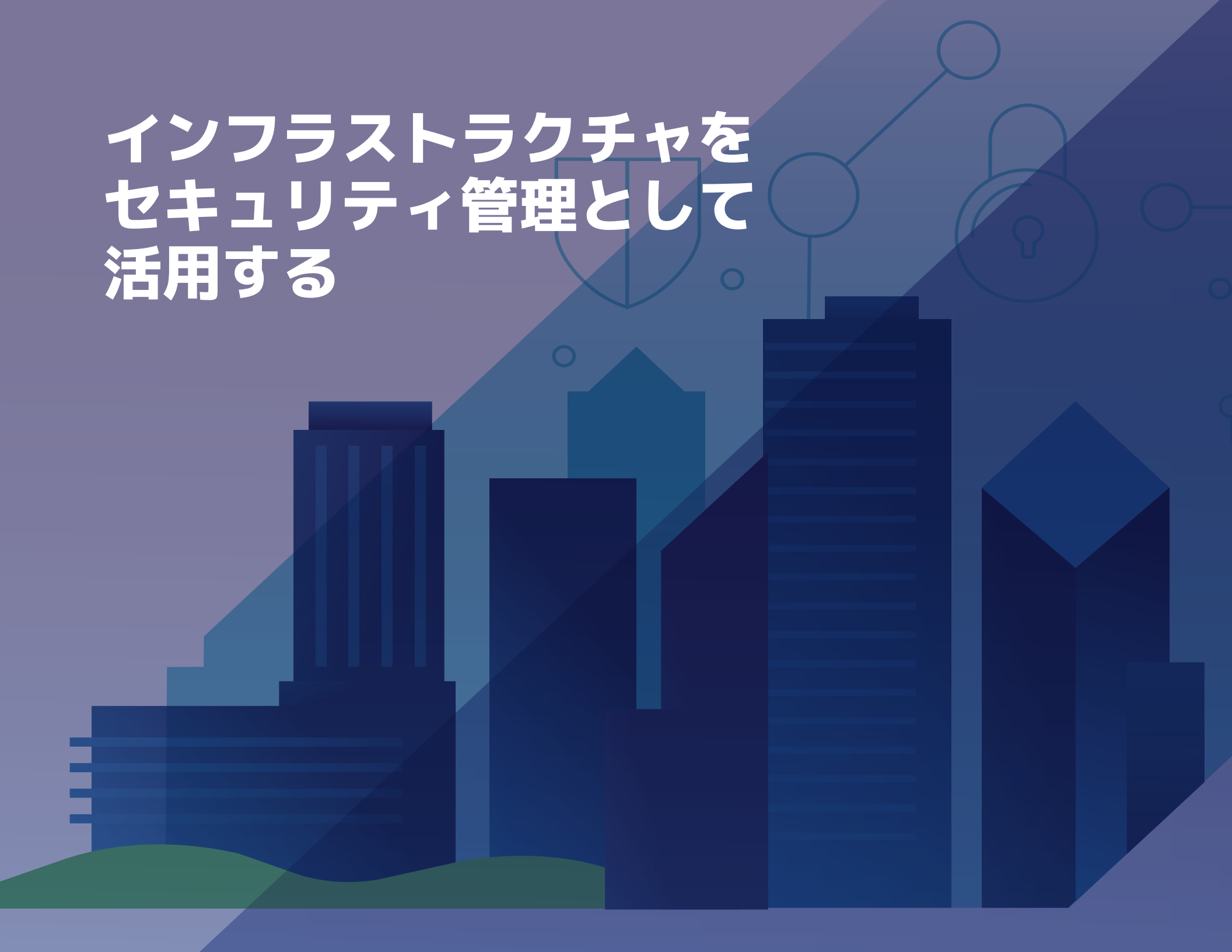
インフラストラクチャを
セキュリティ管理として
活用する



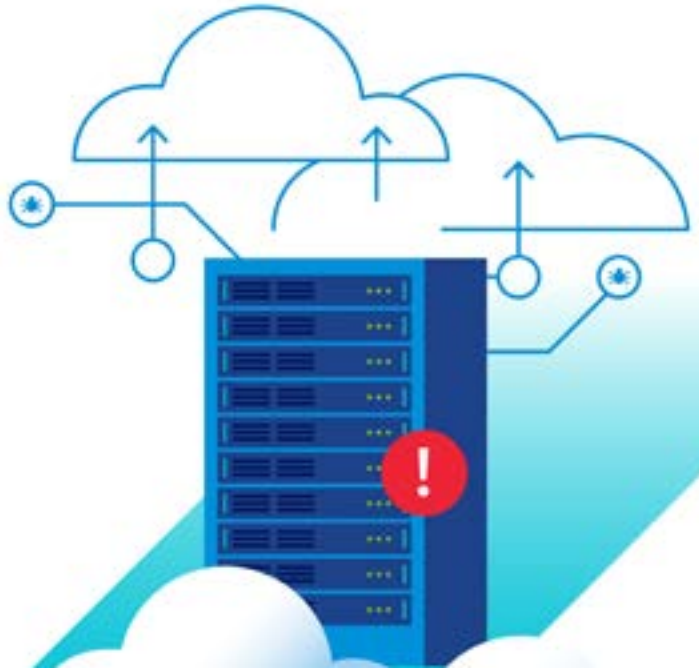
ここでの課題：

複雑化がワークロードの保護を妨げている

急速に拡大する攻撃対象領域は、そのまま放置すると脆弱性となります。ほとんどの組織は数十あるいは数百のセキュリティ ツールを使用していますが、一方で脅威の数は日々増えており、そこから生じるギャップが攻撃者の標的となっています。

Forbes のレポート『Cybersecurity Trailblazers』（2019 年）によると、セキュリティ担当者の 77% が、追跡と管理の対象となる単体製品が多すぎると回答しています。

複雑化は過剰なコスト増を招き、また IT 部門にとっても、すべてのワークロードにセキュリティ エージェントをインストールして常に最新の状態に維持するのは大変な作業です。セキュリティ担当者はシステム インテグレーターさながらに、多数の異なるセキュリティ製品をつなぎ合わせるためのスクリプトを絶えず記述しなければなりません。同時に、部門間の連携が難しいことから、だれもが不満を募らせています。



25 のコスト要因のうち、もっとも費用がかさむのがセキュリティ システムの複雑さで、侵害発生時には平均 292,000 ドルのコスト増を招き、補正後の平均では総額 415 万ドルに達します。

