CISCO
SECURE

The bridge to possible

Cisco Secure Cloud Insights

Cloud security posture, cyber governance and attack surface management

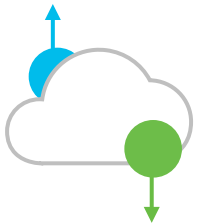
SWA, Japan, Cisco Systems,

2022年2月

Contents

クラウド時代におけるサイバーガバナンスの課題

マルチクラウド、ハイブリッドクラウドのアプローチによる急激なクラウド導入



2021年までに、中堅・大企業の75%以上がマルチクラウドやハイブリッドIT戦略を採用すると言われている[1]

監視すべきアタックサーフェス(攻撃対象領域)* の拡大

*アタックサーフェス：インターネットに公開されている攻撃対象となりうるサイバーアセット

今後2年間で、組織がサポートするアプリケーションの数が50%増加し、分散したワークロードが急増する[2]

断片的かつサイロ化されているサイバーアセット管理

組織の55%が、正確なサイバーアセットのインベントリー管理ができていない[3]

The result:コンプライアンス上のギャップや脆弱性は、全体的なセキュリティ態勢を低下させる

2021年、セキュリティ侵害を特定するまでの平均時間は207日[4]

1. Gartner Predicts., 2. IDG Report, August 2019, 3. ZK Research 2019, 4. Ponemon report, 2021

クラウドの可視性とコントロールの欠如

01 クラウド上のアセットや環境が増え、たえず構成が変化している

02 クラウドアセット全体のリスクモニタリングと自動修復の相互運用性が欠如

03 影響を受けたリソースの影響を迅速に把握することが困難

04 クラウドアセット全体の潜在的なセキュリティリスクやギャップに対する洞察が不足

クラウドの潜在的セキュリティリスク

➢ クラウド設定不備が及ぼす大きなリスク

クラウド設定不備によるインシデント事例

- 2017年12月　データ分析会社Alteryx社が運営する、AWS S3のアクセス権限の設定ミスにより、1億2千万世帯以上のアメリカの世帯情報が公開されていたことが発覚
- 2019年7月　米金融大手 Capital Oneは不正アクセスにより1億人を超える個人情報が流出したと発表。WAFの設定ミスに起因して攻撃を許し、WAFを介して直接AWS S3にアクセスが可能であった

出典：クラウドセキュリティアライアンス（CSA）：クラウドコンピューティングに対するトップ脅威 2019年10月

https://japan.zdnet.com/article/35176859/

構成ミスが原因で流出したレコードが前年比で10倍近く増加しており、2019年に侵害されたレコード全体の86%を占めている　出典：IBM X-Force Threat Intelligence Indexの2020年版レポート

