Neat Pulse
Security White Paper

Last updated June 2026

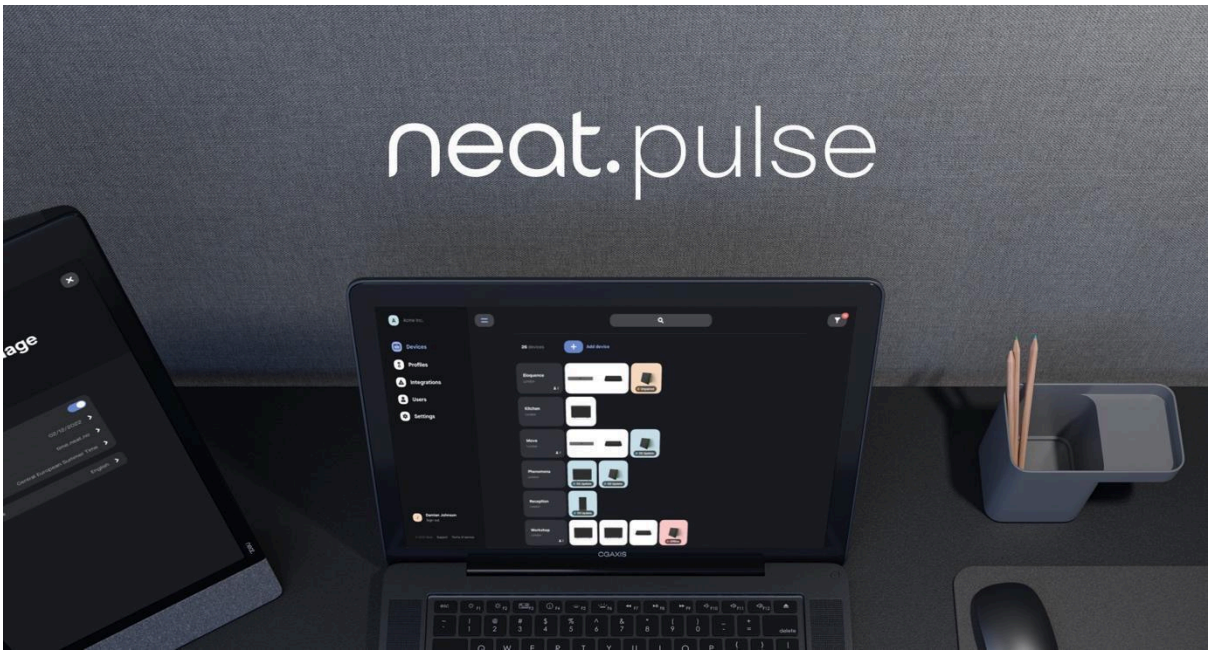


Table of Contents

Introduction

Security is essential to us, and we continuously invest in the tools, processes, and technologies necessary to protect our customers, partners, and their networks. This commitment encompasses implementing robust information security controls, safeguarding data, and ensuring the high availability of the Neat Pulse services.

This whitepaper provides an overview of the security measures implemented within the Neat Pulse service.

Neat Pulse offers customers and partners a secure web portal for the enrollment and comprehensive management of their Neat devices. This includes the ability to modify device configuration settings, update firmware, generate reports, and execute various other device management functions.

The foundational design of Neat Pulse incorporates a modern perspective on security and privacy. Our approach is informed by and aligns with leading standards, such as ISO/IEC 27001:2022 and NIST SP 800-53 Rev. 5. Security considerations are integrated throughout the entire software development lifecycle—from initial concept and design to implementation, testing, change management, and final release. These processes and procedures are supported by a team of experienced stakeholders dedicated to building high-quality, secure systems.

User and Device Authentication in Neat Pulse

User Authentication and Identity Management

Neat Pulse utilizes Microsoft Azure B2C as its core identity provider, offering a robust and flexible framework for user authentication. This implementation facilitates both seamless single sign-on (SSO) experiences and traditional username/password login methods, accommodating diverse organizational IT policies.

The Azure B2C environment within Pulse is configured to support integration with multiple external identity providers (IdPs), significantly enhancing flexibility. Currently, this includes native support for Microsoft Entra ID (formerly Azure Active Directory) and Google Identity Services, allowing users from organizations leveraging these platforms to authenticate easily.

A key component of Pulse's security architecture is its commitment to safeguarding user credentials. Crucially, Neat Pulse never stores user passwords or their cryptographic hashes. Instead, it relies on Azure B2C and the integrated IdPs to manage authentication. Pulse maintains only the minimal necessary reference data from Microsoft to authorize successful logins, strictly limiting any user-specific metadata to what is essential for application functionality. This design ensures that customers can access Pulse without ever having to share their sensitive login credentials directly with Neat.

For organizations requiring tighter control over their identity ecosystem, Neat Pulse also supports integration with various Identity Providers (IdPs) using the SAML (Security Assertion Markup Language) protocol for SSO. This capability allows enterprises to leverage their existing IdP infrastructure—such as Entra ID, Okta, or others—to govern user access to Neat Pulse. By integrating via SAML, organizations achieve centralized identity management, which simplifies user provisioning, de-provisioning, and access control, while also providing users with a streamlined, consistent login experience across corporate applications.

To ensure the security of accounts that utilize the native username/password method within Azure B2C, strict password policies are enforced. The Azure B2C password rules are set to 'strong complexity.' This mandate requires a password that is a minimum of 8 characters and a maximum of 64 characters in length, and must contain at least three out of four of the following character types: lowercase letters, uppercase letters, numbers (0-9), or symbols (special characters).

Device Enrollment and Authentication

The process for bringing a Neat device securely under the management of Neat Pulse is designed to be straightforward yet highly secure.

Devices are enrolled using a randomly generated enrollment code provided within the Pulse administration portal. This code acts as a one-time credential for device registration. A key operational feature is that the enrollment code remains active and available until a device is successfully registered—there is no inherent time-based timeout for the initial availability of the code.

Security is paramount once the enrollment process is initiated. As soon as a device utilizes the code to register itself with the platform, the specific enrollment code is automatically set to expire within a strict 8-hour window. This short expiry window limits the opportunity for a code to be misused or intercepted for subsequent fraudulent enrollments.