IBM、『Cost of a Data Breach Report 2020』

考えられる解決策：

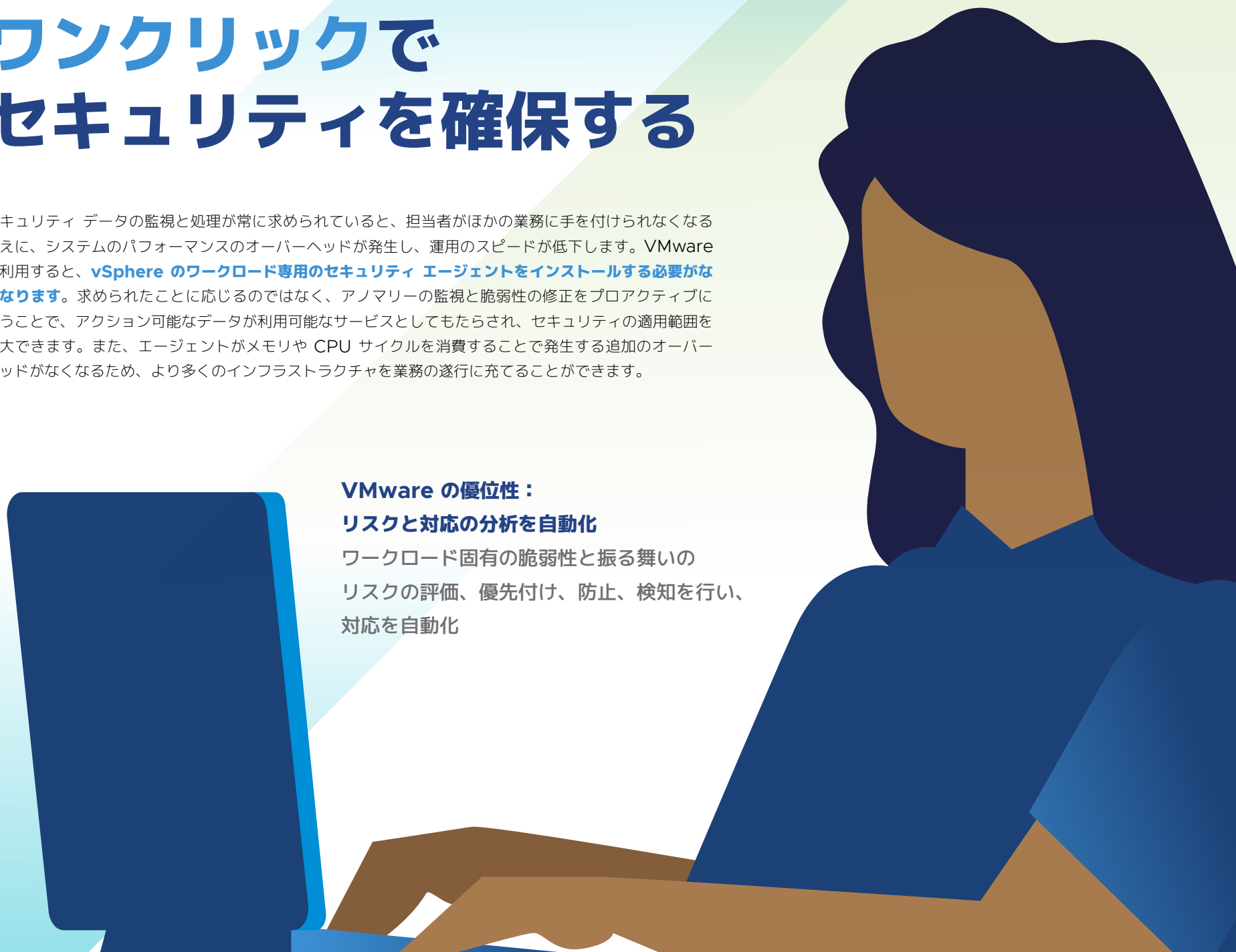
運用上の障害を取り除く

セキュリティとインフラストラクチャの連携、そしてその担当チームの積極的な参加がなければ、労力をかける意味がありません。VMware とパートナーシップを組めば、**セキュリティ データの収集プロセスを合理化**できるようになります。また、**高度なセキュリティ機能を拡張**して vSphere Client コンソールに組み込むことも可能になります。さらに、**複数のユースケース間でポリシーの整合性を確保**することもできるようになります。

その仕組みの説明はこちら

ワンクリックで
セキュリティを確保する

セキュリティ データの監視と処理が常に求められていると、担当者がほかの業務に手を付けられなくなるうえに、システムのパフォーマンスのオーバーヘッドが発生し、運用のスピードが低下します。VMware を利用すると、**vSphere のワークロード専用のセキュリティ エージェントをインストールする必要がなくなります**。求められたことに応じるのではなく、アノマリーの監視と脆弱性の修正をプロアクティブに行うことで、アクション可能なデータが利用可能なサービスとしてもたらされ、セキュリティの適用範囲を拡大できます。また、エージェントがメモリや CPU サイクルを消費することで発生する追加のオーバーヘッドがなくなるため、より多くのインフラストラクチャを業務の遂行に充てることができます。



VMware の優位性：
リスクと対応の分析を自動化

ワークロード固有の脆弱性と振る舞いの
リスクの評価、優先付け、防止、検知を行い、
対応を自動化

脅威とリスクの分析を自動化する