Secure Cloud Insights の概要

Secure Cloud Insights

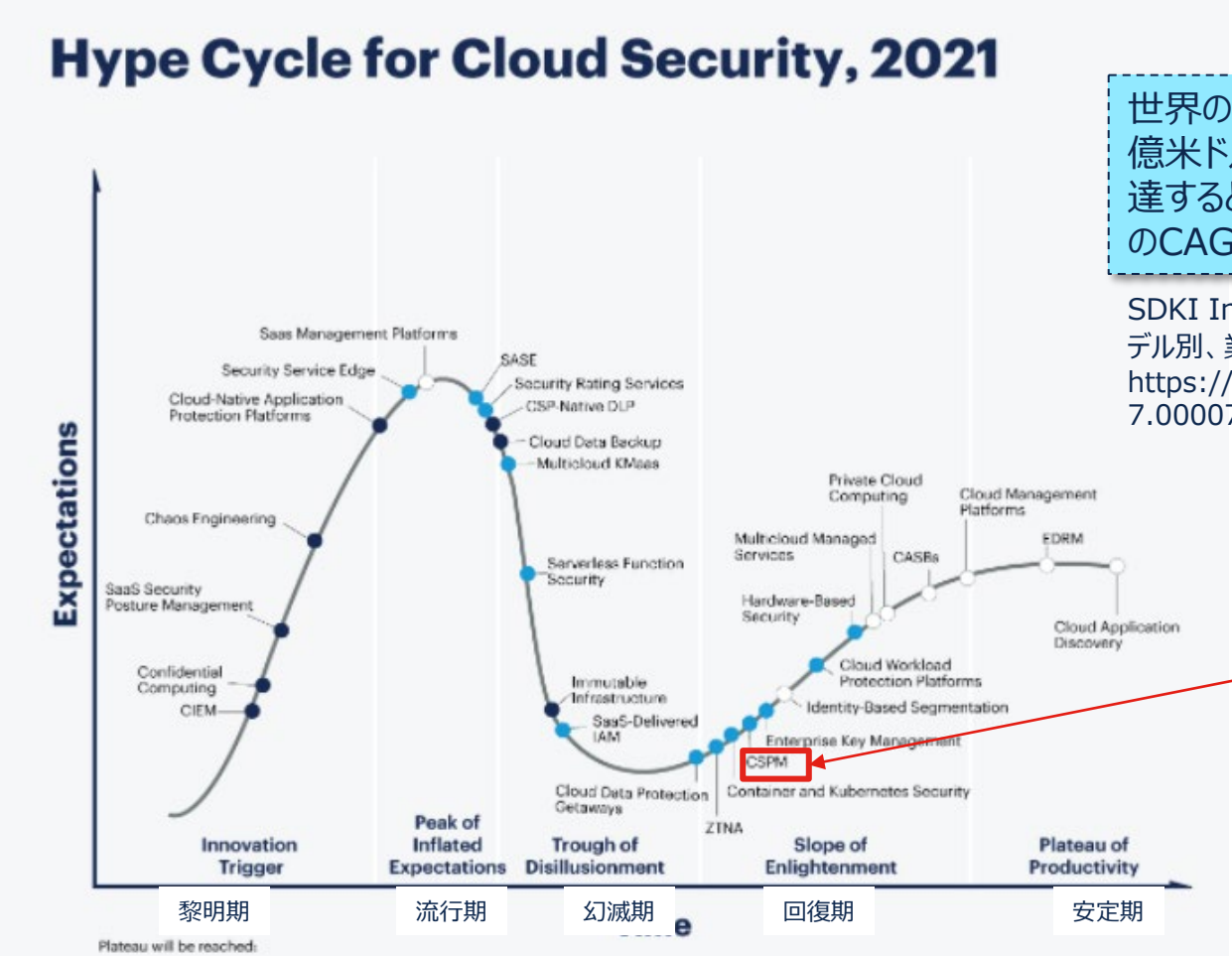
➢ **CSPM –** Cloud Security Posture Management

IaaSなどパブリッククラウドに対してAPI連携により、クラウド側の設定を自動的に確認し、セキュリティの設定ミスや各種コンプライアンスフレームワーク等への違反が無いかを継続してチェックする

➢ **CAASM –** Cyber Asset Attack Surface Management

既存のツールとのAPI連携により、すべてのサイバーアセット(内部および外部)を可視化し、アタックサーフェス(攻撃対象領域)の全体像を把握。
連携されたデータに対するクエリを実行し、脆弱性の範囲やセキュリティ管理のギャップを特定する

CSPMマーケット状況



世界のCSPM市場規模は、2020年の40億米ドルから、2026年までに90億米ドルに達すると推定され、予測期間中に14.4%のCAGRで成長すると予測されている

SDKI Inc.：CSPM市場ーコンポーネント別、クラウドモデル別、業種別、および地域別ー世界の予測2026年
https://prtimes.jp/main/html/rd/p/00000023
7.000072515.html

