TANIUM

サイバーセキュリティの安全対策:

コンバージド・エンドポイント管理 (XEM)

エンドポイントセキュリティの未来像 - XEM
セキュリティとIT運用を統合する時代が到来

TANIUM

サイバーセキュリティの安全対策: コンバージド・エンドポイント管理 (XEM)

エンドポイントセキュリティの未来像 - XEM
セキュリティとIT運用を統合する時代の到来

もくじ

この1年間でセキュリティにかける予算は、増加しているのではないでしょうか。レポート[1]によると、世界的にセキュリティの平均支出額は60%増加しています。ハイブリッドワークの増加に伴い、CIOやCISOはセキュリティポリシーを再評価し、エンドポイントのセキュリティ強化に取り組んでいます。

そして、それは予想以上に大きなプロジェクトとなっています。最近の調査では、CISOの82%が「エンドポイントのセキュリティを見直しているものの、保護できていない」あるいは「エージェントの競合により過負荷になっているエンドポイントがある」と回答しています。また、エンドポイントの5台に1台は攻撃に対して脆弱であることが判明しています。

企業はこれまで以上に多くの攻撃を受けています。サイバーセキュリティベンチャーズは、2022年末までに企業に対するランサムウェア攻撃が11秒に1回の割合で発生すると予想しています。2021年には、企業に対する毎週のサイバー攻撃が50%増加しました。

また、サイバー犯罪者はより標的を絞った攻撃を行うようになっています。マイクロソフトが最近発表したDigital Defence Reportによると、この1年間で攻撃が急速に巧妙化しており、発見されにくい手法で熟練のセキュリティチームすらも脅かすようになっています。国家主導型の場合は、価値の高い標的を狙えるように、偵察活動も行われています。犯罪グループはインフラをクラウドに移行し、正規のクラウドサービスに紛れて潜伏するようになりました。また、ランサムウェアの脆弱性のあるシステムをインターネット上でスキャンする新しい手法も開発されています。

このように攻撃が増加して複雑化し、さらに世界的にセキュリティの専門家が不足していることが企業にとって大きな問題となっています。英国では、サイバーセキュリティの人材は昨年65,000人減少し[2]、33,000人の人材不足に陥っています。政府によると、企業の5分の2（39%）が2021年にサイバー攻撃やデータ漏洩を経験したと報告しています[3]。

