

SecureQLab Opens Post-Quantum Validation of Cloud-Native Firewalls

Independent AMTSO-registered methodology validates cloud-native firewalls against NIST post-quantum standards as CISA procurement mandate takes effect.

AUSTIN, TX, UNITED STATES, May 6, 2026 /EINPresswire.com/ -- [SecureQLab](#) today published the first independent cloud-native firewall validation methodology to include NIST post-quantum cryptography standards.

Key facts:

- First independent cloud-native firewall (CNFW) validation methodology to include NIST post-quantum cryptography (PQC) standards: ML-DSA-65/87 for digital signatures, ML-KEM-768/1024 for key establishment, and SHA-384/512 for integrity.

“

Every cloud-native firewall vendor will soon claim quantum-safe posture. Enterprises and federal agencies need a way to verify those claims against a repeatable, vendor-neutral benchmark.”

David Ellis, VP of Research, SecureQLab

security.

QUANTUM THREAT TIMELINE
The attack curve has fallen **1,000x** in 13 years.

— FIRST INDEPENDENT PQC CNFW VALIDATION —

Qubits required to break RSA-2048 dropped from ~1 billion (2012) to ~1 million (2025).
Independent post-quantum validation can't wait for the rest.

Year	Qubits required to break RSA-2048
2012	~1 billion (10 ⁹)
2025	~1 million (10 ⁶)

FS Labs, State of Post-Quantum Cryptography on the Web (June 2025)

19-30%+ Probability of an RSA-2048 break within 10 years

32 Leading quantum-computing experts surveyed

Dec. 2024 Global Risk Institute, Quantum Threat Timeline Report

SecureQLab CONTACT US: media@secureqlab.com
DOWNLOAD THE FULL METHODOLOGY: secureqlab.com/go/pr-cnfw-methodology

SecureQLab is a research and advisory firm focused on cybersecurity validation for the cloud era. © 2026 SecureQLab. All rights reserved.

The qubits required to break RSA-2048 have fallen 1,000x in 13 years. SecureQLab has completed the first independent post-quantum cryptography validation of a Cloud Native Firewall. Key data points: - ~1 billion qubits required in 2012; ~1 million requi

- Registered with the [Anti-Malware Testing Standards Organization \(AMTSO\)](#) as Test ID AMTSO-LS1-TP195.

- Up to 16 vendors evaluated across three pillars (Security Efficacy, Operational Efficiency, Compliance Validation), with compliance mapping to GDPR, HIPAA, PCI DSS, NIST 800-171, SOC 2, ISO/IEC 27001:2022, and Secure by Design/Default.

- Validation spans multi-cloud (AWS, Azure, GCP), Kubernetes (EKS, AKS, GKE), serverless, GenAI inference endpoints, and Model Context Protocol (MCP) server

- Non-commissioned validation begins June 2026; results published by end of October 2026.

The methodology, [Cloud Native Firewall CyberRisk Validation v1.0](#), is registered with the Anti-Malware Testing Standards Organization (AMTSO) as Test ID AMTSO-LS1-TP195. It arrives in the same window as two landmark federal PQC mandates.

The Cybersecurity and Infrastructure Security Agency (CISA) published a January 2026 list of product categories for which agencies must acquire only PQC-enabled technology. Federal agencies were also due to submit comprehensive PQC transition plans under National Security Memorandum 10 (NSM-10) and OMB Memorandum M-23-02 by the end of April 2026.

The urgency is backed by data. According to the Trusted Computing Group's 2025 State of PQC Readiness survey, 91% of organizations have no PQC roadmap in place. Cloud Security Alliance Labs reports that only 5% of organizations have deployed quantum-safe encryption, while 81% say their cryptographic libraries and hardware security modules are not ready for migration.

Meanwhile, the attack curve is tightening. The estimated qubits required to break RSA-2048 has fallen from roughly 1 billion in 2012 to approximately 1 million as of May 2025, per F5 Labs. The Global Risk Institute's 2024 Quantum Threat Timeline Report draws on 32 leading experts. It places the probability of a quantum computer capable of breaking RSA-2048 within 10 years at 19% to more than 30%, depending on how expert opinion is weighted.