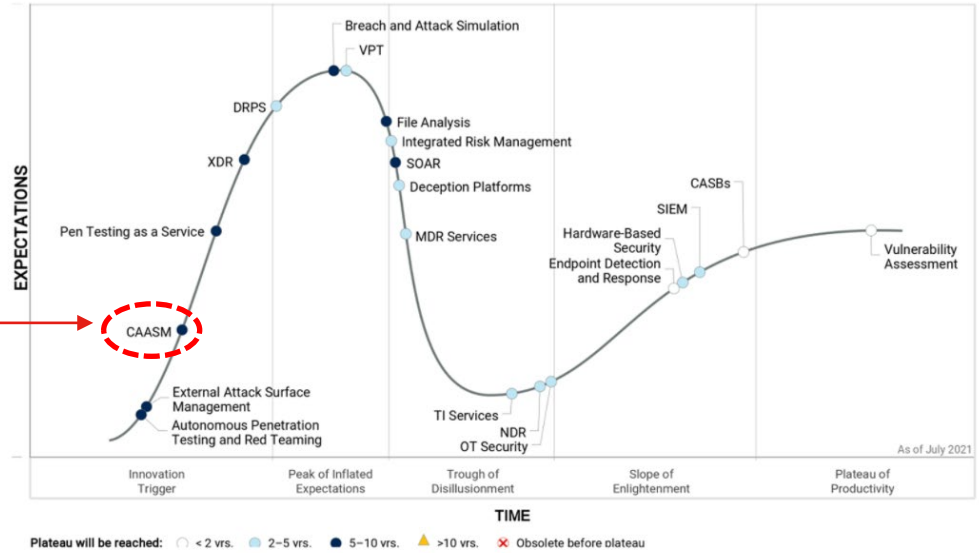
CSPM

CAASM：新しいセキュリティマーケットカテゴリ by Gartner

- CAASM (Cyber Asset Attack Surface Management)
-

CAASM

Figure 1: Hype Cycle for Security Operations, 2021



https://info.jupiterone.com/resources/gartner-hype-cycle-security-operations?utm_campaign=CAASM&utm_medium=ppc&utm_source=adwords&utm_term=caasm&hsa_mt=p&hsa_net=adwords&hsa_ver=3&hsa_kw=caasm&hsa_acc=9405854578&hsa_grp=126397058805&hsa_tgt=kwd-1410719155090&hsa_src=g&hsa_ad=550251265620&hsa_cam=14874578122&gclid=CjwKCAiA4veMBhAMEiwAU4XRr5LMqw6M2-WMWF9Mr63YhrnXissVg55jbeXSQqFkQ1oicQdtqWN0hhoCb5UQAvD_BwE

Secure Cloud Insights with JupiterOne

コンプライアンスやリスク管理には全体の可視化がポイント

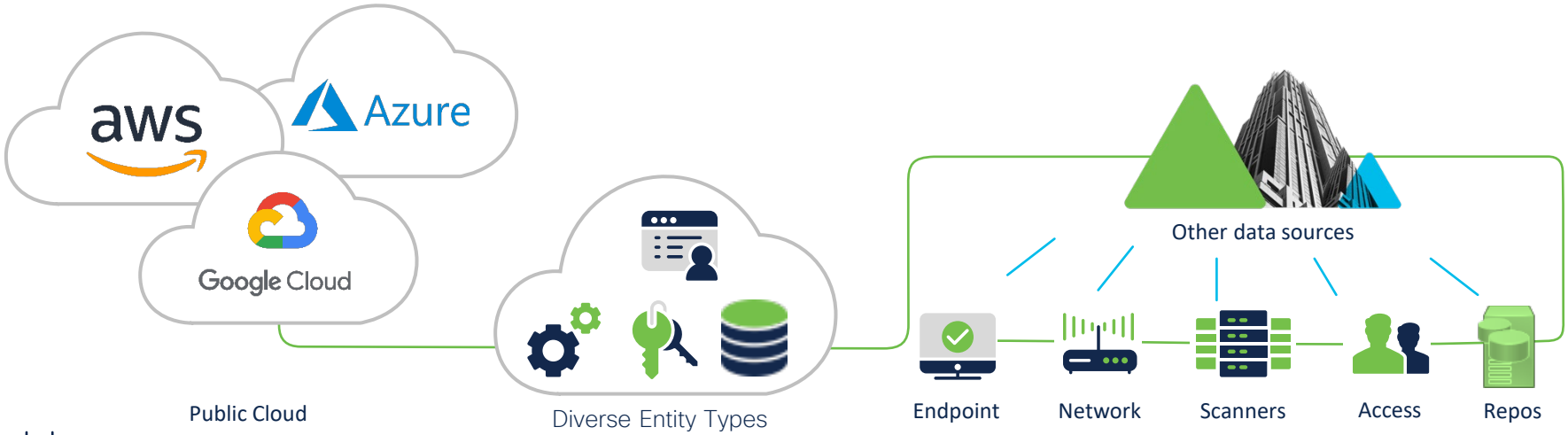
全てのアセットを可視化

アセット同士の関連付け

現状の設定状況を把握

設定状態の継続的なチェック

リスクをアラート



Secure Cloud Insights ハイレベルアーキテクチャ

SaaS型の提供形態

1. ネイティブデータの取り込み

クラウドやオンプレミスのアセットをAPIやデータストリームを介してネイティブに統合

2.アセットの検出とマッピング

複数のデータソースにまたがるアセットやエンティティの認識し、複数のアセットの相関関係をマッピング

- 継続的なコンプライアンスチェック
- リレーショングラフの可視化

- シンプルなクエリ言語
- 定期的なデータポーリング

3.アラートとレスポンス

アラートが検出されると、チケッティングシステム等に通知

Secure Cloud Insights

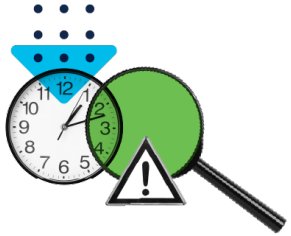
クラウドセキュリティポスチャ管理(CSPM)＋サイバーアセットアタックサーフェス管理（CAASM)

