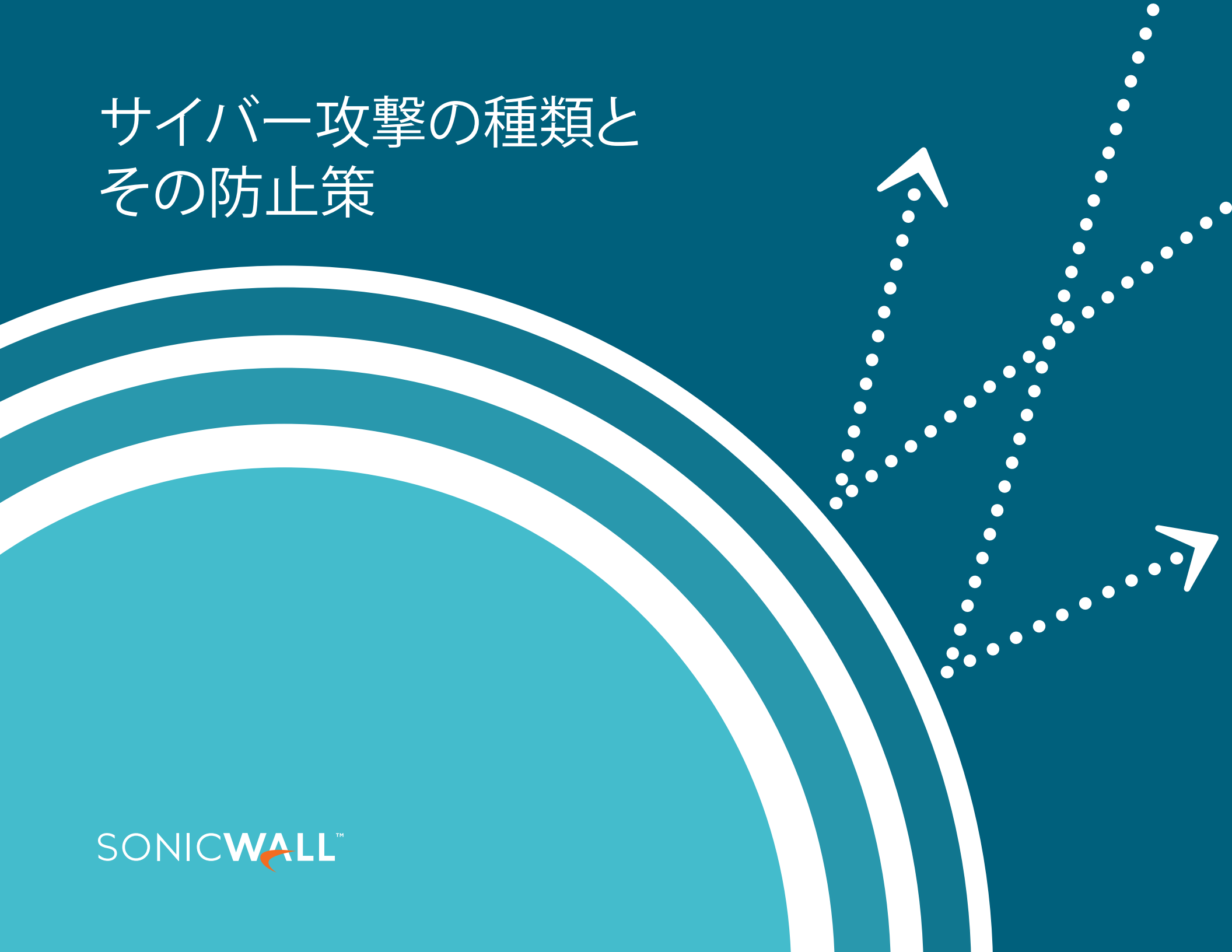
# サイバー攻撃の種類とその防止策



SONICWALL™

# はじめに

今日のサイバー犯罪者は、複数の複雑な手法を使用してひそかに企業ネットワークへ侵入し、知的財産を盗んだり、ファイルを押さえて身代金を要求したりします。こうした脅威では、検出を逃れるために暗号化がよく使用されます。

標的の脆弱性を悪用した攻撃者は、侵害されたシステムにマルウェアをダウンロードしてインストールしようとします。多くの場合、従来のアンチウイルスソリューションでは認識されない、新たに進化を遂げたマルウェアが使用されます。