“Every cloud-native firewall vendor will soon claim quantum-safe posture. Enterprises and

POST-QUANTUM VALIDATION OF CLOUD-NATIVE FIREWALLS
Up to 16 vendors | 3 pillars | NIST PQC standards
FIRST INDEPENDENT PQC CNFW VALIDATION

REGULATORY TIMELINE

JAN 2026	APR 2026	MAY 2026	JAN 2027	2033
CISA publishes PQC product-category list	Federal agency PQC transition plans due (NSM-10, OMB M-23-02)	SecureQLab CNFW methodology v1.0 published	NSA CISA 2.0 applies to new NIS acquisitions	Full-National Security System PQC compliance deadline

THE READINESS GAP

91% of organizations have NO PQC roadmap Trusted Computing Group, 2025	5% have deployed quantum-safe encryption Cloud Security Alliance Labs, 2026	81% say crypto libraries and HSMs are not migration-ready Cloud Security Alliance Labs, 2026
---	--	---

THREE-PILLAR FRAMEWORK

- SECURITY EFFICACY**
 - NIST PQC: Mc-DSA, Mc-KEM, SHA-384/512
 - MITRE ATT&CK: Cloud Matrix
 - GenAI + MCP server security
- OPERATIONAL EFFICIENCY**
 - Multi-cloud: AWS, Azure, GCP
 - Kubernetes: EKS, AKS, GKE
 - IoT deployment + scalability
- COMPLIANCE VALIDATION**
 - GDPR, HIPAA, PCI DSS
 - NIST 800-171, SOC-2, ISO 27001:2022
 - Secure by Design/Default

Why cloud-native firewalls require a separate methodology
Cloud-native firewalls embed in the cloud control plane, enforce policy via API across Kubernetes clusters, inspect east-west container traffic, and must now also prove post-quantum cryptographic support. Traditional firewall methodologies cannot evaluate these mechanisms.

Non-commissioned validation begins June 2026; results expected to publish by the end of October 2026.

SecureQLab | CONTACT US: media@secureqlab.com | DOWNLOAD THE FULL METHODOLOGY: secureqlab.com/go/pr-cnfw-methodology | SecureQLab is a research and advisory firm focused on cybersecurity validation for the cloud era. © 2026 SecureQLab. All rights reserved.

Post-Quantum Validation of Cloud-Native Firewalls
FIRST INDEPENDENT PQC CNFW VALIDATION

WHAT'S NEW IN THIS METHODOLOGY

- PQC STANDARDS VALIDATION**
 - Mc-DSA (digital signatures)
 - Mc-KEM (key establishment)
 - SHA-384/512 (integrity)
- GENAI & MCP SECURITY**
 - Inference endpoint protection
 - MCP access control
 - tool-call data exfiltration, prompt-injection hijacking
- MULTI-CLOUD ENFORCEMENT**
 - AWS, Azure, GCP
 - Kubernetes (EKS, AKS, GKE)
 - Serverless runtimes
 - East-west traffic inspection

THREE-PILLAR FRAMEWORK

- SECURITY EFFICACY**
 - Validates threat detection and prevention, PQC implementation (Mc-DSA, Mc-KEM, SHA-384/512), and MCP server security across cloud network scenarios.
- OPERATIONAL EFFICIENCY**
 - Evaluates deployment, agility, policy management, scalability, incident response, and performance on live cloud workloads.
- COMPLIANCE VALIDATION**
 - Maps firewall capabilities to major regulatory and security compliance frameworks.

Why cloud-native firewalls require a separate methodology
Cloud-native firewalls embed in the cloud control plane, enforce policy via API across Kubernetes clusters, inspect east-west container traffic, and must now also prove post-quantum cryptographic support. Traditional firewall methodologies cannot evaluate these mechanisms.

Non-commissioned validation begins June 2026; results expected to publish by the end of October 2026.

SecureQLab | CONTACT US: media@secureqlab.com | DOWNLOAD THE FULL METHODOLOGY: secureqlab.com/go/pr-cnfw-methodology | SecureQLab is a research and advisory firm focused on cybersecurity validation for the cloud era. © 2026 SecureQLab. All rights reserved.

SecureQLab's first independent post-quantum validation methodology for cloud-native firewalls extends traditional firewall testing into PQC standards, GenAI and MCP server security, and multi-cloud enforcement. What's new in this methodology: - PQC stan

federal agencies need a way to verify those claims against a repeatable, vendor-neutral benchmark,” said David Ellis, VP of Research and Corporate Relations at SecureQLab. “Our methodology is the first to require empirical PQC evidence at the firewall layer, alongside GenAI workload security and multi-cloud enforcement, so security leaders can meet federal and enterprise mandates with reproducible evidence rather than vendor self-attestation.”

