Trellix

SOLUTION BRIEF

Qatar Information & Cyber Security Regulation for Payment Service Providers

Leverage Trellix® for cybersecurity resilience and compliance

Executive summary

This report provides a detailed mapping between Trellix cybersecurity solutions and the Qatar Central Bank (QCB) Information & Cyber Security Regulation for Payment Service Providers (PSPs). It aims to help PSPs demonstrate compliance by implementing Trellix technologies and services. The alignment focuses on regulatory domains such as governance, risk management, monitoring, incident response, and business continuity.

Overview of QCB Information & Cyber Security Regulation for PSPs

The QCB Information & Cyber Security Regulation for PSPs establishes a mandatory cybersecurity baseline for all payment institutions operating in Qatar. It enforces measures to safeguard payment data, secure IT systems, and manage cyber risks. The regulation requires PSPs to implement structured governance, risk management, and incident response practices in alignment with international standards (ISO 27001, NIST CSF, PCI DSS).

Core regulatory areas include:

- Governance and policy management
- Risk assessment and asset inventory
- Access control and identity management
- Data protection and encryption
- Security monitoring and incident response
- Vendor and third-party security
- Business continuity and disaster recovery

Overview of Trellix

Trellix is a global cybersecurity company formed through the merger of McAfee Enterprise and FireEye. It provides an integrated IT-OT security platform that protects against threats and data loss across endpoint, server, network, email, and cloud services. The Trellix platform, powered by Operational Threat Intelligence and Generative AI, helps organizations maintain resilience by disrupting sophisticated attacks, preventing data loss, accelerating detection, analysis, and response to threats in real time while maintaining compliance with regulatory frameworks.

Core components of the Trellix ecosystem include:

- **Trellix Helix:** Centralized log collection, real-time monitoring, threat intel and event correlation, AI-guided investigations, and playbook automation.
- **Trellix Endpoint Security (ENS), Trellix Endpoint Detection and Response (EDR), Trellix Application and Change Control (TACC):** Malware prevention for end-user device and server workloads, behavioural detection, compliance assessment, application allowlisting, and change control.
- **Trellix Data Loss Prevention (DLP)**: Data discovery, classification enforcement, and endpoint, network and cloud DLP policies, blocking sensitive data loss and exfiltration.
- **Trellix Email and Collaboration Security:** Inbound and outbound email scanning, phishing protection, attachment sandboxing, and DLP integration to prevent sensitive data leakage.
- **Trellix ePolicy Orchestrator (ePO):** Centralized management of security policies and compliance assessment reports across multiple types of end user devices, operational technology (OT) systems, and server workloads.
- **Trellix Network Detection and Response (NDR)**: Network-level threat prevention and detection of malicious lateral movement, and forensic analysis of network traffic.
- **Trellix Insights:** Real-time operational threat intelligence feeds, behavioral indicators, and threat actor reporting integrated into all products and delivered as a service.
- **Trellix Guardian Services:** Deep threat intelligence blended with agile cyber operations and AI-driven automation, cyber defenders deliver adaptive protection against evolving threats. Holistic services that span cover proactive threat mitigation, incident response, training, and program development.

Alignment between QCB regulation and Trellix portfolio

QCB Regulation Area	Trellix Solution(s)	Evidence / Audit Artifact	Implementation Notes
Governance & Policy Framework	ePolicy Orchestrator (ePO), Helix Governance, Risk and Compliance Program Development and Assessment	Information security policies, ePO configuration exports, Helix governance dashboards	Align policies with QCB clauses and automate enforcement through ePO.
Risk Assessment & Management	Helix, Insights Threat Intelligence Risk Management Program Development and Assessment	Risk dashboard reports, vulnerability context logs, threat scoring output	Integrate vulnerability scanner with Helix and for consolidated risk posture.
Asset Inventory	ePO Asset Discovery, Helix Inventory Cybersecurity Controls Configuration Review Vulnerability Assessments and Penetration Testing	Asset inventory reports, classification tags, discovery audit logs	Ensure continuous synchronization of asset databases across all business units.
Access Control & Identity Management	ENS, ePO, Helix UBA (User Behavior Analytics) Zero-Trust Architecture Assessment and Strategy and Roadmap Development	Access control matrix, privileged account audit logs, user behavior alerts	Integrate with Active Directory or SAML to provide identity context.
Data Protection & Encryption	Trellix DLP, Email Security, Helix Monitoring Data Security Assessment and Data Protection Program Development	DLP incident logs, encryption configuration records, alert history	Deploy DLP on endpoints and enforce encryption for payment data at rest and in transit.
Monitoring & Logging	Helix (SIEM/XDR), ePO, NDR Security Assessments SOC Maturity Assessment Threat Hunting	Event correlation reports, alert summary, log retention policy	Centralize all logs in Helix and configure 12-month retention in accordance with QCB.

Alignment between QCB regulation and Trellix portfolio (cont.)

QCB Regulation Area	Trellix Solution(s)	Evidence / Audit Artifact	Implementation Notes
Incident Response & Reporting	Helix (Hyperautomation), EDR, Threat Intelligence Incident Response Retainer and Readiness Workshop Tabletop Exercise	Incident playbooks, response reports, notification records	Define incident classification and establish QCB notification procedures
Third-Party Security	Helix Integrations, ePO Compliance Policies Third-Party Risk Assessment	Vendor security review reports, connection monitoring logs	Maintain vendor register with periodic security evaluation and SIEM integration.
Business Continuity & Disaster Recovery	Helix Automation, ePO Backups Ransomware Resiliency Assessment	BCP/DR test results, recovery logs, restoration time reports	Conduct annual DR drills and ensure configuration backups in multiple locations.
Awareness & Training	Helix Reporting, Email Security Simulation Insights Malware Analysis Fundamental Training Digital Forensics and Incident Response Fundamental Training Threat Hunting Fundamental Training	Training logs, phishing test reports, awareness metrics	Run quarterly awareness campaigns focused on payment fraud and phishing.

Evidence and audit documentation

To demonstrate ongoing compliance with QCB's cyber regulation, PSPs should maintain a structured evidence repository containing technical and procedural artifacts. These records support both internal reviews and QCB audits.

Recommended evidence includes:

- Approved cybersecurity policies and risk assessments
- ePO policy snapshots and Helix playbook exports
- Incident response reports and escalation logs
- Penetration testing and vulnerability management results
- Business continuity and recovery testing documentation
- Vendor security attestations and data sharing agreements

Recommendations

1. Establish centralized management using Trellix ePO for all endpoints and servers. Leverage Policy Auditor for continuous compliance assessments and reports.
2. Integrate Trellix Helix as the unified SIEM/XDR for real-time monitoring and response.
3. Deploy DLP and Email Security to prevent unauthorized data transfers.
4. Implement Endpoint Detection and Response (EDR) capabilities to identify and contain threats.
5. Ensure long-term log retention and regular incident reporting in accordance with QCB requirements.
6. Conduct regular testing (vulnerability scans, DR drills, phishing simulations) and maintain records.
7. Implement regular training and phishing simulation programs.
8. Review and update incident response plans quarterly.

Conclusion

Trellix provides PSPs with a robust, integrated cybersecurity framework that aligns closely with the Qatar Central Bank's Information & Cyber Security Regulation. By leveraging Trellix's Helix, ePO, EDR, NDR, and DLP capabilities, PSPs can achieve proactive protection, streamlined compliance reporting, and enhanced cyber resilience. Trellix's integrated ecosystem of tools supports continuous protection, monitoring, and incident response across digital assets, ensuring both regulatory compliance and operational assurance.

For more information, please refer to www.trellix.com.