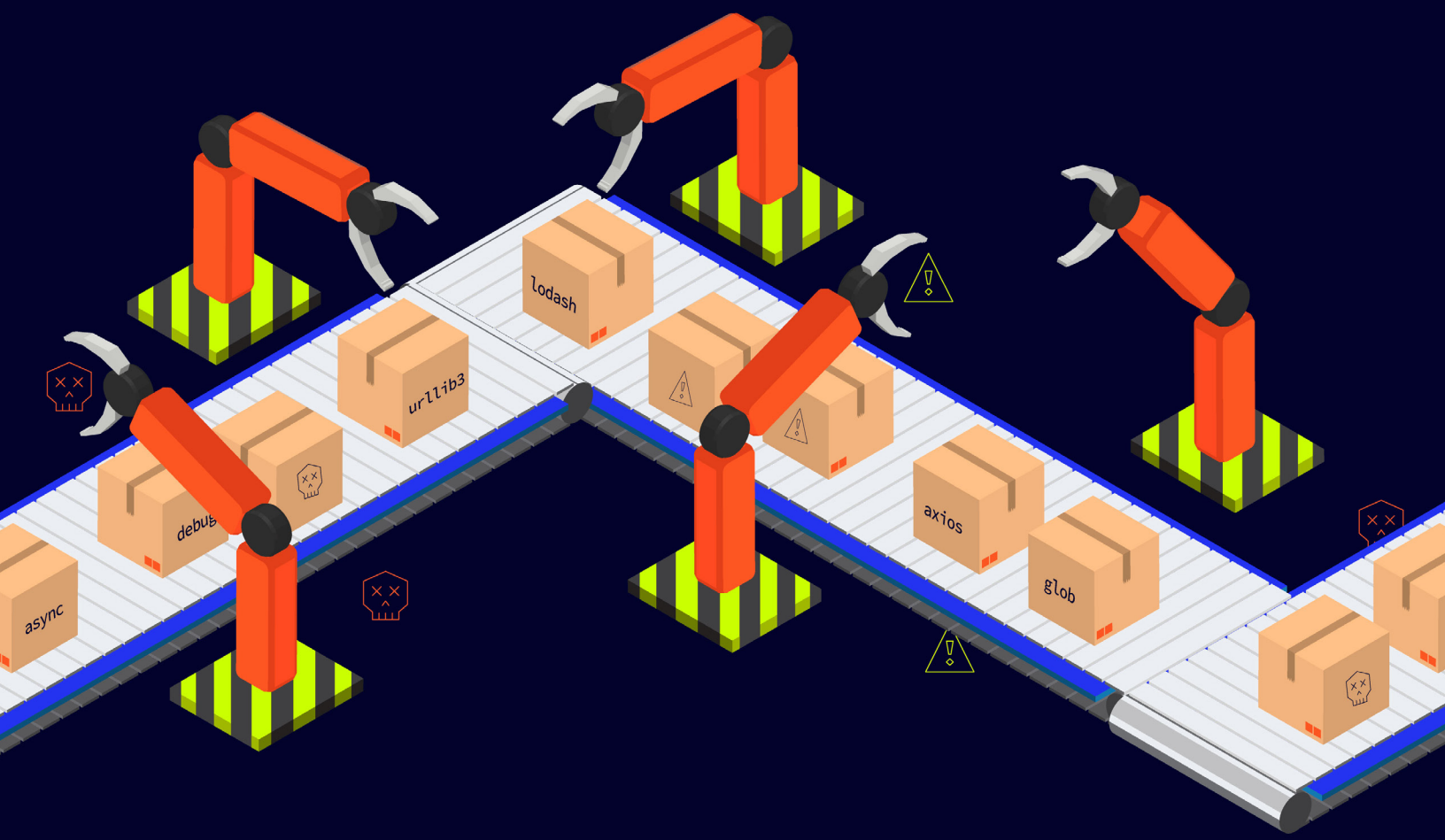
sonatype

The AI-Era Software Assembly Line

How AI Is Changing Software Risk Before Code Ever Reaches Production



Executive Summary

Security isn't written one dependency at a time anymore. It's assembled by developers, AI assistants, package managers, and increasingly autonomous agents at machine-speed.

