Transform cybersecurity
from a barrier into a Catalyst

foresite.com

google@foresite.com

Foresite
Cybersecurity

Predict and prevent, with Google-grade threat intelligence. Proactive threat management and dark web monitoring — delivered as a managed service.

Version: 1.0
Revised: Jun 16, 2026

Catalyst Command

Catalyst Command

Cybercriminals move fast. Catalyst Command moves faster.

Command is Foresite's managed threat-intelligence module, powered by Google Threat Intelligence (GTI). It continuously scans the dark web and open sources for references to your people, brands, and assets - then escalates findings to Foresite's Cyber Fusion Center for investigation and response. Command gives security teams early warning of the threats taking shape outside their perimeter.

Threats take shape outside your perimeter - where you can't see them

Leaked credentials, spoofed brands, and exposed assets are traded and weaponized long before they surface as an incident. Without external threat intelligence, the first sign of compromise is the breach itself.

01 Stolen credentials are sold and reused for **initial access** before they're noticed

02 Brand and executive **impersonation** evades perimeter controls and erodes trust

03 Unknown internet-facing assets quietly **expand the attack surface**

04 Raw threat feeds generate **noise without the context** to act on them

Threat intelligence, operationalized by experts

Four always-on monitoring services powered by GTI - plus on-demand threat management: advisory, training, and industry threat-actor analysis from named Foresite experts.

Proactive dark web monitoring

Continuously scans dark web and underground sources for references to your critical resources — domains, VIPs, email addresses, and product names — using Google Threat Intelligence

Leaked credential monitoring

Surfaces compromised employee and customer credentials before threat actors can use them for initial access — closing the gap attackers rely on most.

Brand monitoring

GTI-driven monitoring of your brands and executives for impersonation, spoofing, and reputational threats — across domains, social, and the open web.

Attack surface management

Initial discovery at onboarding, then recurring reports on new internet-facing assets and exposures — each with prioritized, practical change recommendations.

Run Command standalone - or amplify it with Citadel

Standalone deployments require GTI licensing procured independently. Threat hunting requires a Foresite-managed data lake such as Google SecOps.

CAPABILITY	STANDALONE	WITH CITADEL
Dark web, brand, credential & attack-surface monitoring	•	•
GTI findings delivered to your team	Forwarded to your systems	Via Catalyst cases
CFC investigation & triage of alerts	-	•
Intelligence context added to incident response	-	•
Threat hunting	-	With Google SecOps
Third-party & SOAR integration	-	•
Client review cadence	Monthly	Aligned to your MDR

Who Command is for

Teams that need eyes beyond the perimeter

- You have little visibility into dark web or external threat activity targeting your organization.
- Leaked credentials and brand impersonation are real risks that currently go unmonitored.
- Shadow or unknown internet-facing assets are expanding your attack surface.
- You need GTI-grade intelligence without standing up an in-house threat-intel team.
- You want external intelligence that plugs directly into your MDR and incident response.

Why Foresite

Built on Google, operated by experts.

- Google Cloud Partner of the Year 2026 with Advanced Security & MSSP specializations.
- SOC 2 Type II and ISO/IEC 27001:2022 certified.
- Expertise across Google SecOps, Wiz, and the GTI / Mandiant ecosystem.
- Human-led service with platform-driven automation — analysts govern every response.

Ready to act on what matters?

Schedule a discovery call to see Command in your environment.

SETUP A DISCOVERY CALL →

Foresite Catalyst

DEMO CITADEL IN ACTION →

Google Cloud SecOps Delivery Partner

FORESITE GOOGLE CLOUD SOLUTIONS →