Phoenix Launched open access Agentic Intel Platform, Zero-Day Detection, MCP for threat intel, Malware, Package Firewall

Phoenix Blue unifies all vuln intelligence with AI/LLM for 0-day detection, risk scoring, and malicious package ID across major open source libraries.

Phoenix Blue, Phoenix Security, Vulnerability Intelligence, Agentic AI, Zero-Day Detection, Real-Time Risk Scoring, Malware, Malicious Packages, CVE, CISA KEV, Supply Chain, VulnCon 2026

PHOENIX, AZ, UNITED STATES, June 30, 2026 /EINPresswire.com/ -- With the increase in Vulnerability and the disconnect of NVD Phoenix Security opens the database of intelligence

We Launch Blue Intelligence 2.0 platform provides security teams, developers, researchers, and AI-enabled security workflows with access to continuously enriched vulnerability intelligence across CVEs, products, vendors, open source libraries, package ecosystems, and malicious packages.

Phoenix Blue is designed to help organizations reduce fragmentation across vulnerability intelligence sources. Security teams frequently rely on separate feeds for CVE records, known exploitation, exploit probability, proof-of-concept evidence, vendor advisories, open source package data, and malicious package research. Phoenix Blue brings these signals together into a single intelligence layer accessible via the web interface, REST APIs, and Model Context Protocol integrations.

“Security teams and developers are now operating in an environment where attackers move faster, automation is increasing, and software supply chain risk is harder to track manually,” said Francesco Cipollone, CEO and Co-Founder of Phoenix Security. “Phoenix Blue was relaunched to make vulnerability intelligence easier to access, easier to validate, and easier to use inside

human and AI-assisted workflows. The objective is simple: give defenders better context before they prioritize, assign, or remediate."

Phoenix Blue, Phoenix Security, Vulnerability Intelligence, Agentic AI, Zero-Day Detection, Real-Time Risk Scoring, Malware, Malicious Packages, CVE, CISA KEV, Supply Chain, VulnCon 2026

Phoenix Blue is available now with a free public tier. Users can register through Phoenix Security at:

A Single Intelligence Layer for Vulnerability and Supply Chain Risk

Phoenix Blue currently indexes more than 380,000 vulnerability and malware intelligence records and more than 2,080,000 advisory references from authoritative and specialist sources.

The platform combines data from sources including NVD, CISA Known Exploited Vulnerabilities, EPSS, VulnCheck, Shadowserver, GreyNoise, zero-day intelligence sources, ransomware intelligence, malicious package repositories, vendor advisories, and Phoenix Security's own research.

> "In the era of agents, we created Phoenix Blue to empower all defenders to fight AI with AI, providing the high-quality data and realistic formulas needed for effective decision-making"
>
> *Francesco Cipollone*

Each record is enriched with structured intelligence, including CVSS v3.1 and CVSS v4.0 data, CWE mapping, CPE associations, EPSS probability, KEV status, exploit evidence, affected product and vendor context, malware and package signals, remediation information, and advisory references.

Phoenix Blue also includes Phoenix Security's proprietary scoring models, designed to help users compare vulnerability urgency across multiple dimensions rather than relying on a single severity score.

Built for Security Teams, Developers, and AI Agents

Phoenix Blue has been designed as an intelligence platform for both human analysts and AI-enabled security workflows.

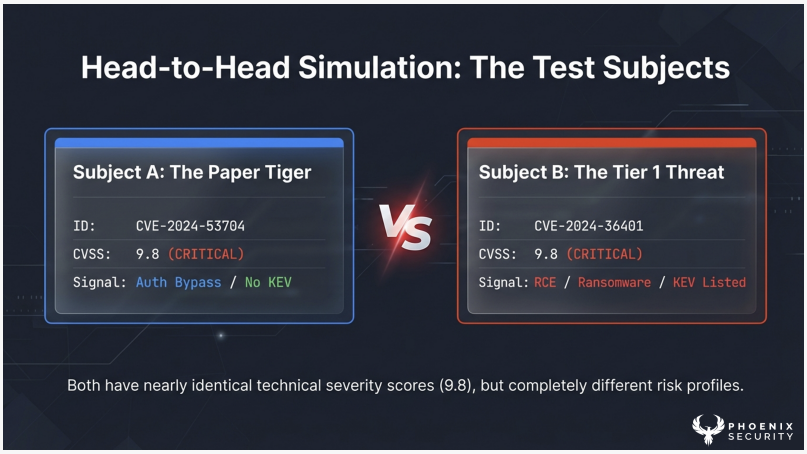
The platform exposes vulnerability intelligence through:

- A public web interface at https://phxintel.security
- REST API access
- MCP server integrations
- Structured vulnerability, product, vendor, and package intelligence modules
- Tier-based access controls for Free, Registered, Pro, and Enterprise users