Upon successful enrollment into Neat Pulse, the device is provisioned with a secure, secret key. This secret key serves as the permanent, unique, non-shared credential for the device. It is used to authenticate the device for all future communications with the Neat Pulse platform, ensuring that only authorized, enrolled devices can send and receive management commands and status updates. This mechanism establishes a strong, cryptographic identity for each device within the ecosystem.

User Roles and Access Controls

The management and security of the Neat Pulse platform are fundamentally governed by a robust access control mechanism, which delegates responsibilities and permissions across two primary administrative user roles: Owner and Admin. This clear delineation ensures both

comprehensive organizational control and restricted regional management, maintaining a strong security posture.

Owner Role: Full Organizational Authority

The Owner role represents the highest level of administrative access within a Neat Pulse organization. Owners are entrusted with complete oversight and control across the entire platform instance.

- Comprehensive Access: Owners have unfettered access to *all* settings, configurations, and data within their organization's Pulse environment. This includes, but is not limited to, billing information, security policies, global platform integrations, and all organizational-level profile settings.
- User Management: A critical function of the Owner role is user management. Owners have the sole authority to invite other users to the platform, including new Owners and Administrators, thereby controlling the overall administrative footprint. They are also responsible for managing user deactivation and permission changes.
- Remote Control Feature: Owner accounts possess the ability to use the remote control feature on *any and all* devices that are currently enrolled and managed under their organization, regardless of the region in which the devices are deployed. Multiple individuals can be assigned the Owner role within a single organization to ensure continuity and shared high-level oversight.

Admin Role: Restricted Regional Management

The Admin role is designed for more localized and operational management, restricting access to specific, predefined subsets of the organization's device fleet.

- Region-Based Restriction: An Admin's access is strictly scoped to the devices and management functions within the specific regions they have been assigned. They can only administer endpoints—such as Neat devices—that are provisioned within these designated regions.
- Limited Configuration: Admins cannot edit or modify global organization settings, nor can they alter device configuration profiles. Their role is focused purely on the operational maintenance and monitoring of the endpoints under their regional purview.
- No User Management: Admins do not possess the ability to add new users to the platform (Owners or other Admins) or edit broader organization-wide settings.
- Remote Control Feature: Admin accounts can utilize the remote control feature exclusively on devices that are set up within their specific administrative region. This restriction aligns with the need for targeted, local troubleshooting and support without granting access to the entire organizational fleet.

External Support Access

For troubleshooting and dedicated support, Neat support personnel require explicit, secure access to a customer's specific Pulse instance. This access is never automatic or persistent. It is strictly granted via an invitation mechanism controlled by the customer's Owner role,

ensuring that external access is always consensual, auditable, and limited to the duration of the required troubleshooting activity.

Data Security

Data transferred to and from Neat Pulse is secured using industry-leading protocols and encryption standards. All communication, whether initiated by a user navigating to the Neat Pulse web interface in their browser or by the Neat Pulse agent residing on Neat devices, exclusively utilizes HTTPS with a minimum of TLS v1.2, or the more modern and secure TLS v1.3 where supported.

This unified approach to security ensures that the protocols and defenses are consistently applied across all connection types, significantly minimizing the Internet-facing attack surface of the product. Any attempts to access the service using the insecure HTTP protocol are immediately intercepted and upgraded to HTTPS, thereby enforcing the encryption of all connections from the outset.

The foundation of this secure communication is rigorously managed. TLS certificates and the associated cipher suites are subject to regular, comprehensive reviews and validation checks using respected third-party security tools. To adhere to best practices for certificate management, TLS certificates are issued with short expiration dates and are renewed on a weekly cycle. This aggressive renewal policy limits the window of opportunity for potential compromise.

Furthermore, cipher suites are continuously updated in accordance with the latest industry guidelines and security research, currently favoring strong, modern algorithms such as AES 128/256 or ChaCha20, ensuring Forward Secrecy and robust performance.

The security posture of Neat Pulse extends to the data stored within the service. All data persisted on the Neat Pulse cloud service is protected by robust encryption at rest using the AES 256-bit standard, which is compliant with FIPS 140-2.

This comprehensive encryption scope includes all types of stored assets, such as relational databases, binary image files, operational log files, and any other persistent data. This data is physically hosted and managed on the Microsoft Azure platform, leveraging the extensive security controls and infrastructure of one of the world's leading cloud providers.

In addition, access to the underlying physical servers is strictly restricted and is only available through the established, audited, and controlled mechanisms provided by the cloud provider. There is no direct, unmanaged physical server access outside of the Microsoft Azure operational framework, adding an essential layer of physical and infrastructure security to the data.

Data Resiliency & Residency

The integrity and availability of data within Neat Pulse is key, and a robust, multi-layered backup and durability strategy has been implemented to meet this commitment.

Comprehensive Backup Management:

Pulse data backups are managed through a dual-system approach, ensuring redundancy and reliability:

1. **Microsoft Azure Backups:** The built-in capabilities of Microsoft Azure Backups are utilized as the primary, foundational layer for data preservation.
2. **Customized Operations Backups:** A secondary, customized backup solution is executed daily by the dedicated Pulse operations team. These custom backup jobs are designed with an extra layer of security and independence.
    - **Encryption:** All customized backups are strongly encrypted both in transit and at rest, protecting sensitive data from unauthorized access.
    - **Separate Storage:** The encrypted custom backups are stored in a physically and logically separate, secure location within the Azure ecosystem, minimizing the risk of a single point of failure affecting both the live data and the backups.
    - **Retention Policy:** Backups are retained for a period of up to 30 days, providing a sufficient window for point-in-time recovery and addressing potential data loss scenarios.

