SecureLogix

TOPICS

Call Filtering Software

Learn about call filtering software solutions, including how they work, key benefits, and advanced features for protecting business communications.

< Previous Topic Next Topic >

As business telephone lines are increasingly targeted by robocalls, scams, and fraud, call filtering has become critical to protecting organizations and their employees. Call filtering solutions are designed to automatically block unwanted or malicious calls that could compromise security and reduce productivity. While traditional approaches to call filtering and authentication have been complex and costly, new technologies are paving the way for smart, efficient, and affordable filtering that can scale easily across an entire enterprise.

What Is Call Filtering Software?

Call filtering software is a form of call security technology that screens incoming phone calls and allows, blocks, or redirects them based on pre-defined rules and criteria. By analyzing each incoming call, these software solutions can identify spam, telemarketing, fraud, and other unwanted calls and automatically prevent them from connecting. Call filtering software has evolved from simple caller ID systems to sophisticated technology that leverages machine learning, real-time databases, and call authentication protocols.

Threats Addressed By Call Filtering Software

Call filtering solutions are designed to protect businesses from several critical threats.

- **Robocalls and Spam Calls**

  Robocalls are automated calls generated by computer systems that can dial thousands of numbers in a few seconds. These calls are typically used for telemarketing, political campaigns, or surveys, but they are also the favorites of fraudsters and cyber criminals. The sheer volume of robocalls is a nuisance, and they can cause significant trouble when a user is duped into visiting a malicious website or placing a call to a fraudulent number.

- **Phishing and Social Engineering Scams**

  Phone phishing threats, also known as voice phishing or "vishing" scams, involve callers posing as representatives of legitimate organizations like banks, tech support, or government agencies to trick individuals into divulging sensitive information like account numbers, passwords, or Social Security numbers.

- **Caller ID Spoofing**

  In caller ID spoofing, scammers make their calls appear as if they're coming from a trusted source like a local business, government agency, or a familiar contact. This trust increases the likelihood of a scam's success.

How Call Filtering Software Works

Call filtering software uses a variety of techniques to identify and block potentially unwanted callers.

Caller ID Authentication

Call filtering software analyzes the caller ID data for incoming calls to determine if the number belongs to a known contact, a reputable source, or if it's of

suspicious origin. To combat caller ID spoofing, filtering software may rely on STIR/SHAKEN (Secure Telephony Identity Revisited/Signature-based Handling of Asserted information using toKENs), a critical protocol that digitally signs and verifies the origin of a call to prevent cyber criminals from using fake caller IDs.

Real-Time Threat Intelligence

If a caller ID is determined to be authentic, call filtering software may check it against databases of known spam, telemarketing, and scam numbers. These databases are maintained by telecom providers, security firms, government agencies, and other organizations.

Machine Learning And AI

Sophisticated call filtering software incorporates advanced machine learning algorithms and artificial intelligence to identify suspicious calls by analyzing call patterns, caller behavior, and contextual clues. For example, if an unknown number is rapidly calling multiple users within a short timeframe, the software might flag it as spam even if it's not yet in a database. AI-powered algorithms can learn from past data to better identify and block emerging threats.

User-Defined Settings

Most call filtering solutions allow businesses to create "whitelists" of trusted contacts and "blacklists" of blocked numbers. Many call filtering technologies allow users to set filtering thresholds. Some users may choose a low threshold to avoid inadvertently missing client calls mistakenly identified as spam, while others may choose a high threshold to block all telemarketing and robocalls. Call filtering software also typically allows users to choose to block calls, redirect to voicemail, or flag certain calls for review.

The Advantages Of Call Filtering Software

Deploying effective call filtering software offers clear advantages for businesses.

- **Stronger Security**

  Call filtering software provides an essential layer of security by proactively blocking calls from spammers, scammers, and suspicious numbers. By preventing these calls from reaching employees or contact center agents, filtering software significantly reduces the potential for phishing scams and fraudulent activity.

- **Greater Efficiency**

  Call filtering software is a powerful tool for reducing disruptions to employee routines and boosting productivity. By minimizing the number of spam or scam calls received each day, filtering software prevents disruptions to workflow and allows employees to focus on important calls.

- **Better Customer Experiences**

  By preventing telemarketing, spam, and robocalls from tying up phone lines, filtering software increases the ability of legitimate users to quickly reach their desired contacts.

- **Lower Cost**

  Effective call filtering technology saves money by preventing employees' time from being wasted and by avoiding the significant costs associated with data breaches, compliance failures, and loss of customer trust.

Limitations Of Traditional Call Filtering Software

While traditional call filtering software offers some protection, it has not been a foolproof solution for several reasons.

- **Reliance on Static Databases**

Cyber criminals and scammers change phone numbers frequently, causing static blacklists to quickly become out of date and making it harder for telephony threat intelligence databases to stay current.

- **Limitations of STIR/SHAKEN**

  The STIR/SHAKEN protocol is only effective in networks that have adopted the protocol — anytime a call crosses to a network that doesn't use the protocol (such as an international network), the protection is lost. Additionally, while the protocol is effective at preventing caller ID spoofing, it doesn't protect against phishing or social engineering attacks.

