White Paper

コンバージド（統合型）エンドポイント管理がもたらす価値：リスク低減、生産性の向上、ライセンス費用の削減、従業員エクスペリエンスの改善

Sponsored by: Tanium

Michael Suby　　Phil Hochmuth
April 2023

IDC の見解

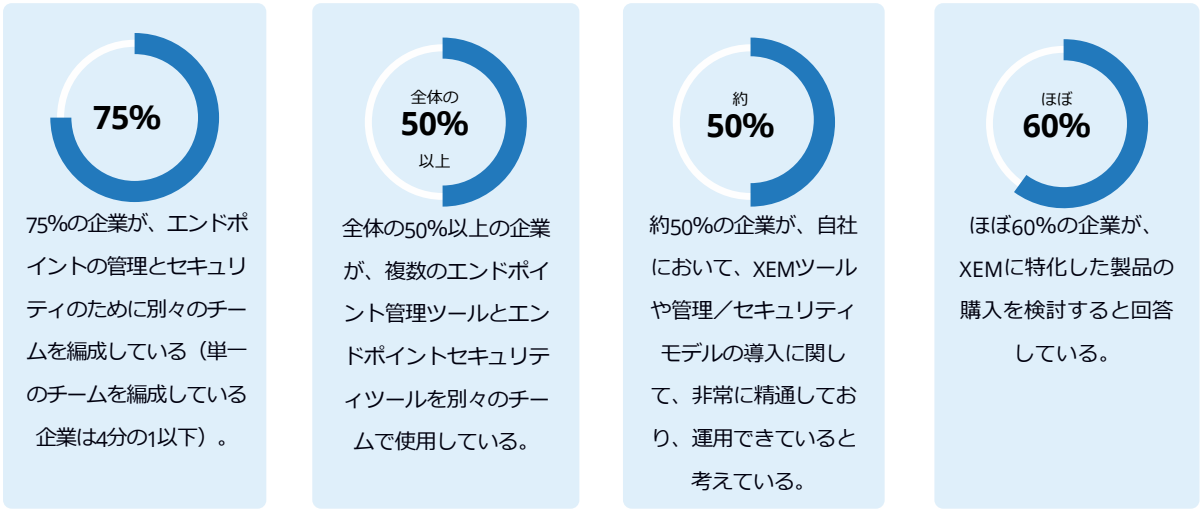
企業において、セキュリティに対する予防を優先したアプローチの本質的な価値は認識されているものの、それを実現することは容易ではない-。エンドポイントに関わるセキュリティチームとIT 管理チームは、必ずしも共通の見解を持ち合わせているわけではない。両チームはリスク低減という共通の目標を掲げてはいるものの、別々に作業することが多い。その結果、テクノロジー製品の選定において、両チームの機能をサポートする製品ではなく、それぞれのチームの機能をサポートする製品を選定することになり、構造的なリスク低減、社内の生産性向上、ソフトウェアライセンス費用の削減、従業員エクスペリエンスの改善を通した組織強化の機会を逸している。IDC の調査では、こうしたベネフィットは、テクノロジーアプローチを個々に独立した製品のポートフォリオから統合型エンドポイント管理（XEM）プラットフォームへと移行した企業によって実現されていることが判明している。

エンドポイントデバイスの管理とセキュリティの統合

専門的な IT 環境におけるエンドポイントの管理は、従来、エンドポイントデバイスのセキュリティとは別の機能であった。前者には、デバイスの導入、OS やアプリケーションの配布／更新、ソフトウェア／ハードウェアの全般的なライフサイクル管理などが含まれる。その関連業務として、しばしば継続的なサポート業務やヘルプデスク業務が挙げられる。後者には、エンドポイントセキュリティ技術の導入が含まれる。その他の関連業務としては、ポリシーの施行、脅威の監視、インシデント対応を始めとするセキュリティ環境の継続的な管理などがある。

これら 2 つの領域は常に重なり合っているが、チームはそうはなっていない。ポリシーの施行は、OS 構成とセキュリティコントロールの双方にまたがる。エンドポイントセキュリティソフトウェアのインストール自体は、IT 運用の業務領域である。脆弱性管理（検出とパッチ適用）とコンプライアンスに対する責任を考慮すると、境界はさらに曖昧になる。

