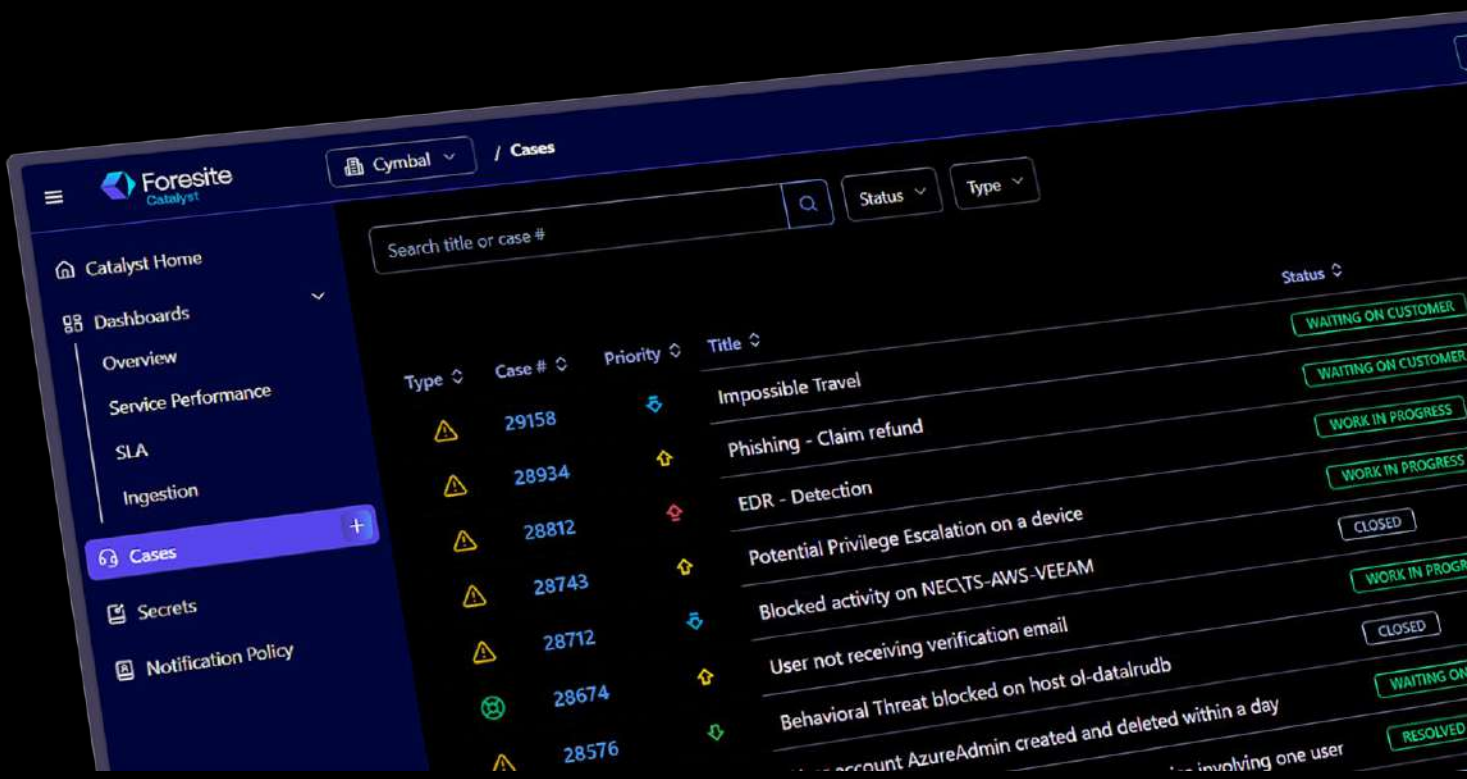


Foresite Cybersecurity

Enhancing every managed alert with agentic AI

FORESITE MANAGED SERVICES · MANAGED DETECTION & RESPONSE · JUNE 2026

Catalyst Triage Agent

OVERVIEW

AI-accelerated triage, human-owned judgment

Foresite has built an AI Triage Agent that runs internally within Foresite's security operations pipeline as part of our MDR process. AI is assisting and accelerating our analysts as they work your incidents — before your analysts ever open a case. When a detection fires, the Triage Agent automatically gathers context, evaluates the evidence, and delivers prepared data and recommendations to the analyst.