The attack surface is expanding, vulnerability discovery is accelerating, and AI is giving attackers unprecedented scale and speed.

Security teams have responded by investing in automation, and engineering teams are accelerating remediation all to streamline vulnerability management. In best-of-class organizations, those efforts are working. However, they were built for an era when humans made most software decisions. As AI begins assembling software at machine speed, the scale of new dependencies, updates, and component choices threatens to outgrow even mature vulnerability management programs.

To understand how AI-era software assembly differs, Sonatype Research Labs examined four years of software assembly data to understand how software risk has changed since the beginning of the AI era. Rather than examining a changing customer base, this research follows the same applications over time, allowing us to isolate how the software environment itself has evolved.

Our analysis revealed five concurrent facts:

- **Applications are accumulating more risk** than they did only two years ago.
- **The vulnerability landscape is expanding** faster than historical trends predicted.
- **Organizations are remediating vulnerabilities faster than ever,** driven by automation.
- **Software production is accelerating,** creating more dependency decisions than ever before.
- **Safer dependency choices remain difficult,** even when better alternatives already exist.

Together, these trends point to a fundamental shift:

SOFTWARE RISK INCREASINGLY BEGINS BEFORE SOFTWARE REACHES PRODUCTION.

Whether driven by AI, changing attacker behavior, or the growing complexity of modern software, organizations are operating in a fundamentally different environment than they were only a few years ago. This report examines the evidence behind that shift and what it suggests about the future of software supply chain security.

4.31x

Increase in Critical & High risk vulnerabilities per application

46x

Increase in newly affected component versions

59%

Reduction in median vulnerability age

4.84x

Increase in enterprise application creation

FACT 1

Applications Are Accumulating More Risk

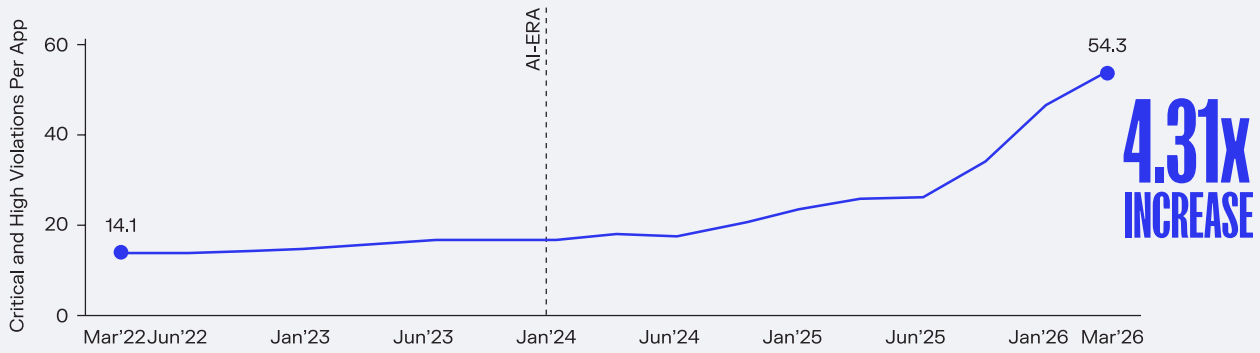
One of the simplest questions we asked was also one of the most important: Has enterprise software actually become riskier?

To answer it, we analyzed a stable cohort of enterprise applications continuously monitored since June 2022. The customer population, application portfolio, security policies, and severity scoring remained consistent throughout the study.

