Precryption™ で最大の死角をなくす

Gigamon Precryption テクノロジーにより、水平方向のトラフィックをプレーンテキストで可視化し、仮想、クラウド、コンテナを含むセキュリティスタック全体で活用できます。復号化の必要はありません。

第1

の IT セキュリティ責任者の懸念は、*存在さえ知らない死角を突かれることです*[2]

91%

の脅威が**暗号化されたチャネルを使用しています**[3]

81%

の組織が**昨年クラウドセキュリティインシデントを経験しています**[1]

5 倍

セキュリティ・ツールは、トラフィックが暗号化されていない場合**5 倍から 7 倍の効率を発揮できます**[4]

31%

のデータ侵害（昨年）がセキュリティ・ツールや監視ツールで検出されませんでした[2]

Gigamon Precryption™ テクノロジーは、仮想、クラウド、およびコンテナ化されたアプリケーションのセキュリティを再定義し、暗号化された通信をプレーンテキストで可視化することで、従来のように復号化のコストや手間をかけることなく、セキュリティスタック全体での活用を可能にします。

情報セキュリティの課題

1. クラウド導入の増加
2. 開発チームのスピードアップ
3. 隠された脅威活動

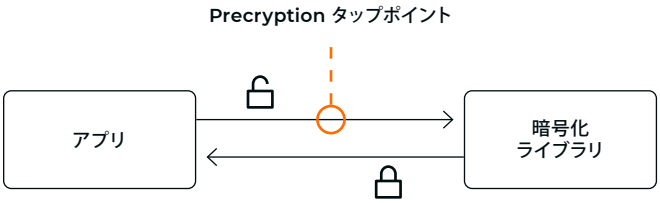
暗号化通信は、現代のハイブリッドクラウドインフラストラクチャ全体に遍在しており、機密データを従来の傍受技術から保護しています。脅威者は、より洗練された新しい侵入アプローチでこれに対応し、重要なシステムを侵害し、機密データにアクセスしています。これらの侵入者は現在、同じ暗号化された通信チャネルを使用して、自分たちの活動、特に水平方向の移動、機密データへのアクセス、流出を隠蔽しています。仮想ワークロード間を水平方向に移動する暗号化トラフィックをプレーンテキストで可視化することは、市場に出回っている既存のソリューションではほぼ不可能であり、隠された脅威活動を検知することはきわめて困難です。これが、暗号化された水泳方向の通信が最大のセキュリティの死角であり続ける理由です。

隠された脅威活動を検知する Precryption 技術

Prectyption 技術は、今日のハイブリッド・クラウド・インフラにおける最大の死角である、TLS 1.3 を含む最新の暗号化方式によって難読化された脅威社の水平方向の活動に、直接対処する革新的なソリューションです。Precryption は、費用のかかる復号化を実行したり、鍵の収集や管理に煩わされたりすることなく、効率的でフォームファクターへの負荷なく、暗号化された仮想通信をプレーンテキストで可視化します。

Prescription 技術の仕組み

Precryption 技術は、Linuxのネイティブ機能を活用して、アプリケーションと OpenSSL などの暗号化ライブラリとの間の通信をタップ（コピー）します。



このようにして、Precryption は、暗号化される前、あるいは復号化された後のネットワーク・トラフィックをプレーンテキストでキャプチャします。Precryption 機能は、メッセージの実際の暗号化やネットワーク上での送信を妨げることはありません。プロキシも、再送も、ブレーク&インスペクションも不要です。代わりに、このプレーンテキストのコピーはさらなる最適化、変換、複製、ツールへの配信のために Gigamon ディープ・オブザーバビリティ・パイプラインに転送されます。

Precryption テクノロジーは、GigaVUE® Universal Cloud Tap（UCT）上に構築され、オンプレミスおよび仮想プラットフォームを含むハイブリッドおよびマルチクラウド環境で動作します。

さらに、Precryption テクノロジーが組み込まれたUCTは、アプリケーションから独立して実行されるため、アプリケーション開発のライフサイクルに組み込む必要がありません。

主要なユースケース

サイバー犯罪の阻止：クラウドにおける水平方向の動きは、サイバー攻撃において特に顕著な死角です。一旦セキュリティの境界防御を通過されてしまうと、暗号化されたパケットは監視されなくなるため、脅威者はあらゆるトリックやテクニックを駆使して検知を逃れることができます。