What you see in Catalyst is a clear result: prepared by our analysts and accelerated by agentic AI.

THE PRINCIPLE

Autonomous triage runs at machine speed. Named practitioners validate every high-impact action before it executes.

Agentic never means uncontrolled.

Seconds
to a prepared, oriented case

Every alert
consistent depth, any shift or volume

24×7
Foresite MDR owns every verdict

HOW IT FITS TOGETHER

The Foresite incident response pipeline

Foresite's managed security services are built on Google Unified Security: Google Security Operations, Google Threat Intelligence, and the broader Google Security Operations stack. Every alert that enters our pipeline is automatically enriched — IOC reputation, MITRE ATT&CK mapping, entity history, behavioral signals, and timeline reconstruction. That enrichment has always been the foundation of how our analysts investigate and reach verdicts on your behalf.

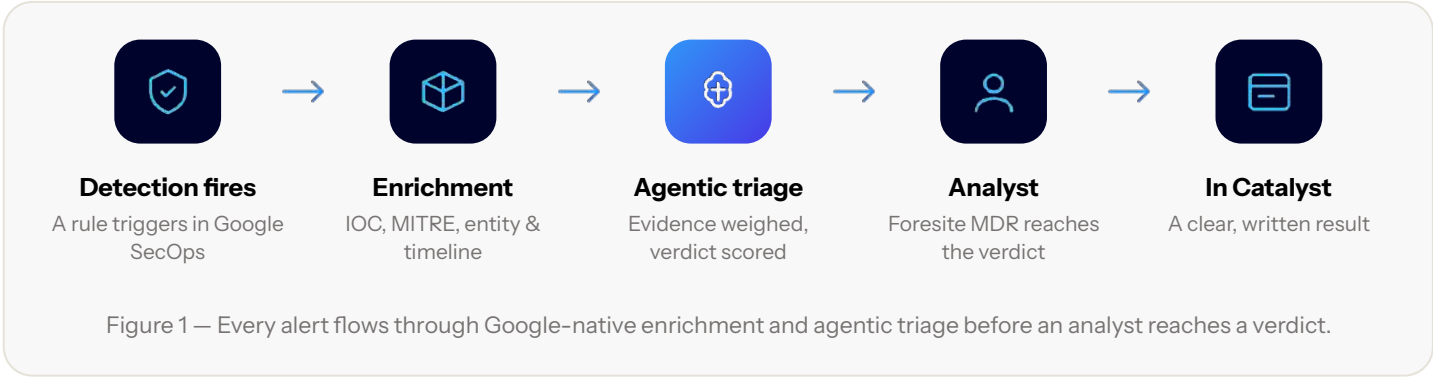


Figure 1 — Every alert flows through Google-native enrichment and agentic triage before an analyst reaches a verdict.

WHAT IS NEW

Agentic triage

What changes now is how that enrichment occurs and how fast it reaches our analysts. Previously, an analyst assessed the alert, collected data from many sources, reviewed it, and wrote an assessment. With the Triage Agent, the initial review, data collection, and preliminary investigation are done by agentic AI in seconds — so analysts arrive at an investigation that is already oriented, not a blank slate.

