FRONTIER DEFENSE™

Autonomous Novel Vulnerability Elimination for CVEF

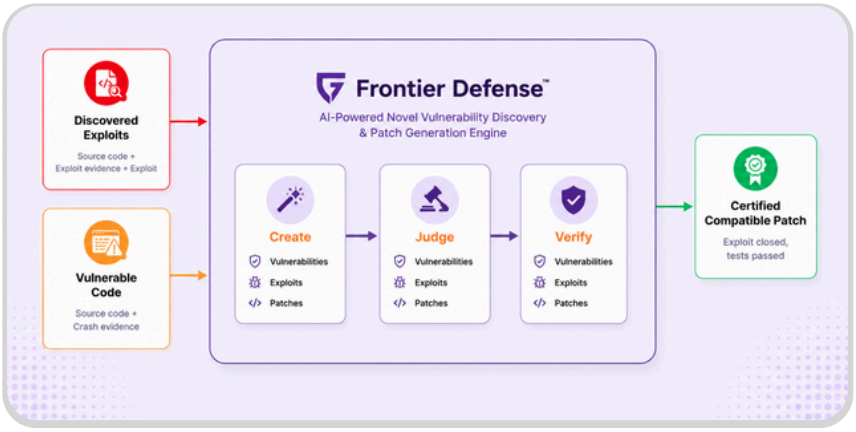
LINEAJE

Vulnerable code in. Verified patches out.

Lineaje Frontier Defense™ is an AI-native security intelligence engine that continuously discovers novel vulnerabilities, validates exploitability, generates verified exploits, creates compatible patches, and verifies successful remediation at scale.

Frontier Defense adds an autonomous, multi-agent AI harness that orchestrates the discovery, validation, verification, and remediation of novel vulnerabilities in first-party code. It leverages multiple frontier AI models—including Mythos, Fable, Opus, and others—to continuously assess code in any Git repository. Frontier Defense reduces security and developer workload while providing a modern platform to discover, validate, remediate, and manage novel vulnerabilities, exploits, and patches at scale.

The Frontier Defense™ Intelligence Engine



The Frontier Defense™ Intelligence Engine

Autonomous AI Harness

Connects with code and LLM of choice to orchestrate isolated, sandboxed AI agents to discover novel vulnerabilities, generate exploits, validate findings, create verified patches, and confirm remediation.

Model Selector

Enables organizations to mix multiple commercial and open-source frontier models for different code repos to manage costs while maintaining governance and developer and security flexibility.

Novel Vulnerability Discovery

Discovers novel vulnerabilities, determines severity, validates exploitability and runtime reachability, and confirms novel vulnerability findings.

Verified Exploit Generation

Generates and safely detonates exploits inside isolated sandboxes to independently validate exploitability before remediation.

Verified Patch Generation

Produces deployment-ready patches that are validated by replaying the original exploit until remediation is confirmed. And applications are rebuilt to confirm compatability.

Evidence-Backed Pull Requests

Automatically delivers review-ready pull requests containing exploit evidence, verified patches, and complete remediation validation for developers to approve eliminating developer toil.

Mission Control

Maintains immutable lifecycle tracking for novel vulnerabilities, verified exploits, generated patches, and remediation progress. Eliminates rework, provides verifiable evidence management.

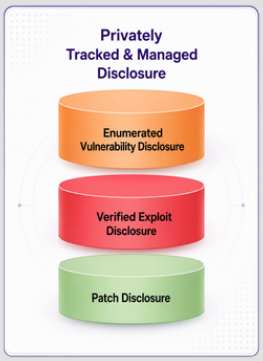
Flexible Deployment

Deploy across SaaS, customer cloud, hybrid, and on-premises environments while meeting data residency and sovereignty requirements.

Disclosure Management

Maintains immutable evidence for novel vulnerabilities, verified exploits, and deployment-ready patches while supporting secure disclosure, VEX, CSAF, and compliance workflows.

