



アプリケーションにCDRテクノロジーを統合

課題

ゼロデイ、エクスプロイトなど、最新技術を備えた検知ツールを回避するほど洗練されつつあるファイルベースの攻撃。この種類の攻撃はコンテンツを武装化するのが手口のため、ファイル転送、Webポータル、ブラウザ分離サービスのサードパーティアプリケーションからファイルを受け取ることはリスクを伴います。信頼できると思われたコンテンツ配信チャネルから悪意のあるファイルが受信、組織のデータセンターに保存されれば、重大なセキュリティインシデントに至る可能性があります。

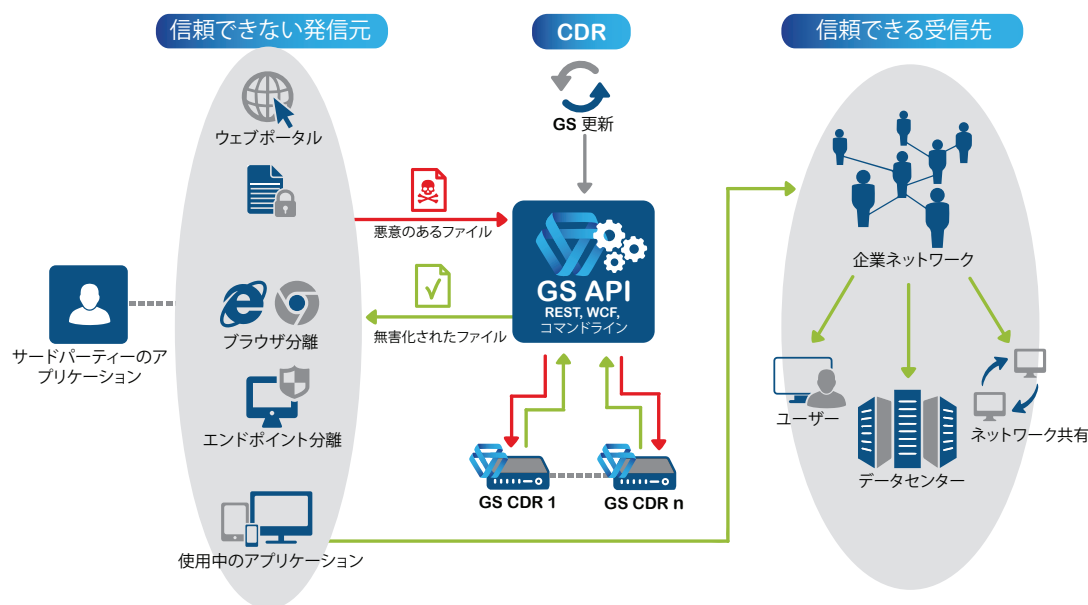
ソリューション

『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、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。Gate Scanner® 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® API

ITアドミニストレーターやMSSP、ISVが、当社のCDRテクノロジーを既存のアプリケーションとシームレスに統合できるようにするのがGate Scanner® APIです。堅牢かつ柔軟性に優れたプラットフォームで、ファイルを安全にGateScanner® CDRエンジンリッドに送信し、無害化されたファイルを送信します。インテグレーションは、業界標準REST API使用のWebベース管理アプリケーションで一元管理。一度に複数のアプリケーションを接続でき、セキュリティポリシーに確実に遵守しつつ、ステータスを完全に把握することができます。

サードパーティアプリケーションにはGate Scanner® APIで接続



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

Gate Scanner® 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を無害化。未知の脅威を機能停止に追い込んだ後は、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

