mitrais | MEMBER OF CAC HOLDINGS GROUP

VERACODE - Application Risk Management Platform

Build, Scale and Secure Software with Independent Validation

Mitrais has been a pioneer in the development of near-shore software development services to Australia and other markets for more than 30 years. With over 500 software engineers, Mitrais provides services from development centers in Bali, Jakarta, Bandung and Yogyakarta in Indonesia.

www.mitrais.com

Security That Goes Beyond Scanning

Traditional and AI scanning both have blind spots. Your enterprise security demands more:

Pattern Scanning Misses Complexity

Business logic flaws and broken access control slip through credential detection.

Compliance Demands Independence

Audit trails and policy enforcement aren't optional, they're regulatory mandates.

Single-Vendor Control Creates Risk

Independent validation is non-negotiable, regardless of who wrote the code.

Confidential © Mitrais

Why Independent Validation Matters for Enterprise Security:

Regulators Require Independent Verification and Audit Trails

GDPR, PCI-DSS, and ISO 27001 auditors demand third-party attestation with documented evidence. Self-validation by code generators fails compliance.

Enterprise Governance Needs Centralised Control

Without unified visibility across AI tools and developers, you cannot enforce policies, track remediation, or report risk to your board.

One Vendor Shouldn't Control Both Sides

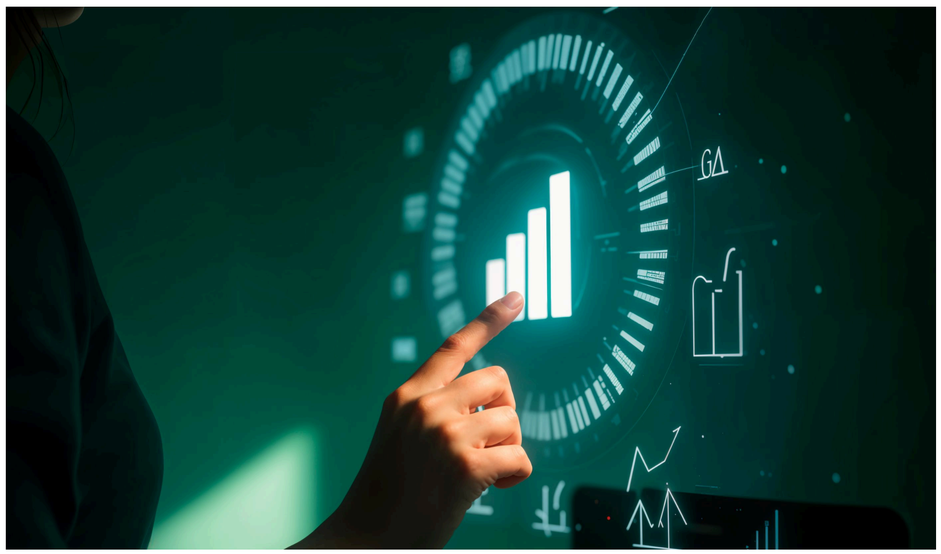
When the same tool writes and validates code, you lack independent verification and accountability when vulnerabilities slip through.

Supply Chain Attacks Exploit Unmonitored Dependencies

80% of your code comes from third-party libraries. Without independent monitoring, your largest attack surface remains unprotected.

Secure Apps with Independent Validation and Compliance Built In

Deliver secure code faster with compliance built in and validation independent of your development tools. Veracode validates code from any source, providing centralized visibility, risk prioritization, and automated remediation across your portfolio. We monitor dependencies with Package Firewall and generate the audit trails and SBOMs regulators require. Think of Veracode as your independent security layer working with any development approach, protecting applications while proving compliance effortlessly.



