Yazam Media

Securing Files from and to Removable Media

The Challenge

Removable media remains a critical vector for transferring files into and out of secure networks and isolated environments. While often used for legitimate and essential purposes, it can also introduce malicious components and enable sensitive data leakage.

Payloads carried on such media, ranging from simple files to complex or encrypted content, can bypass conventional gateway and endpoint defenses, including XDR, antivirus solutions, and device control.

Removable media encompasses a wide range of devices:

REMOVABLE MEDIA

- USB Devices
- Mobile Devices
- CDs / DVDs

Yazam Suggests an Indispensable Layer of Proactive Protection

Yazam Media provides a crucial layer of protection for file transfer between removable media and secure networks, based on YazamTech's unique inbound and outbound CDR technology.

YazamTech's technology removes embedded threats and prevents data leakage by detecting, disarming, and reconstructing files in real time.

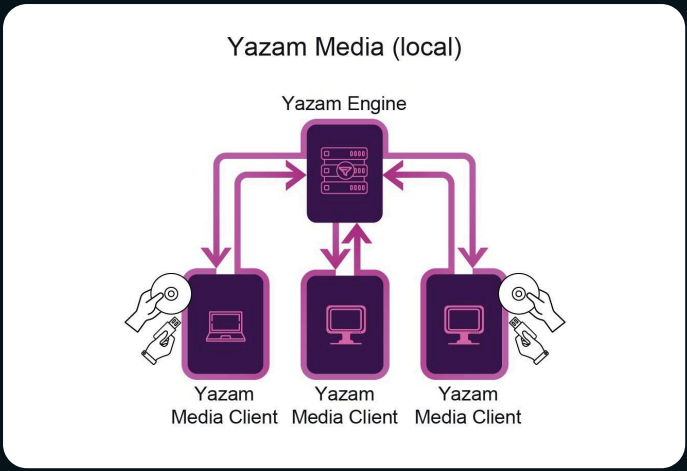
Secure Transfer Without Compromising Productivity

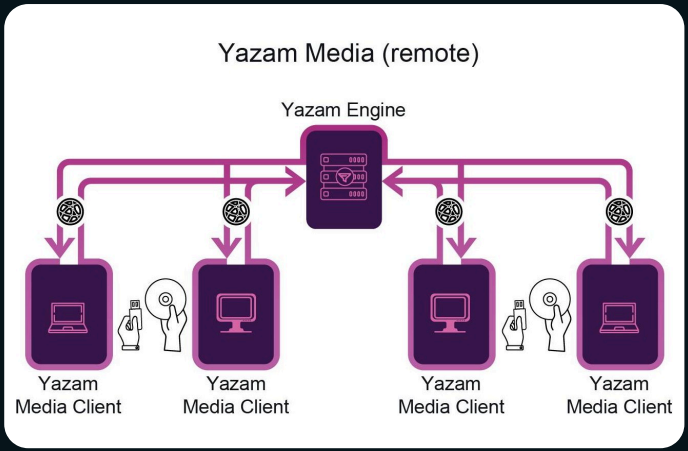
Yazam Media enables organizations to safely use removable media where it is operationally required, without relying only on blocking or detection.

It helps protect both inbound file flows and outbound data movement while preserving business continuity.

Key Features

- Proactive CDR filtering for files transferred between removable media and secured networks through workstations and dedicated kiosks.
- Real-time user notifications about CDR results. Multilingual UI.
- Hybrid deployment: the Yazam Engine can be installed on-prem, on a private cloud, or supplied as SaaS.
- Multi configurations: Yazam Client can be deployed on dedicated kiosks or installed on endpoint workstations that require removable media access.
- Password handling for encrypted files.
- Seamless deployment.
- High-performance filtering.
- Integration with Active Directory and Device Control.
- Comprehensive logging and reporting.
- 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/