TLS 1.3 準拠：暗号化されたトラフィックを可視化できないことを理由に、本来するべきTLS 1.3 の適用を遅らせている組織すらあります。また、復号化ソリューションを別途管理している組織もあります。

ゼロ・トラスト：効果的なゼロ・トラスト・アーキテクチャの重要な基盤は、パケットを見る能力、ネットワーク上のリソース間のすべての相互作用を検査する能力、そしてポリシーを適用する能力です。

ネットワーク由来のインテリジェンス：SIEM などのセキュリティ・ツールは、脅威をより的確に検知するために、メタデータの変換やエンリッチメントに依存することが多いです。

Gigamon Precryption を選ぶべき理由

Precryption テクノロジーによる GigaVUE Universal Cloud Tap は、最新のハイブリッド・クラウド・インフラに存在する死角を排除し、仮想、クラウド、コンテナ・プラットフォームの水平方向の可視性を実現する、軽量で低負荷なソリューションです。TLS 1.3 を含むすべての暗号化タイプを、復号鍵を管理・維持することなく、明瞭に可視化を提供します。これによりIT 組織は、コンプライアンスを管理しつつ非公開の通信を非公開のままにし、ゼロ・トラストに必要な基盤を構築し、セキュリティ・ツールの効率を 5 倍以上に高めることができます。

主な特徴

- **モダン暗号化**（完全前方秘匿性を備えた TLS 1.3、mTLS、TLS 1.2）**による通信のプレーンテキスト可視化**
- **レガシー暗号化**（TLS 1.2以前）**による通信のプレーンテキスト可視化**
- コンテナワークロード内でエージェントを実行することなく、**非侵入型のトラフィックアクセスを**実現
- 従来型のトラフィック復号化手法に伴う**高価なリソース消費の排除**
- 従来型のトラフィック復号化で必要だった**鍵管理の排除**
- 暗号タイプ、強度、バージョンに基づく**パフォーマンスへの影響は**ゼロ
- オンプレミス、仮想、コンテナ・プラットフォームを含む**ハイブリッドおよびマルチクラウド環境に対応**
- 脅威活動がプレーンテキストでセキュリティ・ツールに配信される一方で、ネットワーク全体では**非公開の通信を非公開のまま維持**
- **Gigamonディープ・オブザーバビリティ・パイプラインとの統合により、**最適化、変換、ブローカリングの全機能を実現

主なメリット

- ファイアウォールを通過しないトラフィックも含め、暗号化されたEast-West（水平方向）およびNorth-Westの通信の**死角をなくす**
- 独立した手法であるため、開発チームを煩わすことなく、**アプリケーション通信を監視**できる
- **セキュリティ・ツールの可視性を、**暗号化の種類に関係なく、すべての通信に拡大する
- 仮想環境全体で**最大限のトラフィック・タッピング効率を実現**
- セキュリティ・ツールは暗号化されていないデータだけを処理すれば良いので**パフォーマンスが5〜7倍向上する**
- ディープ・オブザーバビリティに立脚した**ゼロ・トラスト・アーキテクチャをサポート**
- 復号化されたトラフィックの管理において**プライバシーとコンプライアンスの遵守を維持**する

課題：詳細

IT 組織は、保護を委託されているシステムやデータを保護する上で、次の 3 つの重大な課題に直面しています。それは、仮想化およびクラウドの導入の増加、開発チームに求められる行動の迅速化、そして隠された脅威活動です。

1.バーチャルおよびクラウドの導入拡大

昨年、81% の組織がクラウド・セキュリティ・インシデントを経験しています[1]

オンプレミス、プライベートクラウド、パブリッククラウド、VM、コンテナのいずれであっても、仮想化システムへの移行は増加の一途をたどっており、その勢いが衰える兆しはほとんどありません。これらの最新のアーキテクチャは、運用上効率的に設計されており、境界防御に依存したセキュリティ・アーキテクチャの進化を大きく上回っています。水平方向の動きを検出するのは非常に困難です。リスクを認識した上で、暗号化された通信がハイブリッド・クラウド・インフラを流れることを許容する組織もあれば、ファイアウォールを追加導入することで仮想アーキテクチャを補強し、本来必要な効率をセキュリティのために犠牲にしている組織もあります。企業の大半が複数の仮想プラットフォームを持つようになれば、課題とリスクは増大します。

