BRIEF

/ Remediation & Resilience for Wayfinder Frontier AI Services

LevelBlue | SentinelOne

Wayfinder Frontier AI Services found it. We fix it.

Expert-led remediation of the exploitable findings Wayfinder Frontier AI Services surfaces.

LevelBlue turns a validated report into a prioritized program your engineers can execute, then verifies the fixes ongoing hold.

Wayfinder Frontier AI Services uncovers several confirmed-exploitable findings in a single run. Now what? As SentinelOne's Premier Remediation Partner, LevelBlue closes that gap.

What we do

Prioritize by Real Exploitability. We calibrate severities against your environment and the controls you already run, informed by LevelBlue SpiderLabs threat intelligence on what attackers are exploiting now.

Guide Your Developers to the Fix. Every finding becomes a clear task: what it is, why it matters, and how to remediate it, delivered as a guided walkthrough with your engineers rather than a document handed over the wall.

Verify it Holds. We retest in pre-production to catch regressions and bypasses, then validate in production, so a closed finding stays closed.

How it works

Step 1: Remediation Sprint.
Tactical advisory and remediation assistance tied to a single set of Wayfinder findings. Milestone-based and sequenced by severity, because remediation timelines vary.

Step 2: Application Resilience Program.
Strategic resilience consulting and posture trend reporting that improves the practices which produced the findings in the first place.

Getting Started. SentinelOne delivers the findings, the client engages LevelBlue, and a scoping call follows within 36 hours.

What this is not

Our engineers prioritize, guide, and verify remediation. Writing the code changes is your development team's work and is not part of the standard offer. Hands-on remediation can be scoped case by case for smaller, less complex environments.

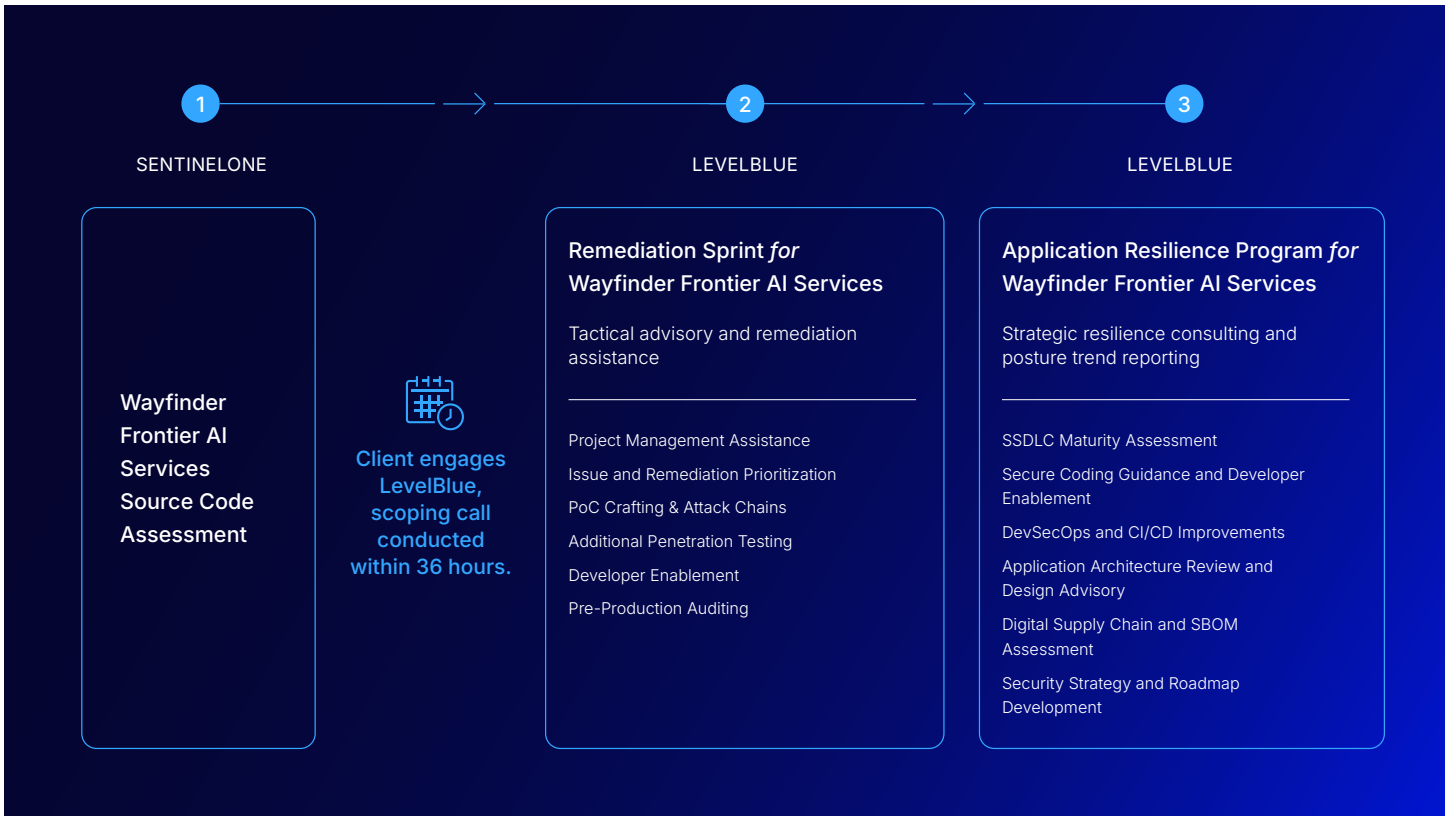
Backed by SpiderLabs threat intelligence

Our experts don't work in a vacuum. Every engagement is informed by LevelBlue SpiderLabs, our threat intelligence unit tracking active adversaries and their tactics, techniques, and procedures. That means we prioritize the findings attackers are most likely to exploit right now, not just the ones with the highest severity score.

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 1084 07-2026

© 2026 SentinelOne, Inc. All rights reserved. SentinelOne and the SentinelOne logo are trademarks or registered trademarks of SentinelOne, Inc.

From assessment to resilience



Benefits

- Prioritize findings by real-world risk and exploitability, not severity scores alone
- Equip developers with actionable, finding-level remediation guidance
- Validate fixes before and after deployment to confirm they hold
- Reduce mean time to remediation and enable faster, safer releases
- Strengthen software supply chain resilience
- Improve application security maturity, with posture trends over time

Who does the work

Engagements are delivered by senior security engineers, DevSecOps specialists, and security architects, with a LevelBlue senior expert acting as engagement project manager from scoping through closure.

- More than 1,000 cybersecurity experts worldwide
- 200,000+ hours of penetration testing conducted annually
- Prioritization informed by LevelBlue SpiderLabs threat intelligence
- Delivered worldwide, in your region

LevelBlue | SentinelOne

Contact us levelblue.com/sentinelonewfai

© 2026 LevelBlue Intellectual Property. LevelBlue logo, and registered trademarks are service marks of LevelBlue Intellectual Property and/or LevelBlue affiliated companies. All other marks are the property of their respective owners. | 1084 07-2026

© 2026 SentinelOne, Inc. All rights reserved. SentinelOne and the SentinelOne logo are trademarks or registered trademarks of SentinelOne, Inc.