Trellix

SOLUTION BRIEF

Qatar National Information Assurance Standard (NIAS)

Leverage Trellix® for cybersecurity resilience and compliance

What is the Qatar National Information Assurance Standard (NIAS)?

The Qatar National Information Assurance Standard (NIAS)—also referred to as the National Information Assurance Standard (NIA Standard)—is a regulatory framework developed by the National Cyber Security Agency (NCSA) to ensure that all entities handling national or critical information assets follow a consistent and comprehensive set of cybersecurity practices.

Version 2.1 of NIAS (released in 2023) defines technical and administrative controls covering governance, risk management, asset protection, incident response, and operational security. The standard applies to all Qatari government entities, semi-governmental organizations, and private sector operators of critical infrastructure. It aligns with international standards such as ISO 27001, NIST, and CIS Controls, while incorporating national requirements for data sovereignty and the protection of classified information.

How to approach NIAS compliance with Trellix

This document maps the Trellix security portfolio and capabilities (Helix, Endpoint Security, DLP, Email Security, ePO, Network Detection, etc.) to the control domains and requirements of the Qatar NIAS (NIA Standard) v2.1. The goal is to provide a clear, implementable set of recommendations showing how Trellix can help an organization meet NIAS requirements and what evidence artifacts to collect for certification or audits.

Scope and assumptions

- **Scope:** This map is intended for government entities and critical infrastructure operators in Qatar seeking alignment with NIAS v2.1.
- **Assumptions:** The baseline NIAS v2.1 control objectives apply (May 2023 release). This document maps technical and operational controls only — governance/policy artifacts (e.g., policies, contracts) must be produced by the organization.

This is a portfolio-to-control mapping; additional administrative and physical controls are likely required per NIAS.

Approach

1. Identify NIAS domain and control objective.
2. Map Trellix portfolio/capability that supports the control.
3. Provide implementation notes and evidence artifacts to demonstrate compliance.

Trellix products and solutions for NIAS compliance

At a high level, Trellix products and solutions for NIAS compliance 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 devices 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, to block 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, 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 proactive threat mitigation, incident response, training, and program development.

Mapping Trellix portfolio and capabilities to select NIAS domains

NIAS v2.1 groups controls across governance & processes and security controls. Below are primary domains mapped to Trellix capabilities with suggested evidence.

Asset and inventory management

- **NIAS objective:** Maintain an accurate inventory of information assets and their owners.
- **Trellix mapping:** ePO (Policy Auditor and Application Control modules) as well as Trellix Endpoint agents for software and hardware. Trellix Guardians Advisory Services offers vulnerability assessments and penetration testing.
- **Implementation notes:** Deploy Trellix agents across endpoints and configure automated inventory reporting with Policy Auditor and Application Control to ePO. Leverage third-party tools for unmanaged asset discovery and incorporate into Helix. Engage Trellix Guardians Advisory Services for vulnerability assessment and penetration testing.
- **Evidence artifacts:** Asset inventory export, agent deployment spreadsheet, ePO inventory reports, reconciliation logs and risk register.

Configuration and hardening / product security

- **NIAS objective**: Enforce secure baseline configuration and product lifecycle management.
- **Trellix mapping:** ePO policy enforcement (configuration baselines), Trellix Endpoint Security Application Control, DLP configuration management. Trellix Guardians Advisory Services, such as cybersecurity controls and configuration review.
- **Implementation notes:** Define hardened baselines in ePO, push policies, verify continuous compliance via Policy Auditor module and ePO reports. Engage Trellix Guardians Advisory Services for cybersecurity control configuration review.
- **Evidence artifacts:** ePO baseline policy profile, compliance reports, change control records and hardening guidelines.

Identity, authentication and access control

- **NIAS objective:** Strong identification and authentication; least privilege access.
- **Trellix mapping:** Trellix Endpoint controls (Application Control, Privilege Elevation controls), integration with IAM for endpoint sign-in events into Helix, and policy enforcement via Trellix ePO. Trellix Guardians Advisory Services offers Zero-Trust Architecture Assessment and Strategy and Roadmap Development.
- **Implementation notes:** Integrate Trellix agents with AD/IdP logs forwarded to Helix for identity-based detection; use application control to limit privileged actions. Engage Trellix Guardians Advisory Services in Zero-Trust Architecture Assessment and Strategy and Roadmap Development.
- **Evidence artifacts:** Trellix Helix logs show authentication events, Trellix ePO applied policy shows least-privilege configs, access control exception records and Zero-Trust Architecture blueprint and strategy roadmap.

