SECURITY WHITEPAPER
BIAMP WORKPLACE
V0425 (002)

APPLICATIONS

- WORKPLACE WEB ADMIN (WORKPLACE.BIAMP.APP)
- WORKPLACE BOOKING APP
- WORKPLACE CONNECT

PRODUCTS

- TESIRA DSP PROCESSORS
- DEVIO CONFERENCE ROOM HUBS
- VOLTERA AMPLIFIERS
- PARLÉ CONFERENCE BARS AND MICROPHONES
- CAMBRIDGE SOUND MASKING SOLUTIONS
- BIAMP NPX PAGING STATIONS
- MAX CONNECT WIRELESS PRESENTATION SYSTEMS
- EVOKO NASO ROOM MANAGER
- EVOKO KLEEO DESK MANAGER

SECURITY WHITEPAPER
BIAMP WORKPLACE
V0425 (002)

ABOUT BIAMP WORKPLACE

Our 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 defense contractors. Security is a top priority for Biamp, and Biamp Workplace has been specifically developed to be a highly secure, enterprise grade solution, following the best global security practices and guidelines.

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 cyberattack 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 bug fixes can be 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.

SECURITY WHITEPAPER
BIAMP WORKPLACE
V0425 (002)

SYSTEM ARCHITECTURE

Network Architecture

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

Ports

Workplace Connect App uses api.evoko.app with network port 443

The Workplace Connect App is installed with Biamp Device Discovery Service. The Biamp Device Discovery Service uses the Multicast DNS protocol with UDP port 5353 as part of the process of discovering Biamp devices on a Local Area Network.

Biamp devices download and upload files using workplacenext0001.blob.core.windows.net with network port 443

Biamp devices using NATS messaging secured via TLS use device0.workplace.biamp.app with network port 7422

Endpoints

Evoko Naso & Kleeo endpoints:

- evoko.app
- biamp.app
- core.windows.net

Workplace web admin:

- evoko.app
- biamp.app
  - workplace.biamp.app
  - licenses.workplace.biamp.app
  - iam.workplace.biamp.app
- core.windows.net
- grafana.net
- sentry.io

SECURITY WHITEPAPER
BIAMP WORKPLACE
V0425 (002)

HARDWARE DEVICES

Data access

The Evoko Naso room managers and Evoko Kleeo desk managers always boot directly into the user application which can not be exited and since the system does not include any other standard user interface. It will not expose any other system UI even in case of severe malfunctioning. The data pushed to the devices is limited to include only the data that is 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.

Evoko Naso

Connectivity

The Evoko Naso room manager connects to the network using Ethernet or Wi-Fi (WPA2-PSK). For added security, isolate the installation on a VLAN (having the units on a separate virtual network with restricted access).

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 Evoko Naso device needs to connect to the Biamp Workplace cloud using the Biamp Booking mobile app. Not until the device is claimed will it connect to the Biamp Workplace cloud or access the network. To claim a device, a user must sign into the Biamp Booking mobile app using their Microsoft O365, Google WS or email credentials and the device can only be connected to the Biamp Workplace cloud associated with that user and belong to that workplace white labeled domains. NFC is used for data transfer of credentials to the device.

Evoko Kleeo

Connectivity

The Kleeo desk manager connects to the network using Wi-Fi, WPA2-PSK. For added security, isolate the installation on a VLAN (having the units on a separate virtual network with restricted access). The Kleeo devices are powered by a single USB-C. The device ports have been disabled for data use and have a sole purpose: To provide electricity to the device. This eliminates the ability of tampering, even directly on the device.

Setup

On first installation, each Evoko Naso device needs to connect to the Biamp workplace cloud using the Biamp Booking mobile app. Not until the device is claimed will it connect to the Biamp Workplace cloud or access the network.

To claim a device, a user must sign into the Biamp Booking mobile app using their Microsoft O365, Google WS or email credentials and the device can only be connected to the Biamp Workplace cloud associated with that user and belong to that workplace white labeled domains. NFC is used for data transfer of credentials to the device.

Encryption and authentication

Encryption

Customer data is encrypted when in-transit. All connections with the Biamp Workplace 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.

Passwords are hashed and salted using industry standard one-way encryption, which protects them even in the unlikely event of unauthorized database access. End user calendar service account credentials are also encrypted at rest.

Application credentials are stored separate from the code base using Microsoft Azure Key Vault. Azure Key Vault helps safeguard cryptographic keys and secrets used by cloud applications and services.

Authentication

Password authentication is available by default to end users. The Biamp Workplace supports single sign-on through Microsoft and Google WS services using modern authentication standards (which encompasses OIDC/OAUTH2 and MFA).

SECURITY WHITEPAPER
BIAMP WORKPLACE
V0425 (002)

DATA COLLECTION AND STORAGE

Calendar Syncing (only for room booking)

Once an external calendar account is connected to Biamp Workplace, it will begin to synchronize data with the designated room calendars. In doing so, a subset of your calendar events and their details will be saved in the Biamp Workplace.

Biamp Workplace will keep this data in sync with your calendar system. Events booked through different tools in Biamp Workplace will similarly synchronize the data back to your calendar service, so that the Biamp Workplace and the connected calendar stays consistent. Synced event details include:

- Meeting subject
- Start and end times Start and end times
- Location (e.g. "Conference Room")
- Organiser
- Attendees
- Online Video Conference links

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 Policies

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 within Microsoft Azure Data Centres with backups available for immediate recovery,

Backups

Customer data is continuously backed up and can be restored back to any point-in-time within the retainment time. Backups are retained for 7 days to recover in the event of a disaster. They are destroyed automatically at the end of this period.

Data Centre

Biamp Workplace is a cloud service, and hosted by Microsoft Azure data centers 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 United States.

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 Compliance 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 organization may also be removed on request. We retain backups for 7 days, after which time the data will be completely unobtainable.

SECURITY WHITEPAPER
BIAMP WORKPLACE
V0425 (002)

Uptime & Reliability

We constantly monitor our service performance and have automatic notifications to ensure rapid response for service interruptions. 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.

REQUIRED MICROSOFT GRAPH PERMISSIONS (FOR CALENDAR INTEGRATIONS ONLY)

To provide a seamless, secure, and efficient room booking experience, Biamp's calendar integration requires minimal yet essential permissions from Microsoft Graph API. These permissions enable core functionality while adhering to strict data minimization principles. Our integration requires access only to specific data elements necessary for booking operations, and synchronizes calendar information only after explicit user authorization.

The permissions outlined below represent the minimum access requirements needed to deliver reliable room booking capabilities while maintaining robust security and privacy standards.

Calendar.ReadWrite

This permission allows us to add and modify events in calendar. Essential for the functionality of both the Workplace App and Biamp Devices.

Place.Read.All

Required to discover available resources in your system for connecting to Biamp devices.

Important notes:

- Calendar information is only synced after an active connection is established between a resource and a calendar
- We only track changes in calendars that you specifically choose to connect.
- Before connection, we only store three basic fields from the Places API:
    - id
    - email
    - displayName

User.Read.All

Needed to identify existing user calendars in your system for Biamp account connections.

Important notes:

- Calendar event information is never synced until a user registers an account in BWP.
- Before registration, we only store five basic fields from the Users API:
    - id
    - email
    - displayName
    - userPrincipalName
    - etag

MailboxSettings.Read

Used solely to read the timeZone field. This ensures calendar events created through Biamp Workplace admin or App are set in the appropriate time zone for both users and places.