この点に関して、グローバルな IT チームの多くは、いまだばらばらなままであるが、これらのチームが統合し始めていることを示す兆候はある。IDC は、大手企業および中堅企業の IT 意思決定者 1,524 人を対象にグローバル調査を実施し、チームとツールを統合してエンドポイントの管理とセキュリティの一貫性を高める統合型エンドポイント管理の概念に関して、エンドユーザーのデバイス管理とセキュリティに対するアプローチ、およびこれらの機能の交わりについてたずねた。



IDC では、今回の調査に加え、Tanium（タニウム）のエンドポイント管理／セキュリティツールのプラットフォームを部分的または全面的に使用している企業の IT セキュリティおよび IT 管理の専門家 4 人に詳細なインタビューを実施した。以降のセクションでは、XEM の利点と課題、および Tanium 独自の XEM アプローチについて取り上げる。

統合型エンドポイント管理の利点

リスクと複雑さの低減

エンドポイントデバイスの管理チームとエンドポイントセキュリティチームは、機能、ツール、プロセスの統合という点ではかなり前進しているものの、多くのグループが依然として複雑さという問題を抱えている。エンドポイント管理チームとエンドポイントセキュリティ運用チームに共通する主な業務の一つは、新たな脅威の継続的な特定と脆弱性に対するパッチの適用である。エンドポイント環境のリスク可視化のために、各チームが類似しているが別々のツールを利用してセキュリティアラートや、ログを収集している状況が、よく見られる。こうした行動は、往々にして、協調性がない上に、無駄が多く、最悪の場合、非生産的なものとなってしまう。

監査とデータのスプロール化（無秩序な拡大）を削減するアナリティクス

企業のエンドポイントデバイスの管理とセキュリティを担当するチームはいずれも、監査範囲の縮小や、少なくともコンプライアンスプロセスの合理化という既得権益を有している。このようなタスクは管理業務とセキュリティ業務にまたがることが多い。というのも、エンドポイントのオペレーティングシステムやデバイスの構成から、機密データの保存場所、特定のセキュリティツールや機能（エンドポイントのマルウェア対策や暗号化など）の有無に至るまで、要求される項目は多岐に渡るためである。

脅威の監視と検出は重要であるが、エンドポイントには潜在的に機密情報が保存される可能性がある。ある種の規制対象データや機密データがエンドポイントに不用意に保存された場合、企業は重大なコンプライアンス違反や規制当局による罰金に直面する恐れがある。

本調査レポート用に IDC がインタビューした、アジア太平洋地域に拠点を置く大手高齢者向け介護サービス会社を例に挙げると、この企業は XEM アプローチを用いて機密データのスプロール化に対処している。同社の使命の一つは、高齢者や移動が困難な患者の自宅で彼らの体調を確認す

ることであるため、フィールドワーカーが現地まで出向いて、モバイルコンピューターでデータを収集する必要がある。同社が直面している特定の課題は、従業員や家庭訪問員の新型コロナウイルス感染症予防接種証明書（電子版）を収集し、検証するための要件が強化されたことに起因している。この証明書には健康に関わる機密情報が含まれており、いかなるエンドポイントにも保存してはならないとされている。

「（我々が答えを出す必要があった）問題は、当社の環境のどこに新型コロナウイルス感染症予防接種証明書があるのかということでした。Tanium プラットフォームのおかげで、当社のランドスケープ全体を横断的にスキャンして、エンドポイントデバイスに存在するこれらの証明書のインスタンスをすべて見つけることができました」と、同社のサイバーセキュリティ、リスク、コンプライアンス（CRC：Cybersecurity, Risk, and Compliance）部門の責任者は述べている。その結果、同社は新しい要件を満たし、コンプライアンスを維持することに成功した。

リアルタイムでの脆弱性／脅威の検知

企業の IT 運用チームとセキュリティチームは、脆弱性に関する問い合せだけでなく、導入されたエンドポイントデバイス群の全体的な状態やステータスについても、迅速に回答する必要がある。新たな脆弱性がベンダーアラート速報や技術専門誌、オンラインフォーラムで取り上げられた場合、企業は、運用チームにネットワーク上のすべてのシステムに対する長時間の監査や評価を課すことなく、自社がその脆弱性にさらされているかどうかを把握しなければならない。IDC の調査では、エンドポイントの状態をリアルタイムで可視化することは、XEM 中心のプラットフォームが提供する機能の中で最も望まれているものであり、58%の企業が必須であると回答している。