2.開発チームのスピードアップ

83 パーセントの組織が、IT チームとセキュリティ・チームの間で連帯責任制を採用しています[2]

ソフトウェア開発チームの主なインセンティブは、アプリケーションを開発して、収益の拡大に貢献したり、組織の時間とコストを節約したりすることです。納期を守るために急かされ続ける中、DevOps チームは中核機能に集中します。セキュリティにもある程度関心があるでしょうが、彼らは侵入防御の専門家ではなく、侵入される可能性のある脆弱性にただ気づかないことがあります。さらに、彼らはソフトウェアやシステムにセキュリティ・エージェントを導入することをためらうかもしれません。エージェントはテストを妨げ、ソフトウエア開発ライフサイクルに要する作業と時間を増やす可能性があるからです。

セキュリティ組織はこの問題にさまざまな方法で取り組んでいます。コンプライアンスのために厳しい練習を行い、すべてのコードにエージェントを強制する組織もあれば、セキュリティ担当者を開発チームに配属する組織もあれば、厳格なセキュリティ監視を行わずに、開発者に迅速に進めさせるしかない組織もあります。大半の組織では、少なくともある程度のセキュリティ責任を開発チームに負わせています。

3.隠された脅威活動

脅威の 91% が暗号化されたチャネルを使用[3]

暗号化された通信は、ある種の脅威を防ぐには最適ですが、別の脅威を作り出します。脅威者は、システムにアクセスすると、手始めにログを削除、無効化、修正するのが一般的です。そして、コマンド & コントロール・サーバーへの呼び出し、特権の昇格、水平方向の動き、データの秘密コピー、最終的にはデータの流出などが、すべて暗号化された通信を利用して行われます。

暗号化されたトラフィックに対しては、セキュリティ・ツールの効率が5〜7倍低くなる可能性があります[4]

一般的な暗号化方式は 2 つのカテゴリに分けられます。

- **モダン暗号化**。完全前方秘匿性（PFS）を使用し、傍受された通信のブレイク&インスペクション解読を防ぎます。傍受された暗号鍵はすべて一時的なものであり、アウトオフバンドでの解読には無価値だからです。モダン暗号化には、TLS 1.3、mTLS、および PFS をオプションで有効にした TLS 1.2 の一部のデプロイメントが含まれます。Gigamon の推定では、現在ネットワーク・トラフィックのおよそ 30 〜 40 パーセントがモダン暗号化を使用しており、この割合は今後も増え続けるでしょう。

- **レガシー暗号化**。PFSを使用せず、傍受した鍵で復号化できます。これには、TLS 1.2 や古いバージョンの TLS、SSL（Secure Sockets Layer）のデプロイメントが含まれます。

暗号化された通信でネットワークを監視できるセキュリティ・ツールは存在します。レガシー暗号化の場合、それらのツールは通常、トラフィックを自身で解読しようとします。この場合、復号化のための処理能力を満たすために多くのサーバーを必要とするので、コンピューティングコストが高く、かくパフォーマンスに大きな影響を与えます。さらに、基礎となる鍵ライブラリは継続的に更新されなければならず、鍵の管理も時間がかかり複雑です。しかし、これだけのことをしてもなお、レガシー暗号化にしか対応できず、モダン暗号化は無視されます。

モダン暗号化の場合、通信を「途中で」復号化することはできないため、これらのツールは異なるアプローチをとる必要があります。そのため、パケットヘッダ、パケットサイズ、パケット頻度、その他のシグネチャを機械学習アルゴリズムに送り込み、任意の通信のリスクを評価する手法が取られます。これは何もしないよりはましですが結果は芳しくなく、一部の組織は境界セキュリティを信頼してレガシー暗号化だけを監視したり、あるいはアプリケーションにモダン暗号化を禁止したりしています。どれも理想的なセキュリティ態勢とはいえません。

1,000 人以上の IT およびセキュリティ・リーダーを対象とした最近の調査では、データ侵害の 31% がセキュリティ・ツールや監視ツールで検出されなかったことが明らかになりました。

より良い解決策が必要です。

暗号化ソリューション：詳細

GigaVUE ユニバーサル・クラウド・タップ（UCT）は、Precryption テクノロジーを搭載し、暗号化された仮想およびコンテナ通信の死角をなくし、IT およびセキュリティ・リーダーがコントロールを取り戻すことを可能にします。

