EVOKO NASO

Security Whitepaper
Version 1.0 (006)

EVOKO

ABOUT EVOKO NASO ECOSYSTEM

Evoko's room booking solutions have been used worldwide since 2010 in many industries where security is of the highest level. This list includes governments, banks, and defence contractors. Security is a top priority for Evoko and Evoko Naso has been specifically developed to be a highly secure, enterprise grade solution, following the best global security practices and guidelines.

The Evoko Naso ecosystem is a suite of software applications and a custom-built booking device made to help organizations enable business advantage from workspace optimisation. The Evoko Naso is a fully custom-build hardware design with security in mind with hardened software specifically developed for the Evoko Naso device.

As part of our Testing, Security and Quality Assurance processes, we have also had external security experts perform penetration testing (PEN-testing) on the system before it was released. These tests include a 360-degree assessment of all components included in the solution, e.g.

- Attack Surface Mapping
- Embedded Device testing
- Firmware Reverse Engineering and analysis
- Web, Mobile and Cloud endpoints assessment
- Radio communication security assessment

With the ever-changing threat landscape, building and maintaining a system with the highest security demands is an ongoing process. New attack vectors and tools are invented by hackers all the time. To ensure the most robust cyber-attack resilience, we have alongside our regular internal testing processes, engaged an independent company to carry out security reviews on new software releases and to regularly review hardware installations to ensure ongoing compliance with our security requirements and industry standards. These tests not only simulate real-world installations but, to ensure the highest levels of security, they go even further. With access to all source code, they can search for vulnerabilities and variations that would not be available to a regular hacker. Every new software release improves security further.

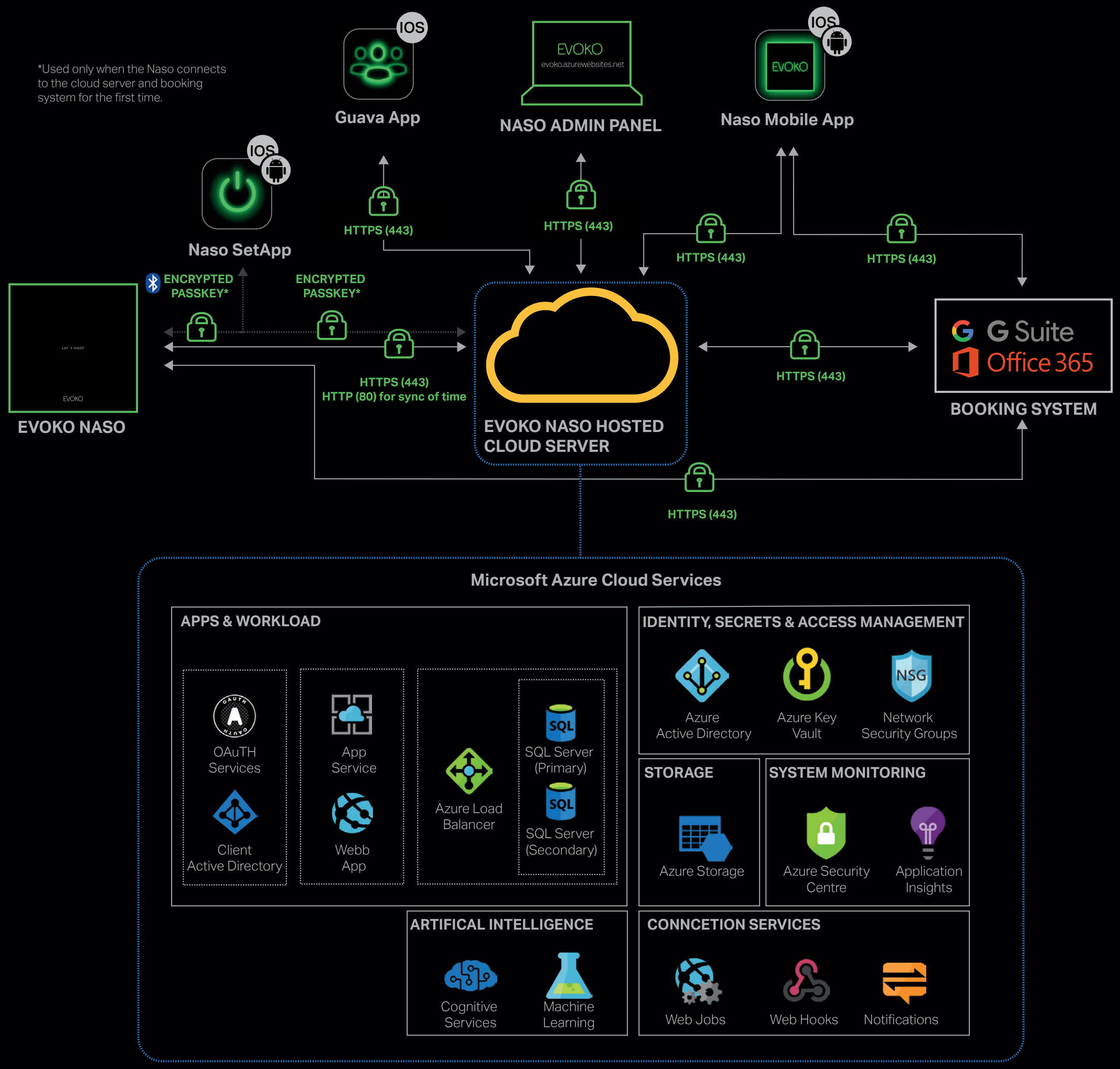
We do not share our PEN-test reports as the testers we use (unlike a hacker) have had access to the actual source code. This is for our internal use only and is sensitive, confidential, and proprietary information that is not shared.