XEM アプローチには、重要な要件である脅威の検出、パッチ適用、修復を迅速に行うツールが含まれる。前述の高齢者向け介護サービス会社の CRC 責任者は「過去に行ったパッチ適用は、オペレーティングシステムに関するものばかりでした。現在は、実際に何がインストールされているかを確認できるようになったため、サードパーティ製アプリケーションのどのバージョンが古いのか、あるいは期限切れになっているのかが分かるようになりました。従業員の PC に搭載されているマイクロソフトのオペレーティングシステム（にパッチを適用する）だけでなく、サードパーティ製アプリケーションにもパッチを適用できるようになりました」と述べている。

影響力の大きいマルウェアや標的型サイバー攻撃（WannaCry、NotPetya、Log4j など）に対するより迅速な対応の必要性が、同社における Tanium XEM ソリューションの導入を後押しすることとなった。Tanium 導入前は、重大な脆弱性への暴露に関する報告書の作成や、環境内に潜む危険なマルウェアの検出は、非常に時間がかかるものであった。「以前のプラットフォームでは、どのシステムに脆弱性が潜んでいるのかを知るのに丸一日かかっていました」と、同社の CRC 責任者は述べている。丸一日脆弱性にさらされるとなると、システムやデータに侵入するのに十分すぎるほどの時間を攻撃者に与えてしまうことになる。

エンドポイントのセキュリティと管理の統合を目指す企業にとって重要な目標の一つは、脆弱性の検出と影響を受けるソフトウェアへのパッチ適用との間のギャップを埋めることである。高齢者向け介護サービス会社の IT チームは、この利点を実感していた。CRC 責任者はこう語る。「影響を受けたシステムにパッチを迅速に適用できたため、エンドポイントのコンプライアンスは極めて短い期間で 1%から 90%以上へと急上昇しました」

「Tanium のおかげで、影響を受けたシステムにパッチを迅速に適用できたため、エンドポイントのコンプライアンスは極めて短い期間で 1%から 90%以上へと急上昇しました。以前のプラットフォームでは、どのシステムに脆弱性が潜んでいるのかを知るのに丸一日かかっていました」CRC 責任者

予防優先のセキュリティ

予防優先のセキュリティは、デバイスの衛生管理（ハイジーン）におけるベストプラクティスである。XEM はこのアプローチを強力に支援する。デバイスの衛生管理（OS やサードパーティ製アプリケーションを含むソフトウェアのパッチ適用と更新）とセキュリティ（アプリケーションホワイトリスト、ポリシー設定）の慣行と手順を改善することで、XEM を中心に据えている企業は、アタックサーフェス（攻撃対象領域）を狭め、侵害に対する全体的なリスクと脆弱性を低減できる。

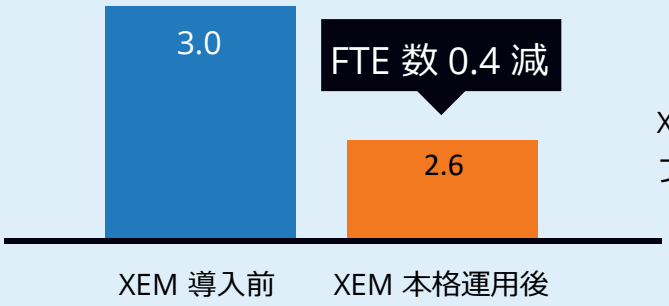
もう一つの予防優先アプローチとして、デバイス上で動作するソフトウェアのフットプリントを削減することが挙げられる。これには、アプリケーション数やソフトウェアパッケージ数の抑制も含まれる。デバイスのユーザー権限によっては、未承認のアプリケーションやプログラムがユーザー環境にダウンロードされ、インストールされるという危険な領域まで、アプリケーションのスプロール化が進む恐れがある。その結果、エンドユーザーのソフトウェア環境について、企業の IT 部門が把握できている部分だけでなく、把握できていない部分についても、懸念が生じる。

コストの削減

企業のエンドポイント環境における複雑さは、コストと密接に関連している。複雑な環境ほどコストが高くなり、効率的で複雑でない環境ほど運用や維持にかかる費用が抑えられる傾向にある。企業は、使用するテクノロジーの数を減らすことでコストと複雑さを低減できる。複数のプラットフォームを維持し、運用するためには、より多くのスタッフが必要となることを考えると、このアプローチは最も効果的なコスト削減策の一つであると言える。

