SonicWall

総合カタログ 2020

INNOVATE **MORE.**
FEAR**LESS.**

Real-Time Breach Detection and Prevention

SONICWALL®

近年のネットワーク脅威と巧妙化するサイバー攻撃

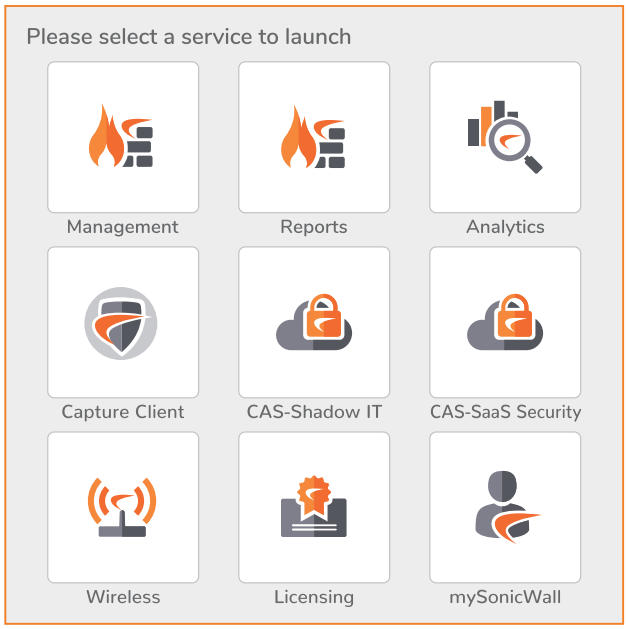
2016 年にはマルウェア検出数の減少がみられ、一部では全体的なサイバー犯罪が減少しているのではないかとの見方もありましたが、それ以来 マルウェア攻撃は 30%以上増加しています。2018 年には、SonicWall が全世界で記録したマルウェア攻撃は過去最高の 105 億 2 千万件に上りました。SonicWall の脅威研究者らが通年脅威データを分析した結果、「ランサムウェア攻撃」が、イギリスとインドの二国を除くほぼすべての地域で増加したという、衝撃的な事実が明らかになりました。

最近の調査では、Meltdown、Spectre などプロセッサの脆弱性に付け込んでデータを盗み出すサイドチャネル攻撃が猛威をふるうという警告が出ています。プロセッサの様々な脆弱性は修正することができず、はるかに深刻なセキュリティ問題となりつつあります。したがって、サイドチャネル攻撃がコンピューティング環境にとって継続的なリスクとなることは必至であり、これらの攻撃を緩和できるテクノロジーが不可欠となります。SonicWall の RTDMI は新種のマルウェアを検出するだけでなく、特許申請中のテクノロジーを利用して危険なサイドチャネル攻撃を緩和します。

一般的なセキュリティ製品を回避する攻撃も増加しています。暗号化通信にして隠れたり、ファイルサイズを大きくすることで検査機能の制限を利用し検知を逃れたり、MS オフィスや PDF ファイルや脅威と判断されない複数の仕掛けを合わせたマルウェアであったり、攻撃は常に巧妙に進化しています。さらに、クラウドストレージや USB メモリ、セキュリティ対策の取れていない BYOD（持込端末）からマルウェアが侵入するなど、今日多くの脅威が存在しています。

SonicWall のセキュリティ製品は、あなたの大切なネットワーク環境を守る最適なソリューションを提供します。

Capture Security Center



1つのインターフェイスから すべてのセキュリティ機能をコントロール

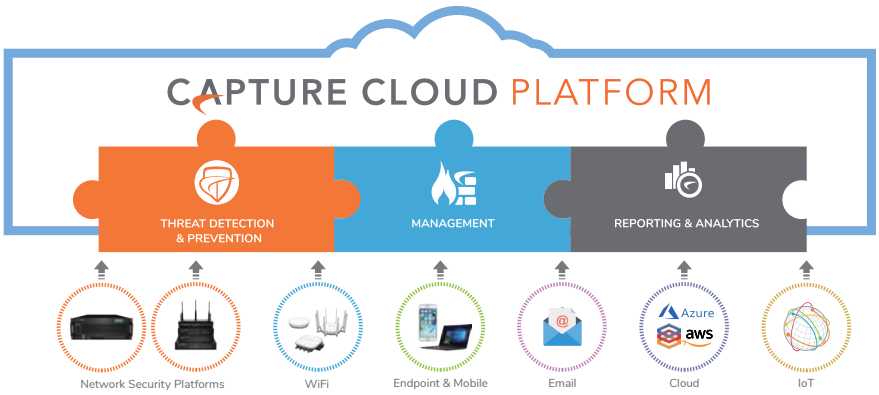
Capture Security Center は SonicWall 製品やサービスをインターネット上で一括管理できる拡張性の高いクラウドセキュリティ管理システムです。シングル・サインオンおよび「単一画面」での管理機能を備えています。ネットワーク、電子メール、モバイルやクラウド・セキュリティ・リソースの全ポートフォリオにわたる強固なセキュリティ管理、分析およびリアルタイム脅威インテリジェンスを提供する **Capture Cloud Platform** を統合します。

SonicWall のセキュリティ運用およびサービスの全範囲を管理する Capture Security Center は、アセットの管理やサイバー脅威から全ネットワークの防衛を支援する貴重なチームリソースを提供しています。アップデート、サポート、セキュリティリスクの監視およびコンプライアンスの遂行を統一、同期、これらすべてを正確に素早く行います。

Capture Cloud Platform

セキュリティと管理サービスを緊密に統合するクラウド&サービス指向のアーキテクチャ

Capture Cloud Platform は、SonicWall の全製品にわたりセキュリティ、管理、分析、およびリアルタイムの脅威インテリジェンスを強固に統合します。このアプローチにより、当社の高性能ハードウェア、仮想アプライアンス、およびクライアントの完全なポートフォリオは、クラウドの力、敏捷性、およびスケーラビリティを利用することができます。



SonicWallのテクノロジー

SonicWallについて

SonicWall Inc. は 27 年以上にわたってサイバー犯罪と戦い、世界中の中小企業、大手企業、政府機関を守り続けています。受賞歴のある当社のリアルタイム侵害検知･防御ソリューションは、SonicWall Capture Labs の研究によってその効果が裏付けられています。このソリューション群は、実に 215 以上の国と地域で、100 万以上のネットワークとその中の電子メールやアプリケーション、データを保護しています。これによって多くの組織がより効果的に稼働し、セキュリティ上の懸念を軽減しています。