セキュリティポスチャの完全可視化

- API連携によりクラウド上のサイバーアセットを自動検出、可視化
- クラウド上の設定ミスなどをアラート通知、センシティブデータの不用意な露出を回避

セキュリティとコンプライアンスのギャップを容易に把握

- カスタマイズ可能なコンプライアンススタンダードを用いた継続的な監査、ギャップの可視化
- 550の事前に定義されたクエリとカスタムクエリによる迅速なコンプライアンス課題の発見



アタックサーフェス管理

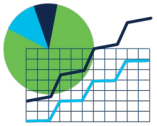
- クラウド上のサイバーアセット間の相関関係を自動的に理解しリレーションシップマップを作成
- アタックサーフェスを把握し、セキュリティギャップやリスク、影響範囲、根本原因などを特定

主要なユースケース

Secure
Cloud Insights

ハイブリッドクラウドの可視化	パブリッククラウドやプライベートクラウド、オンプレミスなどの複数のインフラとネイティブに統合し、ワークロードフレームワーク全体を統一的に把握
リレーションシップマッピング	エンティティ間の関係を自動的にマッピングし、可視化
クラウドセキュリティポスチャ管理(CSPM)	AWS、Azure、GCP環境のセキュリティポスチャーを監視し、コンプライアンス準拠のためのエビデンスを容易に追跡
継続的なコンプライアンス	あらかじめ用意された20以上のコンプライアンススタンダードだけでなく、カスタムスタンダードも作成可能
サイバーガバナンス	脆弱性とカバレッジのギャップの最新の状態を把握することでサイバーガバナンスを実現
迅速な調査	迅速に根本原因を突き止め、影響範囲を把握し、調査と対応にかかる時間を短縮
Attack Surface Management	すべてのエンティティをコンテキスト化して、相関関係を柔軟な粒度で把握することで、内部および外部を問わずアタックサーフェスの把握が可能

クラウドセキュリティポスチャ管理 (CSPM)



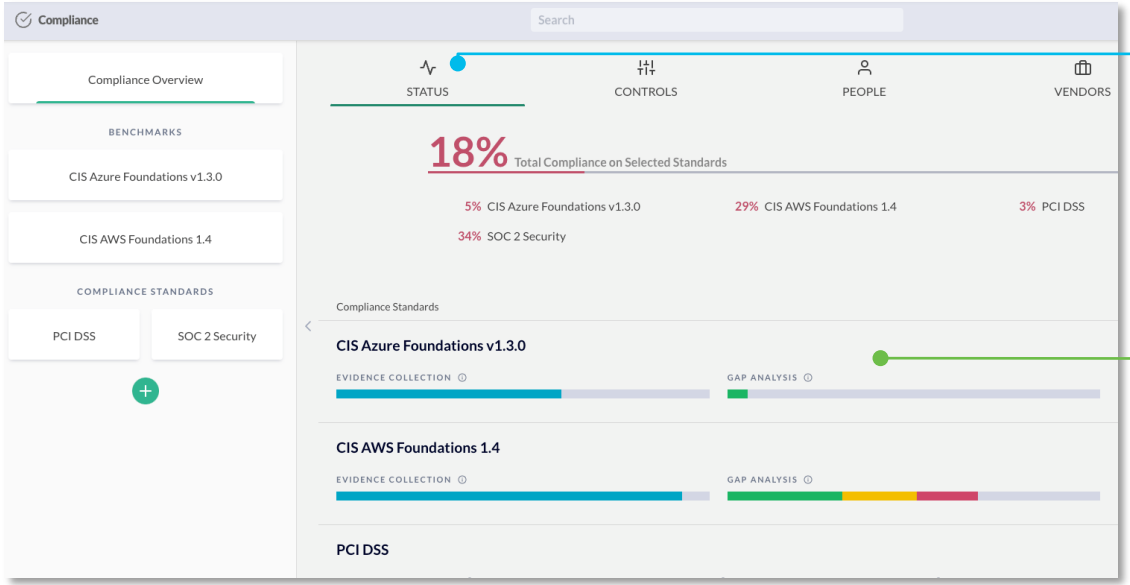
主要なコンプライアンススタンダードをサポート

継続的なコンプライアンスレポート

カスタムコンプライアンスレポートの作成

主要なコンプライアンススタンダードをサポート

単一画面で全てのコンプライアンスレポートをカバー



特定のベンチマークごとにステータスを表示するオプションにより、コンプライアンスの状況を即座に確認

コンプライアンスの状況を把握するためのギャップ分析や、コンプライアンスを証明するためのエビデンス収集

SOC2, CIS Framework, PCI DSS など主要なコンプライアンスレポートをサポート

NIST CSF | NIST 800-53r4 CIS PCI Data Security Standard V 3.2 AICPA SOC SOC 2 HIPAA COMPLIANCE General Data Protection Regulation

