Enterprise Strategy Group
By TechTarget

### ハイブリッドクラウドやマルチクラウド環境に適した

# 強靭なセキュリティで<br>ビジネスの成長を後押し

今日、組織はデジタル トランスフォーメーションや生産性の最適化、イノベーションへの対応を求められていますが、ハイブリッドクラウドとマルチクラウド環境にわたってワークロードを保護できるセキュリティもおろそかにはできません。シスコは展開された場所を問わずアプリケーションを保護できる最新のセキュリティを提供し、お客様の開発速度の向上とビジネスの成長を後押しします。

このインフォグラフィックは、シスコの委託を受けて Enterprise Strategy Group が作成したものです。
本紙は TechTarget, Inc. のライセンスに基づいて配布されます。

## 分散環境全体のアプリケーションを保護できるセキュリティのニーズ

基盤となるインフラや保守の問題に煩わされずに最先端のコンピューティング プラットフォームを利用するべく、パブリッククラウド インフラストラクチャを活用しようという動きが組織に広がっていますが、同時にオンプレミス環境のアプリケーションをサポートすることも求められています。こうしたニーズがクラウドサービスへの移行を難しくし、複数のクラウドプラットフォームやオンプレミス環境に分散しているワークロードの管理を困難にする課題として、セキュリティチームの前に立ち塞がっています。

**現在**

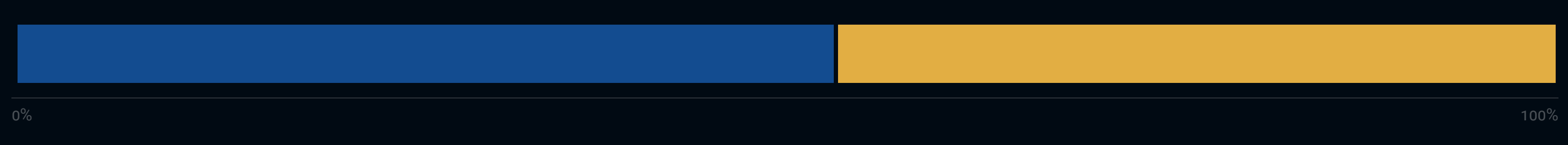
**パブリッククラウドサービス（IaaS、PaaS など）**上で稼働している生産性向上アプリケーション / ワークロードの割合
**49%**

**オンプレミス インフラストラクチャ**上で稼働している生産性向上アプリケーション / ワークロードの割合
**51%**

**現時点から 24 か月**

**パブリッククラウドサービス（IaaS、PaaS など）**上で稼働している生産性向上アプリケーション / ワークロードの割合
**53%**

**オンプレミス インフラストラクチャ**上で稼働している生産性向上アプリケーション / ワークロードの割合
**47%**



> 「過半数(63%)の組織が **3 社以上**のクラウドサービス プロバイダー(CSP)を利用しています」
>
> - Enterprise Strategy Group サイバーセキュリティ担当 **Melinda Marks**

セキュリティは CSP が直面するもっとも大きな課題であり、規模の問題、アプリケーションの可用性とパフォーマンスの確保がそれに続きます。

- **31%** セキュリティに求められる期待に応える
- **30%** 多様な API を管理する
- **29%** 継続的インテグレーション / 継続的デリバリ（CI/CD）と統合する
- **26%** ネットワーク相互接続の可否 / 不一致
- **26%** 一貫性のある展開手法を導入する

