C1 Cloud Calling Voice Traffic Filtering

As voice-based threats continue to evolve, organizations require a robust VoIP security solution to protect their communication channels.

C1 Voice Traffic Filtering, an add-on service to C1 Cloud Calling, provides multi-layered protection against robocalls, spoofed calls, scams, spam storms, vishing, smishing, and social engineering attacks, ensuring secure, reliable, and uninterrupted voice communications. It allows your organization to meet regulatory requirements and prevent unauthorized access while increasing employee productivity by reducing time wasted on spam and fraudulent calls.

Key benefits

- **Comprehensive voice security:** Five-layered protection against a wide range of voice-based threats
- **STIR/SHAKEN compliance:** Verifies caller legitimacy to prevent spoofed calls using the STIR/SHAKEN standard
- **Dynamic threat intelligence:** Continuously updated proprietary database of known threats
- **Customizable call filtering:** Organization-specific allow/block lists for maximum control
- **Voice CAPTCHA screening:** Additional vetting for suspicious calls before they reach the user

How it secures VoIP calls

1. Traffic monitoring and analysis: C1 continuously monitors inbound and outbound voice traffic on an organization's telephony network. It uses AI-driven analytics, machine learning, and rule-based heuristics to evaluate the legitimacy of calls.

2. Identification and categorization: Calls are assessed and categorized based on multiple risk factors, including:

- Known spam sources (e.g., blacklisted numbers, robocall databases).
- Call patterns and behaviors indicative of scams or vishing.
- Anomalous call volumes that may indicate a TDoS attack.

The system distinguishes between legitimate business calls and potential threats.

3. Filtering and blocking unwanted traffic: Once a call is identified as spam or malicious, C1 applies filtering policies, which may include:

- **Blocking:** Completely rejecting calls from high-risk sources.
- **Flagging:** Marking suspicious calls for further review.
- **Routing or quarantining:** Sending suspect calls to a designated system for manual verification.

Organizations can customize filtering rules to meet their specific security needs.

Features

Carrier-level call authentication
Analyzes STIR/SHAKEN data to detect spoofed and manipulated caller IDs

Proprietary threat database
Maintains a continuously updated list of known robocallers and fraudsters

Advanced threat radar
Uses AI-powered analytics to detect patterns associated with nefarious calls

Custom allow and block lists
Enables organizations to whitelist or blacklist specific numbers

Voice CAPTCHA technology
Routes high-risk calls through interactive voice screening for verification

Availability

Voice Traffic Filtering is available as an add-on for C1 Cloud Calling and as a direct sale for bring your own carrier (BYOC) SIP customers.

Learn more

Protect your business with multi-layered protection against robocallers and fraudsters.

For more details about C1 Cloud Calling Voice Traffic Filtering, contact us today!

C1, the global technology solutions provider, transforms businesses by creating connected experiences that shape the future. With more than 6,000 customers, C1 empowers industries through secure, innovative technologies, collaborating with leading partners to deliver total lifecycle solutions. Learn more at **onec1.com**.