SonicWallのビジョン

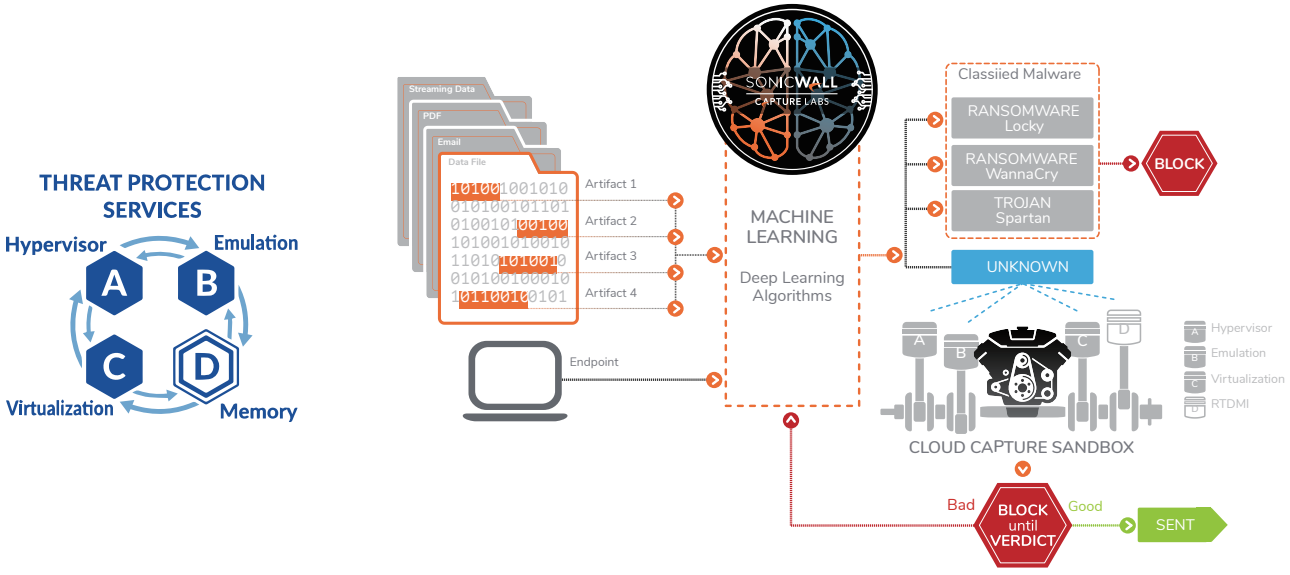
自動化されたリアルタイム侵害検知と防御
(Automated real-time breach detection and prevention)

高品質の証し

2018 年の NSS Labs によるテスト結果では、
・6 年連続で「推奨製品」として評価
・NGFW 回避脅威を 100% 検知
・安定性、信頼性テスト 100% 合格
・低 TCO で高いセキュリティ効果を達成

Capture ATP (Multi-Engine Sandbox) with RTDMI

Capture ATP (Advanced Threat Protection) は、3 つのエンジンで多重監視する SonicWall 独自のクラウドサンドボックスシステムに加え、**RTDMI** エンジンを構成した CPU トラッキングサンドボックスからなります。一般的なサンドボックスは 1 つのエンジンで監視・解析を行っていますが、SonicWall はサンドボックスに 4 つのエンジンを採用し、疑わしいファイルの振舞いを監視します。



Emulation
外科的な検視を行う。フルシステムエミュレーションで CPU やメモリの動きも再現し不振な動きを検査する。

Hypervisor
内視の役割を果たす。ハイパーバイザーから実験台マシンを透過して隅々までモニタリングする。

Virtualization
触診・内科的な役割として、世界で 100 万以上展開するセンサーから届くリアルタイム分析結果を活用して実験台の仮想マシンの不振な動きを検知する。

RTDMI (Real Time Deep Memory Inspection)
通常のセキュリティエンジンでは監視が難しいメモリ内での行動 / 振舞いを監視し、脅威につながる動作の予兆を見逃さずに審査・推理していきます。Meltdown,Spectre をどこよりも早く発見したように、未知の CPU 脆弱性を突くマルウェアを検出し防御します。

・最新脅威に対し **100 ナノ秒以下の速さ**で判定
・ディープラーニングによる**誤検知と検知漏れの排除**
・**Meltdown, Spectre** を利用する攻撃にも対応

2018 年、**Capture ATP** は、サイバー攻撃の新たなマルウェアとして 391,689 の亜種を特定しました。これは、1 日に 1,072 件超の新たな攻撃が発見され、阻止されたことになります。さらに **RTDMI** と共に、動的な自己学習と自己強化を行っています。**RTDMI** が 2018 年に特定した新種の攻撃は 74,290 件に上りました。これらは非常に新しい、独特または複雑なマルウェアの亜種で、SonicWall が発見した時点では、他のどのベンダーもそれらを追跡したり、シグネチャ（マルウェアの定義ファイル）を作成することができませんでした。

Solution ソリューション

組織のNetworkを守る

次世代ファイアウォール(UTM)

ファイアウォール、サンドボックス（振舞い・予見防御）、SSL インスペクション、ゲートウェイアンチウィルス、不正侵入防御、アンチスパイウェア、アプリケーション制御／可視化、ボットネットフィルタ、地域 IP フィルタ、Web フィルタ、VPN、ZeroTouch デプロイ

リモートアクセスを安全に利用する

セキュアモバイルアクセス

SSL-VPN、利用者端末制御（エンドポイントコントロール）、ユーザ認証、シングルサインオン、ポータルサイト、二要素認証、リモートデスクトップ、アクセスコントロール、モバイル VPN 接続、サンドボックス（振舞い・予見防御）、SD-WAN

Wi-Fi接続を守る

セキュアWi-Fiアクセスポイント

Wi-Fi アクセスポイント、802.11ac Wave2、複数 SSID、PoE 給電、Wi-Fi プランナー、Wi-Fi Cloud マネージャー、サンドボックス（振舞い・予見防御）、Web フィルタ

エンドポイントの挙動監視と遠隔制御

エンドポイント・セキュリティ

クライアント脅威防御、次世代 AV エンジン、EDR、サンドボックス（振舞い・予見防御）、隔離、ロールバック、証明書管理

Cloudサービスを守る

クラウドサービス・SaaSセキュリティ

ウェブアプリケーションファイアウォール、SaaS セキュリティ、Web メールセキュリティ、次世代 FW on Cloud プラットフォーム

装置の統合管理とレポーティング

マネージドセキュリティ・リスク管理

統合管理、リモート・クラウド管理接続、定期レポート送信、レポーティング、解析ツール、監査

Products 製品

TZ シリーズ

NSa シリーズ

NSa9000 シリーズ

NSv シリーズ

仮想装置
クラウドプラットフォーム

P6 - P7

SMA100 シリーズ

SMA1000 シリーズ

SMA v シリーズ

仮想装置
クラウドプラットフォーム

P8 - P9

SonicWave シリーズ

P10

Capture Client

P11

WAF
Web Application Firewall

CAS
Cloud App Security

NSvシリーズ

HES
Hosted Email Security

P12

Management

Analytics & Reporting

リスク・メーター

P13

ネットワークセキュリティ（次世代ファイアウォール/UTM）

SonicWall の次世代ファイアウォールは、あらゆる規模のネットワークに対しマルチギガビット速度での包括的な脅威防御を実現し、組織の革新と急成長に必要なネットワーク・セキュリティ、制御、および視認性を提供します。

当社の受賞歴のあるハードウェアおよび仮想ファイアウォールは、幅広い製品、サービス、および技術と強固に統合されており、顧客のニーズに合わせて規模を拡大縮小できる完全な高性能セキュリティ・ソリューションを構築します。

- Real-Time Deep Memory Inspection（RTDMI）および Reassembly-Free Deep Packet Inspection（RFDPI）技術
- マルチエンジン・サンドボックス、マルウェア対策、侵入防止、ウェブ・フィルタリングなどを特徴とするクラウドベースおよびオンボックスの脅威防止機能
- TLS/SSL および SSH トラフィックをリアルタイムで復号化および検査
- 高速マルチコア・ハードウェア・アーキテクチャによる処理性能の向上
- 内蔵ワイヤレス・コントローラを使用する高速ワイヤレス機能の追加

