Cisco Secure Cloud Insights with JupiterOne

クラウドファースト戦略とデジタル トランスフォーメーション戦略が継続的に採用されるようになったことで、ビジネスの運営方法が根本的に変わりました。組織は今、ビジネスを推進するだけでなく、急速に変化する世界を生き抜くために、新しいツールやシステム、プロセスへの移行を進めています。俊敏性の向上、市場投入までの時間短縮、生産性の向上、コストの削減に移行が寄与したのは事実です。

しかし一方で、サイバーセキュリティの面で新たな問題も生じています。オンプレミスのデバイスからクラウドへと IT 資産が移行するのに伴い、クラウドの持つ一時的な性質によって資産が急増しました。それだけでなく、規模や複雑性も増しています。そのうえ、拡大し続けるクラウド資産全体を一元管理する術がありません。サイロ化されたセキュリティツールで把握できるのは、全体像のほんの一部です。

このためセキュリティチームは、クラウド環境や資産に関する極めて基本的な問いにすら答えるのが難しくなっています。見えないものや知らないものは、保護できるわけがありません。重要なのは、豊富なコンテキストに基づいてクラウド資産を可視化することです。そうすれば、エンドツーエンドのアタックサーフェス（攻撃対象領域）を把握し、クラウド環境を脅威から保護し、潜在的なセキュリティギャップを埋めることができます。

セキュリティリスクと複雑性を大幅に低減

シスコは、当社のソリューションである Cisco® Secure Cloud Insights によってこれらの課題に対応するため、JupiterOne 社と提携しました。Secure Cloud Insights が提供するクラウド環境の完全な可視性により、セキュリティとコンプライアンスのギャップの特定が可能となり、脅威の調査と対応が促進されます。

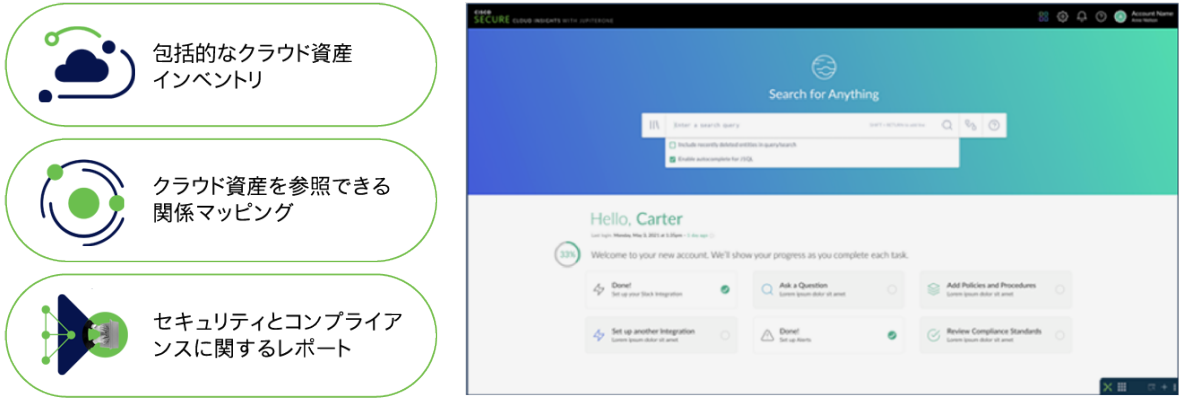
資産の包括的なインベントリによってクラウド資産が可視化され、クラウドベースのエンティティとアクセス権をナビゲートする関係マッピングをアタックサーフェスの把握に役立てることができ、クラウドのセキュリティポスチャの強化に加え、セキュリティとコンプライアンスレポートのコンプライアンス向上が実現します。

メリット

- 複数のクラウドにまたがるクラウド セキュリティ ポスチャを完全に可視化して把握
- クラウド環境を継続的にモニタリングし、ポリシー違反と設定不備を検出
- 資産間の関係をマッピングしてアタックサーフェス全体を把握
- 影響範囲を特定することにより、影響を受けた資産を迅速に調査して修復

それだけではありません。Secure Cloud Insights は、他の Cisco Secure ポートフォリオとも緊密に統合されています。Cisco SecureX™ プラットフォームと統合しているため、SecureX に組み込まれている Device Insights 機能だけでなく、Cisco Secure Cloud Analytics（旧 Cisco Stealthwatch® Cloud）とも密接に連携します。

