SIGNALWIRE CLOUD AND STACK SECURITY

SignalWire is a leading provider of real-time communications technology, powering a wide range of mission-critical services across various industries. From healthcare to video doorbells to online communications providers, SignalWire's technology forms the backbone of these services. We understand the importance of security and privacy in today's digital landscape and strive to ensure that all of our decisions reflect the regulations and needs of the global community.

As a responsible and reliable partner, we understand the need for transparency and visibility when it comes to our security and software development processes. This document is intended to provide an in-depth look into SignalWire's security protocols, best practices, and compliance measures. It also serves as a valuable resource for our customers and partners as they work to improve and secure the applications they build with SignalWire. By providing this level of detail and insight, we hope to foster trust and confidence in the security and reliability of our technology.

Engineering teams at SignalWire are continually working to create a best-in-class product offering. The following guidelines help us to organize and achieve this goal at every stage of product development:

Internal Security Designs

SignalWire engineers maintain a constant vigilance to ensure the security of our products with activities including:

- Engineering security reviews before, during, and after product development
- Regular vulnerability scans and tests performed by independent third parties
- Targeted internal security audits and permissions review by senior Engineering personnel
- Additional threat assessment and mitigation processes

Static Code Analysis

SignalWire developers use automated static code analysis tools to identify potential vulnerabilities and security issues within the codebase. These tools can detect issues such as SQL injection, cross-site scripting, and other common web application vulnerabilities.

Dependency Management

SignalWire uses a dependency management system to ensure that all third-party libraries and packages used in the codebase are up-to-date and free of known vulnerabilities. This includes regular updates and security patches to ensure that any known vulnerabilities are addressed as soon as they are discovered.

Threat Intelligence

SignalWire uses threat intelligence feeds to stay informed about the latest threats and vulnerabilities. This includes monitoring industry-wide security advisories, feeds from security researchers, and subscribing to threat intelligence feeds from leading security vendors.

In addition to monitoring these external sources, SignalWire also employs Intrusion Detection and Prevention Systems (IDS/IPS) software to proactively detect and prevent potential threats on our network. This software continuously monitors our network traffic, looking for patterns and anomalies that may indicate a security breach. The software is configured with a set of rules and signatures that are continuously updated to detect the latest known threats. Our team also monitors the software logs and alerts on a daily basis to detect and respond to any potential threats.

Advanced Encryption

SignalWire engineers implement advanced encryption methods such as HTTPS and secure websockets to ensure that all data transmitted between the client and our servers is encrypted and secure. We also use advanced encryption methods such as AES-256 and RSA-4096 to protect sensitive data stored on our servers. SignalWire supports TLS 1.2, 1.3 to encrypt network traffic between the customer application and SignalWire.

Encryption at Rest

SignalWire uses encryption at rest to protect data stored on disk. This includes using industry standard encryption algorithms such as AES to encrypt customer data and using key management systems to securely store and rotate encryption keys.

Continuous Security Improvements

Our engineers are constantly researching and implementing the latest security technologies and best practices to improve the security of our products. We regularly conduct security assessments and penetration testing to identify and address any potential vulnerabilities in our systems.

Account Security Measures

SignalWire implements a variety of advanced account security measures such as multi-factor authentication, password hashing, and user session management to protect our clients’ sensitive information.

Vendor Security Audits and Certifications

The cloud hyperscalers that SignalWire uses are regularly audited by independent third-party organizations to ensure that they comply with the latest security standards and regulations. This includes certifications such as SOC 2, ISO 27001, and PCI DSS.

In addition to its hyperscalers, SignalWire itself is certified under SOC 2, ISO 27001, and PCI-DSS frameworks, all of which require regular audits. SignalWire is responsible for maintaining those certifications as part of its ongoing security commitments. By leveraging these certifications, SignalWire is able to provide its customers with an added layer of security and assurance that their data is being protected to the highest standards.

Security Awareness Program

We have implemented a comprehensive security awareness program to ensure that all personnel are aware of the importance of security and understand their role in maintaining the security of our systems and data. This program includes regular communications and education on security topics and best practices, as well as simulated phishing attacks to test and reinforce employee awareness of potential security threats.

Access Management

Access to infrastructure, networks, and data is tightly controlled to only those persons or services that require direct access. Encrypted overlay networking helps to prevent any possibility of data leakage during transmission along with mandatory SSL encryption of all control plane and messaging bus protocols. Production services are only accessible through a tightly curated, audited list of employees utilizing only certificate authentication for login or deployment scenarios. This ensures that only authorized personnel can access our infrastructure and customer data. All identity is centralized and managed by an IAM.