Incidents are inevitable. Panic is optional.

**At-a-Glance**
Founded: 2022  
HQ: Greater New York  
Funding: $8M Seed  
Investors: J2 Ventures, Glasswing Ventures, Unusual Ventures  
[www.kusari.dev](http://www.kusari.dev)

**Securing your software supply chain** starts with understanding your dependencies. Understanding dependencies means you know the attributes and relationships through the supply chain. Then, you can determine which are most critical, and thus highest priority, to protect. Close the gap between identifying vulnerabilities and taking action against them with Kusari. We help you know all your components, how they interact, and the blast radius, making your life significantly easier.

Having experienced this problem for years, Kusari resolved to bring transparency and security to the software supply chain.

Backed by J2 Ventures, Glasswing Ventures, and Unusual Ventures, Kusari seeks to help organizations identify, prioritize and quickly remediate supply chain vulnerabilities while powering secure development practices.

**Our Founders**

**Tim Miller, CEO and Co-founder**  
- Technical leader with 20+ years in financial industry (Citi, MUFG, Bridgewater) engineering the development and security for mission-critical trading systems.

**Parth Patel, CPO and Co-founder**  
- Engineer with over 15 years of experience in cybersecurity (DevOps).  
- Has led projects across the supply chain, including with USG contractors in situations of significant security.

**Michael Lieberman, CTO and Co-founder**  
- Extensive expertise in cloud-native technologies and security use cases.  
- Co-chair, CNCF Financial Services User Group; ex Citi, MUFG, Bridgewater.
Gone are the days of feeling secure by signing containers and running vulnerability scans. Now, you must protect every line of code and process involved in developing, distributing and deploying your organization’s software. There’s no silver bullet when any weak point or vulnerability in the chain can become compromised. Yet, there are solutions that deliver value and make securing software infinitely less painful.

**The Kusari Platform** delivers transparency and intelligence to secure your software development lifecycle end-to-end.

**With our platform, you can:**

- Connect the dots between the knowns, the unknowns and deciding what next action to take.

- Be proactive in tackling both the everyday challenges of managing dependencies AND the next critical incident.

- Close the gap between identifying dependencies and vulnerabilities and taking remediation actions.

---

**GUAC**

Kusari builds on Graph for Understanding Artifact Composition (GUAC), a tool that it built with Google and other partners.

GUAC allows you to collect, ingest, collate, and query all the components of your software. With it, you can evaluate software artifacts before they are ingested into a system, automatically preventing risky or vulnerable dependencies from entering your supply chain.

**Active Users:**

Adobe | AWS
Bloomberg | Cisco
ClearAlpha Technologies | Google
GitHub | Intel
Guidewire | Microsoft
Microsoft | Red Hat
VMware | Yahoo!

---

Vigilance across the entire development lifecycle

| Proactive: Understand most used critical components in your software supply chain ecosystem, weak points in overall security posture, and exposure to risky dependencies. | Operational: Guarantee applications to be deployed meet organizational policy; ensure all binaries in production trace back to a securely managed repository. | Responsive: Understand how a new vulnerability affects your organization’s inventory and in the face of a suspicious project lifecycle event, quickly deduce where risk has been introduced. |
Kusari Benefits

Complete transparency to know all your dependencies
Kusari provides insight into the components and health of your entire software supply chain, generates accurate and complete SBOMs, and provides actionable guidance to quickly mitigate risk.

- Kusari ingests data from all of your first and third party tools and software to provide a complete picture of your supply chain, including direct and transitive dependencies, vulnerabilities and misconfigurations.
- Kusari works with all of your existing tools to generate a single source of truth that developers and security teams can trust.

Intelligence to make better decisions, reduce risk
By understanding how dependencies and vulnerabilities impact your entire supply chain, Kusari prioritizes remediation efforts and provides actionable guidance to quickly reduce exposure time.

- Identify in seconds rather than days if your organization is impacted by a day zero.
- Reduce developer toil and MTTR by understanding a vulnerability’s origin, reachability and blast radius.
- Allow developers to fix the highest risk items first and in the fewest places.

Start simple, scale fast
Kusari is cloud-based SaaS and works with all tools in your supply chain, just as they are.

- No need to retool or change any of your internal processes to get started. Simply download and start sending us your software bills of material (SBOMs).
- Quickly connects to your software development environment and updates as your codebase, tools and processes evolve.
- Backed by an active community of security experts, promoting continuous improvement.
## Company Background

<table>
<thead>
<tr>
<th>Before Kusari</th>
<th>With Kusari</th>
</tr>
</thead>
<tbody>
<tr>
<td>● See a limited portion of your supply chain, miss dependencies, and have security unknowns.</td>
<td>● Manage SBOM requirements using full supply chain visibility; know all your dependencies.</td>
</tr>
<tr>
<td>● Unaware if you have an SBOM and whether or not it’s complete.</td>
<td>● No surprises about software tools and their owners.</td>
</tr>
<tr>
<td>● Miss vulnerabilities because you don’t know what is in your software supply chain and how the pieces fit together.</td>
<td>● Proactively protect critical infrastructure using knowledge and context of dependencies, vulnerabilities and misconfigurations.</td>
</tr>
<tr>
<td>● Inefficient remediation efforts and friction between security and development teams.</td>
<td>● Make secure updates part of the software development lifecycle.</td>
</tr>
<tr>
<td></td>
<td>● Pinpoint and prioritize the vulnerabilities that matter, ahead of production.</td>
</tr>
<tr>
<td>● Take days after an incident to discover if the vulnerable component is in use, and if it is reachable.</td>
<td>● Remediate compromised systems in seconds using actionable data, such as the origin and authenticity of all your software components.</td>
</tr>
<tr>
<td>● When a vulnerability is found, it’s unclear which team should fix it and how.</td>
<td>● Give the right developer the right information, share common fixes with multiple developers.</td>
</tr>
<tr>
<td>● Developers waste time trying to understand if they even have the ability to fix the issue and if the vulnerability is actually exploitable.</td>
<td>● Reduce risk exposure and time to remediate; prioritize the items that pose real risk.</td>
</tr>
</tbody>
</table>

## About Us

Kusari empowers enterprises to understand and secure their complex software supply chains, from code to cloud. Our platform delivers complete visibility into all components of the supply chain and context for how they interact so developers can quickly pinpoint and efficiently respond to threats that matter, and security teams gain a single source of truth from which they can generate accurate/complete SBOMs, manage risk and meet compliance requirements.