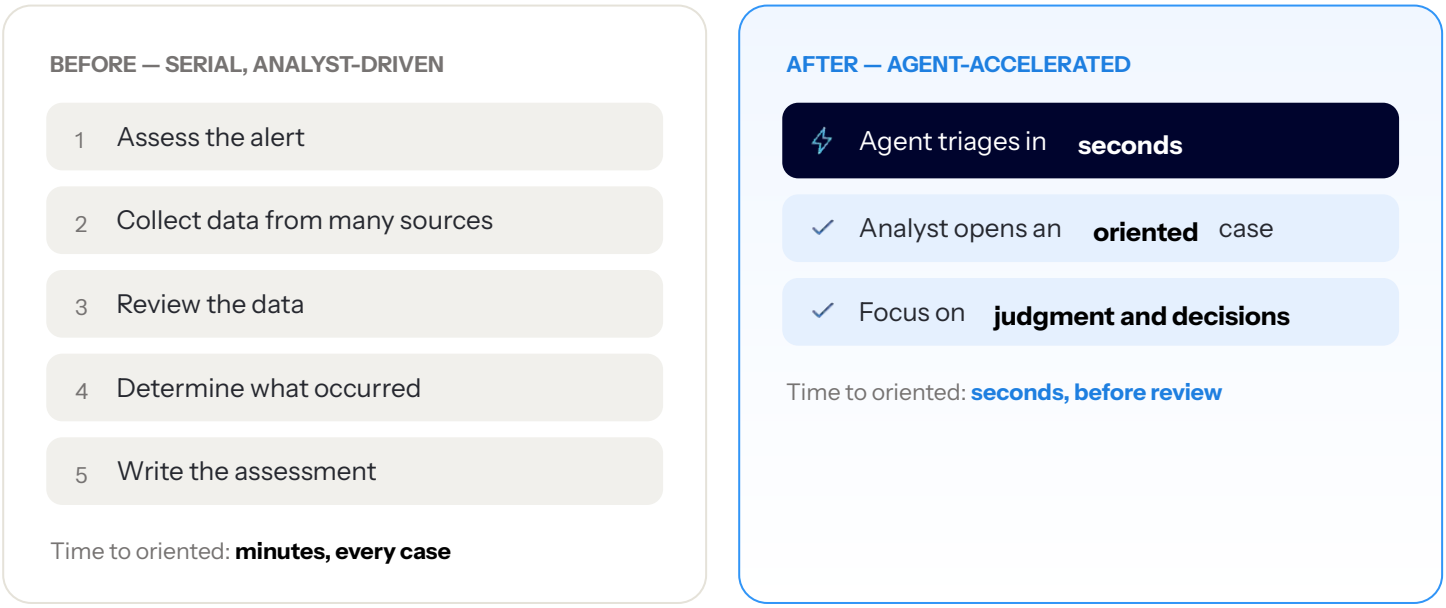


Figure 2 — The agent absorbs the orientation work that used to open every investigation.

Faster resolution — analysts focus on investigation and decision-making, not on gathering context.

Consistent, thorough analysis on every alert — not dependent on shift, analyst experience, or volume.

A clear written explanation of what happened, why it fired, and the evidence — visible in Catalyst.

IN CATALYST

Every case opens with an agentic triage

