

VoxGuard: Turvallinen tiimikommunikaatio ja hätävastealusta, tietoturva

VoxGuard on huippuluokan mobiili viestintäalusta tiimeille, jotka tarvitsevat välitöntä, turvallista ja luotettavaa koordinoitua haastavissa ympäristöissä. Oli kyseessä sitten hätävaste, suuri tapahtuma tai yritysviestintä.



Miksi VoxGuard?

Kun tiiminne viestintä on kriittinen, oli kyseessä päivystys, operatiivinen johtaminen tai arkaluonteinen tiedon välitys, VoxGuard on kumppani, joka ei petä. Yhdistämme tietoturvan saumattomaan käyttökokemukseen.

Tehtävämme on yksinkertainen: teidän tietonne ovat teidän tietojanne. Aina.



Monikerroksinen suojaus

Riippumattomat turvakerrokset varmistavat, että yksittäisen kerroksen pettäminen ei vaaranna kokonaisuutta.



Vähimmäisoikeuksien periaate

Käyttäjät ja palvelut saavat vain sen, mitä tehtävänsä vaativat—ei enempää.



Yksityisyys ensin

Keräämme vain palvelun toiminnan kannalta välttämättömät tiedot.



Täysi läpinäkyvyys

Järjestelmänvalvojallanne on kattavat hallintatyökalut ja audit-näkyvyys.

Viestintä on suojattu, siirrossa ja levossa

Salaus kaikissa tiedonsiirroissa

Jokainen bitti on suojattu modernilla TLS-salauksella (versio 1.2+), hyödyntäen alan vahvinta AES-256-algoritmia. Estää salakuuntelun, tietojen väärentämisen ja man-in-the-middle -hyökkäykset.

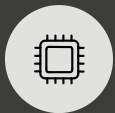
- Sertifikaattien kiinnitys (certificate pinning) tuettu hallituissa laitteissa
- Kaikki API-pyynnot todennetaan lyhytikäisillä tokeneilla
- Lunastetut tokenit mitätöidään välittömästi

Tiedot turvassa

Kaikki tietokannat ja objektitallennus on suojattu.

- Rivitason pääsynhallinta (RLS) — käyttäjät näkevät vain omat tietonsa
- Salatut varmuuskopiot tiukoilla säilytyskäytännöillä
- Jokainen palautustoiminto dokumentoitu ja jäljitettävissä

Reaaliaikainen ääni



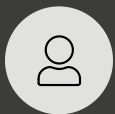
Ammattimainen mediavirtojen suojaus

Push-to-talk -puhelunne on suojattu AES-pohjaisella salauksella. Äänenne kuulee vain se ryhmä, jolle se on tarkoitettu—ei välikäsiä, ei sivukuuntelijoita.



Päästä päähän -salaus saatavilla

Korkeampia tietoturvavaatimuksia omaaville organisaatioille tarjoamme konfiguraatioita, joissa äänivirrat on salattu päästä päähän.



Tiukka pääsynhallinta

Vain todennetut käyttäjät oikeilla ryhmäoikeuksilla voivat liittyä kanaville. Pääsynvalvonta toteutetaan sekä sovellus- että palvelintasolla.



Identiteetti ja pääsynhallinta

Vain oikeat ihmiset oikeaan paikkaan



Vahva todennus

Standardipohjainen sähköposti/salasana-todennus tiukoilla käytännöillä. Salasanakäytännöt määriteltävissä organisaationne tarpeiden mukaan.



Tarkkarajainen valtuutus

Roolipohjainen ja ryhmäpohjainen käyttöoikeuksien hallinta. Jokainen toiminto on valtuutettu—ei oikoteitä.



SSO ja monitekijätodennus

Single Sign-On (SSO) ja monitekijätodennus (MFA) tuettu identiteettipalveluntarjoajastanne riippuen. Yksittäinen kirjautuminen, moninkertainen suoja.



Token-hygienia

Lyhytikäiset istuntotokenit ja turvalliset päivitysvirrat minimoivat vuotaneen tokenin vaikutuksen. Lunastetut tokenit mitätöidään välittömästi.

Sovellus- ja laiteturva alusta alkaen

Turvalliset oletusasetukset

VoxGuard tallentaa minimaalisen määrän tietoa laitteelle.
Arkaluonteiset istuntotokenit säilytetään käyttöjärjestelmän suojatussa tallennustilassa.

- iOS Keychain / Android Keystore — ei tekstitiedostoissa
- Vähimmäisoikeudet: mikrofoni puheelle, sijainti karttaominaisuuksille
- Ei mystisiä käyttöoikeuspyyntöjä

Ajonaikaiset suojaukset

Kaikki käyttäjäsyöte validoidaan ja yleisimmät mobiili- ja web-uhkat on torjuttu.