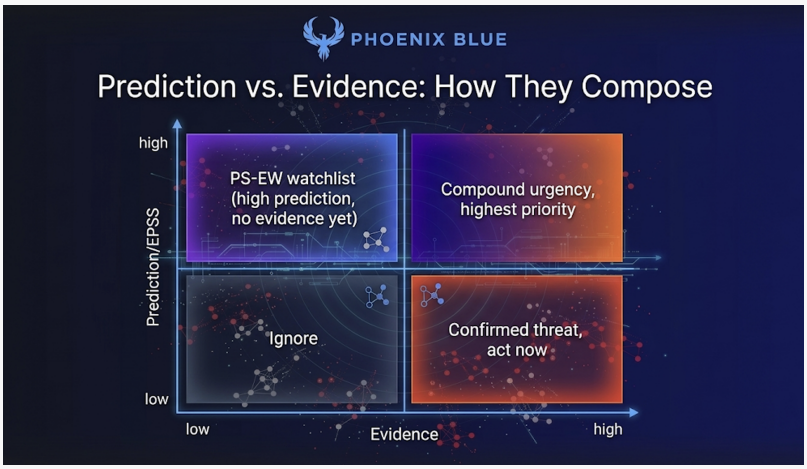
The MCP integration allows AI assistants and security agents to query Phoenix Blue intelligence directly inside security research, developer, and remediation workflows.

This enables AI-assisted workflows to retrieve structured information about vulnerabilities, exploitability, affected technologies, likely root cause, remediation guidance, affected package ecosystems, and related threat context.

Phoenix Security designed this architecture to support agentic security workflows without removing human control. AI-generated intelligence is structured, validated, scored, and reviewable.



Phoenix Security Paper Tiger - Phoenix Blue, Phoenix Security, Vulnerability Intelligence, Agentic AI, Zero-Day Detection, Real-Time Risk Scoring, Malware, Malicious Packages, CVE, CISA KEV, Supply Chain, VulnCon 2026



Phoenix Security Blue Prediction vs evidence- Phoenix Blue, Phoenix Security, Vulnerability Intelligence, Agentic AI, Zero-Day Detection, Real-Time Risk Scoring, Malware, Malicious Packages, CVE, CISA KEV, Supply Chain, VulnCon 2026

AI-Enriched Advisory Intelligence With Validation Controls

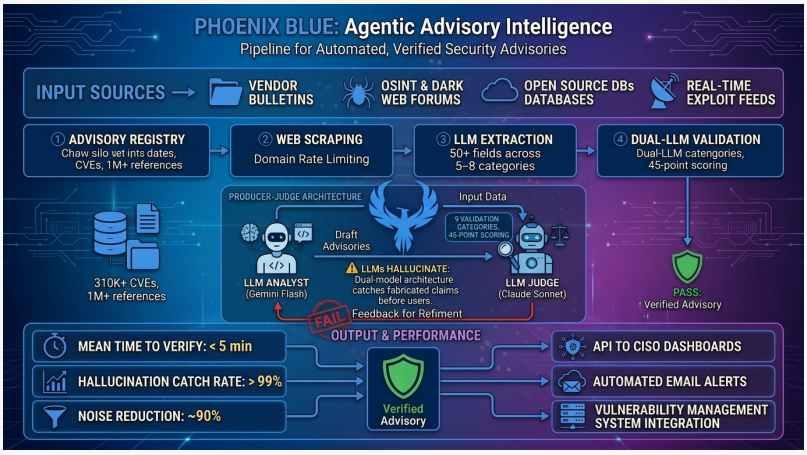
Phoenix Blue includes an AI-assisted advisory intelligence pipeline that extracts and structures vulnerability context from advisory data and related sources.

The pipeline is designed to enrich records across key categories, including:

- Root cause
- Affected scope
- Exploitation status
- Technical impact

- Remediation guidance
- Detection indicators
- Timeline information
- Threat actor or campaign attribution, where available

To reduce the risk of inaccurate AI-generated output, Phoenix Blue uses a producer-and-judge validation model. AI-generated analysis is reviewed by a separate reasoning-capable model and scored across quality categories such as evidence discipline, technical accuracy, logic flow, CWE and CVSS mapping quality, detection engineering usefulness, remediation practicality, and vendor patch accuracy.



Phoenix Blue unifies all vuln intelligence with agentic AI/LLM for 0-day detection, risk scoring, and malicious package ID across major open source libraries.

Outputs that do not meet Phoenix Security's quality threshold are rejected before reaching users. Users can also rate AI-generated content, creating a feedback loop for quality monitoring and future improvement.

Zero-Day Monitoring Preview

As part of the relaunch, Phoenix Security is previewing zero-day monitoring capabilities within Phoenix Blue.

The zero-day monitoring workflow is designed to watch source code repositories for security-relevant commits that may indicate a vulnerability fix before a CVE has been assigned.

Users can register repositories such as the Linux kernel, Apache httpd, OpenSSL, or other high-risk projects for monitoring. Phoenix Blue analyzes commit history, extracts diffs, and classifies whether a change appears to be security-relevant, what vulnerability type it may address, and whether there is evidence of exploitability.