- **False Positives and Negatives**

  Traditional filtering software often has a higher rate of false positives resulting in legitimate calls being blocked, and false negatives that let spam calls through.

- **High Costs**

  Traditionally, the expense to authenticate inbound calls has been quite high, involving expensive per-call charges and costly security interrogations.

SecureLogix: Sophisticated Call Filtering Software

SecureLogix provides call branding, security, and authentication solutions designed to solve call security and trust issues while reducing costs and maximizing revenue. For 20+ years, we've profiled, tracked, and defended customers against evolving schemes and threats that plague contact centers and unified communications networks. With highly effective technology and the most skilled team in the industry, we offer solutions that monitor and protect some of the world's largest and most complex contact centers and voice networks.

SecureLogix® Call Defense™ System

Call Defense™ System is an award-winning voice channel and call protection technology that sits at the edge of your voice network, acting as a call firewall to effectively identify and block unwanted calls. As a highly effective call filtering software solution, Call Defense™ System effectively blocks robocalls, spam, spoofing and impersonation calls, social engineering calls, toll fraud and call pumping attempts, and other unwanted calls.

With Call Defense™ System, you can:

- Enforce unified security policies across the enterprise.
- Bring greater visibility into telephony activity.
- Respond to malicious or unwanted calls with alerting, blocking, and/or redirection.
- Rely on a Call Intrusion Prevention (IPS) system to detect the pattern of attacks and identify anomalies.
- Enforce call volume thresholds and traffic velocity limits.
- Improve reporting with voice network usage/Call Detail Record (CDR) analytics and attack/fraud forensics.

Orchestra One™ Call Authentication Service

SecureLogix Orchestra One™ quickly verifies and authenticates every inbound call with automated, cloud-based call authentication and spoofing detection services. With this call filtering software solution, you get a solution that dramatically lowers the cost of call authentication while improving filtering effectiveness.

Orchestra One™ provides:

- **Low-Cost Authentication**

  To minimize the cost of call authentication, Orchestra One™ employs multiple zero-cost low-cost metadata services to authenticate each call at its lowest possible price.

- **High-Value Risk Scores**

  By analyzing thousands of call details along with real-time carrier network metadata (including STIR/SHAKEN when present), Orchestra One™ delivers a rigorous verification/authentication score for each call to effectively filter out unwanted and malicious calls.

TrueCall™ Spoofing Protection Service

SecureLogix® TrueCall™ Spoofing Protection Service is an outbound calling solution that identifies and blocks spoofed calls attempting to use your corporate calling numbers to impersonate your brand. This network API-integrated spoofed-call filtering software is the industry's strongest and most secure approach to spoofing prevention. It integrates with major wireless carriers and their call analytics vendors to only allow legitimate out bound calls to pass through.

With TrueCall™, you can:

- Prevent malicious actors from spoofing your enterprise calling numbers, protecting your reputation score.
- Increase call answer rate by protecting your legitimate outbound enterprise calls from being labeled as fraud or spam.

FAQ

Q: What Is Call Filtering Software?

Call filtering software is a tool designed to screen and manage incoming calls, helping companies avoid spam, robocalls, and potential scam calls that can disrupt operations. This software typically relies on techniques like caller verification, blacklisting, and customizable filtering rules to protect employees and improve productivity by reducing unwanted interruptions. Many call filtering

solutions also offer analytics and reporting tools, enabling companies to track call patterns and identify potential security threats.

Q: How Does Call Filtering Software Identify Spam Or Scam Calls?

Call filtering software identifies spam or scam calls by cross-referencing incoming numbers with databases of known spam, scam, and telemarketing numbers. Advanced systems may use machine learning to detect patterns associated with spam behavior and even analyze the call's content if it is answered.

Q: Does Call Filtering Software Block Important Calls By Mistake?

While most call filtering software is designed to prioritize legitimate calls, there can occasionally be false positives. Many systems allow users to review blocked calls or adjust settings to prevent important calls from being filtered out. Adding trusted contacts to a whitelist can further ensure that essential calls come through.

Q: Does Call Filtering Software Prevent Caller ID Spoofing?

Some call filtering solutions, especially those with STIR/SHAKEN technology, can detect and prevent calls from spoofed numbers. However, caller ID spoofing is complex, and effectiveness may vary. Advanced filters are better equipped to identify spoofing by verifying caller authenticity.

Additional Reading

- Call Answer Rate
- Call Authentication
- Call Filtering
- Caller ID Spoofing

- Toll Fraud

#call filtering #call security #cybersecurity

< Previous Topic Next Topic > All Topics

Webinars
White Papers

ETM System
Nova Cloud Architecture
PolicyGuru Controller
Red List Database
Vox Research Lab

Contact
Support
Partners

IN THE NEWS

As Vishing Gains Momentum, It's Time To Fight Back

Next-Gen Phishing: The Rise Of AI Vishing Scams

Poilievre To Force Banks, Telecoms To Block Scams Targeting Seniors

Smishing Triad Fuels Surge In Toll Payment Scams In US, UK

Ransomware Incidents Increase By 132%, Vishing By 1,633%

Attorney General Bonta Defends Rule To Stop The Flood Of Robocalls

Open Source Privacy Policy Trademarks

website by Lightning Jar