. Rooted in the concept of continuous improvement, Stairwell is able to instantly apply and derive new learnings from everything an organization has ever seen. Leveraging static, dynamic, and AI-powered analysis out of the reach of your adversaries, Stairwell protects your past, present and future.

Stairwell Innovation

Stairwell's evasion-resistant architecture captures and preserves every executable and related artifact in a secure cloud vault. This enables organizations to analyze and continuously re-analyze files using the latest Cyber Threat Intelligence (CTI). Stairwell employs a wide range of detection methods and sources including Stairwell's own threat research team, threat intelligence feeds, and Stairwell's AI analytics engine. Truly cloud-based analytics offer faster and more scalable detection than traditional cybersecurity offerings.



KEY BENEFITS

- ✓ Detect malware that evade traditional AVs and EDRs
- ✓ Historical insight even if malware was previously deleted
- ✓ Cloud-based analytics with no impact to device performance
- ✓ Proactively identify possible malware variants
- ✓ YARA rules at scale across all executables and related artifacts

Key Capabilities

Evasion-Resistant Architecture Adversaries constantly refine malware to evade many security offerings such as AVs and EDRs. Stairwell's evasion-resistant architecture uses a lightweight forwarder to send executables and related artifacts to the cloud for preservation and analysis. Since no analytics run on the device, it's difficult for adversaries to figure out how to avoid detection by Stairwell.

Rapid Detection with Out-of-Band Analytics Stairwell performs all threat detection in the cloud, offering speed and comprehensive analytics that on-device solutions cannot match. Stairwell's detection engine constantly improves with new techniques, ensuring accurate threat detection without slowing down servers or endpoint devices.

Superior Insight with Historical Threat Analysis Stairwell preserves all executables and related artifacts since the first day of deployment. This allows new detection techniques and vulnerability analysis to be applied to everything in the private data vault. Organizations gain insights not possible with traditional solutions such as when they were first compromised, which security gaps need attention, and what malware previously existed in their network.

Proactive Malware Variant Detection Adversaries continuously modify their malware to avoid detection, leading to countless malware variants. Instead of simply reacting to these new variants, Stairwell's Variant Discovery uses advanced analytics on all preserved files to identify possible variants. This proactive approach helps organizations stay protected against this ever growing problem.

Gain Hindsight, Insight and Foresight with Stairwell

Stairwell's innovative approach helps organizations quickly detect cyber attacks that evade traditional security offerings while continuously improving their defenses. The AI-powered analytics and evasion-resistant architecture future-proof organizations against advanced threat actors. With Stairwell, organizations can stay resilient before, during, and after cyber attacks.