複数のセキュリティ機能を1台に集約し、利便性を向上させつつ巧妙化するサイバー攻撃からネットワークを守る

ファイアウォール
通信の許可・禁止だけではなく、DoS攻撃にも対応

VPN
通信を暗号化することで拠点間や外出先のPCとセキュアにやりとり

SSLインスペクション
SSL通信を解析(別途セキュリティ機能との併用が必要です)

ワイヤレス
ワイヤレス機能を標準搭載(対象モデルのみ)別売の無線APを集中管理ができます。

HA
機器を冗長化することで対障害性を向上

コンテンツフィルタリング
業務に関係のない怪しいサイトへのアクセスを禁止

レポーティング
状況把握が簡単にわかる脅威レポートを出力可能

SD-WAN
用途や状況に応じて経路を動的に管理し安定したネットワーク運用を可能にする

ゲートウェイアンチウィルス
インターネットの出入口でウイルスチェック

アンチスパイウェア
スパイウェアをブロックすることで、不正に情報を送らないように

アプリ可視化/コントロール
通信を見張り、業務に関係の無いアプリの利用を把握/制御

不正侵入防御
セキュリティパッチの未適PC/Serverに対する攻撃をブロック

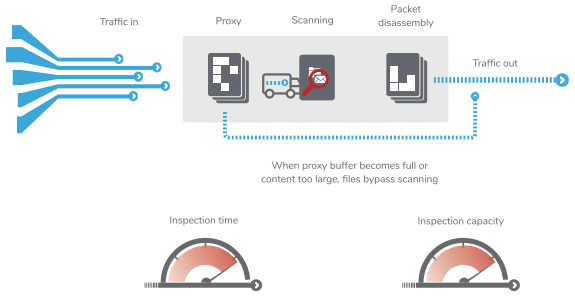
Botnet/地域IPフィルタ
ハッカーが悪用するインターネット上のホストとの通信をブロック

サンドボックス
添付ファイルの挙動をクラウド上で確認、未知の脅威をブロック

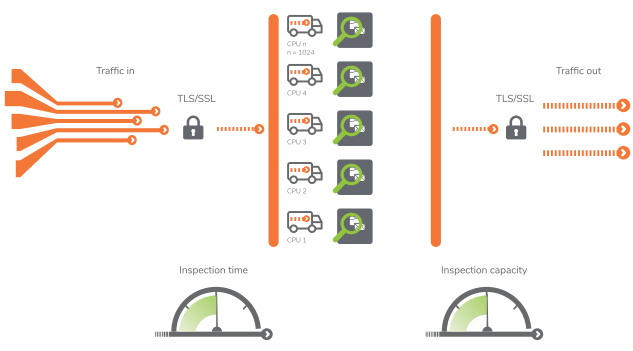
Zero Touch
ユーザはWANと電源をつなぐだけでCloudから管理可能

RFDPI (Reassembly-Free Deep Packet Inspection) とマルチコア

- バッファやプロキシを使用せずに**ストリームベース**の分析。検査するファイルにサイズ制限が無いため全てのファイルを検査。
- バッファする時間とバッファが解放されるまでの処理待ち時間による遅延が無い。
- 同時に複数処理を可能にする**マルチコア**によりパケット検査を高速に実現。
- ポート番号やプロトコルに関係なくアプリケーショントラフィックを識別しながら、攻撃を効果的に発見。
- 暗号化されたネットワーク・トラフィックも保護。検査前に TLS/SSL 復号化が適用。
- エンジンは、検査専用に設定することも、ビジネスに不可欠なアプリケーションにレイヤ 7 帯域幅管理を提供するように設定することも可能。



他ソリューションの検知プロセス



SonicWall RFDPIの検知プロセス

NSsp シリーズ

ハイエンドファイアウォール

クラウド・インテリジェンスを活用したスケーラブルな最先端のセキュリティ

SonicWall ネットワーク・セキュリティ・サービス・プラットフォーム（NSsp）シリーズは、信頼性の高い高性能プラットフォームでアプライアンスベースの保護とクラウド・インテリジェンスを組み合わせることにより、脅威を検出および防止する革新的なアプローチ実現します。大規模な分散型企業、データ・センター、およびサービス・プロバイダ向けに設計された NSsp シリーズは、性能を低下させることなく、数百万もの接続に対して、最新の脅威に対し実証済みでスケーラブルな保護を提供します。

NSa シリーズ

ミッドレンジファイアウォール

高性能セキュリティプラットフォームにおける高度な脅威防御

SonicWall ネットワーク・セキュリティ・アプライアンス（NSa）シリーズは、自動化された高度脅威防御技術をミッドレンジの次世代ファイアウォールプラットフォームに統合します。10GbE および 2.5GbE インターフェースを備えたマルチコア・ハードウェア・アーキテクチャ上に構築された NSa シリーズは、規模を拡大縮小できるため、中規模ネットワーク、支店、分散型企業のパフォーマンス要求を満たします。 NSa シリーズのファイアウォールは、TLS/SSL 復号化と検査、アプリケーション・インテリジェンスおよび制御、Secure SD-WAN、リアルタイム視覚化、WLAN 管理などのクラウドベースおよびオンボックス機能を備えています。

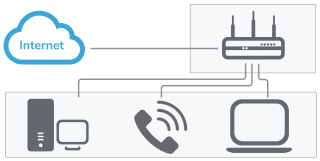
TZ シリーズ

中小企業および分散型企業向けの高性能統合脅威防御プラットフォーム

SonicWall TZ シリーズは、柔軟で統合されたセキュリティ・ソリューションで高速な脅威防御を実現します。遠隔地や支店を持つ分散型企業と小規模ネットワーク向けに設計された TZ シリーズは、特定のニーズに合わせて調整できる 5 つの異なるモデルを提供します。Secure SD-WAN や Zero-Touch Deploy などの高度なネットワーキングおよび管理機能により、必要に応じて新しいサイトを簡単に立ち上げることができます。PoE/PoE+ サポートと 802.11ac Wi-Fi などのオプション機能を追加して、有線および無線接続を経由する最新の脅威からネットワークとデータを保護する統合セキュリティ・ソリューションを構築します。

安全で使いやすいモバイル接続性

- ネイティブの SSL VPN を使用してファイアウォールの背後にあるリソースにリモートで安全にアクセス
- Apple® iOS、Google® Android、Windows® 8.1、Mac OS® X、Kindle Fire および Linux などのあらゆるオペレーティング・システムから実質的に接続
- VPN 接続を経由する隠れた脅威をスキャンして削除



SOHO 250 W / TZ 350 W

NEW PRODUCT

- 速度を最適化したセキュリティプロセッサーによる超高速パフォーマンス
- 機械学習を使った深いレベルでの脅威防御
- 継続的にアップデートされるセキュリティのために共有された脅威インテリジェンス
- ゼロタッチデプロイを使い、ファイアウォールを直ちに起動
- キャプチャ・セキュリティ・センターを利用し、1つの場所からすべてを管理