図 1.　Secure Cloud Insights の概要



クラウド セキュリティ ポスチャを完全に可視化

Secure Cloud Insights では、複数のクラウド環境を可視化できます。これにより、クラウド セキュリティ ポスチャを含め、クラウド資産に関する情報を包括的に把握することが可能となります。可視化できる環境としては、Amazon Web Services（AWS）、Microsoft Azure、Google Cloud などのパブリック クラウド プロバイダのほか、コンテナやサーバーレス環境などがあります。

また、何百もの業界トップクラスのテクノロジーとの統合により、クラウド資産についての信頼できる唯一の情報源として機能するため、正確でエンドツーエンドのクラウド資産のインベントリを簡単に構築することができます。そしてこのインベントリには、資産関係についての詳細なコンテキストも含まれます。というのも、Secure Cloud Insights ではグラフベースのアプローチが採用されており、検出、マッピング、可視化、資産間の関係を簡単に確認できるからです。

これは価値のある機能です。クラウド資産間の関係を把握することは、資産の所在地を把握することと同じくらい重要なのです。資産同士の関係を可視化することにより、クラウド資産がセキュリティ環境に与える影響と潜在的なリスクを理解できるようになります。たとえば資産に対する可視性とコンテキストに基づく関係を使用すれば、クラウドのアタックサーフェスに関するエンドツーエンドのインサイトが得られます。その結果、複数のクラウドにまたがる複雑なアタックサーフェスのマッピング、分析、理解が可能になります。

クラウドのセキュリティとコンプライアンスのギャップを簡単に特定

クラウドの可視性を提供するだけでありません。Secure Cloud Insights はクラウド環境を継続的にモニタリングして、ポリシー違反と設定不備を検出します。クラウド環境は非常に動的なものであり、クラウド資産、設定、およびそれらを管理するポリシーは頻繁に変更される可能性があります。つまりクラウド環境では、継続的にモニタリングを行って設定不備やコンプライアンス違反を通知する必要があるということになります。

Secure Cloud Insights は、クラウド資産を列挙して詳細な分析を実行し、潜在的なセキュリティリスクやコンプライアンス違反、クラウドの設定不備についてアラートを出すことにより、セキュリティチームとコンプライアンスチームがクラウド環境内のすべてについて常に最新情報を把握できるようにします。クラウド サービス プロバイダ(CSP) と直接統合されていて、クラウドリソースの設定が継続的に評価、監査、評価されるため、全体的なクラウドセキュリティリスクを軽減し、コンプライアンス違反を迅速に検出できるようになります。

さらに、Secure Cloud Insights はダッシュボードとレポート機能も備えているので、セキュリティとコンプライアンスのステータスを素早く確認するとともに、セキュリティとコンプライアンスのフレームワークのギャップを特定できます。CSPM ベンチマーク、CIS、NIST、SOC 2、PCI DSS などの複数の標準とフレームワークが、ギャップを特定する対象として事前構築されています。こうしたセキュリティ標準とコンプライアンス フレームワークは、クラウドの資産と環境に直接マッピングされています。そのため当て推量をすることなく、クラウド セキュリティ ポスチャの強化とコンプライアンスの達成に向けた最短ルートをたどることに専念できます。