Confidential © Mitrais

The Veracode Solution: Correlated, Prioritised and Fixed

Application Risk Management Platform

Traditional and AI scanning have blind spots. Compliance demands independent governance. One vendor shouldn't control both sides. ***Veracode provides independent, third-party validation with enterprise-grade governance, validating code regardless of source.***

With Veracode, you get unified risk visibility: ***correlated, prioritised, and actionable.*** *Risk Manager shows you the fewest actions for greatest impact.*

We bring structure to chaos by deduplicating noise, correlating risk across silos, and surfacing the ***5 "Best Next Actions"*** *to mitigate your greatest security risks.*

How It Works:

Scattered findings from any tool, including AI-assisted code, become correlated issues through our vendor-neutral platform. Generic alerts become targeted solutions. Manual remediation becomes automated fixes delivered in developers' IDEs with complete audit trails.

Why It Matters:

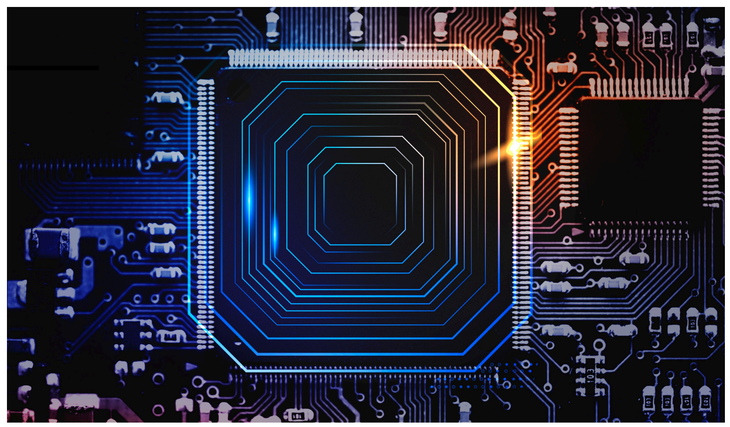
We integrate with 100+ languages, GitHub, GitLab, Azure DevOps, and major cloud platforms to assess risks across infrastructure, containers, and applications. Whether code comes from developers or AI assistants, Veracode provides independent validation with centralized governance, audit trails, and compliance documentation that regulators require. You gain visibility into exploitable risks and the fewest actions to secure them with third-party verification enterprises demand.

Confidential © Mitrais

Platform Components

Risk Manager – Application Security Posture Management (ASPM)

Our Risk Manager is an advanced Application Security Posture Management solution designed to reduce organisation risk by identifying and remediating risks that matter most to your business. It delivers a unified view of risk by easily integrating with existing security tools across code repositories, pipelines, IaC, and cloud infrastructure. This empowers teams to quickly remediate application and cloud vulnerabilities through consolidated, correlated, and contextualised findings.



60 to 1 Noise Reduction

Risk Manager identifies risks and calculates the Best Next Action to deliver unprecedented noise reduction, enabling teams to focus on what truly matters.

Vendor Neutral Platform

Connects to any finding source, no matter where it lives in the security ecosystem. Integrates with over 50 easy-to-set-up connectors across Cloud, AST, and Identity tools.

Unified View from Code to Runtime

Provides comprehensive understanding of security risk across tools by aggregating, deduplicating, and correlating findings.

Automated Root Cause Analysis

Automatically pinpoints the owner and root cause of each security issue, translating issues into actionable root solutions to efficiently fix multiple problems with far fewer developer tickets.

Best Next Actions™

Get prioritised, step-by-step remediation solutions and manage issue status with two-way ticket sync, focusing on risk reduction instead of managing an ever-growing backlog.

Confidential © Mitrais

Software Supply Chain Security

Protect your software supply chain with comprehensive security analysis of open-source and third-party components. With 70% of vulnerabilities originating from open-source code, securing your supply chain is critical.

Software Composition Analysis (SCA)

Our Software Composition Analysis enables organisations to leverage open-source capabilities while effectively mitigating associated risks. SCA continuously monitors your software ecosystem, delivering automated remediation for open-source vulnerabilities and ensuring licence compliance.

