



アプリケーションを検知、 可視化、制御するための ベストプラクティス

要旨	2
はじめに	2
アプリケーション制御の課題	2
可視性と制御の喪失	2
アプリケーションは新たな脅威をもたらす	3
バンド幅の使用を制限する必要性	3
情報漏洩の可能性	3
従来のアプリケーション制御	3
ポートブロッキングおよび URL フィルタリング	3
必要とされている新たなアプリケーション制御手法	4
完全なコンテンツプロテクション	4
インターネットベースのアプリケーションの検知	4
FortiGuard Application Control Database	5
アプリケーション制御リスト	5
エンドユーザーとアプリケーションの関連付け	5
アプリケーション制御の粒度	6
アプリケーショントラフィックの把握	6
アプリケーションモニタリング/ レポート	6
アプリケーション制御のパケットロギング	7
エンドポイントにおけるアプリケーション制御	7
オンラインリソース	7
結論	7
フォーティネットについて	8
FortiOS について	8

要旨

IT アプリケーションで使用される新しいテクノロジーは、企業内およびインターネットゲートウェイにおけるネットワークトラフィックの量を増大させ、複雑化させています。このような新しいテクノロジー実装に伴う新たなセキュリティ脅威を発見し、回避することは、新しいテクノロジーを積極的に活用する企業にとって、先送りすることができない、待たなしの重要課題になってきています。この重要課題に対応するために、今、インターネットベースのアプリケーションを監視、制御する新たな方法を配備することが不可欠になっています。

はじめに

IT とビジネスの一体化によって、IT アプリケーションは今日の企業の生命線となりました。IT アプリケーションの支援なしにはビジネスの遂行は不可能になっていると言っても過言ではありません。そして、今日では、企業ネットワークやインターネットを介してのアプリケーションへのアクセスが許可されることで、ワークグループ内部、全社横断的、外部パートナー、お客様との更なる情報共有が推進され、新たなビジネスを生み出してきています。IT アプリケーションを企業ネットワーク内のデスクトップコンピューターやサーバーからしか起動できなかったつい最近まで、データセキュリティポリシーは比較的に容易に実行できました。しかし、今日の企業は、新世代のセキュリティ脅威に立ち向かっています。コンシューマー主導の新しいテクノロジーは、インターネットベースのアプリケーションの新たな波を巻き起こし、ファイアウォールなどの従来のネットワークセキュリティの障壁を容易に迂回し、企業ネットワーク環境内へと浸透してきています。

Facebook、Twitter、Skype といった、アプリケーションとして知られるこれらの新しいインターネットベースのコミュニケーションツールは、企業内部に着実に浸透しています。悪意ある脅威や情報漏洩から自社ネットワークを守ろうとする企業には、必然的に、新たな課題が生じています。従業員にアプリケーションへのアクセスを許可することが、データセキュリティポリシーの実行をより一層複雑な問題にしています。さらに悪いことに、多くの企業には、これらのアプリケーションを検知するのはもちろん、制御するための方法がありません。結果として、機密情報が意図的または誤って不正流用される可能性が高まっています。

アプリケーション制御の課題

アプリケーションは、従業員、契約社員、パートナー企業、お客様の間で、常時接続されたリアルタイムのコミュニケーションを可能にし、生産性に大きな飛躍をもたらしています。この結果、多くの企業はインスタントメッセージング、Twitter フィード、Facebook ページを日々のビジネスプラクティスに統合し始めています。しかし、これらの新しいアプリケーションは、セキュリティに対する懸念を生み出しています。信頼あるポートを潜り抜けたり、独自開発の暗号化アルゴリズムを使用したり、場合によっては、他のアプリケーションのふりをして従来のファイアウォールによる検知とブロックを逃れたりすることができるからです。これにより、内部の企業ネットワークからデジタル情報を難なく、検知されずに転送したり、新世代のウイルスおよび脅威が従来のネットワークファイアウォールを突破したりすることが極めて容易になります。