IT部門とセキュリティ部門のスタッフ

（サポート対象のエンドユーザー用デバイス100台当たりのFTE（Full-Time Equivalent）数）



XEM 導入後、従業員用デバイス 200 台につき
フルタイム従業員 1 人分の人件費削減を実現

ベンダーとツールの統合

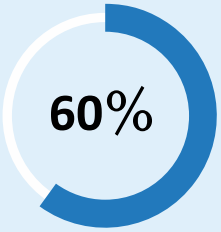
企業はさまざまな理由から、複数の管理ツールやセキュリティツールを使用している。IDC の調査では、米国企業の半数以上が、複数のエンドポイント管理およびセキュリティ製品／ベンダーを使用して、さまざまな種類のエンドポイント（Windows、Mac、Linux、モバイルデバイスなど）を管理している。セキュリティ製品の中には、エンドポイント保護（EPP：Endpoint Protection

Platform）や検出および対応（EDR：Endpoint Detection and Response）など、特定の機能に秀でたものや特化したものがある。

大企業や多国籍企業では、各地域の状況（特定のテクノロジーやベンダーの知名度や、特定の場所でしか利用できないなど）によって、使用するツールが異なる可能性がある。

一方、ベンダー統合を成功させるには、脆弱性管理、資産管理、コンプライアンス、ファイル整合性監視、セキュリティ構成管理、脅威対応に使用される単一目的のツールの使用を廃止する必要がある。前述の機能すべてを組み込んだ統合レポート機能も利点となる。

多くの企業が複数の製品の使用に伴う複雑さから抜け出せずにいる今、60%の IT 意思決定者が、エンドポイントの管理とセキュリティの両面において使用するベンダーとツールの数を減らしたいと考えている。その主な理由として、コスト削減や複雑性の解消、高度な機能を利用可能にすることなどが挙げられる。



60%のIT意思決定者が、エンドポイントの管理とセキュリティの両面において使用するベンダーとツールの数を減らしたいと考えている。

XEM に組み込まれた機能によって製品全体の置き換えを実現

あるグローバルな物流企業では、複数のセキュリティツールを統合することで、ソフトウェアのライセンス費用とサブスクリプション費用を半減させ、年間数十万ドルのコストを削減できたと述べている。同社は、資産の管理と検出を目的として Tanium XEM を導入したが、導入後に、ファイル整合性監視などの他の分野のツールを置き換えられるモジュールと機能が XEM プラットフォームに組み込まれていることを発見した。初期の段階でこのような統合を行ったことで、支出の大幅な削減に成功した。このコスト削減は、以前の製品から Tanium XEM への置き換えを決断する上で十分な決め手となった。

「複数のセキュリティツールを統合することで、ソフトウェアのライセンス費用とサブスクリプション料金を半減させ、年間数十万ドルのコストを削減できました」

グローバルな物流会社のテクニカルディレクター

「人は自分が使い慣れているものを変えたがらないものです。これまで何度もそのような場面を目にしてきました」と、物流会社のテクニカルディレクターは言う。しかし、Tanium に一本化し

た結果、大幅なコスト削減が実現したことで、同社内のそうした考えは一変した。「あまりにも多額の費用を削減できたため、ただ慣れ親しんだものだからという理由だけで、大切にしてきたものを残しておきたいという気持ちを誰も擁護できませんでした」と述べている。

Tanium を使用してセキュリティ機能と管理機能を統合したことで、この物流会社では多くの手作業によるプロセスが排除された。「以前は、資産やアプリケーションを追跡するために、スプレッドシートのような手法が多く用いられていました」とテクニカルディレクターは話す。同社は現在、IT 資産の検出とインベントリーのために Tanium XEM プラットフォームを導入し、IT 資産の全体像をより正確かつ自動的に把握できるようになっている。このような自動化レベルの向上と効率化は、Tanium ソリューションの大規模導入の副産物としてもたらされたものである。同社は、コスト増を伴うことなく資産管理の簡素化と質を向上させ、同時に全体的な IT 支出を削減した。

米国のある大手医療機関では、XEM の導入によって年間 100 万ドル以上のコスト削減を実現したと試算している。IT スタッフは、Tanium ソリューションが、別のベンダーから購入している資産追跡機能を備えていることに気づき、すぐに二重払いをやめた。

