SONICWALL

SonicWall Capture Security appliance 1000

クラウドでの解析のためのファイル送信がコンプライアンスおよびポリシーにより禁止されている、または全データを自社組織内に留め置きたいお客様向に、SonicWall Capture Security appliance™(CSa) はCapture Advanced Threat Protection™ (ATP) およびサンドボックス・マルウェア解析機能をオンプレミスにて提供いたします。CSa 1000は、他のSonicWall製品から送られてくる不審なファイルを解析し、お客様がファイルを保持したまま、これまでは検知できなかった脅威を迅速かつ高精度に検出することができます。さらに、CSaのREST API機能により、脅威インテリジェンスチーム、サードパーティのセキュリティシステム、公開APIとの統合が可能なソフトウェアスタックがこの非常に効果的なファイル解析機能の利点を利用できるようになります。

CSaは、レピュテーションベースのチェック、静的ファイル解析およびSonicWallが特許を取得したReal-Time Deep Memory Inspection™ (RTDMI) エンジンを組み合わせて動的解析を行い、悪意のあるファイルの検出率を最大にするだけではなく、これを最短時間で効率的に行えるようにします。SonicWallセキュリティ製品エコシステムは既にクラウド型Capture ATP解析と完全に統合されており、Block Until Verdict (判定が出るまでの間は遮断)などの機能によりインラインセキュリティを強化できます。

クラウドCapture ATPの代わり、SonicWall製品がCSaシリーズに接続されている場合も、同じ機能がサポートされます。

RTDMI

特許出願中のSonicWallのReal-Time Deep Memory Inspection (RTDMI) ファイル解析エンジンは、メモリ内のアプリケーションの挙動をモニタリングすることで疑わしいファイルを解析する新しい方法です。RTDMIは、最新のマルウェアがネットワーク解析やサンドボックス解析を回避するために展開する可能性のある難読化技術や暗号化技術を見破り、文書、実行ファイル、アーカイブファイルやその他のさまざまな種類のファイルによる攻撃を極めて高精度に検出することができます。

リアルタイム保護

レピュテーションチェック、グローバルインテリジェンスチェック、静的解析およびRTDMI技術を組み合わせて協調して動作させることで迅速に結果が得られるため、SonicWall製品群にあるBlock Until Verdictのような技術が可能になります。この機能により、検査が完了しCapture ATPまたはCSaによる判定が下されるまでまでは、疑わしいファイルをエンドユーザーがダウンロードすることをファイアウォール上のファイル検査ポリシーで防止することが可能になります。

メリット:

- RTDMIによるメモリーベースの検査
- レピュテーションチェック、静的解析および動的解析によるマルチステージ解析
- 脅威解析のためのAPIアクセス
- 広範囲のファイルタイプをサポート
- 判定中遮断機能
- 高いセキュリティ有効性
- レポーティングとロールに基づくアクセス

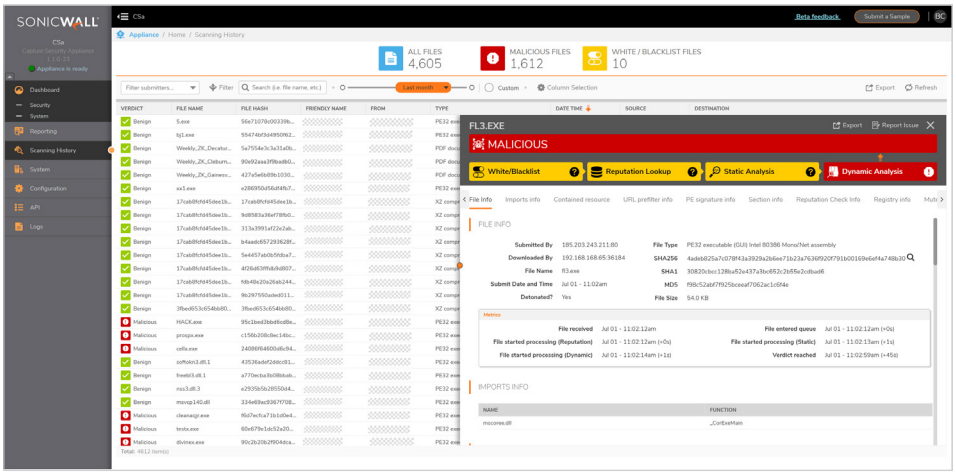
1.解析スループットはネットワーク接続性、ファイルの種類、圧縮レベルに依存することから、公表された値とは異なることがあります。
2.ハードリミットはありませんが、各デバイスが提出するファイル数によってデバイス数が決定されることになります。推奨範囲は公表時において約250デバイスです。
3.SonicOS 6.5.4.6以降を動作させることができるすべてのTZシリーズ、NSaシリーズおよびSuperMassiveシリーズ。SuperMassive 9800およびNSsp 12000シリーズではサポートされていません。