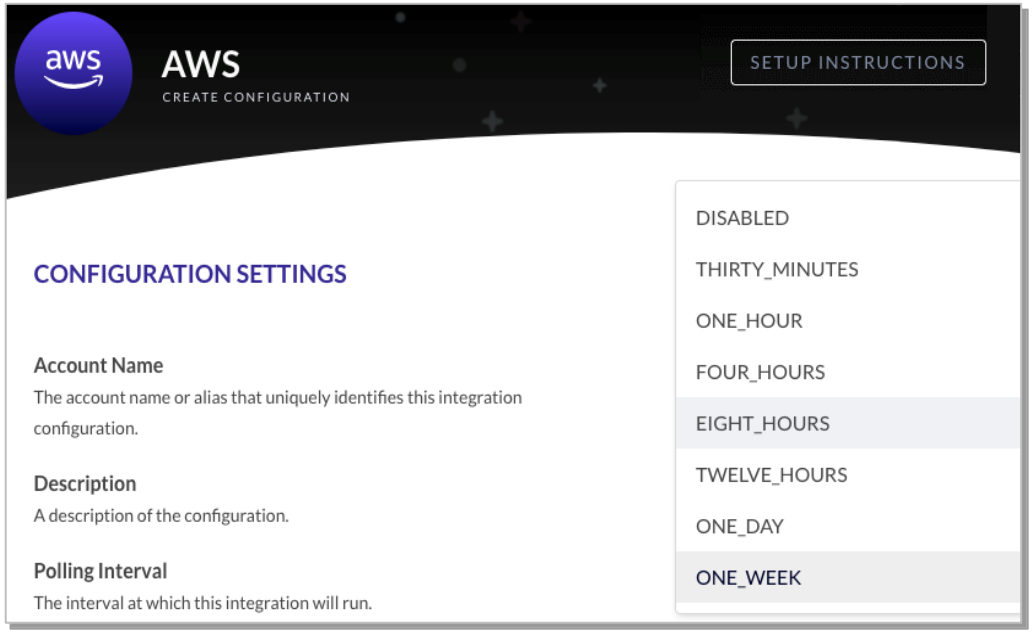
継続的なコンプライアンスレポート

常時コンプライアンスチェック

- データソースから収集したデータのポーリング間隔をカスタマイズ可能
- 最新のデータでコンプライアンス状況を毎日更新

準拠違反の自動検出

- コンプライアンススタンダードからの準拠違反を自動的に検出



シンプルなクエリでコンプライアンス課題を迅速に発見

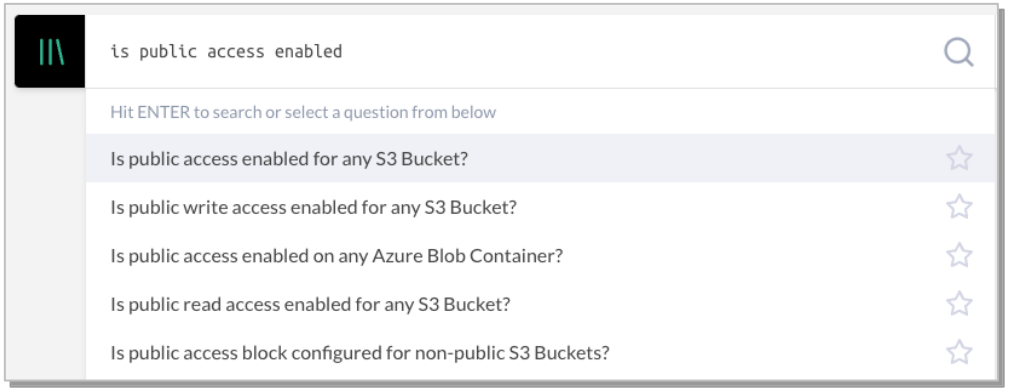
継続的なコンプライアンス監視

ALERT: ギャップの検出