Rather than a summary of a detection rule firing, each case opens with a prepared triage: a written explanation of what happened, the evidence evaluated, and a confidence-scored verdict. Foresite analysts use it as the starting point for their investigation.

CATALYST · CASE INC-4821

Suspicious OAuth grant to third-party app

True Positive · 88%

EVIDENCE EVALUATED

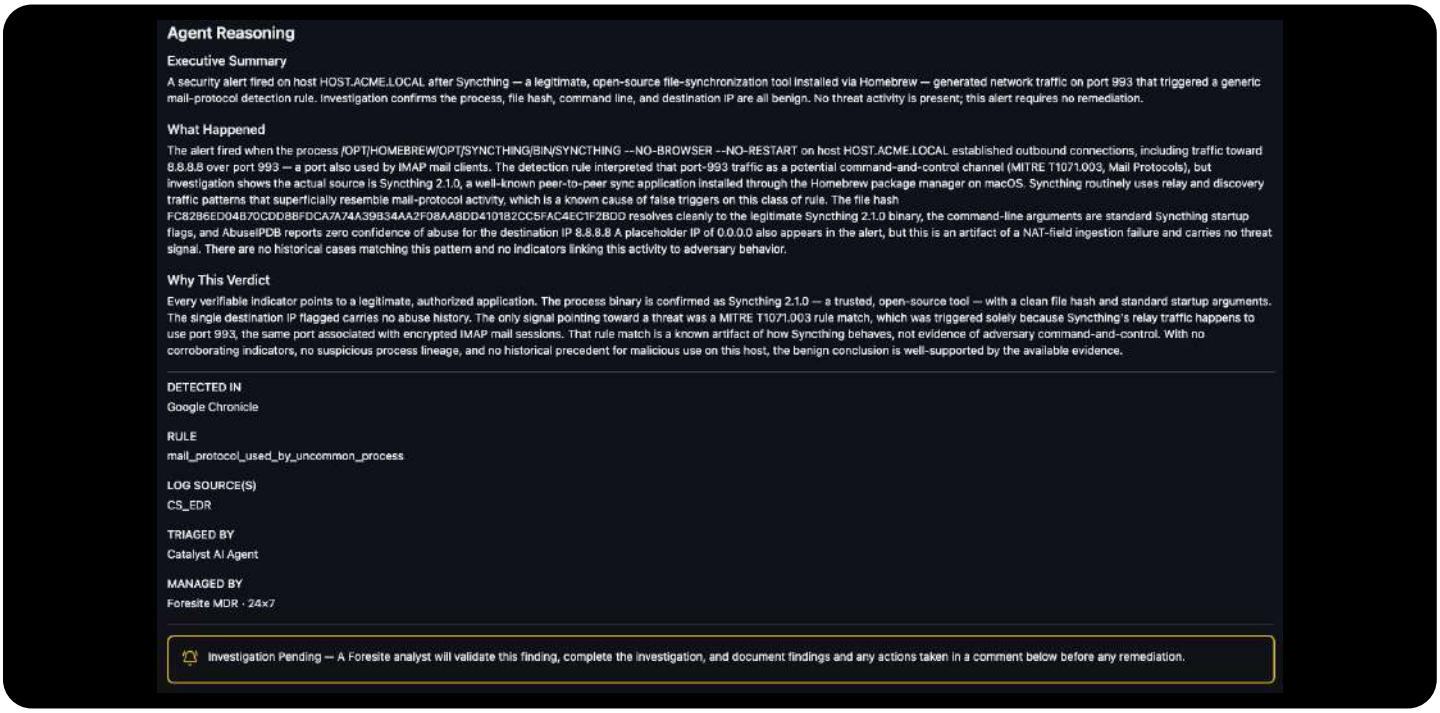
- IOC reputation — grantee domain flagged malicious (GTI)
- MITRE ATT&CK — T1528 Steal Application Access Token
- Entity history — first grant from this account in 90 days
- Timeline — followed an anomalous sign-in from a new ASN