この e-book では、サイバー犯罪者がネットワークへの侵入に使用するツールと戦略について詳述し、こうした侵入の防止策を提示します。

サイバー犯罪者は 24 時間 365 日 活動しており、
脆弱性を悪用しようとしています。

サイバー攻撃の戦略 1

# マルウェアで ネットワークを 絶え間なく攻撃

電子メール、モバイルデバイス、Web トラフィック、さらには自動化されたエクスプロイトなど、あらゆるベクトルを通じて攻撃が仕掛けられます。企業の規模は関係ありません。ハッカーにとって重要なのは IP アドレスや電子メールアドレスであり、水飲み場型攻撃の可能性です。攻撃者は、自動化ツールを使用してエクスプロイトを実行します。または、昼夜を問わずにフィッシング電子メールを送りつけます。

多くの組織が直面している問題は、対策を講じる適切なツールを所有していないことです。多くの場合、トラフィックの浄化、エンドポイントの保護、不正な電子メールの除去に役立つ自動化ツールが不足しています。ほかにも、現在のファイアウォールでは暗号化されたトラフィックを調べることができず隠された脅威を発見できないケースや、限られたオンボード・システム・メモリを使用してマルウェアシグネチャを保管しているケースなどが見られます。

SONICWALL™

攻撃への対策 1

# 24 時間、週 7 日体制でネットワークを保護

多くの新型マルウェアが常に開発され続けているため、組織は随時更新されるリアルタイム保護で最新の脅威に対抗する必要があります。セキュリティソリューションが効果を挙げるには、24 時間、週 7 日の継続的な更新が不可欠です。さらに、マルウェアの種類と変種は多岐にわたるため、ファイアウォールで利用可能なメモリの容量を超過します。

ファイアウォールでは、広範な視野でマルウェアを監視し、最新の変種を見つけて正しく特定できるように、ネットワークサンドボックスとクラウドを使用する必要があります。加えて、セキュリティソリューションが保護の動的な更新をサポートしていることも確認します。その対象には、ファイアウォールゲートウェイだけでなく、モバイル/リモートのエンドポイントや電子メールも含まれます。



最新マルウェアの脅威にリアルタイムで対抗するために、クラウドのパワーを活用したセキュリティプラットフォームが求められています。


サイバー攻撃の戦略 2

# さまざまな形態のマルウェアがネットワークに感染

サイバー攻撃者は各種の攻撃ベクトルとマルウェアを使用してネットワークに侵入します。最も一般的なマルウェアとして、ウイルス、ワーム、トロイの木馬、スパイウェア、ランサムウェアの 5 つが挙げられます。

**コンピューターウイルス**は、当初、感染したフロッピーディスクの共有によって広まりました。テクノロジーの進化に伴って、ウイルスの配布方法も進化を遂げてきました。今日のウイルスは、一般にファイル共有、Web ダウンロード、電子メールの添付ファイルを通じて広まります。

**コンピューターワーム**は 1980 年代の後半から存在しますが、蔓延するようになったのは組織内でネットワークインフラが普及してからです。コンピューターウイルスとは異なり、ワームは人間を関与させずにネットワーク内を移動できます。

**トロイの木馬**は、ネットワークから機密データを抽出するように特別に設計されています。トロイの木馬の多くは、感染したシステムを制御し、バックドアを開けて攻撃者が後でアクセスできるようにします。トロイの木馬は、ボットネットの作成にしばしば使用されます。

**スパイウェア**は、本来は悪意のあるものではありませんが、Web ブラウザに感染してほとんど使用不能にすることが多いため、非常に迷惑な存在です。正規アプリケーションを装ったスパイウェアがユーザーに何らかの恩恵を与えながら、ユーザーの行動と使用パターンをひそかに記録することもあります。

**ランサムウェア**は、多くの場合、エンドポイントやサーバーのファイルを暗号化する攻撃であり、暗号化キーの受領と引き換えに身代金をビットコインで支払うことをエンドユーザーに要求します。ランサムウェアがビジネスクリティカルなシステムに拡大すると、身代金のコストが数十万ドルに膨れ上がるおそれがあります。