“Post-quantum readiness is about to become one of the most-claimed and hardest-to-verify properties in security. That's exactly where AMTSSO's transparency and reproducibility standards matter most. They give enterprises and regulators a shared baseline for separating real implementations from marketing. SecureQLab's CNFW methodology extending into PQC is a meaningful expansion of what independent validation can credibly cover,” said John Hawes, COO of the Anti-Malware Testing Standards Organization.

Cloud-native firewalls require a separate methodology because they are architecturally distinct from cloud-deployed firewalls. Existing firewall methodologies, including SecureQLab's own Advanced Cloud Firewall validation, measure VM-based appliances at VPC perimeters. Cloud-native firewalls embed in the cloud control plane, enforce policy via API across Kubernetes clusters, inspect east-west container traffic, and must now also prove quantum-safe cryptographic support. Traditional firewall methodologies cannot evaluate these mechanisms.

The methodology uses three pillars. Security Efficacy validates threat detection and prevention across scenarios mapped to the MITRE ATT&CK Cloud Matrix, STRIDE, OWASP Cloud-Native Guidelines, and the CSA Cloud Controls Matrix. Encryption validation covers all 22 TLS 1.2 cipher suites, three TLS 1.3 cipher suites, TLS session reuse, and NIST PQC standards ML-DSA, ML-KEM, and SHA-384/512 (NIST FIPS 203/204/205). GenAI workload validation covers inference endpoint protection and MCP server security, including access control, tool-call data exfiltration, and prompt-injection hijacking. Operational Efficiency evaluates IaC-driven deployment, policy



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

management, scalability, incident response, and performance across AWS, Azure, GCP, and Kubernetes environments. Compliance Validation maps firewall capabilities to GDPR, HIPAA, PCI DSS, NIST 800-171, SOC 2, ISO/IEC 27001:2022, and Secure by Design/Default.

The methodology's PQC coverage aligns with a sequence of federal milestones. CISA published product-category guidance in January 2026, and federal agencies were due to file transition plans by the end of April 2026. NSA Commercial National Security Algorithm (CNSA) 2.0 compliance applies to new National Security System acquisitions from January 2027, with full NSS compliance due by 2033. In the European Union, regulators increasingly treat quantum-vulnerable cryptography as failing the “state-of-the-art” standard under the Digital Operational Resilience Act (DORA) and the NIS2 Directive.

The non-commissioned study, funded entirely by SecureQLab, evaluates up to 16 CNFW vendors across managed cloud-provider firewall services and third-party containerized solutions. The full planned vendor list is published in the methodology document. Testing begins in June 2026, with individual and comparative reports published by the end of October 2026. The AMTSO attestation is signed by David Ellis, VP of Research and Corporate Relations.

The full methodology is available at <https://secureiqlab.com/go/pr-cnfw-methodology>. Vendors interested in participation details may contact SecureQLab directly.

Frequently asked questions about the methodology follow.

Q: What does post-quantum cryptography validation mean in this context?

A: The methodology verifies that a cloud-native firewall correctly implements NIST's standardized quantum-safe algorithms: ML-DSA-65 and ML-DSA-87 for digital signatures, ML-KEM-768 and ML-KEM-1024 for key establishment, and SHA-384/SHA-512 for integrity. Validation covers both standard and advanced security levels defined by NIST.

Q: Why now?

A: Federal agencies must submit PQC transition plans in April 2026, and CISA published the list of product categories where agencies must acquire only PQC-enabled technology in January 2026. Enterprise and government procurement teams need independent evidence that vendor PQC claims are real and interoperable, not self-attested.

Q: How are vendors scored?

A: The methodology scores each validation case on a 4-tier Prevention + Detection framework: Prevent and Detect (100%), Prevent No Detect (75%), Detect No Prevent (25%), and No Detect No Prevent (0%). Operational Efficiency and Compliance Validation use parallel 4-tier scales per category.

Q: Is this validation commissioned by any vendor?

A: No. This is a non-commissioned validation funded entirely by SecureQLab. Vendors do not

pay to participate, cannot influence the validation process, and cannot prevent publication of results.

Q: When will results be available?

A: Individual and comparative reports will be published by the end of October 2026. The methodology is available now at <https://secureiqlab.com/go/pr-cnfw-methodology>.

About SecureIQLab

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 enterprise use cases to specific business challenges. SecureIQLab is a principal member of Mplify (formerly MEF) and a member of the Anti-Malware Testing Standards Organization (AMTSO), AVAR, and NetSecOPEN.

SecureIQLab Communications

SecureIQLab

+1 512-575-3457

media@secureiqlab.com

Visit us on social media:

[LinkedIn](#)

[Bluesky](#)

[Instagram](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/910592097>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.