E-BOOK

クラウドセキュリティの進化

予防から検知、そして対応へ

sysdig

目次

はじめに

クラウドセキュリティは大きな進化を遂げています。ここ数年、私たちは見慣れた歴史を映し出すような変貌を目の当たりにしており、経験豊富なセキュリティ専門家は既視感を覚えるかもしれません。

エンドポイントセキュリティの黎明期を覚えているでしょうか？初期の取り組みは、保護対策のみに重点を置いていました。しかし、それだけでは不十分であることに気付くのにそう時間はかからず、エンドポイントセキュリティ戦略は、増大する脅威の数に対応するために、検知と対応の対策を取り入れるまでに発展しました。今日、私たちは、自分たちがクラウドセキュリティについても同様のサイクルに陥っていることに気付いています。私たちは以前と同じような厳しい教訓を学んでいます。ただし今回は、はるかに大規模でかつ複雑な舞台の上で、それを行っているのです。

このeBookでは、エンドポイントセキュリティの歴史的な発展と類似点を描きつつ、クラウドセキュリティへの進化への過程をを紹介します。このよう繰り返される歴史を検証することで、重要なインサイトを明らかにします。そして、過去の過ちを回避するためにセキュリティリーダーが取るべき重要な措置について詳しく解説します。

歴史から学び、よりセキュアなクラウドの未来への道を切りひらきましょう。

時代を超えたエンドポイントセキュリティの旅

クラウドで何が起きているのかを理解するためには、エンドポイントセキュリティの進化について簡単に復習する必要があります。最初のウイルス対策製品から今日のエンドポイント保護プラットフォーム（EPP）に至るまでの道のりは、1980年代に始まり、その後40年間にわたって進歩と統合の荒波を乗り越えてきました。

保護対策

アンチウイルス

黎明期において、コンピューターウイルスは無防備なシステムを大混乱に陥れました。2000年代初頭までに、ウイルスは世界的に蔓延していましたが、アンチウイルス（AV）ソフトウェアがその危機を救いました。シグネチャベースの手法で武装したAV製品は、既知のウイルスを検知して退治するように設計されており、一時的にシステムを効果的に保護することに成功しました。

改善された保護対策

次世代アンチウイルス

従来のAVソリューションは、マルウェアの進化に後れずについて行くことが難しくなっていました。検知を回避するためにコードを変更するポリモーフィックなマルウェアの台頭により、シグネチャベースの保護はますます効果を失って行きました。このため、次世代アンチウイルス（NGAV）が開発されました。NGAVソリューションは、単純なシグネチャにとどまらず、機械学習や振る舞い分析などの高度な技術を取り入れ、脅威を検知して侵入前にブロックするようになりました。しかし、それでもなお、保護に主眼が置かれることに変わりはありませんでした。

検知と対応

エンドポイント検知と対応（EDR）

NGAVの進歩にもかかわらず、サイバー攻撃は成功し続けました。一旦ネットワーク内に侵入されると、それを検知する手段がないため、長い滞留時間と対応の後れにつながっていました。このようなセキュリティギャップが、エンドポイント検知と対応（EDR）ソリューションを誕生させました。EDRは、リアルタイムで脅威を監視、検知、対応までを行う機能を導入し、NGAVによる保護対策を補完するものとなりました。

プラットフォームの統合

最新のエンドポイント保護プラットフォーム（EPP）

サイバーセキュリティの環境が改善されるにつれ、より統合されたソリューションの必要性も高まりました。業界は、統合プラットフォームに機能を集約し始めました。主にMITRE ATT&CK評価により、エンドポイント保護プラットフォーム（EPP）の概念が再定義され、攻撃者の行動を包括的に検知する能力が強化されました。最新のEPPは、統合EDRと呼ばれることもあり、保護、検知、および対応を1つのまとまったソリューションに統合したものとなっています。これらのプラットフォームは、40年にわたるエンドポイントセキュリティの進化の集大成であり、高度な脅威に対する強固な防御を提供します。

ここで、クラウドに焦点を移し、クラウドがどのように急速に進化してきたかを、エンドポイントセキュリティの歴史と興味深い類似点を引きながら探ってみましょう。

クラウドのアタックサーフェス

クラウドセキュリティの歴史は、ある厳しい現実から始まりました。すなわち、クラウドは新たなアタックサーフェスとして、それ自体が自らに牙をむく「攻撃者」となりうるのです。

企業がクラウドに移行するにつれ、アタックサーフェスはますます複雑になりました。データとアプリケーションをオフロードする単純な方法として始まったクラウドは、サービスや接続が複雑に入り組んだ、広大な網の目へと変化しました。このようなデジタル環境は、比類のない柔軟性と拡張性を提供する一方で、新たな独自のセキュリティリスクももたらしました。