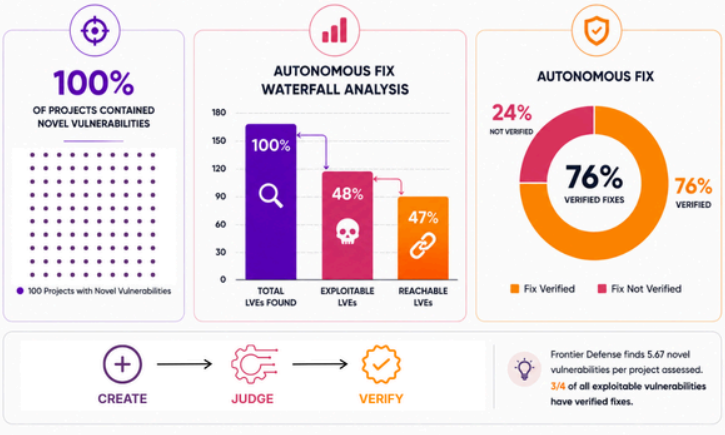
Novel Vulnerability Infrastructure



Frontier Model Support

Amazon Bedrock	Amazon Bedrock
ANTHROP\C	Claude Fable, Claude Mythos, Claude Opus
Google AI	Gemini, Gemma
Meta	Llama
Microsoft	MDASH
OpenAI	GPT-5.5, GPT-5.6
OpenRouter	OpenRouter

LINEAJE FRONTIER DEFENSE FIND & FIX CONTINUUM



FRONTIER DEFENSE™ IN ACTION

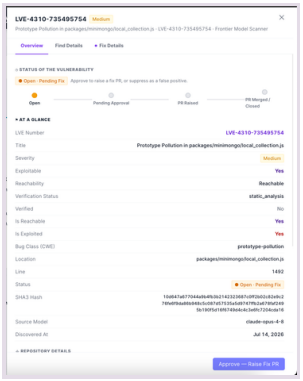
FROM NOVEL FINDING TO VERIFIED PATCH

LINEAJE

Discover and Validate Novel Vulnerabilities

Detect What Traditional Scanners Miss

Frontier Defense discovers novel vulnerabilities in first-party code, assesses exploitability and runtime reachability, and distinguishes confirmed risk from false positives.



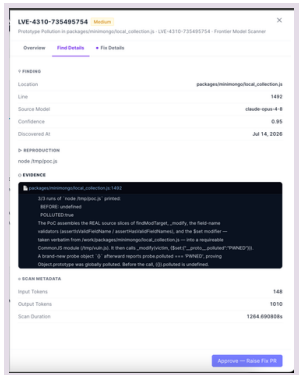
- AI-discovered vulnerabilities (LVEs)
- Full Context Assessment
- Runtime verification
- Source-model attribution
- Evidence-backed prioritization

The source material specifically supports runtime validation, reachability assessment, and triage beyond theoretical findings.

Generate and Verify Exploits

Prove the Vulnerability Is Real

Frontier Defense generates an exploit for each confirmed novel vulnerability and validates it inside a network-isolated sandbox. Judge and verification agents assess impact, repeatability, and exploitability before remediation begins.



- Reproducible exploit evidence
- Isolated sandbox execution
- Repeatability confirmation
- Runtime crash validation
- Complete evidence trail

The Frontier document describes exploit generation inside gVisor-based, single-use containers with independent validation of impact and repeatability.

Generate Verified, Deployment-Ready Fixes

Patch, Verify, and Deliver

Frontier Defense generates deployment-ready patches and reruns the original exploit against the patched code until exploit closure is confirmed. Approved fixes are delivered through evidence-backed pull requests.

- AI-generated fixes
- Original exploit replay
- Verified exploit closure
- Review-ready code changes
- Human-approved pull requests

The source explicitly states that patches are validated by rerunning the original exploit until it can no longer be reproduced, then delivered with evidence in review-ready pull requests.

Autonomous AI Harness

Iterates from discovery to verified remediation.

- ✔ Nine isolated AI sandboxes
- ✔ Up to five iterations per finding
- ✔ Judge and verification agents
- ✔ Human approval at final PR stage
- ✔ Repeatable, evidence-backed workflows

Mission Control and Disclosure

Preserve the complete vulnerability lifecycle.

- ✔ Novel vulnerability tracking
- ✔ Exploit and patch evidence
- ✔ PR and remediation status
- ✔ VEX and CSAF support
- ✔ Audit-ready disclosure records

LINEAJE

AI-NATIVE MULTI-AGENT SECURITY INTELLIGENCE ENGINE

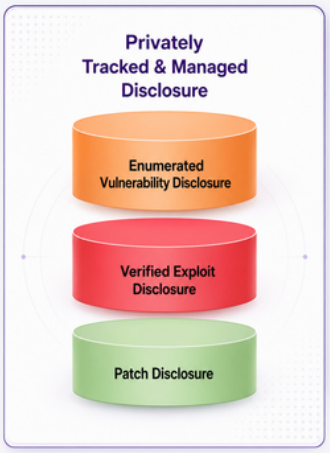
Nine autonomous AI agents work together to continuously Find & Fix novel vulnerabilities through discovery, exploit validation, patch generation, and verified remediation.

