GATE SCANNER by Sasa Software

Appliance Security

Ensuring Cyber Security for Critical Assets

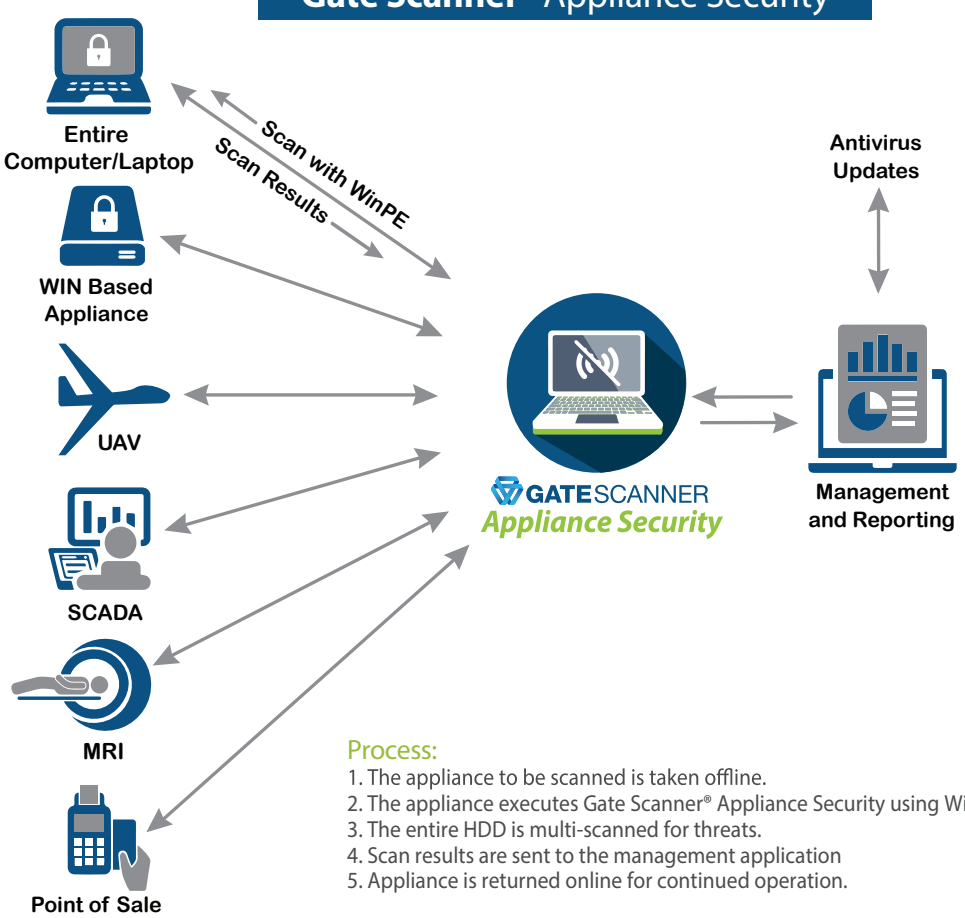
The Challenge

Operational computing appliances are exposed to cyber-attacks due to limitations in deploying traditional security technologies on appliance-based platforms such as SCADA/ICS, aviation computers, medical-imaging equipment, and point of sale (POS) devices. While solutions exist to monitor traffic in operational (OT) networks and to detect and prevent file-based attacks prior to saving files on appliances, it is challenging to verify that the appliance itself hasn't been compromised. A full system scan will ensure security, while maintaining the integrity of the appliance.

GateScanner® Appliance Security

GateScanner® Appliance Security scans MS-Windows based appliances and computing assets using WinPE technology. The solution is loaded into the appliance memory during pre-execution boot, scanning the entire hard disk drive (HDD) with multiple commercial anti-virus engines. Since the solution is activated in memory prior to boot time, it achieves access to all HDD areas including protected sectors. Since no software is installed and no configuration changes are made, the appliance integrity is maintained. The resulting combination of multi-AV scans and entire HDD coverage dramatically improves security against threats.

Gate Scanner® Appliance Security



Process:

1. The appliance to be scanned is taken offline.
2. The appliance executes Gate Scanner® Appliance Security using WinPE.
3. The entire HDD is multi-scanned for threats.
4. Scan results are sent to the management application
5. Appliance is returned online for continued operation.