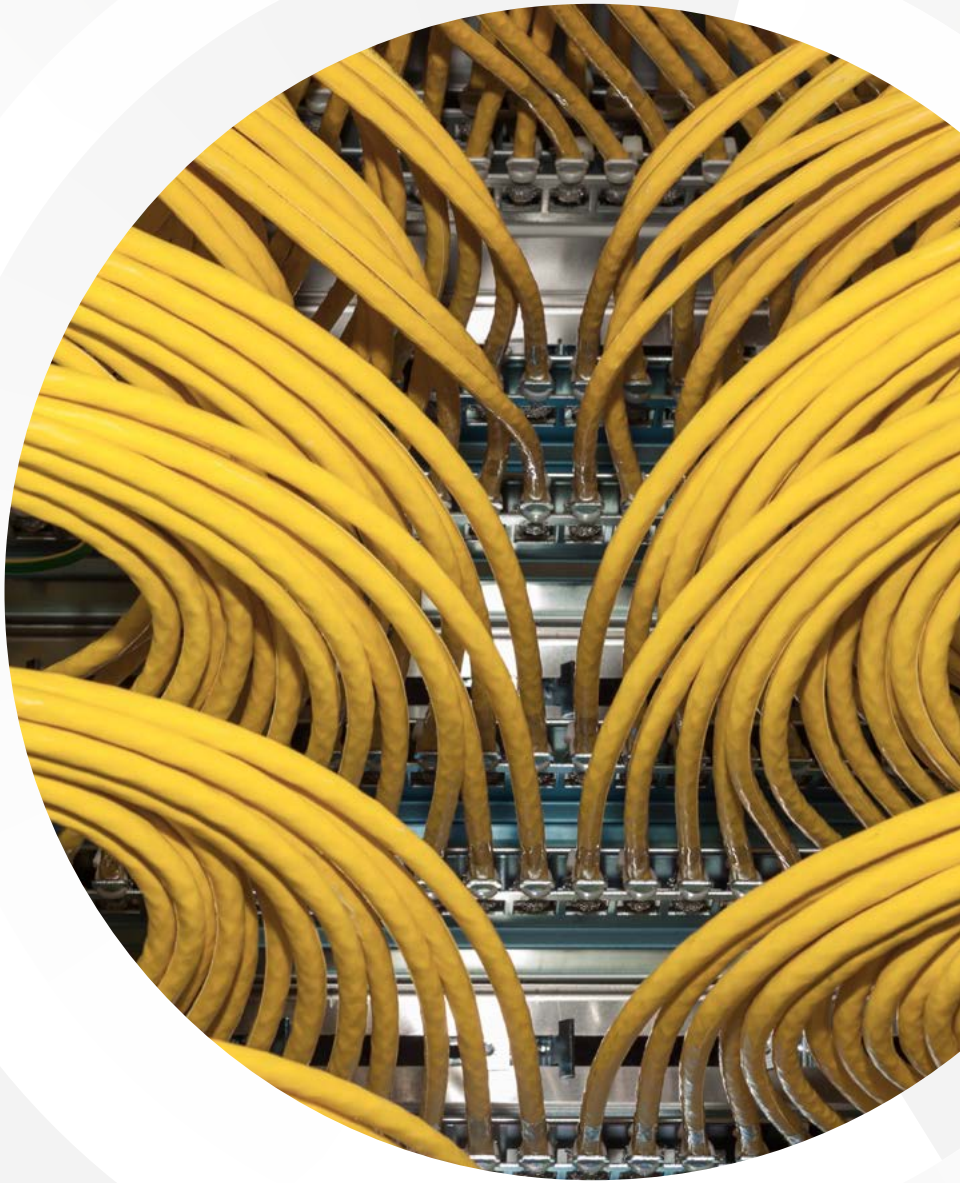
変革が求められている

タニウムは、多くの企業のセキュリティ管理へのアプローチに根本的な問題があると考えています。セキュリティの脅威が指数関数的に増加するなかで、企業はポイントソリューションを導入して対応することがよくあります。この1年間で90%の企業が、新たなセキュリティソリューションを1つ以上購入しており、FoundryのSecurity Priorities Studyによると、ほぼ半数（45%）は4つ以上の新製品を購入しています。

> **一般的な企業では、43種類のセキュリティツールやセキュリティ管理ツールを使用**

このようなやり方は持続可能ではありません。新たなツールを追加しても必ずしも保護が強化されるわけではないのです。新たな脅威はほとんどの企業が追いつけないスピードで出現しています。この状況は、現代の分散化した企業には特にあてはまります。また、一部のポイントソリューションの有効性が低下しているというエビデンスもあります。New York Timesの最近のレポートによると、一部のアンチウイルスツールの初回検出率は5%を下回っています。

さらに、ポイントソリューションはそれぞれデータ、インターフェイス、所有者が異なり、それらの増加に対応するという問題も発生します。例えば、あるツールはIT運用部門が管理し、毎日データを報告する一方で、別のツールはコンプライアンス部門が管理し、四半期ごとに別の経路で報告を行っているような場合もあります。このような状態が数十回と繰り返されるとCIOやCISOは途方もないデータの問題を抱えることになります。



このようなツールを寄せ集めたアプローチでは、環境を完全に保護することはできず、むしろセキュリティ対策に悪影響を及ぼす可能性があります。いくつものセキュリティツールを複数の場所で使用しているとCIOはエンドポイントの数を把握できず、ましてや保護の状況や必要な変更などについて明確な情報を手にすることはできません。

