

# WHY STAIRWELL IF YOU ALREADY HAVE AN EDR?

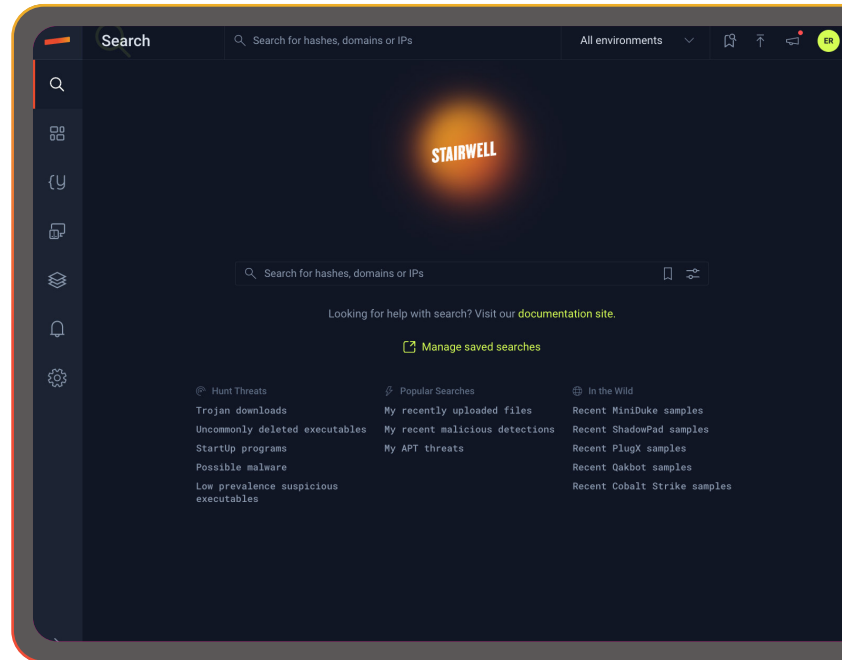
EDR Sees What Executes. Stairwell Explains.

## THE PROBLEM: LIMITED EDR VISIBILITY

An endpoint detection and response (EDR) tool is built for runtime detection. It tells you when something executes on an endpoint. It generates alerts based on behavior. Unfortunately, not everything runs, and the reality is that what doesn't run can still matter. EDR only shows the execution moment. Not the full picture.

## THE GAP: ALERTS WITHOUT UNDERSTANDING

EDR produces alerts. But every alert is more than a notification. It is evidence. A signal that something happened somewhere. Most teams treat alerts as a burden. Something to triage and close. The result is partial and fragmented investigations, limited in scope, and falsely assumed containment. Typically, the real problem is beyond one single alert. Visibility to connected threats is ignored in a world where closing tickets matters more.



## THE SOLUTION: STAIRWELL CONNECTS THREAT INTELLIGENCE TO YOUR ENVIRONMENT

Operationalize the intelligence EDR already gives you.



### FROM ALERTS TO INTELLIGENCE

Every EDR alert becomes a starting point for full investigation instead of just a ticket to close.



### SEE WHAT EXISTS

Analyze every file across your environment, whether it executed or not.



### UNDERSTAND FULL SCOPE

Instantly map related files, variants, and spread across your environment.



### PROVE CONTAINMENT

Know exactly where a threat exists and where it does not and you are "All clear".

# WHY STAIRWELL IF YOU ALREADY HAVE AN EDR?

TECHNICAL DATASHEET | STAIRWELL + ENDPOINT DETECTION & RESPONSE (EDR)

## HOW EDRs & STAIRWELL WORK TOGETHER

### EDR

- ✔ Tells you something ran that triggered a behavior signature.



### STAIRWELL

- ✔ What it is?
- ✔ What else is related?
- ✔ Where it exists across your environment?
- ✔ Is it truly gone?

## WHY STAIRWELL MATTERS

EDR alerts are not noise. They are intelligence for security teams to operationalize. Stairwell turns that intelligence into understanding. From one alert, you get full context including scope, impact, and exposure. Stairwell removes sampling and eliminates guesswork. Instead containment is proven and never assumed.

## STAIRWELL DELIVERS

### TURN ALERT VOLUME INTO INTELLIGENCE VALUE

Every detection becomes actionable insight rather than operational burden.

### REDUCE RISK EXPOSURE

Understand the full blast radius of threats, not just the triggering event.

### ELIMINATE BLIND SPOTS

Analyze every file, instead of only those that executed.

### INCREASE ANALYST LEVERAGE

Replace manual triage with instant, complete investigations.

CONTINUOUS ANALYSIS OF EVERYTHING. IN YOUR OWN PRIVATE VAULT.

[STAIRWELL.COM/REQUEST-A-DEMO/](https://stairwell.com/request-a-demo/)

STAIRWELL