Security Overview

Before starting Rhombus Systems, the founding team created Mojave Networks, a cybersecurity company acquired by Sophos. With decades of cybersecurity experience, the Rhombus design and engineering workflows all begin with a security-first approach and a zero-trust theme to prevent internal and external threats.

Rhombus complies with many of the requirements listed for NIST 800-171, ITAR, ISO27001, and CMMC Level 3 certification. However, as of today, there are no formal certifications available.

In this document, we will outline all of the security measures and best practices employed by Rhombus Systems to protect customer privacy and data. These security measures have been followed since the inception of Rhombus.

Table of Contents

Proprietary and Confidential.
All specifications are subject to change without notice.
Copyright Rhombus Systems Inc. All rights reserved.

Identity Management and Access Control

- Centralized Identity + ACL via OKTA
- 2FA Enforced
- VPN required for all internal services
- Access to internal resources restricted by group policies
  - Sales
  - Developer
  - Support
  - Camera SSH (used only in unprecedented cases)
    - Locked down to CTO, Chief Architect, VP of Eng
    - Each SSH session requires an extra 2FA check

Employees

- Continuous phishing and cybersecurity best practices training
- Workstations with Encrypted Disk, AV, and VPN
- Workstations managed via MDM
  - Software install management
  - Remote wipe
  - Remote locate
- Physical office access protected with Rhombus cameras + badge system

---

Cloud Infrastructure

- Hosted on Amazon AWS with well defined VPC's
- Internal + External access isolated
- AWS Console restricted to select team members
- Video/Audio/Images stored in S3 encrypted with SSE-KMS
- Data access only available to Rhombus servers
- No employee has access to any customer video/audio data
- Access to Rhombus servers restricted behind VPN to select employees

Proprietary and Confidential.
All specifications are subject to change without notice.
Copyright Rhombus Systems Inc. All rights reserved.

Cloud Infrastructure Cont.

- All Databases are fully encrypted
- Sensitive information is fully encrypted
- Passwords are stored using a one-way strong hash
- All cloud data is continuously backed up
- All actions are fully audited
- Anomalous login and access attempts are monitored and reported instantly to customers
- Customers can view login/session activity and log out any sessions on any device at their own will

---

Internal Infrastructure

- Hosted on Amazon AWS with separate VPC from the Customer Cloud VPCs
- No WAN Access
- Access only via VPN
- All actions are fully audited
- Anomalous activity and login attempts monitored and reported
- PKI – completely isolated internal server with access available only to the CTO and VP of Engineering

---

Hardware

- Physical access via the hardware UART port is locked
- Data is stored in a fully encrypted disk with LUKS AES-256 and rotating keys
- All communication with the cloud is over TLS 1.2 using a 128 bit AES cipher
- Data tamper and deletion is not possible
- Hardware security audits completed by third party security firmware and are available upon request

Proprietary and Confidential.
All specifications are subject to change without notice.
Copyright Rhombus Systems Inc. All rights reserved.

Firmware

- Signed and verified secure firmware updates
- All TCP connections use TLS1.2/128 bit AES cipher
- All connections enforce mutual authentication
- Man in the middle (MITM) attack protection
- Firmware has locked down certificate trust store
- Bluetooth channel fully encrypted with custom encryption protocol
- Firmware security audits carried out by third party firm and available on request

---

Support / Partners

- No god-mode or super admin account exists for accessing customer console and/or data
- Support / Partner can only access a customer account with access approval by the customer
- This access can be revoked at any time by the customer
- Support / Partner access is fully audited and can be viewed by the customer at any time in the audit logs
- For more information about support / partner access, view the in-depth blog post

---

Incident Management

As soon as Rhombus becomes aware of a security breach involving unauthorized access, loss or tamper of customer data, the effected parties are notified within 24-48 hours with all necessary details outlining the breach and any action items, if any, that are required on the customer's part.

Product Security

For additional information regarding product security, view the security page on the Rhombus website

Proprietary and Confidential.
All specifications are subject to change without notice.
Copyright Rhombus Systems Inc. All rights reserved.