多くの場合、セキュリティはデータの問題に起因します。数十のシステムやセキュリティソリューションを運用し、それぞれが異なる速度で膨大なデータを生成するような状況で、データを統合して理解することは不可能です。簡単に言うと「見えないものは守れない」のです。

セキュリティの意思決定者はサポートを必要としています。エンドポイントの増加に対応し、各エンドポイントの状況や、脅威の危険性、そして脅威から保護するための方法を正確に把握するためのプラットフォームが必要です。こうした情報は一ヶ所にまとめて、リアルタイムにアクセスできるようにするべきです。そうすることでCIOは環境を効果的に保護するために必要なセキュリティの見解を示し、適切なタイミングで適切な対策を優先する戦略を策定することができます。

そこで必要なのが、統合型のソリューション(コンバージド・ソリューション)です。

悪化の一途をたどる状況

タニウムがセキュリティの意思決定者数百人に話を聞いたところ、誰もがセキュリティ管理の負荷を軽減し、簡素化する方法を求めていることがわかりました。

特にIT運用とセキュリティの各チームが連携しておらず、セキュリティデータをすばやく効率的に共有できないなど大きな課題に直面しています。にもかかわらず、多くのビジネスリーダーは保護について誤った自信を持っています。そして、セキュリティデータが可視化できていないことでネットワークが攻撃に対して脆弱な状態になっています。

約64%の企業は今後12ヶ月の間にサイバー攻撃を受けると予測

さらに、サイバー攻撃が企業ブランドの評価に影響を及ぼし、コンプライアンス違反の罰金につながることも懸念されています。

状況を可視化できずツールが統合できないことで、金銭的損失、ダウンタイム、ブランド力の低下、コンプライアンス違反による罰金などのリスクにさらされることになります。企業で発見される脆弱性の20.4%が高リスクか重大リスクに分類されることを考えると、これは大きな懸念材料です。また、Edgescanによると重大なリスクの修正には平均61.4日かかります。さらに、侵害を特定し封じ込めるまでに平均247日かかります[4]。これは、企業にとって大きなセキュリティリスクとなります。

セキュリティ管理はビジネスリーダーが優先度を上げるべき項目です。最近のHarvard Business Reviewの調査では、70%が「リーダーシップはサイバーセキュリティにもっと関心を持つべきだと考えている」と回答しています。

セキュリティ管理に新たなアプローチを

次々と発生する脅威に対応するためには、エンドポイント管理に新しいアプローチが必要です。

> **「CIOやCISOは、IT運用、セキュリティ、リスク、コンプライアンスの各グループに導入されたバラバラのポイントソリューションの寄せ集めに頼るしかない状態になっています」**
>
> タニウム CMO スティーブ・デハブ

CIOやCISOは目的に合わせて何十種類もソリューションを購入し、それらを自分たちで連携して、古くて精度が低く、かつ互換性のないデータに基づいて意思決定することを余儀なくされています。

多くの企業がランサムウェアの被害に見舞われるのは、使っているツールが巧妙な攻撃に対応できていないからです。ツールのスピードが遅く、信頼性に欠け、データの共有が難しいことで、本質的にサイロを生み出してしまっています。

このようなアプローチではうまくいきません。**コンバージド・エンドポイント管理(XEM)**という統合型ソリューションで、ツールとデータを統合すべき時が来ています。

コンバージド・エンドポイント管理 (XEM)とは

コンバージド・エンドポイント管理(XEM)とは

タニウムは統合型のセキュリティ管理を推進しており、複数のツールとデータを統合し、1つのインターフェイスですべてのエンドポイントを可視化し、リアルタイムのデータにアクセスできるプラットフォームを提供しています。

> **「XEMを使えば、従来の断片的なエンドポイント管理とは異なり、環境の規模や複雑さに関係なく、すべてのエンドポイントを可視化してデータをリアルタイムに取得し、数秒でエンドポイントにアクセスすることが可能になります」とデハブは話します。**