Data Durability and High Availability:

Beyond standard backup procedures, the core database infrastructure is engineered for exceptional durability and continuous operation:

- **Database Redundancy:** The underlying database system is configured to maintain three local redundant synchronous copies of all database files. This triple-redundancy ensures high data durability, as any localized hardware failure will not result in data loss or service interruption, with the system automatically failing over to one of the two remaining copies.
- **High Availability (HA) Architecture:** Where technically appropriate and beneficial for service continuity, High Availability (HA) architectural patterns have been implemented across the Pulse infrastructure. This HA framework is designed to deliver:
    - **Automatic Failover:** In the event of a component failure, the system automatically and instantaneously switches operations to a healthy standby instance with minimal to zero disruption to service.
    - **Scalability:** HA patterns also enable horizontal scaling of resources, allowing the system to seamlessly accommodate fluctuations in user demand and processing load while maintaining optimal performance and reliability.

Neat Pulse services are built upon a foundation of robust, third-party cloud hosting infrastructure, enabling global service delivery and high availability. To ensure optimal performance and adherence to regional data requirements, Neat strategically leverages

top-tier cloud hosting providers. The current geographic locations of the primary data centers and cloud services utilized for Neat Pulse delivery are detailed in *Table A*.

A Note on Scope: The hosting locations listed in *Table A* are exclusively for the Neat Pulse cloud services. They do not represent the hosting locations for any other applications, services, or embedded operating systems running directly on Neat hardware devices (e.g., Neat Bar, Neat Pad, etc.). Those device-specific services may utilize separate hosting environments.

Table A

Cloud Hosting Provider Name	Location
Microsoft Corporation (Azure)	West Europe - Netherlands
Microsoft Corporation (Azure)	US West 2 - Washington

Audit Logs

Neat Pulse offers robust security and compliance features, including the crucial ability for Customers to export detailed audit logs. These logs serve as an essential resource for monitoring activity and maintaining compliance standards within the organization's use of Neat Pulse.

Components of the Audit Logs:

The exported audit logs are comprehensive and consist of two primary categories of information:

1. **User Action Logs:** These logs meticulously record the actions performed by authorized users within the Neat Pulse platform. This includes, but is not limited to, configuration changes, administrative operations, access attempts, and other significant interactions.
2. **Device Change Logs:** These logs track modifications and status changes pertaining to the devices managed through Neat Pulse. This provides a historical record of device lifecycle events, software updates, configuration deployments, and health status changes.

Data Contained within the Logs:

It is important for Customers to be aware that both the user action logs and device change logs may contain personal data. This data is included to ensure the accountability and traceability of actions within the system. Personal data elements that may be present include:

- First and Last name
- Email address

- Device or profile names

Availability and Retention:

Access to and download of these critical audit logs are features reserved for Customers subscribed to the appropriate service plan tier. This tiered access ensures that advanced security and compliance tools are available to organizations requiring them.

A key feature of the Neat Pulse audit log functionality is the commitment to data longevity. Audit logs are retained indefinitely. This policy ensures that Customers have a complete and unalterable historical record for forensic analysis, regulatory compliance, long-term trend analysis, and dispute resolution, offering maximum transparency and accountability over the platform's usage.

Managed Cloud Services

Pulse is built upon a foundation of Microsoft Azure cloud services, which provides a robust and secure underlying infrastructure. A key advantage of leveraging Azure is the automatic management of the core operating systems and underlying infrastructure. This means that application and operating system patches, updates, and maintenance are handled continuously and seamlessly by Azure's dedicated platform management teams.

This strategic choice to utilize managed services significantly minimizes operational complexity for the Pulse development and operations teams. When new system components or services are designed and integrated into the Pulse architecture, a conscious effort is made to prioritize Azure-managed services over custom-built or self-managed solutions. This approach not only accelerates development but, more critically, inherently increases the overall security posture of the system. By offloading critical infrastructure management and patching to Microsoft Azure, Pulse benefits from their global security expertise, continuous monitoring, and adherence to industry compliance standards, allowing the development teams to focus their efforts on the security and functionality of the application layer.

Business Continuity

Neat Pulse is hosted on top-tier cloud platform, Microsoft Azure, ensuring robust infrastructure resiliency.

- **High Availability:** The Azure infrastructure is engineered and continuously monitored to achieve a consistently high uptime, performing above the benchmark of 99.9%.
- **N+1 Redundancy:** All essential systems for power, cooling, and network services within Azure's data centers utilize N+1 redundancy to prevent single points of failure.

Data Protection and Recovery

- **Comprehensive Backups:** All customer data is fully backed up.
- **Immediate Failover:** Data is replicated across multiple live instances, allowing for immediate failover and uninterrupted service in the event of a database failure.
- **AES-256 Encryption:** All stored backups are secured with AES-256 encryption, maintaining data confidentiality even during recovery processes.

Continuous Monitoring and Compliance

- **24/7/365 Operations:** Our DevOps teams provide round-the-clock monitoring of application and infrastructure health.
- **ISO 27001 Certified Resilience**: Neat holds the internationally recognized ISO 27001 certification. This requires a documented and tested Business Continuity Plan (BCP) as part of our Information Security Management System (ISMS). These business continuity processes are subject to mandatory annual audits by independent third parties to confirm adherence to global resilience standards.