多くの経験に基づく信頼と利益

- CSaは、世界中で15万人以上のお客様に信頼され使用されているクラウドベースのサービスであるSonicWallのCapture　ATPの技術をアプライアンスの形態に統合しています。
- また、CSaはSonicWall　Capture　ATPファイル解析を介して世界中で収集された脅威インテリジェンスと同期するために、定期的に最新インテリジェンスを取得します。

報告、解析および管理

- CSaは、簡単に操作できるダッシュボードとファイル解析履歴を用いてすべてのソースから提出されたファイルについての知見を示すことで、解析のために提出されたファイルに関する頻度、ソース、判定などの情報を提供します。
- レポート機能により、組織全体にわたるATP保護について全体的な見解が得られ、各ロールに基づいて構成された定期的レポートのスケジュールを立てることができます。
- 管理者は、CSa 1000へのアクセスをさまざまなロールにきめ細かく付与することで、UIの一部へのアクセスを制限することができます。
- セキュリティアナリストは、スキャン履歴にアクセスすることで、ホワイトリスト/ブラックリストを変更し、デバイスを許可し、偽陽性または偽陰性の疑いを報告することができます。
- ネットワークレベルの管理者に対し、アプライアンスの動作設定を許可する方で、機密保持上のため提出されたファイルおよびそのソースの閲覧を制限することも可能です。



機能

- レピュテーション判定およびグローバル判定の検索（構成可能）
- 静的解析およびRTDMIによる動的解析
- ハッシュ/ドメインのホワイトリスト/ブラックリスト
- 構成可能なレポートのスケジュール
- ロールに基づく管理（構成可能な役割）
- 管理 – 専用管理インターフェイスまたは通常のネットワークインターフェイスを介したHTTPSまたはSSH
- SSHコンソールへのアクセス
- ログインと警告
- 自動ホワイトリスト/ブラックリストによる偽陽性および偽陰性の報告
- 直接接続またはVPN経由（IPアドレス可能）
- 閉域ネットワークでの運用
- ファイルの提出および解析のためのREST APIサポート
- Secure Bootで強化されたOSと、改ざん防止のためのチェイン・トラスト
- ローカルロギング

1.解析スループットはネットワーク接続性、ファイルの種類、圧縮レベルに依存することから、公表された値とは異なることがあります。
2.ハードリミットはありませんが、各デバイスが提出するファイル数によってデバイス数が決定されることになります。推奨範囲は公表時において約250デバイスです。
3.SonicOS 6.5.4.6以降を動作させることができるすべてのTZシリーズ、NSaシリーズおよびSuperMassiveシリーズ。SuperMassive 9800およびNSsp 12000シリーズではサポートされていません。

展開オプション

- SonicWall CSaの展開は迅速・簡単で、必要とされるのは基本的なネットワークとレポーティングの設定であり、デバイスにアクセスして開始できます。
- CSaはIPアドレスでアクセスできるように構築されており、したがって、解析用のファイルを提出するデバイスによるアクセスが可能である限りどこにででも展開できます。