クリプトジャッキングやクラウドデータ侵害についてのニュースを耳にし始めたのはこの頃です。そして突然、盗まれた認証情報、誤った設定、過剰に許可されたIDなどに関するニュースが大量に出回るようになりました。Adobe、Facebook、CapitalOneなどの企業に対する大規模なハッキングが見出しを飾るたびに、私たちはクラウドにおけるサイバー攻撃の急増を思い知らされました。サプライチェーンのハッキングに焦点を当てた攻撃や、ヒューマンIDおよびマシンIDの悪用は、驚くほど一般的になりました。

しかし、このデジタルカオスの中で、企業や組織はクラウド環境の可視性が限られていることに気付きました。攻撃者が自由に動き回り、データを吸い上げるため、侵害は数日間、場合によっては数週間も発見されないこともありました。クラウド攻撃のスピードと複雑さは、従来のオンプレミスへのサイバー脅威をはるかに凌駕していたため、防御する側はそれについて行くだけでも精一杯の状態でした。

クラウド攻撃は速いだけでなく、セキュリティに対して異なるアプローチが必要であることが明らかになりました。クラウドセキュリティのための「十分な」ソリューションとして、従来のEPPツールに依存するだけでは、決して十分とは言えなかったのです（詳細は後述）。ありがたいことに、サイバーセキュリティ業界はこのような状況に適応し始めました。企業や組織は、より強固なクラウドセキュリティプラクティスを採用し始めたのです。

「シフトレフト」や「シールドライト」のような用語が登場し、プロアクティブな対策（事前対策）とリアクティブな対策（事後対策）の必要性が強調されました。さらに、クラウドセキュリティポスチャー管理（CSPM）、クラウドインフラストラクチャーエンタイトルメント管理（CIEM）、クラウドワークロード保護プラットフォーム（CWPP）、コンテナセキュリティといった言葉も聞かれるようになりました。

歴史は繰り返す：予防か、さもなければ破綻か

エンドポイントセキュリティの黎明期と同様、クラウドセキュリティに対する初期のアプローチは、予防がすべてでした。目標はクラウドの要塞を構築することであり、攻撃者が壁を突破するチャンスを得る前に撃退することでした。

クラウドの脅威対策は、クラウドセキュリティポスチャー管理（CSPM）とクラウドインフラエンタイトルメント管理（CIEM）から始まりました。これらのツールは、セキュリティ管理を実施し、脆弱性、設定ミス、および潜在的な脅威を監視するために設計されたものです。

クラウドセキュリティポスチャー管理（CSPM）を導入することは、プロアクティブなセキュリティコンサルタントを社内に常駐させるようなものです。これにより、クラウドインフラストラクチャーの各レイヤーにセキュリティを組み込み、脆弱性が悪用される前にそれらを確実に特定できるようになります。CSPMにより、チームはクラウド環境全体にセキュリティポリシーを適用し、あらゆるアクセスポイントと脆弱性に対処できるようになります。

一方、CIEMはゲートキーパーの役割を果たすものであり、誰が何にアクセスできるかを管理します。CIEMは、人もマシンも、いかなるアイデンティティも必要以上のアクセス権を持てないようにするために、権限に目を光らせています。権限を監視し調整することで、CIEMは不正アクセスや潜在的な侵害を防ぐのに役立ちます。

これらのクラウド脅威対策が最初に導入された際、それらは間違いなくゲームチェンジャーでした。しかし、クラウドの複雑な環境にはそれ以上のものが必要でした。クラウドセキュリティの進化における次なるステージでは、防御は不可欠ではあるものの、それはパズルの1ピースに過ぎないことが明らかになるでしょう。

検知と対応：クラウドの最前線を越えて

ネタバレ注意：クラウドでは予防策は十分ではありませんでした（そして、それは今もなお十分ではありません）。クラウド攻撃は息をのむようなスピード（時には数分以内）で展開されます。このようなスピードに対応できるかどうかが、攻撃を封じ込めることができるか、それとも壊滅的な被害を受けるかの分かれ目となります。そして、攻撃はしばしば組織のクラウドフットプリント全体に足場を築くことに成功します。実際、侵害の39%は複数のクラウド環境にまたがっており、その平均コストは475万ドルに上ります[1]。