Cloud Security

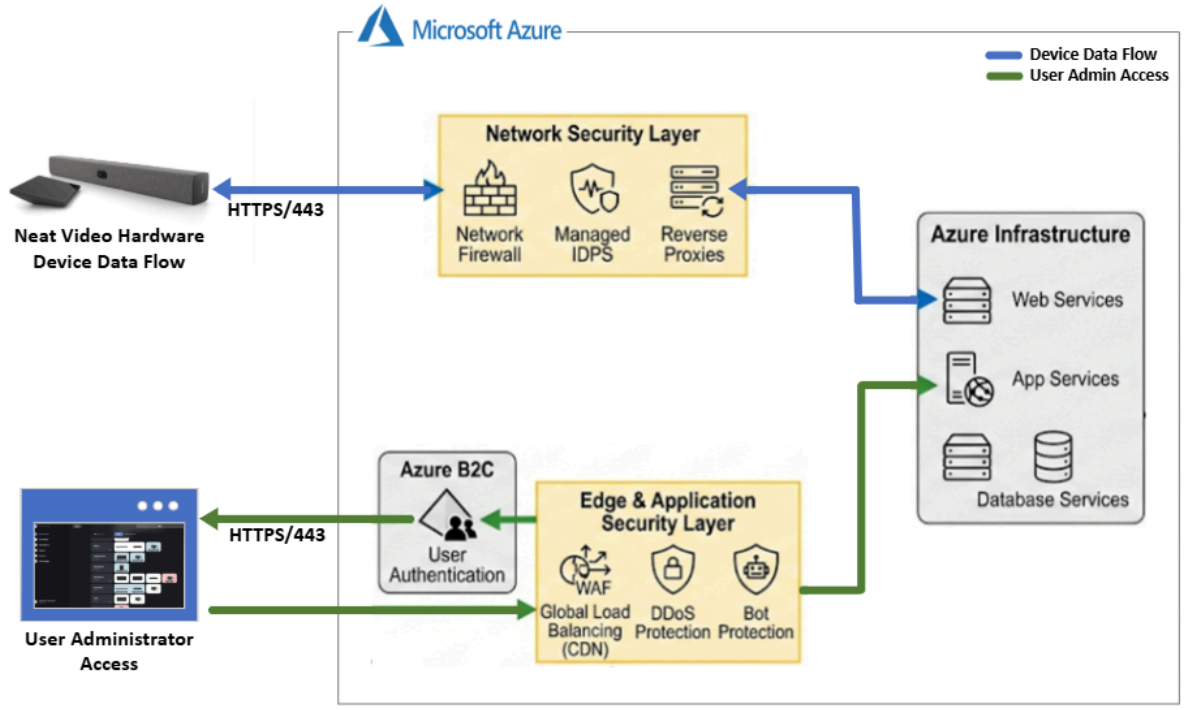
Neat Pulse utilizes a defense-in-depth architecture that leverages Microsoft's global network infrastructure to provide robust DDoS and WAF protection at the edge. Internal security is maintained through multi-layered intrusion defense—combining stateful firewalls with a managed IDPS—and strict resource isolation via Azure Virtual Networks. This secure framework is reinforced by dedicated traffic management through reverse proxies and load balancers, ensuring that backend systems remain protected from external threats while maintaining high availability and consistent performance.

Neat Pulse platform requires specific configurations to manage devices remotely and maintain a stable connection. For comprehensive technical specifications on required services, network ports, and target IP addresses for all Neat devices and services, please refer to the following support article for details on the network and firewall requirements for all Neat products.

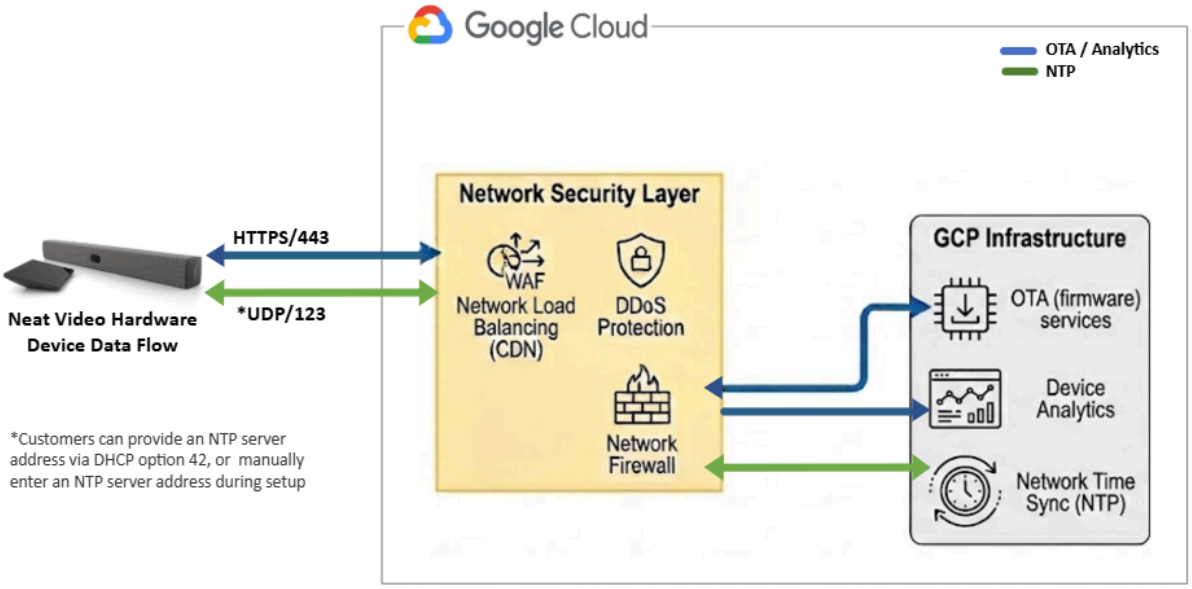
High-Level Pulse & Device Architecture

This section provides a high-level, logical overview of the Neat Pulse and Neat video hardware services. The diagrams illustrate the service components, communication protocols, and access management controls. The services are distributed across two primary cloud platforms: Neat Pulse services are hosted on Microsoft Azure, while the device-dependent services utilize Google Cloud Platform.

Neat Cloud High-Level Architecture - Pulse



Neat Cloud High-Level Architecture - Devices



Refer to the following support article for details on the network and firewall requirements for all Neat products.

APIs

The Neat Pulse platform utilizes centralized management, primarily facilitated by the Neat Pulse API, to provide administrators with comprehensive control over their device fleet's security and configuration. The Management API offers operational oversight, enabling device health monitoring and robust configuration capabilities, including updating settings, remote device control (like restarts), and provisioning (generating enrollment codes, managing organizational hierarchy).

A key feature is the API's capacity for bulk configurations, which provides efficiencies for large-scale deployments, automation, and integration with IT systems like CMDBs and SIEMs, ensuring consistency and reducing errors. Pulse APIs have rate limits in place to ensure that load and request traffic is being handled efficiently. The rate limit defines the maximum number of requests that can be made to the API within a given period of time.

Webhooks

Neat Pulse Webhooks allow customers to receive near-real-time event notifications from the Neat Pulse platform, enabling integrations with ITSM, monitoring, and collaboration systems such as ServiceNow, Microsoft Teams, or Slack.