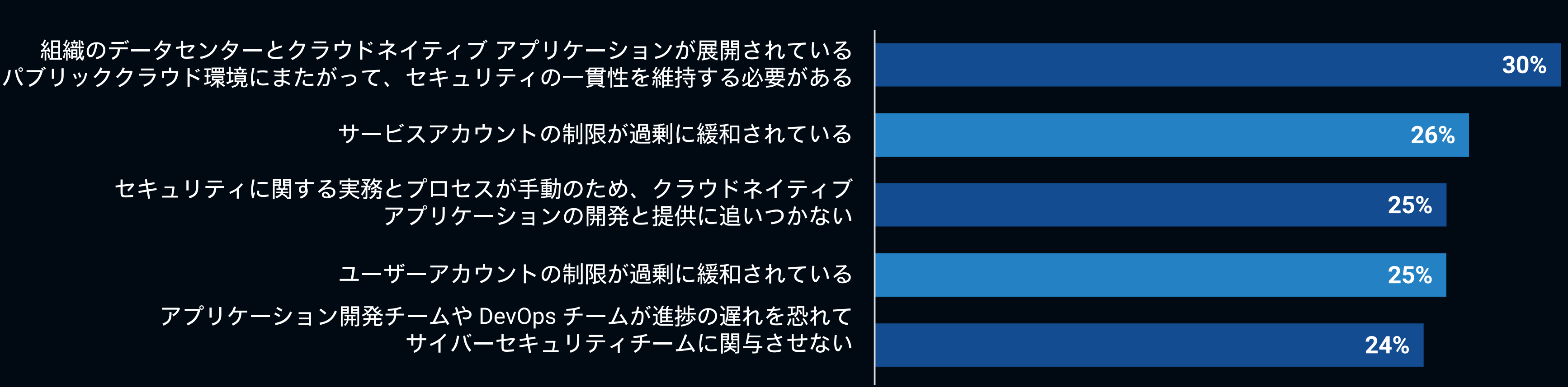
クラウド移行における最大の懸念事項はセキュリティで、コストと時間に関する懸念がそれに続きます。

- **25%** セキュリティに求められる期待に応える
- **25%** コストに対する期待に応える
- **25%** 多様なアーキテクチャの学習時間とコスト
- **24%** ネットワーク相互接続の可否 / 不一致
- **26%** 複数のパブリッククラウドサービスの間でアプリやデータを移動させる時間と労力

