

Embed intelligent security into development and cloud foundations

Modern organisations must secure increasingly complex cloud and AI-driven environments. Traditional reactive security approaches are no longer sufficient.

Arinco's Platform Security Accelerator embeds AI-powered security tooling directly into development pipelines and cloud platforms. Leveraging capabilities such as GitHub Advanced Security (GHAS), AI-driven code scanning, automated vulnerability detection and intelligent remediation workflows, we help organisations move from reactive security to proactive defence. By combining DevSecOps practices, policy-as-code guardrails and AI-enabled auto-remediation capabilities, we reduce vulnerability exposure windows and close critical security gaps faster. The result is a continuously monitored, intelligently protected platform that strengthens compliance, reduces operational risk and scales securely alongside innovation.

Why organisations use Arinco's Platform Security Accelerator



Address gaps in software and infrastructure with modern DevSecOps practices.



Identify and resolve code risks while embedding security into pipelines.



Achieve alignment with strict regulatory and industry standards.



Assess and remediate cloud environments with Microsoft's security tools.



Establish enduring security guardrails through policy-as-code and best practices.

Our process

Assess

Assess current tooling and processes, including existing maturity level and gaps against industry benchmarks and best practices.

Design

Develop an outlined plan to address high-priority gaps and confirm target environments for remediation.

Implement and remediate

Deploy the agreed solution to address platform security gaps, pilot priority remediation, then roll out full-scale uplift.

Customer success story

An Australian retail bank partnered with Arinco to uplift and secure its cloud foundations by aligning Azure environments to Microsoft's Cloud Adoption Framework and embedding security guardrails as code. Arinco modernised the organisation's network architecture with vWAN and PaaS firewalls, implemented a GitHub Enterprise DevSecOps platform with advanced security scanning, and upskilled internal teams in modern engineering practices, creating a scalable, secure and well-governed platform ready for future growth.

Deliverables



Platform security assessment report and maturity gap analysis.



Target-state design and prioritised remediation roadmap.



DevSecOps pipeline integration with vulnerability remediation.



Policy-as-code security guardrails applied consistently across environments.



Cloud security posture uplift using Microsoft Defender and security management tools.