Security, reliability, and data integrity are central to how we design and operate this feature. This document summarizes how authentication, encryption, and signing are implemented to meet enterprise security expectations.

Secure Delivery Architecture

Encrypted Transport

All webhook traffic is transmitted over HTTPS (TLS 1.2 or higher).

- HTTP endpoints (http://) are not supported.
- Certificates must be valid and issued by a trusted Certificate Authority (CA).
- Self-signed or expired certificates will be rejected.

This ensures that webhook payloads are encrypted in transit and protected from interception or tampering.

Default Event Format

As a default, webhook messages follow the CloudEvents 1.0.2 binary JSON format, a CNCF open standard used across major SaaS providers. See here for more information.

This guarantees schema consistency, simplifying parsing and validation on the receiving side.

Each message includes standard headers:

```HTML
content-type: application/cloudevents+json; charset=utf-8

user-agent: Neat-Pulse-Webhook/1.0

ce-id: <eventId>

ce-source:
https://pulse.neat.no/{orgId}/p/rooms/device/{deviceId}

ce-specversion: 1.0.2

ce-time: 2025-11-29T09:04:22Z

ce-type: no.neat.pulse.device.teams_signed_in

x-neat-timestamp: <UNIX_EPOCH>
```

All event formats, current and future, will be versioned and the message body will be UTF-8 encoded JSON.

Additional Event Formats

Neat Pulse also offers additional delivery formats for increased compatibility across multiple platforms. Currently, the following additional event formats are supported:

- CloudEvents 1.0.2 (Structured format)
- Adaptive Cards (for Microsoft Teams)
- Block Kit (for Slack)

Authentication

Neat Pulse supports multiple authentication methods so that customers can match their internal security posture and integration preferences.

The following methods are supported:

- **None (default)**
  - Used for testing or closed beta environments, or in environments where authentication isn't required.

- **Bearer Token**
  - The customer provides a long, random token. Pulse includes it in the Authorization header as Authorization: Bearer <token>.

    - Tokens are encrypted in KeyVault, never displayed again after creation, and must be rotated by the customer.
    - Use for controlled endpoints with rotating credentials.

- **Basic Authentication**
    - The customer provides a username and password pair
    - These will be Base64 encoded and passed as Authorization: Basic <base64(user:password)>.
    - Used for modern API gateways or systems using token-based verification.

- **Custom Header**
    - The customer provides a custom header where the value can contain both a token and other parameters. Pulse includes it in the Authorization header as Authorization: <custom_header>.
    - Use when other Authorization headers are required ie Authorization: Splunk <splunk_token>.
    - Customer headers are stored and otherwise treated like Bearer Tokens.

Credential Storage

Customers configure authentication per webhook endpoint via the Pulse UI or API. Before being stored, all usernames and shared secrets are obfuscated using industry standard encryption.

These encrypted values are then managed within Azure Key Vault, which provides multi-layer, FIPS-compliant key protection through a hierarchy of encryption methods.

Credentials are encrypted at rest and are never visible after creation.

Message Signing

To ensure recipients can verify that webhook messages were genuinely sent by Neat Pulse and not altered in transit, HMAC-based message signing is available.

Algorithm

Pulse uses HMAC-SHA256 with a customer-provided secret key. For every webhook event, Pulse:

1. Concatenates the event body and timestamp (UNIX epoch).
2. Computes a hex encoded HMAC digest using the shared secret.
3. Includes the signature in the X-Neat-Signature header.

Computation

```
Shell

base = "<raw_body>.<timestamp>"

signature = hex(hmac_sha256(secret, base))
```

Header

```
HTML

X-Neat-Signature: v1=<signature>
```

Verification

Recipients can verify authenticity by recomputing the HMAC on their side and comparing it with the received header value.

It is recommended that recipients should reject messages older than 5 minutes based on X-Neat-Timestamp (UNIX epoch, UTC) to mitigate replay attacks.

This process prevents tampering and validates both origin (message came from Pulse) and integrity (message wasn't altered).

Operational Controls

Access Scope

Webhooks are scoped at the organization (tenant) level. Only users with Owner-level access can create or manage webhook configurations.

All webhook lifecycle actions — create, update, delete, activate, deactivate — are recorded in Pulse Audit Logs.

Delivery Expectations

- Pulse expects a 2xx response within 10 seconds from the receiving endpoint.
- Deliveries that fail (non-2xx or timeout) are marked as unsuccessful
- Event messages are delivered once per subscribed webhook.

Platform Security & Data Protection

Neat Pulse webhooks inherit Neat's global security controls: encryption at rest, credential obfuscation, TLS 1.2+ in transit, ISO 27001-aligned operations, GDPR compliance, and bi-annual third-party penetration testing. See below for a summary:

- **Data residency:** Hosted in geographically distributed, ISO-certified data centers with regional separation (currently EU and US).
- **Access control:** Role-based permissions enforced through Azure AD B2C identity and internal IAM policies.
- **Encryption in transit:** All webhook data is encrypted in transit as it is transmitted over HTTPS using TLS 1.2 or higher.
- **Encryption at rest:** All data, including webhook credentials, are encrypted at rest using AES-128 at the application layer, and a hierarchy of encryption keys protected by FIPS 140-2 compliant modules in the keyvault. See more here.
- **Auditability:** All administrative and configuration actions are recorded and accessible via Pulse Audit Logs.
- **Penetration testing:** Neat conducts regular independent penetration tests across Pulse APIs, webhooks, and backend infrastructure.
- **Compliance alignment:** Neat is aligned with GDPR principles and ISO/IEC 27001 information-security practices.

Customer Responsibilities

To maintain a secure integration, customers should:

- Use HTTPS endpoints with valid TLS certificates.
- Keep authentication credentials or HMAC secrets confidential.
- Rotate tokens and secrets periodically.
- Validate X-Neat-Timestamp to prevent replay attacks (e.g., reject messages older than 5 minutes).
- Verify message signatures when signing is enabled.
- Respond with 2xx codes promptly to acknowledge receipt.

