SKOCH GROUP
GROWTH | LIVELIHOODS | EQUITY
www.skoch.in

CASE STUDY # 140

JIO PLATFORMS LIMITED

JPL's Cyber Security Solution

Abstract

As digital networks become more complex and mission-critical, conventional cybersecurity architectures are increasingly inadequate for protecting telecom, cloud, enterprise and national digital infrastructure. Jio Platforms Ltd addressed this emerging risk through JPL's Cyber Security Solutions, a sovereign, quantum-safe cybersecurity suite designed to protect India's 5G standalone network, enterprise cloud infrastructure and critical communication systems versus present-day cyberattacks and upcoming quantum threats. The solution integrates Post-Quantum Cryptography, Quantum Random Number Generators, Jio Cloud Native Security Center, Unified Security Operations Center, Enterprise SASE Gateway, JioSafe and quantum-safe network protection into an end-to-end defence architecture. Operational from October 2024 and launched nationally in January 2025, the platform protects more than 228 million 5G users.

Introduction

JPL's Cyber Security Solutions were conceptualised in response to a changing threat landscape in which classical encryption, fragmented security tools and manual cyber operations are becoming insufficient. The project began on 1 October 2024, with the evaluation period running from 1 August 2025 to 28 November 2025. Jio Platforms positioned the initiative under Digital Transformation, Cybersecurity and Data Protection, with a focus on cybersecurity structures and protocol implementation.

The solution was designed for telecom-scale security. At the more specific outcome level, quantum-safe protection is extended to more than 228 million 5G users. The initiative integrates a Quantum-Safe 5G Core, an AI-powered Unified SOC, a Cloud Native Security Center, an Enterprise SASE Gateway, a Quantum Random Number Generator and JioSafe for secure communication.

The platform provides sovereign protection across signalling, authentication, subscriber data, enterprise cloud, edge workloads, remote access and critical sector communication. It is designed not as a single security product but as an integrated defence stack combining prevention, detection, response, encryption, policy enforcement and secure connectivity.

The Problem Statement

The central issue addressed by the project was the growing inadequacy of traditional cybersecurity tools in a telecom, cloud and AI-powered era. Distributed digital infrastructure now spans 5G core networks, edge clouds, enterprise applications, IoT devices, hybrid cloud workloads and remote users. This expansion increases the attack surface and makes siloed security systems ineffective.

A second and more strategic challenge was the emergence of quantum computing. Quantum computers have the potential to break classical encryption systems, creating serious risks for telecom networks, banking, defence, governance platforms, citizen data and national digital infrastructure. JPL recognised that delaying action would leave critical infrastructure exposed.

The third problem was functional scale. Existing SOC environments struggled to process and correlate trillions of logs in real time. Security teams also faced alert fatigue from false positives generated by cloud security scans, creating the risk that critical threats could be missed while analysts spent time on low-value alerts.

The fourth challenge was complexity across multi-cloud, hybrid, edge and containerised environments. Tracking assets, security configurations, vulnerabilities, compliance posture and malware exposure across such diverse environments created blind spots and conventional scanning tools were often unable to scale with dynamic cloud infrastructure.

The fifth problem was sovereignty. India required an indigenous cybersecurity framework to protect national networks and critical infrastructure without overdependence on foreign technologies. For Jio, this meant designing a security stack in line with national resilience, data localisation, regulatory assurance and future 6G readiness.

Strategic Vision

Jio Platforms approached cybersecurity as a basic requirement for India's digital future. The objective wasn't merely to protect enterprise systems, but to create a sovereign, future-proof, export-ready security framework for telecom, cloud, edge, enterprise and government ecosystems.

The strategic mandate was established in Q1 2024, when Jio leadership defined the need for a sovereign quantum-secure cybersecurity architecture. At this stage, the core pillars approved included PQC integration, Quantum-Safe 5G Core, Unified SOC, Cloud-Native Security Center and enterprise SASE. A key decision was taken to embed quantum-resistant cryptography directly into 5G standalone authentication flows.

The initiative also reflects JPL's larger technology leadership agenda. The organisation's patent portfolio covers 4,067 patents across 168 distinct products in mobility, home and enterprise sectors. Its IP portfolio includes 1,726 patents in core network, 696 in IP and transport, 570 in Jio Brain AI/ML, 386 in IoT and blockchain, 228 in OSS/BSS solutions, 64 in automation and 39 in 5G/6G radios. This IP base reinforces the project's positioning as an indigenous technology-led cybersecurity intervention.

Solutions Stack

The first layer of the solution is the Jio Cloud Native Security Center. It provides end-to-end threat management for cloud infrastructure, containers, edge applications, 5G core workloads and OSS/BSS platforms. It performs real-time security scans across MEC edge and cloud environments.

The CNSC performs automated vulnerability and malware scanning for containerised and cloud workloads. It processes and scores CVEs from more than 20 global sources covering more than 4.8 million CVEs. It also provides Cloud Security Posture Management that supports CIS, GDPR, HIPAA, PCI-DSS, NIST, SOC-2, NSA-CISA and other compliance frameworks, while detecting misconfigurations across AWS, Azure, GCP, Kubernetes and Linux.

The second layer is Jio SOC, a unified cybersecurity platform that integrates SOAR, SIEM and XDR capabilities. It collects telemetry from endpoints, cloud systems and applications; normalises logs and events; correlates suspicious patterns; automates predefined response playbooks; and generates compliance reports conforming to industry standards.

The third layer is Enterprise SASE Gateway. It integrates SD-WAN, Zero Trust Network Access and Secure Web Gateway capabilities to secure distributed environments, remote work, mobile connectivity and cloud adoption.

