nuwave

SECURITY QUESTIONNAIRE

Authentication

Office 365/Teams

User login to Applications - Mobile Web, Desktop App and Hardware phones
Login is via Username and Password for Office 365 managed by client/customer.

Administrator or Service Accounts
Tenant level login managed by client

IPilot

User Accounts- iPilot login in manage by Nuwave on a per request bases.

Direct Routing Service Account- Initially this account must be Global Administrator, roles may be reduced to User Admin, Teams Admin, and Skype for Business Admin after initial tenant validation is completed. Multifactor Authentication for Service accounts is recommended.

Hardware SBC Administration

VPN authentication with Security Role groups to control what entities are accessible by personnel.

Nuwave uses secure 1Password Vaults for all password management for Internal Administrators. Physical Access to Data Centers is restricted to limited staff with multi factor authentication, username password, and biometric scanning.

Authorization

Office 365/ Teams

A service account provided by client/ customer permits Nuwave to provision user for Direct Routing services.

iPilot

Internal Administrators have limited functionalities within the applications, these are based on defined employee roles and responsibilities.

Data Center

Security groups are set for role base access within a Palo Alto Firewall that will limit staff's ability to make change in both Lab and Production environments.

Physical Access to Data Centers is restricted to limited staff with multi factor authentication username password and biometric scanning.

Logging

Office 365/ Teams

Reporting is done by Microsoft Teams, Azure and Security and Compliance.

Logging for Tenant Validation and user providing is monitored by Nuwave staff, alerting is in place for any failed processes.

Hardware and SBC

Audit logs with all activity are continuously running on hardware with triggers alerting Administrators of any changes.

Authentication is logged using audit log's which are stored in element management system.

Kentik is used to capture full-resolution network data flows and records. It Provides real-time and forensic data for insights, anomaly detection, and ad hoc queries.

High Availability SBC signaling and RTP (The Real-time Transport Protocol) packets are monitored by OCOM (Oracle Communication Monitor) analytics and reporting platform. SIP (Session Initiation Protocol), RTP and all metrics are reviewed by Nuwave Network Operations.

All Nuwave network elements are monitored from a centralized NMS (Network Management System) that will alert any faults and report current network status

Encryption

Nuwave' s network utilizes TLS(Transport Layer Security) Encrypted SIP signaling and SRTP(Secure Real-time Transport Protocol) for encrypted media (voice packets) when running over untrusted networks.

Certificates and private keys are securely stored in an encrypted database that is limited to authorized personal.

Data protection

All customers data is treated as sensitive data. Customer Data Recorders are restricted to necessary staff. Disclosures and Policies are outlined on the company site. Non-Disclosure Agreements are required prior to the exchange of material information.

Data Governance

The NuWave Information Security Policy is made available to new and existing employees for review as part of an information security education and awareness program. NuWave employees represent that they have reviewed, and agree to adhere to, all policies within the NuWave Information Security Policy documents.

Infrastructure Protection

Change Management mandates that all new features and software releases are first tested in the lab and certified against Nuwave's regression testing plans. Lab results and production rollout are reviewed and approved by product owners. The Changes are then rolled out to production in a controlled fashion one market at a time.

Full backups are run nightly with some systems running change backup incrementally throughout the day for multiple restore points.

RedShift is used for advance threat intelligence analytics for VoIP network surveillance and fraud detection. Alongside with real-time threat mitigation.

Infrastructure Resilience

Nuwave' s data centers operate in a fully geographical redundant mode ensuring carrier grade availability at all times. All core equipment within the Nuwave Data center runs in a HA (High Availability) mode to ensure maximum resiliency

Device Controls

Nuwave offers hardware that will interface with Microsoft Teams. These devices are Managed by the client within the Teams Administration Portal.

Critical Controls

All Nuwave personnel have system restriction and levels of access they are granted. Nuwave employee accounts are locked when a threshold is reached or an irregular event occurs.

VPN also has an invalid password attempt lock out. The lock will not be removed until administrator approves the access and password is automatically rest.

Third Party Risk

Third party security and privacy requirements are established through vendor due-diligence reviews, conducted by the designated NuWave manager, and included in signed contractual agreements prior to engaging in third party services. The engaging team within NuWave is responsible for managing their third-party relationships, including contract management, monitoring of metrics such as service level agreements, and vendor access to relevant applications. Third party vendors are required to meet important privacy and security requirements.