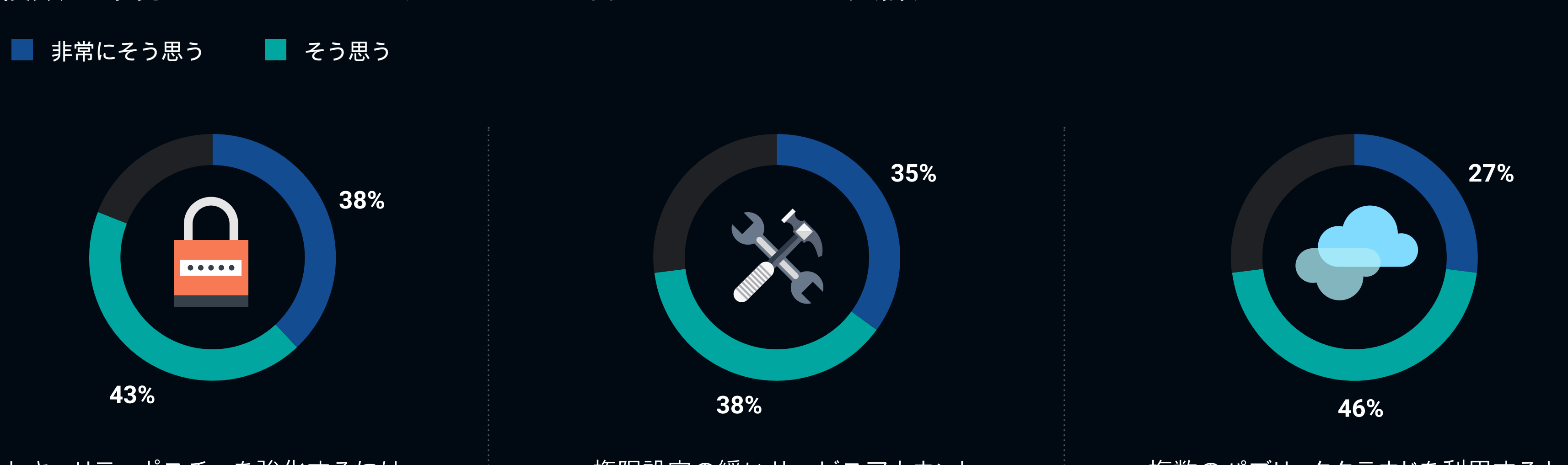
## 成長を支える効果的なセキュリティ戦略

セキュリティチームに求められているのは、成長やイノベーションの歩みを遅らせることなく実現することです。そうした期待が、環境全体でセキュリティリスクを効果的に管理し、アプリケーションを保護する方法を求める圧力となってチームにのしかかり、チームがそれぞれのプログラムに適応し、環境全体でアプリケーションの成長と規模の拡大に対応する上での課題となっています。

クラウドセキュリティにおいてもっとも困難とされているのが一貫性と権限、規模の問題です。



複数の環境にまたがってセキュリティを管理する上での 3 大課題



セキュリティポスチャを強化するには、業界が定めたセキュリティに関するベストプラクティスに従うことが重要である。

権限設定の緩いサービスアカウントは重大なセキュリティリスクやコンプライアンス上のリスクを招く。

複数のパブリッククラウドを利用すると、環境全体で一貫したセキュリティを保つのが難しくなる。

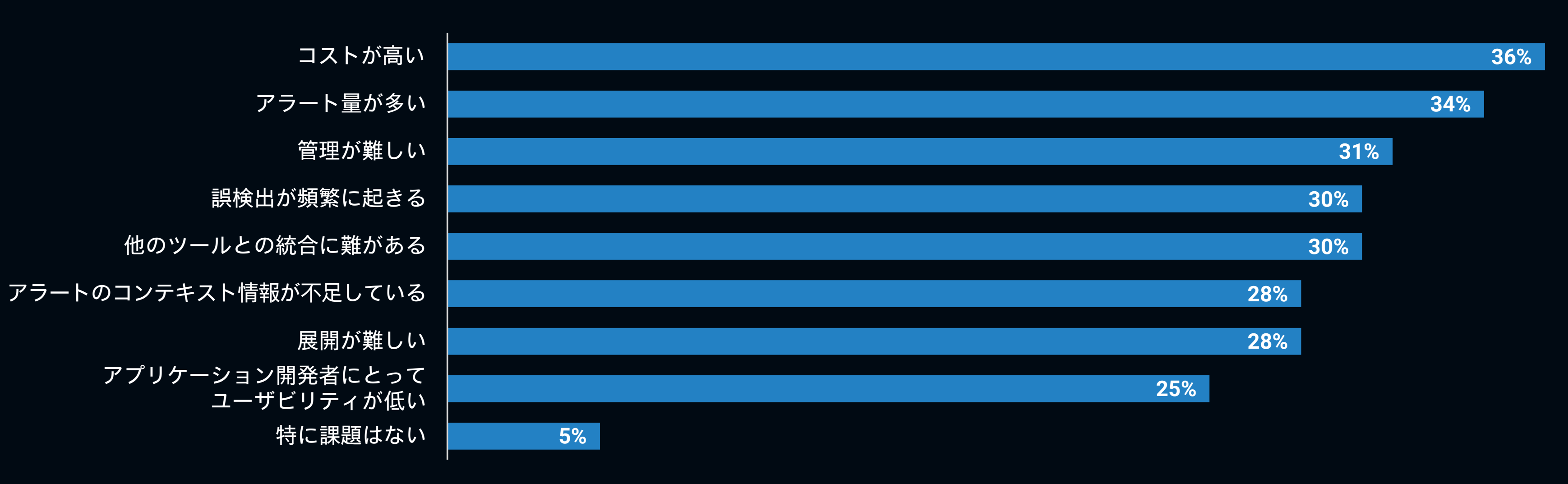
## サイロ化した複数のツールから、より効率的なソリューションへの移行

チームにとって扱うのが難しく、時間のかかる個別のセキュリティツールが多すぎるというのも、組織を悩ませている課題の 1 つです。この課題を解決するにはセキュリティツールを統合し、相互接続された 1 つの動的なフレームワークによって環境全体のすべてのアプリケーションを可視化できる手法を探す必要があります。そうした手法があればチームの運用効率もその効果も高まるだけでなく、アセット全体のコンテキストを把握できるため、速やかなセキュリティ運用によってリスクを抑え、円滑に脅威に対応できます。