The fourth layer is Quantum Random Number Generation. Jio's QRNG generates unpredictable, true-random numbers with maximum entropy. Since conventional encryption systems depend on pseudo-random number generators that may be vulnerable to prediction, QRNG provides stronger foundations for future-safe networks. It regenerates random numbers during periodic authentication, protects signalling communication between devices and the network.

Implementation Journey

The implementation followed a phased and technically disciplined roadmap. In Q1 2024, JPL defined the strategic mandate and architecture blueprint. In Q2 2024, engineering teams built the indigenous PQC suite, QRNG and key-management layers and early prototypes of PQC-enhanced 5G authentication and signalling encryption were validated in controlled testbeds.

In Q3 2024, Unified SOC and CNSC architectures were completed. AI models for anomaly detection, threat scoring and automated incident response were integrated and log pipelines were optimised to handle more than one trillion logs per day.

In October 2024, cross-domain pilot testing began across select 5G core sites, cloud zones and enterprise networks. PQC authentication, SASE Gateway and quantum-safe communication through JioSafe were tested for interoperability with legacy and multi-vendor systems.

In January 2025, the Quantum-Safe Security Suite was officially launched and deployed across India's 5G standalone core, RAN interfaces, enterprise cloud and remote-access architectures. SASE and JioSafe adoption expanded across BFSI, government and critical sectors.

From Q1 to Q3 2025, the programme entered scaling, hardening and enterprise expansion. PQC deployment scaled to millions of subscribers. AI-based SOC automation reduced detection time by 65 percent and false positives by 40 percent. JioSafe adoption increased across defence, government and regulated industries.

Challenges During Implementation

The first major challenge was integrating PQC into a live 5G core without disrupting more than 228 million active users. This required extensive compatibility testing, phased rollout planning and careful validation throughout authentication and signalling flows.

The second challenge was multi-vendor interoperability. JPL had to ensure that PQC, QRNG and Zero Trust controls could operate across diverse network functions, enterprise systems, cloud environments and legacy infrastructure.

The third challenge was AI model training at telecom scale. The SOC had to process trillion-scale logs while sustaining accuracy, low latency and minimal false positives. This required high-quality telemetry pipelines and continuous model refinement.

The fourth challenge was policy homogeneity across cloud, edge and on-premise deployments. Enterprise environments differ substantially in architecture, compliance obligations and security maturity.

The fifth challenge was regulatory coordination. PQC standards are still evolving globally and the project required coordination with telecom compliance, sovereign cybersecurity requirements, 3GPP, NIST PQC and ETSI directions.

Highlights

- JPL's Cyber Security Solution is a quantum-safe cybersecurity framework that protects India's 5G networks, cloud infrastructure, enterprises and critical digital systems against current and future cyber threats.
- It protects 228+ million 5G users with quantum-safe authentication, secure communications and AI-powered threat detection.
- The platform processes over one trillion security logs daily, using AI-driven automation to enable anomaly detection, threat correlation and incident response.
- Key capabilities include vulnerability management across 4.8 million+ CVEs, cloud security posture management, Zero Trust access, secure remote connectivity and compliance monitoring.
- Outcomes include a 50 percent reduction in potential data breaches, 65 percent faster threat detection and response, 40 percent fewer false positives and 30 percent OPEX savings through security automation.

Outcomes

The project produced measurable cybersecurity, operational and strategic-level outcomes. Possible data breach incidents reduced by 50 percent due to PQC-enabled authentication and AI-led threat detection throughout cloud, core and edge environments.

Security threat detection and response became 65 percent faster through automated SOC workflows and real-time correlation of more than one trillion daily logs. False positives reduced by 40 percent, improving analyst productivity and accelerating incident triage.

Quantum-safe protection was extended to more than 228 million 5G users, securing signalling, access and communication streams through future-proof cryptography. The solution generated approximately 30 percent OPEX savings through SOC automation, centralised policy management and unified security orchestration. It additionally strengthened compliance readiness across critical infrastructure by supporting multiple regulatory and industry frameworks.

The platform has been designed for national-scale expansion across Jio networks, enterprise clients and government infrastructure. Its configurable, cloud-native deployment model allows replication across operators and critical infrastructure providers.

The framework is consistent with 3GPP, NIST PQC and ETSI, enabling global replication by telecom operators seeking sovereign, quantum-resistant cybersecurity without an architectural overhaul. It is also export-ready and can be licensed to international telcos, sovereign cloud ecosystems and critical infrastructure providers.

Future plans include SOC hyper automation, cross-operator threat-sharing networks, deeper IoT and OT security. The architecture is also designed to support 6G evolution, future PQC algorithms, quantum key distribution and sophisticated AI-driven threat intelligence.

Conclusion

JPL's Cyber Security Solutions represent a landmark intervention in India's cybersecurity evolution. Through integrating PQC, QRNG, AI-powered SOC, Cloud Native Security Center, Enterprise SASE, JioSafe and quantum-safe 5G protection, Jio Platforms possesses created a sovereign, future-ready defence architecture for telecom-scale digital infrastructure.

The initiative demonstrates that cybersecurity for the coming decade must be predictive, automated, quantum-resistant and sovereign. It also shows that national-scale digital infrastructure cannot be secured with fragmented tools; it requires integrated protection across the cloud, edge, core, enterprise, IoT and communication layers. Most importantly, the project establishes India's capability to create and deploy advanced cybersecurity system at global scale.

SKOCH GROUP

GROWTH | LIVELIHOODS | EQUITY

www.skoch.in

SKOCH

ECO-SYSTEM FOR GROWTH

e-Mail: info@skoch.in

www.skoch.in