GigaVUE UCT は、Linux ネイティブのeBPF テクノロジーを活用した最新の仮想タップで、仮想環境での通信をミラーリングする最も効率的な方法として設計されています。UCTは暗号化されていないデータを取得し、それを効率的に Gigamon ディープ・オブザーバビリティ・パイプラインに提供します。そこで更なる最適化、変換、フィルタリング、ブローカリングが行われ、最終的に物理か仮想かを問わず、正しいデータが正しいツールに提供されます。

Gigamon Precryption テクノロジーは、GigaVUE UCT 上に構築され、Linux や OpenSSL などの暗号化ライブラリとシームレスに統合され、ネットワーク上で暗号化される前に、あるいはアプリケーションによってはネットワーク上で復号化された後に、仮想通信やコンテナ通信を取得します。

- ✓ ネットワーク通信に手が加えられることはなく、ネットワーク全体で暗号化されたままです。
- ✓ 高価な復号のための計算リソースは必要ありません。このように、Precryption テクノロジーは、モダン暗号化にもレガシー暗号化にも対応し、暗号のタイプ、強度、バージョンに影響されることはありません。
- ✓ アプリケーション・キーが公開されることもなく、アプリケーション・キー管理の煩わしさもなく、不自然な仮想ルートも必要ありません。
- ✓ Precryption 技術は、監視対象のアプリケーションから独立して実行されるため、アプリケーションのリソースやライフサイクル管理への影響がなく、アプリケーション内で障害を引き起こすことがありません。

Gigamon Precryption 技術の仕組み：シングルノード（図1）

1. アプリがメッセージを暗号化する必要がある場合、OpenSSL などの暗号化ライブラリを使用して実際の暗号化を行います。

2. GigaVUE Universal Cloud Tap (UCT)は、Precryption テクノロジーにより、ネットワーク上で暗号化される前にこのメッセージのコピーを取得します。

3. 暗号化されたメッセージは、暗号化されたままで受信アプリに送信されます。プロキシなし、再暗号化なし、再送信なし。

4. GigaVUE UCT は、必要に応じてパケットヘッダを作成し、トンネルでカプセル化し、ディープ・オブザーバビリティ・パイプラインで GigaVUE V シリーズに転送します。Gigamon はさらにデータを最適化し、変換し、ツールに配信します。更なる復号化は不要です。