The preview supports:

- Live pull request and commit monitoring
- Historical repository analysis
- Full repository traversal
- Verification workflows for analyst review
- True-positive and false-positive feedback
- Budget controls for LLM usage

- User-selected LLM provider options

Each finding includes supporting evidence and version context to help analysts determine whether further investigation is required.

Intelligence Across CVEs, Products, Vendors, Libraries, and Package Ecosystems

Phoenix Blue provides dedicated intelligence views for different dimensions of vulnerability exposure.

Vulnerability and Malware Intelligence

Phoenix Blue enriches CVE and malware-related records with severity, exploitability, CWE mapping, CPE association, known exploitation, advisory references, root cause classification, impact classification, executive summaries, and proprietary Phoenix Security scoring.

Product Health Scorecards

The Product Health Score evaluates products using indicators such as CVE severity distribution, known exploited vulnerabilities, exploit availability, EPSS exposure, ransomware association, patch coverage, and end-of-life status.

This helps security teams understand whether a product's vulnerability profile is improving or degrading over time.

Vendor Risk Scorecards

The Vendor Risk Scorecard rolls product-level data into vendor-level intelligence. This includes exploitation exposure, threat type distribution, zero-day activity, and time-to-exploit patterns.

The scorecard is designed to support vendor risk review, product selection, and exposure management workflows.

Open Source and Package Intelligence

Phoenix Blue provides open source package intelligence across major ecosystems, including Maven, npm, PyPI, NuGet, Cargo, RubyGems, Go, and Linux-related package data.

The platform assesses packages using indicators such as exploitation evidence, EPSS likelihood, CVSS severity, dependent package blast radius, researcher attention, bug bounty activity, license risk, popularity, compromise history, and repeat-offender patterns.

Malicious Package Detection Across Software Supply Chains

Phoenix Blue includes malicious package detection capabilities designed to identify suspicious and confirmed malicious activity across open source ecosystems.

For npm packages, the platform uses static analysis detectors to identify patterns such as:

- Obfuscated code
- Base64 payloads
- Eval-based execution
- Hex-encoded strings
- Suspicious post-install hooks
- Network exfiltration behavior
- DNS lookups to unknown domains
- WebSocket connections
- Attempts to read environment files, SSH keys, or browser credential stores
- Dependency confusion indicators
- Typosquatting patterns

Packages that trigger static analysis alerts can be escalated for AI-assisted behavioral analysis to classify likely intent.

Phoenix Blue also integrates intelligence from malicious package repositories, including OSV-format advisories, to identify confirmed malicious packages across major ecosystems. Confirmed detections are linked to affected versions, indicators of compromise, timelines, and package-level intelligence.

The platform is also being extended to support broader ecosystem coverage, including package managers, VSX extensions, skills, plugins, and other emerging software distribution mechanisms increasingly targeted by supply chain attackers.

New Scoring System

Phoenix Blue includes six proprietary scoring systems designed to compare vulnerability and ecosystem risk across different use cases:

- PS-HP — High-Profile Score: identifies high-priority CVEs based on exploitation evidence, likelihood, severity, blast radius, popularity, bug bounty activity, and end-of-life status.
- PS-EW — Enterprise Watchlist: flags enterprise-relevant CVEs that may not yet have exploitation evidence but show elevated future risk.
- PS-OSS — Open Source Score: evaluates package and library risk across major open source ecosystems.
- PS-PHS — Product Health Score: grades products based on vulnerability and exploitation indicators.

- PS-PVS — Vendor Score: provides vendor-level exposure and risk signals.
- PS-ADQE — Advisory Quality Score: rates advisory source quality and reliability to support automated source prioritization.

Phoenix Blue also uses trained machine learning models for vulnerability classification, including root cause classification, impact classification, CWE prediction, and threat intelligence extraction.

Time-to-Exploit Analytics

Phoenix Blue calculates time-to-exploit data for vulnerabilities with confirmed exploitation evidence.

The platform measures the gap between CVE publication and first known exploitation signal, then classifies exploitation speed into categories such as zero-day, same-day, within-week, and within-month exploitation.

These analytics help security teams understand which vulnerabilities, products, vendors, and ecosystems are being weaponized quickly.

Phoenix Blue uses these signals inside its scoring models to increase urgency where exploitation pressure is high.

Phoenix Blue by the Numbers

- 380,000+ vulnerability and malware intelligence records indexed
- 2,080,000+ advisory references tracked
- 15+ authoritative and specialist intelligence sources
- 6 proprietary Phoenix Security scoring systems
- 5 trained AI and neural network classification models
- 200+ API endpoints across REST, GraphQL, and MCP-related access paths
- Coverage across major package ecosystems, including Maven, npm, PyPI, NuGet, Cargo, RubyGems, Go, and Linux package data
- Expanded supply chain coverage for malicious packages, extensions, skills, and software distribution ecosystems

Phil Moroni
Phoenix Security
+1 919-594-8888
email us here

try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.