SONICWALL™

攻撃への対策 2

# あらゆる種類のマルウェアからネットワークを確実に保護

すべてのファイアウォールは、ウイルス、ワーム、トロイの木馬、スパイウェア、ランサムウェアから組織を守る必要があります。これを最も効果的に達成するには、低遅延で単一パスのアプローチにこれらの保護を統合し、ゲートウェイだけでなく、従来の境界を越えたエンドポイントでも攻撃ベクトルをブロックします。求められる機能の例を以下に示します。

- **ネットワークベースのマルウェア保護**: 侵害されたシステムへのマルウェアのダウンロードや転送を阻止します。
- **継続的でタイムリーな更新**: 多くのマルウェアの変種が新たに生じています。それらが発見されたらすぐに防御できるようにネットワークを 24 時間体制で保護します。
- **侵入防止サービス（IPS）**: 攻撃者がネットワークの脆弱性を悪用するのを防ぎます。
- **ネットワークサンドボックス**: 疑わしいコードはクラウドベースの隔離された環境に送信して除去と分析を行い、未知のマルウェアを見つけます。
- **アクセスセキュリティ**: ネットワーク境界の内外にあるモバイル/リモートエンドポイントにセキュリティ対策を施します。
- **電子メールのセキュリティ**: フィッシング、スパム、トロイの木馬、ソーシャルエンジニアリングの攻撃が電子メールで送られてくるのを防ぎます。

ネットワークにアクセスするデバイスのすべてに最新のアンチウイルス保護ソフトウェアを組み込むことで、ネットワークのマルウェア防御に新たな層が追加されます。PC 上でのアンチウイルス実行とネットワークのファイアウォールを組み合わせることで、サイバー犯罪者がネットワークへの侵入に使用する手段を大幅に削減できます。

脅威の一歩先を行くために、マルウェアに対する多層型の保護策を検討します。

サイバー犯罪者の多くは、発見したネットワークの脆弱性に基づいて標的を定めます。

サイバー攻撃の戦略 3

# 最も脆弱なネットワークを見つけて侵入

ファイアウォールベンダーの多くは優れた脅威防御を提供していると主張しますが、そのソリューションの効果を実証できるベンダーの数は多くありません。性能が劣るファイアウォールを使用している組織も、自社のネットワークは保護されていると信じているかもしれません。しかし熟練したサイバー犯罪者は、検出を逃れる複雑なアルゴリズムを使用することで、侵入防止システムをひそかに通過しシステムに侵入することができます。

一部のファイアウォールはパフォーマンスを犠牲にして保護を提供しているため、こうしたファイアウォールを使用している組織は、高性能なネットワークの需要を満たすために、セキュリティ対策を停止または制限したい気分に襲われているかもしれません。これはきわめて危険であり、回避すべき行為です。

ネットワークセキュリティのもう 1 つの弱点は人的要因です。サイバー犯罪者は、フィッシング手法によってログイン情報や他の認証情報を取得し、内部から攻撃を仕掛けることでファイアウォールによる保護を回避できます。さらに、従業員がネットワークセキュリティの境界外でモバイルデバイスを使用しているときに、そのデバイスを紛失したり、侵害を受けたりするおそれがあります。

SONICWALL™

攻撃への対策 3

# 優れた脅威防御と高いパフォーマンスを実現する、包括的なセキュリティプラットフォームの選択

ネットワークベースのマルウェア防御に対して、ICSA ラボによる中立的なテストと認証を受けたセキュリティソリューションを探します。

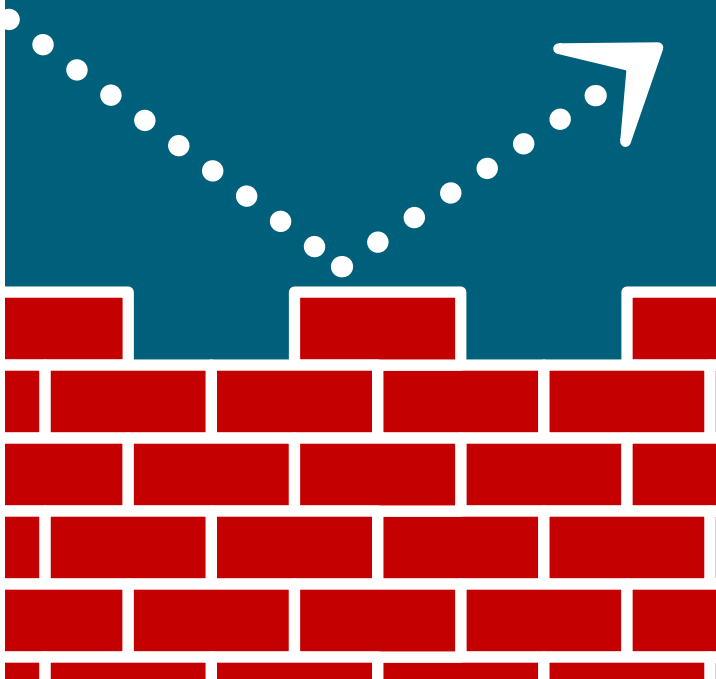
あらゆるサイズや種類のファイルをスキャンして、トラフィックフローの変化に対応できる、マルチコアのプラットフォーム設計について検討します。すべてのファイアウォールは、パフォーマンスを損なわずに内外の攻撃からネットワークを保護するエンジンを必要とします。