Frontier Model Defense

One autonomous engine For AI Generated Novel Vulnerabilities & Patches

	Create Generate	Judge Assess	Verify Prove
Code	01 Vulnerability Discovery Finds code weaknesses and hotspots	02 Finding Triage Scores severity, drops false positives	03 Vulnerability Confirmation Confirms the flaw is real at runtime
Exploit	04 Exploit Generation Builds a working proof-of-concept	05 Impact Assessment Rates exploitability and impact	06 Exploit Reproduction Proves it reproduces reliably
Gold FM Patch	07 Patch Generation Writes a minimal source-code fix	08 Patch Risk Review Grades fix quality and regressions	09 Verified Remediation Certifies the exploit stays closed

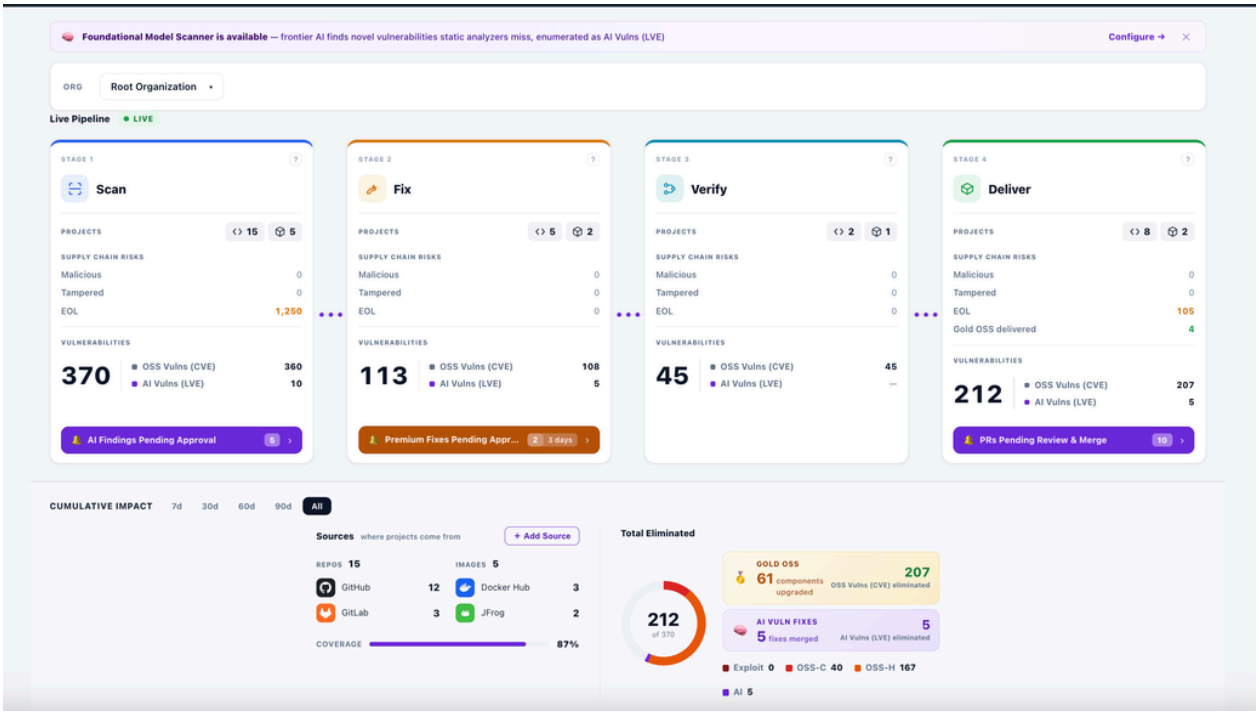
Novel Vulnerability Infrastructure



Supported Frontier Models & Platforms

Amazon Bedrock	ANTHROP\C	Google AI	Meta	Microsoft	OpenAI	OpenRouter
Amazon Bedrock	Claude Fable, Claude Mythos, Claude Opus	Gemini, Gemma	Llama	MDASH	GPT-5.5, GPT-5.6	OpenRouter

Works WIth CVE Factory



BEYOND CVEs. BEYOND SIGNATURES. BEYOND TRADITIONAL SCANNERS.

