CLAIRVOYANT

Uncovering Hidden Threats in Third-Party Software Applications and Updates

2026

"Like having a thousand reverse engineers vetting every inbound binary 24/7."

- Infosec CISO

The Software Approval Bottleneck

The modern enterprise faces a fundamental challenge in its software approval process. The traditional model, dependent on manual checks and siloed teams, has become a significant bottleneck that hinders agility and creates critical Third-Party Risk Management (TPRM) gaps.

The Efficacy Gap

Enterprises, afforded little visibility into binary code, have few defenses against hidden threats embedded within third-party applications and updates. Security teams often have no recourse but to deploy software, relying on reactive measures like Endpoint Detection and Response (EDR) and patching. The damage is often done before these measures are even implemented.

The Flaw in Trust-Based Controls

CISOs are increasingly turning to proactive measures to detect hidden threats, including pre-procurement vendor questionnaires, code attestation validation, and Software Bill of Materials (SBOM). Unfortunately, the efficacy of such techniques depends heavily on the trust placed in software vendors – many of whom do not know, or fully account for, the contents of the software they publish.

Introducing the Clairvoyant Software Integrity Platform™ (SIP)

SIP is a preventative control for third-party software supply chain security. It automatically and continuously detects latent threats embedded in applications and updates before they are deployed. This is a radical departure from traditional methods and is specifically designed to address previously unknown instances of supply chain infiltration.

The AI-Driven Advantage

Clairvoyant's Agentic Reverse Engineering™ (ARE) technology leverages an AI/ML engine to uncover known threats and highlight hidden GRC and operational concerns.

A Foundational Paradigm Shift in Moving Beyond Legacy Security

By basing its analysis on what the code does rather than the trustworthiness of the vendor, SIP provides a zero-trust approach to software risk assessment.

SIP is specifically designed to proactively detect previously unknown instances of supply chain infiltration, which stands in contrast with legacy tools that focus on license compliance and known vulnerabilities (CVEs). Departing from signature-based antivirus or sandboxing, SIP leverages a static behavioral approach to detection, ensuring latent threats are discovered regardless of how they are crafted.

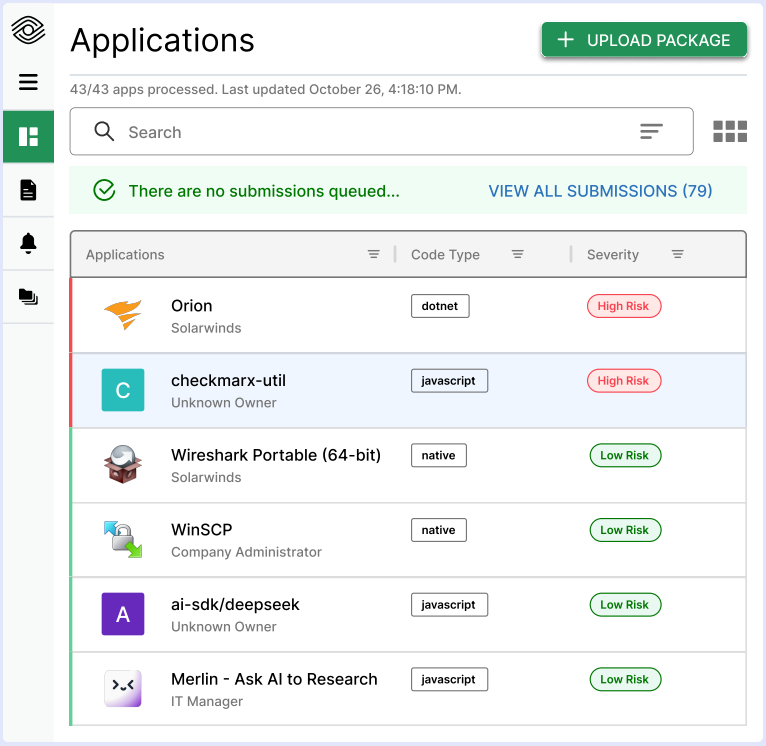

Figure 1:
SIP automatically and continuously analyzes new software and updates, providing deep visibility into latent threats missed by other tools.

Automated Risk Analysis

The platform is easy to operationalize, automatically analyzing every new application or software update for hidden risk.

- It integrates seamlessly with popular enterprise distribution mechanisms, such as Microsoft SCCM, to automatically pull new packages for analysis.
- The system then reports its findings via the Clairvoyant dashboard and other channels, making it simple to verify every update before deployment.

Agentic Reverse Engineering (ARE)

The core of the product is Clairvoyant's Agentic Reverse Engineering™ (ARE) technology. This unified architecture addresses the computational challenges of enterprise-scale software supply chain security. ARE empowers an autonomous AI agent to mirror an expert human reverse engineer—continuously vetting software and intelligently orchestrating traditional analysis tools to provide explainable behavioral assessments and actionable risk insights. This agentic approach represents a significant departure from legacy systems that followed predetermined analysis sequences.

The LLM agent's adaptive problem-solving behaviors enable it to determine the optimal sequence and combination of reverse engineering tools to apply, mirroring how expert human reverse engineers approach unknown software packages.

The Company

Founded by cybersecurity startup veterans from FireEye and Menlo Security, Clairvoyant Intelligence is a cybersecurity leader making a big impact in the area of software supply chain security for the enterprise.