Network and gateway security

- **NIAS objective:** Protect network boundaries and gateways from threats.
- **Trellix mapping:** Email Security for mail gateways, network detection/inspection via Trellix NDR integrations and sandboxing for suspicious files. Trellix Guardians Advisory Services offers zero-trust architecture assessment and roadmap development.
- **Implementation notes:** Place Trellix Email Security in front of mail infrastructure; feed network telemetry and gateway logs into Helix for correlation. Engage Trellix Guardians Advisory Services in zero-trust architecture assessment and roadmap development.
- **Evidence artifacts:** Email gateway policy configs, sandbox analysis reports, Helix correlation alerts showing gateway detections, and zero-trust architecture blueprint and roadmap.

Data protection and data loss prevention

- **NIAS objective:** Prevent unauthorized disclosure or modification of sensitive data.
- **Trellix mapping:** Trellix DLP (discovery, endpoint control, network/email integration) and Trellix Database Security, Trellix Email Security and Trellix DLP integration for outbound email scanning; IVX+DLP integration for enterprise and cloud application scanning. Trellix Guardians Advisory Services such as Data Security Assessment and Data Protection Program Development.
- **Implementation notes:** Classify sensitive data per National Data Classification Policy; create DLP policies matching classifications; enforce blocking/quarantine for violations on email, collaboration, business and cloud apps. Engage Trellix Guardians Advisory Services in Data Security Assessment and Data Protection Program Development
- **Evidence artifacts:** ePO and DLP policy definitions, incident logs showing blocked data loss or exfiltration attempts, data discovery reports, data protection program.

Logging, monitoring, and security operations

- **NIAS objective:** Centralized logging, retention, detection and monitoring for anomalous activity.
- **Trellix mapping:** Trellix Helix ingests logs from endpoints, network devices, cloud; provide correlation, alerts, and SOC workflows. Trellix Guardians Advisory Services offers security assessments, SOC maturity assessment and threat hunting.
- **Implementation notes:** Configure log sources to forward to Helix with required retention; tune detection rules to NIAS baselines (priority levels). Trellix Guardians Advisory Services offers security assessments, SOC maturity assessment and threat hunting.
- **Evidence artifacts:** Log ingestion dashboard, retention policies, incident investigation reports, timelines, vulnerability findings, active and dormant indicators of compromise.

Incident response and forensics

- **NIAS objective:** Prepare, detect, respond to, and recover from security incidents with reporting.
- **Trellix mapping:** Helix provides investigation playbooks, automated containment (isolate endpoint, block IP, etc), EDR and telemetry for forensic timelines; Trellix services for incident response (IR) and intelligence support. Trellix Guardians Advisory Services offers incident response retainers, readiness workshops and tabletop exercises.
- **Implementation notes:** Implement automated playbooks in Trellix Hyperautomation for common incidents (ransomware, phishing), define containment thresholds. Engage Trellix Guardians Advisory Services for Incident Response Retainers, readiness workshops and tabletop exercises.
- **Evidence artifacts:** IR playbook definitions, post-incident reports, forensic artifacts,timelines, investigations, forensics, incident analysis and dry-run exercise for users, IT and management team.

Vulnerability management and patch management

- **NIAS objective:** Identify and remediate vulnerabilities in a timely manner.
- **Trellix mapping:** Trellix ePO and Policy Auditor reporting identify missing patches and vulnerable software. For prioritization, integrate with vulnerability scanners via Helix and insights Trellix Guardians Advisory Services offers vulnerability assessments and penetration testing.
- **Implementation notes:** Use ePO patch and compliance reports to complement the vulnerability management process and generate patch compliance reports. Engage Trellix Guardians Advisory Services for vulnerability assessments and penetration testing.
- **Evidence artifacts:** Patch compliance dashboards, vulnerability scan-to-remediation tickets, and risk register.

Third-party and outsourcing security

- **NIAS objective:** Ensure outsourced services maintain NIAS controls.
- **Trellix mapping:** For managed services, Trellix Helix and ePO logs alongside DLP can demonstrate control. Trellix Professional Services can provide attestation and SOC services. Trellix Guardians Advisory Services offers third-party risk assessments.
- **Implementation notes:** Include Trellix SOC/MSSP SLAs and security configs into third-party contracts. Request evidence exports for audits. Engage Trellix Guardians Advisory Services for third-party risk assessments.
- **Evidence artifacts:** SLAs, service acceptance reports, exported logs from third-party-managed systems and third-party risk register, and security posture improvement plan.