「XEMを選択したことで、複数の製品を置き換え、他の製品から機能を引き継げたため、年間100万ドル以上の節約になりました」

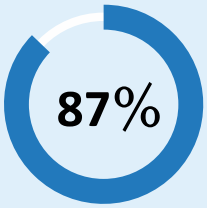
米国の大手医療機関のエンドポイント管理ディレクター

統合と機能拡張

コスト削減は、多くの企業において XEM 導入の推進要因となっている。IDC の調査では、北米を拠点とする企業の IT 意思決定者の 87%が、今後 18 か月以内に複数のエンドポイント管理製品をシングルベンダーソリューションに統合する予定であると回答している。半数以上の企業は、さらにペースが速く、今後 6〜12 か月以内に統合することを検討している。

その目標は、より少ないリソースでより多くのことを行うこと、つまり単一のソフトウェア製品やプラットフォームからより多くの機能、特徴、能力を引き出すことである。IT チームがガバナンス、リスク、コンプライアンスに関する要件の増加に直面する中、単一のプラットフォームの機能を複数のチームに拡張できる XEM の機能は、このグローバルな物流企業にとって非常に貴重なものであった。

「SOX（Sarbanes-Oxley Act：サーベンスオクスリー法）や HIPPA（Health Insurance Portability and Accountability Act：医療保険の携行性と責任に関する法律）を始めとするあらゆる規制要件に対応する必要があると分かったとき、GRC（Governance, Risk, and Compliance：ガバナンス、リスク、コンプライアンス）チームは、全般的な PC 導入を管理するチームよりも早く拡大しました」と物流会社のテクニカルディレクターは言う。GRC チームは自らの拡大に伴い、複数のコンプライアンスソフトウェア製品やツールを購入していった。その結果、IT 支出は驚くべきスピードで増加した。



IDCの調査では、北米を拠点とする企業のIT意思決定者の87%が、自身の企業において今後18か月以内に複数のエンドポイント管理製品をシングルベンダーソリューションに統合する予定であると回答している。

この物流会社の GRC チームは、自社の成長と新規ビジネスの獲得をサポートするため、Tanium XEM プラットフォームを活用して、認定とコンプライアンスのチェック作業を完了した。これによって、継続的に事業を行う上で重要な要件である、セキュアで信頼性の高い IT 環境を同社が確立していることをパートナーや顧客に周知できた。

より大きなコラボレーションの創出

XEM のベネフィットを最大限に生かすには、運用チーム間でより高度なコラボレーションを浸透させる必要があることを企業は認識している。しかし、チーム横断的なコラボレーションを強制することは、成功への近道ではない。有機的なコラボレーションの促進こそが優れたアプローチであり、これによってチームは新たなコラボレーション手段を見出し、結果に対して責任を持てるようになるのである。

さらに、コラボレーションを発見し、育むことができる場も必要である。ここで XEM の本領発揮となる。米国のある大手医療機関は「エンドポイント管理チームとエンドポイントセキュリティチームは、以前はうまくコラボレーションができていませんでしたが、＜中略＞（当機関では）Tanium XEM は同じサンドボックスに入っており、そのサンドボックスから、より大きなコラボレーションが生まれています」と述べている。

場合によっては、コラボレーションは必要に迫られることもある。あるグローバルなソフトウェア企業のケースでは、2023 年に強制的なダウンサイジングが行われ、IT チームとセキュリティ運用チームにおいて 4 人（約 30%）のフルタイム従業員が削減された。同社はすでに Tanium XEM プラットフォームに移行しており、IT チームとセキュリティチームが Tanium 上で統合され、同じデータセットを利用してリアルタイムに連携できたため、人員削減の影響を緩和しながら、IT チームとセキュリティチームのモダナイゼーションを継続できた。

従業員エクスペリエンスの改善

エンドポイントセキュリティチームとエンドポイント管理チームが管理監督するデバイスの使用からも部分的にもたらされる従業員エクスペリエンスは、非常に重要である。従業員エクスペリエンスが劣っていると、生産性が低下し、組織が自分の貢献をどのように評価しているかに関する認識にマイナスの影響を及ぼす。

エンドポイントセキュリティ機能とエンドポイント管理機能は、従業員の活動の妨げを最小限に抑えるために、ユーザーにほぼ影響を与えないアプローチをとる必要がある。しかし、影響を最小限に抑えることは、XEM の目標の出発点にすぎない。XEM は、従業員のデバイスを詳細に、ほぼリアルタイムで可視化することで、ユーザーに影響を与える状況が迫っている前兆を検出し、ユーザーにマイナスのエクスペリエンスがもたらされる前にその問題を解決できる。IDC の