企業のネットワーク環境を標的にした最新のマルウェアの発見に役立つネットワークサンドボックスを備えたファイアウォールを探します。これが通常の日と、ファイルが人質に取られる日の分かれ目になるかもしれません。

セキュリティ戦略には、ネットワーク境界の内外にあるモバイル/リモートエンドポイントの保護を含める必要があります。

さらに、電子メールのセキュリティ体制を整え、フィッシング、スパム、ウイルス、ソーシャルエンジニアリング、およびその他のメール経由の脅威から保護する必要があります。

すべての
ファイアウォールは、
パフォーマンスを
損なわずに内外の
攻撃から
ネットワークを
保護するエンジンを
必要とします。



世界中で常に新たな脅威が
生まれています。

サイバー攻撃の戦略 4

# 頻繁な形態変化とグローバルな攻撃

サイバー犯罪者の多くは、継続的にマルウェアを新たに作り直し、それを世界中のサイバー犯罪者と共有することで成功を収めています。つまり、世界中で常に新たな脅威が生まれているのです。サイバー犯罪者の多くは、攻撃するときに「ショーウィンドー破り」の手法を使用します。つまり、侵入し、取れるものを取って、誰かが警報を発する前に逃げるのです。その後、ほかの場所で同じ攻撃を繰り返します。

長い時間をかけてより多くのデータにアクセスできるように、慎重に行動するサイバー犯罪者もいます。Web 経由の攻撃もあれば、電子メール経由の攻撃もあります。あるいは、ネットワークセキュリティの境界外でローミングしていたデバイスに感染し、それを介してネットワークに侵入する攻撃もあります。

SONICWALL™

攻撃への対策 4

# グローバルな脅威を防御するファイアウォールの選択

保護を最大限に高めるには、脅威への迅速な対応が不可欠です。新たな脅威への対策をファイアウォールに迅速に導入するために、セキュリティ対策の専門家で編成された、対応の速い独自の社内チームを擁するセキュリティ・ソリューション・プロバイダを探します。さらに、このチームは、広範なセキュリティコミュニティと連携して活動範囲を広げる必要があります。

世界全体にわたるクラウドベースの包括的なマルウェアカタログを広範なソリューションで活用し、ローカルなファイアウォール分析を強化します。

最後に、シンプルなファイアウォールでも地理的な情報を使用した識別とブロックが可能ですが、高性能なファイアウォールは、ボットネットフィルタリング機能を追加して、危険なドメインから送られるトラフィックや特定の場所に対する接続をブロックすることで、グローバルな既知の脅威にさらされるリスクを軽減します。



最新のグローバルな脅威を防ぐには、世界規模のセキュリティソリューションに投資してください。

# まとめ

サイバー攻撃は増加の一途をたどっていますが、効果的な防御策があります。自社のネットワーク環境に合った攻撃対策ソリューションを評価するには、ホワイトペーパー『Achieving Deeper Network Security（より強固なネットワークセキュリティの実現）』をダウンロードして詳細を確認してください。

SONICWALL™

## 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、E 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。

If you have any questions regarding your potential use of this material, contact:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Refer to our website for additional information.
**www.sonicwall.com**

**© 2016 SonicWall Inc. ALL RIGHTS RESERVED.**

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with SonicWall Inc. and/or its affiliates' products.No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of SonicWall products.EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON- INFRINGEMENT.IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. SonicWall Inc. and/or its affiliates do not make any commitment to update the information contained in this document.

Ebook-TypesOfCyberAttacks-US-KJ-24644



SONICWALL™