プルーフポイントで医療情報を保護

内部脅威、データ損失、クラウド拡張から患者データを保護する

製品

- Proofpoint CASB (Cloud App Security Broker)
- Proofpoint Email DLP (Data Loss Prevention)
- Proofpoint Endpoint DLP (Data Loss Prevention)
- Proofpoint ITM (Insider Threat Management)
- Proofpoint Web Security
- Proofpoint ZTNA (Zero Trust Network Access)
- Proofpoint MSIP (Managed Services for Information Protection)

おもなメリット

- 不注意なユーザー、不正アクセスを受けたユーザー、悪意のある内部関係者を識別し、そのリスクを軽減する
- Eメール、クラウド、エンドポイントからのデータ損失を阻止する
- 広範囲に分散し増加し続けるクラウドサービスに対応できるよう、スケーラブルな保護機能を強化する

医療業界は、長きにわたってサイバー犯罪者にとって格好の標的となってきました。そのうえ、新型コロナウイルス感染症の大流行が、さらにその状況を悪化させる一方となっています。攻撃者は、ワクチンの治験情報、保護されるべき医療情報 (PHI)、財務データなどの重要なデータを入手する活動を強化しています。その一方、医療機関においては、クラウドへの移行や、リモートでログインできる従業員や患者の増加により、攻撃対象領域が拡大しています。また、悪意の有無に関係なく、内部関係者がリスクを高めています。

プルーフポイントは、「人」を中心にセキュリティを構築する People-Centric なアプローチにより、広範囲に分散した医療ネットワーク上の機密データを保護します。プルーフポイントの情報防護ソリューションは、導入と保守が容易であり、堅牢なセキュア アクセス サービス エッジ (SASE) やセキュア サービス エッジ (SSE) の構築が可能です。外部からの攻撃、不注意や内部脅威のリスクから従業員と機密データを保護できるようサポートします。保護対象は、クラウドサービス、E メール、エンドポイント、オンプレミスのファイル共有のすべてに及びます。

増大する脅威

データ侵害は、コンプライアンス違反による罰金、訴訟、医療機関としてのブランド価値の毀損、さらには人命の損失にもつながります。残念なことに、米国保健福祉省の報告によると、2020 年前半には、医療業界に関連するセキュリティ侵害が 50% 増加しました。さらに、2021 年には、ランサムウェアによる全攻撃件数は 2 倍以上に増加しています。この年、医療業界は、もっとも標的になる可能性が高い 2 業種のうちの 1 つとなりました。

救命医療で用いられるモノのインターネット (IoT) デバイスの数が増えると、多くの人命を救うことができるようになりますが、複雑性を伴います。また、新型コロナウイルス感染症により、遠隔医療サービスを利用する医療従事者が増加しており、クリニックや病院だけではなく、中には自宅からサービスを提供している医療従事者も存在します。

したがって、ムーディーズ・インベスターズ・サービスでは、医療業界ではサイバーリスクの高い状況が当面続くだろうと予想しています。既存のリスクをほぼ 2 年にわたって管理してきた医療機関は、今後も警戒を続けなければなりません。

情報保護に関する課題

病院、クリニック、医療保険会社、バイオテクノロジー企業は、この深刻な脅威状況において、情報保護を最優先課題と捉える必要があり、患者の保護されるべき医療情報 (PHI)、個人を特定できる情報 (PII)、およびクレジットカード情報を守らなければなりません。これらの組織は、さまざまな課題に直面します。

内部関係者による電子健康記録 (EHR) のスヌーピング (覗き見) やその他の脅威を防止する

医療従事者は、新型コロナウイルス感染症の大流行において英雄というべき存在です。危機の到来とともに、終わりがまったく見えない時も、彼らは日々きわめてストレスの多い仕事をしていました。このようなストレスは、内部脅威のリスクを高めます。たとえば、好奇心旺盛な従業員が息抜きに、有名な患者の医療記録をこっそり見たくなるかもしれません。このようないわゆる電子カルテ (EHR) のスヌーピング(覗き見)から、たとば富裕層の患者情報が公にさらされてしまうと、医療機関に大きなリスクを引き起こします。