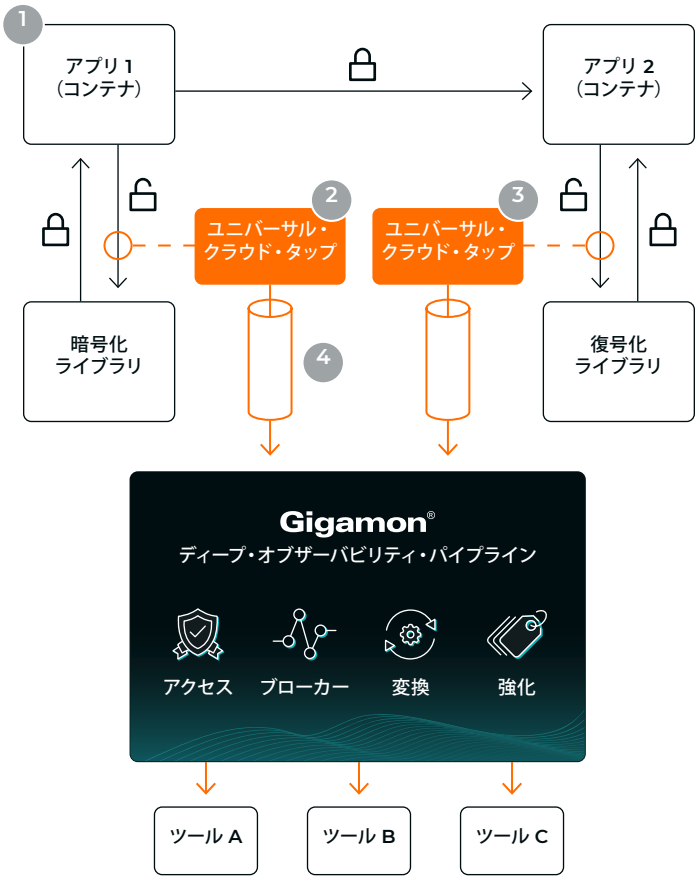


図 2

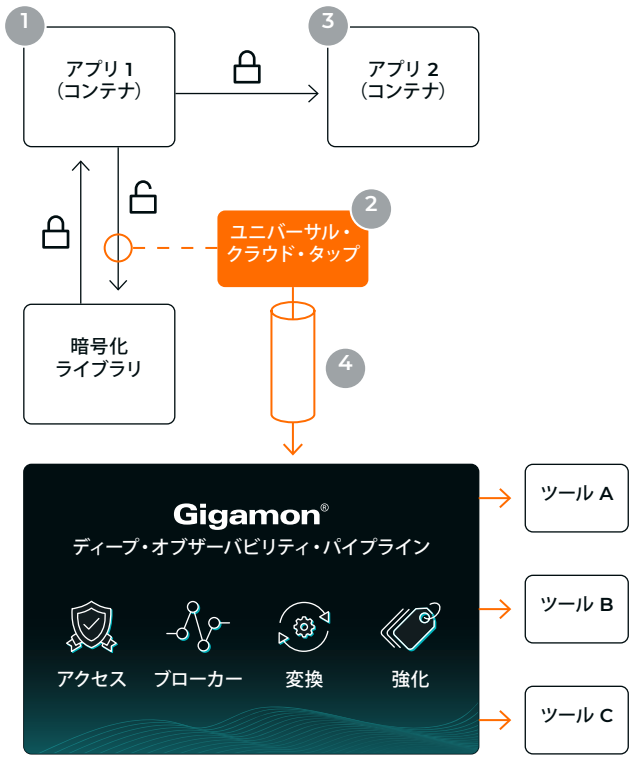


図 1

Gigamon Precryption 技術の仕組み：マルチノード （図2）

1. アプリがメッセージを暗号化する必要がある場合、OpenSSL などの暗号化ライブラリを使用して実際の暗号化を行います。

2. GigaVUE Universal Cloud Tap (UCT)は、Precryption テクノロジーにより、ネットワーク上で暗号化される前にこのメッセージのコピーを取得します。

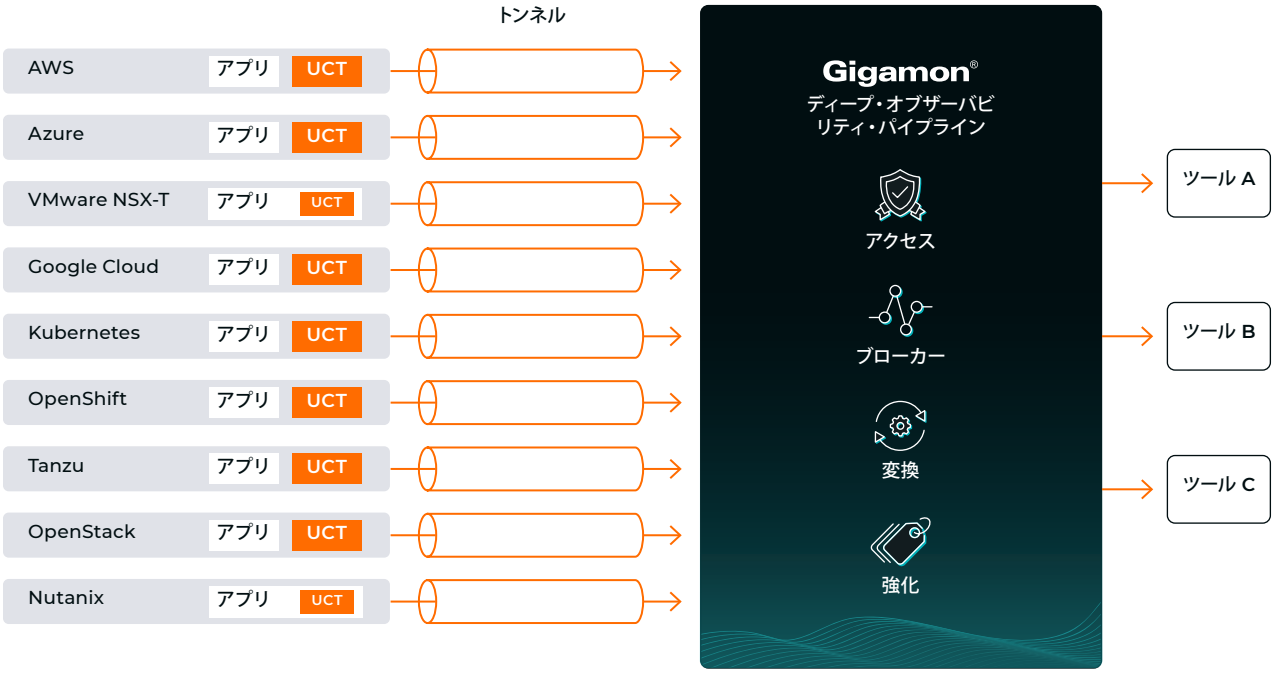
3. オプションとして、Precryption が有効化された GigaVUE UCT は、復号化後にサーバー側からメッセージのコピーを取得することもできます。

