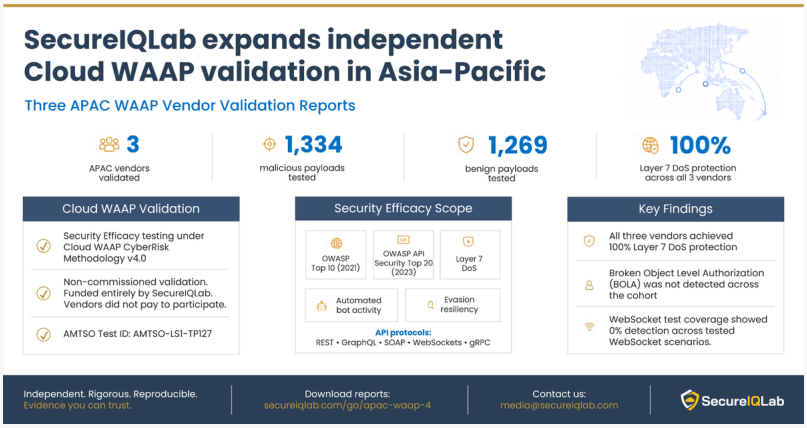
SecureIQLab Publishes Three APAC WAAP Validation Reports

Three Asia-Pacific WAAP vendors complete Security Efficacy validation under SecureIQLab's AMTSO-compliant Cloud WAAP CyberRisk Methodology v4.0.



SecureIQLab's APAC Cloud WAAP CyberRisk Validation program expansion in 2026

AUSTIN, TX, UNITED STATES, June 2, 2026 /EINPresswire.com/ -- SecureIQLab today published three Asia-Pacific Cloud WAAP CyberRisk Validation Reports, expanding the lab's independent WAAP validation program into the region. Each report was completed under the SecureIQLab Cloud WAAP CyberRisk Methodology v4.0, the same framework used in the 2025 global comparative of 15 enterprise WAAP solutions.

> Bringing our AMTSO-aligned methodology to regional vendors gives APAC security teams the same evidentiary baseline buyers in North America and Europe have relied on for years."
>
> *Bijay Limbu Senihang, Director of APAC Region, SecureIQLab*

Asia-Pacific is one of the fastest-growing markets for web application and API security. Regional enterprises increasingly require independent technical validation over vendor self-attestation. These reports deliver that.

Key Facts

- Three Asia-Pacific Cloud Web Application and API Protection (WAAP) vendors completed independent Security Efficacy validation
- All three reports use the same methodology that supported the 2025 global comparative evaluation of 15 enterprise WAAP solutions
- Registered with the Anti-Malware Testing Standards Organization (AMTSO) as Test ID AMTSO-LS1-TP127
- Aligned to OWASP Top 10 (2021) and OWASP API Security Top 10 (2023); each vendor evaluated against 1,334 malicious payloads and 1,269 benign payloads

- All three vendors achieved 100% Layer 7 DoS protection scores
- Non-commissioned validation, funded entirely by SecureIQLab; vendors provided product access for testing only

How does the APAC validation compare to the 2025 global comparative?

The three APAC Cloud WAAP CyberRisk Validation Reports apply the same methodology, testbed, and payload set used in the 2025 global comparative of 15 enterprise WAAP solutions. Scope covers the Security Efficacy pillar: OWASP Top 10 (2021) web application threats, OWASP API Security Top 10 (2023) API threats, Layer 7 denial-of-service, automated bot activity, and evasion resiliency. API testing covers five protocols: REST, GraphQL, SOAP, WebSockets, and gRPC. The 2025 global comparative additionally assessed Operational Efficiency and Compliance Validation; those pillars are outside the scope of the individual APAC reports. The full methodology documentation is available on the SecureIQLab methodology page.

SecureIQLab is an independent cloud security validation laboratory based in Austin, Texas. Unlike traditional analyst firms that rely on subjective surveys, SecureIQLab provides empirical, real-time security metrics based on testing that maps real-world e

Where did the APAC cohort show consistent strength?