また、悪意はなくても対応しきれなくなった従業員が、本来ならばそれと気づくようなフィッシングメールをクリックする可能性もあります。精神的ストレスが、雇用主に悪意のある内部脅威をもたらす場合もあります。そこで、このような脅威をすべて阻止する対策を講じる必要があります。

医療業界におけるクラウド導入に伴って拡大を続ける攻撃対象領域に対処する

多くの医療機関は、これまでクラウドをなかなか導入しませんでした。しかし今では、ほぼすべての機関が、パブリックとプライベート両方のクラウドで、複数のサービスを採用しています。これにより、業務効率が向上しました。また、IT インフラを構築するための投資資金を確保する必要もなくなりました。しかしその一方で、医療機関の攻撃対象領域は拡大しました。

電子カルテ (EHR) がオンプレミスのインフラに保管されていたとしても、その記録の詳細は当然ながら、他の場所からアクセスされ、共有、保管されることになります。そこで、モバイル デバイス、リモート エンドポイント、医療 IoT デバイス、クラウドベースのメールシステムについて考えてみましょう。医療情報が移動する範囲が拡大するにつれ、それを保護することはさらに大きな課題となります。

また、クラウドの利用が拡大するにつれ、認証情報が窃取されるリスクが高くなります。Microsoft Office のソフトウェアやコラボレーション機能は、Microsoft 365 や Google Workspace などのクラウドサービスを介して提供される場合が多くなっていますが、これらのサービスはサイバー脅威に脆弱です。このように一般に認識されているファイル共有をサイバー犯罪者が悪用するようになっていることが問題をよりいっそう複雑にしています。

提供モデルの進化に伴い、医療スタッフや遠隔患者の保護を強化する

新型コロナウイルス感染症の大流行により 2020 年初頭に働き方改革が、ほぼ強制的に巻き起こりました。中には一時的な措置だったものもありますが、改革の多くは今後の働き方にも大きな影響を与えるものです。医療業界では、遠隔医療によるケアの増加が続いている傾向にあります。ある研究によると、2021 年 2 月には、遠隔医療の利用が、2019 年の基準の 38 倍にもなりました。これにより、企業リソースにリモートアクセスする患者の数が大幅に増加しました。

その上、少なくともパートタイムの場合、多くの従業員が今でも在宅勤務をしています。彼らの多くが、電子医療記録 (EMR)、患者の財務情報、研究データを管理しています。リモートログインの回数が増えると、組織内で特定の役割を担う人物への攻撃リスクが高まります。

「人」を中心にセキュリティを構築する PEOPLE-CENTRIC アプローチを採用

情報を保護するための従来のアプローチでは、データのみに目が向けられますが、情報は勝手に流出するものではありません。データ損失を引き起こすのは「人」なのです。人は意図せずに、あるいは悪意から、データ損失を引き起こします。サイバーセキュリティでは可視性が鍵なので、リスクをもたらす可能性が非常に高い人物像を理解しなければなりません。People-Centric アプローチは、そのようなデータを扱うユーザーの行動を理解する取り組みです。

プルーフポイントにできること

プルーフポイントの情報防護クラウドセキュリティ プラットフォームは、機密情報の管理者に焦点を当てることにより、企業がその情報を保護できるようサポートします。

Proofpoint CASB (Cloud App Security Broker)

Proofpoint CASB (Cloud App Security Broker) は、クラウドの脅威からユーザーを保護します。機密データを保護し、Microsoft 365 内のクラウドおよび OAuth アプリ、Google Workspace に加え、IT 部門が承認したアプリや IT 部門に許容されているアプリを 900 個以上も制御します。クラウドベースのサービスに対して、プルーフポイントによる Very Attacked People™ (VAP) の視認性を高めるので、クラウドアカウントとデータの保護を強化することができます。Proofpoint CASB は、クラウドアクセス、ユーザー行動、保護されるべき医療情報 (PHI) のような機密データの取り扱い状況を詳細に表示し、プライバシー規則やデータセキュリティ規則を常に遵守できるようサポートします。