- **Critical Statistics:** 80% of open-source codebases contain known vulnerabilities, making continuous monitoring essential.
- **Comprehensive Coverage:** Scans across 1.24M+ open-source repositories, integrating seamlessly into your pipeline to prioritise and remediate vulnerabilities beyond the National Vulnerability Database (NVD).
- **Malicious Package Detection:** Harness advanced AI and threat intelligence to detect and block malicious packages with 60% greater accuracy than competitors, preventing supply chain attacks before they start.
- **Automated Remediation:** Automate fixes with intelligent auto-pull requests to apply the best fix with guidance on how it impacts code functionality, eliminating guesswork.
- **Automated Remediation:** Automate fixes with intelligent auto-pull requests to apply the best fix with guidance on how it impacts code functionality, eliminating guesswork.
- **Reachability Analysis:** Vulnerability Method Analysis pinpoints where your code interacts with risks in libraries and components, allowing you to zero in on the code that matters most.
- **SBOM Generation:** Generate and analyse Software Bills of Materials (SBOMs) to gain unprecedented insight into your software supply chain risk.

Confidential © Mitrais

Package Firewall

Package Firewall is an automated governance solution designed to dynamically control and monitor the use of software packages by blocking vulnerabilities, malware, and policy violations before they enter development pipelines.

- **Critical Threat Landscape**: Malicious packages skyrocketed by 9 times in 2024, posing an unprecedented risk to software development.

- **Proactive Detection:** Identify and block malicious packages in real time with industry-leading threat detection technology, protecting enterprises from the rising tide of open-source threats.

- **Policy Flexibility**: Built on Open Policy Agent (OPA), offering policy-as-code with 20+ pre-built policies and customisable analytics across vulnerabilities, malware, licences, authors, and engineering risks.

- **Developer Experience:** Empowers developers with real-time, in-console feedback via Slack or Teams integration, with workflow for requesting policy exceptions to ensure business agility.

- **Audit Mode**: Test policies in warn mode to assess impact without disrupting workflows, enabling security teams to evaluate benefits before full enforcement.

Confidential © Mitrais

Threat Intelligence

Our Threat Intelligence service provides real-time threat data and vulnerability intelligence to help organizations prioritize security responses based on active exploits and emerging attack patterns. This proactive approach ensures your security team focuses on the threats that pose the greatest risk to your organization.

