

CUSTOMER SUCCESS STORY

Wibmo Achieves Seamless Compliance with SISA ProACT MXDR

About Wibmo

Wibmo is a payments technology company and an industry leader in payment security, digital payments, and financial services. Its solutions are driving growth for Banks, Fintechs, and Businesses. Wibmo, a subsidiary of PayU, plays a crucial role in Naspers' strategy to secure digital payments across its online retail ventures. This integration enhances Naspers' capabilities in providing secure and seamless payment solutions, reinforcing its commitment to digital financial services.

The Business Requirement

As a leader in digital payment solutions, Wibmo handles critical and sensitive customer data globally. Operating in a highly regulated industry, the organization must adhere to stringent compliance requirements and maintain rigorous security standards.

Wibmo recognized that compliance is not just a necessity but a strategic enabler for growth and expansion. Regulatory frameworks such as PCI DSS, ISO 27001, RBI guidelines, SOC 2, and GDPR demand comprehensive oversight, with a particular focus on log monitoring and threat detection—key pillars of organizational security.

While leveraging SISA's ProACT MXDR, an advanced Managed Extended Detection and Response (MXDR) solution powered by AI and ML, Wibmo achieved proactive threat detection and response against evolving cyber threats. However, meeting the stringent scrutiny of compliance audits and maintaining effective security controls over time remained critical. To protect sensitive financial data, uphold customer trust, and address the demands of multi-framework compliance, Wibmo required a robust service framework with a strong emphasis on superior threat detection and compliance enablement.

The business requirement was twofold:

Supported Audits

- PCI DSS
- PCI 3DS
- PCI SSLC
- ISO 27001
- ISO 22301
- ISO 27701
- Reserve Bank of India
- RBI SAR (System Audit Report)
 - Pre-paid card instrument (PPI) audit
 - Data localization
 - Tokenization
- Bank Audits (Third-Party Audits for Fintechs and Payment Gateways/Aggregators)
- SOC 2 (Service Organization Control 2)
- GDPR



Streamline Compliance Adherence – Stay ahead of compliance requirements across multiple frameworks without overburdening operational security teams.



Enhance Security Posture – Ensure robust cybersecurity measures, continuous monitoring, reliable business continuity plans, timely incident responses, and detailed reporting, all while navigating limited team resources and mitigate the risk of non-compliance penalties.

Wibmo needed a solution that could extend beyond threat detection, evolving into a compliance partner capable of addressing regulatory requirements while seamlessly integrating into their existing operational workflows. With these goals in mind, Wibmo deepened its engagement with SISA, exploring how ProACT MXDR could deliver more than proactive security—it could serve as a cornerstone for both compliance and security excellence.

The Solution

ProACT MXDR emerged as an outcome-driven solution that not only delivers superior threat detection but also simplifies complex regulatory processes, ensuring seamless compliance. By streamlining security operations and enhancing oversight, it drives significant business value and measurable ROI, reinforcing compliance as a catalyst for growth and resilience.

Through joint brainstorming sessions and use case development, the teams worked together to identify Wibmo's unique audit needs and tailor the platform's capabilities accordingly. This collaborative approach ensured that ProACT MXDR not only addressed immediate security challenges but also supported Wibmo in meeting specific compliance requirements mandated by multiple regulatory frameworks.

ProACT MXDR's impact on Wibmo's compliance efforts was three-pronged:

1. Advanced Compliance Facilitation

Leveraging its unique combination of regulatory compliance features and deep sectoral experience, ProACT MXDR proved instrumental in facilitating adherence to multiple standards, including PCI DSS, ISO 27001, RBI, SOC 2, and GDPR. The platform's strategically designed workflows addressed key regulatory needs:



Compliance Evidence and Audit Readiness: ProACT MXDR ensured timely provision of compliance evidence, making audit processes seamless.



Continuous Monitoring and Early Detection: The platform supported real-time threat detection to meet continuous monitoring mandates, offering robust protection against emerging threats.



Incident Response and Risk Management: ProACT MXDR streamlined rapid incident response while helping manage vulnerabilities and risks, both critical for regulatory adherence.

2. Robust Governance Processes

SISA's governance framework complemented ProACT MXDR, providing periodic reports tailored for CXOs and stakeholders. These reports delivered actionable insights into Wibmo's compliance status and overall security performance. The strong governance model ensured that Wibmo always had access to the right information at the right time, strengthening its compliance and security posture.

3. Simplified Insights And Dashboards

ProACT MXDR's intuitive dashboards further simplified compliance management by offering real-time visibility into critical metrics. Customizable visualizations catered to industry-specific regulations, ensuring that sensitive data remained protected while empowering Wibmo with easy access to historical data, log availability, and audit reports. These dashboards made security monitoring and compliance efforts effortless, helping Wibmo navigate complex requirements with ease.

Through this integrated approach, ProACT MXDR was positioned to offer more than just a security solution for Wibmo—it emerged as a comprehensive compliance partner, enabling the company to meet its regulatory obligations while maintaining a strong security posture.