アセットインベントリに使用される複数のツール

- **52%** IT アセット管理システム
- **40%** サイバーアセットの攻撃対象領域の管理技術
- **37%** エンドポイントセキュリティ
- **34%** ネットワークスキャン
- **33%** クラウドのセキュリティポスチャ管理ツール
- **33%** エンドポイント管理
- **32%** 脆弱性スキャン/アセスメントツール
- **26%** ネットワーク アクセス コントロール
- **26%** 構成管理とパッチ管理
- **25%** 外部攻撃対象領域管理プラットフォーム

複数の Web アプリケーション保護ソリューションを使用する上でのツール関連の課題



異なる環境で複数のセキュリティツールを使用する上での管理に関する 4 大課題

- **45%** セキュリティ製品ごとに別々のトレーニング、導入、管理、運用が必要なため、セキュリティ部門のリソースに負担がかかっている
- **36%** 使用しているセキュリティ製品の数が多すぎて、セキュリティ状況の全体像を把握するのが難しい
- **33%** セキュリティ担当者が独立したセキュリティテクノロジーからの結果を集約しなければならないため、セキュリティ運用全体が複雑で時間を要するものになっている
- **30%** セキュリティ製品を適切に管理できるスタッフやスキルが不足している

組織に必要なのは、セキュリティチームが生産性の向上や成長に対応できるような、プロセスと制御の一貫性を保ちつつ環境全体でセキュリティを効果的に管理し、展開している場所を問わずアプリケーションを保護できる方法です。

### プログラムの効果を高めるために重要な要素

**広範な可視性**により環境全体のすべてのアセット（ネットワーク、アプリケーション、クラウド）を見通し、セキュリティポスチャの正確な全体像を把握。

**修復効率を高めるコンテキスト情報。**リスクスコアを使用して環境全体の脆弱性に効率的に優先順位を付け、リスクの軽減に必要なもっとも効果的な修復アクションを提示。

**一貫性のある統合されたセキュリティ制御**でポリシーやセキュリティフレームワークを環境全体のワークロードに矛盾なく適用。

**包括的なワークロード保護**によりネットワーク、クラウド、VPC 全体にわたってトラフィックを保護し、環境全体に正確で一貫性のあるマクロセグメンテーションとマイクロセグメンテーションを適用することで不正なラテラルムーブを防止して、アプリケーションとデータを保護。

Cisco Cloud Protection Suite は、ハイブリッドおよびマルチクラウドのアプリケーション環境にエンドツーエンドのセキュリティを提供することで、最新のアプリケーション セキュリティ アプローチを実現します。ベアメタルからクラウドネイティブ インフラストラクチャまで、お客様に包括的なアプリケーション セキュリティを提供し、オンプレミスもクラウドも含めた環境全体でワークロードを保護します。

**詳細はこちら**

出典：『Complete Survey Results: *Distributed Cloud Series: The State of Infrastructure Modernization Across the Distributed Cloud*』、Enterprise Strategy Group、2023 年 8 月。
出典：『Research Report: *Cloud Entitlements and Posture Management Trends*』、Enterprise Strategy Group、2023 年 4 月
出典：『Research Report: *Security Hygiene and Posture Management Remains Decentralized and Complex*』、Enterprise Strategy Group、2023 年 7 月
出典：『ESG Complete Survey Results: *ESG/ISSA Cybersecurity Process and Technology Survey*』、Enterprise Strategy Group、2022 年 6 月