調査と対処をスピードアップ

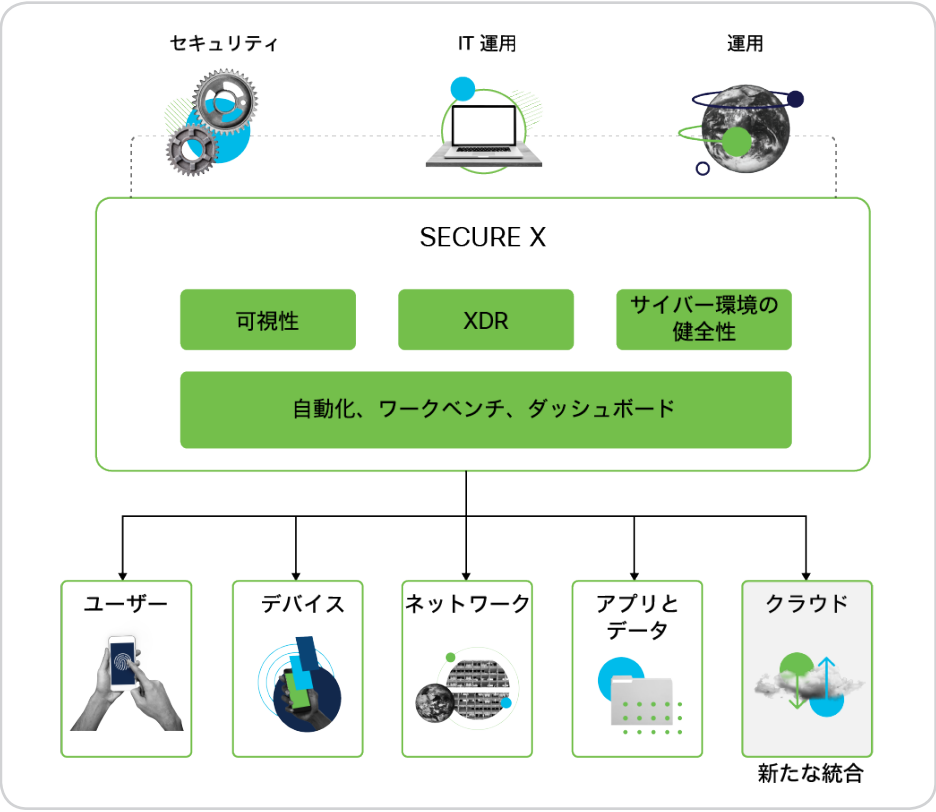
Secure Cloud Insights ではクラウド資産のナレッジグラフが提供されます。このグラフはクラウド資産全体を把握して理解するのに役立ち、すべてのクラウドリソース、環境、資産の関係を照会するだけで、クラウド資産に関する複雑なセキュリティ関係の問いに答えられるようになります。たとえば次のような質問に答えることができます。

- AWS の S3 バケットはエクスプロイト可能か。
- クラウド資産は CSPM ベンチマークに適合しているか。
- インターネットに接続している CSP にデータストアはあるか。

さらに Secure Cloud Insights は、脅威の調査と対応を迅速化する、クラウド資産と関係に関する詳細コンテキストを提供します。コンテキストに基づく豊富な情報により、脆弱な資産の影響と関係を把握し、侵害の影響が及ぶ可能性のある範囲を正確に特定できます。たとえば侵害されたデバイスやユーザーに接続されているすべてのクラウド資産を簡単に特定し、優先順位を付けて修復することが可能です。

Secure Cloud Insights はまた、Cisco SecureX プラットフォームを強化し、統合します。業界で最も広範かつ最も統合が進んでいる SecureX は可視化の機能を一体化したセキュリティ プラットフォームであり、脅威への対応をシンプルにして自動化を実現します。高度な脅威検出と対応 (XDR) 機能を備えているため、安心して対応と修復の自動化を図ることができます。SecureX は、複数のセキュリティ製品から提供されるインサイトを 1 つのコンソールに集約するほか、追加のコンテキストと統合制御を提供します。さらに、事前定義されたワークフローとカスタムワークフローを使用して、事前に定義されたインシデント対応プレイブックをトリガーする自動対応を有効化できます。

図 2.　Secure Cloud Insights と SecureX プラットフォームの統合



Secure Cloud Insights によって、クラウド資産とその関係に関する貴重なコンテキストが SecureX に追加され、アラートの信頼度が高まり、調査と対応のスピードが向上します。また、Cisco SecureX の Device Insights と組み合わせれば、クラウドとオンプレミスの両方の資産に対する比類なき可視性が得られます。Device Insights はオンプレミス資産の包括的なインベントリとして機能し、複数のデバイスマネージャ、エンドポイントでの検出と対応(EDR)、ウイルス対策などのエンドポイントセキュリティ製品を SecureX 内の単一の統合ビューに統合します。セキュリティギャップの迅速な特定、調査の簡素化と自動化、侵害された資産を特定して修復するためのコンテキスト情報の把握に役立てることができる機能です。

詳細については、https://www.cisco.com/c/en/us/products/security/secure-cloud-insights/index.html を参照してください。