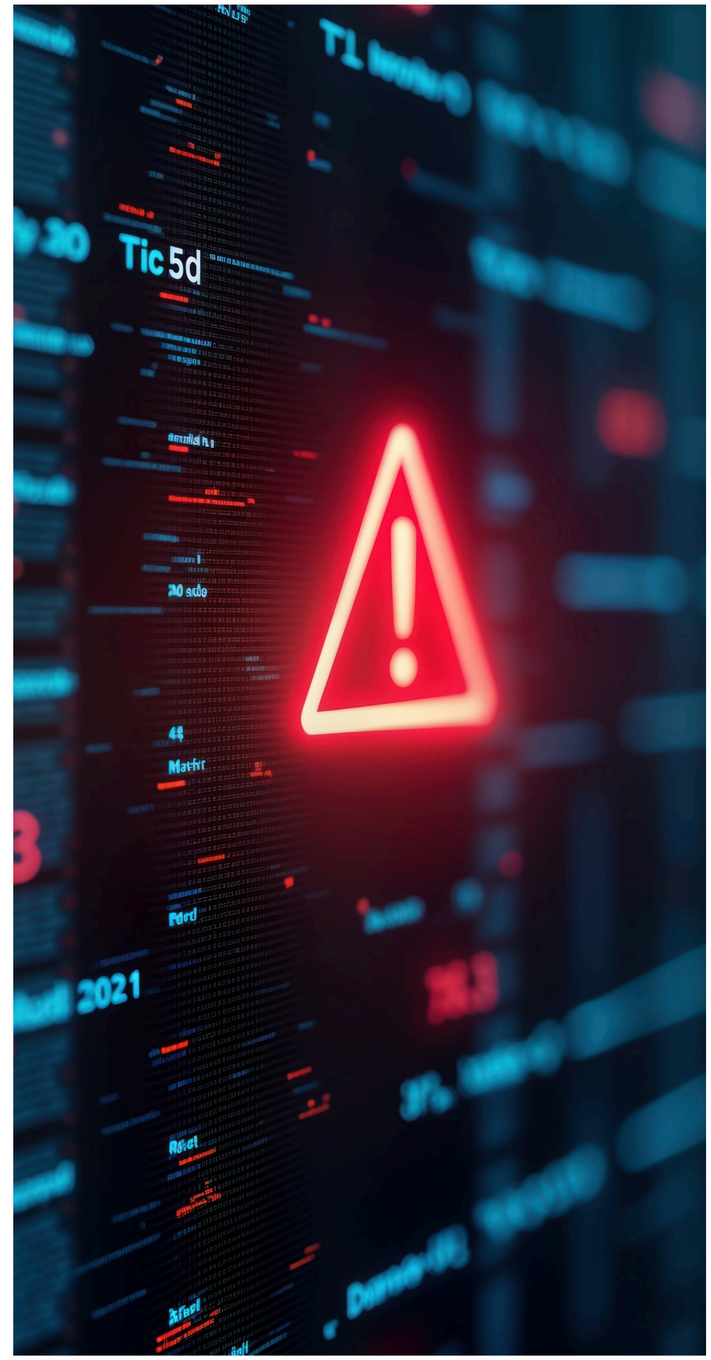
- **Real-Time Threat Data: Access**: continuously updated intelligence on emerging vulnerabilities, active exploits, and attack vectors affecting your technology stack and industry.

- **Contextual Prioritization:** Correlate vulnerability data with threat intelligence to understand which security issues are actively being exploited in the wild, enabling risk-based prioritization of remediation efforts.

- **Attack Pattern Analysis:** Identify emerging attack patterns and tactics used by threat actors, helping security teams stay ahead of evolving threats and adjust defensive strategies accordingly.

- **Industry-Specific Intelligence:** Receive threat intelligence tailored to your industry sector, understanding the specific attack vectors and vulnerabilities that threat actors target in your domain.

- **Integration with ASPM:** Threat intelligence seamlessly integrates with Risk Manager to enrich vulnerability findings with exploitability data, helping calculate more accurate Best Next Actions™.



Confidential © Mitrais

Application Security Testing

Comprehensive testing methodologies to identify vulnerabilities throughout the development lifecycle, from code creation to runtime deployment.

Static Application Security Testing (SAST)

A powerful, developer-friendly solution designed to identify security weaknesses in your code during the development process. Seamlessly integrated from your IDE to CI/CD pipeline, SAST empowers developers to catch flaws early, prevent vulnerabilities in real-time, and ensure compliance before deployment.

- **Industry-Leading Accuracy:** Less than 1.1% false positive rate without manual tuning, delivering the most precise results in the industry.
- **Comprehensive Language Support:** Supports over 100 languages and frameworks including Java, JavaScript, Python, C#, C++, PHP, and more.
- **Growing Threat Landscape:** 181% increase in percentage of apps with high-severity flaws since 2020, making early detection more critical than ever.
- **Real-Time IDE Integration:** Integrates security directly into your IDE (VS Code, IntelliJ, Visual Studio, Eclipse, PyCharm) for real-time feedback to catch and fix flaws early.
- **CI/CD Pipeline Integration:** Embeds security into development workflows from IDE to CI/CD pipeline, bug tracking, and SSO for seamless DevSecOps.
- **Intelligent Prioritisation:** Triages findings and uses AI to prioritise flaws based on their potential impact, providing contextual guidance to focus on critical issues first.