Remote Control

The Pulse Remote Control is a feature allowing full remote access to a Neat Device from the Pulse web portal. The power of this is accompanied by a thorough set of privacy controls. Any remote-control session allows both visibility of the remote control being active, and ability to refuse the start of the session.

Devices maintain a configuration setting that is not managed by Pulse: whether to Allow, or Not Allow remote control requests.

When remote control is requested from Pulse:

- If the setting is set to **Not Allowed**, then the remote control will not proceed.
- If the setting is set to **Allowed with Confirmation**, a time-limited dialogue is shown requiring someone present in the room to approve the request. If no action is taken within 15 seconds, the request is automatically denied.

- If the setting is set to **Always Allowed**, a time-limited dialogue is shown allowing a user to cancel the remote session. If no action is taken within 15 seconds, the request is automatically accepted.

If the remote-control session does proceed with the required consent / configuration, then information that the session is active is shown on the device or devices being remote controlled. The remote-control session can be ended on the endpoint at any time.

Remote control sessions are audited to the audit log. The remote-control feature can be disabled from the endpoint, you can only re-enable control again from the endpoint. In the event a device is factory reset, the device then needs to be re-enrolled into Pulse. By default, remote-control is enabled after enrolling in Pulse. Please visit the neat support site (https://support.neat.no) for more information on remote-control features.

Neat Open Security

Neat Open AI Notes and Wireless Screen Sharing functionalities capture audio data to generate comprehensive meeting summaries and facilitate seamless wireless screen sharing. Neat Open is engineered with a security-by-design architecture, ensuring the robust protection of your audio data through powerful encryption at every stage of its lifecycle—both during transmission between services and while stored in our cloud infrastructure.

Customers must opt-in to Neat Open services to enable advanced AI capabilities like meeting transcriptions and summaries through the Neat Pulse management platform and device-level settings.

When Neat Open device controls, wireless screen sharing, audio transcription are enabled, then:

- The device will make a WebSockets (secure) connection to our cloud mentioned above,
- And it will be possible to use the pairing to pair to the device

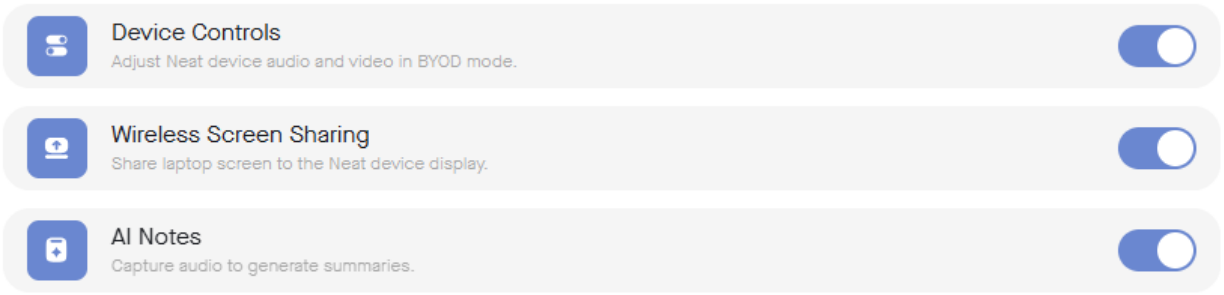
Enabling Neat Open Features

Neat Pulse Enrollment: Devices must first be enrolled in the Neat Pulse management platform (pulse.neat.no). Access to Neat Open and native third-party apps is an initial requirement that is enabled after successful enrollment.

Platform Selection: During the initial "Out-of-Box" (OOB) setup or through the Pulse dashboard, administrators select to enable Neat Open.

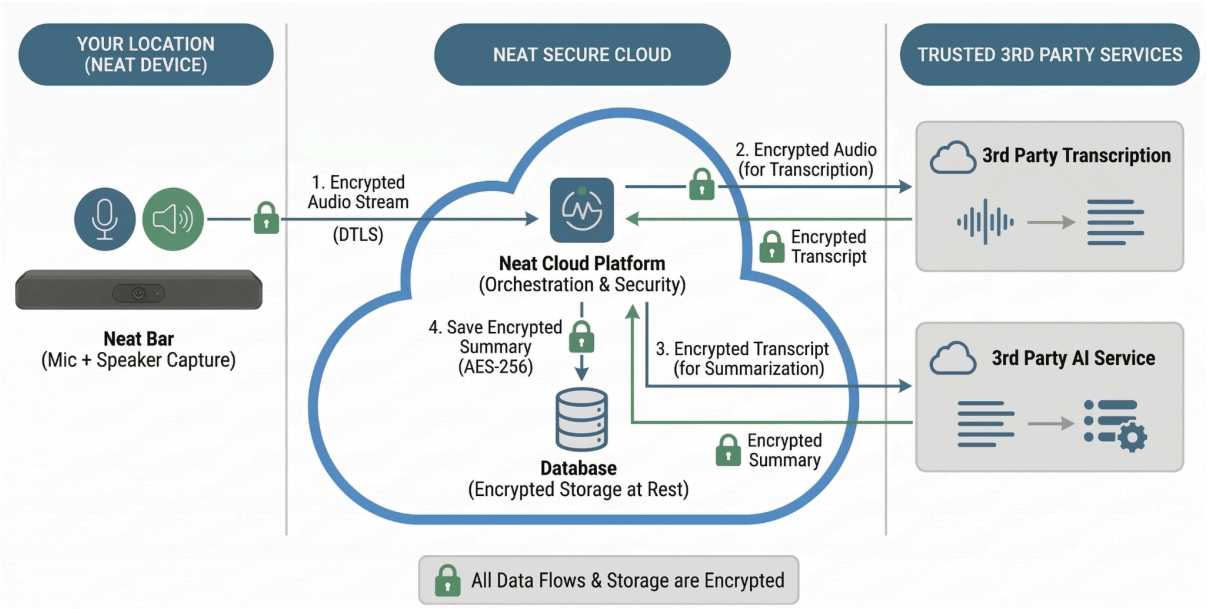
Neat Open Activation: Within the Neat Pulse dashboard, administrators will have the option to enable Neat Open under "device settings" (see *figure 1*).