New features, performance improvements, and bugfixes are deployed multiple times per month. While agile, our development cycle relies heavily on a strict system for code quality and security. All code is peer reviewed and requires multiple levels of acceptance on test/staging environments prior to deployment on production.

SYSTEM ARCHITECURE

Network Architecture

The diagram below provides a high-level overview of the Evoko Naso service architecture and external entities connected to our environment.



Ports

All traffic is sent over encrypted port 443 except for Naso initialisation and boot sequences, which require port 80 to sync time prior to switching to port 443.

DEVICE SECURITY

Connectivity

The Evoko Naso devices connect to the network using Ethernet or Wi-Fi. For added security, you can isolate the Evoko Naso installation on a VLAN (having the units on a separate virtual network with restricted access). The Evoko Naso support 802.1x

The devices are powered by Power over Ethernet (802.3at PD type 1, 13W) or by a separate power supply. No other physical ports than RJ45 and DC barrel jack are exposed which eliminates the risk for tampering even on-site.

Setup

On first installation, each device needs to be connected to the Evoko Naso services using the smartphone app Evoko SetApp ("claiming the device"). Not until the device is claimed it will connect to Evoko Naso services or access the network. To claim a device, a user must sign into the Evoko SetApp using their O365 credentials and the device can only be connected to the Evoko Naso services associated with the domain for that O365 account. The claiming process also use two-step verification to avoid Man In the Middle (MITM) attacks.

Data access

The Evoko Naso devices always boot directly into the application, and from within the application there is no way of exiting. The data pushed to the devices is limited to include only the data that displayed on the screen, so the risk of sensitive data being eavesdropped or extracted from the device is effectively removed. The meeting data is stored in the RAM memory of the devices making sure that a stolen unit does not include any retrievable data.

Application architecture

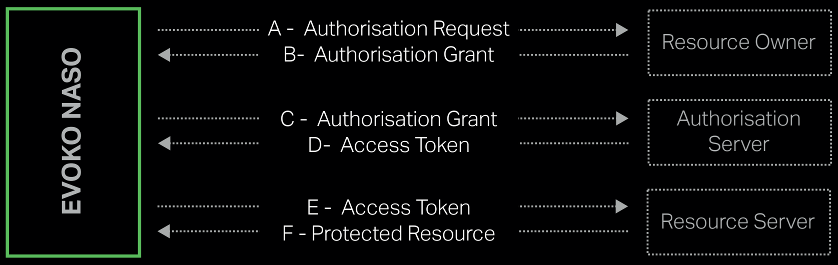
- Presentation layer: This is the graphical user interface of our application that shows information and takes input from users.
- Business logic: We process input from the presentation and data layers and update each layer as required.
- Data layer: The data layer that resides in Evoko Home outside the actual device. All data is maintained on the booking system. We send requests to read data and to update data. For business-critical data the booking system is the "master" which makes the Evoko Home data layer less sensitive. Any data corruption or loss of meeting data would be read back automatically from the booking system.

ENCRYPTION AND AUTHENTICATION

Encryption

Customer data is encrypted when in-transit and at rest. All connections with Evoko Naso's services are encrypted and served through SSL/TLS 1.2. You cannot access the service without using HTTPS. All certificates are verified on both sides with third party authorities.

