SonicWall Capture Advanced Threat Protection サービス

ゼロデイなどの未知の攻撃を検出して阻止

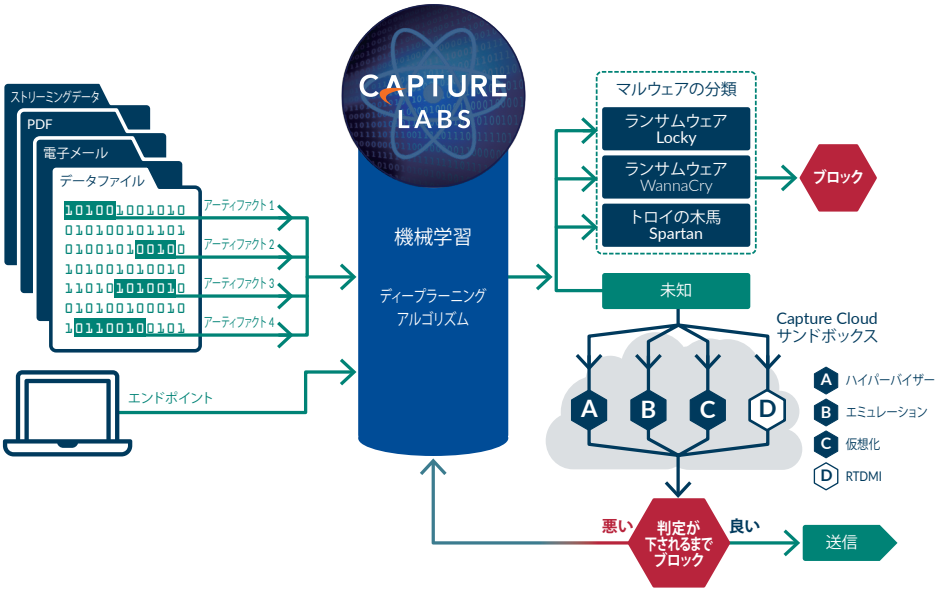
ゼロデイ脅威を効果的に防御するには、マルウェア分析テクノロジーを搭載し、検知を回避する高度な脅威やマルウェアを現在および将来にわたって検出できるソリューションが必要です。

SonicWall ファイアウォールとともに使用可能なクラウドベースのサービスである SonicWall Capture Advanced Threat Protection サービスは、高度な脅威を検出し、判定が下るまでゲートウェイでブロックすることで、高まり続けるゼロデイ脅威の危険からお客様を保護します。このサービスは、フルシステムエミュレーションや仮想化技術など、多層型のサンドボックス機能を組み合わせて疑わしいコードの動作を分析する、唯一の高度な脅威検出オファリングです。この強力な組み合わせにより、コンピューティング環境に固有の回避されやすい単一エンジンのサンドボックスソリューションよりも多くの脅威を検出できます。

このソリューションはトラフィックをスキャンし、疑わしいコードを分析対象として抽出しますが、他のゲートウェイソリューションとは異なり、さまざまなサイズおよび種類のファイルを分析できます。グローバルな脅威インテリジェンスインフラストラクチャにより、新たに特定された脅威の修復シグネチャがすべての SonicWall Network Security Appliance へ迅速に配布されるため、その後の侵入を防ぐことができます。お客様は、高度なセキュリティによる効果的な防御、迅速な応答時間、総所有コストの削減といった恩恵が受けられます。

導入効果：

- 未知の脅威に対する高いセキュリティ効果
- ほぼリアルタイムのシグネチャ配布により、その後の攻撃を阻止
- 総所有コストの削減



未知の攻撃やゼロデイ攻撃をゲートウェイで阻止する、クラウドベースのマルチエンジンソリューション

ゼロデイ脅威の防御効果を最大限に高めるため、このソリューションは、脅威状況の変化にともなって、新しいマルウェア分析テクノロジーを動的に追加するよう設計されています。

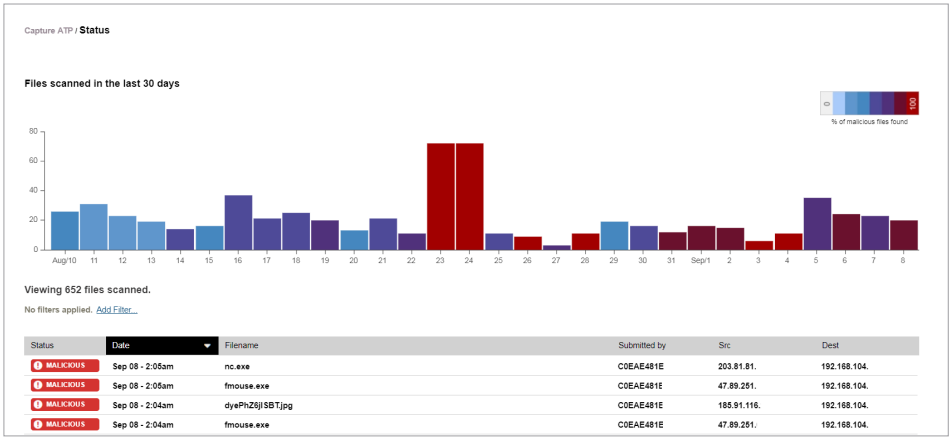
特長

マルチエンジンによる高度な脅威分析 — SonicWall Capture サービスは、ファイアウォールの脅威防御を拡張し、ゼロデイ攻撃を検出して阻止します。ファイアウォールはトラフィックを検査し、侵入や既知のマルウェアを検出してブロックします。疑わしいファイルは、分析用に SonicWall Capture Cloud に送られます。仮想サンドボックス機能、フルシステムエミュレーション、ハイパーバイザーレベルの分析テクノロジーを備えたマルチエンジンのサンドボックスプラットフォームは、疑わしいコードを実行して動作を分析し、悪意のある活動を包括的に監視しながら、回避戦術に対抗し、ゼロデイ脅威の検出を最大限に高めます。