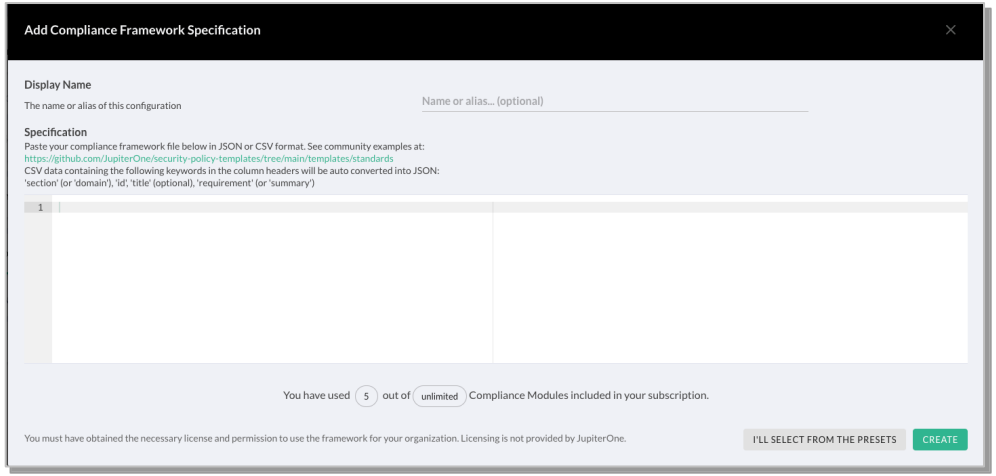
- 550 の事前に定義されたクエリとカスタムクエリ
- 任意のクエリをアラートに変換したり、コンプライアンスフレームワークに追加可能

定義済クエリ例

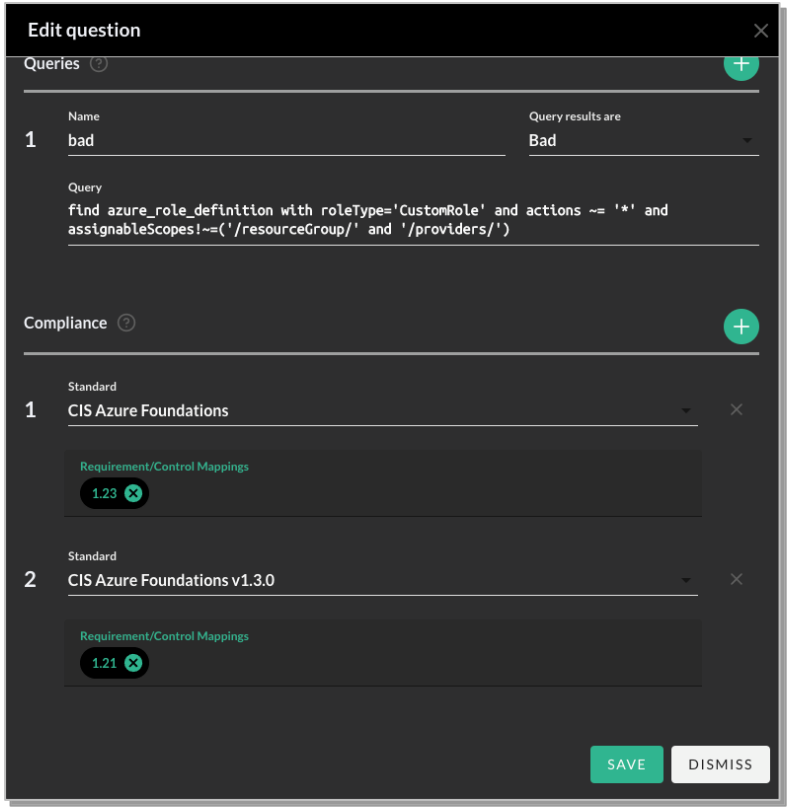
- 暗号化されていないクラウドストレージバケットは？
- ロギングが有効になっていないストレージは？
- 本番系インスタンスは？
- インターネットに公開されているどのコンピューティングインスタンスが非公開S3ストレージにアクセスしているか？
- 昨年の脆弱性スキャンの結果は？



