CHECKLIST

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で考慮すべき重要事項

ハイブリッドでハイパースケールなデータセンターを保護する最新アーキテクチャには、その速度に十分に対応できるセキュリティが必要です。しかしながら、今日の多くのデータセンター環境では、従来のネットワークセキュリティソリューション、特に時代遅れの従来型ファイアウォールのパフォーマンスや機能が不十分であるため、セキュリティとパフォーマンスの危ういトレードオフを強いられています。

最新のデータセンターインフラストラクチャのセキュリティ設計にあたり、すべての企業の IT 管理者が考慮すべき 5 つの重要事項を以下に示します。

☑ 可視化と制御

ハイパフォーマンスネットワークのセキュリティリスクを管理するには、攻撃対象領域をプロアクティブに減らす必要があり、そのためには、環境全体、エンドポイント、ネットワークセグメント、さらには、これらのセグメントを通過するトラフィック、アプリケーション、アクセスされるデータの完全な可視化と制御が不可欠です。データセンターネットワークに接続するあらゆるデバイスが潜在的な脅威ベクトルになります。しかしながら、最新のデータセンターには、従来のオンプレミスのデータセンターをはるかに超える、広範囲で強力なセキュリティが必要です。また、さまざまな環境（オンプレミス、コロケーション、クラウドなど）に導入されているセキュリティ要素に加えて、ユーザー、アプリケーション、デバイスすべてを可視化する機能も要求されます。さらには、ネットワークをリアルタイムで監視して高度な脅威をチェックし、防御する、侵入防止システム（IPS）も必要です。

☑ ゼロトラストの原則

特権アクセスと適応型のトラストに関するゼロトラストの原則では、ゼロトラストのモデルを採用し、データのすべてのトランザクション、移動、反復を疑うことを前提で処理します。ゼロトラストシステムを正しく実装することで、ユーザーやネットワークの振る舞い（ユーザー対ユーザー、ユーザー対マシン、マシン対マシン）やデータフローをリアルタイムで追跡し、例外あるいは異常な振る舞いが検知された場合に、アラートを送信したり、アカウントからのアクセスを取り消したりできるようになります。

☑ セグメント化

ネットワークトラフィックのセグメント化では、コントロールポイントの実装により、攻撃者のラテラルムーブメントやデータセンターの多くの場所に存在する脆弱性のエクスプロイトの可能性を低くします。これは、すべてのトラフィックを、アプリケーションやポートのレベルで、異なるセグメントに分類することを意味します。もちろん、ホストレベルやネットワークレベルでのセグメント化も可能です。セグメント化が正しく実装されることで、各セグメントが他のすべてのセグメントから分離されます。ネットワークのセグメント化は、多層防御の考え方を採用することで、セキュリティポリシーの適用を簡素化します。

☑ サービスデリバリに要する時間

現在の多くのデータセンターソリューションは、パフォーマンスの低さと遅延の大きさから、ハイパースケール時代に求められる時間、俊敏性、信頼性に耐え得るサービスを提供できません。サービスはセグメント化が不可欠であると同時に、膨大な物理 / 仮想両方の資産の相互運用にも対応する必要があります。最新のデータセンターファイアウォールは、VXLAN（Virtual Extensible LAN）のターミネーションと再オリジネーションを、ハードウェアを活用して加速させ、レイヤー 4 またはレイヤー 7 のセキュリティを動的にサポートできるものでなければなりません。わずかなダウンタイムやサービスデリバリの些細な問題であっても、収益、信頼、ブランドの評価に対する大きな損失を招く恐れがあります [1]。

☑ システム性能

大量のデータセットが 1 つの接続で転送される「エレファントフロー」で、多くのセキュリティインフラストラクチャは大きな負担を強いられます。しかしながら、ハイパースケール時代には、特に、製薬、e コマース、航空、金融証券などの分野ではエレファントフローが当たり前のように発生し、データセンター間やデータセンターと複数のクラウドの間で、高スループットのフローを使用して大規模なデータセットを安全に暗号化して転送する必要があります。ハイパースケールデータセンターのネットワークファイアウォールには、このようなレベルのパフォーマンスが常に求められます。

[1]「Downtime Can Cost a Company up to $67 Million Over Two Years, Threatening Brand Reputation」、Filip Truta 著、Security Boulevard、2019 年 2 月 21 日（英語）：https://securityboulevard.com/2019/02/downtime-can-cost-a-company-up-to-67-million-over-two-years-threatening-brand-reputation/

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

CL-critical-considerations-for-hybrid-and-hyperscale-202203-R1