FIGURE 1

Critical and High Vulnerabilities Per Application

Applications now carry 54.3 Critical and High-severity vulnerabilities per application, a remarkable increase over over four years ago, when they carried 14.14 Critical and High-severity vulnerabilities each.



If software risk had remained stable, we would expect the average application to carry roughly the same level of Critical and High risk over time. Instead, Sonatype observed that between June 2022 and June 2026, the average enterprise application accumulated 4.31× more Critical and High risk.

Because the organizations and evaluation criteria remained consistent, this increase is best explained by changes in the software ecosystem, not by organizations suddenly becoming less secure.

> **APPLICATIONS DON'T BECOME RISKIER ONLY BECAUSE DEVELOPERS CHANGE THEM. THEY BECOME RISKIER BECAUSE THE SOFTWARE ECOSYSTEM AROUND THEM CHANGES.**

NOT JUST A LEGACY APPLICATION STORY

This trend persists even after excluding legacy applications newly brought under management.

Risk per application still increased 3.91×, indicating the growth reflects changes in the software ecosystem rather than customer onboarding.

The picture is more nuanced than rising risk alone suggests. As we'll see in the next chapter, organizations are making measurable progress in reducing vulnerabilities and accelerating remediation. But they're racing against an environment that is changing faster than ever, where AI is increasing both the speed and scale of software risk.

FACT 2

Every Dependency Has Become a Moving Target

If applications are accumulating more risk over time, the question seems obvious: **Has the software ecosystem itself become riskier?**

The answer is yes. Our analysis shows risk has always been there, but the tooling to discover and exploit this risk is now easier than ever to use.

We examined the growth of the global vulnerability catalog and compared it against the trajectory established before March 2024. Rather than continuing along its historical path, vulnerability disclosures accelerated beyond what earlier trends predicted. Every month since the beginning of the AI era has exceeded that historical baseline. The rate of new vulnerability advisories entering the research catalog grew 4.17x over 49 months. The impact side is more dramatic — new component-level implications represent 46x the pre-AI rate over the same window.

FIGURE 2A

Quarterly Average of Vulnerability Advisories

The vulnerability landscape is no longer following historical trends. Since March 2024, every month has exceeded the pre-AI baseline, with new vulnerability advisories growing 4.17x over 49 months.

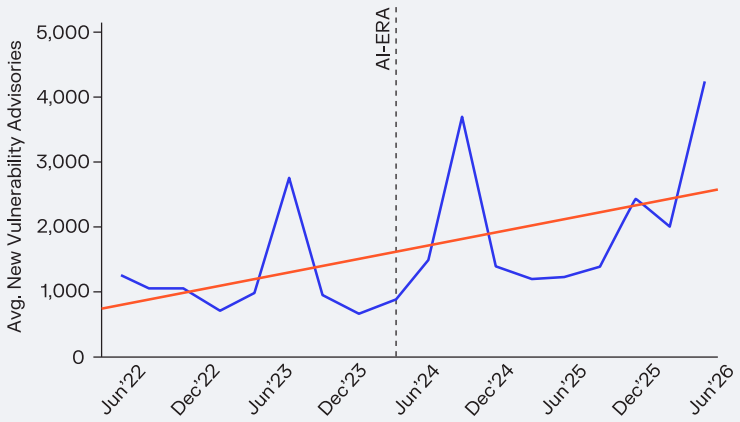
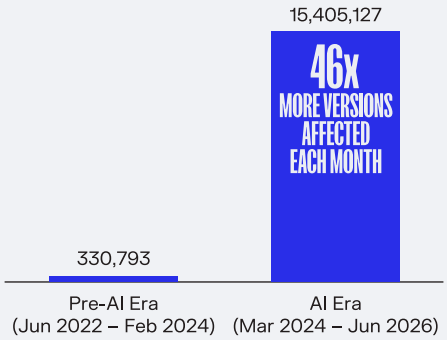


FIGURE 2B

Newly-Affected Component Versions

Finding vulnerabilities is only half the story. The number of newly affected component versions visible to organizations grew at 46x the pre-AI rate, dramatically expanding the volume of software requiring evaluation and response.