4. GigaVUE UCTは、必要に応じてパケットヘッダを作成し、トンネルでカプセル化し、ディープ・オブザーバビリティ・パイプラインで V シリーズに転送します。そこでさらに強化、変換され、改めて復号化する必要なくツールに配信されます。

マルチクラウドや大規模環境にも対応

GigaVUE UCT with Precryption technology は、VMware、AWS、Microsoft Azure、OpenStack、Google Cloud、Nutanix など、複数の仮想プラットフォームやクラウドプラットフォームで動作し、単一のグローバル管理インターフェイスで共通のデータパイプラインに供給します。

- ✓ 拡張を容易にするため、Kubernetes での自動デプロイにも対応しています
- ✓ すべてのクラウド環境で1つの共有ライセンスプール、無制限のインスタンス



GigaVUE UCT はアプリケーションから独立して動作します

「エージェント」という言葉は、文脈によって異なる意味を持つことがあります。典型的なエージェントと比較したUCT の利点を理解するために、次の比較表を検討してみましょう。

代表的なエージェント	GigaVUE UCT
X アプリケーションスペース/ポッド内で動作	✓ 独立したポッド内の独立したユーザー空間
X アプリケーションリソースの使用に影響	✓ 独立ノードリソース
X バージョンアップ管理が必要	✓ 独立したアップグレード
X アプリとともにテストが必要	✓ 独立したライフサイクル管理
X アプリの応答速度に影響する可能性がある	✓ アプリから独立したキャプチャ
X アプリに不安定性や、異常停止をもたらす可能性がある	✓ アプリから独立した故障領域

ネットワーク由来のインテリジェンスを追加し、開発スピードを維持したままセキュリティ態勢を改善する

暗号化されていないデータが抽出されると、Gigamon ディープ・オブザーバビリティ・パイプラインをさらに活用して、生の通信データをフローレベルのメタデータ・レコードに変換します。これにより誤検知を減らし、ポート・スプーフィングのような悪意のあるアクティビティを特定するのに役立ち、リアクティブ・フォレンジックではなくプロアクティブなリアルタイム・モニタリングによって脅威の検出を加速させることができます。このネットワーク由来のインテリジェンスは、ログの修正の影響を受けず、IoT やその他のエージェントレスデバイスに対応し、SecOps と DevOps の両チームが使用する監視ツールにデータを供給します。

機密性の高い環境では、UCT はオプションで、ディープ・オブザーバビリティ・パイプラインに送られるミラー通信を再暗号化したり、ツールに転送する前にクレジットカードや個人を特定できる情報（PII）のような機密データをマスクしたりすることもできます。

ユースケース

Precryption 技術を利用したサイバー犯罪の検知

ランサムウェア攻撃としても知られるサイバー攻撃は、通常、脅威者がフィッシングやその他のクレデンシャル・ハーベスティング手法によって、従業員のノートパソコンにネットワーク経由でアクセスすることから始まります。エンドポイント・セキュリティがこれを検知または防止してくれることを期待したいところですが、残念ながら、必ずしもそうなるとは限りません。

ネットワーク内部に侵入した脅威者は、ログを削除し、権限を昇格させ、より機密性の高いデータを持つホスト、アプリケーション、ワークロードなど、より興味深い他のネットワークリソースを探し出す高度なテクニックなど、多くのリソースを利用することができます。十分な時間と攻撃ベクトルがあれば、こうした他のネットワークリソースにも侵入できるでしょう。このテクニックはラテラルムーブメント(水平方向の移動)として知られています。

