POINT OF VIEW

ハイブリッドで ハイパースケールな データセンターの保護

組織では、コンポーザブルでスケーラブルなアーキテクチャから成るハイブリッドデータセンターが構築されています。こうしたハイブリッド設計により、分散した拠点、キャンパス、オンプレミスのデータセンターが、複数のクラウドに展開されたさまざまな重要サービスをホストするデータセンターと相互接続されるようになります。こうしたハイブリッドのアプローチにより、ビジネスクリティカルなアプリケーションをクラウドに展開し、オンプレミスのデータセンターで他のアプリケーションやデータを管理してコンプライアンスや制御を確保することで、運用のアジリティを向上させることができます。この分散型のモデルは、従業員の要求の変化にも適切に対応し、時間や場所を問わず、すべてのアプリケーションへのアクセスを向上させることができます。しかし、こうしたクラウドモデルにおいても、従業員、顧客、パートナーが利用するクラウドに移行できないアプリケーション、データ、ワークロードを保護するために、オンプレミスの企業データセンター[1]が不可欠であることを忘れてはなりません。

データセンターインフラストラクチャの進化に伴い、ハイパースケールアーキテクチャを採用して最適なユーザーエクスペリエンスの要求を満たしつつ、今までにないパフォーマンス、拡張性、容量を提供する企業が増えています。

しかし、ハイブリッドデータセンターモデル全体でハイパースケールやハイパーパフォーマンスを採用することで、セキュリティ関連の問題が発生し、ユーザーエクスペリエンス、パフォーマンス、拡張性に悪影響を及ぼす可能性があります。従来のセキュリティソリューションでは、ハイブリッドデータセンターのパフォーマンスや拡張性の要件に対応するのは困難です。組織は、データやアプリケーションのパフォーマンスを高速化するか、従来のセキュリティツールで環境を保護するためにコストをかけるかの選択に迫られています。セキュリティは簡単にボトルネックとなってしまいます。多くの場合、競争力を維持するとなると、高パフォーマンスが優先されます。しかし、その結果生じるセキュリティの低下は、ランサムウェアなどの攻撃を招く大きな要因となり、ビジネスの中断、金銭的損失、ブランドや評判への長期的な損害を招くおそれがあります。

組織は、データセンターのセキュリティ戦略を見直す必要があります。まず、ハイブリッドやハイパースケールの傾向によってチームが直面する主要な問題を把握し、ハイブリッド / ハイパースケールデータセンターに適した以下のようなセキュリティを提供できるプロバイダーを評価します：

- **アプリケーションアクセス制御：**組織が、時間や場所を問わずアプリケーションを使用するフルタイムのハイブリッドワーカーを採用した場合、2 つのことが明らかになります。1 つ目は、ローカルまたはクラウドベースのアプリケーションへのアクセスで使用するリモートアクセス VPN（仮想プライベートネットワーク）が、過度の信頼をもたらしてしまうことです。2 つ目は、クラウドで使用するアプリケーションでは、トラフィックが詳細調査によりオンプレミスのデータセンターに差し戻されない限り、セキュリティがほとんど機能しないということです。

- **限定的な可視性：**場所に縛られない働き方への移行に伴い、組織はハイブリッドデータセンターを採用して運用のアジリティを向上させています。これを行うには、複数のクラウドにリソースを展開しながら、他のビジネスクリティカルなアプリケーションやデータをオンプレミスのデータセンターに保管し、コンプライアンスや制御に対応する必要があります。しかし、データセンターインフラストラクチャの分散が進むほど、攻撃対象領域が拡大してしまいます。その結果、盲点が増え、可視性が低下し、侵害や攻撃の可能性が高まります。重大な盲点の1つは、アプリケーションや他のトランザクションを暗号化したものです。組織は、暗号化されたフローをインスペクションして、特に安全なチャネルに潜むマルウェアをはじめ、あらゆるタイプの攻撃を検出する必要があります。そうすることで、ランサムウェアをはじめ、HTTPS（ハイパーテキスト トランスファー プロトコル セキュア）ビーコンを介して確立されたコマンド & コントロールセッションの中断により、顧客や企業のデータが盗まれるのを防ぐことができます。しかし、多くの場合において、従来のファイアウォールは暗号化されたデータをインスペクションすることがネックとなり、アプリケーションのパフォーマンスやユーザーエクスペリエンスの大幅な低下を招いてしまいます。
- **脆弱なアプリケーションの保護：**スタンドアロン IPS デバイスを使用するのではなく、侵入防止システム（IPS）機能を次世代ファイアウォール（NGFW）ソリューションに統合した場合、パフォーマンスの低下やパッチ管理の問題が発生する可能性があります。しかし、スタンドアロン IPS を使用した場合、運用や所有のコストが、多くの組織にとって非常に高額になります。これは、二者択一にすべきではありません。
- **ハイパースケールパフォーマンス：**エレファントフロー、エッジコンピューティング、高精細度テレビジョン（HDTV）や他のリッチメディアトラフィックの保護、5G ネットワーク、動的コアセグメンテーションなど、新たな高パフォーマンスのイノベーションでは、NGFW などのソリューションにおいて今までにないパフォーマンスレベルが求められます。しかし、ほとんどの NGFW の設計ではそこまでのレベルのパフォーマンスが想定されていないため、莫大な費用をかけなければソリューションによっては将来どころか現在の需要を満たすことさえできません。そして多くの場合、未だ費用をかけられずにいます。
- **全体的な管理の複雑さ：**シンプルな一元管理ができなければ、大規模な自動化やオーケストレーションは、多様なハイブリッド IT 環境では特に困難です。しかし、これを行わなければ同時進行ができなくなり、適用されるポリシーに一貫性がなくなり、可視性や制御が乱れ、セキュリティの欠陥が生じ、常に悪用され得る状況になります。

