

GATE SCANNER Kiosk



The Challenge

We live in a world of increasingly sophisticated cyber threats. APT's, ransomware, and other malware continually evade detection technologies. Inside of the organization, users inevitably open files containing threats, leading to IT security incidents. Most recently, WanaCry and Petya ransomware became a global scare, spreading rapidly across organizations, and the Brutal Kangaroo APT used portable media to attack air-gapped networks.

Portable Media (USB drives, CD/DVDs)

Portable media pose a critical risk, as using them bypasses IT security layers. Media can contain multiple threats, including files on the media, threats in hidden partitions, and malicious hardware/firmware.

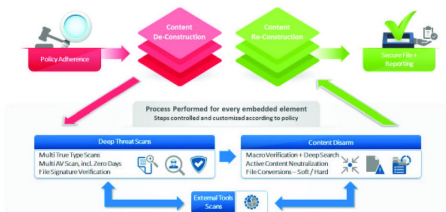
The Solution

Gate Scanner® Content Disarm and Reconstruction (CDR) treats every file as suspicious, performing deep threat scans, transforming files into a safe and neutralized (harmless) copy, ensuring security. Gate Scanner® prevents unknown and undetectable malicious code attacks, including ransomware, while maintaining full usability, visibility and functionality of the files.

Gate Scanner® Kiosk

The Gate Scanner® kiosks are placed at central locations in a facility, acting as a "Gate" to prevent malicious threats, and enforcing policy on files copied from portable media. Users insert portable media into the kiosk, files are scanned and disarmed according to a role based policy, then securely copied into the organization's network. Gate Scanner® Kiosks can be deployed standalone or networked, installed at multiple locations, and optionally coupled with a unidirectional data diode (Gate Scanner® Injector). Solution is centrally managed and updated.

Gate Scanner® Content Disarm and Reconstruction (CDR) Process



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 Gate Scanner® prevents up to 99.9% of undetectable threats*

Contact Us:

Sasa Software (CAS) Ltd.
Telephone: +972-4-691-8959
Kibbutz Sasa, Israel
info@sasa-software.com
www.sasa-software.com

US Office:

Bavelle Technologies -
Authorized Sasa Software Agent
100 Eagle Rock Avenue, Suite 301
East Hanover NJ 07936, USA
Telephone: +1-973-422-8112
sasa-cdr@bavelle.com
www.bavelle.com

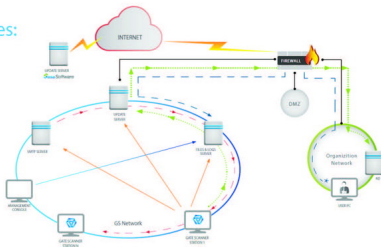
Singapore Distributor:

Athena Dynamics
8 Penjuru Lane, Singapore
Telephone: +65-6210-8099
contact@athendynamics.com
www.athendynamics.com

*The images above are for illustrative purposes only

Gate Scanner® Kiosk scanning features:

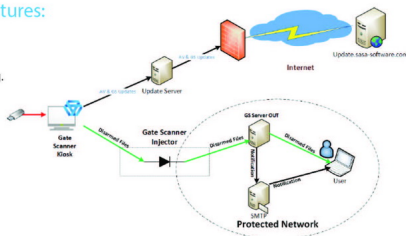
- ✓ **File de-construction:** Understanding that today's threats are deeply hidden, complex files are disassembled into individually embedded elements.
- ✓ **Deep threat scans:** Embedded elements are deeply scanned using multiple True Type and multiple AV engines, dramatically increasing detection rates, and preventing file spoofing. File and Macro signatures are verified to confirm a trusted source.
- ✓ **File re-construction:** Files are disarmed ("sanitized") removing embedded elements, scripts, macros, links and undergo structural conversions, creating a **neutralized (harmless) copy of the file.**
- ✓ **File redaction:** Security for outgoing files, via deep content search and replace, metadata removal, conversions of outgoing files, and outgoing file policy enforcement.
- ✓ **External tools integrations:** Optionally integrates with external security solutions, such as Sandboxes, Next-Gen AVs, etc.



Sample installation #1: Centrally managed multiple kiosks in a shared VLAN, Scanned files are sent to an internal network

Gate Scanner® Kiosk technical features:

- ✓ **Management and UI:** Multi-lingual, touchscreen enabled, central administration of multiple Kiosks, detailed activity reports, interfaces with SIEM/Syslog. Automated updates.
- ✓ **User and scan policy management:** Scanning profiles are customizable according to user/group policies. Authentication integrates with Active Directory, and email addresses.
- ✓ **Scan verification:** Files processed at the Kiosk can be digitally signed and sealed, to validate they have been scanned by a Gate Scanner®.
- ✓ **Password self-extraction:** Automatically opens and deep-scans password protected files.
- ✓ **Security:** System is deployed as an encrypted, tamper proof, hardened physical appliance. Kiosks return to zero-state upon the completion of each scan to prevent malware tampering. Vendor is not exposed to scanning activities.



Sample installation #2: Secure delivery of files from a Kiosk into a secure network, using a Gate Scanner® Injectornetwork

Gate Scanner® Kiosk Specifications:

- ✓ **Scanning Performance:** Up to 20Gb/hr. SMB 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 hundreds of file types, including the entire suite of MS-Office, PDF, Media files (images, audio, video), Archives, PST, .eml, Installation files, executables, XML, HTML, other text files, Medical imaging files (DICOM), customized files.
- ✓ **Supported media:** USB, CD/DVD, Memory cards, Portable Hard Drives (with Combo option).