Confidential © Mitrais

Dynamic Application Security Testing (DAST)

DAST integrates enterprise-level dynamic scanning with external attack surface visibility and an intuitive, modern user experience. This powerful combination enables teams to discover shadow web apps and APIs while leveraging advanced features like highly-configurable, in-depth scans and industry-low false positives.

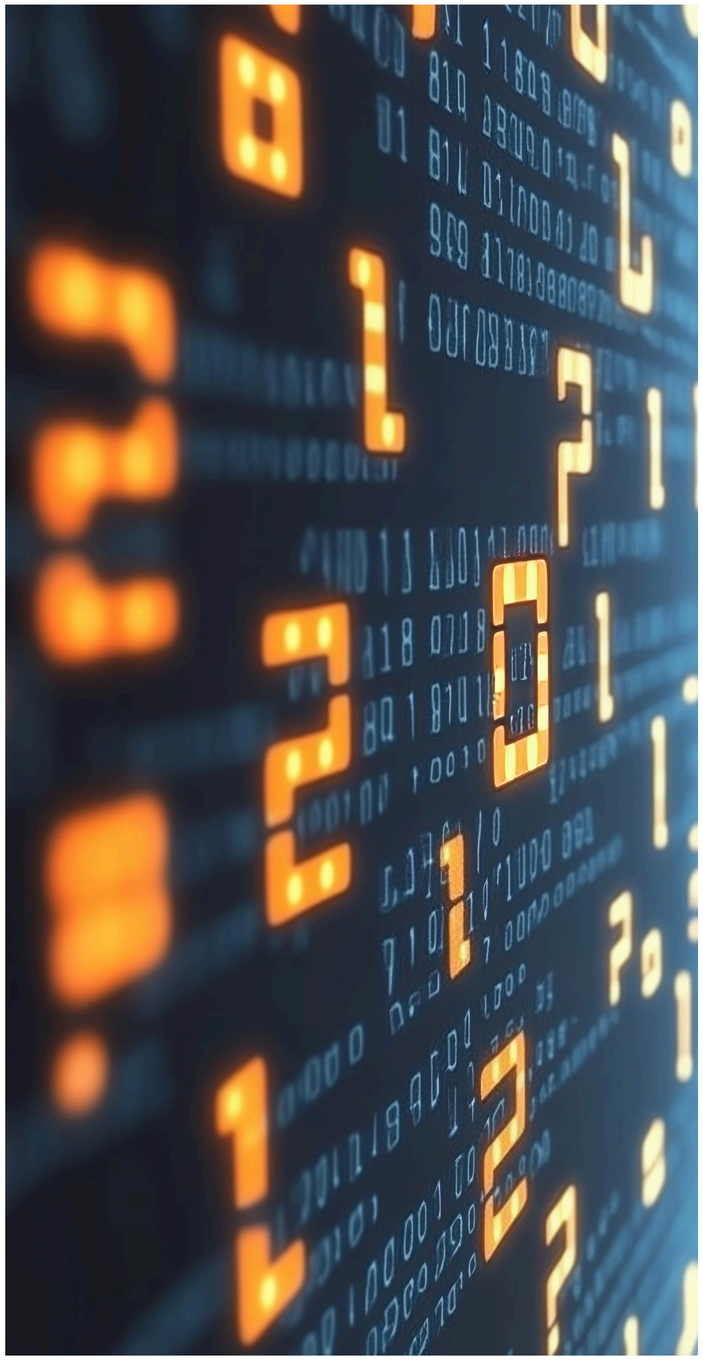
- **Critical Coverage:** 80% of web applications have a critical vulnerability that can only be found with a dynamic scan, making DAST essential for comprehensive security.
- **Industry-Low False Positives:** Less than 1% false positive rate, ensuring robust security without slowing down modern development cycles.
- **Rapid Results:** Real-time vulnerability detection with scan results delivered in as little as 3 minutes, enabling faster risk mitigation.
- **AI-Assisted Login:** Streamline complex scan authentication with unique AI-powered automation for intricate login scenarios, significantly reducing manual effort
- **Internal Scanning:** Scan applications behind corporate firewalls with Internal Scanning Management (ISM), providing comprehensive coverage for enterprise environments.
- **Seamless Pipeline Integration:** Launch scans in just a few clicks, embedding real-time scans into CI/CD pipelines to catch vulnerabilities early and speed up compliant deployments.

