Cada llamada con su evidencia.

El SIP VAULT guarda la señalización SIP, las estadísticas RTP/RTCP, los logs de OpenSIPS y el CDR de cada llamada en una bóveda por cliente, con prueba de integridad e indexada por Call-ID. El ingeniero abre la evidencia en un clic; la IA lee los mismos datos por MCP.

Call-ID	Menos de 30 s	eBPF	MCP
una clave, toda la evidencia	para el diagnóstico con IA	agente Go sin dependencias	dashboard e IA, mismos datos

EL DESAFÍO

El soporte es el impuesto silencioso del SIP

Recolectar antes de analizar

Reproducir el problema y reunir trazas y logs consume la mayor parte del tiempo de troubleshooting.

SSH, grep y ngrep

Sin un índice por llamada, la investigación se hace a mano y puede llevar una hora de un ingeniero sénior.

Personal escaso

Los ingenieros SIP calificados son difíciles de encontrar y más difíciles de retener, y un mal soporte hace que el cliente se vaya.

LA SOLUCIÓN

Cómo lo resuelve el SIP VAULT

El CDR como puerta de entrada

Cada fila del CDR tiene el enlace VAULT: un clic abre el pcap, los logs y las estadísticas RTP de esa llamada. Sin SSH, sin grep.

Calidad por tramo

MOS, jitter, pérdida y latencia del tramo UAC y del UAS lado a lado, con el tramo degradado señalado antes de que alguien mire.

Acceso de primera clase para la IA

El mismo contrato (FastAPI + MCP) sirve al dashboard y a la IA. La skill /troubleshoot-call busca, correlaciona, analiza y entrega un post-mortem en Markdown con la evidencia.

Bóveda con prueba de integridad

Bucket S3 por cliente y evidencia con hash de contenido: cuando la llamada entra en la bóveda, se puede probar que nadie la editó después.

DIFERENCIALES

Por qué el SIP VAULT

1. **De una hora a segundos**
   Lo que llevaba cerca de una hora de SSH, grep y ngrep, el /troubleshoot-call lo resuelve en menos de 30 segundos.
2. **Abierto en el borde**
   El sipvault-agent es open source (Apache 2.0) y el protocolo de transmisión está documentado: use el servidor SipPulse o construya el suyo.
3. **Respetuoso por defecto**
   Solo diálogos INVITE, y el payload RTP nunca se decodifica. El agente solo se comunica con el servidor que usted configure.
4. **Nada nuevo expuesto**
   Una conexión TCP saliente en el puerto 9060 y un buffer local de 100 MB: una caída de red no pierde datos.

MODELOS

Tres formas de usarlo

SaaS

Alojado por SipPulse

Bucket S3 por cliente, con dashboard y MCP incluidos.

Open source

Agente Apache 2.0

Ejecute el sipvault-agent contra el servidor SipPulse o construya su propio receptor.

On-premise

Operadores

La bóveda completa dentro de su propia infraestructura, bajo consulta.

RECURSOS

Lo que trae cada llamada

Evidencia capturada

- Diálogo INVITE completo (pcap)
- RTCP de emisor y receptor
- RTP: MOS, jitter, pérdida, latencia
- Logs de OpenSIPS por Call-ID
- CDR enriquecido, por Call-ID

Dashboard

- CDR con enlace VAULT por fila
- Búsqueda por fecha, método, código y tags
- Calidad por tramo (UAC y UAS)
- Tramo degradado señalado
- PCAP, RTCP y logs a un clic

IA (MCP)

- FastAPI + MCP, contrato único
- /troubleshoot-call en Claude Code
- Busca, correlaciona, analiza, informa
- Post-mortem en Markdown
- Misma autenticación del dashboard

Agente

- Binario Go estático
- eBPF (kernel 4.18 o superior)
- libpcap para CentOS 6 y 7
- amd64 y arm64, detección automática
- Open source, Apache 2.0

Red

- Una conexión TCP saliente (9060)
- Ningún puerto nuevo expuesto
- Buffer local de 100 MB
- Protocolo de transmisión documentado

Privacidad e integridad

- Solo diálogos INVITE
- Payload RTP nunca decodificado
- Bucket S3 por cliente
- Evidencia con hash de contenido

TÉCNICO

Especificaciones

Captura	Señalización SIP, estadísticas RTP/RTCP, logs de OpenSIPS y CDR
Alcance	Solo diálogos INVITE; el payload RTP nunca se decodifica
Almacenamiento	Bucket S3 por cliente, indexado por Call-ID, tamper-evident
Agente: captura	eBPF (kernel 4.18 o superior); libpcap (CentOS 6 y 7)
Agente: plataforma	amd64 y arm64, detectados en la instalación; binario Go estático
Transporte	Una conexión TCP saliente en el puerto 9060; buffer local de 100 MB
Acceso	Dashboard web y servidor MCP (FastAPI), en el mismo contrato
Skill de IA	/troubleshoot-call <Call-ID> en Claude Code
Código del agente	github.com/sippulse/sipvault, Apache 2.0
Licenciamiento	SaaS, por volumen de llamadas capturadas; agente open source; servidor on-premise bajo consulta.

Más de 200 operadores confían en SipPulse.

Vea el SIP VAULT funcionando en su stack: solicite su demostración.

sippulse.com/es/productos/sipvault
info@sippulse.com