

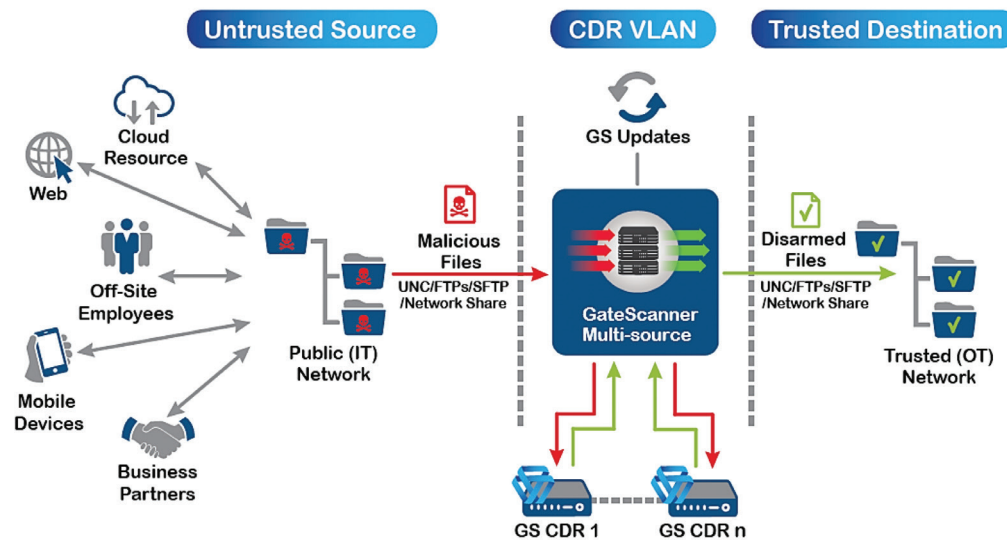
## GateScanner Multi-source

*File transfers with embedded CDR file sanitization*

Content Disarm and Reconstruction (CDR) file sanitization technology is the most powerful anti-malware technology available today to protect networks from file-based attacks.

Inserting CDR processing into cross-network transfers, such as between IT and OT, supports the establishment of highly secure trusted zones where organizations can safeguard their most critical processes and assets.

GateScanner® Multi-source is an API-less file transfer and sanitization tool, moving data from a wide range of third-party sources and applications, securely into internal destinations.



### Highlights

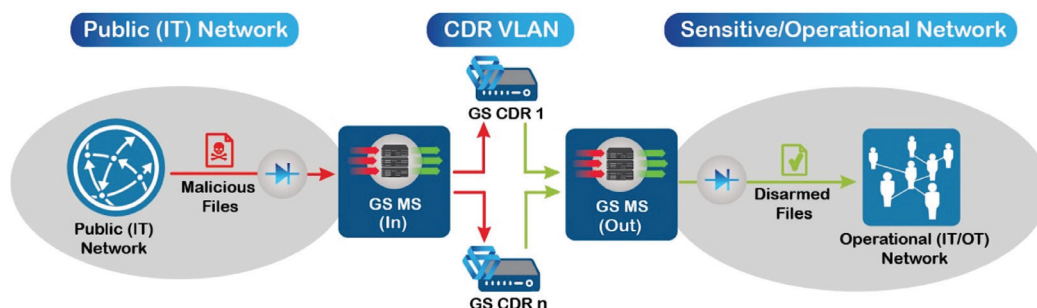
- Secure and sanitized high volume file transfer, for IT/OT network segmentation and cross-domain solutions
- Prevents file-based attacks from known, and previously unseen ('signature-less') malware
- Multiple sources supported – cloud, web, mobile
- No coding required
- Easily scalable with zero-downtime 'active-active' engine architecture
- High-granularity, profile-based scanning management and reporting



Recognized by Gartner as 'Cool Vendor in Cyber- Physical Systems Security' for 2020

The GS Multi-source server monitors incoming sources, automatically invoking the CDR engines to enforce pre-determined file sanitization policies and deliver disarmed content to its destination. The solution is modular, highly scalable, allowing for flexible integration with existing configurations of any complexity.