調査から、XEM を導入した企業において、影響が最小限に抑えられたと同時に、従業員エクスペリエンスの低下が回避されたという事実が明らかになった。

「IDCの調査から、XEMを導入した企業において、XEMの運用が従業員の活動に与える影響が最小限に抑えられ、従業員エクスペリエンスの低下につながるような状況が未然に回避されたという事実が明らかになった」

ハンズオフによる更新頻度とパッチ適用の加速

XEM プラットフォームを本格的に運用している企業とそうでない企業を比較した IDC の調査結果では、XEM を本格的に運用している企業では、Windows のパッチ適用、更新、アップグレードの実装頻度が 22%高く、セキュリティ体制が強化されていることが分かった。また、XEM を本格的に運用している企業では、展開時間が短く、更新プログラムがリリースされると自動的に展開されることが多く、スタッフの生産性も向上している。

さらに、Tanium の一部の顧客から IDC に寄せられた話によると、Tanium を導入する前は、従業員のデバイスに新しいアプリケーションを導入する際に手作業で行っていたため、ユーザーが利用できない時間が長時間に及び、場合によっては、従業員が導入作業に直接関わらなければならなかったということであった。Tanium の導入後、新しいソフトウェアアプリケーションはセルフサービス方式でインストールされるようになった。セルフサービス方式によって、ユーザーエクスペリエンスが改善されただけでなく、エンドポイント管理スタッフの作業時間が短縮され、ソフトウェアの運用開始時期が早まった。

性能の低い機器の排除

Tanium の顧客数社から、「見えないものは守れない」という格言が引用された。また、「従業員がどのような機器を使っているかを知らなければ、従業員に適切な機器を提供できない」という意見も聞かれた。つまり、ある企業では、ユーザーが必要不可欠なビジネスアプリケーションを古くて性能の低い PC で実行していることを知らず、ソフトウェアとハードウェアの不一致を検知する手段も持ち合わせていなかった。Tanium のあるユーザー企業は、「静かな退職（Quiet Quitting）」の可能性を懸念し、XEM プラットフォームから収集したデータを使用して、ソフトウェアとハードウェアの不一致を特定し、より古い PC から順に交換を行った。この取り組みは、従業員のエクスペリエンスを IT チームが真剣に考えていることを再確認させるメッセージとなった。

プロアクティブな監視によるヘルプデスクチケットの減少

IT ヘルプデスクチケットは、企業にとって二重のリソース負担となる。第 1 に、従業員によって発行されたということは、そのチケットは、ユーザーの業務のルーチンや生産性に悪影響が生じていること、従業員が不満を抱いていることを意味する。第 2 に、IT チームはチケットの調査と解決に時間とリソースを割かなければならない。結論として、ヘルプデスクチケットは企業にとって損失であるため、賢明な手段はチケットを削減する方向で管理する以外にない。

XEM プラットフォームでは、分析エンジンを調整して、新たなパフォーマンスの問題を検出することが可能である。同様に、エンドポイントセキュリティチームとエンドポイント管理チームがエンドポイントに対処するために使用するのと同じ精選されたメカニズムによって、性能に影響を及ぼすイベントを修正できる。

その結果、ネガティブな従業員エクスペリエンスや数え切れないほどのヘルプデスクチケットを回避できる。XEM では、IT 担当者は使い慣れたプラットフォームから操作でき、さらに最も重要なことに、XEM は、従業員のパフォーマンス管理とヘルプデスクのチケット発行業務を、コストのかかるリアクティブ（事後対応型）から従業員のルーチン作業をルーチンのまま維持するのに役立つプロアクティブ（事前対応型）へと転換するよう促す。

実現される Tanium XEM の価値

Tanium は、その基盤となる特徴的なアーキテクチャと、リアルタイムデータ、分析、ワークフローを単一のプラットフォーム（クラウドかオンプレミスかを問わず）に統合する能力をベースに、XEM の価値を顧客に提供するのに絶好のポジションにある。

IDC の詳細なインタビューでは、XEM を導入した企業が、Tanium プラットフォームの包括性と信頼性について度々言及していた。IT フットプリントの動的な性質と複雑さ、そして至る所に潜むサイバー攻撃の脅威の不確実性を考慮すると、IT 資産全体に渡って包括的かつ最新の可視性が確保されていない企業は、IT チームとセキュリティチームの行動が組織としての意図に合致しているかどうか分からないというハンディキャップを抱えている。

