SonicWall Capture Client

有効的な脅威検知と人の手を介さない自律的なインシデント対応

ランサムウェアやその他の悪意のあるマルウェアを用いた攻撃の脅威がますます増加しています。それに伴い、エンドポイントコンプライアンスのみを基準としていては、クライアント保護ソリューション効果を測定できないことが明らかになりました。従来のウイルス対策技術では、新興のマルウェアや回避技術のペースに対応できない、時間のかかるシグネチャベースのアプローチが採用されています。

さらに、在宅勤務、モビリティ、BYODの急増に伴い、どこにいてもエンドポイントに対して、一貫した保護、アプリケーションの脆弱性に関する知識、ウェブポリシーの実施を提供することが急務といえます。SonicWall Capture Clientは、複数のEPPおよびEDR機能を備えた統合エンドポイントです。

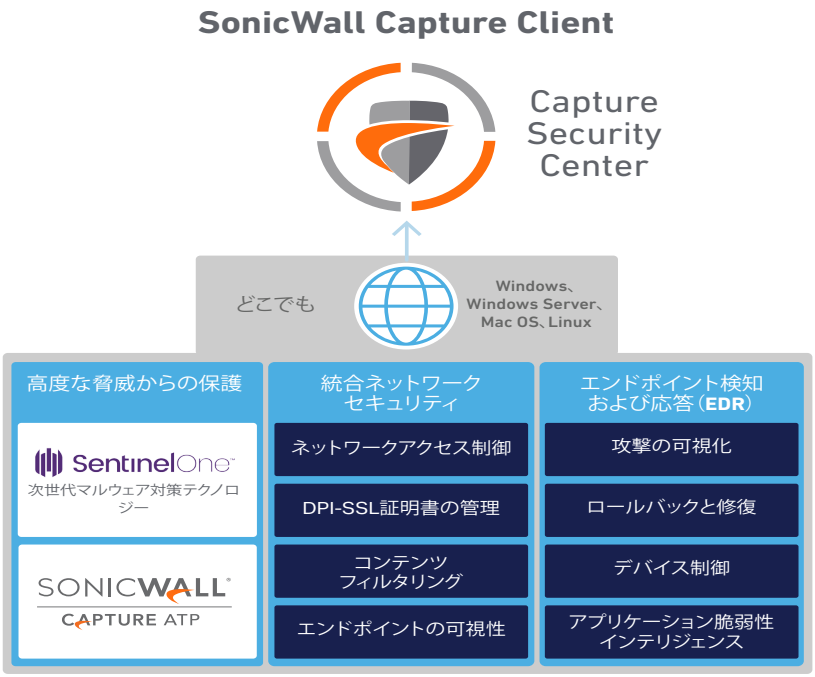
ハイライト

- 高い有効性とノイズのない実用的な脅威検知
- ネットワークおよびエンドポイントのセキュリティを強化する、真のマルチテナント機能を備えた、クラウド提供型の集中管理
- 最新の敵対者を阻止する使いやすくて直感的なソリューションにより、セキュリティチームやIT チームの強化とレベルアップを実現

エンドポイントセキュリティを
自分の組織に合わせる

要約を読む：sonicwall.com

データシート



Capture Clientは、NGAV SentinelOneを活用した行動ベースの高度な脅威保護を適用します。

Capture ATPの統合により、さらに効果的なセキュリティと迅速な応答を実現し、総所有コストを抑えます。

機能と利点

継続的な行動監視

- ファイル、アプリケーション、プロセス、ネットワークアクティビティの完全なプロファイルを把握
- ファイルベースのマルウェアとファイルレスマルウェアの両方に対応する保護
- 360度攻撃ビューと実用的なインテリジェンスを提供

脅威ハンティング

- 深い可視性を活用した、Windows、MacOS、Linuxデバイスの挙動指標およびIOC（セキュリティ侵害インジケーター）に基づく脅威の検索
- カスタムルールとアラートにより脅威ハンティングと対応を自動化する

