GATE SCANNER by Sasa Software

Application Server

The Challenge

We live in a world of increasingly sophisticated cyber threats. APTs, ransomware and other malware continually evade detection technologies. Within the organization, users inevitably open files containing threats, leading to IT security incidents. Most recently, WanaCry and Petya ransomware became a global scare that spread rapidly throughout organizations, and attacks breached prominent financial institutions including Deloitte, Equifax and the US SEC.

IT security for a de-Perimeterized reality

(Network Segmentation)

The reality of advanced threats is compounded since organizations are becoming increasingly perimeter-less. Even with the best IT security technologies, it is virtually impossible to protect all attack surfaces. Organizations must adapt and segment their networks into "untrusted" and "trusted" areas to focus security efforts, and air-gap their critical resources. When an IT security incident occurs, it will be contained in the "untrusted" segments and will not propagate to the "trusted" areas.

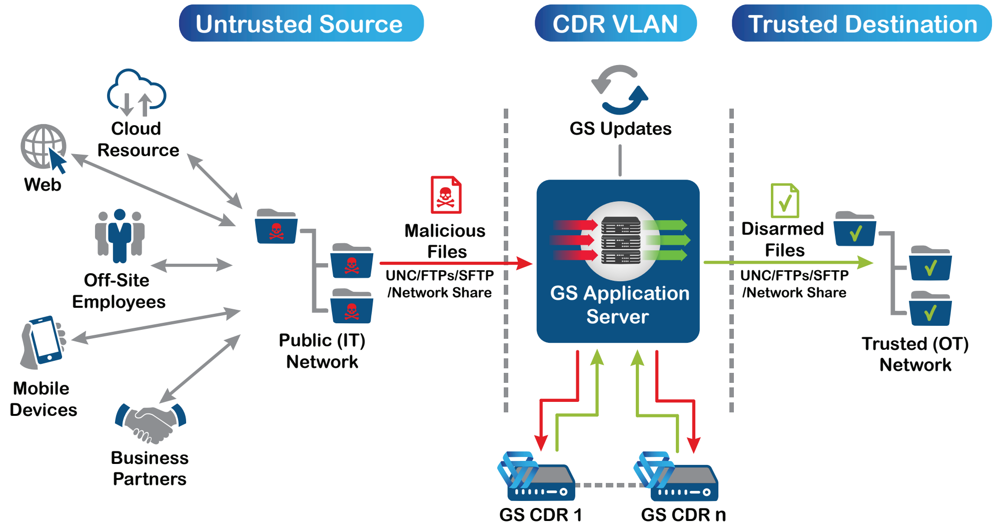
The Solution

GateScanner® Content Disarm and Reconstruction (CDR/Sanitization) ensures security by treating every file as suspicious, performing deep threat scans and restructuring, transforming files into a safe and neutralized copy. GateScanner® prevents advanced undetectable malicious code attacks, including APTs, ransomware and future sophisticated threats, while maintaining full file usability, visibility and functionality.

GateScanner® Application Server

GateScanner® Application Server serves as a bridge to safely transfer files to and from sensitive networks, implementing network segmentation and enabling API-less integration with 3rd party applications. The solution monitors multiple untrusted incoming files sources, automatically invokes GateScanner® CDR, enforces policy, and delivers the disarmed files to the trusted destination. Solution is highly scalable and modular allowing integration of GateScanner® CDR with complex, highly secure network topologies.

Gate Scanner® Appliance Security



Gartner "Cool Vendors in Cyber-Physical Systems Security", Katell Thielemann, et al, 21 April 2020
Gartner Disclaimer: The GARTNER COOL VENDOR badge is a trademark and service mark of Gartner, Inc. and/or its affiliates 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.

Proven Technology

Founded in 2013, Sasa Software successfully protects governmental agencies, defense contractors, financial institutions, public utilities and healthcare enterprises.

Independent tests demonstrate GateScanner® prevents up to 99.9% of undetectable threats*

Industry Recognitions

Gartner
COOL VENDOR 2020™

Awards

INFOSEC AWARDS WINNER
CYBER DEFENSE MAGAZINE
2020

FROST & SULLIVAN
2017 BEST PRACTICES AWARD
ASIA PACIFIC INDUSTRIAL CONTROL SYSTEMS SECURITY VENDOR OF THE YEAR

Contact Us:

Headquarters:
Sasa Software (CAS) Ltd.
Telephone: +972-4-867-9959
Kibbutz Sasa, Israel
info@sasa-software.com
www.sasa-software.com

US Office:
Bavelle Technologies
Sasa Software Authorized Agent
100 Eagle Rock Avenue
East Hanover, NJ 07936, USA
Telephone: +1-973-422-8112
sasa-cdr@bavelle.com
www.bavelle.com

Singapore Office:
Sasa APAC
8 Penjuru Lane, Singapore
Telephone: +65-6210-2354
contact@sasa-apac.com
www.sasa-apac.com

GATE SCANNER *Application Server*

GateScanner® CDR Features

- ✓ **File Deconstruction:** Disassembles complex files to seek deeply hidden threats
- ✓ **Deep Threat Scans:** Dramatically Increases threat detection rates and prevents file spoofing using multiple AV and multiple True Type scans
- ✓ **File Disarm:** Removes ("Sanitizes") potentially malicious elements, scripts, macros, links, while keeping trusted content and restructuring files to disrupt the integrity of deeply hidden malicious code
- ✓ **File Reconstruction:** Reconstructs into a harmless file, maintaining visibility and usability
- ✓ **External Tools Integrations:** Integrates with external security solutions, such as Sandboxes, Next-Gen AVs