Crucially, vulnerabilities are not limited to newly published software. Every software dependency already inside an application has an increasing chance of receiving a newly disclosed vulnerability over time. We should revisit the concept of persistent risk, where exposure accumulates over time as vulnerabilities remain unresolved. The application itself may not have changed, but our understanding of its weaknesses has. Each newly discovered vulnerability creates another opportunity for exploitation until it is remediated.

In that sense, software becomes riskier not because the code has changed, but because the number of known attack paths has increased. However, applications are becoming riskier due to poor choices in tooling that are not using the proper data intelligence. The reasons for this acceleration are likely multifaceted. Greater investment in vulnerability research, improved disclosure processes, and AI-assisted security research may all contribute. This report does not attempt to isolate the impact of any one factor.

But the observable trend cannot be ignored. Today's software ecosystem discovers new vulnerabilities faster than yesterday's. Every application inherits that change and, as a result, every application inherits a continuously evolving security profile, even when development activity remains unchanged.

The natural response to a faster-moving vulnerability landscape is faster remediation. The challenge is that the volume of incoming software risk continues to grow just as quickly.

FACT 3

Organizations Are Responding Faster Than Ever

One of the most encouraging findings in this research is that organizations are getting significantly better at vulnerability remediation.

Over the past several years, automation has transformed how security teams respond to newly discovered vulnerabilities. Tools such as automated dependency updates, policy-driven workflows, and CI/CD integrations have reduced the time required to identify and resolve many issues.

Sonatype has observed the effects: between January 2024 and May 2026, the median age of unresolved violations fell by more than half, even as the total volume of vulnerabilities continued to grow. At the same time, more than half of resolved violations were addressed within a single day, a dramatic change from just two years earlier.

FIGURE 3A

Median Age of Unresolved Critical & High Vulnerabilities

Lower median age indicates organizations are resolving vulnerabilities more quickly. The typical unresolved Critical and High vulnerability was 45% younger during the AI era than before it (228 vs. 126 days). By May 2026, the median age had fallen even further to 103 days — a 59% reduction from its January 2024 peak.

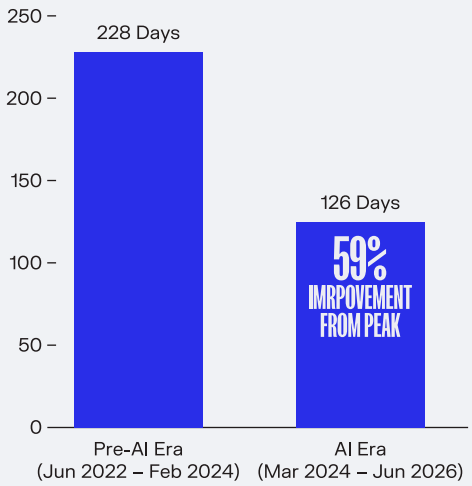
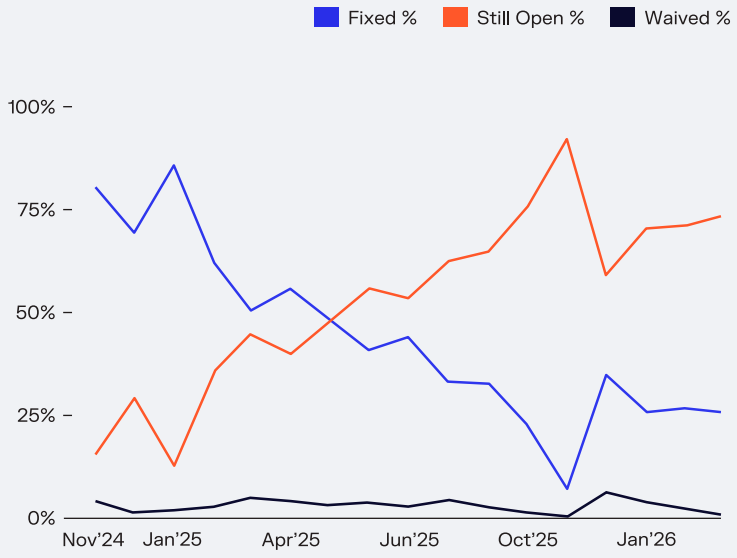


