CHECKMARX ONE · AGENTIC APPLICATION SECURITY

Checkmarx

Triage Assist & Remediation Assist

Prioritize attackable risk, keep backlog current, and accelerate remediation.

SOLUTION BRIEF

Frontier AI changed the economics of creating, discovering, and exploiting application risk. It can generate more code, surface more findings, and compress the time between vulnerability discovery and exploitation faster than manual review cycles can absorb. But frontier AI alone cannot reliably determine what matters inside an enterprise environment. It lacks the complete code context, reachability, exploitability, policy, governance, and auditability required to consistently prioritize risk and drive safe remediation.

Checkmarx Triage Assist and Remediation Assist are generally available in Checkmarx One for eligible SAST and SCA risks. Triage Assist evaluates new and existing findings using Attackability-based context, while automated triage rules and cadence help teams continuously assess eligible risks and keep backlog current.

Remediation Assist provides context-aware remediation guidance in Checkmarx One across supported project types. For supported GitHub Code Repository Integration projects, teams can additionally generate review-ready fix pull requests that developers review, approve, and merge through their existing GitHub workflows.

The result: less repetitive manual triage, faster remediation, lower rework, measurable adoption and impact visibility, and a governed path from finding to action across backlog, SCM, and developer workflows.

The agent proposes. Humans approve. And Checkmarx One governs and measures the impact.

Attackability-Based Prioritization

Reachability, exploitability, code context, and policy signals help teams focus on findings that present concrete risk, not simply the highest generic severity score.

Automated Backlog Triage

Configure triage rules and cadence to continuously assess eligible risks without overriding vulnerabilities that have already been triaged.

Up to 95% Lower MTTR

Reduce repetitive triage and accelerate movement from finding to review-ready remediation, with more than 65% of findings fixed on the first attempt.

Usage, Adoption & Impact Visibility

Track AI triages and remediations, developer adoption, estimated time saved, pull request usage, recommendation engagement, suspected false-positive outcomes, and remediation activity in Checkmarx One Analytics.

THE CHALLENGE

Frontier AI Increases Security Pressure Alongside Vulnerability Discovery.

AI-assisted development is increasing code volume, vulnerability volume, and remediation pressure at the same time. Frontier models are also accelerating the discovery of legacy flaws, expanding the backlog from both sides: vulnerabilities introduced through new code and previously unknown risks uncovered in existing applications.

AppSec teams need a faster, governed way to determine what matters, explain why it matters, keep existing risk current, and help developers move from finding to fix.

The real bottleneck is no longer discovery alone. It is execution:

- Determining which findings require action
- Continuously reassessing risk as code and context change
- Keeping vulnerability backlog current
- Delivering useful remediation guidance
- Preserving human oversight and traceability
- Measuring adoption, time saved, engagement, and remediation outcomes
- Proving that AI-assisted AppSec is improving operational efficiency

Without enterprise security context, trusted scan results, policy controls, auditability, approval workflows, and measurable outcome visibility, frontier AI can endlessly generate more signal and more noise – creating additional triage work rather than reducing risk.

Checkmarx One provides the governed application-security control plane needed to turn findings into decisions, decisions into review-ready fixes, and activity into measurable outcomes.

WHAT DOES TRIAGE ASSIST & REMEDIATION ASSIST DO?

From Findings to Governed Decisions and Review-ready Fixes

Triage Assist and Remediation Assist help teams close the gap between what Checkmarx One finds and what AppSec and developers can act on.

For eligible SAST and SCA findings, Triage Assist applies Attackability-based context – including reachability, exploitability, code context, and policy signals – to help distinguish theoretical vulnerabilities from risks that require action.

AppSec teams can configure automated triage rules and cadence to assess eligible vulnerabilities continuously rather than one at a time or in manual batches. Previously triaged risks remain unchanged, helping teams maintain established decisions while keeping the rest of the backlog current.

Within Risk Orchestration, security teams can:

- Review AI-generated triage and remediation context
- Re-trigger AI analysis when a risk needs updated review
- Access related pull requests where available
- Update a risk's state based on AI Triage results
- Identify AI-driven updates through visible indicators and changelog history

Remediation Assist turns prioritized risk into context-aware remediation guidance within Checkmarx One across supported project types. For supported GitHub Code Repository Integration projects, it can additionally generate a separate remediation pull request containing suggested code changes for developer review and approval.

AppSec retains governance, developers retain control of the code, and Checkmarx One preserves visibility and traceability across the process. This process gives leaders the data needed to measure adoption and impact.

DESIGNED FOR APPSEC, LOVED BY DEVELOPERS

Built on Checkmarx One

Triage Assist and Remediation Assist extend Checkmarx One beyond vulnerability detection and into governed, measurable risk execution.