Confidential © Mitrais

Container and Infrastructure as Code (IaC) Security

Empowers developers to build secure containers and IaC files early in the SDLC. Integrated into CI/CD pipelines and accessible via an intuitive CLI, it scans for vulnerabilities, misconfigurations, and secrets, delivering actionable insights to fix issues fast.

- **Accelerated Remediation:** 50% faster remediation time with CLI and actionable insights, cutting time from hours to minutes.
- **Sub-Minute Scans:** Handles 10,000+ containers with sub-minute scans in high-velocity environments, supporting AWS, Azure, or on-premises setups.
- **Comprehensive Scanning:** Scans container images, IaC files (Terraform, CloudFormation, Kubernetes manifests, Dockerfiles, Helm charts) for vulnerabilities, misconfigurations, and hardcoded secrets.
- **Secrets Detection:** Detects hardcoded secrets including cloud keys (AWS, GCP), platform tokens (GitHub, GitLab, Slack), and cryptographic keys (RSA), addressing 75% of container vulnerabilities.
- **SBOM Generation:** Generates Software Bills of Materials in JSON, CycloneDX, and SPDX formats for compliance and supply chain transparency.
- **Policy Enforcement:** Prioritises critical issues with pre-built policies aligned with CIS Benchmarks, highlighting severe vulnerabilities for rapid remediation.



Confidential © Mitrais

AI-Powered Remediation (Veracode Fix)

Veracode Fix is an AI-powered remediation solution that proactively identifies and automatically generates secure code fixes, empowering organizations to aggressively manage security debt and secure software at scale. The meteoric rise of generative AI in code creation has ignited a vulnerability wildfire, with average fix times reaching 252 days. Veracode Fix directly addresses these challenges by dramatically accelerating remediation.

- **Critical Challenge:** Average fix time for software security vulnerabilities has reached 252 days according to the State of Software Security 2025 report, creating massive security debt.
- **Responsible AI in Practice:** Trained on proprietary, secure reference patches (not open-source code prone to flaws or IP issues), avoiding model poisoning and prompt injection. Uses supervised learning with Veracode's Threat Research Team for expert-aligned, consistent fixes.
- **Purpose-Built for Remediation:** Unlike generalist AI tools like ChatGPT or GitHub Copilot, Veracode Fix excels specifically at fixing flaws rather than finding them or generating potentially insecure code.
- **High Fix Accuracy:** Automatically resolves flaws with high accuracy across multiple languages, achieving 3-out-of-4 success rate for Java static findings. Supports Java, C#, JavaScript, TypeScript, Python, PHP, Scala, Kotlin, and Ruby.
- **Comprehensive CWE Coverage:** Targets prevalent vulnerabilities including CWE-80 (XSS), CWE-89 (SQL Injection), CWE-117 (Log Injection), addressing 92% of critical open flaws across supported languages.
- **Batch Remediation:** Bulk remediation of flaws across files in one CLI operation, ideal for scalable fixes like sanitizers, dramatically reducing the time needed to address security debt.
- **IDE Integration:** Real-time fixes delivered directly in VS Code (with IntelliJ, PyCharm, Visual Studio Code, and Eclipse in development), keeping development context intact and minimizing workflow disruption.
- **Simple Execution:** A single 'fix' command delivers secure patches without manual effort, integrating seamlessly into developer workflows via CLI or IDE.

Confidential © Mitrais

Business Outcomes Delivered

Real-world results from organisations that have implemented our Application Risk Management Platform, demonstrating measurable improvements across multiple industries.