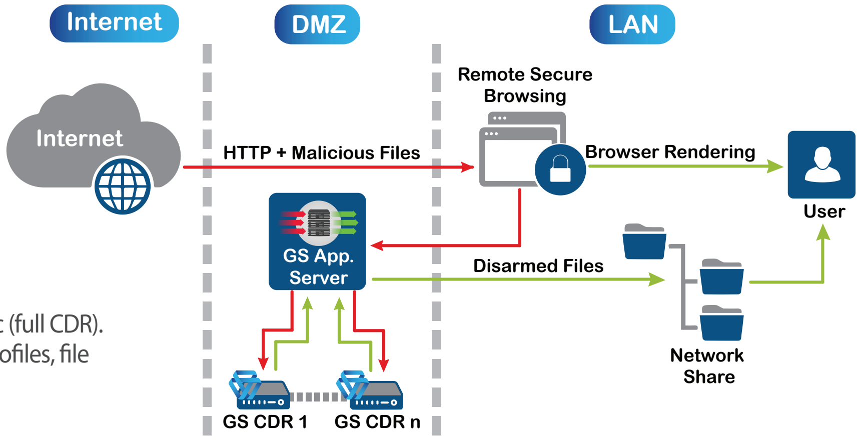
GateScanner® Application Server Technical Features

- ✓ **Supported file sources/destinations:** FTP, FTPS, SFTP, UNC, SMB, shared/local folders
- ✓ **Seamless integration with GateScanner® Injector:** Integrates with GS Injector optical data diode for uni-directional data transfers
- ✓ **Customized scanning policies:** Dedicated scanning policies can be defined for every source, including mapping of active directory (AD) users to individuals sources/targets with notifications upon scan completion
- ✓ **Designed for Security:** Highly modular design allow seamless integration with complex network topologies with strict security requirements, emphasizing uni-directional data flow
- ✓ **Highly scalable w/load balancing:** Easily and highly scalable without system interruptions, built in Active/Active load balancing
- ✓ **Central Management:** Central administration, detailed activity reports, interfaces with SIEM/Syslog, automated updates

GateScanner® Application Server Specifications

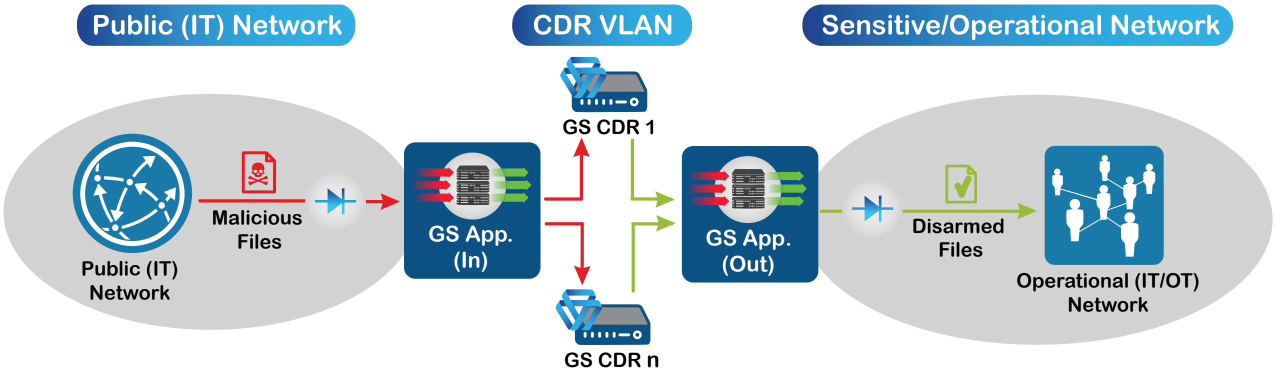
- ✓ **Application Server Front End (in/out service)**
  Supports on premise, private cloud, HA and multi-Front End deployments
  Installed on a Windows
- ✓ **Scanning Engine(s)**
  Supplied as a pre-configured virtual or physical hardened appliance
- ✓ **Scanning Performance**
  Up to 20Gb/hr. 5Mb MS-Office document: Up to 30 sec (full CDR). Scanning performance varies according to scanning profiles, file type/structure and hardware used
- ✓ **Supported File-types**
  Supports full CDR for hundreds of file type combinations, including the entire suite of MS Office, PDF, 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

Sample Deployments



Sample #1: API-less integration with remote secure browsing

Users access the internet using a remote secure browsing solution (e.g. Citrix, Cigloo). Downloaded files are automatically disarmed using GS Application Server, and delivered to the user's home drive.



Sample #2: Network segmentation with Data-Diodes

Users access the internet using an untrusted IT network, files are disarmed using GS App Server, with the installation divided to "in" and "out" components separated by data diodes (GS-Injector), to ensure a highly secure uni-directional delivery of the files into the operational (OT) network.

*Security results depend on scanning profile used.
Specification and features subject to change without prior notice.

GATE SCANNER by Sasa Software