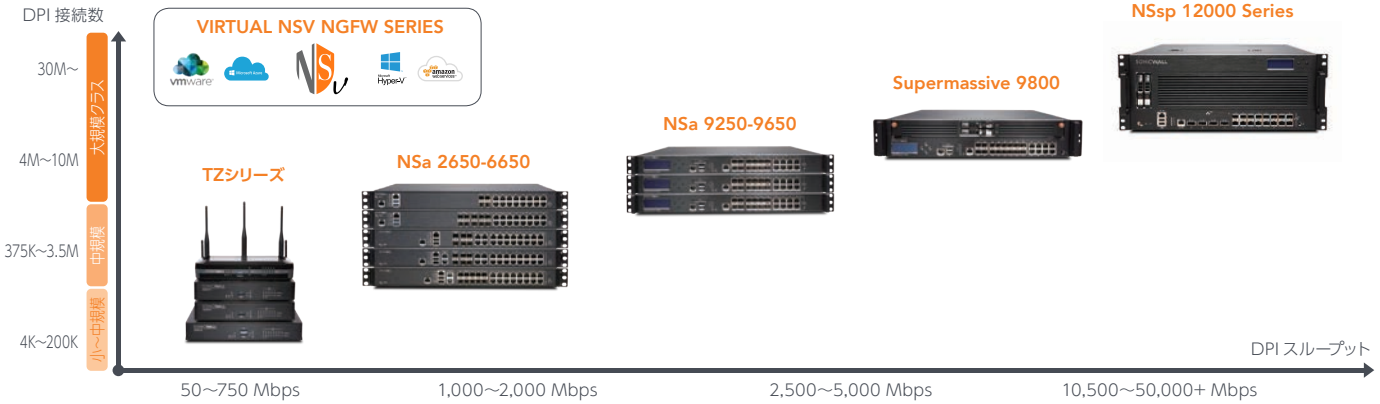
NSv 仮想NGFWシリーズ

最も適応性のある仮想ファイアウォール

- VMware ESXi, Microsoft Hyper-V, Amazon Web Services（AWS）および Microsoft Azure での安全なワークロード
- インフラストラクチャの規模を適切に調整
- システムの回復力、サービスの信頼性、および規制上の適合性を保証
- 性能を低下させることなく敏捷性とスケーラビリティを提供
- CAPEX から OPEX モデルに移行することで費用対効果と効率性を達成

パブリック / プライベート クラウドに対するクラス最高の高度な保護

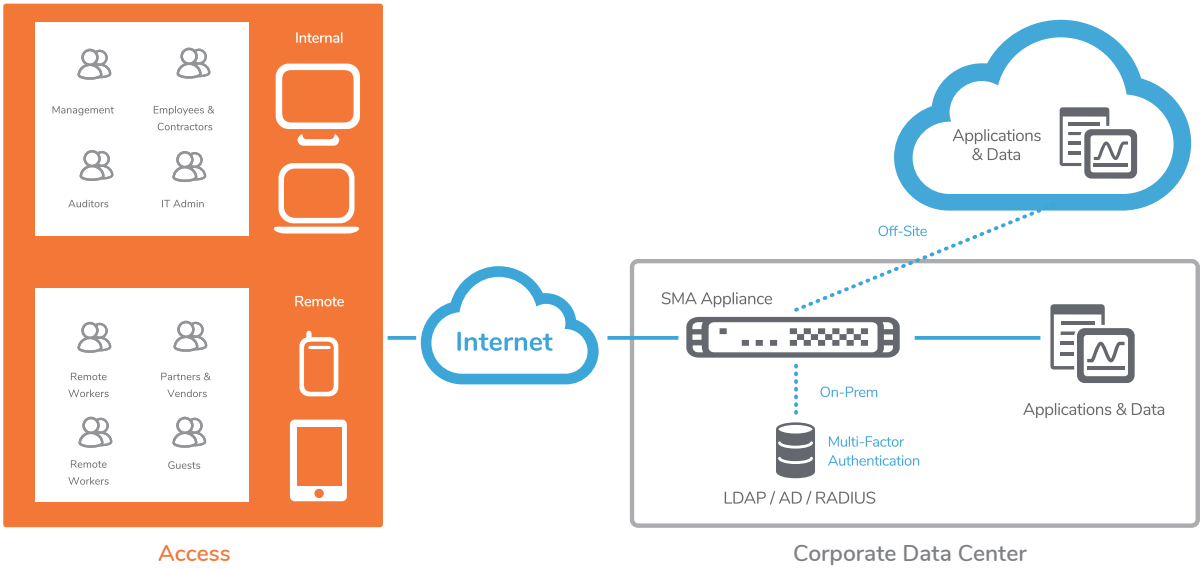
- 一貫したリアルタイム自動侵害検知および防御機能を提供
- Real-Time Deep Memory Inspection（RTDMI™）と Reassembly-Free Deep Packet Inspection（RFDPI®）を活用
- Capture ATP マルチエンジン・サンドボックスを利用してゼロデイ脅威を阻止
- ウイルス、スパイウェア、マルウェア、侵入、暗号化された脅威、悪意のあるアプリやウェブサイトをブロック



Secure Mobile Access

セキュアモバイルアクセス

SonicWall のセキュアモバイルアクセス（SMA）は、スマートフォンやタブレットなど多種多様なデバイスから社内リソースへ、柔軟な接続制御と安全にアクセスするセキュアなネットワーク環境を提供します。



●多種多様なデバイスの接続

Mobile Connect アプリケーションは、Apple iOS、macOS、Google Android、Kindle Fire、および Windows デバイスのリモートユーザにレイヤー 3 トンネル接続を提供します。Apple Store、Google Play、Windows Store を通じてアプリケーションのインストールやアップデートが行われるため、管理者の負担を軽減することができます。

●豊富な二要素認証

SMA シリーズは標準機能として、ワンタイムパスワード認証機能を有しています。メールサーバと連携することで、リモートユーザにワンタイムパスワード送信することができます。ご利用中の ActiveDirectory、PKI プラットフォーム、RADIUS 等の認証プラットフォームと柔軟に連携します。認証を多重化することでキーロガー、総当たり攻撃等に対する防御を可能にします。

サードパーティ認証アプリとの連携

Microsoft Authenticator

Google Authenticator

●End Point Control(EPC)

SMA に接続した際に、OS バージョン、デバイス固有の ID, アンチウイルスソフトの稼働状況、クライアント証明書の有無等のクライアント端末の情報に応じて接続の許可 / 拒否またはアクセス先のコントロールを行うことが可能になります。脆弱な端末の排除を実現し、BYOD 端末やスマートデバイスのリモートアクセス導入に最適な機能です。

●スパイクライセンス

SMA は登録ユーザ数ではなく、同時接続ユーザ数に合わせてユーザライセンスや保守契約を購入します。 自然災害、インフルエンザ・パンデミックなど外的な要因で一時的にリモートワーカーを増やす場合、スパイクライセンスを活用すると既存の保守契約やユーザライセンスには影響を与えず、一定期間同時接続ユーザ数を拡張することができます。

●SAML 2.0 / SAML IDP Gatekeeper

SMA SAML Idp プロキシは、クラウドサービスと複数の Identity Provider(Idp) 間でブリッジとして機能し、シームレスなシングルサインオンユーザーエクスペリエンスを提供しながら、ポリシー実施を行うことができます。

●SaaSアプリケーションをセキュアに利用

SAML と End Point Control を組み合わせて利用することで、管理者が指定したデバイスだけが SaaS アプリケーションにログインさせるような制御が可能になります。さらに SaaS アプリケーションの接続元 IP アドレスをセキュアモバイルアクセス経由にすることで、第三者からの不正なログインを防ぐことも可能です。

●デバイス管理

EPC で利用できるデバイス固有の ID を使用したアクセス制御を自動化する機能です。SMA 接続時にユーザ情報、デバイス ID、OS 情報などを自動的に収集して本体にストアします。管理者はストアされた情報を確認して接続の許可・拒否を制御できます。
※ Windows, Mac, iOS, Android をサポートします。
(事前に専用アプリをインストールしておく必要があります)