Discover novel vulnerabilities. Generate verified exploits. Deliver deployment-ready patches.

Schedule a Demo. Lineaje.com

Talk to the Product Team. devs@lineaje.com

Subscribe to AI Threat Alerts →

DETAILED CAPABILITIES

Detailed capabilities powering AI-native novel vulnerability discovery, verified exploit generation, and deployment-ready patch validation.

FRONTIER DEFENSE™ INTELLIGENCE ENGINE CAPABILITIES

MODULE	FEATURE	DESCRIPTION	USE CASE	USER OUTCOME
FM Scan & Fix	Model Selector	Customers choose from a maintained list of commercial and open-source frontier models and supported platforms, select the model and project, and Frontier Defense orchestrates the downstream scan-to-fix workflow.	Scan using approved AI infrastructure, model governance, and project-level security priorities.	Teams can use approved frontier models and platforms without locking into a single vendor or changing governance standards.
FM Scan & Fix	Agentic Novel Vulnerability Detection, Judgment & Verification	Discovers zero-day novel vulnerabilities in first-party source code and triages them for false positives, exploitability, severity, and reachability in the customer environment. Runtime verification confirms that the flaw is real.	Assess heap overflows, out-of-bounds read/write, integer overflow/underflow, divide-by-zero, and denial-of-service classes that static tools cannot enumerate.	Security teams receive validated, reachable, exploitable findings with reproducible evidence instead of unverified alerts.
FM Scan & Fix	Agentic Exploit Generation, Judgment & Verification	Generates an exploit for each confirmed novel vulnerability and detonates it inside a gVisor-based, network-isolated, single-use container with no egress. instrumented crash validation confirms exploit execution.	Independently assess exploitability, impact, and repeatability before remediation work begins.	Teams can prioritize confirmed, executable exploits rather than theoretical vulnerability reports.
FM Scan & Fix	Agentic Patch Generation, Judgment & Verification	Generates verified, deployment-ready fixes for confirmed exploits. A patch-verification ladder reruns the original exploit against patched code in a separate sandbox until the exploit can no longer be reproduced.	Confirm exploit closure, remove duplicates across iterations, and narrow focus on novel vulnerability classes not yet enumerated.	Engineering teams receive verified fixes that have already defeated the original exploit in isolation.
FM Scan & Fix	Autonomous Agentic Vulnerability Harness	Runs a fully autonomous multi-step harness covering source ingestion, isolated sandbox deployment, exploit generation, exploit confirmation, patch creation, and patch verification without human intervention at each stage.	Iterate up to five times per finding until no exploit can be confirmed; reserve human review for final PR approval only.	Each finding moves from discovery to verified remediation through isolated, repeatable agent workflows.
Reporting	Evidence-Backed Pull Requests	Integrated into the CVEF, every confirmed and patched novel vulnerability produces a review-ready pull request containing vulnerability details, exploit evidence, patch diff, verification confirmation, and audit trail.	Provide security reviewers, developers, and auditors with a complete evidence chain for each fix.	Developers receive actionable PRs with evidence rather than manual remediation instructions.
Reporting	Vulnerability, Exploit & Patch Disclosure Management	Maintains immutable evidence repositories for novel vulnerabilities, exploits, and patches in a private local instance. Supports disclosure, sharing, and mitigation workflows through Lineaje SBOM Manager.	Manage customer and internal stakeholder disclosures with VEX and CSAF support out of the box.	Organizations can preserve a defensible record of vulnerability discovery, exploitation, mitigation, and disclosure.
Deployment	Flexible Deployment	Deploys across Lineaje SaaS, customer cloud environments, on-premises environments, or hybrid mode. Hybrid deployments keep code and scan execution entirely inside the customer environment.	Meet infrastructure, security control, and data residency requirements while sending only findings metadata to the SaaS control plane.	Regulated organizations can run Frontier Defense where their code, controls, and sovereignty requirements already live.
Reporting	Mission Control & Lifecycle Tracking	Centralized lifecycle tracking covers novel vulnerabilities, verified exploits, generated patches, and statuses across multiple frontier-model runs.	Track exploitable findings, critical non-exploitable findings, false positives, PR status, and remediation progress in one place.	Security and engineering teams reduce confusion, improve handoffs, and move faster from discovery to verified remediation.