Figure 1



High-Level Architecture & Data Flow

Below is an overview of how we process your meeting data securely.



Architectural Process Description

This architecture ensures that Neat acts as the secure gatekeeper for your data. Your raw audio is never stored permanently by our third-party processing partners.

1. Secure Audio Capture & Transport

The process begins on your Neat device. We capture a combined audio stream—what is said in the room (microphone) and what is heard from remote participants (speaker)—to ensure a complete record of the meeting.

- **Security Action:** This combined audio data is immediately encrypted using industry-standard protocols (DTLS 1.2+) before it leaves the device, creating a secure tunnel directly to our cloud service.

2. Encrypted Transcription (Text-to-Speech)

Once the secure audio stream reaches our cloud service, we temporarily forward it to our trusted transcription partner to convert the speech into text.

- **Security Action:** Audio is transported over an encrypted connection. The third-party service processes the audio and does not retain or store the audio file after processing is complete.

3. AI-Powered Summarization

Our cloud service receives the text transcript and then securely sends it to our AI partner. The AI analyzes the text to generate concise meeting summaries, action items, and key topics.

- **Security Action:** This data exchange is fully encrypted. Furthermore, our agreements with these AI partners ensure that your meeting data is not used to train their public models.

4. Secure Storage (Encryption at Rest)

Finally, the generated summary is returned and stored in the Neat Cloud service.

- **Security Action:** Only the final summary is saved into our Neat Cloud database. It is protected using advanced AES-256 encryption "at-rest," meaning the data remains encrypted even when stored on disk. Only the person who initiates the session, and anybody who joins locally via the pairing code, with the summary link can access the content.

Content Sharing via Local Browser

Neat Open allows users to share content wirelessly from their local browser to the room display without the need for physical cables or proprietary dongles.

- **Content Sharing:** Content sharing is managed via browser utilizing WebRTC (Web Real-Time Communication). Data flows to Neat's SFU (Selective Forwarding Unit) to optimize the media stream.
- **Encrypted Stream:** Media streams are transmitted using Datagram Transport Layer Security (DTLS) to ensure that content remains private between the laptop and the Neat device.
- **Session Isolation:** Each sharing session is ephemeral. Once the browser tab is closed or the "Stop Sharing" button is pressed, all session-related temporary data is purged from the Neat device's memory.

Encryption of Data Flows

Neat Open employs industry-standard encryption protocols to protect data at every stage of its journey.

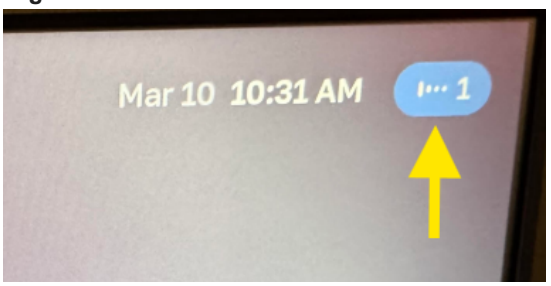
Data State	Encryption Standard
Data In-Transit	Protected via TLS 1.2+ for all control signals and DTLS for media
Data At-Rest	Stored summaries and configuration data are encrypted using AES-256

Camera Control from Local Laptop

When using Neat Open in BYOD mode, your laptop gains control over the Neat camera and microphones while maintaining strict hardware-level safeguards.

- **User-Centric Control:** The local laptop can adjust framing (Neat Symmetry) and boundaries (Neat Boundary), but these controls are only active during a physical connection or authenticated pairing session.
- **Visual Indicators:** The **VU (Volume Unit) meter** displayed on the device provides an immediate visual cue whenever the microphone is active, ensuring users are never recorded unknowingly. This is always displayed at the top right corner of the device when a recording is active (see *figure 2*).

Figure 2



Access Controls

To streamline the rollout, Neat Open utilizes a simplified access model that prioritizes ease of use while maintaining security.

- **Pairing Codes:** Instead of individual user accounts, the browser-to-room connection is established via a short-lived 6-digit Pairing Code displayed on the Neat screen.
- **Physical Presence Requirement:** Because the code is only visible on the physical display in the room, unauthorized remote users cannot hijack the session.

Data Residency and Retention

Data Residency

All meeting transcriptions and summaries generated by Neat Open are stored securely within the Neat Cloud. This infrastructure is currently hosted using the Microsoft Azure West Europe (Netherlands) hosting service, ensuring that your data resides within a highly secure and resilient cloud environment.

Data Retention

To ensure that administrators and users have continuous access to meeting insights, Neat's current data retention rules are configured to allow all hosted data to be stored indefinitely.

Data Privacy & Model Integrity

We believe your data belongs to you. Neat Open is governed by strict "No-Training" policies.

- **No Training on Customer Data:** Neat **does not** use your meeting transcripts, audio, video, or summaries to train, retrain, or improve our underlying LLMs or AI models.
- **Model Isolation:** AI processing occurs in a secure, multi-tenant environment where data from one customer is never accessible to another.
- **No Third-Party Selling:** Your meeting data is never sold to third parties or used for advertising purposes.

Note: These security measures are subject to regular third-party audits and penetration testing to ensure they stand up to the latest cybersecurity threats.

Secure Development Lifecycle

Security and Privacy by Design

Neat Pulse operates in a shared multi-tenancy environment. Each organization or tenant's data is stored in its own independent database within Neat Pulse. Access Controls prevent sharing data across customer tenants/organizations. Architectural decisions follow a collaborative design process, security and privacy review, and require sign-off by the senior level of engineering before implementation.

Software Development

Software and source code is developed and stored on GitHub, guaranteeing change history, availability, and resilience of the assets. Changes are peer reviewed before being merged into a release, and changes are accompanied by unit and integration tests suitable for the feature or fix. Tests are run on every change (continuous integration) and software releases

are only produced if all tests pass. Every successfully tested build automatically results in a new release (continuous delivery), which can be deployed to production quickly and easily.