可視性と制御の喪失

telnet および FTP といった従来のインターネットベースのアプリケーションへのアクセスは、ネットワークゲートウェイで個々の TCP ポートおよび UDP ポートをブロックまたは有効化することで、実現しています。今日、複数のアプリケーションが同一のポートを使用できる一方で、1つのアプリケーションが複数のポートを使用する場合もあります。回避行動をとるアプリケーションは、検知および制御を避けるために非標準のポートや SSL 暗号化を使用できます。“アプリケーション”という定義さえも変化しました。一部のアプリケーションは、Web ブラウザ内からプラグインとして実行されるほか、ホストアプリケーション内で実行されるアプリケーションもあります。Facebook といったソーシャルメディアサイトによって、ユーザーはチャットしたり、動画を見たり、ゲームしたり、他のアプリケーションを起動したりすることさえできます。このすべては、ブラウザ内から実行されるのです。

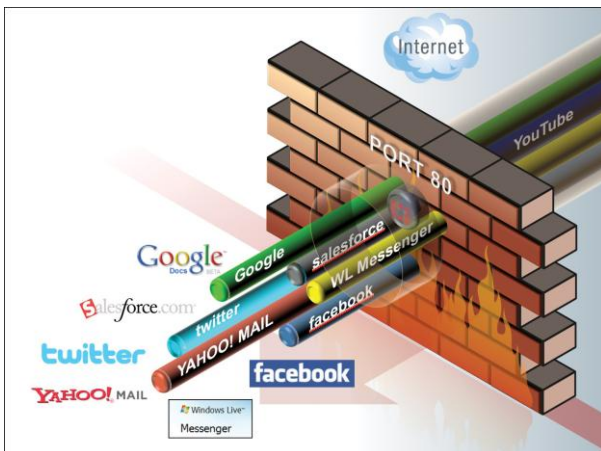


図 1: 従来のファイアウォールを通過するアプリケーション

アプリケーションは新たな脅威をもたらす

Koobface ウイルスなどの Web ベースの脅威から防衛する場合、ポートやプロトコルのブロッキングのみのステートフルファイアウォールは、十分ではありません。たとえば、Koobface は、Facebook、Twitter、Friendster といったソーシャルネットワーキングアプリケーションのユーザーをターゲットにしたコンピューターワームですが、疑いを持たないユーザーがリンクをクリックして動画などのメディアをダウンロードすると、実際には Koobface の“ボット”、すなわち、ボットネットワーククライアントをインストールしているのです。ボットは、感染コンピューターから悪意あるサービスを開始し、他のボットとの通信を通して、また、インターネット経由で“コマンド・アンド・コントロール”(C&C)サーバーへと通信を開始することで、グローバルなボットネットを形成できます。Koobface ボットは、個人情報とパスワードを Koobface C&C サーバー¹にアップロードし、ユーザーを他の悪意あるサイトに誘導します。このサイトでは、さらなるマルウェアがダウンロードされる可能性があります。Koobface によってダウンロードされるコンポーネントのうち、著名なセキュリティサイトへのアクセスのほか、攻撃者による感染コンピューターのさらなる不正使用を可能にするプロキシツールへのアクセスをブロックするのは、DNS フィルタープログラムです。他の最近の脅威には、Sasfis、Hiloti、Bredolab、Mariposa/Butterfly のボット²があります。

バンド幅の使用を制限する必要性

たとえば、動画のストリーミング、Web ベースのゲームへの参加のために企業内部からアクセスされるアプリケーションは、野放しにしておく大量のネットワークリソースを消費する可能性があります。ネットワークの大量使用は、そのネットワーク上で実行されているミッションクリティカルなコミュニケーションおよびアプリケーションの速度を低下させる可能性があり、結果として、作業者の生産性を低下させ、不必要なバンド幅の購入を企業に強いることとなります。マイケルジャクソンの告別式やサッカーワールドカップの決勝戦といったイベントは、全世界の企業およびサービスプロバイダーのネットワークに大きな負荷をかけます。しかし、多くの企業は、これらの新たなテクノロジーやアプリケーションへのアクセスをブロックしたがりません。重大なコミュニケーションが制限されたり、従業員との間に不和が生じることを恐れているのです。情報漏洩の可能性