CSa 1000には主に3つの展開方法があります。

単一オフィス/単一ロケーション

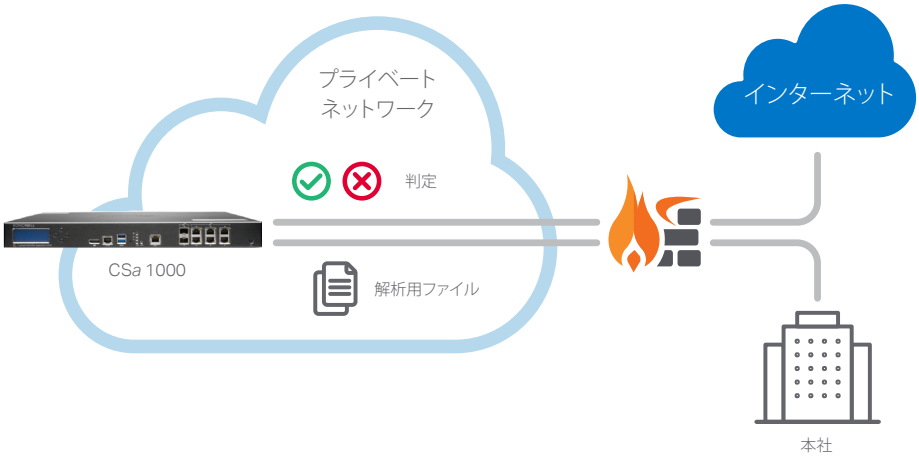
- CSaは、それを使用する製品がIPを介してアクセスできる限り、ネットワーク内のどこにでも展開できます[1]。
- CSaが展開した後は、疑わしいファイルをATP解析用のクラウドではなくCSaにリダイレクトするようにファイアウォールおよびメールセキュリティシステム（その他のソリューションについては対応待ち）を構成できます。

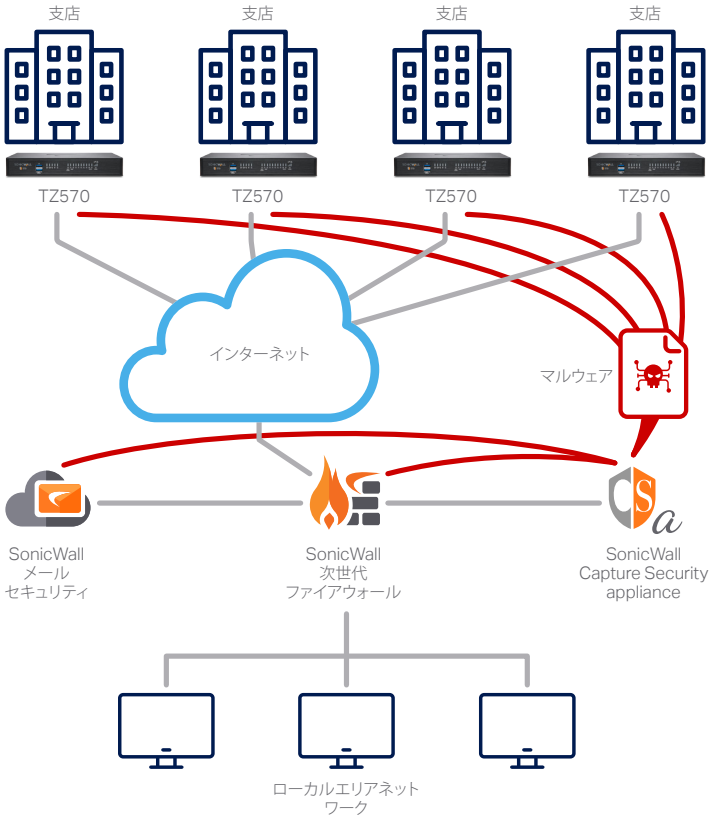
分散されたエンタープライズ/マルチロケーション

- 中央本社データセンターまたはすべてのデバイスでアクセス可能なリモートデータセンターのいずれかにCSaデバイスを展開して、単一のCSaデバイスへのアクセスを共有するように複数のオフィス/拠点を構成できます。
- インターネットまたはVPN経由で直接アクセスすることができます。
- CSaをポイントするSonicWallシステムの大規模構成を行う場合、GMSまたはクラウドベースのNSM集中管理ソリューションにより迅速な構成と展開が可能です。

REST APIゲートウェイ

- CSaシリーズはREST　APIインターフェースを備えています。このインターフェースを使用することで、脅威インテリジェンスチームが独自のスクリプト、ウェブ・ポータル統合およびその他のセキュリティ製品を使用して解析のファイルを提出し、その結果を問合せできます。
- CSaのAPIスクリプティングを開始する方法およびコードーサンプルについては、https://github.com/sonicwallをご覧ください。