手作業に頼ると進捗が遅くなり、視野が狭くなります。VMware では、脆弱性を評価しインシデントを調査するためのワークロード分析を自動化できます。また、環境全体を通してもっともリスクの高い振る舞いをより迅速に特定し、首尾一貫した偏りのない方法でポリシーを適用することが可能です。さらに、対象システムの強化のために脅威の優先順位付けを行いながら、コンプライアンスに違反する行為を防止することもできます。VMware のエコシステム内では、一貫性のある API と統合機能を使用した自動化が容易に実現可能です。

VMware の優位性：

リスクと対応の分析を自動化

ワークロード固有の脆弱性と振る舞いのリスクの評価、優先付け、防止、検知を行い、対応を自動化

単体セキュリティ ツールの数を減らす

別々のコンソールを常に行き来しながら、すべてのセキュリティ ポリシーの整合性を確保することは至難の技です。VMware の統合ツールセットを使用すると、ワークロードのライフサイクル全体を通して、セキュリティ アプリケーションの制御を簡単に定義、調整、監視することができます。スタックを連携させるためのスクリプト作成も、複数のエージェントもトレーニングも不要になります。さらに、セキュリティ チームとインフラストラクチャ チームが、適切なコンテキストに基づいて同じ情報にアクセスできるため、環境全体で一貫したセキュリティを推進することが可能です。

VMware の優位性：
セキュリティを単一のプラットフォームに統合、エージェントは不要

応答、検知、防止、監査など、vSphere の運用管理に統合された複数のセキュリティ ユースケースの整合性を確保できる

運用上の障害要因を解消すると、エージェントなしのスムーズな使用環境を実現し、リスクと対応の分析を自動化し、セキュリティを単一のプラットフォームに統合することができます。

VMware 導入の効果：

セキュリティ ソリューションの導入と管理に費やす労力を減らし、IT 環境をより効果的に活用

精度の高いアラートにより、的確なアクションを迅速に実行

将来的な脅威に備える強化を行うための調整をより容易かつ効果的に実施

詳しくは **VMware のサイト**をご覧ください