Yazam Processes

Securing Files from Endpoint Applications

The Challenge

Workstation applications serve as a primary entry point for files entering your protected network. Their payloads, from simple to complex or encrypted, can slip past conventional gateway and endpoint defenses.

Widely used workstation applications include:

BROWSERS

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

CHATS & MESSAGING

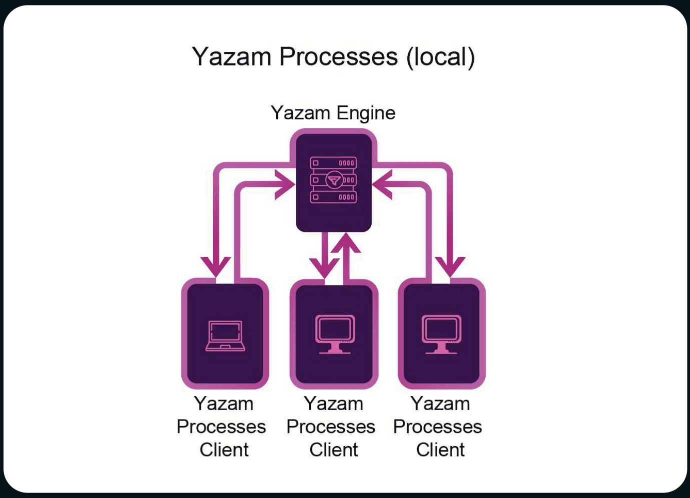
- WhatsApp
- Telegram
- Signal
- Zoom
- Microsoft Teams
- Amazon Connect
- Google Meet

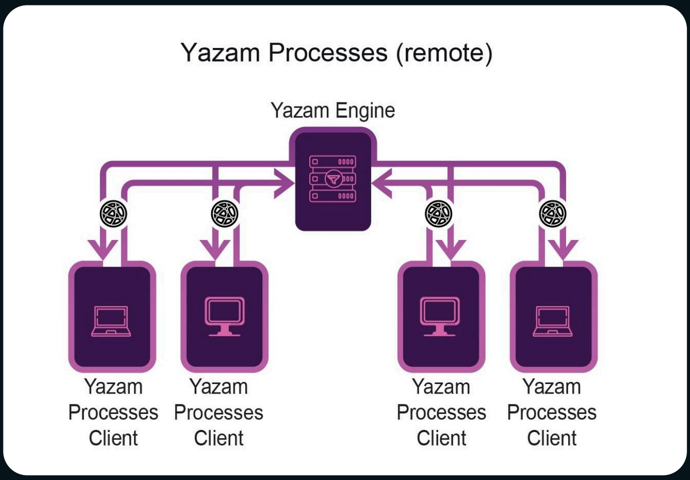
Yazam Suggests an Indispensable Layer of Proactive Protection

Yazam Processes solution provides a crucial layer of protection for files from endpoint applications, based on our unique inbound and outbound CDR technology. It actively removes embedded threats by intercepting, disarming, and reconstructing files in real-time. These filtering actions maximize file remediation, maintaining productivity without compromising security.

Key Features

- Proactive CDR filtering for files from leading browsers and messaging platforms.
- High performance and speedy filtering processes on standard hardware.
- On-the-Fly sanitization when files are written to the disk.
- Integration with Windows Active Directory for user management and isolation.
- Real-time user notifications about filtering results. Multilingual UI.
- For encrypted files, passwords are requested in real time from the user.
- Hybrid solution deployed on-premise (LAN) / on cloud (internet) / supplied as a service (SaaS), whether users are on-site (LAN) or remote (internet).
- Comprehensive logging and reporting of all filtering activities.
- Seamless deployment, manual or script installation, without conflicts with other clients.
- Flexibility to define custom security levels, tailored to business needs.





Yazam Engine The Intelligent Core

YazamTech's proprietary filtering Engine, developed in-house by YazamTech and based on inbound and outbound CDR technology, is a collection of many dedicated engines that work as focused processing units, which are engineered to identify and neutralize sophisticated threats across an unparalleled spectrum of more than 240 file types belonging to a wide range of family formats.

YazamTech's unique technology goes beyond detection. Yazam solutions meticulously disassemble, analyze, and rebuild incoming files and emails. They aim to eliminate hidden threats and zero-day exploits, ensuring your business operations remain uninterrupted and users' experience remains seamless.

PDF · MS Word · MS Excel · MS PowerPoint · MS Visio · Images · OpenDocument · Plain Text · Audios · Videos · Messages · XML · Archives · HTML · Bioinformatics · Macros · Scripts · Links · CRL · DICOM · CAD-CAM

× CONVENTIONAL DEFENSES

Firewalls · Antivirus/Antimalware · Secure Email Gateways/Mail Relays · Web proxies · Secure browsers · EDR/XDR · WAF · Sandboxes · many more...

- Inherently reactive focus on detecting and blocking known threats rather than actively removing threats.
- Fail to handle and neutralize cyber threats within complex file structures, and even within the basic files themselves.
- Limited response to encrypted protocols (like Telegram).
- Limited filtering before files arrive to the device.

✓ YAZAM PROACTIVE CDR

- Active sanitization at every entry point files are rebuilt clean before reaching your network.
- No blocking, no productivity loss. Encrypted-file handling and real-time notifications across 240+ file formats.
- On-the-Fly sanitization when files are written to disk, ensuring no threat persists.
- Seamless integration with Windows Active Directory and hybrid deployment options.

Yazam Solutions

Yazam provides a proven active layer of security for existing information channels without reducing their availability, without unnecessary file or email blocking. Yazam's solutions' comprehensive approach ensures security at every entry point.

Yazam Email

Actively disarms threats in on-prem, 365 and Gmail emails (body and attachments)

Yazam Processes

Actively disarms threats in files imported and saved by endpoint applications

Yazam Directories

Actively disarms threats in files from local and network directories

Yazam Media

Actively disarms threats in files from removable media devices

Yazam API

Actively disarms threats in files by customers' applications

Yazam MFT

Managed File Transfer (MFT) cloud service, including active CDR sanitization

Yazam Diode

Unidirectional optic data transfer solution, hardware-based

Yazam Bridge

Moves files between locations, converts files to emails, and emails to files

Yazam ICAP

Actively disarms threats in files exchanged between security applications via ICAP protocol

CONTACT US

✉ info@yazamtech.com ☎ EMEA: +972.9.7435965 | US: +1.949.284.1136 https://www.yazamtech.com/