●アプリケーションオフロード Web Application Firewall

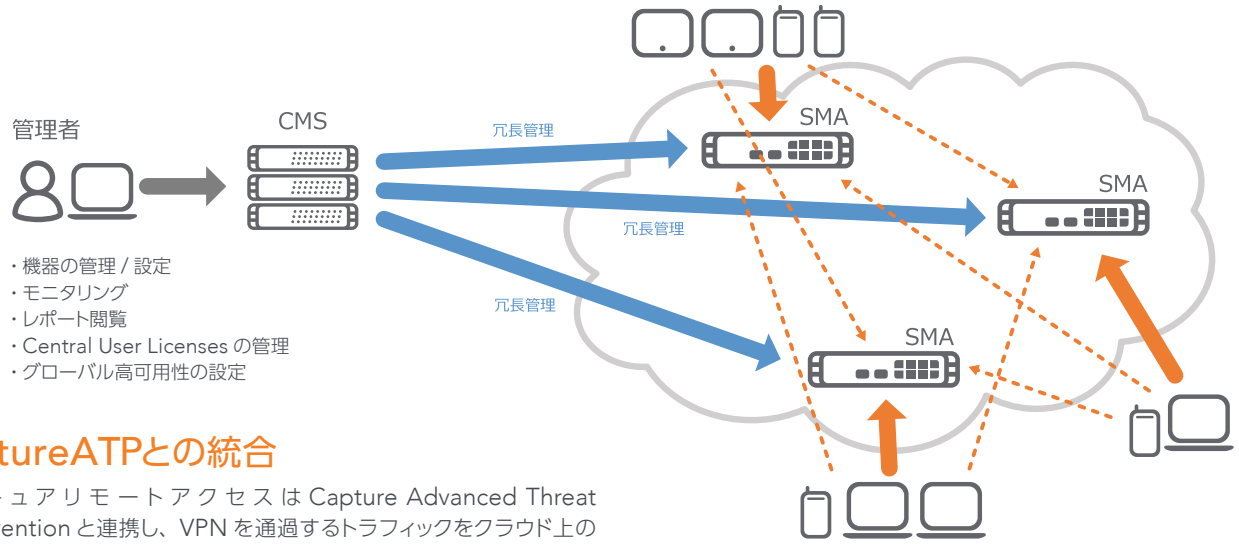
SMA を SSL オフローダーとして利用することができます。例えばイントラネットに設置されている WEB サーバを外部に公開したい場合、負荷の掛かる SSL 暗号処理を SMA で行い、通信を HTTP(平文) で中継することで WEB サーバの負荷を減らすことができ、パフォーマンスが向上します。また、外部公開する WEB サーバを保護するため、WAF は直感的に運用でき、だれにも扱い易い日本語の GUI を完備しています。

Central Management Server(CMS)

CMS は、セキュアリモートアクセスを提供する SonicWall SMA シリーズを単一のコントロール (CMC：Central Management Console) から迅速に配備するための柔軟かつ、直感的に操作可能な一元管理ツールを提供します。CMS を利用することで複数のセキュアリモートアクセスデバイスに対し遠隔から機器の管理 / 設定、モニタリング、レポート、ライセンス管理の操作が可能となります。
※ CMS は Virtual Appliance となります。

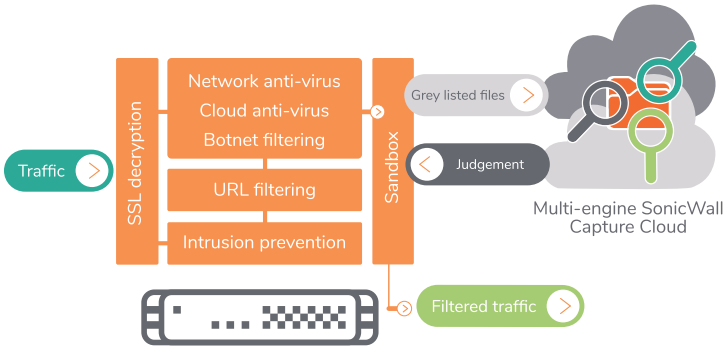
Global High Availability グローバル高可用性

SonicWall のセキュアリモートアクセスは可用性の問題を単純な機器の並列構成によって解決するものではありません。可用性を維持するためには Active-Standby の考え方が一般的ですが、SonicWall ではセキュアリモートアクセスデバイスの設置された場所にかかわらず全てのデバイスが CMS によって高可用性を実現します。たとえばデバイスが日本、アメリカ、EU に配備される場合、ユーザは最適なデバイスに接続を試みます。



CaptureATPとの統合

セキュアリモートアクセス は Capture Advanced Threat Prevention と連携し、VPN を通過するトラフィックをクラウド上のサンドボックスで脅威の解析・検知が可能です。一般的に SSLVPN 装置とサンドボックス製品を利用する場合、別アプライアンスとして配備しますが、SonicWall ではセキュアリモートアクセスデバイス 1 台でセキュアなネットワーク環境を提供します。

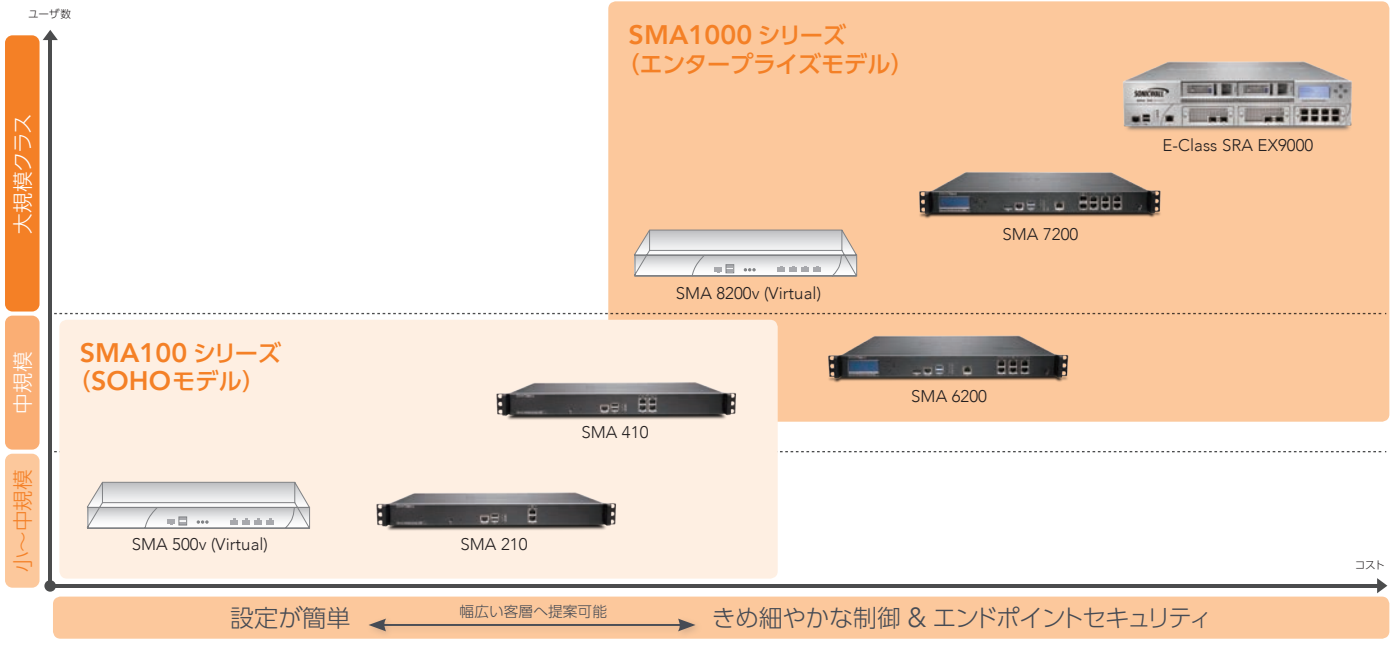


A cloud-based, multi-engine solution for stopping unknown and zero-day attacks at the gateway