CONFIDENCE

88 %

Prepared by Catalyst AI Agent · validated by a Foresite analyst before it reaches you

Figure 3 — Illustrative agentic triage: a written explanation, the evidence, and a confidence-scored verdict.



NEW IN CATALYST

Context Hub

Alongside the Triage Agent, we are releasing Context Hub. It gives your team a place to tell the agent what matters most in your environment. When a detection involves an asset or account you have registered, the agent weights its assessment accordingly — surfacing cases that might otherwise appear routine.

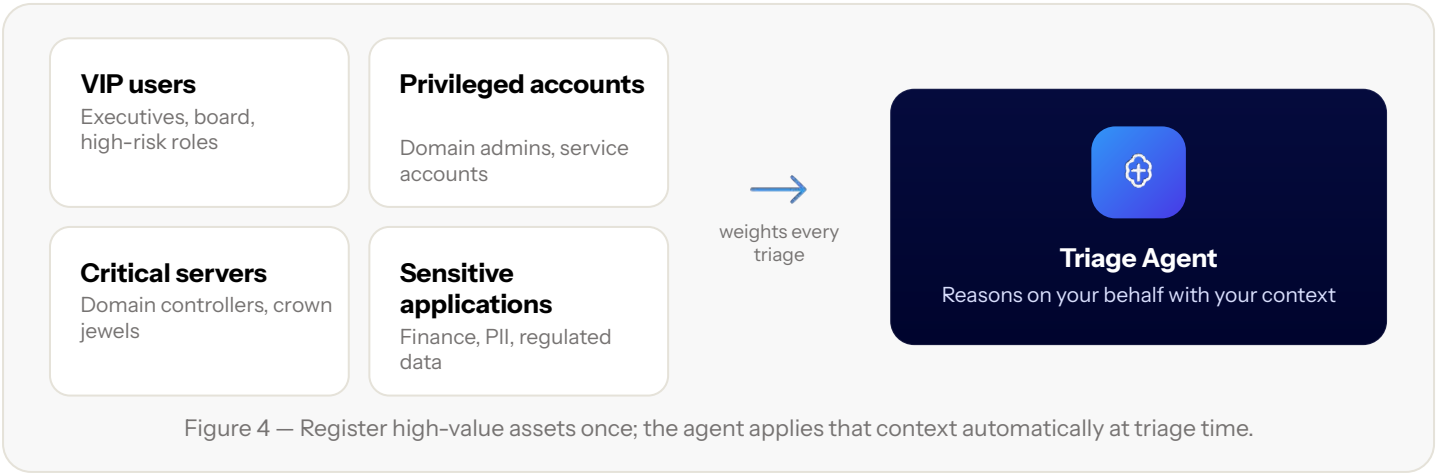


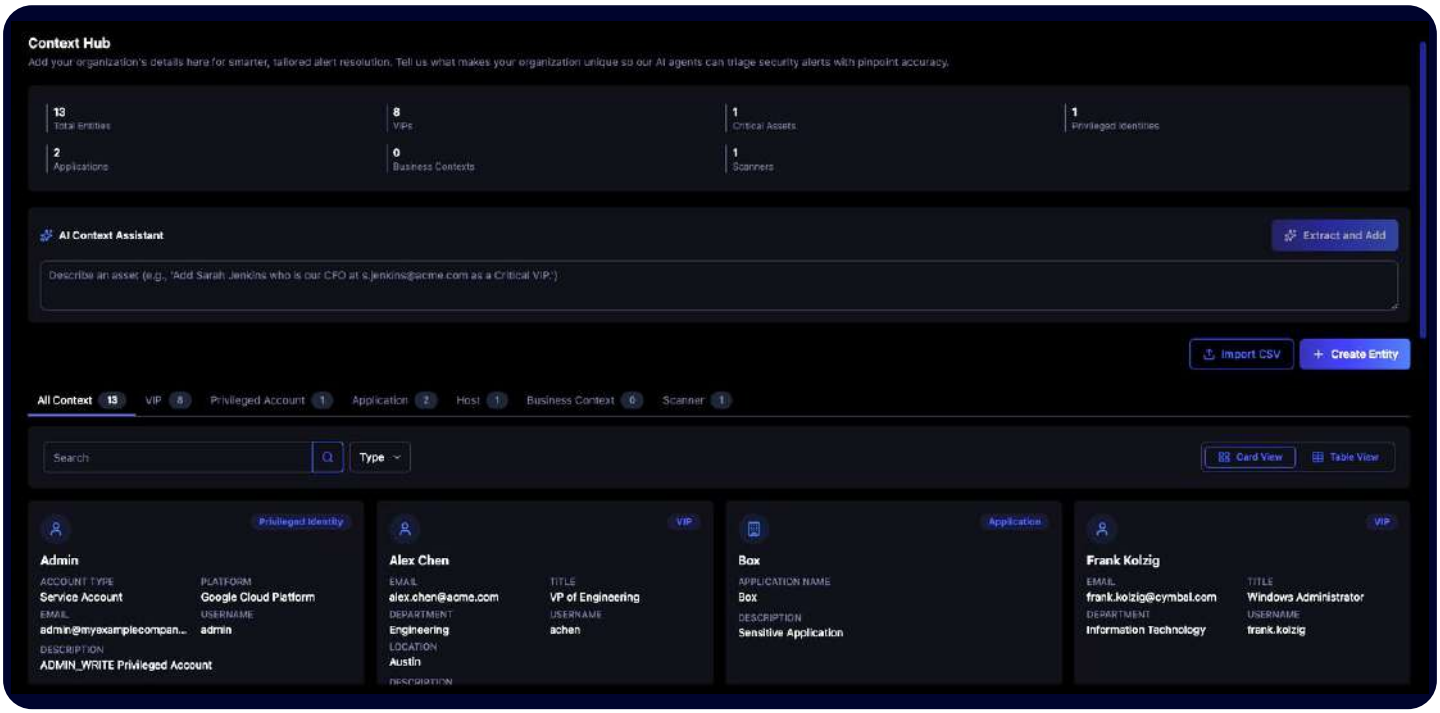
Figure 4 — Register high-value assets once; the agent applies that context automatically at triage time.

Register assets directly in Catalyst — VIP users, privileged accounts, critical servers, and sensitive applications, with no professional services required.

The agent incorporates your context automatically at triage time. The more you define, the more precisely it reasons on your behalf.

Included in your managed service at no additional cost.

Figure 3 — Illustrative agentic triage: a written explanation, the evidence, and a confidence-scored verdict.



INSIDE YOUR SERVICE

Built on Google. Stays on Google.

The Triage Agent runs entirely within Foresite's Google Cloud infrastructure, deeply integrated with Google Unified Security. There is no third-party AI vendor involved, no data leaving the Foresite environment, and no AI compute cost passed to your organization. Foresite absorbs the operational cost as part of your managed service.