適切な問題を解決

ネットワーキングとセキュリティの管理者たちは、やるべきことが山ほどあります。データセンターの進化（ハイブリッドデータセンター環境のセキュリティ確保の問題は言うまでもありません）は、問題も多方面に及ぶため、扱いにくい議論だと思うことでしょう。

しかし、ハイブリッドでハイパースケールなデータセンターのセキュリティは、非常に身近なものとなっています。ソリューションをリサーチするにあたり、次の優先事項を評価する必要があります。

シームレスなユーザーエクスペリエンスを実現するための制御

まず、アプリケーションやリソースにアクセスできる人間と、その目的を判断します。ゼロトラストネットワークアクセス（ZTNA）では、ユーザー、場所、デバイスを常に認証し、ポリシーに基づいてリソースへのアクセスのみを許可することで、これを実現することができます。従来の VPN テクノロジーは絶対的な信頼を置きすぎてしまうことが最大のネックでしたが、このアプローチでは、その傾向を抑えることができます。ユーザーからアプリケーションへのマッピングを作成し、NGFW などのセキュリティツールで使用したり実行したりできるようになれば、完全なコンプライアンス管理を適切に行いながら、一貫したエンドツーエンドのセキュリティが実現します。

包括的な可視性を活用して、より優れた制御を実現

従来のセキュリティの展開は、ほとんどが盲点だらけです。しかし、あきらめる必要はありません。HTTPS などの暗号化されたフローを完全に可視化することで、組織は隠れた脅威を迅速に特定して阻止できるようになります。高度なツールを使用することで、ランサムウェア、機密データの盗難や破損、その他の高度な脅威など、さまざまなネットワーク、アプリケーション、ファイルを中心とした攻撃を積極的に防止できるようになります。エンドツーエンドで一貫したセキュリティを提供することで、ネットワークインフラストラクチャ全体を保護し、ネットワークやビジネスの運用を継続的に維持します。さらにネットワークセグメンテーションなどのツールを使用すれば、攻撃対象領域がさらに縮小し、脅威が水平方向に広がるのを防ぎ、アプリケーションやトランザクションのコンプライアンス（データガバナンス）を向上させることができます。

重要性が高く、パッチの適用が困難なレガシーシステムをコンピューター上で最新の状態に維持

セキュリティ侵害の 60% は、パッチ管理が何かしら不十分であったことが明らかになっています[2]。また、脆弱性の悪用やその他のパッチ関連の問題が発生する可能性は、主にレガシーシステムや古いインフラストラクチャを多用する大企業で高くなります。脆弱性があり、パッチ適用が困難なレガシーアプリケーションを保護するために IPS を使用する場合、IPS テクノロジーが、「ホットパッチ適用」などのパッチ管理において重要な役割を果たします。また、スタンドアロンソリューションとしてではなく、両方のシステムを実行するのに十分なパフォーマンス力を備えたネットワークファイアウォールに統合される場合も同様です。IT チームは、さまざまなネットワークおよびセキュリティ運用グループ間の制御を維持しながら、コストや複雑さを軽減できるようになります。(実際のところ、きめ細かい統合により、ラックスペースの削減やデータセンターの電力や冷却のコスト削減など、総所有コスト（TCO）の削減が可能になります)。