Web ベースのマルウェアや悪意ある Web サイトは、アプリケーションを悪用して貴重な顧客情報や企業機密を盗みます。しかし、これらの脅威の一方で、アプリケーションは、瞬時の一般共有や情報表示を意図的に極めて効果的に実行できるようになっています。時には、アプリケーションによって、機密データが誤った人に送信されたり、間違っただけの人と共有してしまうことがあります。これは、企業を罰金、訴訟、否定的報道にさらすものです。たとえば、Twitter Direct Message は、テキストメッセージを他の Twitter ユーザーに直接送信できる機能です。受信者は返信の際に必ずメッセージの前に「dm」と入力する必要がありますが、これを忘れると、Twitter はその返信を一般向けの「Tweet」として扱い、自動的にそのフォロワーすべてに送信し、誰もがアクセスできるようになります。

従来のアプリケーション制御

これまで、セキュリティ管理者は、ネットワークの周囲にステートフルファイアウォールをインストールすることで、アプリケーションによる組織外部へのデータ転送を防ぐことができました。ステートフルファイアウォールは、OSI 7 層モデルのネットワークレイヤーで動作し、パケットのヘッダーを調べて、確立されたネットワーク接続を状態表において追跡します。接続が一度確立されると、その接続に関連する以後の全トラフィックは安全であると見なされ、非常に限定的な検査(インスペクション)あるいは検査なしでファイアウォールを通過します。

ポートブロッキングおよび URL フィルタリング

ステートフルファイアウォールは、アプリケーションのブロックに効果的でした。というのも、アプリケーションはこれまで、ネットワーク経由で通信される場合には特定のコンピューターポートおよびプロトコルに関連付けられていたからです。アプリケーションに「危険」のフラグが付けられると、ネットワーク管理者はすばやくファイアウォールポリシーを変更して、そのアプリケーションに関連するポートおよびプロトコルをブロックまたは許可することができました。しかし、従来のポート

¹ Koobface Worm Doubles C&C Servers in 48 Hours
http://threatpost.com/en_us/blogs/koobface-worm-doubles-cc-servers-48-hours-031110

² Security Minute: November Edition Looks at Spam Reduction, Koobface Takedown and Hiloti Trojan
<http://blog.fortinet.com/security-minute-november-edition-looks-at-spam-reduction-koobface-takedown-and-hiloti-trojan/>

ベースのプロテクションは、お客様の要件に合致しない場合もあります。なぜなら、たとえばポート 80 をブロックするということは、Web アクセスを完全にブロックするというものであり、大多数の企業にとってのオプションではなくなっているためです。

URL フィルタリングも、信頼のない Web サイトや、従来の Web ベースのアプリケーション (Yahoo メールなど) へのアクセスをブロックするゲートウェイにおいて、適用することが可能でした。しかし、多くの新しいアプリケーションは、Web ブラウザからまたはブラウザのプラグインとしてインターネット経由で実行されるため、Web ベースの脅威やドライブバイ攻撃は、従来の URL フィルタリングやアンチウイルス保護の隙間をすり抜けることもできます。さらには、Web フィルタリングはサイト全体へのアクセスをブロックすることが得意ですが、複雑なソーシャルネットワーキングサイトへのアクセス制御には役立ちません。こうしたサイトには、貴重な機能とブロックすべき機能の両方があるのです。