さらに、今回の IDC の調査と詳細なインタビューの両方において、予防優先セキュリティアプローチの重要性、成果を犠牲にすることなくソフトウェアのライセンス費用を削減する必要性、ベンダーの統合を通じてチーム横断的なコラボレーションを高めたいというニーズが確認された。以前は、分離した個別のデータストアやテクノロジーが正当化されていたかもしれないが、現在ではあまり適切ではない。企業は、信頼できるパートナーが提供する幅広い機能を備えたプラットフォームアプローチを求めている。

企業が XEM の利点を実現するための手段であるこのプラットフォームアプローチは、一晩で出来上がるものではない。むしろ、企業の進化するニーズに段階的に対応するよう、漸進的に構築、改良されている。さらに、以下のような Tanium XEM プラットフォームのネイティブな機能に基づいて構築されている。

- **リスクとコンプライアンスの管理**：チームは、ファイルやレジストリーの変更を監視でき、プライバシーに関する規制や慣行の遵守を確保できる。
- **クライアントの管理**：すべてのシステムは、自動化されたパッチ適用と最小限のダウンタイムによって、常に最新の状態に保たれ、稼働し続けることが可能である。
- **脅威ハンティング**：プロアクティブなアプローチでは、脅威ハンターがシステムをくまなく調査し、セキュリティ侵害の証拠をフォレンジック調査によって見つけ出し、リスクを特定し、攻撃者が損害を与える前に一掃する。
- **資産の検出とインベントリー**：コンバージドプラットフォームによって、ハードウェア資産とソフトウェア資産の完全なインベントリーを容易に入手できるようになる。
- **機密データの監視**：機密データを追跡、管理することで、攻撃者からデータを保護できる。
- **サービス管理**：IT チームは、従業員に対してより適切なサポートを提供でき、ヘルプデスクチケットの解決も可能となる。チームは、正確なリアルタイムデータを使用して、合理化されたヘルプデスクのワークフローを作成できる。
- **場所を選ばない有効性**：コンバージドプラットフォームは、リモートワークを行う、分散して働く従業員をサポートし、IT の問題を未然に解決する。

プラットフォームモデルとは、統合された機能だけでなく、顧客とプラットフォームプロバイダーとの関係も含まれる。顧客に対するインタビューでは偏った見解が示されることもあるが、Tanium の顧客による証言は信憑性の高いものであることから、Tanium と顧客の関係を示す以下の側面については繰り返し述べるに値する。

- **目に見える価値**：Tanium のテクニカルアカウントマネージャーは、より深く、より効果的なプラットフォームの利用を促進するのに役立っていると評価されている。ある顧客が焦点を合わせたように、Tanium はマネージドサービスプロバイダーを雇うよりも有力な選択肢となる。
- **予防優先**：デジタル世界では、脆弱性は避けて通れないものである。脅威アクターは、新しいソフトウェアとレガシーソフトウェアの両方で新たに見つかった脆弱性に飛びつくため、エンドポイントセキュリティチームとエンドポイント管理チームは、対策を実行できるように、新たな脅威を効果的に突き止める脆弱性スキャンスクリプトを迅速に作成しなければならない。脆弱性スキャンスクリプトの作成における、複雑さを問わない Tanium のプロアクティブな姿勢は、予防優先のセキュリティアプローチを証明するものとして、顧客から高く評価されている。
- **ベンダーというよりむしろパートナー**：プラットフォームモデルは、モジュールを実際のニーズに合わせるのではなく、顧客の支出総額を増やそうとする過剰なアカウントチームによって利用される危険性がある。IDC のインタビューに応じた Tanium の顧客は、企業規模の大小を問わず、顧客のニーズと時間枠に最も適したモジュールの組み合せを見つけるという Tanium の真摯な努力を評価しており、取引上のベンダー関係というよりもパートナーの関係を形成している。

課題と機会

価格交渉力の喪失の可能性

複雑なマルチベンダー環境は、可視性のギャップや機能の阻害、全体的なコストの上昇を招く恐れがあるため、企業にとってリスクとなり得る。しかし、IT グループがベンダーを絞り込み、機能を数社、あるいは 1 社にまで集約した場合、価格交渉力を失ってしまいかねない。かつては、複数の企業を競合させて最良の価格を引き出していた企業も、単一のソースやプロバイダーに依存しすぎると、身動きが取れなくなる恐れがある。とは言え、ちょっとした機能の追加やアップグレードによる段階的なコスト削減は、ツール数を削減することで実現される全体的な効率向上やコスト削減によって相殺されることが多い。