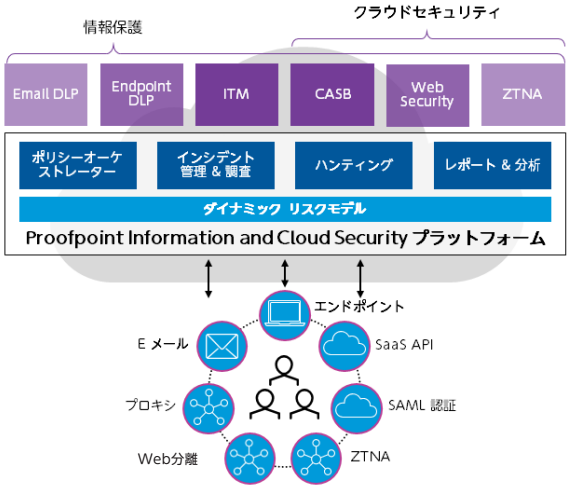

図 1: プルーフポイントの情報防護クラウドセキュリティ プラットフォーム

また、ユースケースに応じて、複数のモードで導入することができます。 ほぼリアルタイムの可視化を実現するとともに、早期の投資効果を実感できるよう、お使いのクラウドアプリの API とインフラログを CASB に統合します。リアルタイムでのアクセスとデータ制御については、リスクベースの SAML 認証、Web分離、およびインライン フォワード プロキシ機能を使用できます。実際のセキュア サービス エッジ (SSE) では、Proofpoint Web Security および Proofpoint ZTNA (Zero Trust Network Access) と CASB を統合し、Web およびクラウド アプリケーションを通じて、リモートワーカー同士を接続・保護します。

Proofpoint DLP (Data Loss Protection)

Proofpoint Data Loss Prevention では、情報漏えい対策 (DLP) に People-Centric アプローチを採用しています。コンテンツ、行動、脅威をひとつにまとめ、これら 3 つ全体のコンテキストを提供します。最新タイムラインビューに正確で詳細な情報を提示するため、特定のイベントをより包括的かつ詳細に理解することができます。この情報は、フラグつきのユーザーが不正アクセスを受けているユーザーなのか、悪意を持ったユーザーなのか、不注意でミスをしたユーザーなのかを理解するのに役立ちます。

Proofpoint ITM (Insider Threat Management)

Proofpoint ITM (Insider Threat Management) はユーザー アクティビティとデータの移動を関連づけます。これにより、セキュリティチームは、潜在的な内部脅威に対して、検知、調査、対応することができます。「人」を中心に行動を認識でき、データ持ち出し、権限の悪用、アプリケーションの不正使用、不正アクセス、危険な可能性が高いアクション、異常行動に対して、リアルタイムで検知、対応します。これにより、タイムラインベースで可視化と分析がおこなわれ、電子健康記録 (EHR) のスヌーピング (覗き見) のような脅威に対して、検知、阻止、対応することができます。

内部脅威が特定された時点で、ワークフローと不正行為の確固たる証拠を提供し、インシデント レスポンスを迅速化します。軽量のエンドポイント センサーにより、インテリジェンスが収集され、その後、スケーラビリティ、セキュリティ、プライバシーのために構築された最新のアーキテクチャにおいて分析されます。また、Proofpoint ITM は、オンプレミスやソフトウェア アズ ア サービス (SaaS) 提供モデルを用いてデプロイできる柔軟性も備えています。