やがて脅威アクターは、データを暴露し、通信をスパイできるような、より興味深いアプリケーションに進出していくでしょう。脅威者は、ネットワーク内の自分たちがコントロール下におく場所にゆっくりとデータを吸い上げます。この吸い上げは、パフォーマンスに影響を与えたりアラームを作動させたりしないよう、慎重に行われます。十分なデータが揃い準備が整うと、最後に迅速かつ大規模なデータ漏洩を実行し、盗んだデータを外部にさらし、組織から金銭を脅し取ります。

このシナリオでは、脅威アクターによって行われる活動には大きく分けて 4 つの種類があります。

1. エンドポイント・セキュリティを迂回するための初期フィッシングやクレデンシャル・ハーベスティング
2. ネットワーク内での水平方向の動き
3. 機密データを投下場所へゆっくりと吸い上げる
4. 迅速なデータ漏洩イベント

ここでは、Gigamon Precryption テクノロジーを使用したプレーンテキスト可視化により、ツールがどのようにこのアクティビティを検出するかを紹介します。

	Precryption がない場合のセキュリティ・ツール	Precryption がある場合のセキュリティ・ツール
最初のフィッシング	正常な従業員のアクティビティ	正常な従業員のアクティビティ
水平方向の動き	無害なノイズ	既知の攻撃が展開され、サーバーへの侵入に成功
データ吸い上げ	無害なノイズ	重要データが不正な経路でアクセスされ、送信される
データ流出	大容量データ転送	盗まれたデータの詳細説明

サイバー犯罪シナリオの詳細については、インフォグラフィックをダウンロードしてください。

結論

暗号化されたトラフィックの可視化とメタデータを活用することで、ハイブリッド・クラウドのセキュリティ、モニタリング、トラブルシューティングが劇的に改善されます。Gigamon ディープ・オブザーバビリティ・パイプラインは、オンプレミスとパブリッククラウドの両方で、仮想およびコンテナ・トラフィックを監視するための最新のセキュリティ課題に直接対応します。GigaVUE UCT は、堅牢なプラットフォームサポートと単一の管理インターフェイスにより、クラウドの採用拡大に対応します。Gigamon のネットワーク由来のインテリジェンスは、DevOps、CloudOps、SecOps チームのセキュリティツールに高品質のメタデータを供給します。そして Gigamon の Precryption テクノロジーは、最新の暗号化を使用してクラウド上の隠されたアクティビティをどのように監視するかという特に厄介な問題に対処し、セキュリティ態勢を向上させ、悪者を寄せ付けないように設計されたエレガントで軽量な手法です。

Gigamon について

Gigamonは、ネットワーク由来の実用的なインテリジェンスを活用し、お客様のオブザーバビリティ・ツールを強化するディープ・オブザーバビリティ・パイプラインを提供しています。この強力なコンビネーションを活用すれば IT 組織は、セキュリティとコンプライアンスのガバナンスを維持しながら、パフォーマンスのボトルネックとなる根本原因をすばやく分析し、ハイブリッドおよびマルチクラウドの IT インフラストラクチャ管理に伴う運用コストを削減できます。その結果、現代の企業の完全なクラウド変革を実現できます。Gigamon は世界中で 4,000 社以上の顧客にサービスを提供しています。これにはFortune 100 企業の 80% 以上、10 大モバイルネットワークプロバイダーのうち 9 社、世界中の何百もの政府および教育機関が含まれます。詳しくは、gigamon.comをご覧ください。

1. Shelley Boose81% of Companies Have Had a Cloud Security Incident in the Last Year.Venafi, September 28, 2022. https://venafi.com/blog/81-companies-have-had-had-cloud-security-incident-last-year-venafi-research.
2. 2023 Hybrid Cloud Security Survey:Perception vs.Reality.Gigamon, 2023. https://www.gigamon.com/content/dam/gated/wp-gigamon-survey-hybrid-cloud-security-2023.pdf
3. Internet Security Report – Q2 2021.Watchguard, 2021. https://www.watchguard.com/wgrd-resource-center/security-report-q2-2021
4. Deepen Desai Encrypted Attacks Rise 314%：New ThreatLabz State of Encrypted Attacks Report.Zscaler, October 28, 2021. https://www.zscaler.com/blogs/security-research/encrypted-attacks-rise-314.

Gigamon®

本社
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com

09.23_01