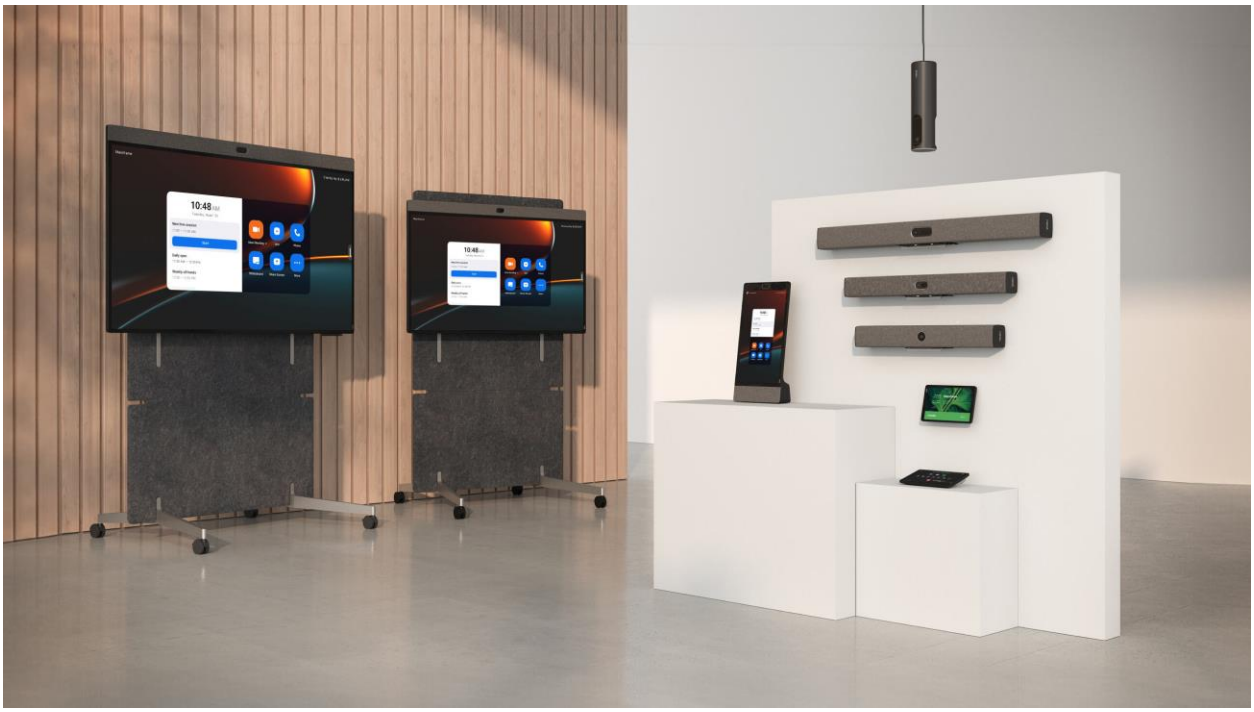
# Neat Security and Privacy for Zoom Rooms Appliances

Last Updated March 2025

## Introduction

This whitepaper intends to provide all relevant technical details which have an impact on the security of Neat video devices. It contains details of the architecture, software, and hardware aspects of Neat devices running Zoom Rooms.

Neat devices are incredibly easy to install, set up and use and have unique features to support a safer, more enhanced and engaging hybrid working and learning environment going forward.



## Information Security

Neat implements several security and privacy by design principles to ensure hardware and software security controls are built into Neat's devices. The goal of following these basic principles and security protocols will help reduce the chances that cyber-attacks will impact our products and customer environments.

### Secure Development Lifecycle

Neat has been following Security Development Lifecycle (SDL) best practices since our founding and continues to adhere to these standards today. All our Neat products are developed following standard development lifecycle practices including requirements definition, design, implementation, testing, and final release. The implementation phase has both automated functional testing and manual reviews of the code by our development team.

### Secure Operating System (Firmware)

The Neat OS (Operating System) is a purpose-built implementation of the Android Open-Source Project (AOSP). All modifications are aimed at optimizing the software for its task of being a video collaboration device. Many changes to the Neat OS have been made, from kernel modification to removal of unused services. Removing unneeded services and libraries prevents them from being used for anything else but Zoom Rooms video conferencing applications. Neat software does not adhere to Android compatibility standards for OEMs (such as smartphones or tablets).

Neat devices do not run GMS (Google Mobile Services) which are a set of applications and services such as Google Play Store, Search, Chrome, and others. and do not allow any application installations outside of the tested and approved Zoom Rooms APKs or other Neat approved software packages, which could become a source for introducing security vulnerabilities directly to the operating system.

In addition, methods to install or sideload applications do not exist. Code signing certificates are used to validate upgrade packages to ensure only Neat built upgrades can be installed. When updates are downloaded, the signatures are validated prior to the upgrade being performed.

By design, our Neat firmware does not provide a user any access to the operating system or access to components outside of the designated Zoom user experience.

Refer to the *Device Model and Operating System Matrix* below for a listing of the supported versions of the Android operating system and related Neat product line.

The Neat OS employs a multi-layered security approach. This includes hardware-backed secure boot and verified boot for a tamper-proof startup that confirms the state of each stage of the boot process.