FIGURE 3B

AI-Era Critical & High Vulnerability Outcomes

Organizations are resolving vulnerabilities faster, but remediation still cannot keep pace with incoming risk. Among the earliest AI-era Critical and High vulnerability cohorts with at least 12 months of remediation runway, 52.6% were resolved, while 44.3% remained open. Waivers accounted for just 3.1%, showing the backlog reflects unresolved risk rather than policy exceptions.



This does not suggest remediation efforts are failing. On the contrary, organizations have fundamentally improved how they identify, prioritize, and remediate vulnerabilities. The challenge is that vulnerability discovery, software production, and dependency growth are all accelerating simultaneously. Faster remediation is reducing the age of the backlog, but not the rate at which new risk enters the software ecosystem.

Security teams have fundamentally changed how they remediate vulnerabilities. Organizations have invested in automation that enables vulnerabilities to be identified, prioritized, and remediated faster than ever before. In many cases, issues that once required days or weeks to resolve are now addressed within hours.

Yet despite those gains, applications continue accumulating more risk. Automation catches only ~8% of new violations same-day and only ~53% eventually; the rest sit in the manual queue or stay open. That isn't because remediation has become less effective. It's because the volume of incoming risk has increased at the same time organizations have accelerated their response — an important distinction.

> **ORGANIZATIONS ARE PROVING THEY CAN AUTOMATE REMEDIATION. THE HARDER CHALLENGE IS REDUCING THE AMOUNT OF AVOIDABLE RISK ENTERING SOFTWARE IN THE FIRST PLACE.**

FACT 4

Software Production Is Accelerating

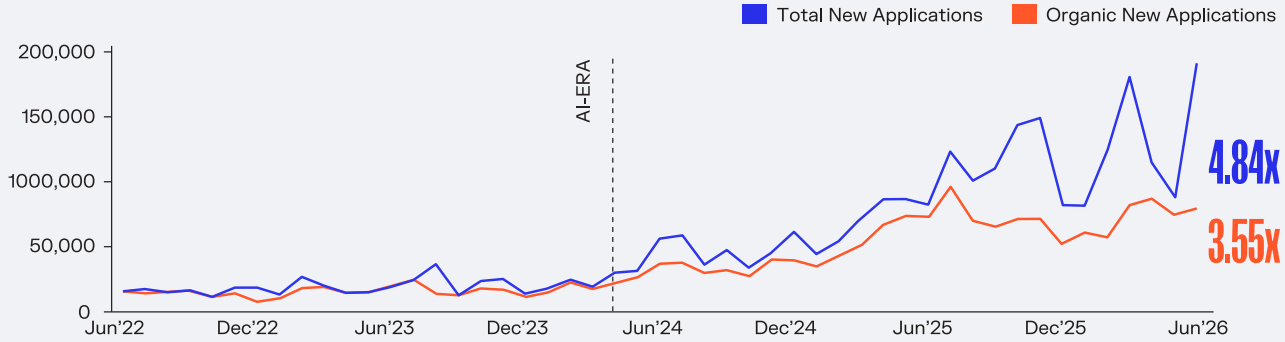
As organizations improve remediation and the vulnerability landscape continues to expand, one additional trend is reshaping software risk: they're building significantly more software.

Our analysis found that enterprise organizations created substantially more new applications after March 2024 than they did in the preceding two years. Even after accounting for customer onboarding and portfolio expansion, the rate of new application creation remained materially higher than the pre-AI baseline. Roughly 58% of AI-era new apps in this cohort are organic new development; 42% are bulk-onboarding of existing customer portfolios.