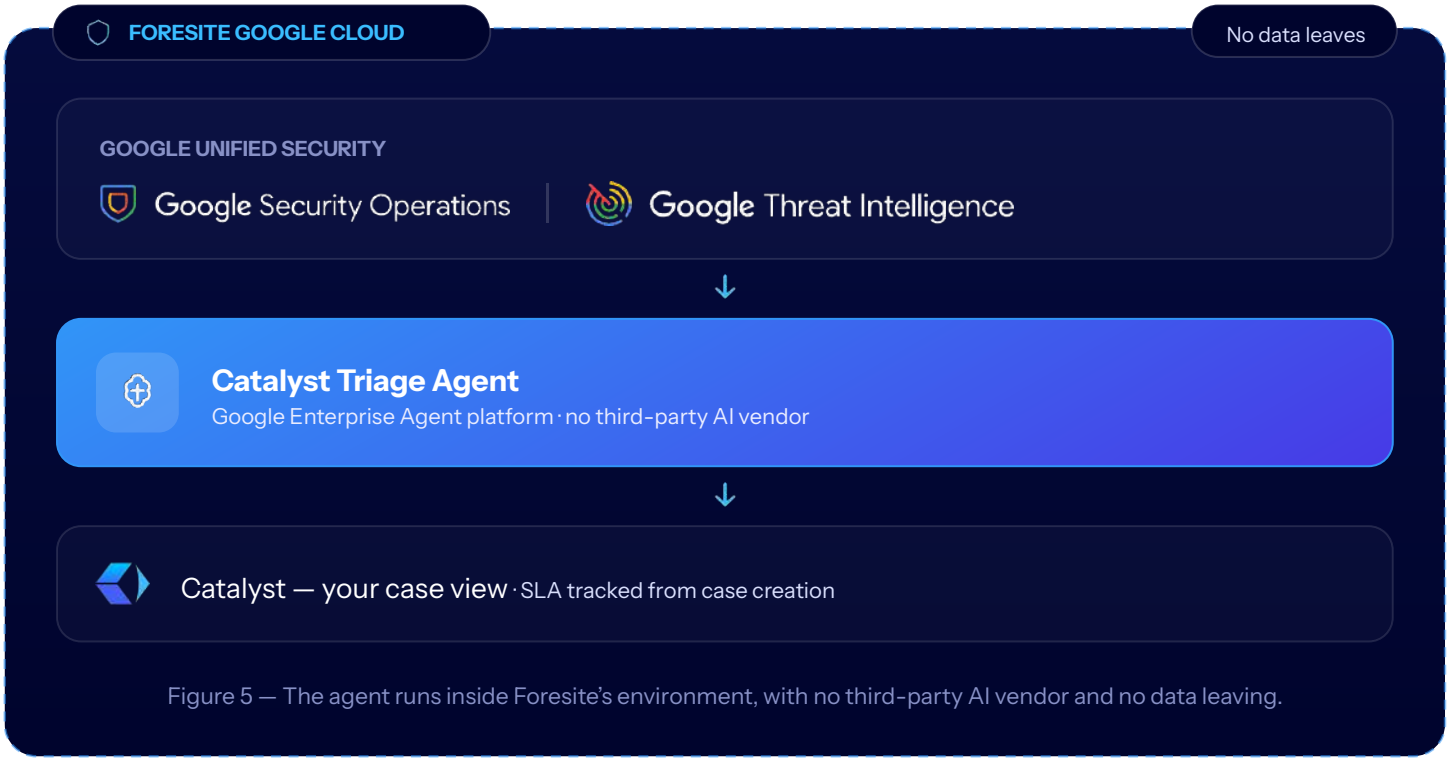


Figure 5 — The agent runs inside Foresite's environment, with no third-party AI vendor and no data leaving.

Zero configuration
Activates automatically on every alert — no playbook changes.

Posts before review
Agentic triage posts to your case before analyst review begins.

SLA from creation
SLA tracking begins the moment the case is created.

THE FOUNDATION

Why this works: SecOps engineering excellence

The efficiency and quality of agentic triage depends entirely on what sits beneath it: healthy client integrations, well-structured log sources, and detection rules that are precise and purposefully built. Foresite's years of Google SecOps engineering are the prerequisites that make the Triage Agent effective — an agent working from a well-engineered environment produces the quality of analysis you see in Catalyst today.

