



信頼と実績のテクノロジー

2013年の設立からSasa Softwareは、行政機関、軍需産業、金融機関、公共事業、保健医療機関を守ってきました。

外部の組織が実施した試験では、GateScanner®が検知不能な脅威による攻撃の99.9%を防止したことが実証されています。

業界の評価

Gartner
COOL
VENDOR
2020

受賞



お問い合わせ

本社:

Sasa Software (CAS) Ltd.
Telephone: +972-4-867-9959
Kibbutz Sasa, Israel
info@sasa-software.com
www.sasa-software.com

クロスドメイン環境のためのITセキュリティ

課題：マルチステージ型サイバー攻撃

ゼロデイ、エクスプロイトなど、コンテンツを武装化するファイルベースの攻撃は、検知技術を回避するため、外部ソースからファイルを受信することはリスクを伴います。今日のサイバー攻撃は、マルチステージで標的に近づいていき、組織の運用環境を損なおうとします。OT/ICSネットワークを始め、機密性の高いネットワークが狙われ、ひとつのセグメントに入り込むことに成功した悪意のあるファイルは、ほかのセグメントにも潜入し、環境全体の崩壊に至る可能性があります。

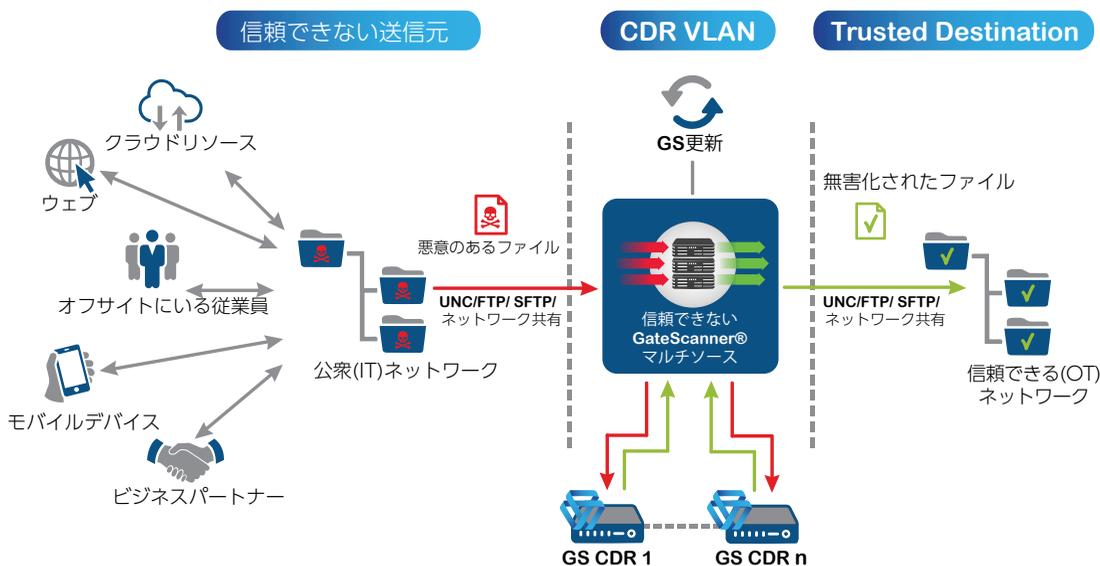
ソリューション

『コンテンツの非武装化と再構築』、『ファイル無害化』とも呼ばれるCDRテクノロジーは、次世代人工知能検知技術と、高度に最適化されたスキャン技術を駆使して、既知の脅威を検知し、検知不能な脅威からの攻撃を未然に防ぎます。GateScanner®CDRは、次世代人工知能検知技術と、高度に最適化されたスキャン技術を駆使して、ファイルの使用性、視認性、機能性を維持したまま、かつては見られなかったエクスプロイトやコンテンツを武装化するファイルベースの攻撃からも防御します。

GateScanner®マルチソース

GateScanner®マルチソースは、ネットワーク分離を行い、サードパーティーアプリケーションとAPIなしで統合を図って、機密ネットワーク間で安全にファイルの転送を可能にします。信頼できない着信ファイルの送信元を常に複数監視しながら、GateScanner®CDRを呼び出してポリシーを適用し、無害化されたファイルを信頼できる送信先に配送することで、攻撃が重要なネットワークセグメントに広がるのを防ぎます。このソリューションはさらに、高度なスケーラビリティと優れたモジュール性で、GateScanner® CDRを複雑で、高い安全性の求められるネットワークポロジにシームレスに統合します。