FIGURE 4

Enterprise Application Creation Accelerated After the AI Era

Enterprise application creation accelerated sharply after the beginning of the AI era. Average monthly application creation increased 4.84×, while organic new application creation (excluding large-scale onboarding events) still increased 3.55×, demonstrating that the acceleration reflects substantially more than portfolio expansion.



This growth reflects a broader shift in how software is developed. AI coding assistants, reusable frameworks, and mature open source ecosystems have reduced the time required to create and ship new applications, enabling organizations to deliver software at an unprecedented pace.

Building more software isn't the problem.

Every application creates new dependency decisions, new attack surfaces, and new security work.

That means software growth doesn't simply increase the amount of code organizations maintain. It multiplies the number of component selections, vulnerability disclosures, updates, and policy decisions that follow.

This is where the trends explored throughout this report begin to converge.

Organizations are building more applications. Each application relies on an expanding ecosystem of open source components. That ecosystem is generating new vulnerabilities faster than historical trends predicted, even as organizations improve remediation through automation.

Software growth doesn't create one new problem. It amplifies every existing one.

EVERY APPLICATION INHERITS TODAY'S ECOSYSTEM

A newly created application doesn't start with a blank slate. It inherits the current state of the software ecosystem, including today's dependency landscape, vulnerability disclosures, and security risks.

As organizations build more software, they also inherit more of that ecosystem with every new project.

The final chapter examines one of the most important consequences of that acceleration: the growing importance of dependency decisions at the moment software is assembled.

FACT 5

Dependency Decisions Matter More Than Ever

Not every vulnerable dependency represents a poor decision. Sometimes, maintainers simply have not published a safer release.

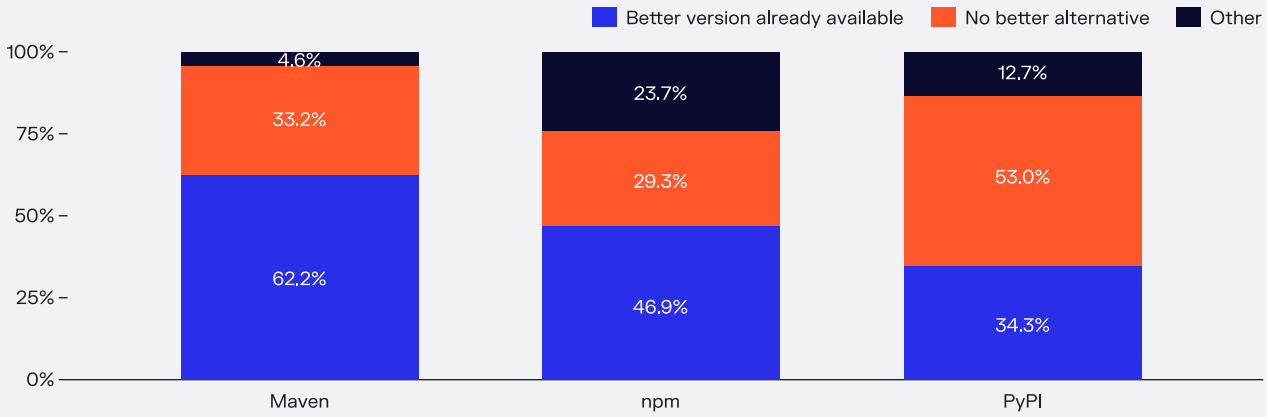
When that happens, organizations have little choice but to accept the available risk until the ecosystem catches up. But in many cases, developers and AI assistants are choosing between multiple versions with meaningfully different security characteristics.

To understand how often those decisions were avoidable, we examined every vulnerable dependency introduced by AI-era applications and asked a simple question: At the time the dependency was adopted, was a materially lower-risk version already available?

