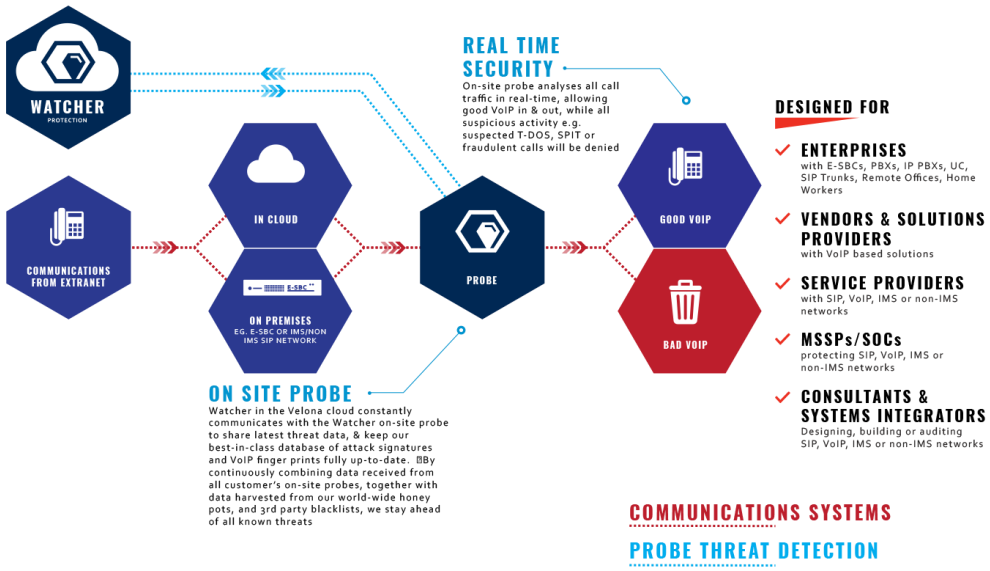
WATCHER Real-time VoIP detection & protection

Nobody can tell the bad calls from the good calls faster

Product Description

Real-time VoIP detection and protection

WATCHER runs real-time deep-DNA analysis on the signalling of your VoIP traffic to prevent Toll Fraud, D/T-DoS & SPIT attacks, much faster than any solution using CDR analysis.



FEATURES

1. Monitors for any 'out-of-the-ordinary' or strange calling patterns
2. Stops Toll Fraud, Nuisance Calling, Phone Reboots, SIP Parser Stressing/Fuzzing
3. Finds threat patterns or single malformed messages, SIP Port Scanning, Extension Discovery, Password Attacks, Registration Hijacking, Telephony D/DDOS Attacks
4. Identifies zero-day threats, attacker geo-locations & tools used
5. Real time alert to NOC, SOC or on-call personnel
6. Cloud-SaaS delivery for easy, scalable, resilient service delivery

Available as Cloud SaaS or on-premise solutions entirely inside an end-customer's private IP network, WATCHER can be run on any form of SIP based VoIP network, from the smallest Enterprise using just a single SIP trunk, to the very largest VoIP centric networks.

BENEFITS

1. WATCHER's central analytics engine monitors all our clients and instantly informs everyone of new threats
2. Integrates with your NOC or SOC
3. Focuses only on the threat data signatures - your own client data is discarded
4. No CAPEX or Admin costs
5. Cloud SaaS delivery means all updates are automatically picked up, with no impact on your performance or productivity
6. Zero touch provisioning of on-site tap.
7. Continuously updated with all data from all networks (threat patterns & Blacklists continuously maintained)

WATCHER can integrate with on-site SBCs via RADIUS or other protocols to implement the required authorisation on both outgoing as well as incoming calling, thereby preventing toll fraud, T-DOS & SPIT attacks. Confidentiality is fully designed in, as we focus only on the threat data signatures.

Why deploy WATCHER?

Increasing Toll Fraud & T-DoS attacks

Toll fraud now costs approx. $60.8 Billion US dollars (USD) p.a. (source: FINNA 2015) while 'Telephony Denial of Service (T-DoS) attack as an out-sourced service' is now obtainable from as little as $50.00 USD per hour.

Voice over IP (VoIP) has unique attributes when compared with other forms of traffic that run over IP networks. Accordingly, it must be treated differently to ensure next-generation network communications security - Gartner

SIP (Session Initiated Protocol) remains the dominant VOIP signalling protocol, with approx. 80% of the entire market. One percent (1%) of all Internet Fraud originates from SIP, with 88% of attacks happening outside of office hours.