### Network segmentation with GateScanner® Multi-source and GS Injector data diodes



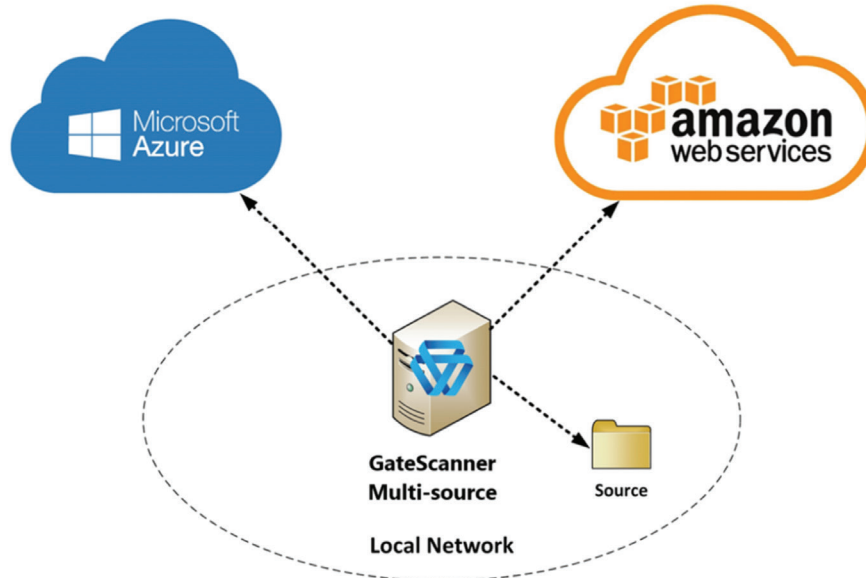
### A Proven Technology

GateScanner is protecting government agencies, defense contractors, financial institutions, critical infrastructure and healthcare organizations, since 2013.

Independent client testing repeatedly shows GateScanner preventing up to 99.9% of undetectable ('signature-less') threats.

Gartner Disclaimer: The GARTNER COOL VENDOR badge is a trademark and service mark of Gartner, Inc. and/or its aliases and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

**Secure file transfer between local and cloud storages with embedded CDR file sanitization**



**CDR - because prevention trumps detection**

Most network attacks begin with a malicious payload delivered through an email, web download or shared files arriving from trusted partners (i.e. supply chain). CDR offers the best protection from both known as well as previously unseen file-based malware, empowering network defenders to prevent attack from outside the network - rather than trying to detect it after it has already entered and detonated inside the network



**Headquarters**

**Sasa Software (CAS) Ltd.**

Telephone: +972-4-867-9959

Kibbutz Sasa, Israel

[Info@sasa-software.com](mailto:Info@sasa-software.com)

[www.sasa-software.com](http://www.sasa-software.com)

**About Sasa Software**

Sasa Software is a cybersecurity company specializing in the prevention of file-based attacks.



**Bavelle Technologies**

100 Eagle Rock Avenue

East Hanover, NJ 07936

973-422-8100

973-992-8086

[info@bavelle.com](mailto:info@bavelle.com)

[www.bavelle.com](http://www.bavelle.com)

**GateScanner Multi-source technical & CDR features**

- **Supported file sources/destinations** include FTP, FTPS, SFTP, UNC, SMB, shared/local folders.
- **Customizable scanning policies:** dedicated scanning policies can be defined for every user & source, including mapping of active directory (AD) users to individual source/target.
- **Central Management:** central administration, detailed activity reports, interfaces with SIEM/Syslog, automated updates.
- **CDR processing** includes file type verification; file deconstruction to the most basic components (including multi-layer archive decompression); deep scanning with multiple AV's and NextGen AI; proprietary file reconstruction fatally obstructs remaining undetected malware.
- More than 300 file types supported including MS Office, PDF, RAR, ZIP Media files (images, audio, video), AutoCad, Hanword (HWP), Archives, PST, .EML, installation files, XML, HTML, other text files, medical imaging files (DICOM), and customized files.

**System requirements**

**Multi-source Server** Windows

Server 2019 or later **System**

**specification:** 6vCores, 16GB

RAM, 500 GB SSD

**GateScanner CDR engines**

Preconfigured, secured, Windows 10 IoT virtual/physical appliance

**System specification (per engine):**

4 vCores, 8 GB RAM, 60 SSD (minimal requirement)