



CDRプロテクション内蔵のメールセキュリティ

課題

電子メールは極めて重要な通信チャネル。そのため標的となりやすい攻撃ベクトルです。脅威はますます高度化し、ソーシャルエンジニアリング手法を利用する、狙いを定めた攻撃が後を尽きません。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、検知技術を回避できます。セキュアメールゲートウェイ (SEG) の検知を逃れ、悪意あるコードを含むメールが組織内に潜入すると、情報漏洩やランサムウェアによるインシデントに至ることがあります。そのため、防止に重点を置いた、新しいアプローチが求められます。

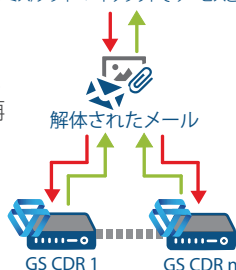
ソリューション

Gate Scanner®メールは、すべての着信メールを疑わしいものとして扱い、組織内メールリレーサーバーやSEGでもうひとつのセキュリティ層として機能します。Gate Scanner®メールは、従来の検知技術の代わりに、『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テクノロジーで、メールのコンテンツを無害化し、使用性、視認性、機能性はそのままの、安全な複製を作成します。Gate Scanner® CDRは、APTやランサムウェアなど、高度化され、検知不能な脅威に対しても威力を発揮します。

GateScanner®メールの典型的な配置例



セキュアメールゲートウェイはSMTPリレー経由でメールが送られてくると、Gate Scannerメールはそれを分解し、各埋め込みエレメントにCDRを適用、無害化した後、再構築して組織のメールサーバーに送ります。



GateScanner® メール・スキャンの特長

- ✓ **当社独自のメール分解テクノロジー:** RFC 2822形式に沿ってメール本文、埋め込みエレメント、添付ファイルをディープスキャン
- ✓ **脅威をディープスキャン:** 複数のTrue Type解析エンジン、マルチアンチウィルス、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
- ✓ **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。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
- ✓ **暗号化されたメディアとファイル:** パスワード保護されたファイルやハードウェア暗号化されたメディアを自動スキャン
- ✓ **パスワード保護されたファイルのスキャン:** ファイルをスキャンし、暗号化ファイルを悪用する脅威の検知回避を防止。ファイルパスキーの使用をユーザーに許可するオプションあり
- ✓ **電子署名されたPDFファイルの検証:** 使用性、視認性、機能性はそのままの、無害化されたファイルの複製
- ✓ **外部セキュリティソリューションとの統合:** サンドボックスや次世代アンチウィルスなどの外部セキュリティソリューションと統合、組織の既存のセキュリティ資産のレバレッジ
- ✓ **外部ツールの統合:** サンドボックス/動的検査、次世代アンチウィルスなど、外部セキュリティソリューションも統合可能。組織内の既存セキュリティ資産を最大限に活用します
- ✓ **ディープリンクの分類:** クラウドベースのメール本文や添付ファイルに含まれるリンクをリアルタイムで検査

信頼と実績

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®メールの特長

- ✓ Office365 Exchangeと統合。MXレコードの変更不要
- ✓ クラウドやオンプレミスのセキュアメールゲートウェイ（SEG）とシームレスに統合
- ✓ ドメイン、ユーザーグループ、アドレスごとにポリシーのカスタマイズが可能、アクティブディレクトリ対応
- ✓ 例外やカスタム定義のユーザー通知に沿ってメッセージ再構築のカスタマイズが可能
- ✓ メッセージのアーカイブと隔離
- ✓ スキャンアクティビティ、パフォーマンス、例外の詳細をわかりやすくレポートシステムで見える化、イベントごとにドリルダウン可能
- ✓ 優れたスケーラビリティ。手動による介入は一切不要
- ✓ 詳細なスキャン解析、SIEM/Syslog管理連携、自動更新など、すべて一元管理

GateScanner®メールのパフォーマンス

- ✓ **フルCDR機能（ディープスキャンとメール無害化）使用の場合のスキャン容量※：**
GateScanner®メールフロントエンドごとの毎時メール処理総数：GSエンジン7台で最大100,000件、GSエンジン4台で50,000件、GSエンジン2台で20,000件
15%が添付ファイル付きメールであることを想定
※最適化されたリソースを使って試験済み

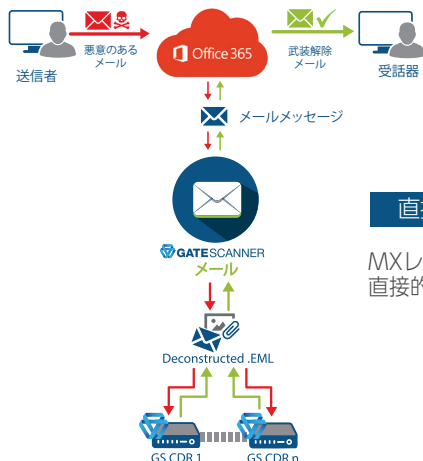
GateScanner®メールの仕様

- ✓ **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
- ✓ **GateScanner®メールフロントエンド：**Windowsサーバーにインストール
システム要件：仮想CPU8コア、16 GB RAM、600 GB HDD（SSD推奨）
- ✓ **GateScanner®エンジン：**Window 10 IoTで事前構成済みの仮想アプライアンスとして供給
システム要件：仮想CPU4コア、8 GB RAM、60 GB SSD
- ✓ **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

メールセキュリティの比較

利点	セキュアメールゲートウェイ	GateScanner®メール
アンチスパム、アンチフィッシング、URLフィルタリング	✓	✓
既知の脅威のスキャン	✓	✓
未知の脅威の検知	-	✓
検知不能な脅威の防止	-	✓

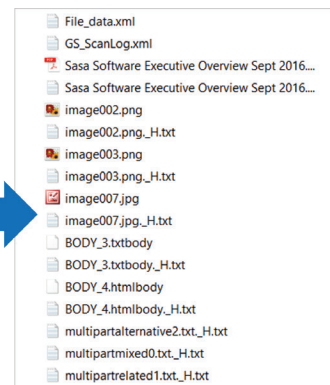
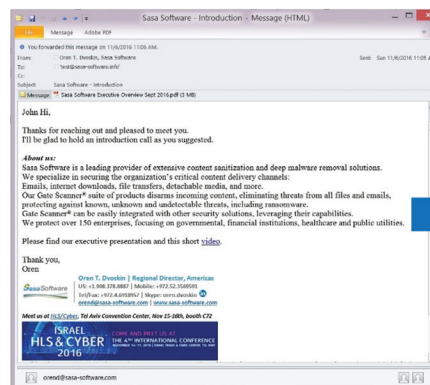
検知不能なGate Scanner®メールは、メール内に潜む高度で検知不能な悪意ある脅威をブロックするパワフルな技術です



直接的な Office 365 統合

MXレコードの変更を伴わない
直接的なクラウドベースのO365統合

メール分解のサンプル



メッセージ1件に攻撃ベクトル複数
Gate Scanner®メールで分解されるメールのメッセージ

*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。