- XSS, CSRF ja SQL-injektio torjuttu
- Deserialisointi suojattu
- Parametrisointi ja kehyssuojaukset käytössä

Infrastruktuuri, karaistu pilvipohja



Vankka perusta

Verkon segmentointi, palomuuuri ja vähimmäisoikeuksien IAM-roolit. Jokainen komponentti on eristetty ja suojattu.



Jatkuva valvonta

Kaikki tietoturvaan liittyvät tapahtumat lokitetaan ja poikkeavuuksista hälytetään automaattisesti.



Turvallinen kehitys

Koodikatselmoinnit, riippuvuuksien tietoturvascanaukset ja CI/CD-putken automaattiset tarkistukset. Turvallisuus on osa jokaista sprinttiä.



Salaisuuksien hallinta

API-avaimet ja salausavaimet tallennetaan hallittuihin salaisuusvarastoihin. Jokainen pääsy on auditointivalmis.

Vaatimustenmukaisuus ja yksityisyys

Tietojen sijainti

Tietonne tallennetaan EU:n sisällä oleviin pilvipalveluihin. Alueellisista sijoitusvaihtoehtoista voidaan keskustella erityisvaatimusten mukaisesti.

Yksityisyys sitoumuksemme

- Emme myy tai jaa tietoja kolmansille osapuolille
- Emme seuraa käyttäjiä sivustojen välillä
- Emme rakenna profiileja myyntiä varten
- Tietosi ovat tietojasi. Aina.

Säädösten noudattaminen

VoxGuard on suunniteltu noudattamaan yleisiä turvallisuus- ja yksityisyysodotuksia, mukaan lukien GDPR:n periaatteet.

Muodollisista sertifikaateista ja erityisvaatimuksista voidaan keskustella tapauskohtaisesti.

Jaettu vastuu, kumppanuus, joka toimii

Tietoturva on tiimityö. VoxGuard vastaa omasta osuudestaan, ja te vastaatte organisaationne osuudesta.

VoxGuardin vastuu

Komponentti	Vastuualue
Sovellus	Koodi, arkkitehtuuri, suojausmekanismit
Taustajärjestelmät	Palvelimet, tietokannat, infrastruktuuri
Salaus	Siirrossa automaattisesti
Konfiguraatio	Palvelun asetukset ja päivitykset
Valvonta	Operatiivinen lokitus ja hälytykset

Teidän vastuunne

Komponentti	Vastuualue
Laitteet	Mobiililaitteiden hallinta ja päivitykset
Identiteetti	SSO/MFA-konfiguraatio
Verkko	Organisaation verkkokäytännöt
Käyttöoikeudet	Sisäinen pääsynhallinta ja roolitus

Usein kysytyt kysymykset

Onko viestintä päästä päähän salattua?

Äänivirrat on salattu siirrossa oletuksena (AES-pohjaisella salauksella). Päästä päähän -salaus on saatavilla organisaatioille, joilla on erityisiä tietoturvavaatimuksia. Ota yhteyttä, niin kerromme lisää.

Voitteko integroitua SSO:hon ja MFA:han?

Kyllä. Single Sign-On (SSO) ja monitekijätodennus (MFA) ovat tuettuja standardipohjaisten identiteettipalveluntarjoajien kautta.

Missä tietomme tallennetaan?

Tiedot tallennetaan salattuihin pilvitietokantoihin EU:n sisällä. Alueellisista sijoitusvaihtoehtoista voidaan sopia erikseen.

Onko järjestelmänvalvojilla audit-näkyvyys?

Kyllä. Kaikki kirjautumiset, käyttöoikeuden myönnykset ja tietojen muutokset lokitetaan. Voimme räätälöidä kojelautoja ja vientiraportteja tarpeidenne mukaan.

Mitä tapahtuu, jos laitteeni katoaa tai varastetaan?

Istuntotoken voidaan mitätöidä etähallinnan kautta. Sovellus tallentaa arkaluontoista tietoa minimaalisesti käyttöjärjestelmän suojatussa tallennustilassa.

Voiko kolmannet osapuolet päästä käsiksi tietoihini?

Ei. Emme myy, vuokraa tai jaa tietojanne kolmansille osapuolille. Ainoa poikkeus on lakisääteinen tietopyyntö.

VoxGuard, tietoturva on perusta

Organisaationne on suojattu kerroksellisella turvallisuudella.



Salattu viestintä — kaikkialla



AES-256 salaus siirrossa



Vahva identiteetti: todennus, valtuutus, auditointi



Hienojakoinen pääsynhallinta



Karaistu pilvipohja, valvonta ja palautus

Haluatteko keskustella tarkemmin? Ota yhteyttä, niin suunnittelemme yhdessä tarpeisiinne sopivan ratkaisun.