The answer varied across ecosystems, but a clear pattern emerged. In Maven Central, nearly two-thirds of vulnerable dependency selections occurred even though a lower-risk version already existed. npm showed a similar, though less pronounced, trend, while PyPI more frequently reflected genuine ecosystem constraints, where no materially safer alternative was available.

FIGURE 5

Lower-Risk Version Ability At Adoption



This finding should not be interpreted as developer error, but rather points to the need for organizations to rethink software risk. Some vulnerabilities are unavoidable consequences of the ecosystem. Others are information problems, where developers or AI assistants simply lack the context needed to choose the safest available option.

As software development accelerates, those information gaps become increasingly expensive. Every dependency decision now happens against a backdrop of a rapidly expanding vulnerability landscape, compressed release cycles, and AI systems capable of introducing components faster than humans can reasonably evaluate them.

The result is an information problem rather than a human one. Keeping software current is no longer simply about knowing which version is newest. It requires continuously understanding which versions are compatible, actively maintained, and lower risk as the ecosystem changes around them.

The software decisions that carry the most weight are increasingly the ones made before the first security scan ever runs.

VULNERABLE DEPENDENCY SELECTED

Was a lower-risk version already available?

YES

Developers could have chosen a safer version.

NO

The ecosystem offered no materially better alternative.

Software Risk Is Moving Earlier

In the AI era, organizations are building more applications. The vulnerability landscape is expanding faster than historical trends predicted. Security teams are remediating issues more quickly through automation. Yet despite those improvements, enterprise applications continue accumulating more risk.

This report does not argue that AI alone caused these changes. AI is one plausible accelerant among many, influencing how software is built, vulnerabilities are discovered, and attackers operate. But proving direct causation is difficult. Organizations rarely measure how AI influences development decisions, and attackers don't disclose whether their campaigns were AI-assisted.

Fortunately, the broader conclusion does not depend on proving causation.

- **The environment changed.**
- **There's more risk.**
- **Developers are making better software decisions.**
- **Security improved.**
- **The environment moved faster.**

Vulnerability management isn't becoming less important. It's no longer the only place where security outcomes are determined. In fact, our data shows organizations are getting better at it. Concurrently, more security outcomes are being shaped before remediation ever begins.

As more software is assembled from open source components and AI-generated recommendations, the earliest software decisions increasingly shape everything that follows.

> **THE SOFTWARE DECISIONS THAT MATTER MOST ARE INCREASINGLY THE ONES MADE BEFORE THE FIRST SECURITY SCAN EVER RUNS.**

That shift has implications beyond AI. It suggests the next evolution of software supply chain security will be defined not only by how quickly or at which perimeter organizations detect, find, and remediate vulnerabilities but by how effectively they help developers make better software decisions at the point of assembly.

Methodology

This report analyzes how software risk has evolved throughout the AI era using a fixed cohort of enterprise applications continuously monitored by Sonatype between June 2022 and June 2026.

Unless otherwise noted, all findings are based on enterprise customers whose applications have been continuously scanned since June 2022. By holding the customer cohort constant over the full study period, this research isolates changes in software risk over time rather than changes driven by customer acquisition or sample composition.

Throughout this report, March 2024 marks the beginning of the AI era. Most analyses span the full 49-month period from June 2022 through June 2026, allowing comparisons before and after the widespread adoption of AI-assisted development. Where data availability differs, individual figures note the applicable time window. For example, remediation flow analysis uses data from November 2024 through March 2026, reflecting the availability of detailed fix-tracking telemetry, while analyses comparing newly created AI-era applications with established applications use the same enterprise cohort but separate applications first scanned after March 2024 from pre-existing applications meeting equivalent health and freshness criteria.

All analyses were performed using Sonatype's internal security telemetry and software composition analysis data. Technical implementation details, SQL queries, and statistical methodology for each figure are documented separately in the companion technical methodology.