View Stream Figure	Situation	Customer Outcome
Speed to Market	Automotive industry organisation struggling with slow security scans taking days instead of minutes, drastically slowing development processes and delaying software releases.	Reduced scan time from days to minutes and successfully onboarded over 400 applications, dramatically accelerating time to market whilst maintaining robust security.
Security Posture	Supply chain solutions provider transitioning to cloud-native SaaS required automated security to protect customer data and maintain zero security breaches whilst scaling operations.	Implemented comprehensive security programme with automated scanning, maintaining zero security breaches and providing single pane of glass visibility across all applications.
Development Efficiency	Community management software provider using multiple vendors resulting in scattered reports, delayed releases, and inability to optimise security programme effectively.	Streamlined security with centralised reporting, empowering developers to write secure code from the outset and eliminating months of potential rework.
Scalable Growth	Financial services platform with 20M+ customers facing aggressive expansion plans requiring ability to confidently release new software whilst ensuring compliance and protecting growing customer base.	Accelerated scans from 16 to under 6 minutes enabling 1,000+ monthly deployments. Gained scalable security solution supporting rapid international expansion with full compliance assurance.
Risk Reduction	Global trade management software provider moving platform to cloud with perimeter security unable to support increased demands, requiring embedded AppSec in developer workflows.	Integrated AppSec early in SDLC reducing risk whilst improving developer efficiency. Elevated security awareness across teams and strengthened customer confidence through validated practices.

Confidential © Mitrais

Why Mitrais?

Mitrais stands out as a trusted provider of application risk management solutions, delivering enterprise-grade security to organisations across finance, healthcare, and technology.

Comprehensive Coverage

Supports SAST, DAST, SCA, Container/IaC security across 100+ languages and frameworks, ensuring no vulnerability goes undetected.

Supply Chain Security

Package Firewall and Threat Intelligence protect against supply chain attacks and vulnerable dependencies.

Advanced Risk Prioritisation

60 to 1 noise reduction with Best Next Actions™, focusing your team on what matters most.

Developer Empowerment

Offers eLearning, hands-on labs, and remediation coaching to upskill teams in secure coding practices.

Seamless Integration

Integrates with over 40 DevOps tools, including GitHub, GitLab, and Azure DevOps, for frictionless workflows.

Trusted Partner

30+ years serving clients globally, partnering with Veracode, a global leader in application security founded in 2006 with 369+ positive Gartner Peer Insights reviews. This partnership combines Mitrais' local expertise and software development capabilities with Veracode's industry-leading security platform.

Confidential © Mitrais

Ready to Secure Your Applications?

Whether you're building new applications or securing existing systems, Mitrais provides the expertise and technology to help you manage application risk at scale. Contact Mitrais to discuss how our Application Risk Management Platform can enhance your security posture.

Confidential © Mitrais

MITRAIS | MEMBER OF CAC HOLDINGS GROUP

Contact Us

Indonesia 0361-849-7952

Bali

Jl. By Pass Ngurah Rai
Gg. Mina Utama No. 1,
South Denpasar, Denpasar,
Bali 80223

Jakarta

Wirausaha Building, 8th Floor,
Jl. H.R. Rasuna Said Kav. C5,
South Jakarta,
Jakarta 12940

Bandung

Jl. Prof. Drg. Surya Sumantri No. 8D,
Sukawarna, Sukajadi, Bandung,
West Java 40164

Yogyakarta

Jl. Sidobali No. 2, Muja Muju,
Umbulharjo, Yogyakarta,
Special Region of Yogyakarta
55165

Overseas

Singapore

3158-1185

10 Anson Road,
#03-05
International Plaza,
Singapore 079903

Australia

1800-755-025

New Zealand

0800-755-025

MITRAIS | MEMBER OF CAC HOLDINGS GROUP

Terima Kasih　　**Thank** You　　**ありがとう**ございました