さまざまな種類のファイルを分析 — このサービスは、実行可能プログラム (PE)、DLL、PDF、MS Office ドキュメント、アーカイブ、JAR、APK など、さまざまなサイズおよび種類のファイルのほか、Windows、Android をはじめとする多くのオペレーティングシステムの分析に対応しています。管理者は、分析対象としてクラウドに送信するファイルを、ファイルの種類やサイズ、送信者、受信者、プロトコルに基づいて選択または除外することで保護をカスタマイズできます。管理者は、分析対象のファイルを手動でクラウドサービスに送信することもできます。

判定が下るまでブロック — 悪意がある可能性のあるファイルがネットワークに侵入するのを防ぐため、分析対象としてクラウドサービスに送信されたファイルを、判定が下るまでゲートウェイで保持できます。

修復シグネチャの迅速な配布 — 悪意のあるファイルであることが確認されると、SonicWall Capture サブスクリプションが有効なファイアウォールにシグネチャがただちに配布され、その後の攻撃が阻止されます。さらに、SonicWall Capture Labs 脅威研究チームにマルウェアが送信され、さらに詳しく分析されて、ゲートウェイアンチウイルスと IPS シグネチャデータベースに脅威情報が取り込まれます。加えて、マルウェアは、URL、IP、ドメインの評価データベースにも 48 時間以内に送信されます。

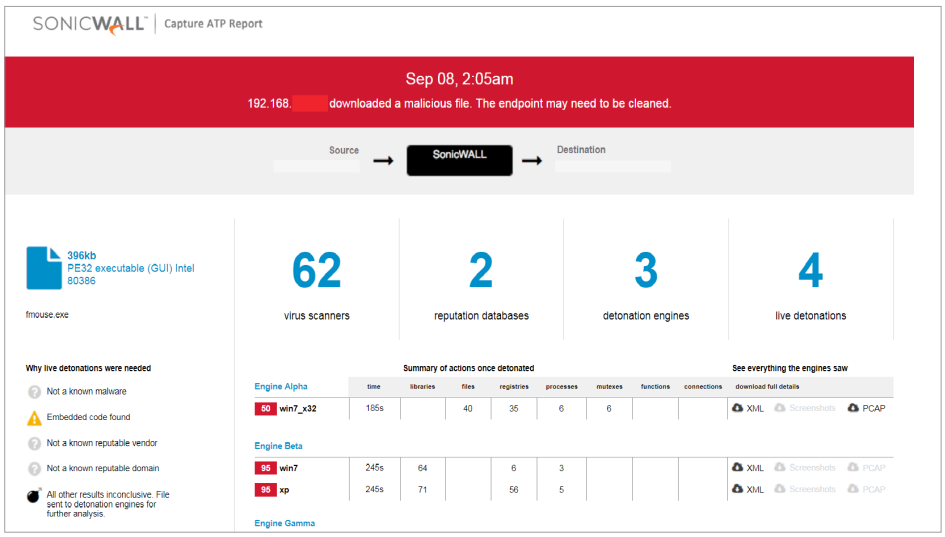


SonicWall Capture のレポートページには、一目でわかる日々の結果が表示されます。レポートのカラーバーは、マルウェアが発見された日数を示します。管理者は、日々の結果を個別にクリックしてフィルタを適用し、悪意のあるファイルを結果と併せて表示できます。

レポートとアラート — SonicWall Capture サービスには、一目でわかる脅威分析ダッシュボードとレポートが用意されており、サービスに送信されたファイルの分析結果 (送信元、送信先、要約のほか、実行されたマルウェアアクションの詳細を含む) が詳しく表示されます。ファイアウォールログのアラートは、SonicWall Capture サービスに送信された疑わしいファイルについて通知し、ファイル分析の判定を示します。

当社について

創設後 25 年以上にわたり、SonicWall はこの業界の信頼できるセキュリティパートナーとして存在しています。ネットワークセキュリティから、アクセスセキュリティ、電子メールセキュリティまで、SonicWall は自社の製品ポートフォリオを継続的に進化させることで、組織の革新、促進、成長を可能にします。世界の約 200 の国と地域に 100 万台を超えるセキュリティデバイスを持つ SonicWall は、お客様が自信を持って未来を受け入れられるようにします。



分析したファイルの詳細な分析レポートを入手して、改善を図ることもできます。

サポートされるプラットフォーム

SonicWall Capture サービスは、SonicOS 6.2.6 以降を実行する、次の SonicWall ファイアウォールでサポートされています。

SuperMassive 9800
SuperMassive 9600
SuperMassive 9400
SuperMassive 9200

NSA 6600
NS*a* 5650
NS*a* 4650
NS*a* 3650
NS*a* 2650

TZ600
TZ500 および TZ500 Wireless
TZ400 および TZ400 Wireless
TZ300 および TZ300 Wireless

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

DataSheet-CaptureAdvancedThreatProtection-US-VG-MKTG2101