テレワークによる働き方改革

日本では政府主導のもと「働き方改革」の意識が高まっており、場所 / 時間に捉われることなくどこからでも働くことのできる環境整備が企業に求められています。SonicWall はこの課題に対し、セキュアリモートアクセスをご利用いただくことでセキュアなテレワーク環境を実現させ、労働の効率化と多様化、さらには災害対策の面でも寄与します。

幅広いユーザ層に適合するラインアップ



ワイヤレスネットワークセキュリティ

SonicWall ワイヤレス ネットワーク セキュリティ ソリューションは、SonicWave シリーズ のラインアップを用意しています。ギガビットの高速通信、信頼性を提供する最新の IEEE802.ac Wave 2 高速ワイヤレステクノロジーを安全・お手軽にご利用できます。

SonicWave400シリーズ

SonicWave200シリーズ

管理の特徴

- すべての SonicWall ファイアウォールには、ネットワーク上で SonicWave AP を自動検出し、自動プロビジョニングするワイヤレスコントローラが組み込まれています。SonicWall ファイアウォールと連携せず単独で AP としてご利用いただくことも可能です。新たに追加されたゼロタッチ機能により、インターネット接続されている Ethernet ケーブルを AP に差し込むだけでセットアップが完了します。これにより配備とセットアップが大幅に簡素化され、総所有コスト (TCO) が大幅に削減されます。
- ワイヤレスの管理と監視は Capture Security Center(CSC) を通じて一元的に処理され、ネットワークのすべての側面を管理するための一元管理画面を管理者に提供します。

セキュリティ面での特徴

- AP と SonicWall ファイアウォールと連携することで、ディープパケットイインスペクション技術を駆使してネットワークに出入りするすべての無線トラフィックをスキャンし、マルウェアや侵入などの有害な脅威を除去します。また、SSL/TLS 暗号化通信も検査できます。
- コンテンツフィルタリング、アプリケーション制御と可視化 Capture ATP などその他のセキュリティおよび制御機能により、追加の保護層が提供されます。
- SonicWave を単独で利用する場合でも CaptureATP と連携し、無線トラフィックの脅威を排除します。

ワイヤレス信号解析ツール Wi-Fi Planner

- ワイヤレス信号解析ツール (Wi-Fi Planner) は、ブラウザベースのアプリで、納入先のオフィスや敷地の図面を読み込むと、どの場所にどの AP モデルが最適で何台必要なのかを視覚化します。AP の導入設計コストを下げることが可能です。

モバイルアプリによるゼロタッチ展開

- すべての SonicWave デバイスでゼロタッチ機能を利用できます。ゼロタッチはお使いのモバイルアプリを使用し、製品のアクティベーションから設定、監視まで行うことが可能です。AP を箱から出して 3 分でご利用することができます。モバイルは iOS および Android をサポートしており、アプリは AppStore・Android Market でダウンロードすることができます。

SONIC Wi-Fi MOBILE APP

- どこからでも簡単にネットワークにアクセス
- AP を簡単にセットアップして監視
- 簡単にデバイスを登録・組み込み
- iOS および Android で入手可能

設置する場所を選ばない屋外モデル

- 屋外のイベントや工事現場といった雨の降る場所でも SonicWave を利用することができます。さらにゼロタッチ機能を組み合わせてご利用いただければ、設置コストと時間を掛けず手軽にセキュアな無線ネットワーク環境を整備することが可能です。

Capture Client
エンドポイントセキュリティ

SonicWall Capture Client は、さまざまな保護機能を備えた統合エンドポイント製品です。
Capture Client は、SentinelOne が提供する次世代型のマルウェア防御エンジンを搭載し、機械学習やシステムロールバックなどの高度な脅威防御技術を提供します。

・あらゆる状況下での攻撃を軽減
・ご利用のコンピュータを継続的に監視
・感染したコンピュータをクリーンな状態にロールバック

SYSTEM REQUIREMENTS
Operating Systems
Windows 7 and upwards
Windows Server 2008 R2 and upwards
Mac OS/OSX 10.10 and upwards

AIを駆使した次世代アンチウイルス

次世代のマルウェア対策や暗号化されたトラフィックの可視化など、複数のエンドポイント保護機能を提供する統合クライアント・プラットフォームです。クラウド・サンドボックス・ファイル・テスト、包括的なレポート作成、およびエンドポイント保護を行います。

次世代ファイアウォールとの統合

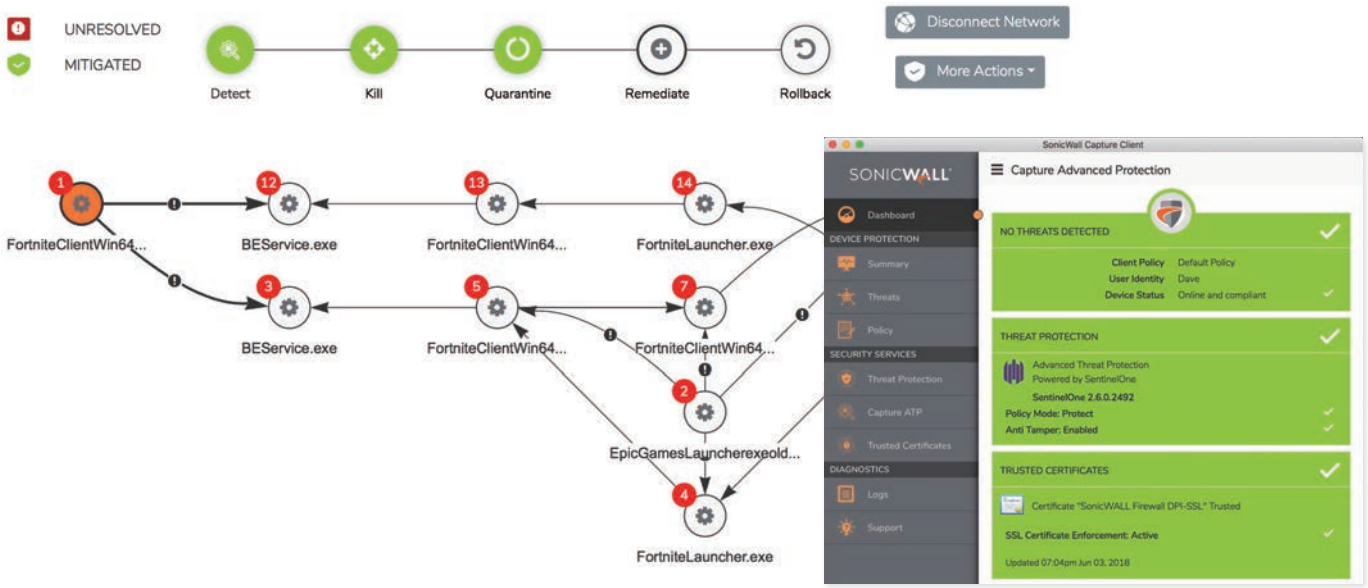
Capture Client は SonicWall の次世代ファイアウォールと連携し、包括的なセキュリティ対策を実現します。Capture Client をインストールしていないデバイスはファイアウォール通信を許可しないといったデバイス制御が可能です。管理画面は一元化され、IT 管理者の運用負担を軽減します。

