働き方の進化に合わせたセキュリティの再考

今、多くの組織のIT部門が、本社やブランチオフィス、自宅など、あらゆる場所で働くようになった従業員を保護する必要に迫られています。しかし、状況に対応するためにVPNを用い従業員をリモートワークに移行させた結果、クラウドアプリにダイレクト接続するユーザが増加し、セキュリティポリシーやコントロールが回避されてしまう例が増えています。サイバー犯罪者もこの事実に注目し、増え続けるリモートワークの従業員が攻撃の標的にされています。

これらの要因によって、さらに大きなリスクにさらされるようになった企業は、セキュリティの課題をすべて解決できる、シンプルで効果的なソリューションを求めています。

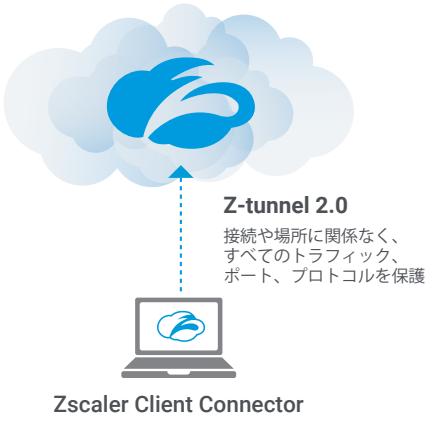
強力で柔軟なZscaler Internet Access（ZIA）の機能を活用することで、ビジネスの場所や方法に関係なく、進化する従業員を完全に保護できます。クラウドファイアウォール、クラウドサンドボックス、クラウドDLPがユーザ接続を追従するため、IT部門は、リスクを増大させることなく、高速のダイレクトインターネット接続を提供できます。侵害や漏洩に対して鉄壁の保護を可能にしつつ、あらゆる場所で働ける環境がユーザに提供されるほか、これらすべてを従来のアプローチよりはるかに少ないコストで実現することが可能です。

ユーザは、あらゆる場所で働ける柔軟な環境を求めています。問題は、ユーザがネットワークを離れてポリシーを回避するようになると、それらのユーザを標的にする脅威が増加することです。ネットワークとセキュリティに、実際の価値以上のコストを要する現状の問題を解決するには、より良いアプローチを採用する必要があります。

WFA（Work From Anywhere）の従業員を保護する方法

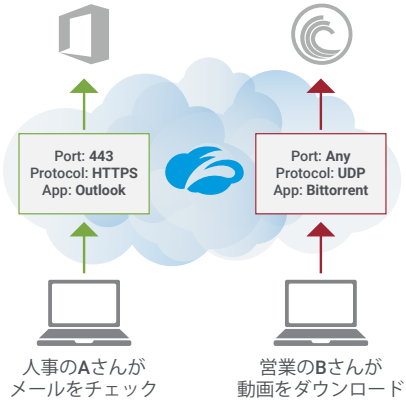
Zscaler Client ConnectorとZ-tunnel 2.0によるアプローチ

まず必要となるのはZscaler Client Connector（旧Zscaler App）の導入です。ユーザのデバイスがインターネットに接続する前に、Client Connectorがゼットスケーラーのクラウドへのセキュアな接続を確立します。ゼットスケーラーの新しいZ-Tunnel 2.0アーキテクチャを活用することで、すべてのトラフィック、ポート、プロトコルがインスペクションされます。Client Connectorは、高速かつ安全なユーザ接続をあらゆる場所に提供するためのビルディングブロックです。



オフネットワーク接続をAdvanced Cloud Firewallでコントロールする

ユーザがオフネットワークである場合も、会社のポリシーがユーザを追従する必要があります。Advanced Cloud Firewallを導入し、Advanced Cloud FirewallとZ-Tunnel 2.0を連携させることで、VPN、バックホール、高価なアプライアンスを必要とすることなく、ユーザの接続を完全にコントロールして保護し、リスクを軽減できます。ゼットスケーラーのAdvanced Cloud Firewallは、BitTorrentのブロックはもちろん、FTP、RDP、またはSIPの接続のコントロールによるRing CentralやZoomなどのユーザグループアクセスの定義までのすべてに対応します。また、一貫性のある単一ポリシーを、ユーザが接続する場所に関係なく活用できます。