All three vendors achieved 100% Layer 7 DDoS protection, mitigating every tested application-layer flood vector. The result aligns with patterns from the 2025 global comparative, where leading products also reached full Layer 7 coverage.

What about API security results?

API authorization enforcement was the cohort's most significant gap. None of the three products detected Broken Object Level Authorization, which is ranked as the #1 risk in the OWASP API Security Top 10 (2023). Vendor-specific OWASP API category breakdowns are published in each individual report at secureiqlab.com/apac-waap-4-0/.

"In Asia-Pacific, we work directly with regional vendors who have historically lacked access to

consistent, independent validation. Bringing our AMTSO-aligned methodology to regional vendors gives APAC security teams the same evidentiary baseline that buyers in North America and Europe have relied on for years," said Bijay Limbu Senihang, Director of APAC Region, SecureIQLab Nepal.

About the v4.0 methodology

SecureIQLab's Cloud WAAP CyberRisk Methodology v4.0 is registered with AMTSO as Test ID AMTSO-LS1-TP127. It aligns with OWASP Top 10 (2021), OWASP API Security Top 10 (2023), and CISA Secure by Design principles. All three APAC validations were non-commissioned and funded entirely by SecureIQLab. Vendors did not pay to participate. Vendors did not influence the validation process. Vendors could not prevent publication of results. The AMTSO attestation is signed by David Ellis, who serves on the AMTSO Board of Directors.

The three individual APAC reports are available at secureiqlab.com/apac-waap-4-0/.

SecureIQLab's Cloud WAAP CyberRisk Methodology v5.0 is currently in vendor testing, covering up to 25 enterprise WAAP solutions. Comparative results are expected in late 2026.

Data Integrity Disclosure. SecureIQLab does not endorse specific vendors. The findings in these reports represent objective data captured during the specified test period under controlled conditions. The results are presented as verified performance metrics. The results do not constitute a recommendation of any product. SecureIQLab disclaims all warranties regarding the application of this data to unique user environments.

Frequently Asked Questions

Q: How does this validation differ from a vendor's own product testing?
A: SecureIQLab designs the methodology, selects the payload set, and runs all assessments without vendor influence. Vendors do not pay to participate. The methodology is registered with AMTSO, which requires transparency in payload selection, scoring, and dispute resolution.

Q: What does the AMTSO-LS1-TP127 designation mean?
A: AMTSO-LS1-TP127 is the AMTSO Test ID assigned to SecureIQLab's Cloud WAAP CyberRisk Methodology v4.0. The designation confirms the methodology has been reviewed against AMTSO's testing protocol standard for reproducibility, payload disclosure, and vendor-dispute procedures.

Q: What is SecureIQLab's APAC footprint?
A: SecureIQLab's APAC office opened in 2025 in Kathmandu, Nepal. The office supports validation logistics, regional vendor coordination, and direct engagement with APAC enterprise security teams. The office is led by Bijay Limbu Senihang, the first cybersecurity auditor and penetration tester from Nepal.

Q: When will the Cloud WAAP CyberRisk Methodology v5.0 results be published?
A: The v5.0 cohort covers up to 25 enterprise WAAP solutions and is currently in vendor testing. Comparative results are expected in late 2026. Individual vendor reports may publish ahead of the comparative on a per-vendor basis. The full v5.0 methodology and vendor categorization is available at the SecureIQLab methodology page.

About SecureIQLab

SecureIQLab is an independent cloud security validation laboratory based in Austin, Texas. SecureIQLab provides empirical, real-time security metrics based on testing that maps real-world enterprise use cases to specific business challenges. SecureIQLab is a principal member of Mplify (formerly MEF). The lab is a member of the Anti-Malware Testing Standards Organization (AMTSO), AVAR, and NetSecOPEN.

SecureIQLab Communications
SecureIQLab
+1 512-575-3457
email us here