Capture Advanced Threat Protection（ATP）の統合

- Windowsデバイス上の疑わしいファイルを高度なサンドボックス分析のために自動的にアップロード
- タイミング遅延が組み込まれたマルウェアなど、休眠中の脅威を実行前に検出
- ファイルをクラウドにアップロードすることなく、Capture ATPのデータベースでのファイル判定を参照する

独自のロールバック機能

- 脅威を完全に除去するというポリシーに対応
- 悪意のあるアクティビティが始まる前に、自動的にエンドポイントを元の健全な状態に復元

多層ヒューリスティックベース技術

- クラウドインテリジェンス、高度なスタティック分析、ダイナミック行動保護の活用
- 攻撃中または攻撃後の、既知のマルウェアおよび未知のマルウェアに対する保護と是正

アプリケーション脆弱性インテリジェンス

- インストールされたすべてのアプリケーションと関連するリスクのカタログ
- 既知の脆弱性をCVEや深刻度レベルといった詳細と併せて検証
- このデータを使用してパッチ適用の優先順位を決定し、攻撃対象を削減

エンドポイントネットワーク制御

- ファイアウォールのような制御をエンドポイントに追加
- 追加の隔離ルールベースを利用して感染したデバイスに対処

リモートシェル[1]

- 物理的にデバイスに触れなくてもトラブルシューティング、ローカル設定の変更、フォレンジック調査の実行が可能

定期的なスキャンや定期的な更新が不要

- ユーザーの生産性を損なうことなく常に最高レベルの保護が可能
- インストール時にフルスキャンを受信し、その後継続的に疑わしいアクティビティを監視

オプションでSonicWallファイアウォールと統合

- エンドポイントで暗号化されたトラフィック（DPI-SSL）の詳細なパケット検査を実施
- 各エンドポイントに信頼できる証明書を簡単に配置
- ファイアウォールが実装されている場合、保護されていないユーザーがインターネットにアクセスする前にCapture Clientのダウンロードページに誘導

コンテンツフィルタリング

- 悪意のあるサイトのIPアドレスとドメインをブロック
- 帯域幅を縮小したり、不快または非生産的なウェブコンテンツへのアクセスを制限することでユーザーの生産性を強化

デバイス制御

- 感染の可能性があるデバイスのエンドポイントへの接続をブロック
- 詳細な許可リストポリシーを使用

Capture Clientの特徴

特徴	Advanced	Premier
クラウドの管理、レポートおよび分析 (CSC)	✔	✔
ネットワークセキュリティ統合		
エンドポイントの可視性と実施	✔	✔
DPI-SSL証明書の展開	✔	✔
コンテンツフィルタリング	✔	✔
高度なエンドポイント保護		
次世代のマルウェア対策	✔	✔
Capture Advanced Threat Protectionサンドボックス	✔	✔
ActiveEDR(エンドポイントの検知と応答)		
攻撃の可視化	✔	✔
ロールバックと修復	✔	✔
デバイス制御	✔	✔
アプリケーションの脆弱性およびインテリジェンス	✔	✔
不正		✔
エンドポイントネットワーク制御		✔
ActiveEDR脅威ハンティングおよびインテリジェンス		
脅威ハンティング		✔
リモートシェル[1]		✔
除外カタログ		✔

[1] リモートシェルは、(2FAが有効になっている)新しいアカウントで、オンデマンドによりS1コンソール上で直接利用できるようになります。

Capture Client – システム要件 | SonicWall

グローバルエンドポイントセキュリティのベストプラクティス MSSPおよび分散型企業のための運用

ソリューションの要約を読む:www.sonicwall.com

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、中小企業をサポートします。詳しくはwww.sonicwall.comをご覧ください。

SonicWall Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
詳細は当社ウェブサイトをご覧ください。
www.sonicwall.com