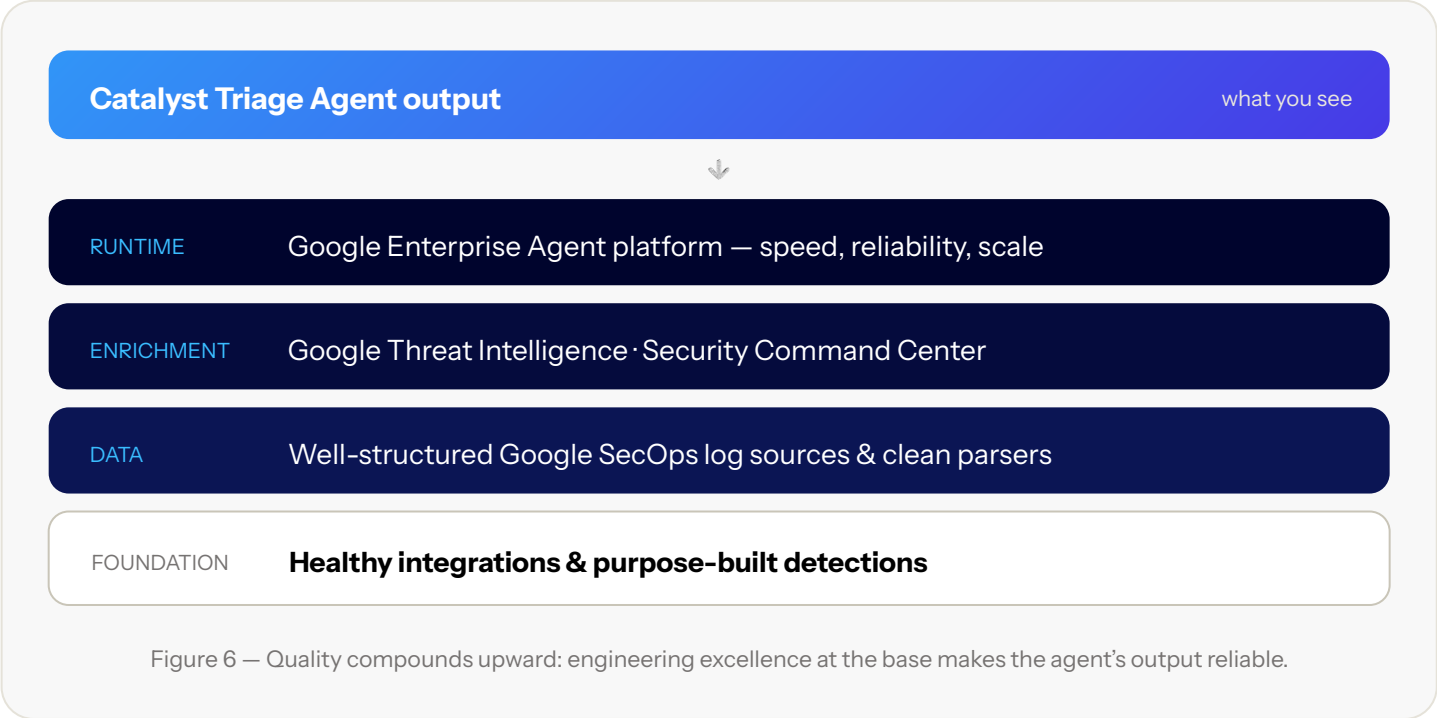


Figure 6 — Quality compounds upward: engineering excellence at the base makes the agent's output reliable.

Token efficiency — Google-native enrichment feeds structured, high-quality inputs rather than raw logs, so every token counts.

Balanced enrichment and agentic depth — reputation, entity context, and correlation happen before the agent reasons only where needed.

Runtime efficiency at Google scale — built into the same stack that powers the detection and response pipeline, not bolted on.

NEXT STEPS

Already included. Rolling out now.

The Catalyst Triage Agent is rolling out across Foresite's managed services. Your Foresite team will walk you through what to expect in your case view and work with you to populate Context Hub with your high-value assets.

- Rolling out across Catalyst, Citadel, Command, and Adapt
- No procurement decision and no new tooling required
- Your Foresite team walks you through Context Hub setup

Google Security Operations | Google Threat Intelligence | Mandiant