Proofpoint Web Security

より多くの従業員が、ネットワーク境界の外からログインするようになってきています。Proofpoint Web Security は、このように分散して Web を閲覧する従業員を高度な脅威から保護し、安全なインターネット ブラウジングを実現します。SSL トラフィックをすべて検査することにより、ランサムウェアやゼロデイフィッシング攻撃などの脅威を突き止めてブロックします。また、従業員が危険なコンテンツやコンプライアンスに違反しているコンテンツを閲覧するのも阻止します。

Proofpoint ZTNA (Zero Trust Network Access)

アプリケーションがクラウドに移行するにつれ、医療従事者はリモートワークをする機会が非常に多くなっています。これを受けて、セキュアなアクセスを実現するために、より優れた VPN 代替策が求められています。Proofpoint ZTNA は、ユーザーごとにソフトウェア定義による境界 (SDP) を活用し、データセンターやクラウド内のリソースへのセキュアなリモートアクセスをクラウドで実現する環境をユーザーに提供します。

各ユーザーは、必要なアプリケーションのみにアクセスすることが許可されます。アクセスが許可されたネットワーク以外は、ユーザーからは見えません。Proofpoint ZTNA では、ユーザーがネットワークに入る前に入念に検査されるため、セキュリティと可視性が高まります。

Proofpoint MSIP (Managed Services for Information Protection)

Proofpoint MSIP (Managed Services for Information Protection) では、世界中の弊社データセキュリティ専門家チームが、お客様のチームをサポートします。プルーフポイントは、長年の経験から、お客様のプログラムを最適化するためのベストプラクティスと成熟度モデルを構築しました。アプリケーションの管理、範囲、およびポリシーのガバナンス、イベントの優先順位づけ、インシデント管理、レポーティング、分析を提供します。これにより、知的財産の盗難や患者様のデータ侵害からお客様をお守りします。プルーフポイントの専門家が、お客様のセキュリティおよびコンプライアンスのニーズに合わせたプログラムを設計、実装、運用します。情報漏えい対策 (DLP) から、クラウド アクセス セキュリティ ブローカーや内部脅威管理 (ITM) に至るまで、高度な機械学習と、関連する人間分析を利用することで、お客様のヘルスケア情報を保護します。アラートが発せられるとすぐに検証され、侵害の試みには迅速に対処します。セキュリティ改善や、チームを活かすためのサポートはプルーフポイントにお任せください。お客様にはセキュリティ以外の問題に向き合う時間ができます。

まとめ

新型コロナウイルス感染症の影響により、医療機関は職場環境を大きく変化することを余儀なくされました。これは、サイバー攻撃の対象領域が広がったことを意味します。今や、複数のクラウドに情報保護対策を取ることが必要となりました。また、従業員と患者によるリモートログインは、増加の一途をたどり、ネットワークエッジにある医療 IoT デバイスの数も増え続けています。

各組織はほぼ 20 年にわたり、境界防御の保護に努めてきました。最近のクラウドサービス利用の急増と、リモートワークの増加により、今や従業員一人一人が境界となり、ひいては境界線となっているのです。

このように急激に変化することで、新たなセキュリティ アーキテクチャが求められています。その新たなアプローチは、多くの場合セキュア サービス エッジ (SSE) と呼ばれています。SSE は セキュア アクセス サービス エッジ (SASE) のセキュリティを担い、クラウド データ センターを経由してあらゆるクラウドサービスに安全にアクセスするのに必要な環境をユーザーに提供します。これにより、ゼロトラスト ネットワーク アクセスや、ID およびアクセス管理がおこなわれるとともに、管理者は集中管理でアクセスを監視できます。

プルーフポイントの情報防護クラウドセキュリティ プラットフォームを活用することで、堅牢な SSE または SASE アーキテクチャを構築できます。これにより、場所やデバイスの種類にかかわらず、従業員がアプリケーションやデータにアクセスするなかで、組織がセキュアなアクセスと脅威保護を適用できるようになります。機密情報を取り扱う従業員を保護することにより、機関を守ることにつながります。

詳細はこちら

詳細は proofpoint.com/jp でご確認ください。