ProACT MXDR: Key Drivers For Compliance And Security

Ongoing
Compliance
Assurance



Proactive Threat
Management with
Compliance Alignment



Governance
and Strategic
Insights



Enhanced Data
Integrity and
Transparency



Evidence-Based
Compliance
Management



Streamlined
Incident Reporting
and Investigations



Standardized
Operations for
Compliance

Business Impact

The SISA ProACT MXDR team played a pivotal role in enabling Wibmo to exceed compliance requirements, maintaining a flawless record with zero Non-Conformities (NCs) or observations.

By integrating ProACT MXDR's capabilities with Wibmo's strategic goals, the partnership delivered a scalable compliance framework capable of adapting to evolving regulatory demands in the digital payments sector.

The ProACT MXDR platform delivered benefits across multiple aspects

 Unified log management and detailed reporting simplified audit preparation, reducing the time and effort required to demonstrate compliance across multiple regulatory standards.

 The platform's support for extended data preservation ensured compliance with long-term regulatory requirements while its hybrid hosting options provided flexibility to meet diverse regulatory needs, including data localization mandates.

 In addition swift identification, containment, and mitigation of threats, combined with detailed forensic support, allowed Wibmo to meet strict regulatory reporting timelines and enhance incident response capabilities.

Accountability was reinforced through active participation in auditor Q&A sessions, where the SISA team showcased the tool's evidence and methodologies, fostering transparency and trust in compliance practices.

"Regulatory audits and compliance are critical to our business operations, and SISA's ProACT MXDR solution has been instrumental in ensuring that key controls required for audits like PCI DSS, RBI, and Bank Audits are consistently met. The ProACT solution streamlined the process by enabling data localization, ensuring the availability of logs and reports, and facilitating timely evidence sharing and appraisal for auditors. This made navigating complex regulatory requirements a seamless experience.

SISA's 18+ years of expertise, coupled with their structured approach and dependable support, ensured efficiency and reliability throughout the process, making them a valued and trusted partner in our compliance journey."



**Ravi
Bhushan**

CISO & DPO, Wibmo

SISA is a global forensics-driven cybersecurity solutions company, trusted by leading organizations for securing their businesses with robust preventive, detective, and corrective cybersecurity solutions. Our problem-first, human-centric approach helps businesses strengthen their cybersecurity posture. We apply the power of forensic intelligence and advanced technology to offer true security to 2,000+ customers in 40+ countries.

Compliance	Security Testing	Cyber Defense	Data Protection & Governance	Trainings & Certifications	Leading Tech Security
Payment Data Security • PCI DSS • PCI PIN • PCI 3DS • PCI P2PE • PCI S3 • PCI S-SLC • PCI CP (Card Production) • Facilitated PCI SAQ • Quarterly Health Check-ups • Central Bank Compliance • SWIFT Strategy and Risk • CCPA • GDPR • HIPAA • ISO • NIST • SOC 1 • SOC 2 • Cloud Security • HITRUST Unified Audits Managed Compliance	Application Security • Application Penetration Testing • CREST/CERT-in Approved Security Testing • API Security Testing • Secure Code Review Network Security • Vulnerability Assessment • Penetration Testing • Configuration Review • Firewall Rule Review • PCI ASV Scan Phishing Simulation Red Teaming Exercise • Layer Security Testing	Managed Extended Detection and Response Solution - SISA ProACT • 24x7 Monitoring • UEBA • Threat Intel • Advanced Threat Hunting • Breach & Attack Simulation • SOAR • Use-case Factory Digital Forensics and Incident Response • Incident Response / Compromise Assessment Services • Forensic Readiness Audit • Forensic and Incident Response Retainer Service • Payment Forensics Investigation • Internal Forensics Investigation • Ransomware Simulation	Data Discovery and Classification • PCI/PII/PHI Data Discovery • Data Classification in Endpoint (Windows, Linux) • Data Classification in O365, Metadata • Dynamic Masking, Redact, Truncation • Integration to DRM, DLP, SIEM Data Privacy Professional Services • Assessments (Unified Privacy Maturity, DPIA, 3rd Party Risk) • Data Inventory, Mapping and Process flow, RoPA • Data Privacy Framework - Policy, Notice, SoPs • Consent and Notice Management framework • Data Breach and Management • Principal management • Privacy by Design implementation guide • Define Data Retention Guidelines and processes • Technical/Organization measures • Privacy Training/Awareness	Payment Data Security Training and ANSI Accredited Certification • CPISI (2 Day Program) • CPISI (3 Day Program) • CPISI- Advanced (3 Day Program) • CPISI-D (Developers) • CPISI Hybrid (4 Weeks) Certification Program in Cybersecurity for AI – CSPAI • CSPAI • CSPAI - Developers Forensic Briefing Sessions for Senior Management	AI PRISM • AI PRISM LLM Vulnerability Scanner Solution • AI Risk Management and Governance Solution Framework • AI Compliance and Governance Consulting Service Hardware and IoT Security Testing • Firmware Security Testing • Hardware/Embedded Security Testing • IoT Network Security Testing • IoT/Embedded Application and Management Layer Security Testing • MPOC/ PCI PTS Quantum Security • Quantum Cryptographic Consulting • Quantum Security Risk Assessment • Quantum Security Standards Compliance

For more Information visit us at www.sisainfosec.com
or
write to us at contact@sisainfosec.com

Follow us