必要とされている新たなアプリケーション制御手法

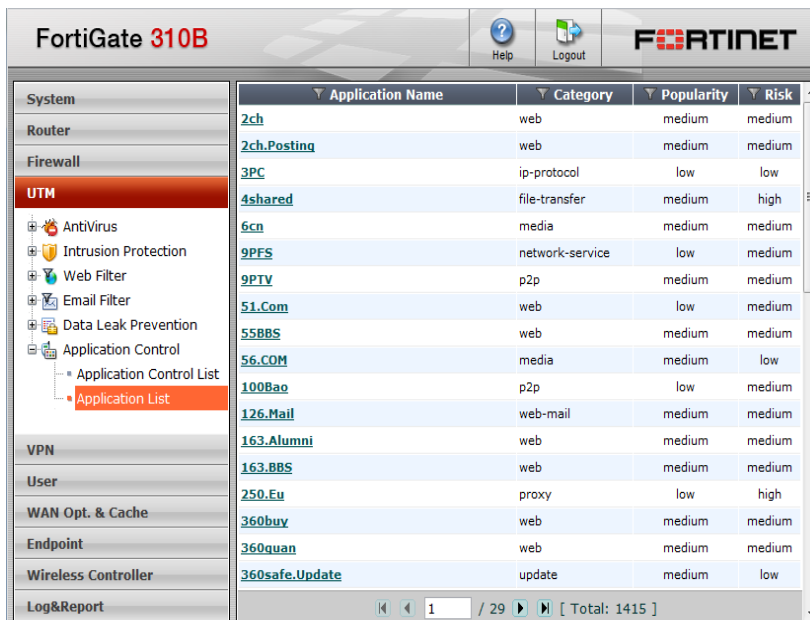
1 つの Koobface 感染によって、企業秘密の漏洩または「なりすまし」が発生する恐れがあります。それでも、多くの企業には、このタイプの悪意あるコードのストリーミングコンテンツを検査するための有効な方法がありません。必要な業務機能を維持しつつ重要な情報を保護したいと考える企業は、自社ネットワークを横切るテクノロジーやアプリケーションをしっかりと制御する必要があるのは明らかです。アプリケーション制御はもはやブロックや許可といった単純な話ではありません。ソーシャルネットワークの到来で、複数のプロテクションレイヤーが今は必要とされています。

完全なコンテンツプロテクション

情報漏洩を防ぎ、新たな脅威を軽減するために、企業は、レガシーアプリケーションに加えて新種のインターネットベースアプリケーションを効果的に制御できるようにする必要があります。また、ゲートウェイやエンドポイントで、アプリケーションの使用状況やトラフィックを検知、監視、制御できるようにする必要があります。さらには、セキュリティポリシーを通して適切なアクセス権が割り当てられるようにするために、アプリケーションとエンドユーザー間の関連付けを作成する必要があります。

Fortinet Application Control は、FortiOS™ が提供するセキュリティ機能であり、分類 (クラシフィケーション)、行動分析、エンドユーザー関連付けに基づいて、ネットワークとエンドポイントにおけるアプリケーションの使用を検知し、制限することができます。アプリケーションをデフォルトで拒否したり、臨機応変に許可したりすることが可能です。FortiOS は、すべての FortiGate® 統合型セキュリティアプライアンスで使用される、セキュリティが強化されたオペレーティングシステムです。以下は、Fortinet Application Control が提供する重要な機能および利点の一部です。

インターネットベースのアプリケーションの検知



Application Name	Category	Popularity	Risk
2ch	web	medium	medium
2ch.Posting	web	medium	medium
3PC	ip-protocol	low	low
4shared	file-transfer	medium	high
6cn	media	medium	medium
9PFS	network-service	low	medium
9PTV	p2p	medium	medium
51.Com	web	low	medium
55BBS	web	medium	medium
56.COM	media	medium	low
100Bao	p2p	low	medium
126.Mail	web-mail	medium	medium
163.Alumni	web	medium	medium
163.BBS	web	medium	medium
250.Eu	proxy	low	high
360buy	web	medium	medium
360quan	web	medium	medium
360safe.Update	update	medium	low

