Sasa Software

GATESCANNER® SOLUTION OVERVIEW

Content Disarm & Reconstruction -
Multi-Vector File Protection



GateScanner's Content Disarm and Reconstruction (CDR) technology removes file-based threats upon first contact - before they enter the network.

HOW CDR WORKS

01 Suspicious file → 02 File deconstruction → 03 Deep Detection → 04 File reconstruction → 05 Disarmed file

03 – DEEP DETECTION
- Multi file type identification
- Multi AV scans
- Advanced static code analysis

External tools integration

04 – FILE RECONSTRUCTION
- Keeps trusted code
- Removes potentially malicious elements
- File restructuring (single/multi pass)

THE CHALLENGE

The most sophisticated attacks still start the same way: a malicious file arriving via email, a shared drive, a USB device, or a web download. Detection-based tools and sandboxes are reactive by design - they require known signatures or triggered behavior to catch a threat. Zero-day and obfuscated malware exploits this gap. IT security teams face a fundamental tension: keeping content channels open for productivity while ensuring the network never becomes the victim of a file-borne attack.

THE SOLUTION

GateScanner's CDR process starts with the de-construction of incoming files to their most elementary components. Multiple AVs and AI-based detection are applied to each component separately, achieving unparalleled levels of threat detection. A proprietary restructuring process then reconstructs the files - re-shuffling components to break up any remaining undetected threats. The resulting files are identical in content and function to their originals, yet perfectly safe to continue into the network.

99.9%
Deconstruction of signature-less / zero-day threats blocked in independent testing

300+
file types supported, including MS Office, PDF, images, DICOM, AutoCAD

350+
organizations protected globally across defense, government & critical infrastructure

Why GateScanner?

Stop Threats Before They Enter
Proactive CDR neutralizes known, unknown, and zero-day attacks instantly — no waiting for signature updates.

Scale Without Limits
Handle high-volume workloads with zero downtime as your organization grows.

Enable Secure Productivity
Users work normally in network folders, browsers, Outlook, and with USB drives while threats are eliminated transparently.

Reduce Complexity & Cost
Single platform replaces multiple point solutions with unified control across all file channels.

Prove Compliance Instantly
Immutable audit trails and SIEM integration satisfy regulators and auditors.

Deploy Your Way
Choose on-premises, private cloud, or SaaS to match your infrastructure and requirements.

Sasa Software (CAS) Ltd.
+972-4-867-9959
sales@sasa-software.com
www.sasa-software.com

Sasa Software



GATESCANNER SUITE
ONE TECHNOLOGY, MANY SOLUTIONS

GateScanner Security Dome
Enterprise-grade Managed File Transfer and secure collaboration hub with built-in CDR. Multi-tenant, cloud-native platform with digital vault, automated workflows, cloud sync, and a browser plugin. Supports email, OneDrive, FTP/SFTP, UNC, and local folders.

GateScanner Mail Protection
Complete enterprise email security deployable as a SEG, SMTP bridge, or direct O365/Exchange integration. Includes deep URL categorization, antiphishing, anti-spam, outbreak detection, IP reputation, and anti-spoofing (DKIM/DMARC/SPF).

GateScanner Kiosk
Hardened, managed physical stations for secure transfer of files from removable media (USB, CD/DVD) to internal destinations. Available as Micro PC, Laptop, tower PC, or wall-mounted/freestanding enclosures. Standalone or networked.

GateScanner Integration Server
Embed CDR file sanitization into any data stream via a RESTful API. Adds a security layer to third-party applications and OEMs. Scanning engines operate on-premises, in virtual environments, or on private/public cloud. Available as a managed service.

GateScanner PE
CDR sanitization for portable executable (PE) files - EXE, DLL, and related binary formats. Neutralizes embedded malicious code while preserving the file's intended functionality, enabling safe transfer of executables across security boundaries.

GateScanner Deep Detector
An enterprise-grade static analysis tool engineered for high-velocity detection of zero-day malware and advanced persistent threats in files. GSDD instantly applies thousands of structural and behavioral rules to discover potential threats, in binary and non-binary code.

GateScanner DLP
AI-driven data loss prevention for file security

GateScanner DLP uses AI to stop sensitive information leaving your organization through files. It detects by meaning and business context, not only fixed patterns, and lets you define your own sensitive-information policies in plain natural language.

AI-powered semantic detection
Interprets content by meaning, context and your policies, including what fixed patterns cannot describe.

Three detection methods
AI analysis, regular expressions and document fingerprinting, with OCR to expose text embedded in images.

Flexible AI deployment
The engine runs on-premises; the AI model is separate, so you can use your own infrastructure or supported external AI services.

Standalone or integrated: use it as a standalone API or with GateScanner Mail Protection, Kiosk, Security Dome, Multi-source and CDR Integration Server. **Complements GateScanner CDR:** CDR covers threats in incoming files; DLP asks whether a file leaving your organization holds information that should not be disclosed.

PRODUCT FEATURES

File Support
300+ types including MS Office, PDF, media, EML, AutoCAD, DICOM, and password-protected archives

Scalability
Up to 10 scanning engines per grid with Active-Active on-the-fly scalability and zero-downtime expansion

DLP & Compliance
Anti-exfiltration and DLP capabilities with immutable audit trails and SIEM-compatible structured export

Integrations
Outlook, Salesforce, O365, MS Exchange, RBI solutions, legacy external security tools

Deployment
SaaS, on-premises virtual appliance, or private/public cloud - AWS, Azure, GCP.

Legacy Integration
Built-in integration with existing/legacy external security tools across all deployment models