AppSec teams can:

- ✓ Enable capabilities for supported projects
- ✓ Configure eligibility and severity thresholds
- ✓ Define automated triage rules and cadence
- ✓ Review AI insights centrally in Risk Orchestration
- ✓ Re-trigger analysis as code or context changes
- ✓ Manage consumption through Checkmarx Credits
- ✓ Track adoption, activity, time saved, engagement, and remediation outcomes in Analytics
- ✓ Analyze usage across projects and time ranges
- ✓ Preserve human review, approval, and auditability

The capabilities are grounded in Checkmarx One scanning intelligence, application context, and policy controls, not raw model judgment alone.

HOW IT WORKS

From Findings to Decisions, Fixes, and Proof

01: Analyze

Checkmarx One identifies eligible SAST and SCA findings across supported repositories and SCM, backlog, and developer workflows.

02: Prioritize

Triage Assist evaluates eligible findings using Attackability-based context, including reachability, exploitability, code context, and policy signals.

This helps teams distinguish findings that represent concrete risk from vulnerabilities that may be theoretical, mitigated, or not exploitable in the application's actual context.

03: Automate and Review

Customers can define automated triage rules and cadence, so eligible vulnerabilities are assessed continuously against predefined criteria.

AppSec teams can review AI-generated context in Risk Orchestration, re-trigger analysis when updated review is needed, and update risk state based on AI Triage results. AI-driven updates are visibly marked for traceability.

04: Remediate

Remediation Assist provides context-aware remediation guidance in Checkmarx One across supported project types. Developers can use that guidance within their existing development workflows. For supported GitHub Code Repository Integration projects, teams can additionally generate a separate fix pull request containing existing GitHub workflow. approve, and merge the remediation through their suggested code changes. Developers review, refine,

05: Measure

The AI Assist Usage view in Analytics gives AppSec and engineering leaders visibility into adoption, activity, and operational impact, including:

- AI triages and remediations performed
- Unique developer participation and adoption
- Estimated developer time saved
- Pull request usage
- Recommendation engagement
- Suspected false-positive outcomes
- Remediation activity and results
- Usage and outcome trends across projects and time ranges

This visibility helps teams understand not only whether AI Assist is being used, but where it is saving time, reducing repetitive work, and improving remediation execution.

Key Capabilities

Attackability-Based Prioritization

Move beyond severity-only queues. Focus on findings that are reachable, exploitable, and relevant in the application's actual code and policy context.

Automated Backlog Triage

Define rules and cadence for continuous AI Triage of eligible risks, reducing repetitive manual work while preserving previously completed triage decisions.

Centralized Review in Risk Orchestration

Review AI-generated triage and remediation context, access related pull requests, re-trigger analysis, and act on findings without leaving Checkmarx One.

Governed Risk-State Updates

Use AI Triage results to update supported risk states while preserving visible AI indicators, changelog history, and human oversight.

Review-Ready Remediation

Deliver actionable remediation guidance across supported projects within Checkmarx One, with review-ready GitHub fix pull requests available where supported.

Checkmarx One Controls

Manage project enablement, severity thresholds, automated rules, cadence, consumption, governance, and traceability through Checkmarx One.

AI Assist Usage Analytics

Measure AI triage and remediation volume, developer adoption, estimated time saved, pull request usage, recommendation engagement, suspected false positives, remediation activity, and trends over time.

Value and Impact

Reduce Repetitive Manual Triage

Automate recurring triage work and give AppSec teams the context needed to make faster, more consistent risk decisions.

Keep Backlog Current

Continuously reassess eligible findings agains defined criteria so teams can focus on the risks that need attention now.

Reduce MTTR by Up to 95%

Move more efficiently from prioritized risk to actionable guidance and review-ready remediation.

Fix More Than 65% on the First Attempt

Context-aware remediation and review-ready fixes reduce rework and help more findings reach successful resolution

Improve Developer Productivity

Give developers relevant remediation context and actionable guidance, with review-ready fix pull requests available for supported GitHub projects, reducing disconnected portals, tickets, and manual research.

Lower Remediation Cost

Reduce unnecessary triage, handoffs, context switching, and repeated fix attempts across AppSec and engineering teams.

Preserve Governance and Human Control

Keep people accountable for triage decisions, code changes, approval, and merge while AI accelerates analysis and execution.

Prove AI-Assisted AppSec Impact

Use Checkmarx One Analytics to measure adoption, activity, estimated developer time saved, PR usage, engagement, suspected false positives, remediation results, and trends across projects and time periods.

Built for How Teams Actually Work

Triage Assist and Remediation Assist connect AppSec and development across Checkmarx One, Risk Orchestration, Analytics, and supported SCM and developer workflows — without replacing trusted scanners, enterprise policies, or human review.
Keep backlog current. Accelerate developer remediation. Prove adoption and impact.

Current availability and scope: *Triage Assist and Remediation Assist support eligible SAST and SCA risks across supported project types. Automated workflows run AI Triage; remediation remains governed and human-approved. Remediation guidance is available within Checkmarx One across supported project types. Automatic remediation pull request creation currently requires a supported GitHub Code Repository Integration project. Checkmarx Credits are required. Performance results may vary by environment and implementation.*