AIG CYBER LOSS PREVENTION PROGRAM

COMPREHENSIVE VULNERABILITY MANAGEMENT SUITE

TECHGUARD SECURITY®

AIG is committed to helping its policyholders reduce cyber risk before a claim ever occurs. As part of that commitment, AIG provides TechGuard Security's vulnerability management suite as a value-added service to insureds — at no additional cost. By proactively identifying and closing security gaps across your insureds' networks, cloud environments, and web applications, AIG strengthens its book of business while delivering measurable protection that sets its policies apart in a competitive market.

CHOOSE ONE OF THE FOLLOWING

	VULNERABILITY SCAN	OR	CLOUD SCAN	OR	WEB APPLICATION SCAN
SCANS FOR	Network devices, servers, endpoints, and OS-level vulnerabilities across your external infrastructure		Misconfigurations, exposed resources, and compliance gaps in AWS, Azure, or GCP environments		OWASP Top 10 threats: SQL injection, XSS, broken auth, and business logic flaws in web apps
TARGET	Network infrastructure		Cloud accounts, services & configurations		Web applications & APIs
FREQUENCY	Annual with a 90-day rescan		Annual with a 90-day rescan		Annual with a 90-day rescan
KEY OUTPUT	CVE-mapped risk scores, patch prioritization, executive dashboard		CIS Benchmark compliance, exposed asset inventory, IAM risk report		CVE-mapped risk scores, patch prioritization, executive dashboard

Vulnerability (VA) Scan

Know Every Weak Point on Your Network

The Problem VA Scan Solves

Attackers scan enterprise networks constantly. Unpatched servers, misconfigured firewalls, and outdated software are open doors. Without regular VA scanning, AIG won't know these doors exist until it's too late.

- Full inventory of all network-connected assets
- CVE severity scoring with CVSS ratings
- Prioritized remediation roadmap by risk level
- Compliance alignment (PCI DSS, SOX, NIST)
- Trend reporting to prove risk reduction over time

Reduce attack surface exposure across thousands of network endpoints

Cloud Configuration Scan

Secure Your Cloud Before It Becomes A Liability

The Problem Cloud Scan Solves

Cloud misconfigurations are the #1 cause of data breaches in financial services. An overly permissive S3 bucket, an exposed storage account, or a misconfigured IAM role can expose customer PII and trigger regulatory penalties overnight.

- Point in time scan
- Misconfiguration detection across all cloud services
- Public exposure identification before attackers find it
- IAM privilege analysis and overpermissioning alerts
- CIS Benchmark & NYDFS/SOC 2 alignment reporting
- Offered for Azure, Google Cloud, AWS, and M365
- Generated reports for specific compliance standards

Eliminate the #1 source of cloud data breach risk

Web Application Scan

Protect the Applications Your Customers Trust

The Problem Web App Scan Solves

Customer portals, claims systems, and partner APIs are prime targets. A single SQL injection or authentication bypass in a web app can give attackers direct access to policyholder data, financial systems, and internal networks.

- Full OWASP Top 10 dynamic application testing (DAST)
- API security scanning (REST, SOAP)
- Business logic flaw detection unique to insurance workflows
- Developer ready remediation guidance with proof-of-concept
- Identify potentially exposed sensitive content

Secure the customer-facing applications that carry your brand and compliance obligations

WHY TECHGUARD FOR AIG

FINANCIAL SERVICES EXPERTISE

Deep experience with insurance and financial sector compliance requirements (NYDFS, SOX, GLBA).

SPEED TO VALUE

First scan results delivered within 48 hours. No lengthy deployment.

BOARD-READY REPORTING

Executive summaries, risk trend graphs, and audit-ready reports your board and regulators expect.

Get started today by submitting the webform to TechGuard, and we will follow up with your onboarding steps.

TECHGUARD.COM/AIG

Please be sure to whitelist TechGuard's domain to ensure you receive all onboarding communications.