Secure software and product lifecycle

- **NIAS objective:** Ensure secure development and supply chain controls for products.
- **Trellix mapping:** Trellix product security posture (vendor-provided SBOM, secure update mechanisms) — include vendor attestations and patch policy documentation. Trellix Guardians Advisory Services offers application security assessments, source code review, threat modeling, plus architecture and configuration review.
- **Implementation notes:** Collect Trellix product security documentation and supplier security questionnaires as evidence for procured solutions. Trellix Guardians Advisory Services offers application security assessments, source code review, threat modeling, plus architecture and configuration review.
- **Evidence artifacts:** Vendor security datasheets, SBOMs, patch/update notifications, vulnerability findings, architecture improvement plan, identified threats, and configuration gaps.

Recommended evidence collection checklist for NIAS audits

In preparation for an NIAS audit, we recommend preparing the following:

1. ePO inventory export showing 100% agent coverage.
2. Baseline configuration profiles and compliance reports from ePO Policy Auditor.
3. EDR and NDR forensic log collection.
4. Helix log ingestion proof and retention settings.
5. DLP policy definitions and incident logs showing enforcement.
6. Email Security logs and sandbox reports.
7. Incident response playbooks and a sample incident timeline from Hyperautomation.
8. Vendor product security and update policy statements.
9. Penetration testing and vulnerability management results.
10. Business continuity and recovery testing documentation.

Suggested implementation roadmap

We recommend taking a four-phase approach to implementation:

1. **Preparation:** Map current state, classify data, identify critical assets.
2. **Foundation coverage**: Deploy Trellix agents to endpoints, enable ePO inventory, configure Email Security, Endpoint Security, and DLP basic policies.
3. **Operational SecOps:** Enable Helix ingestion from endpoints, networks, email gateways, and cloud. Tune detections and create playbooks.
4. **Mature SecOps and resilience:** Incorporate operational threat intelligence. Automate containment, integrate vulnerability scanning, run tabletop exercises and collect audit evidence.

Considerations and next steps

This document maps Trellix technical capabilities to NIAS controls but is not a substitute for formal NIAS compliance assessment.

Recommended next steps include: producing a control-by-control traceability matrix (CBTM) listing each NIAS control ID, required baseline (P1/P2/P3), mapped Trellix artifact, implementation status, and evidence file reference.

Trellix Solution Alignment Summary Table

Category	Trellix Product	Description	NIAS Controls Number
Asset & Inventory	**ePolicy Orchestrator (ePO)**	Centralized inventory of endpoints, software, and compliance state	2.1.1, 2.1.2
Endpoint Security	**ENS / EDR**	Advanced malware protection, behavioral analytics, app control	4.2.3, 4.3.1, 4.3.2
Data Protection	**DLP**	Detects and prevents data exfiltration; integrates with Email Security	5.2.1, 5.2.3
Email Security	**Email Security**	Protects mail gateways against spam, phishing, and malware	4.4.1, 4.4.3
Threat Detection	**Helix**	Correlation, analytics, incident investigation, and threat hunting	61.1, 6.2.1, 6.3.1

Trellix Solution Alignment Summary Table (cont.)

Category	Trellix Product	Description	NIAS Controls Number
Network Security	**NDR**	Detects anomalies and lateral movement within networks	4.1.1, 4.1.2
Patch & Vulnerability	**ePO + Helix Integration**	Tracks patch compliance and integrates with vuln scanners	7.1.1, 7.2.1
Incident Response	**Helix**	Automates containment and incident playbooks	8.1.1, 8.2.1, 8.3.1
Governance & Reporting	**ePO Reporting / Dashboards**	Centralized reporting for compliance evidence	9.1.1, 9.2.1

About NCSA (National Cyber Security Agency of Qatar)

The National Cyber Security Agency (NCSA) of Qatar is the national authority responsible for securing Qatar's cyberspace and ensuring the resilience of critical information infrastructure. The NCSA develops, issues, and enforces the National Information Assurance (NIA) policies and standards that guide all government and critical infrastructure organizations in implementing effective cybersecurity controls.

About Trellix

Trellix is a global company redefining the future of cybersecurity. The company's comprehensive, open, and native cybersecurity platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through artificial intelligence, automation, and analytics to empower over 50,000 business and government customers with responsibly architected security. More at https://trellix.com.

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