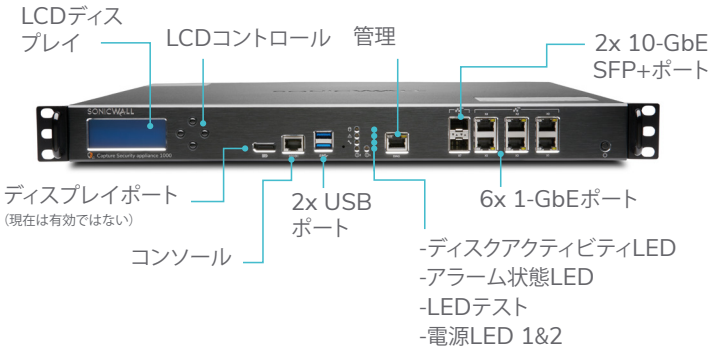


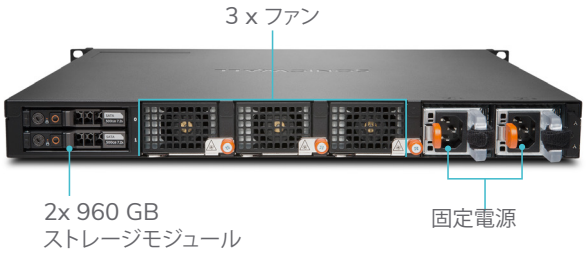


*[1]SonicWallのファイアウォールには、2259ポートのUDPを経由したアクセスも必要です。

1.解析スループットはネットワーク接続性、ファイルの種類、圧縮レベルに依存することから、公表された値とは異なることがあります。
2.ハードリミットはありませんが、各デバイスが提出するファイル数によってデバイス数が決定されることになります。推奨範囲は公表時において約250デバイスです。
3.SonicOS 6.5.4.6以降を動作させることができるすべてのTZシリーズ、NSaシリーズおよびSuperMassiveシリーズ。SuperMassive 9800およびNSsp 12000シリーズではサポートされていません。

CSa 1000





SonicWall CSa 1000仕様

機能	
レビューションおよびグローバル脅威検索スループット(1時間あたりのファイル数)[1]	12,000
実環境ファイルミックススループット(1時間あたりファイル数)[1]	2500
動的解析 (RTDMI) スループット(1時間あたりのファイル数)[1]	300
最大ファイルサイズ	100 MB
サポートする最大デバイス数[2]	パフォーマンスに基づく
アーカイブスキャンの最大深	3
REST-APIサポート	有り
サポートするSonicWallデバイス	TZ、NSa、SuperMassive(SonicOS 6.5.4.6以降を実行)[3] Email Security 10.X NSsp 15000シリーズ - 対応予定 NSvシリーズ(7.X以降) - 対応予定
サポートされているファイルの種類	.cpl .dll .drv .exe .elf .ocx .scr .sys .doc .dot .wbk .docx .docm .dotx .dotm .docb .xls .xlt .xlm .xlsx .xlsm .xltx .xltm .xlsb .xla .xlam .xll .xlw .ppt .pot .pps .pptx .pptm .potx .potm .ppam .ppsx .ppsm .sldx .sldm .o .dylib .bundle .dmg .pdf .jar .apk .rar .bz2 .bzip2 .7z .xz .gz .zip
データ保持期間	無制限、ストレージによる制限
ストレージ	2 x 1TB SATA(RAID 1)
インターフェイス	(6)-ポート 1GE、(2)-ポート10Gb SFP+、(2) USB、(1) コンソール
専用ポート管理	有り (X0)
認証	FIPS 140-2取得予定
製品の特性	
ラック実装高	1U
寸法	17.0 x 16.5 x 1.75 in (43 x 41.5 x 4.5 cm)
アプライアンスの重量	8.3 kg
暗号化データのアクセラレーション (AES-NI)	有り
MTBF (@ 25°Cまたは77°F)(単位は時間)	129,601
電源	冗長電源、ホットスワップ対応
入力定格	100~240 VAC、1.79 A
消費電力	114 W
総発熱量	389 BTU
環境規格	WEEE、EU RoHS、China RoHS
非動作時の耐衝撃性	110 g、2ミリ秒
エミッション規格	FCC、ICES、CE、C-Tick、VCCI;MIC
安全規格	TUV/GS、UL、CE PSB、CCC、BSMI、CB scheme
動作温度	0°C~40°C (32°F~104°F)
TPM	有り