エンドポイントセキュリティの歴史的な進歩に見られるように、クラウドでは脅威を検知し、電光石火のスピードで対応する能力が求められています。しかし、これを実現するための最初の道のりは、試行錯誤の末に遠回りをすることになりました。クラウドネイティブアプリケーション保護プラットフォーム（CNAPP）ソリューションの一部としてクラウド検知対応（CDR）機能が進化する一方で、多くの企業や組織は、現在のEDRソリューションを拡張して自社のクラウド環境をカバーすることで、その場しのぎのクラウドセキュリティ戦略を選択しました。私たちは、同じ過ちを繰り返さないよう、歴史的な過ちを指摘すると約束しましたが、このようなその場しのぎのセキュリティ戦略は、絶対に避けたい落とし穴の1つです。

1 IBM. Cost of a Data Breach Report 2023.

EDRがクラウドセキュリティに適していない理由

目隠しをして迷路を進むことを想像してみてください。EDRはクラウド環境において、これと同様の課題に直面しています。EDRには、コンテナやKubernetesといった、クラウドネイティブの脅威を発見して対処するために不可欠な可視性が欠けています。EDRはホストレベルの脅威をピンポイントで特定することには長けていますが、それは多くの場合、クラウド環境の全体像を把握できないことを意味します。このため、クラウドの検知と対応能力に大きなギャップが生じることになります。

また、EDRの攻撃を検知するアプローチは、クラウド環境にとって十分に高速であるとは言えません。クラウド環境は猛烈なスピードで動いており、コンテナの平均寿命はわずか5分です。脅威がわずか数分で脆弱性を突くこと、そして最大のインパクトを与えるために攻撃を急速に進めることを想像してみてください。ある攻撃シナリオにおいて、セキュリティアナリストは、5分以内に検知を確認できなければ、単なるアラートを超えて、イベントの範囲を把握することが不可能になります。

クラウド上のインシデントはもつれた網のように複雑かつ多次元的であるため、EDRはさまざまなドメインにおける点と点をつなぐことができません。このような操作は、クラウドの検知と対応に不可欠な「**555ベンチマーク（検知に5秒、相互関連付けとトリアージに5分、対応に5分）**」を満たすために必要となるものです。

CDR：クラウドの検知と対応のための頼性できる道筋

クラウド独自のこの性質は、目的に適合した検知と対応能力を要求します。ありがたいことに、セキュリティ市場はCDRによってまさにその能力を提供するように進化しました。クラウドのニーズに対してEDRでうっかり回り道をしてしまった企業や組織は、現在、このような目的に特化したCDR機能に向けて軌道修正を行っています。

CNAPPに統合されたCDRは、コンテナ、Kubernetes、サーバーレスコンピューティング、クラウドのログと証跡、LinuxとWindowsの両サーバーなど、幅広いクラウド技術にわたって高度な検知と対応を提供します。

CDRは、さまざまな物事を単に監視するだけではありません。CDRは、ハッカーが「侵入」を宣言するよりも早く脅威を検知し、調査し、それに対応できるような、フルスケールのセキュリティオペレーションを提供します。エンドツーエンドの機能を持つCDRを導入することで、セキュリティチームはクラウド環境の急速なペースにも対応できるようなり、「555ベンチマーク」を満たすことでクラウドへの脅威に真っ向からリアルタイムで取り組めるようになります。

クラウド セキュリティ プラットフォームの 統合

私たちは今、繰り返す歴史の物語の最終章にいます。この時点で、エンドポイント市場は、保護、検知、対応を単一のエンドポイントプロテクションプラットフォーム（EPP）へとスマートに統合しました。このシナリオからヒントを得て、クラウドセキュリティ市場は、戦略的にツールの武器庫をCNAPPへと統合しました。

このマイルストーンは、真のクラウド中心のセキュリティツールで企業や組織を武装化するものです。これにより、セキュリティチームは次の能力を確保できるようになります。

- **マルチドメインおよびマルチクラウド環境全体をカバーすること：**クラウドのフットプリントがいかに広大で複雑であっても、包括的な保護を提供します。
- **10分以内に検知、調査、対応を行うスピード：**攻撃の一歩先を行き、被害を受ける前に脅威をシャットダウンします。
- **脅威に効果的に対応するためのコンテキスト：**決断を下すために必要となる詳細な情報やインサイトを提供します。
- **部門の垣根を超えたチーム向けの統合ソリューション：**シームレスなコラボレーションを促進し、異なるチーム間の理解度や優先度の違いと言った障壁を取り払い、全員が同じ見解を持つことを保証します。

専用に構築されたクラウドセキュリティが持つ価値

クラウドセキュリティツールがCNAPPに統合されたことで、今や企業や組織は、クラウド時代に適した強力な防御システムを手にすることができました。この画期的な出来事が、世界中のセキュリティチームにとって何を意味するのか、以下に説明します。