感染端末に対する充実した対処機能

Capture Client は検知・防御のみならず、侵害後の被害軽減および復旧にも対応しています。感染端末をネットワークから切り離し、被害拡大を未然に防止するネットワーク隔離や、悪意あるプロセスの強制終了といった対処機能を始め、ランサムウェアの被害にあった際に感染前の状態に復元するロールバック機能を有しています。

USBデバイス制御

USB といった外部デバイスの利用を制御することが可能です。これにより USB 経由でマルウェア感染するリスクを軽減することができます。マルウェアの感染ルートは主にメール・Web・USB と言われており、SonicWall の次世代ファイアウォールおよび E メールセキュリティプロダクトを組み合わせてご利用いただくことで主なマルウェア感染ルートを断つことが可能です。

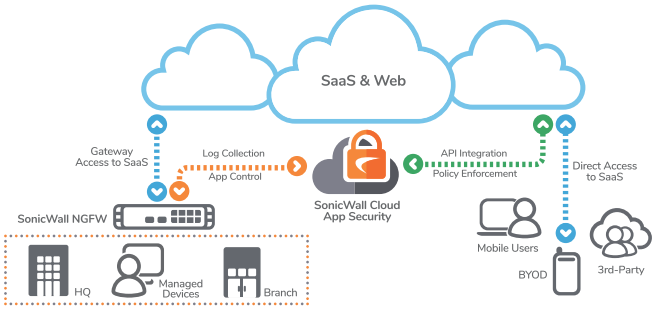


クラウド・セキュリティ

Cloud App Security

Office 365, G Suite など SaaS アプリの次世代セキュリティ

SonicWall クラウド・アプリケーション・セキュリティは E メール、メッセージ、共有ファイルおよびファイルストレージを含む、クラウドアプリケーション内のユーザーとデータに向けた次世代のセキュリティを実現しています。SaaS アプリケーションを採用する組織向けに、SonicWall クラウドアプリケーションセキュリティは最高クラスのセキュリティをシームレスに提供します。



脅威の無いクラウドアプリの利用を実現

- 可視性、データ防御、高度な脅威の防御、クラウド利用のコンプライアンスを実現
- Office 365 と G Suite での標的型フィッシング、なりすまし、アカウント攻撃の防止
- リアルタイムやイベント履歴を分析することで侵害やセキュリティギャップを特定
- API やログを使って帯域外トラフィック分析が可能

NSv 仮想NGFWシリーズ for Cloud

次世代クラウドセキュリティでクラウド上のワークロードをリアルタイムに防御

パブリック / プライベート クラウドに対するクラス最高の高度な保護

- 一貫したリアルタイム自動侵害検知および防御機能を提供
- Real-Time Deep Memory Inspection (RTDMI) と Reassembly-Free Deep Packet Inspection（RFDPI）活用
- Capture ATP マルチエンジン・サンドボックスを利用してゼロデイ脅威を阻止
- ウイルス、スパイウェア、マルウェア、侵入、暗号化された脅威、悪意のあるアプリやウェブサイトをブロック

WEBアプリケーションファイアウォール

WEB アプリケーションを中断なく高速かつ安全に配信

SonicWall WAF シリーズは、コンプライアンス・データを未公開にしたり、最高の性能を維持しながらウェブ・プロパティを中断せずに保護したりするための高度なウェブ・セキュリティ・ツールおよびサービスを備えています。SonicWall WAF シリーズは、アプリケーション対応のロード・バランシング、SSL オフロード、復元力のための高速化、デジタル・エンゲージメントと体験の向上を可能にするレイヤ 7 アプリケーション配信機能を適用します。

Web アプリケーションの保護、脅威管理

- Capture Advanced Threat Protection (ATP) による高度な防御
- ウェブ・アプリケーションのトラフィックの完全な管理および制御による攻撃対象領域の縮小
- 仮想パッチとカスタム・ルールを利用して既知およびゼロデイ脆弱性から保護
- SQL インジェクションやクロスサイト・スクリプティング（XSS）など、OWASP が概説した最新の脆弱性および脅威から防御
- TP、2FA、SSO などの強力なセッション管理および認証要件
- データ漏洩対策（DLP）
- 視覚化、分析、および報告機能を使用して、十分な情報に基づいたセキュリティ・ポリシーを決定

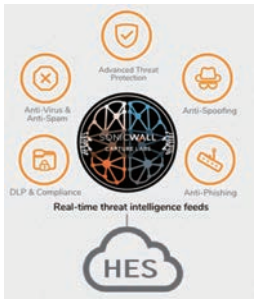
アプリケーション配信を高速化

- キャッシング、圧縮、およびその他の HTTP/TCP 最適化を有効にして、アプリケーション配信を高速化します。
- SSL トランザクションをオフロードすることで、ワークロードを減らし、性能を向上させます。
- レイヤ 7 ロード・バランシングを通じて、クラスタ化されたウェブ・サーバーに負荷を分散させます。
- ウェブ・サーバーの状態とフェイルオーバー・トラフィックを監視して高可用性を確保します。

HES（ホスティド Eメールセキュリティ）

高度な E メール脅威に対するクラウド E メールセキュリティサービス

SonicWall Email Security は包括的な多層防御でランサムウェア、ゼロデイ攻撃、スピアフィッシング、ビジネスメール詐欺 (BEC) といった高度 E メール脅威からインバウンド / アウトバウンド防御します。HES は機器不要でサービスポータルから直ちに設定でき、月契約で時間と経費の節約になります。従って HES は MSP に最適なソリューションです。



管理と分析

包括的セキュリティ管理システム

Capture Security Center（CSC）/ Global Management System (GMS)

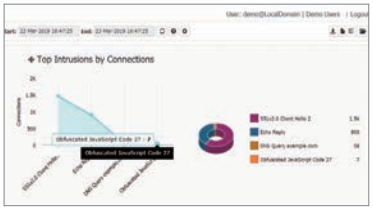
包括的セキュリティ運用管理、監視、レポーティングおよびアナリティクス

総合的アプローチでセキュリティの統制、法令規制準拠そしてリスクマネージメントを実現

- 集中管理、可視化、分析、報告による運用の簡素化
- 統合管理および制御による効率の向上とコストの削減
- 企業やサービス・プロバイダのファイアウォール変更管理要件への準拠
- 定義済みの PCI、SOX、または HIPPA レポートによりセキュリティ監査を自動化
- ソフトウェアまたは仮想アプライアンスの展開オプションにより IT アーキテクチャに簡単に統合

ダッシュボード

アプリ利用状況



侵入阻止状況

脅威アナリティクス

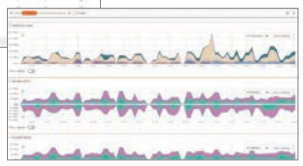
セキュリティ分析、可視化、レポート

CSC Reporting

セキュリティおよびアプリケーション・トラフィック分析、可視化およびレポーティングツール

- 包括的なグラフ報告書を通じて脅威とイベントの可視化と分析
- セキュリティ・エコシステムの健全性と性能を可視化
- セキュリティ監査可能なデータの組み合わせでコンプライアンス報告書をカスタマイズ
- 応答者は重要なリスクと脅威に迅速に対応

