SONICWALL

SonicWall Capture Client

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るみになりました。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一貫した保護を確立することが急務といえます。

SonicWall Capture Clientは、複数の保護機能を備えた統合エンドポイントです。SentinelOneを搭載した次世代マルウェア保護エンジンにより、Capture Clientは機械学習、ネットワークサンドボックスの統合、システムロールバックなどの高度な脅威保護技術を適用します。Capture Clientは、信頼できるTLS証明書をインストールおよび管理することにより、SonicWallファイアウォール上で暗号化されたTLSトラフィック（DPI-SSL）の詳細な検査も活用します。

Capture ClientはSonicWall Global VPN Clientと共存しており、すべての製品のポリシーは単一のクラウドベースの管理コンソールから管理できます。Capture Clientは、Microsoft Active Directoryグループポリシー、その他のサードパーティ製ソフトウェアの展開技術を使用して、またはクライアントが追加の介入なしにダウンロードしてサイレントモードでセルフインストールできるようにカスタマイズされたURLを配信することで簡単に追加することができます。さらに、Capture ClientがSonicWallファイアウォールと統合されることにより、保護されていないクライアントに対しオプションで強制機能を使用してインストールさせるためのゼロタッチエクスペリエンスが可能となります。

機能と利点

エンドポイントの**継続的な行動監視**は、ファイルアクティビティ、アプリケーションとプロセスのアクティビティ、ネットワークアクティビティの完全なプロファイルを作成するのに役立ちます。これにより、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する保護が可能となり、調査に関連する対応を可能とするインテリジェンスと360度攻撃の可視化を提供します。

複数の階層、ヒューリスティックベースの技術での保護には、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が含まれます。これは、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に役立ちます。

定期的なスキャンや定期的な更新が不要であるため、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になります。Capture Clientはインストール時にフルスキャンを行い、その後継続的に疑わしいアクティビティを監視します。

Advanced Threat Protection（ATP）統合は、疑わしいファイルを自動的にアップロードし、エンドポイントが実行できないコード操作によって、高度なサンドボックス分析を行います。タイミング遅延が組み込まれたマルウェアなどは、実行される前に脅威を阻止しましょう。管理者は、分析のために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こともできます。

独自のロールバック機能は、脅威を完全に除去するだけでなく、ターゲットクライアントをマルウェアの活動が開始される前の状態に戻すといったポリシーをサポートしています。これにより、Windowsに対するランサムウェアや同様の攻撃の場合に、手動で復元する必要がなくなります。

導入効果

- 独立したクラウドベースでの管理
- SonicWallファイアウォールとの併用
- セキュリティポリシーの実施
- DPI-SSL証明書の管理
- 継続的な行動監視
- 機械学習によって実現した高精度な判定
- 多層ヒューリスティックベース技術
- アプリケーション脆弱性インテリジェンス
- 独自のロールバック機能
- ホワイト/ブラックリストが簡単
- 自動マルウェア分析のためのCapture Advanced Threat Protection（ATP）クラウドサンドボックス
- 手動ファイル検査のためのアップロード不要の脅威インテリジェンス共有
- コンテンツフィルタリング
- デバイス制御

Application Vulnerability Intelligenceにより、管理者は保護されたエンドポイント上のすべてのアプリケーションとそれに関連するあらゆるリスクを登録できるようになります。リスクは、CVEの詳細と、そのバージョンでレポートされた重大度レベルを含む既知の脆弱性の存在に基づいており、管理者にアクション可能なインテリジェンスを提供し、パッチを優先させ、エンドポイントの攻撃面を減少させます。

SonicWallの第6世代以上およびファイアウォールとの統合（オプション）により、ゼロタッチでの展開およびエンドポイントコンプライアンスの強化を実現します。さらに、各エンドポイントに信頼できる証明書を配置することにより、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装することができます。

コンテンツフィルタリングにより、組織は悪意のあるサイトのIPアドレスやドメインをブロックするだけでなく、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高めることができます。

デバイスコントロールにより、組織は粒度の細かいホワイトリストポリシーを用いて、感染したデバイスがエンドポイントに接続するのを阻止できるようになります。

集中管理とクライアント保護のレポート
SonicWallのクラウドベースの管理コンソールは、次世代のマルウェア保護、DPI-SSL証明書管理、およびコンテンツフィルタリングを含むすべてのクライアントポリシーを管理するために統一されたインターフェースとして機能します。

管理コンソールは、追加料金なしで提供されるマルチテナントクラウドベースのプラットフォームです。クライアントの保護レポーティングおよびポリシー管理を可能にし、Microsoft Active Directory属性に基づくポリシーの割り当て機能など、細かいアクセス制御ポリシーをサポートしています。これにより、管理委託型サービスプロバイダ（MSP）は、複数顧客を持つクライアントを管理し、レポートすることができます。同時に、顧客は各自のクライアントを管理およびレポートすることのみ可能となります。