Change & Release Management

The Pulse system is carefully designed to minimize changes such that a new version of software can be deployed incrementally to users and customers, rather than all at once. This allows a carefully staged software release, and also cutting-edge features to be tested by beta testers, without affecting the majority of users. Changes to the production system follow a DevOps paradigm of using software development processes and principles: peer code review, change history, and infrastructure as code.

Security Scanning

Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) tools are utilized for identifying security vulnerabilities in software applications throughout the software development lifecycle. Additionally, Neat automates the process of maintaining up-to-date software dependencies. The Neat Pulse operations team also conducts regular scans to ensure that all Microsoft Azure workloads that support Pulse adhere to security best practices.

We routinely engage independent third-party security firms to conduct penetration testing across our services. These assessments are designed to identify and remediate potential vulnerabilities, strengthen our security posture, and validate the effectiveness of our controls.

Data Privacy & Processing

Neat Pulse securely processes and stores several distinct categories of data, which are essential for operation, security, and delivering enhanced collaboration experiences.

Refer to the *Neat Data Processing Addendum (DPA) for Customers* which includes details for the processing of personal data that is subject to Data Protection Laws in the scope of Neat Pulse.

User & Authentication Data

This category of data is fundamental to securing the platform and ensuring users have appropriate access (Role-Based Access Control).

- Identity Information: Pulse records basic identifying details for authorized users, including their first and last names and primary email addresses. This information is used for account identification and communication purposes.
- Role-Based Access: To enforce organizational security policies and manage device access, Pulse stores information detailing user permissions (e.g., owner, administrator) and their assigned regions or locations. This dictates which devices and data a user is authorized to manage or view within the platform.

Device & Room Metadata

This data is important for inventory management, remote configuration, troubleshooting, and linking physical devices to their logical location and status within an organization.

- Device Identification: Core identifiers stored include serial numbers, MAC addresses, model types (e.g., Neat Bar, Neat Board), and their current IP addresses (used for network connectivity and troubleshooting).
- Organizational Data: Pulse links devices to their physical and logical locations. This includes assigned "Space" names (e.g., "Main Boardroom," "Huddle Space 3"), organizational site locations (e.g., "Chicago HQ," "Sales Office - APAC"), and the assigned configuration profiles that determine device behavior and settings.
- Software Status: This information is vital for ensuring devices are secure, up-to-date, and fully functional. Pulse continuously monitors and stores the current device firmware versions, the NeatOS version running on the device, and the app-specific status (e.g., Zoom, Teams, or Meet Rooms software version).

Environmental & "Neat Sense" Data

The "Neat Sense" feature uses the devices' integrated sensors to provide actionable data on the room environment, optimizing space utilization and occupant well-being.

- Occupancy: Pulse tracks the total count of people currently in the room. This data is utilized for room usage analytics.
    - *Note on Privacy:* No biometric data, facial recognition data, or identifiable images of individuals are collected or stored for the purpose of occupancy counting. The technology relies on anonymized sensing techniques to ensure occupant privacy.
- Air Quality: Data relevant to health and comfort is collected, including CO2eq (estimated Carbon Dioxide) and VOC (Volatile Organic Compounds) levels.
- Climate: Real-time environmental readings are stored, specifically the temperature (in Celsius or Fahrenheit) and relative humidity of the room.

Audit & Diagnostic Logs

These records are essential for security, compliance, troubleshooting, and maintaining an historical record of changes within the managed environment.

- User Action Logs: A detailed, immutable history is maintained, recording key security and administrative actions. This includes who logged in, what specific settings were changed (e.g., updating a device name, altering a configuration profile), and when the action took place. This is foundational for auditing and tracing security incidents.
- Device Change Logs: Pulse tracks operational and status changes for each managed device. This includes records of device reboots, confirmation of firmware updates being applied, and documentation of configuration shifts (e.g., a change in the primary meeting platform).
- Diagnostic Files: In the event a customer opens a support ticket with Neat, Pulse has the capability to securely pull detailed system logs from the affected devices to help the support team diagnose and troubleshoot complex issues. These diagnostic files,

which may contain temporary system-level information, are handled under strict data retention policies and are typically deleted after the associated support ticket has been officially resolved.

Certifications

Neatframe Limited and its subsidiaries hold an ISO/IEC 27001:2022 certification, which demonstrates Neat's commitment to maintaining a robust Information Security Management System (ISMS) in line with internationally recognized standards. The scope of this certification covers the processes, systems, and services involved in the development, management, operation, sales, marketing, and delivery of all Neat products.

Information Security Incident Management

Neat has a defined Security Incident Response plan detailing the procedures for addressing computer security incidents affecting Neat products and internal information systems. Key elements of this plan include:

- Identifying incident response stakeholders, their roles, and responsibilities.
- Defining incident triggering sources, types, and severity levels.
- Establishing requirements for testing, post-incident analysis (lessons learned),
- and collecting metrics to assess response effectiveness.

Should a data breach occur that could potentially impact sensitive customer data, Neat will promptly notify the affected customer(s) via email of any actual or alleged incident involving unauthorized or accidental disclosure of, or access to, any personal data or other breaches.

Customers who need to report a security concern regarding a Neat device can do so by visiting Neat's security vulnerability reporting policy website.

Customers can also report a security concern regarding a Neat device(s), by visiting https://support.neat.no/ or contacting us at security@neat.no.

Additional Resources

We encourage you to visit our support website and view new articles, FAQs, how-to and troubleshooting guides which are being regularly added there. Please search the following page to find answers to your common questions or problems: https://support.neat.no

If you encounter an issue with your Neat device or service, you can open a ticket in Pulse at https://pulse.neat.no. Customers can submit a ticket directly from their device/room or the portal).

Disclaimer

This document is provided for informational purposes only and does not convey any legal rights to any intellectual property in any Neat product. You may copy and use this document for your internal reference purposes only. All statements, information and recommendations in this document are believed to be accurate but are presented without warranty of any kind, express or implied. This document is not an agreement and in no event will Neat be liable for lost profits or loss of business or for any consequential, indirect, special, incidental or punitive damages arising out of or related to this document. The specifications and information regarding the products and/or services in this document are subject to change without notice.