ログ収集プラットフォームとの統合の課題

顧客が XEM 導入のもう一つの潜在的な課題として挙げたのは、セキュリティ情報イベント管理（SIEM：Security Information and Event Management）プラットフォームのストリーミングログなど、サードパーティ製システムとの統合であった。

企業が標準化するベンダーの種類によっては、異なる導入テクノロジーへの適応も課題となる可能性がある。導入の選択肢をすべて挙げると、オンプレミス型、クラウド型、ハイブリッド型があるが、一般的に業界はクラウド型とハイブリッド型に向かいつつある。

サーバーに関する検討

多くの企業において、エンドポイント管理とエンドポイントセキュリティの境界が曖昧になっているように（デスクトップ PC、ノートブック PC など）、サーバーエンドポイントと従業員用デバイスの責任分界点も曖昧になっている。サーバー、PC、モバイルデバイスなどあらゆるエンドポイントを、管理／セキュリティのための単一の領域とみなし、各チームにおいて責任を分担したり、構成や脅威を個別に管理したりしている企業もある。XEM アプローチを検討している企業は、サーバーエンドポイントが重要な要素であるかどうかを判断する必要がある。これは、データセンターチームがバックエンドのシステム管理、セキュリティ、パッチ適用といった各業務を

担当しているような大企業ではすでに判断されていることかもしれない。中小企業や一部の大企業では、単一の IT チームや専門的なサブグループがこれらの責任を担っている。

XEM ツールや XEM アプローチには、バックエンドのデバイスやシステムも含まれることがある。Tanium の XEM プラットフォームの場合、サーバーの管理やセキュリティも機能として含まれる。多くの企業は、バックエンドサーバーの仮想化やコンテナ管理インフラストラクチャに加えて、Tanium XEM の脆弱性スキャン、リアルタイムの脅威テレメトリー、および高速パッチ適用機能を Windows、Linux、UNIX のサーバーに拡張することで価値を享受できる。これらのユースケースについては、イニシアティブの開始時に注意深く説明し、XEM の導入プランに組み込んでおく必要がある。

結論

IDC の調査では、企業はエンドポイントセキュリティとエンドポイント管理を XEM プラットフォームに移行することで、大きなベネフィットを実現していることが明らかになった。第 1 に、XEM プラットフォームは、チームを統合しサイバーリスクを低減する。企業のエンドポイント資産全体に関する「Single Source of Truth」（信頼できる唯一の情報源）があれば、2 つのチームは予防優先のセキュリティに注意を注ぎ、それに対する取り組みを連携させ、デバイスの衛生管理（ハイジーン）と脆弱性管理の実践を通じて、アタックサーフェスを狭めることが可能となる。第 2 に、XEM プラットフォームの使用経験を共有することで、各チームが協力して、総合的な生産性を向上させる環境が生まれる。第 3 に、ベンダーの統合によって大幅なコスト削減が可能であり、Tanium の顧客エクスペリエンスに基づけば、それは近い将来に実現可能である。第 4 に、Tanium XEM の基盤となるプラットフォームアプローチは、既存のインフラストラクチャ（エンドポイントのエージェント、データベース、分析エンジン）を活用し、全体的な従業員エクスペリエンスの改善やヘルプデスクチケットの回避など、組織のさらなる目標の達成を支援する。

IDC 社 概要

International Data Corporation（IDC）は、IT および通信分野に関する調査・分析、アドバイザリーサービス、イベントを提供するグローバル企業です。50 年にわたり、IDC は、世界中の企業経営者、IT 専門家、機関投資家に、テクノロジー導入や経営戦略策定などの意思決定を行う上で不可欠な、客観的な情報やコンサルティングを提供してきました。

現在、110 か国以上を対象として、1,100 人を超えるアナリストが、世界規模、地域別、国別での市場動向の調査・分析および市場予測を行っています。

IDC は世界をリードするテクノロジーメディア（出版）、調査会社、イベントを擁する IDG（インターナショナル・データ・グループ）の系列会社です。

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200
Twitter: @IDC
blogs.idc.com
www.idc.com