自動化を促進

ネットワーキングおよびセキュリティのリーダーは、今現在でも、手動による操作やツールの過剰な使用に依存していますが、これらを管理できるセキュリティ経験豊富なスタッフが不足しています。これは、ネットワークオペレーションセンター（NOC）やセキュリティオペレーションセンター（SOC）の両方における従来からの問題です。ハイブリッドデータセンター環境を効果的に管理するには、導入されているポイント製品の数を統合するだけでなく、自動化も活用することで運用の複雑さを軽減し、効率を向上させる必要があります。特に機械学習（ML）や人工知能（AI）といった自動化により、全体的なサイバースキルの不足を補い、大きくなりすぎた人員の負担を軽減することができるようになります。多くの場合、効果的な AI ベースのソリューションでは、人的ミスもなく、十数人以上のセキュリティアナリストが行う作業をわずかな時間で実行することができます。

ハイパースケールアーキテクチャだけでなく、ハイパースケールセキュリティも提供

組織は、セキュリティとパフォーマンスの兼ね合いを考慮する必要はありません。しかし、多くの組織において、たいていのハイパースケールデータセンターを出入りするトラフィック（南北のトラフィック）や、データセンター間を行き来するトラフィック（東西のトラフィック）にとってセキュリティは難所になっています。これは、ユーザーエクスペリエンスに悪影響を与え、全体的な生産性を低下させ、競争力と収益に影響を与える可能性があります。ネットワーク管理者は、処理速度が上がるようにセキュリティ対策を緩める必要に迫られる可能性もあります。しかし、十分なセキュリティを確保せずに、すべてのトラフィックが組織のネットワークを自由に出入りするようになると、攻撃や機能停止のリスクが劇的に高まります。

組織では、ハイパースケールアーキテクチャに適合するハイパースケールセキュリティが必要です。これは、複数の NGFW を繋いでハイパースケールセキュリティを「実装」するという面倒で、管理が大変で、不必要にコストがかかる疑わしいやり方を回避することにもなります。こうした戦略は、昨今のハイパーパフォーマンス要件に対応するツールの開発に失敗したメーカーによりもたらされており、こうしたメーカーは今現在も市販のプロセッサーに依存しています。暗号化トラフィックや集中的なインスペクションおよび分析によるプロセッサーの負担で立ちゆかなくなってしまうのは、これが原因です。他のあらゆる業界では、特化型の処理を最適化できる専用の ASIC（特定用途向け集積回路）を開発しています。テレビやコンピューターグラフィックス、スマートフォン、クラウドプラットフォーム、データセンターサーバーおよびスイッチ、さらにスマートカーさえも、すべて専用のカスタムプロセッサのテクノロジーを基盤にして、特化した機能を提供しており、セキュリティも同じであるべきです。

今後なすべきこと

ハイブリッドデータセンター環境のサポートをはじめ、e コマースアプリケーションのアクセス提供、分散型のサイト間での大量データファイルのスピーディな共有、災害復旧サイトの構築に至るまで、時代はハイパースケールです。これにより、ユーザーアクセスが高速化し、モバイルネットワーク事業者による 4G から 5G への移行が促進され、ワイヤレスデバイスでのブロードバンドインターネット配信が可能になります。それだけではありません。すべてにおいて拡大化、高速化、分散化が驚異的なスピードで進んでいます。

その結果、ハイパースケールセキュリティが求められています。ハイパースケールの生産性にまだ対応していない企業でも、ハイブリッドモデルの柔軟性とパフォーマンスの利点を活用できるように、今後はハイブリッドデータセンターアーキテクチャに適したセキュリティを実装することが求められます。

同時に、データセンターコアやあらゆるネットワークエッジを標的とした高度な脅威が衰えることはありません。セキュリティ、ネットワークエンジニアリング、DevOps チーム、オペレーションリーダーは、ネットワークの各部分から一歩離れて、全体像を見て問題の内容を把握する必要があります。また、データセンターは組織の中心であるため、ハイブリッドデータセンターのパフォーマンス、帯域幅、セキュリティのニーズに対応することから始める必要があります。さもないと、自動化された組織的なセキュリティ戦略が提供する保護を維持しながら、分散した従業員やグローバル市場をサポートすることはできません。

これには、一貫したエンドツーエンドのセキュリティや最適なユーザーエクスペリエンスを確保できるように、最新のアーキテクチャのニーズを満たすことができるセキュリティソリューションを適宜検討することが求められます。まずは、ネットワークファイアウォール選びからです。どこにでも展開でき、無限に拡張でき、シームレスに相互運用でき、デジタルビジネスのスピードで実行できるものを選ぶ必要があります。

[1]「What is a Datacenter?」、フォーティネット（英語）：https://www.fortinet.com/resources/cyberglossary/data-center

[2]「Patch Management: Best Practices and Why It's Important」、John Emmitt 著、Security Boulevard、2021 年 3 月 9 日（英語）：https://securityboulevard.com/2021/03/patch-management-best-practices-and-why-its-important/

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ

POV-Hybrid-and-Hyperscale-Data-Centers-202204-R1