



Enabling compliance and security for removable media

The Challenge: Portable Media

Usage of portable media (USB drives, CD/DVDs) presents a critical risk, as using them bypasses IT security layers, and potentially introduces malicious files directly into the organization. These inherent risks cause organizations to disallow their use and led to the creation of compliance requirements such as the Energy Sector NERC CIP 003-7, U.S. Nuclear Regulatory Commission regulations NEI 08-09, and NIST 800-53 (PR.PT-2) for cybersecurity protection of critical infrastructures.

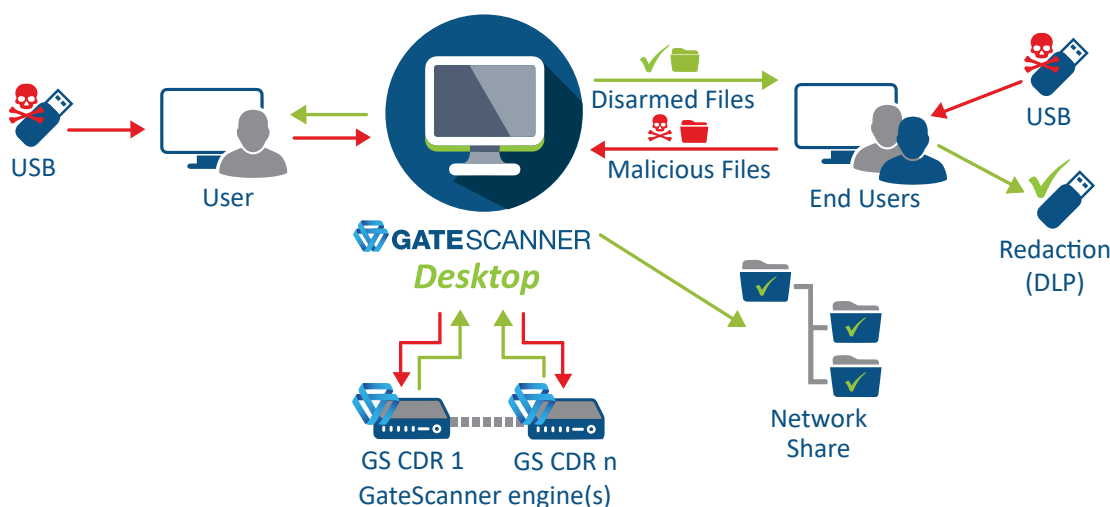
The Solution: GateScanner® Desktop

GateScanner Desktop enables endpoint users to conveniently and securely access files from portable devices, directly at their workstations. The solution prevents media and file-based threats, while enforcing organizational security policies, ensuring visibility, and achieving compliance. GateScanner Desktop is triggered by the insertion of a device, guiding users through an import/export process to save trusted and verified files to the endpoint, or other network destinations.

The Technology: GateScanner® CDR

GateScanner Desktop leverages Content Disarm and Reconstruction (CDR/Sanitization) ensuring proactive protection against malicious content by applying highly optimized scanning technologies including NextGen detection to pre-filter known threats, and proprietary file disarm to prevent undetectable attacks, protecting against exploits and weaponized content that has never been seen before, while maintaining full file fidelity, visibility, and usability.

GateScanner® Desktop – sample workflow



Users insert portable (USB) devices at the endpoint, activating a desktop application, which sends the files to a networked GateScanner service. The disarmed files are then saved to a network location. Files can be securely exported using Redaction (DLP) policies.

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



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

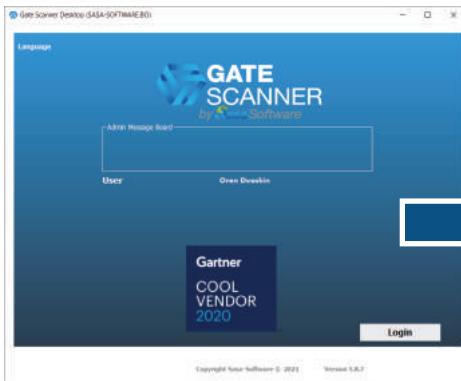
Gartner "Cool Vendors in Cyber-Physical Systems Security", Katell Thielemann, et al, 21 April 2020

Gartner Disclaimer: The GARTNER COOL VENDOR badge is a trademark and service mark of Gartner, Inc. and/or its allies 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.

Solution Highlights

- ✓ **File Vault integration & multiple destinations:** The secured files can be saved into an encrypted file vault, or sent to multiple destinations – the user's endpoint, home drive, network share, and more
- ✓ **File redaction (DLP):** Security for outgoing files via deep content search and replace, metadata removal, policy enforcement and ensures files are threat free with GateScanner CDR
- ✓ **Privacy & GDPR compliance:** All files are scanned offline without an internet connection and information is securely wiped after every operation, so can never be leaked externally
- ✓ **Encrypted media and files:** Automatic scanning of password-protected files, hardware encrypted media, supports BitLocker encryption
- ✓ **Uninterrupted productivity:** The user's endpoint is not impacted since scanning is processed by the GateScanner Desktop service, with an option for automated download and email notification on scan completion
- ✓ **Customizable workflows, Multi-lingual support:** Scanning steps can be fully customized according to the organizational security policy, with an option for admin approval of files submitted for processing. Solutions supports a multi-lingual user interface with customizable graphics
- ✓ **User and scan policy management:** Scanning profiles are adjustable according to user/group policies. Multiple authentication options are available including Active Directory (AD) integration with Single Sign On (SSO), local authentication, and more

Authentication



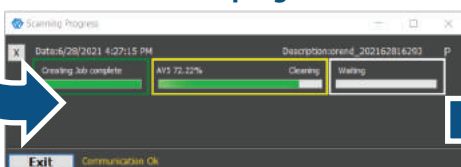
Choose operation: Scan files/DLP



Select files



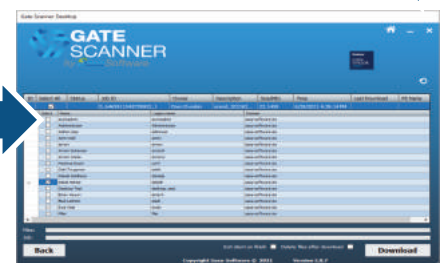
Scan in progress



Scan results



Download/Share files



GateScanner Desktop Specifications

- ✓ **Delivery Options:** Private Cloud, On-Prem
- ✓ **GateScanner Desktop service:** Installed on a Windows server (2012 R2 onwards)
- ✓ **Requirements:** 4 vCores, 8GB RAM, 250 GB HD (SSD Recommended)
- ✓ **GateScanner Engine(s):** Supplied as a pre-configured secured virtual/physical based on Windows 10 IoT
- ✓ **Requirements per engine:** 4 vCores, 8GB RAM, 60 GB SSD
- ✓ **Scanning Performance:** Up to 15Gb/hour per engine.
- ✓ **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, Archives, PST, .EML, installation files, XML, HTML, other text files, medical imaging files (DICOM), and customized files

*Specification and features subject to change without prior notice.
Scanning performance varies according to scanning profiles, file size/structure, and hardware used.
Security results depend on the scanning profile used.