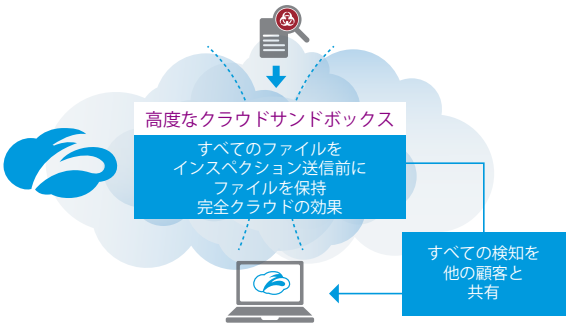
クラウドファイアウォールで会社のポリシーをオフネットワークに適用

「多くのP2Pトラフィックが我々のネットワークに到達し、実態が不明なクライアントへと送られていることが分かりました。ゼットスケーラーの完全なパケットインスペクションファイアウォールを使用することで、それらのP2Pトラフィックをオフにでき、BitTorrentやその他のP2Pファイル共有サービスを停止することができました」

AutoNation
セキュリティオペレーションズ担当ディレクタ
Jeff Johnson氏

Advanced Cloud Sandboxによるリモートユーザのリスクの軽減

ユーザがオフネットワークに移行し、ゲートウェイから離れると、脆弱性が最も高くなります。ランサムウェアや、未知の不正ファイルは、警戒を怠ったユーザを攻撃します。そのため、Advanced Cloud SandboxとZIAプロキシアーキテクチャが必要になります。インラインのゼロデイ保護ですべてのユーザを保護し、未知のファイルについては、無害であると確認されるまで配信を保留にできます。ユーザにダウンロードを許可するすべてのファイルタイプに対応しており、ゼットスケーラーを利用する他の組織からの強力な脅威インテリジェンスも活用できます。さらには、無制限のSSLインスペクションによって、トラフィックのすべてのバイトのインスペクションを実行し、さまざまな場所に隠れる脅威を発見します。



「NOVでは、ゼットスケーラーとクラウドサンドボックスの導入後に、感染マシンが35分の1に減少しました」

あらゆる場所のデータの持ち出しをクラウドDLPでコントロール

ユーザがネットワークを離れても、ユーザが機密データを扱わなくなるとは言い切れません。ゼットスケーラーのクラウドDLPを利用することで、ユーザの接続先に関係なく、機密データの意図的な、あるいは意図的ではない損失を防止できます。完全なSSLインスペクションによって、暗号化されたトラフィックの死角が解消され、コンプライアンス作業の可視性が向上します。さらには、ゼットスケーラーのExact Data Match (EDM) で個人識別情報 (PII) をフィンガープリンティングして照合することで、機密情報の漏洩を防止できます。

すべての接続、SSLの内側の
すべての機密データを保護

「設定不要ですぐに利用できる
DLPディクショナリーは、とても分かりやすく、
これこそが我々の必要としていたものであると
実感しました。ユーザグループへの展開は
極めて容易で、わずかな作業でDLPを
完全に導入できました」

Steptoe & Johnson LLP
情報セキュリティ担当ディレクタ
Brad Moldenhauer氏

まとめ

最近報道されている多くのニュースからも分かるように、本社以外の場所で働く従業員も含め、さまざまな可能性を考慮し、対策を講じる必要があります。つまり、セキュリティポリシーやコントロールも、オフィスから離れた場所へ移動させることが求められているのです。必要なのは、ユーザエクスペリエンスを低下させることなく、あらゆる場所で働く従業員と従業員がアクセスするアプリケーションを保護する新しい方法です。

ゼットスケーラーが提供するソリューションによって、数千もの組織がこの新しいWFA (Work From Anywhere) への移行を成功させてきました。WFAに必要な柔軟性を長期にわたって実現し、働きやすい環境を従業員に提供する方法について、ぜひ弊社からご提案させてください。お問い合わせは**こちらから**。

ゼットスケーラーについて

ゼットスケーラーは、世界をリードする多くの組織を支援し、ネットワークとアプリケーションのトランスフォーメーションによるモバイルとクラウドファーストの環境の実現に貢献しています。代表的なサービスである、Zscaler Internet AccessとZscaler Private Accessは、デバイス、場所、あるいはネットワークに関係なく、ユーザとアプリケーションの高速かつ安全な接続を可能にします。ゼットスケーラーのサービスは100%クラウドで提供されるため、従来型のアプライアンスやハイブリッドソリューションでは実現できないシンプルさと強力なセキュリティを提供し、ユーザエクスペリエンスの向上を可能にします。185か国以上で使用されているゼットスケーラーは、マルチテナントの分散型クラウドセキュリティプラットフォームを運用することで、サイバー攻撃やデータ損失から数千の顧客を保護しています。詳細はzscaler.jpをご確認ください。

ゼットスケーラー株式会社
東京都千代田区大手町1-9-2
大手町フィナンシャルシティ
グランキューブ3階
www.zscaler.jp