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

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

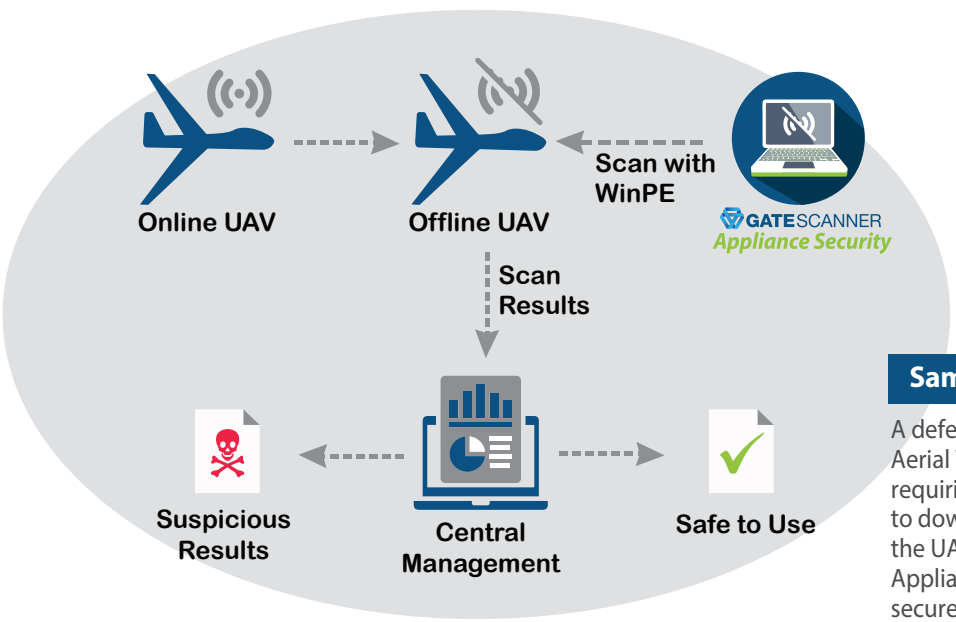
GATE SCANNER *Appliance Security*

Features

- ✓ Uses a WinPE client, running entirely in memory, pre-execution (pre OS) environment:
  No software and no configuration changes are performed
- ✓ Scans the entire appliance HDD using five commercial anti-virus engines, plus one Next Generation Machine Learning / AI technology (powered by Cylance®)
- ✓ Updates AV definitions prior to every scan
- ✓ Parallel scanning for maximum performance optimization
- ✓ Optionally uploads detected files to an encrypted archive for malware analysis by the organization's SOC
  Management application controls connected appliances, defines scan policies, configures exceptions, monitors concurrent clients
- ✓ connection and progress, tracks scan history, and reports incidents via email, SNMP, syslog
- ✓ Web-based reporting system of scan results
- ✓ Activation options:
  CD/DVD, USB Drive, PXE Server

Sample Use Cases

- ✓ Scan an entire computer/laptop before entering an OT/critical network
- ✓ Aviation and naval computers
- ✓ C4ISR systems (e.g. UAV ground controllers)
- ✓ SCADA/ICS Controllers
- ✓ Medical equipment
- ✓ POS Machines: ATMs/retail/vending
- ✓ Scanning of other MS-Windows based appliances



Sample use case - UAV operator

A defense contractor operating UAVs (Unmanned Aerial Vehicle) had to comply with security policies requiring pre/post mission integrity checks on prior to downloading mission data. After every sortie, the UAV's aviation computer is scanned by GateScanner® Appliance Security. Once the UAV is determined to be secure, mission data is downloaded, and the UAV is prepared for the next flight.

System Components and Specifications

- ✓ **Management Server:**
  Installed on a Windows 2012 R2 Server
  Requirements: 4-6 vCores, 12-16 GB RAM, 250-500 GB HDD
  Database: MS-SQL 2014 STD
  Full text search, reporting services, reserved IP and DNS names, required ports
- ✓ **Client Requirements:**
  Valid MS-Windows license, Windows formatted HDD (non-encrypted)
  Requirements: Core i3 & Up, 4 GB RAM, LAN connection

*Specification and features subject to change without prior notice.

GATE SCANNER by Sasa Software