図 2: Fortinet Application Control

ネットワークトラフィックとアプリケーションは通常、使用されるポート、発信/宛先アドレス、トラフィック量を追跡することで、ファイアウォールにおいて制御されます。しかしながら、これらの方法は、インターネットベースアプリケーションからのトラフィックを正確に定義し、制御するには不十分な場合があります。この問題に対処するため、Fortinet Application Control はプロトコルデコーダーを用いて、アプリケーションに一意のシグネチャのネットワークトラフィックを復号化し、調べます。アプリケーションが非標準のポートやプロトコルを使用して姿を隠しても、発見できます。加えて、プロトコルデコーダーは、暗号化されたネットワークトラフィックを復号化して調べることが可能です。これによって、アプリケーション制御を IPSec および SSL で暗号化された VPN トラフィックに適用することができ、HTTPS、POP3S、SMTPS、IMAPS の各プロトコルを網羅します。

Fortinet Application Control には、サーバアドレスやポートといった知識が不要です。

FortiGuard Application Control Database

ネットワークトラフィックは一度復号化されれば、アプリケーションはその一意のシグネチャで識別することができます。Fortinet Application Control は、利用可能な最大規模のアプリケーションシグネチャデータベースの 1 つである FortiGuard® Application Control Database を活用しています。これによって、Fortinet Application Control は、1,400 以上の異なる Web ベースのアプリケーション、ソフトウェアプログラム、ネットワークサービス、ネットワークトラフィックプロトコルを検知できるようになります。FortiGuard Application Control Database は、新しいアプリケーションのシグネチャのほか、既存アプリケーションの新バージョンのシグネチャを使って、継続的にリフレッシュされます。FortiGuard Services は、FortiGate 統合型セキュリティアプライアンスに対して計画的更新を定期的に提供し、Fortinet Application Control が常に最新のシグネチャを利用できるようにしています。

アプリケーション制御リスト

明示的に管理することが必要なアプリケーションは、ファイアウォールポリシー内のアプリケーション制御リストに入れられます。ネットワーク管理者は、複数のアプリケーション制御リストを作成できます。この各リストは、一意のアプリケーションリストからのネットワークトラフィックを許可、ブロック、監視するよう構成することが可能です。アプリケーションの“ホワイトリスト”は、高セキュリティネットワークでの使用に最適です。このリストによって、リストに掲載されたアプリケーションからのトラフィックだけをゲートウェイを通過させることができます。一方、アプリケーションの“ブラックリスト”は、リストに入っていないすべてのアプリケーショントラフィックを通過させることができます。アプリケーションは、個別に制御することも、カテゴリ分けしてグループとして制御することもできます。デフォルトの多数のアプリケーション制御リストには、Fortinet Application Control が備わっています。これらのデフォルトのリストは、追加設定なしで使用することも、特定のセキュリティ要件を満たせるようカスタマイズして使うこともできます。

表 1: フォーティネットが提供するデフォルトのアプリケーション制御リスト(一部)

デフォルトのリストの名称	内容
block-p2p	既知の P2P (Peer-to-Peer) のアプリケーションをブロックする一方で、他のすべてのアプリケーショントラフィックを許可する。
monitor-all	すべてのトラフィックのアプリケーション制御モニタリングを有効化する。すべてのアプリケーショントラフィックを許可する。
monitor-p2p-and-media	P2P カテゴリおよびメディアカテゴリにあるアプリケーションのアプリケーション制御モニタリングを有効化する。すべてのアプリケーショントラフィックを許可する。

FortiGuard Application Control Database との比較を通してアプリケーションが識別されると、そのアプリケーション制御リストにおいて定義されたポリシーが適用されます。ブロックされたアプリケーションからのトラフィックは遮断され、ネットワークバンド幅が節約されてそのトラフィックのさらなる検査が回避されます。その後、FortiOS が提供する追加的な統合脅威管理(UTM)セキュリティ機能(たとえば、不正侵入防止、アンチウイルス/アンチスパイウェアスキャンニング、情報漏洩防止)を残りのネットワークトラフィックに適用できます。