既知と未知の脅威をリアルタイムで検知

クラウド向けに構築された堅牢なクラウド検知対応ソリューションは、組織のクラウド資産全体にわたって、既知と未知の脅威をリアルタイムで検知します。もちろん、最も革新的なCNAPPには、最も高度な機能が備わっています。たとえば、最新のCNAPPは、ポスチャーとランタイムのインサイトを自動的に相互に関連付け、真のクラウドネイティブコンテキストを実現します。これは、ワークフローを加速し、スキルギャップをなくすのに役立ちます。また、これにより、主要な利害関係者のフィードバックループを解放し、分断されたビジネスライン間の摩擦を取り除き、チームに唯一の情報源を提供し、それを共有できます。このような機能を提供するクラウド検知対応ソリューションを導入することで、セキュリティリーダーと実務担当者は、アナリストの効率性の向上、リスク削減、コスト最適化などの分野でメリットを享受できます。

マシンIDとヒューマンIDに対するマルチドメイン相関

クラウドへの脅威が単一のドメインに限定されることはほとんどありません。効果的なクラウド脅威検知は、資産、ユーザー、アクティビティ、リスクを横断するマルチドメイン相関を提供し、脅威をリアルタイムで特定します。CNAPPは、使用中の脆弱性や権限に関するインサイトと即座の検知を重ね合わせることで、環境全体の点と点を結び付け、脅威がエスカレートする前に、先手を打って脅威を和らげます。

イベントを特定しコンテキスト化することで迅速な調査を実現

クラウド環境でサイバーパズルを解いている時に、ピースが欠けていると感じたことはありませんか？今はもう、そんなことはありません。CNAPPは、クラウドとワークロードのイベントとアイデンティティの相互関連付けを自動化し、コマンド履歴、ネットワークトラフィック、ファイルアクティビティに関する完全なコンテキストを提供します。自動化されたキャプチャは、デジタルフォレンジックの証拠をイベントに結び付け、脅威に関する包括的なビューを提供します。さらに、MITREのフレームワークに対応したフィルタリング可能な調査によりワークフローを合理化することで、企業や組織は、脆弱性や設定ミスを迅速に特定してそれらに対処できるようになります。

チーム間のワークフローのサイロを打破

現実に向き合いましょう。サイロとは元々は穀物を貯蔵する、という意味であり、セキュリティチームを表現するためのものではありません。単一の目的で構築されたクラウドセキュリティプラットフォームは、インシデント対応担当者、開発者、そしてその間にいるすべての人の間にある障壁を取り払います。数分以内にチームに実用的なインサイトを提供することで、迅速な調査結果を踏まえた迅速なコラボレーションを実現できます。これは単に攻撃を阻止するだけでなく、長期的な防御の微調整にもつながります。また、インシデントの報告を共有し、予防策を強化することで、リスクを軽減できるほか、クラウドセキュリティへのアプローチを向上させることができます。

結論

クラウドセキュリティの技術革新の道のりを見てみると、明らかなことが1つあります。それは、クラウドの脅威に対するスピードと耐障害性を追求するエンドポイントセキュリティの進化と同じように、クラウドの状況も劇的に変化しているということです。予防に固執したクラウドセキュリティの黎明期から、堅牢な検知と対応機能への進化、そしてCNAPPへのツールの統合に至るまで、その類似性は際立っています。

EDRはエンドポイントセキュリティへの道を切り拓きましたが、CDR機能を備えたCNAPPはクラウドの守護者として台頭してきました。EDRはワークステーション向けの優れたツールですが、セキュリティチームは、広大なクラウド環境全体で脅威を迅速に特定し、無力化するCDRソリューションを必要としています。CDRは、脅威をリアルタイムで検知して対応するだけでなく、最新の脅威に対抗するための俊敏性と広範な能力を提供します。

とりわけ、CNAPPを導入すると、セキュリティチームは「**555ベンチマーク（検知に5秒、相互関連付けとトリアージに5分、対応に5分）**」を達成できるようになります。この戦略的アプローチは、クラウドインフラストラクチャーを保護するだけでなく、新たな脅威に対する防御を将来的に実現できることを保証します。このクラウドセキュリティ戦略を採用することは、単にデータを保護するだけでなく、企業や組織が安心してクラウドの可能性をフルに活用できるようにすることであり、絶えず変化するデジタル環境に直面してイノベーション、成長、レジリエンス を促進することなのです。

Sysdigが、お客様の環境を1秒1秒セキュアに保つのにいかに役立つかをご覧ください。

次のステップに進む。

デモを依頼 →

sysdig

E-BOOK

EBK-013-JA REV. A 9/24