GATE SCANNER by Sasa Software

DICOM Protector

The Challenge

We live in a world of increasingly sophisticated cyber threats, capable of evading detection. Healthcare is the most targeted yet underprepared genre of critical infrastructures, suffering from a deluge of publicized ransomware attacks and data breaches, facing significant direct and indirect costs from incidents and the resulting regulatory violations. Healthcare institutions use portable media devices for sharing data, and in many cases, patients themselves are the primary transporters of these portable media devices. The patient will perform an MRI at the radiologist's office and then will be requested to physically hand-over the media device to their GP/Specialist/Clinic Staff. Inside of the organization, trusted users inevitably open Digital Imaging and Communications in Medicine (DICOM) files containing threats, saving them directly into the hospital's information systems, leading to critical IT security incidents, and system shutdowns.

The Solution

Gate Scanner® DICOM Protector provides unrivaled protection for healthcare customers, when handling DICOM Files. The Gate Scanner® DICOM Protector is a physical appliance, on-site for patients/clinic staff to insert detachable media device carrying the DICOM file. Using the award winning Gate Scanner® Content Disarm and Reconstruction (CDR) Technology, the DICOM Protector performs proprietary deep threat scans into the imaging files, transforming files into a safe and neutralized copy, while maintaining DICOM conformance, allowing for viewing or safe transfer to IT/EHR/PACS servers. Gate Scanner® prevents unknown and undetectable malicious code attacks, including ransomware, while maintaining full usability, functionality and visibility of the files, ensuring the organization's security.

Gate Scanner® DICOM Protector Main Features

Deep Threat Scan Capabilities

- ✓ Performs deep threat scans on the viewer included in the DVD, verifying the viewer against a list software authorized by the organization, and can block unauthorized viewers.
- ✓ Proprietary DICOM deconstruction, performing deep scans on every image slice and metadata embedded in the images.
- ✓ Sophisticated file type identification with multiple "TrueType" engines to process unrecognized and customized files, fake files, tampered files, and performs signature verification.
- ✓ Deep known threat scans with multiple commercial AV systems, performing full featured scans including heuristics / zero-day scans.

File Disarm Capabilities

- ✓ Proprietary DICOM disarm capabilities, preventing dedicated exploits, while preserving exact DICOM conformance.
- ✓ Blocks and removes macros, Java scripts, embedded elements, re-writes / blocks / disables links, searches and removes hidden code.
- ✓ Unique functionality to check macro signatures against a list of macros allowed by the organization.
- ✓ Extensive file conversion capabilities, supporting hundreds of file type combinations, including: the entire suite of MS-Office, PDF, Media files, XML, HTML, other text files, and custom file conversion.
- ✓ Disarm policy can be tailored to balance security and usability.

Award Winning Solution

Sasa Software is the 2017 Frost & Sullivan Asia Pacific Critical Infrastructure Security Vendor of the Year

Proven Technology

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

Approved by the Israeli and Singaporean Cyber Commands

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

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 *DICOM Protector*

User Management

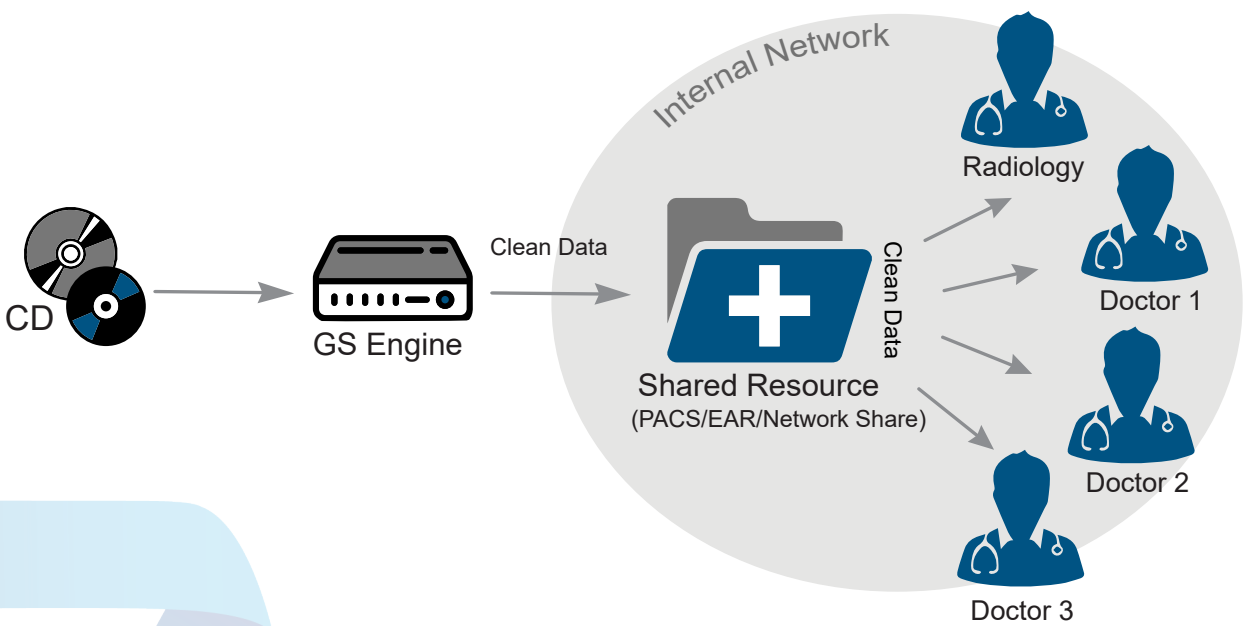
- ✓ User authentication.
- ✓ Verification against user e-mail address or profile groups.
- ✓ Scan policies configured according to user/group identification.

Security

- ✓ Engines are a hardened physical/virtual appliance to prevent external tampering, system is shielded and encrypted – running WIN 8 SE embedded (physical engines).
- ✓ Engines return to zero-state upon the completion of each scan to prevent internal malware tampering.

Managing System

- ✓ Simple, user friendly, multi-language user interface.
- ✓ Central administration including full control, administration and configuration of every user, station and scanning engine.
- ✓ Highly scalable – Adding capacity is done easily by deploying additional kiosks and increasing the license count.
- ✓ Interfaces with the organization's PACS and EHR to allow saving the secured DICOM directly into the organization's IT system.
- ✓ Detailed reports and event logs, interfaces with SIEM/Syslog
- ✓ Central Update server delivers daily AV, software, and OS updates.
- ✓ Allows independent customer management, without access by the software vendor.
- ✓ Vendor is not exposed to scan activities.



*Specification and features subject to change without prior notice.

GATE SCANNER by Sasa Software