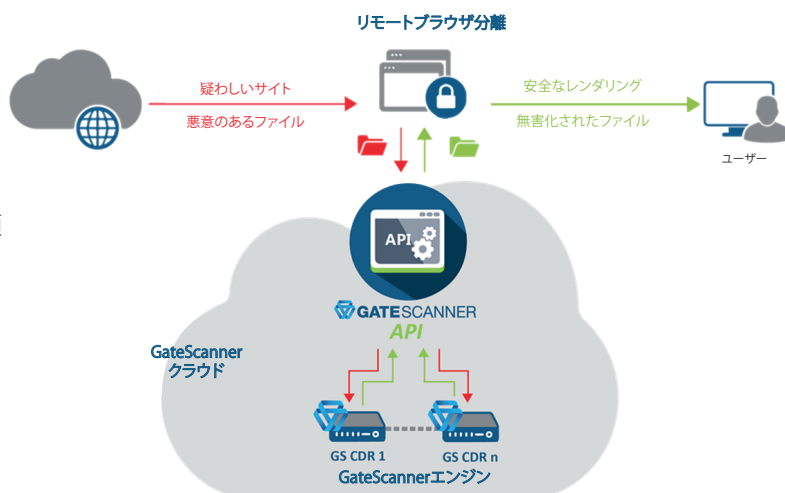
Gate Scanner® REST API の技術的特長

- ✓ **REST APIサービス**
複数のアプリケーションと高速連携
- ✓ **操作モード**
同期/非同期モード
- ✓ **ドキュメンテーション**
豊富な資料とコードサンプル付き
- ✓ **処理容量**
数千件のリクエストを並列処理。複数のサードパーティアプリケーションで、インストールパッケージを始め、大量の複雑なファイルを同時に処理します
- ✓ **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
- ✓ **カスタマイズ可能なスキャンポリシー**
各アプリケーションでユーザーとセキュリティープロファイルに合わせた専用スキャンポリシーを柔軟にカスタマイズ
- ✓ **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
- ✓ **安全性**
厳しいセキュリティ要件を満たす詳細構成設定で複雑なネットワークポロジとシームレスな連携を実現

GateScanner® API の仕様

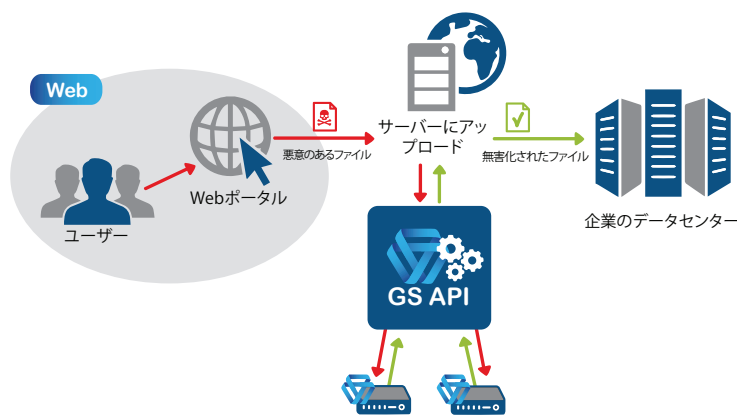
- ✓ **APIサービス**: Windowsサーバーにインストール
システム要件: 仮想CPU4コア、8GB RAM、250 GB HD (SSD推奨)
- ✓ **スキャンエンジン**: Windows 10 IoTで事前構成済みの安全な仮想または物理ハードウェアとして供給
エンジンごとのシステム要件: 仮想CPU4コア、8GB RAM、60 GB SSD
- ✓ **スキャンパフォーマンス**: エンジンごとに毎時最大15GB
- ✓ **対応ファイル形式**: MS Office全ファイル形式、PDF、メディアファイル(画像、音声、ビデオ)、AutoCad、アーカイブ、PST、.EML、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

リモートブラウザ分離



ブラウザ分離

ユーザーはリモートブラウザ分離(RBI)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。ダウンロードされたファイルはGame Scanner CDRを使って無害化され、ユーザーのエンドポイントに保存されます。



文書のアップロード

ユーザーがWebポータルにアップロードしたファイルは、REST APIでGSに送られ、無害化された後、組織のデータセンターに保存されます。

※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。

スキャンパフォーマンスは、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。適用されるセキュリティ保護は、使用するスキャンプロファイルによります。