Nasdaq Boardvantage® Cloud Azure Security

Nasdaq Boardvantage incorporates end-to-end security features for governance and workflow management controlled from a central platform. Additionally, Client Uploaded Content is hosted in the Microsoft Azure ("Azure") environment protected by multiple layers of security, including application security, infrastructure security, process security, physical security, and personnel security.

Nasdaq Boardvantage Service Modules

- The Nasdaq Boardvantage service ("Nasdaq Boardvantage") has been designed with multiple layers of defense to protect the confidentiality, integrity, and availability of documents and materials which the client uploads to the Nasdaq Boardvantage service ("Client Uploaded Content") and client authentication data ("Client Authentication Data"), (together, the "Client Data").
- Nasdaq Boardvantage consists of the service application infrastructure hosting Client Uploaded Content (the "Service Application Infrastructure") and the authentication module verifying and processing Client Authentication Data for authentication purposes ("Authentication Module").

Industry Certifications

SOC 2 and ISO 27001 Certifications

- Nasdaq Boardvantage is SOC 2 certified and the Information Security Management System (ISMS) that governs the information assets, business operations and physical locations for Nasdaq Boardvantage conforms to ISO 27001 requirements and is ISO 27001 certified. The reports and certification can be found in the Nasdaq Boardvantage Audit Portal, which may be made available upon request where appropriate confidentiality undertakings are in place.

Compliance Reports

- Azure provides clients a wide range of compliance reports, certifications, accreditations, and other third-party attestations via https://docs.microsoft.com/en-us/azure/compliance/.

Application Security

Penetration Tests are Performed on the Service Application Infrastructure

- Both internal and external penetration tests are performed on the Service Application Infrastructure.
- Internal penetration tests are performed periodically. Third party penetration tests are performed on the Service Application Infrastructure periodically.
- The most recent third party penetration test attestation letter can be found in the Nasdaq Boardvantage Audit Portal.

Product Development LifeCycle at Nasdaq

- Nasdaq's Information Security Department has a role in the Product Development LifeCycle for both web and mobile applications.
- Prior to software changes, code scans are performed in accordance with Nasdaq's internal Information Security Scanning Guidelines.
- Critical and high-risk vulnerabilities are remediated, as appropriate, before code updates are released to production web site and/or mobile applications.

Encryption

- Transport Layer Security (TLS) v1.2 protocol is used within Nasdaq Boardvantage to encrypt Client Uploaded Content in transit.
- Client Uploaded Content is encrypted at rest with AES-256 encryption.

Control, Auditing and Tracking

- Built–in password and user access policies.
- Unique login per user.
- Customizable time out feature.
- Single Sign-On.
- Passkey support enables users to sign in without entering a username or password. Passkeys offer significant advantages, including stronger security and a smoother, more seamless user experience.
- Support for multi-factor authentication. The application enables administrators to manage user accounts, delegate rights, adjust customizable account settings to determine access rights, and adjust other user permissions and parameters.
- The application is designed to enable administrators to generate audit reports or alert notifications showing detail such as sessions, active/inactive users and password changes. This provides intelligence and visibility around user login activity, document management and alert notifications.

Mobile Device Security

- The Nasdaq Boardvantage mobile application is designed to enable administrators to permanently render Client Uploaded Content within the mobile application inaccessible in the case a device is declared lost or stolen.
- Transmissions to/from the mobile application are encrypted using Transport Layer Security (TLS) v1.2 + protocol.
- Client Uploaded Content is stored using AES-256 encryption.

Infrastructure Security

Azure Data Centers for the Service Application Infrastructure

- Service Application Infrastructure is hosted on servers housed in Azure cloud data centers located in the United States, Europe, Australia, United Arab Emirates, and Canada (coming soon) — depending on client's choice of location.
- Azure provides information on its physical security program via https://docs.microsoft.com/en-us/azure/security/fundamentals/physical-security.

Data Centers for N3A

- Client Authentication Data will be primarily hosted by a third party data center provider within the United States which is SSAE-18 audited.

Global 24/7 Security Operations Team

- The Nasdaq Global Security Operations Center monitors layers of security events related to the Nasdaq Boardvantage service environment and its supporting infrastructure.

Network Firewalls

- For Information on Azure firewalls and Azure network security, please refer to the Azure network security overview via https://docs.microsoft.com/en-us/azure/security/fundamentals/network-overview.

Network Access Controls

- Controls are in place for corporate internally managed networks.
- Nasdaq's Information Security Department deploys strict controls around production network access, including multi-factor authentication.

Web Application Firewalls (WAF)

- WAFs are deployed in blocking mode protecting the Service Application Infrastructure.

Network Segmentation

- VLAN and physical segmentation.

Personnel Security

Code of Ethics

- Nasdaq's company policy is that each employee must annually certify understanding of and compliance with Nasdaq Code of Ethics.

Security Awareness Training

- Yearly Security Awareness Training is required by policy for Nasdaq employees, as well as regular training sessions for software engineers regarding industry security best practices.

Process Security

Dedicated Information Security Team

- Nasdaq has a dedicated Information Security Department headed by the Chief Information Security Officer ("CISO") who reports to the Chief Information Officer within Nasdaq's centralized Global Technology organization.
- Nasdaq has a dedicated staff within the Information Security Department, which has verticals consisting of, Application Security, Governance and Compliance, Security Architecture, Security Engineering, Security Assurance and Threat Intelligence, Security Operations, and Program & Vulnerability Management and Data Protection. Additionally, the head of Corporate IT, the Head of Physical Security, and their supporting functions, report to the CISO.

Nasdaq Internal Audit

- Additional oversight of the Nasdaq Boardvantage service is provided by Nasdaq's Internal Audit Department, who plays a role in managing information security risks.

Disaster Recovery and Business Continuity

- In the event of a system or data center failure, the Service Application Infrastructure will be redirected to the appropriate zonal disaster recovery site if required. Disaster recovery plans have been established and are tested annually to ensure timely failovers between zones.
- Nasdaq has developed a comprehensive internal Business Continuity Plan that facilitates the continuation of client services and system support in the event of issues affecting standard operations, such as a force majeure event. The plan is kept current and tested on a periodic basis.
- In the event of a system or data center failure of the Authentication Module, Client Authentication Data will be redirected from the third party managed data center provider, to a third-party cloud provider, within the United States.

Backups

- Nasdaq Boardvantage is designed to perform regular backups of Client Uploaded Content to ensure continuity of service in the event of a system failure.
- Client Uploaded Content is backed up nightly to a server-based archival system.

Group Risk Management at Nasdaq

- Nasdaq Group Risk Management (GRM) is ultimately responsible for governing, developing, coordinating and controlling the Enterprise Risk Management process and providing relevant support to the line organization.
- GRM is responsible for the Nasdaq-wide risk reporting process and the aggregation of detailed risk information to a consolidated risk portfolio.
- GRM also provides consistent and continuous information on risk exposures and current risk trends to Nasdaq Executive Management and the Board of Directors.

Artificial Intelligence (AI) Security and Governance at Nasdaq

- Nasdaq has established an AI Governance Committee made up of senior technology and business leaders.
- The committee reviews and approves all new AI deployments and AI-related product initiatives.
- Nasdaq has introduced an AI Security Standard that defines the security requirements for any AI-related product or service. The AI Security Standard is available for client review in the Audit Portal.
- The standard is aligned to industry best-practice frameworks, including OWASP, ENISA, and NIST.
- Information specific to the Nasdaq Boardvabntage AI features is available in the Audit Portal.