信頼できないネットワークと信頼できるネットワーク
信頼できないネットワークと信頼できるネットワークをつなぐGateScanner®マルチソース



GateScanner® CDR スキャンの特長

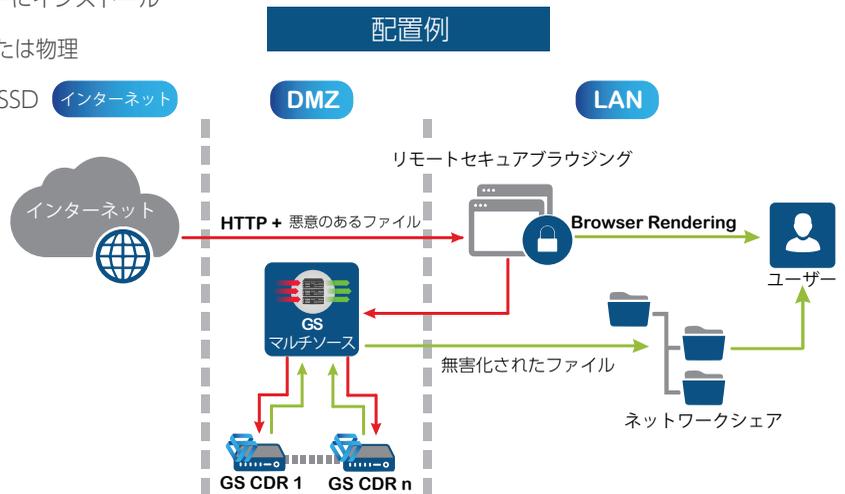
- ✓ **ファイル分解**：ファイルを基本コンポーネントに解体し、奥深く隠れた脅威を見つけ出して除去
- ✓ **脅威をディープスキャン**：複数のTrue Type解析エンジン、マルチアンチウイルス、次世代人工知能検知機能で埋め込みエレメントをディープスキャン。検知率を大幅に向上し、ファイルスプーフィング攻撃を防止します。送信元の信頼性は、ファイルシグネチャとマクロシグネチャで検証します。
- ✓ **ファイル無害化&再構築**：埋め込みエレメント、スクリプト、マクロ、リンクを除去することでファイルは無害化。ファイルの使用性、視認性、機能性を維持したまま、安全な要素で再構築し、無害のファイルの複製を生成します
- ✓ **外部ツールの統合**：サンドボックス/動的検査、次世代アンチウイルスなど、外部セキュリティソリューションも統合可能

GateScanner®マルチソースの特長

- ✓ FTP、FTPS、SFTP、UNC、SMB、共有/ローカルフォルダのファイル受信元と送信先をサポート
- ✓ **GateScanner®インジェクターとのシームレスな統合**：GSインジェクターの光学データダイオードと統合して一方向データ転送を実装
- ✓ **カスタマイズされたスキャンポリシー**：各ソースで専用のスキャンポリシーを定義。スキャン完了後、それぞれの送信元/送信先での処理結果についてアクティブディレクトリ (AD) ユーザーに通知することも可能です
- ✓ **セキュリティ第一の設計**：高度にモジュール化された設計のため、厳しいセキュリティ要件の複雑なネットワークポリシーともシームレスな統合が可能となり、一方向データフローを実現
- ✓ **スケーラビリティに優れた負荷分散**：高度にスケーラブルなActive/Active構成ロードバランサー内蔵。手動による介入は一切不要です
- ✓ **一元管理**：詳細なスキャン解析、SIEM/Syslog管理連携、自動更新など、すべて一括制御

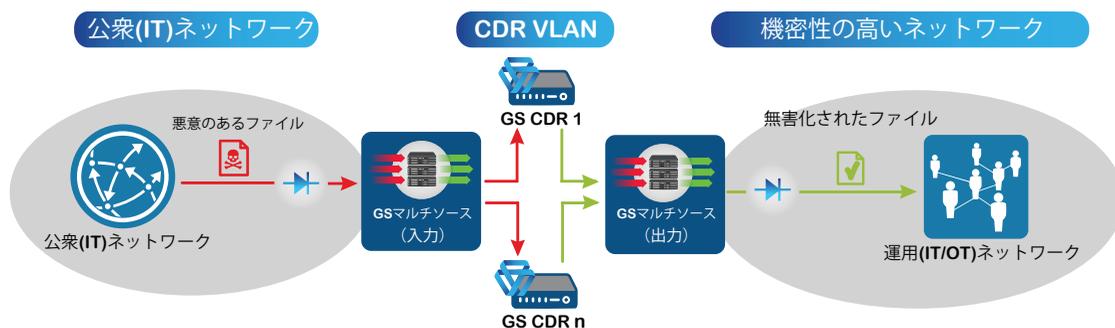
GateScanner®マルチソース

- ✓ **マルチソースのフロントエンド (I/O サービス)**：Windowsサーバーにインストール
システム要件：仮想CPU4コア、8GB RAM、250GB HD (SSD推奨)
- ✓ **スキャンエンジン**：Windows 10 IoTで事前構成済みの安全な仮想または物理ハードウェアとして供給
エンジンごとのシステム要件：仮想CPU4コア、8GB RAM、60 GB SSD
- ✓ **スキャンパフォーマンス**：エンジンごとに毎時最大15GB
- ✓ **対応ファイル形式**：MS Office全ファイル形式、PDF、メディアファイル (画像、音声、ビデオ)、AutoCad、アーカイブ、PST、.EML、インストールファイル、XML、HTML、その他のテキストファイル、医用画像ファイル (DICOM、カスタム) など数百種類のファイル形式に完全対応
- ✓ **配置方法**：オンプレミス、またはプライベートクラウドでサービスとして利用可能



活用事例 #1：リモートセキュアブラウジングとAPIなしで統合

ユーザーは、CitrixやSmartXなどのリモートセキュアブラウジングソリューションを使ってインターネットにアクセスします。ユーザーがダウンロードするファイルは、GSマルチソースで無害化されます。



活用事例 #2：データダイオードを使ったネットワーク分離

ユーザーは、信頼できないITネットワークを使ってインターネットにアクセスしますが、ダウンロードするファイルは、GSマルチソースで無害化されます。GSマルチソースは、データダイオードのGSインジェクターによって『入力』と『出力』のコンポーネントに分けられているため、運用(OT)ネットワークには安全性の高い一方向のファイル配送が保証されます。

*仕様書の内容及び機能は、予告なく変更する場合があります。
スキャン性能は、スキャンプロファイル、ファイルサイズ/構成、使用されるハードウェアによって異なります。
セキュリティの結果は使用されるスキャンするプロファイルによります。