エンドユーザーとアプリケーションの関連付け

FortiOS は、エンドユーザーをユーザーグループのポリシーと関連付けするために Fortinet Server Authentication Extension (FSAE) を提供し、シングルサインオン機能とアプリケーション制御機能を有効化します。FSAE はユーザーのログインを監視し、そのユーザー名、IP アドレス、Active Directory ユーザーグループメンバーシップのリストを FortiGate 統合型セキュリティアプライアンスに転送します。そのユーザーがネットワークリソースにアクセスを試みると、FortiGate は、要求された宛先またはアプリケーションのための適切なファイアウォールポリシーを適用し、ユーザーが認められたユーザーグループの 1 つに属する場合のみ、その接続を許可します。FSAE は、Windows NTLM 認証および Novell eDirectory を使ってネットワーク上のユーザーを識別することもできます。

アプリケーション制御の粒度

ホワイトリストおよびブラックリストは、同一のポリシーを使ってより粒度の細かい制御を実現できます。Fortinet Application Control は、1つのソーシャルネットワークサイトから利用可能な複数のアプリケーションを区別することも可能です。たとえば、ポリシーを識別して、個別に Facebook Chat および Facebook Video からのアプリケーショントラフィックに適用できます。同様に、Fortinet Application Control は、別々のポリシーを 18 の Google 関連アプリケーション(グーグル検索、グーグルマップ、グーグルビデオなど)に適用することができます。これに加え、トラフィックシェーピングを有効化して、一部のアプリケーションに利用可能なネットワークバンド幅を制限したり、他のアプリケーションに優先権を与えたりすることができます。



図 3: 人気のあるアプリケーションの一部

アプリケーショントラフィックの把握

アプリケーショントラフィックの把握によって、ネットワーク管理者はアプリケーションリストエントリで規定されたすべてのアプリケーションまたは個々のアプリケーションが利用可能なネットワークバンド幅を制限したり、保証したりすることができます。たとえば、あるビジネスで、Skype や Facebook チャットで使用されるバンド幅を 1 秒当たりわずか 100 キロバイトにまで制限したり、YouTube のトラフィックを制限してミッションクリティカルなアプリケーションのためにネットワークバンド幅を取っておくことができます。また、トラフィックシェーピングは時間を制限する形で構成することもできます。1 日の特定の時間帯においてユーザーアクセスや、アプリケーションが利用可能なバンド幅を制限します。トラフィックシェーピングポリシーは、管理者が複数のポリシーおよびリストエントリにおいて再利用できるように、ファイアウォールポリシーおよびアプリケーション制御リストとは別に、個別に作成されます。共有されているトラフィックシェーピングポリシーは、個々のファイアウォールまたはすべてのファイアウォールを横断して適用できます。