管理コンソールは、検出されたマルウェアの脅威の根本原因を特定するための調査プラットフォームとしても機能し、それらの再発防止方法についてアクション可能なインテリジェンスを提供します。例えば、管理者は、クライアント上でどのようなアプリケーションが実行されているかを簡単に確認できます。それによって、脆弱または未承認ソフトウェアが実行中のマシンを特定することができます。

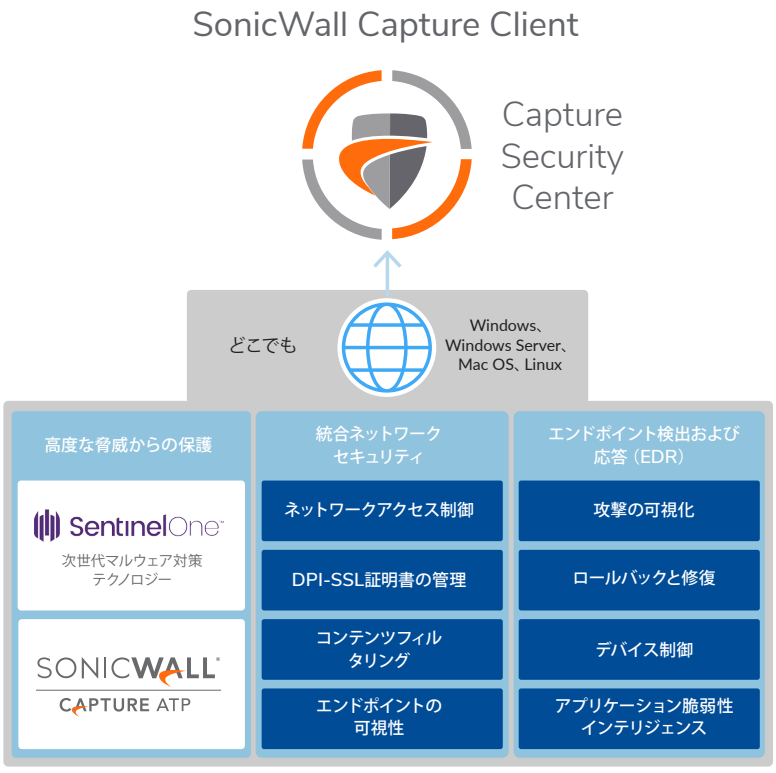
サービスとプラットフォームのサポート

SonicWall Capture Clientには2つの製品があります。

SonicWall Capture Client Basicは、DPI-SSLサポート機能と共にすべてのSonicWall次世代マルウェア対策と修復機能を提供します。

SonicWall Capture Client Advancedでは、Basic、の機能に加え、高度なロールバック機能、Capture ATP統合、Attack Visualization、Application Vulnerability Intelligence、Content Filteringのすべてを提供します。

両製品は、Windows 7以上、およびMac OSX用です。



機能比較		
機能	ベーシック	アドバンスト
クラウドの管理、レポートおよび分析（CSC）	✓	✓
統合ネットワークセキュリティ		
エンドポイントの可視性	✓	✓
DPI-SSL証明書の展開	✓	✓
コンテンツフィルタリング	–	✓
次世代マルウェア対策	✓	✓
高度な脅威からの保護	✓	✓
Capture Advanced Threat Protectionサンドボックス	–	✓
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	–	✓

システム要件
オペレーティングシステム
Windows 7以上
Windows Server 2008 R2以上
Mac OS/OSX 10.10以上
ハードウェア
1 Ghz デュアルコアCPU以上
OSにより要求される場合は1 GB以上のRAM（推奨2 GB）
2 GBの空きディスクスペース