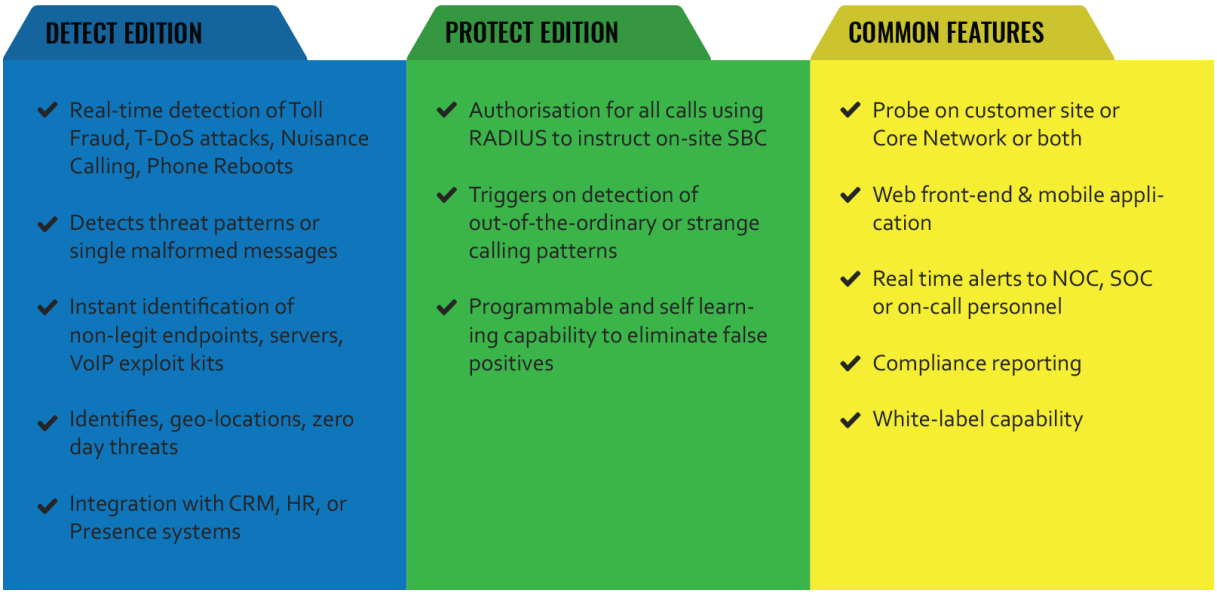
Even with a highly fortified Network you still need SIP "pin-holes" open to service your customers.

VOIP servers or End Points can be turned into a Toll Fraud server leaving you with a massive bill, or your own equipment (such as an E-SBC) can be turned into a D-DOS attacker, with DoS attacks blocking your ability to perform critical business functions, and hugely damaging your brand.

COMPLIANCE

RFC 3261, RFC 3428 Instant Messaging for SIP, RFC 4475 SIP Torture Messaging, RFC 4566 SDP, RFC 3856 Presence for SIP, SIP for IMS 3GPP TS 24.229.

PacketCable: PKT-SP-RSTF-C01-140314
(Residential SIP Telephony Feature Specification)



PLUG INTO VELONA'S CLOUD

WATCHER continuously analyzes SIP messaging via on-site probes on our customer's & service providers' networks, comparing them against our master SIP fingerprints database to ensure no messaging which indicate toll fraud, T-DOS & SPIT attacks are present in your system.

STRONGER TOGETHER

We use the power of the collective to make everyone instantly stronger. By continuously communicating with our big data server we ensure all Voice systems under Velona's protection remain up to date with present threat data.

Want to secure your communications systems?

Give us a call on (+353) 21 242 8400 or email info@velonasystems.com

VELONA SYSTEMS

OUR MISSION

TO ELIMINATE T-DOS AND TOLL FRAUD FROM VOIP COMMUNICATIONS

Real-time VoIP threat detection & prevention via Cloud SaaS solutions to eliminate risk to key infrastructure, productivity loss, revenue loss, or brand damage

OUR PRODUCTS

CRACKER
VoIP penetration & vulnerability testing from the Cloud

WATCHER
Real-time VoIP threat detection & protection

C Libraries via commercial licence

SIP FINGERPRINTER
MALFORMED SIP MESSAGE DETECTOR

FIND US

ADDRESS
Velona Systems Limited, 2nd floor, 11 Anglesea Street, Cork, Ireland

POSTCODE
T12CYR8

ON THE WEB
www.velonasystems.com

VELONA IN DEFENSE OF YOUR BUSINESS