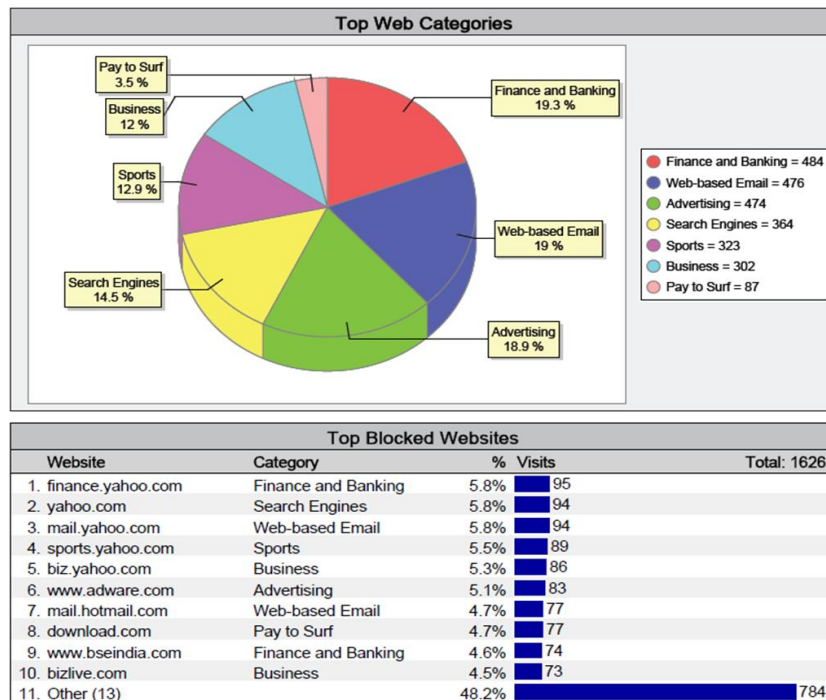


図 4: Web アプリケーション使用レポート

アプリケーションモニタリング/レポーティング

アプリケーションモニタリング/レポーティング機能は、アプリケーションのトラフィック情報を収集し、視覚的なトレンドチャートを使ってその情報を表示します。これによって、管理者はネットワーク上のアプリケーションの使用状況をすばやく把握できます。管理者は、多様なタイプのチャートのために、データをコンパイルすることを選択することもできます。たとえば、上位 Web カテゴリ、上位ブロック対象 Web サイト、上位 10 のバンド幅別アプリケーション、上位 10 のバンド幅別メディアユーザー、ブラウジング時間別上位ユーザーなどがあります。アプリケーションモニタリングが有効化されている各ファイアウォールポリシーのために、トレンドチャートは生成されます。アプリケーショントレンドチャートから得られた知識を使って、ネットワーク管理者は、組織のセキュリティポリシー、作業者のニーズを踏まえた上で、アプリケーション使用を迅速に最適化することができます。

アプリケーション制御のパケットロギング

Fortinet Application Control のパケットロギングは、アプリケーションによって生成されたネットワークパケットをさらなる分析のために保存する機能です。たとえば、フォレンジック調査、誤検出の識別といった分析があります。FortiGate 統合型セキュリティアプライアンスは、そのパケットを格納したり、そのパケットを FortiAnalyzer アプライアンス、さらには FortiGuard Analysis Management Service (FAMS) に転送することができます。

エンドポイントにおけるアプリケーション制御

FortiClient™ Endpoint Security および FortiMobile™ Smartphone Security は、企業のコンピューターシステムおよびモバイルデバイスにセキュリティ機能を提供することを目的とした、クライアントベースのソフトウェアソリューションです。FortiGate アプライアンスと接続されて使用されるか、または独立型のソリューションとして使用される場合に、これらはネットワークエンドポイントのために包括的な脅威プロテクションスイートを提供します。ネットワーク管理者は、FortiGate 統合型セキュリティゲートウェイで、アプリケーション制御リストを作成して配備し、Fortinet Endpoint Security プロファイルに適用できます。そのリストは、ゲートウェイおよびエンドポイントにおいて、どのアプリケーションを許可、監視、またはブロックするかを判断するものです。利用可能なカテゴリ、ベンダー、アプリケーションのリストは、FortiGuard シグネチャデータベースに送信されます。さらに、エンドポイントにおけるアプリケーションの使用を個人ファイアウォールで制御することができます。

オンラインリソース

フォーティネットは、複数のオンラインリソースを提供して Fortinet Application Control を補完しています。FortiGuard Application Control List は、FortiGuard Application Control Database にリスト化されたすべてのアプリケーションに関する詳細を提供しています。FortiGuard Application Control Site は、フォーティネットのお客様が現在使用している上位 10 のアプリケーションのリストを掲載しています。これに加え、お客様は Application Control Submission Form を記入することで、新しいアプリケーション制御シグネチャおよびアップデートを簡単にリクエストすることができます。

Fortinet Application Control および FortiGuard Application Control データベースに関する詳細は、以下のリンクをクリックしてください。

<http://www.fortiguard.com/applicationcontrol/appcontrol.html>

結論

企業はもはや、自社のネットワーク環境におけるインターネットベースのアプリケーションの使用を見ないふりをしていくことはできません。従業員、パートナー、コントラクターは、接続状態および生産性を維持するために、アプリケーションへのアクセスを今後も要求するでしょう。これらは一方で、ネットワークトラフィックや脅威レベルを上昇させる可能性があります。