Android Debug Bridge (ADB) is disabled and locked by design on all devices running our release software. ADB is a command line tool that enables administrators to perform functions on Android-based devices and enables installation of apps, access to the device shell, and other admin functions.

SELinux, which stands for Security Enhanced Linux, is an access control system that is built into the Linux kernel. Neat devices use this feature to enforce the policies that define what level of access users, programs, and services have within the OS/Firmware.

Neat devices do not contain or store personal data on the devices. Third-party applications, such as those from Zoom, may store personal data. We recommend contacting your application provider directly for more information.

Following industry best practices, access to Neat System Settings is protected by a pin code. The configuration of this pin code can be set in the Zoom admin portal. The policy of this pin code is part of the Zoom platform and outside of Neats responsibility. Physical access is required to access the system settings where a web interface may be enabled for remote management capabilities.

Neat Bar, Neat Bar Pro, Neat Frame, and Neat Pad support integrated security lock slots for additional physical security.

**Secure Data Storage & Key Management**

Neat devices contain local storage that is used for the operating system and third-party applications such as Zoom Rooms. The user data storage (e.g., System Settings, Microsoft Teams or Zoom Room token, etc.) is fully encrypted using FBE (File Based Encryption) or Full Disk Encryption (FDE), depending upon the device model.

All keys and certificates on the device are stored encrypted in the device's hardware-based keystore

**Secure Communications**

A secure web interface can be configured on each device (disabled by default). The web interface may only be enabled through physical access to the device. Once it's enabled, access is allowed after authentication, which occurs over Transport Layer Security (TLS 1.2+). This provides both the encryption of data in transit and authentication of the backend systems with which the device is communicating. The web interface contains no Apache code or modules. Only services required are included, limiting exposure to vulnerabilities.

Neat devices only allow outgoing traffic, apart from a set of ports used by paired devices and the web management interface. All data that is sent out from the device is transferred via encrypted protocols.

Neat devices require an NTP (Network Time Protocol) server to operate, and by default will use *time.neat.no* as the NTP server when there is no other NTP server configured. NTP server settings can be manually configured in the system settings.

**USB-C Security**

Neat's Android Operating System (OS) includes a very narrow set of USB drivers. The OS is also stripped of unnecessary services such as file managers that would normally be used to copy files and run executables. Neat devices do not have drivers for USB mass storage (i.e., USB flash sticks) so that it cannot be used to transfer malware.

There are a limited set of use cases for USB usage on Neat devices (outside of the standard keyboard/mouse functions). This includes leveraging USB for touchscreen capabilities, audio for USB headsets, and network connectivity for USB to Ethernet adapters. If any USB device is connected, the system will enumerate this device, however, those devices will not operate unless they have been included in the OS device driver list. This means that the exposure to malicious payloads generated by a USB device is minimal and it's very unlikely that this can be used as a potential attack vector.

**Software Distribution**

Platform vendors provide the relevant APKs to Neat. Neat includes these software APKs in its total software package and tests them thoroughly before this is released as a bundle to the customer. Neat does not have access to the source code of vendor APKs. Zoom is responsible for these packages, and any security concerns towards these APKs should be addressed to Zoom directly.

Updates for both Neat firmware and Zoom Rooms software are available in two ways. By default, Neat products are configured to auto-update to ensure devices are always up to date and include the latest security features. It is also possible to opt-out of Neat’s auto-update functionality and update Neat products manually from the Zoom portal.

**Secure APIs**

Public APIs are not available on Neat devices. The only API available is the Web API that is used for remote administration (if enabled) and for a Neat Pad controller/scheduler. In this scenario, authentication uses a JWT (JSON Web Token). The JWT is valid for the lifetime of the Neat product. Lifetime validity of the JWT is required to maintain pairing between a Neat Bar, Bar Pro, or Board (or other Neat device) and the Neat Pad controller/scheduler for the Zoom Room to work without any downtime. This also helps

when there is a reboot, and will allow the Neat Pad to automatically pair with the associated Neat device.

**Vulnerability Management / Security Audits & Pen-testing**

Our security team continuously monitors and analyzes security risks to Neat devices. If we discover any security vulnerabilities that directly affect our products, we will work on resolving those issues quickly and release patches to our customers through our standard software update channels.

Neat engages independent security consultants to conduct audits and assessments of the Neat Bar and Neat Pad devices. Testing is performed on production hardware with production (user) builds of device software. All issues observed are remediated and retested to ensure the devices are secure. A summary report of the latest test can be made available upon request.

## Device Model and Operating System Matrix

The matrix below lists the Neat device model along with the supported version of the Android operating system.

| Device Model | Android OS Version |
|---|---|
| Neat Bar | 10 |
| Neat Board | 10 |
| Neat Pad | 10 |
| Neat Bar Pro | 10 |
| Neat Frame | 10 |
| Neat Board 50 | 10 |
| Neat Center | 13 |
| Neat Bar Gen2 | 10 |
| Neat Board Pro | 10 |

## Contact Us

To report a security concern regarding Neat devices, please visit https://support.neat.no/ or contact us at security@neat.no.

For general queries or sales, you can also talk to one of our team members over chat by visiting our website www.neat.no.