XEMは精度の高いリアルタイムのデータを提供し、エンドツーエンドの自動化をサポートします。これにより、セキュリティチームは取組みの足並みを揃え、企業を攻撃からより効率的に保護することが可能になります。統合型のアプローチを採用することでIT運用、コンプライアンス、セキュリティ、その他多くの部門が、データの照合や共有に多くの時間を費やす必要がなくなります。単一のインターフェイスでデータを確認できるため、セキュリティチームはより少ないリソースでより多くの作業を行うことが可能になるのです。

状況の可視化と業務の効率化を進める企業では、古い管理システムが問題の根本的な原因となっていることがよくあります。統合型プラットフォームに移行することで、これまで管理にかけていた膨大な時間を削減し、人員を他のタスクに割り振り、危険性の高い脆弱性に社内全体でより迅速かつ効率的に対応できるようになります。

データの品質向上

状況を可視化できず、適切なデータが手に入らない状態では、セキュリティに関する効果的な意思決定を行うことはできません。XEMは、すべてのエンドポイントの情報をリアルタイムに提供できるので、重要な情報がどこかに孤立し、複数のチームが異なるツールを使ってアクセスするようなことはありません。

ツールを単一のインターフェイスに集約することで、セキュリティを効果的に強化するための業務に集中して取り組むことができます。XEMを使用することで、すべてのセキュリティデータを単一のビューで簡単に確認して評価し、管理することが可能になります。そしてデータを共有することで、より効率的に協業し、管理をより簡単にコスト効率よく実施できます。また、信頼性の高いタイムリーな情報を提供することで、よりスピーディに適切な意思決定を下すことが可能になり、これは脅威が刻一刻と変化する中で必要不可欠なものです。

効果的なガバナンスを提供

多くのCIOにとって、ITガバナンスは最優先事項ですが、セキュリティとなると実現がほぼ不可能になります。企業にはコンプライアンス、ガバナンス、IT運用、セキュリティ、リスクなど、セキュリティを担当するチームが複数存在しますが、これらのチームは連携していないことが多く、社内全体の脅威を可視化することは難しくなります。

社内全体のリスクを連携できず、リスクを可視化できなければ、盲点が生じ、セキュリティとコンプライアンスの両方に問題が発生する可能性があります。すべてのエンドポイントを可視化できなければ、アクセスポリシーを施行してITインフラ全体を制御することは不可能に近くなります。

こうした盲点をなくすためには、複雑で時間のかかるプロセスを用意する必要はありません。XEMは不必要な複雑さを軽減し、IT資産を可視化して、効率と有効性を向上するスピーディなソリューションを提供します。

> **「Taniumはプラットフォーム型のアプローチで、リスクやコンプライアンスの管理からデータ監視まで、必要な機能をすべて1つのソリューションで実現します」とデハブは話します。**

Taniumを使えば、すべてのデータの場所をすぐに特定できます。つまり、共通の手法やデータを使って、すべてのエンドポイントにセキュリティツールをデプロイすることができるのです。

違いを生み出す

タニウムのXEMは、複数のチームが協業しながら必要な情報を詳細まで完全な形で手にし、詳しく調査して優先順位をつけ、プラットフォームを超えて修正を行い、継続的に監視することを可能にする唯一のソリューションです。

XEMを使えば、IT運用とセキュリティと併せて、複数のポイントソリューションを使ったセキュリティインフラを統合できます。XEMプラットフォームは市場に変化をもたらし、急増するサイバーセキュリティの脅威と複雑化するセキュリティ管理という2つの課題に対応することを目的としています。

XEMがなければ、より多くの侵害やハッカーのターゲットとなり、データ流出や問題が増加することになります。今こそ変革すべき時が来ています。

タニウムのソリューション:

XEMのメリットを詳しく見る

実際にソリューションをご覧になりたい方は**デモ**をお申込みください

参考資料:

1. https://www.hiscoxgroup.com/sites/group/files/documents/2022-05/22054 - Hiscox Cyber Readiness Report 2022-EN_0.pdf
2. https://www.isc2.org/Research/Workforce-Study
3. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022
4. https://www.ibm.com/downloads/cas/OJDVQGRY