インターネットベースのアプリケーショントラフィックに組み込まれた脅威を発見したり、ソーシャルメディアアプリケーションの不適切な使用に起因する情報漏洩を防ぐには、完全なコンテンツプロテクション(アプリケーションの検知、可視化、制御を含む)を提供するセキュリティソリューションが必要です。これに加え、脅威が発見された場合にこれらの脅威を軽減して、完全なプロテクションと脅威除去を提供するには、コンテンツベースのセキュリティ実行が不可欠です。FortiOS は、Fortinet Application Control が FortiOS UTM 機能(不正侵入防止、アンチウイルス/アンチスパイウェア保護、情報漏洩防止など)に結合されている場合に、これらの複数レベルの脅威プロテクションを提供します。

フォーティネットについて

フォーティネットは、統合脅威管理のほか、今日の高度な脅威をブロックする専門的なセキュリティソリューションを提供しています。フォーティネットの統合化されたアーキテクチャにより、お客様は 1 台のアプライアンスデバイスに完全に統合されたセキュリティテクノロジーを配備して、パフォーマンスの向上、プロテクションの強化、コストの削減を実現できます。フォーティネットのセキュリティハードウェアおよびソフトウェアは、絶えず進化する脅威環境をお客様が常に把握するために必要な高性能で完全なコンテンツプロテクションを提供します。当社のお客様は、世界のあらゆる業界およびあらゆる地域において常に進化している自社ネットワークを保護するために、フォーティネットを信頼しています。さらに、セキュリティに対する自社の姿勢を改善し、セキュリティインフラストラクチャを簡素化して、総所有コストを削減する、堅牢で徹底的に防衛するための戦略を配備しています。

FortiOS について

FortiOS は、ネットワークセキュリティのための専用オペレーティングシステムであり、FortiGate 複合脅威セキュリティプラットフォームのソフトウェア基盤です。FortiOS ソフトウェアは、FortiASIC™ のコンテンツプロセッサおよびネットワークプロセッサが提供するハードウェアアクセラレーションを活用することで、高性能な複合脅威セキュリティを実現します。このカスタムハードウェアおよびカスタムソフトウェアの組み合わせにより、最善のセキュリティおよびパフォーマンスを 1 台のデバイスを通して確保できます。FortiOS は、FortiGuard® Security Subscription Services 経由で提供される、専門家による脅威情報を用いて、今日のネットワークが直面する最新、最先端で、日々巧妙化する脅威を阻止します。

FortiOS 4.0 ソフトウェアは、FortiGate 複合脅威セキュリティプラットフォーム内で統合化されたセキュリティ機能およびネットワーク機能の範囲を拡張することで、ネットワークセキュリティを再定義します。組織の規模にかかわらず、企業は、包括的なセキュリティサービス/ネットワークサービススイートから利益を得ることができます。



フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木7-18-18 住友不動産六本木通ビル8階
TEL:03-6434-8531 / 8533 FAX:03-6434-8532

購入前のご相談: <http://www.fortinet.co.jp/contact>

※記載された社名、各製品名は各社の登録商標または商標です。
※記載された内容は、変更する場合がありますのでご了承ください。

お問い合わせ

Copyright© 2011 Fortinet, Inc. All rights reserved. この文書のいかなる部分も、いかなる方法によっても複製、または電子媒体に複写することを禁じます。この文書に記載されている仕様は、予告なしに変更されることがあります。この文書に含まれている情報の正確性および信頼性には万全を期しておりますが、Fortinet, Inc. は、いかなる利用についても一切の責任を負わないものとします。Fortinet®, FortiGate®, および FortiGuard® は Fortinet, Inc. の登録商標です。その他本書に記載されているフォーティネット製品はフォーティネットの商標です。その他の製品または社名は各社の商標です。

WP-APPCONTROL-201103