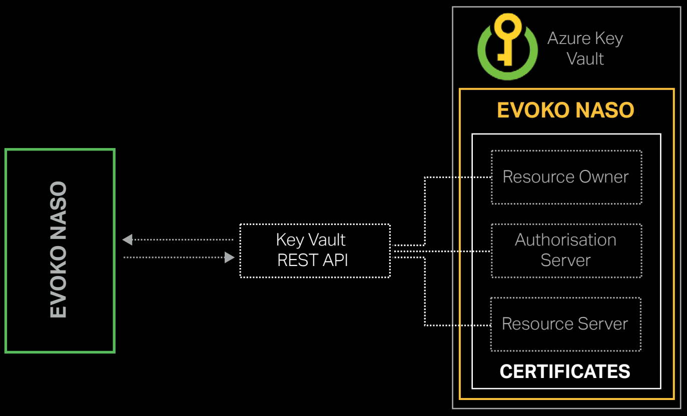
When at rest, customer data is encrypted using a key management system which logs all access automatically. Additionally, passwords are both hashed and salted using one-way encryption, which protect them even in the unlikely event of unauthorised database access. Application credentials are stored separate from the code base. Clients authenticate with Evoko Naso using a token process.



Evoko Naso uses Microsoft Azure Key Vault. Azure Key Vault helps safeguard cryptographic keys and secrets used by cloud applications and services. By using Key Vault, Evoko Naso can encrypt keys and secrets (such as authentication keys, storage account keys, data encryption keys, .PFX files and passwords) by using keys that are protected by hardware security modules (HSMs).

Key Vault streamlines the key management process and enables limited access and encryption of your data.

When a Key Vault certificate is created, an addressable Key Vault and Key Vault secret is also created with the same name. The Key Vault key allows the Evoko Naso services to do key operations and Key Vault secret allows it to retrieve the certificate vale as a secret.



Transparent Data Encryption

Transparent data encryption encrypts all Evoko Naso databases, backups and logs at rest. Evoko Naso uses a service managed key for encryption. Microsoft Azure automatically generates a key to encrypt the databases and manage key rotations.

Authentication

Password authentication is available by default to end users. Evoko Naso supports single sign-on through Microsoft services using Modern Authentication (which encompasses SAML, OATH2, ADFS and MFA).

DATA COLLECTION AND STORAGE

Calendar Syncing

Once an external calendar account is connected to Evoko Naso services, our cloud service will begin to synchronise data with the designated room calendars. In doing so, a subset of your calendar events and their details will be saved in Evoko Naso services.

Evoko Naso services will keep this data in sync with your calendar system. Events booked through Evoko Naso services will similarly synchronise the data back to your calendar service, so that Evoko Naso and the connected calendar stays consistent. Synced event details include:

- Meeting subject
- Start and end times
- Location (e.g. "Conference Room")
- Organiser
- Attendees
- Catering event information
- Online Video Conference links (e.g. Skype or Microsoft Teams link)

We do **not** store event attachments.

Privacy

We take the security of customer data very seriously. You can find more information about this in our privacy policy.

Security Polices

All employees with access to customer data are governed by documented strict security policies covering acceptable use, customer data, and encryption standards.

Disaster Recovery

Application and customer data are stored redundantly at multiple availability zones within Microsoft Azure Data Centres with backups available for immediate recovery,

Backups

Customer data is automatically backed up daily in our data centre. Backups are retained for 30 days to recover in the event of a disaster. They are destroyed automatically at the end of this period.

Data Centre

Evoko Naso is a cloud service, and hosted by Microsoft Azure data centres with the highest level of certifications including ISO27001 and SOC. For more compliance information, please visit **Microsoft Azure Compliance**. The servers are located in the UK.

Decommissioning and Data Removal

All customers' data is stored on Microsoft Azure services, which follows a strict decommissioning policy outlined on the **Microsoft Azure Security, Privacy and Complance Whitepaper**.

For customer-specific data, we will manually remove all identifying calendar data associated with your account from our database. Derivate anonymised data (i.e. "Total events booked on platform this month") will not be removed, as it cannot be linked back to source data. User accounts associated with your organisation may also be removed on request. We retain backups for 30 days, after which time the data will be completely unobtainable.

Uptime & Reliability

We constantly monitor our service performance and have automatic notifications to ensure raid response for servic interrupts. All code is audited and approved by at least two engineers before deploying to production servers. We also monitor updates from the security community and immediately update our systems when vulnerabilities are discovered.