アプリ別レポート



ダッシュボード

即応できる実践的分析

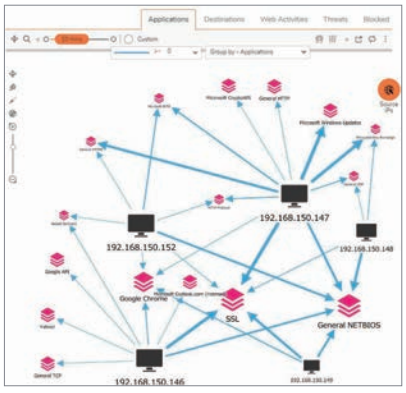
Analytics

データから決定、決定に基いて対応

SonicWall Analytics は、データに基づいた強力な分析サービスです。SonicWall Analytics は、単一画面を通じて、相関性のあるセキュリティ・データのリアルタイムの可視化、監視および警告を提示します。リアルタイムのインサイトと実用的な分析を提供する Analtyics は、セキュリティ・チーム、アナリスト、および利害関係者がセキュリティ・データを発見、解釈し、セキュリティ・リスクの優先順位を決定し、適切な防御措置を取ることができるようにします。

動的分析と洞察

- 単一画面での可視性とネットワーク・セキュリティ環境の完全な状況把握を提供
- 深部調査と科学的分析
- 潜在的なリスクと脅威、実際のリスクと脅威に関する知識と理解
- 明確性、確実性、速度を高めてリスクを探索、検出、修正
- リアルタイムで実用的な脅威インテリジェンスによるインシデント対応時間の短縮



トラフィック視覚化

ネットワーク系に差し迫った脅威リスク検知と防御

リスク・メーター

差し迫ったセキュリティ・リスクを検知し防御対策を実施

クラウドアプリの増加で脅威も企業を超えて広がっています。今や攻撃は web、クラウド、アプリケーション、エンドポイント、モバイル端末、データベースそして IoT を対象としています。 Risk Meter は、このリスクを検知し直ちに対策を取れるようにするツールです。お客様のネットワーク基盤全体にわたり稼働中のセキュリティ・リソースの状況や直面する脅威に応じリスクスコアをカスタマイズして使用できるようになっています。これによりリアルタイムで特定の防御レイヤーのグラフィックによる分析結果が提供されます。今、来ている攻撃、あらゆる脅威の可能性が分かり、潜在的なセキュリティ対策の隙間が見て取れます。

SONICWALL

SonicWall Web リソース

SonicWallホームページ

https://www.sonicwall.com/ja-jp/

データシートはこちらから
https://www.sonicwall.com/ja-jp/resources/

SonicWallセキュリティセンター

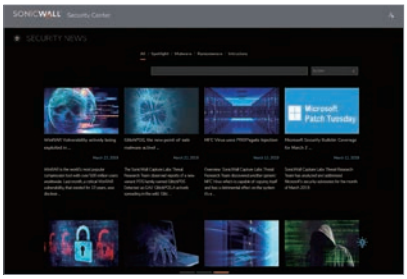
https://securitycenter.sonicwall.com/

WORLDWIDE ATTACKS – LIVE

リアルタイムに世界で発生している攻撃を世界地図で表示。

CAPTURE LABS THREAT METRICS

世界全体の脅威統計情報から前年比を表示、北米、EUR、APJ ごとの情報も表示できます。



SECURITY NEWS

世界で発生しているマルウェア / ランサムウェア / 侵入などのサイバー脅威に関するニュースを掲載しています。

SonicWallライブデモ・サイト

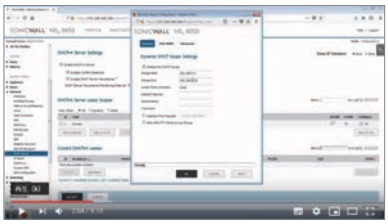
http://livedemo.sonicwall.com/

皆様にご活用いただけるSonicWall製品を体感できる操作デモ・サイトをご用意しています。

SonicWall 動画チャンネル

YouTubeで【SonicWall Japan】を検索

製品紹介動画（日本語字幕）や、トレーニングの動画をご覧頂けます。



MySonicWall

https://www.mysonicwall.com/

所有する製品やサービス、ライセンスをこのサイトで管理します。
SonicWallユーザは製品をここで登録し管理することができます。
Capture Security Center から開くこともできます。

SecureFirst パートナープログラム

https://www.sonicwall.com/ja-jp/partners/

SonicWallの新しいパートナープログラムにより、パートナー様をビジネスの成功へ導きます。
さらにSonicWall Universityにより最新の製品知識を得ることが可能です。

SONICWALL • SecureFirst •

SONICWALL UNIVERSITY

SONICWALL

SonicWall カスタマーサポートセンター

カスタマーサポートセンターへ、お気軽にお問合せください。

SonicWall カスタマーサポートセンター
TEL:0120-914-644

サポートへのお問い合わせ：https://www.sonicwall.com/ja-jp/support/contact-support/

SonicWall が提供するサポートメニュー (8x5 サポート / 24x7 サポートの2種類)

	8×5 サポート Stndard Support 8×5 Dynamic Support 8×5 Silver Support 8×5 と表記される場合あり	24×7 サポート Premier Support 24×7 E-Class Support 24×7 Gold Support 24×7 と表記される場合あり
ハードウェア製品	・技術支援　カスタマーサポートセンターの利用 (受付時間：平日 9:00 ～ 18:00) ・WEB によるサポートの提供 ・交換品先出しセンドバック保守 (受付時間：平日 9:00 ～ 18:00) ・ファームウェアアップグレード	・技術支援　プレミアムカスタマーコールの利用 (受付時間：24 時間 365 日) ・WEB によるサポートの提供 ・交換品先出しセンドバック保守 (受付時間：24 時間 365 日) ※発送は平日 9 ～ 18 時 ・ファームウェアアップグレード
ソフトウェア製品	・Application Support 8x5 ・技術支援　カスタマーサポートセンターの利用 (受付時間：平日 9:00 ～ 18:00) ・WEB によるサポートの提供 ・ファームウェアアップグレード	・Application Support 24x7 ・技術支援　プレミアムカスタマーコールの利用 (受付時間：24 時間 365 日) ・WEB によるサポートの提供 ・ファームウェアアップグレード
オンサイトサポート (ハードウェア製品のみ)	上記サポートに加えてオンサイトサポート契約の締結が可能 技術者を派遣しお客様の SonicWall 製品の交換します オンサイトサポート 24x7 受付時間：24 時間 365 日受付け可能	

※ご購入頂いた製品によって利用できるサポートメニューが変わります。

故障対応のイメージ(交換品先出しセンドバック保守の場合)

Step1

故障の申請

お客さまからサポートセンターへお申込み頂きます。

Step2

交換機の発送

故障受付完了後、交換品を発送します。(受付時間や納品場所によって納品日が変わる場合があります)

Step3

交換機の設置

お客さまにて交換作業を実施頂きます。(サポートセンターに TEL によるサポートを行うことが可能です)

Step4

故障機の返送

故障機を弊社 RMA センターへご返送を頂きます。

以上で交換作業が完了です。

販売代理店

SONICWALL®

https://www.sonicwall.com/ja-jp/

ソニックウォール・ジャパン株式会社　〒100-0011 東京都千代田区内幸町 1-5-2　内幸町平和ビル 20F

SNWL201912-A