CAPTURE CLIENT SKU		
製品	有効期間	SKU
アドバンスト		
SONICWALL CAPTURE CLIENT ADVANCED 5-24 ENDPOINTS 24時間365日サポートつき	3YR	02-SSC-1518
SONICWALL CAPTURE CLIENT ADVANCED 5-24 ENDPOINTS 24時間365日サポートつき	1YR	02-SSC-1519
SONICWALL CAPTURE CLIENT ADVANCED 25-49 ENDPOINTS 24時間365日サポートつき	3YR	02-SSC-1520
SONICWALL CAPTURE CLIENT ADVANCED 25-49 ENDPOINTS 24時間365日サポートつき	1YR	02-SSC-1521
SONICWALL CAPTURE CLIENT ADVANCED 50-99 ENDPOINTS 24時間365日サポートつき	3YR	02-SSC-1522
SONICWALL CAPTURE CLIENT ADVANCED 50-99 ENDPOINTS 24時間365日サポートつき	1YR	02-SSC-1523
SONICWALL CAPTURE CLIENT ADVANCED 100-249 ENDPOINTS 24時間365日サポートつき	3YR	02-SSC-1524
SONICWALL CAPTURE CLIENT ADVANCED 100-249 ENDPOINTS 24時間365日サポートつき	1YR	02-SSC-1525
SONICWALL CAPTURE CLIENT ADVANCED 250-499 ENDPOINTS 24時間365日サポートつき	3YR	02-SSC-1454
SONICWALL CAPTURE CLIENT ADVANCED 250-499 ENDPOINTS 24時間365日サポートつき	1YR	02-SSC-1455
SONICWALL CAPTURE CLIENT ADVANCED 500-999 ENDPOINTS 24時間365日サポートつき	3YR	02-SSC-1456
SONICWALL CAPTURE CLIENT ADVANCED 500-999 ENDPOINTS 24時間365日サポートつき	1YR	02-SSC-1457
SONICWALL CAPTURE CLIENT ADVANCED 1000-4999 ENDPOINTS 24時間365日サポートつき	3YR	02-SSC-1458
SONICWALL CAPTURE CLIENT ADVANCED 1000-4999 ENDPOINTS 24時間365日サポートつき	1YR	02-SSC-1459
SONICWALL CAPTURE CLIENT ADVANCED 5000-9999 ENDPOINTS 24時間365日サポートつき	3YR	02-SSC-1460
SONICWALL CAPTURE CLIENT ADVANCED 5000-9999 ENDPOINTS 24時間365日サポートつき	1YR	02-SSC-1461
SONICWALL CAPTURE CLIENT ADVANCED 10000+ENDPOINTS 24時間365日サポートつき	3YR	02-SSC-1462
SONICWALL CAPTURE CLIENT ADVANCED 10000+ENDPOINTS 24時間365日サポートつき	1YR	02-SSC-1463
ベーシック		
SONICWALL CAPTURE CLIENT BASIC 5-24 ENDPOINTS 24時間365日サポートつき	3YR	02-SSC-1510
SONICWALL CAPTURE CLIENT BASIC 5-24 ENDPOINTS 24時間365日サポートつき	1YR	02-SSC-1511
SONICWALL CAPTURE CLIENT BASIC 25-49 ENDPOINTS 24時間365日サポートつき	3YR	02-SSC-1512
SONICWALL CAPTURE CLIENT BASIC 25-49 ENDPOINTS 24時間365日サポートつき	1YR	02-SSC-1513
SONICWALL CAPTURE CLIENT BASIC 50-99 ENDPOINTS 24時間365日サポートつき	3YR	02-SSC-1514
SONICWALL CAPTURE CLIENT BASIC 50-99 ENDPOINTS 24時間365日サポートつき	1YR	02-SSC-1515
SONICWALL CAPTURE CLIENT BASIC 100-249 ENDPOINTS 24時間365日サポートつき	3YR	02-SSC-1516
SONICWALL CAPTURE CLIENT BASIC 100-249 ENDPOINTS 24時間365日サポートつき	1YR	02-SSC-1517
SONICWALL CAPTURE CLIENT BASIC 250-499 ENDPOINTS 24時間365日サポートつき	3YR	02-SSC-1444
SONICWALL CAPTURE CLIENT BASIC 250-499 ENDPOINTS 24時間365日サポートつき	1YR	02-SSC-1445
SONICWALL CAPTURE CLIENT BASIC 500-999 ENDPOINTS 24時間365日サポートつき	3YR	02-SSC-1446
SONICWALL CAPTURE CLIENT BASIC 500-999 ENDPOINTS 24時間365日サポートつき	1YR	02-SSC-1447
SONICWALL CAPTURE CLIENT BASIC 1000-4999 ENDPOINTS 24時間365日サポートつき	3YR	02-SSC-1448
SONICWALL CAPTURE CLIENT BASIC 1000-4999 ENDPOINTS 24時間365日サポートつき	1YR	02-SSC-1449
SONICWALL CAPTURE CLIENT BASIC 5000-9999 ENDPOINTS 24時間365日サポートつき	3YR	02-SSC-1450
SONICWALL CAPTURE CLIENT BASIC 5000-9999 ENDPOINTS 24時間365日サポートつき	1YR	02-SSC-1451
SONICWALL CAPTURE CLIENT BASIC 10000+ ENDPOINTS 24時間365日サポートつき	3YR	02-SSC-1452
SONICWALL CAPTURE CLIENT BASIC 10000+ ENDPOINTS 24時間365日サポートつき	1YR	02-SSC-1453

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の時代、および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的大躍進をも実現している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大企業や政府、SMB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

Datasheet-CaptureClient-US-VG-2139