1.解析スループットはネットワーク接続性、ファイルの種類、圧縮レベルに依存することから、公表された値とは異なることがあります。
2.ハードリミットはありませんが、各デバイスが提出するファイル数によってデバイス数が決定されることになります。推奨範囲は公表時において約250デバイスです。
3.SonicOS 6.5.4.6以降を動作させることができるすべてのTZシリーズ、NSaシリーズおよびSuperMassiveシリーズ。SuperMassive 9800およびNSsp 12000シリーズではサポートされていません。

製品	SKU
Capture Security Appliance CSA 1000	02-SSC-2853
インテリジェンスアップデートとサポートバンドルを伴うCapture Security Appliance CSA 1000 – 1年	02-SSC-5637
インテリジェンスアップデートとサポートバンドルを伴うCapture Security Appliance CSA 1000 – 3年	02-SSC-5638
インテリジェンスアップデートとサポートバンドルを伴うCapture Security Appliance CSA 1000 – 5年	02-SSC-5639

サービス（CSa 1000の動作に必要です。 CSaにファイルを送信するすべてのデバイスは、Capture ATPのライセンスが要ります。）	SKU
SonicWall CSA 1000のインテリジェンス更新、有効化およびサポート（1年）	02-SSC-4712
SonicWall CSA 1000のインテリジェンス更新、有効化およびサポート（2年）	02-SSC-4713
SonicWall CSA 1000のインテリジェンス更新、有効化およびサポート（3年）	02-SSC-4714
SonicWall CSA 1000のインテリジェンス更新、有効化およびサポート（4年）	02-SSC-4715
SonicWall CSA 1000のインテリジェンス更新、有効化およびサポート（5年）	02-SSC-4716
SonicWall CSA 1000のインテリジェンス更新、有効化およびサポート（6年）	02-SSC-4717

REST APIの有効化（このサービスはREST APIの動作にのみ必要です。 インテリジェンスアップデート、有効化およびサポートサービスに先立って適用する必要があります。）	SKU
SonicWall Capture appliance CSA 1000 のREST API有効化（1年）	02-SSC-4706
SonicWall Capture appliance CSA 1000 のREST API有効化（2年）	02-SSC-4707
SonicWall Capture appliance CSA 1000 のREST API有効化（3年）	02-SSC-4708
SonicWall Capture appliance CSA 1000 のREST API有効化（4年）	02-SSC-4709
SonicWall Capture appliance CSA 1000 のREST API有効化（5年）	02-SSC-4710
SonicWall Capture appliance CSA 1000 のREST API有効化（6年）	02-SSC-4711

1.解析スループットはネットワーク接続性、ファイルの種類、圧縮レベルに依存することから、公表された値とは異なることがあります。
2.ハードリミットはありませんが、各デバイスが提出するファイル数によってデバイス数が決定されることになります。推奨範囲は公表時において約250デバイスです。
3.SonicOS 6.5.4.6*以降を動作させることができるすべてのTZシリーズ、NSaシリーズおよびSuperMassiveシリーズ。*SuperMassive 9800*およびNSsp 12000シリーズではサポートされていません。*

SonicWallについて

SonicWallは、Boundless Cybersecurityを提供することにより、誰もがリモート、モバイル状態で危険にさらされながら仕事をするという超分散化時代のビジネスの現実に対処します。未知の領域を探求し、リアルタイムの可視性を提供しながら経済の大躍進を実現しているSonicWallは、サイバーセキュリティ業務上の課題を解決して世界中の企業や政府、SMBをサポートします。詳細は、www.sonicwall.comをご確認ください。

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
詳細については弊社ウェブサイトをご覧ください。
www.sonicwall.com

Datasheet-CaptureClient-US-COG-2099