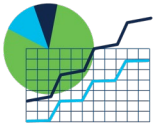
カスタマイズ可能なコンプライアンスレポートとクエリ



新しいコンプライアンススタンダードの作成や既存のカスタマイズが可能



サイバーアセットの可視化

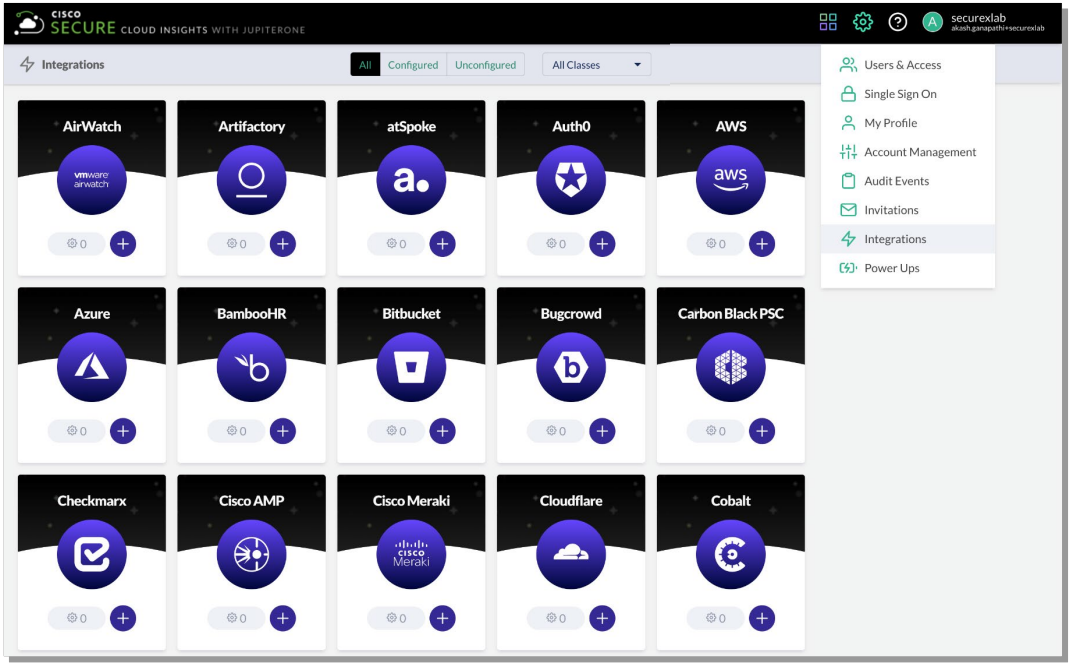


インテグレーション

リレーションシップマッピング

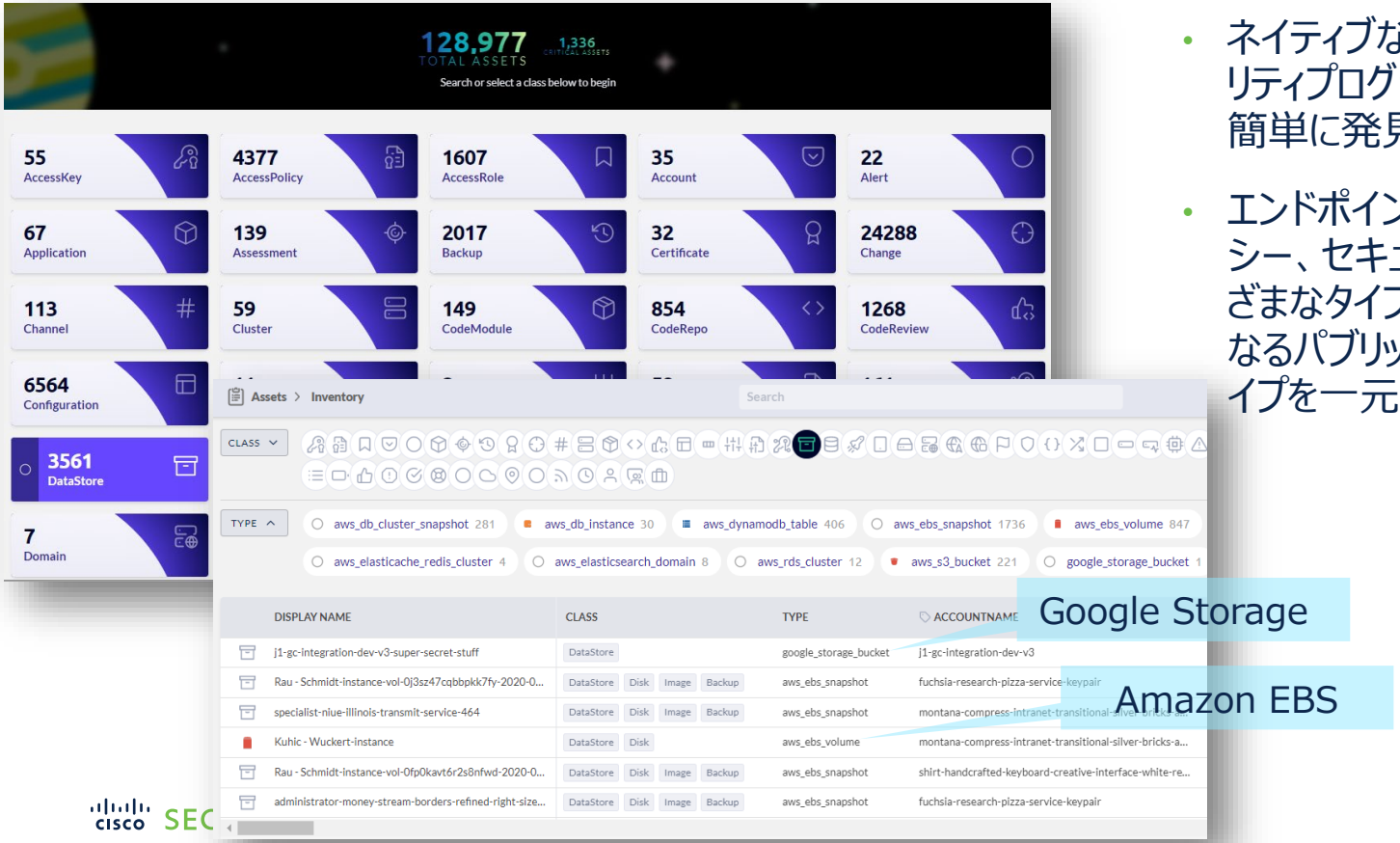
アセットやプロパティの検索

インテグレーション



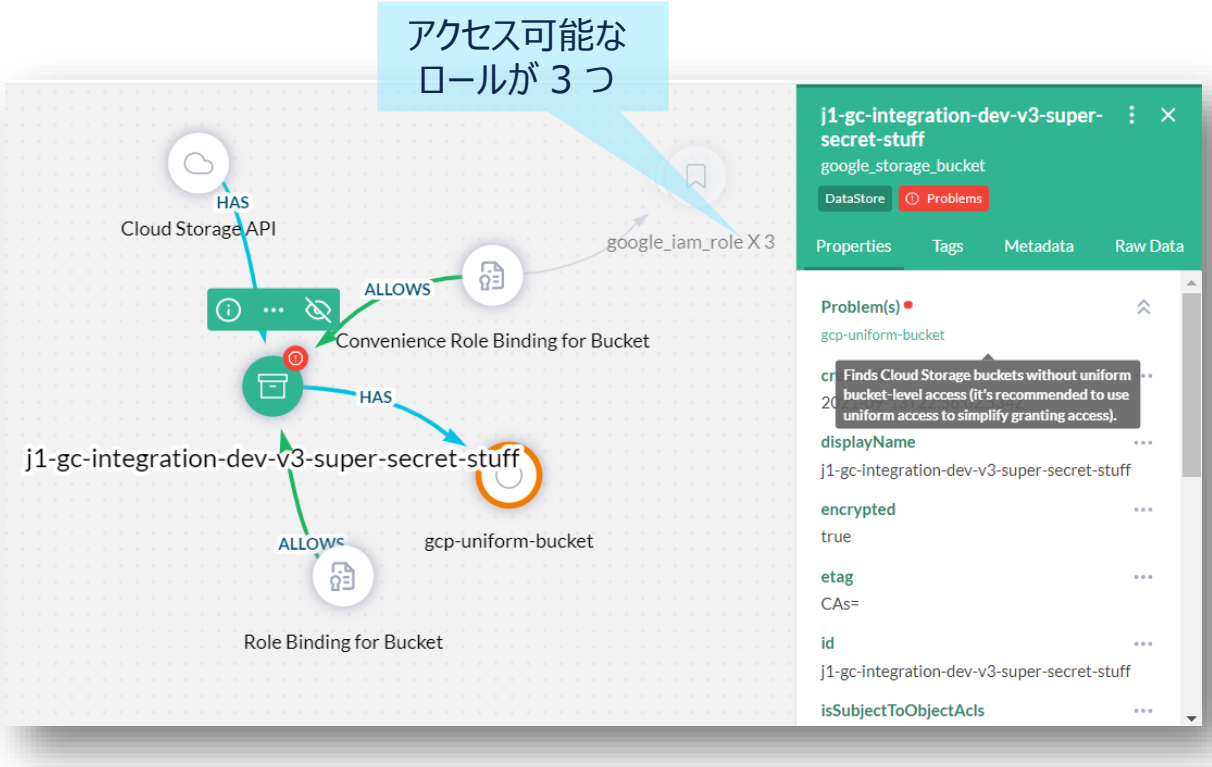
- インテグレーション対象のアセットのコンフィグレーションメニューが用意されている
- API連携のため、読み取り専用の認証情報を使用してデータを取り込む。エージェントのインストールは不要
- IaaS, エンドポイント、データストア、ポリシー、セキュリティグループなど、さまざまなタイプのアセットのインテグレーションが可能

サイバーアセットの可視化



- ネイティブな統合機能により、セキュリティプログラム全体からアセットを簡単に発見することができる
- エンドポイント、データストア、ポリシー、セキュリティグループなど、さまざまなタイプのアセットを発見し、異なるパブリッククラウドやアセットのタイプを一元管理することができる

アセットのリレーションシップマッピング

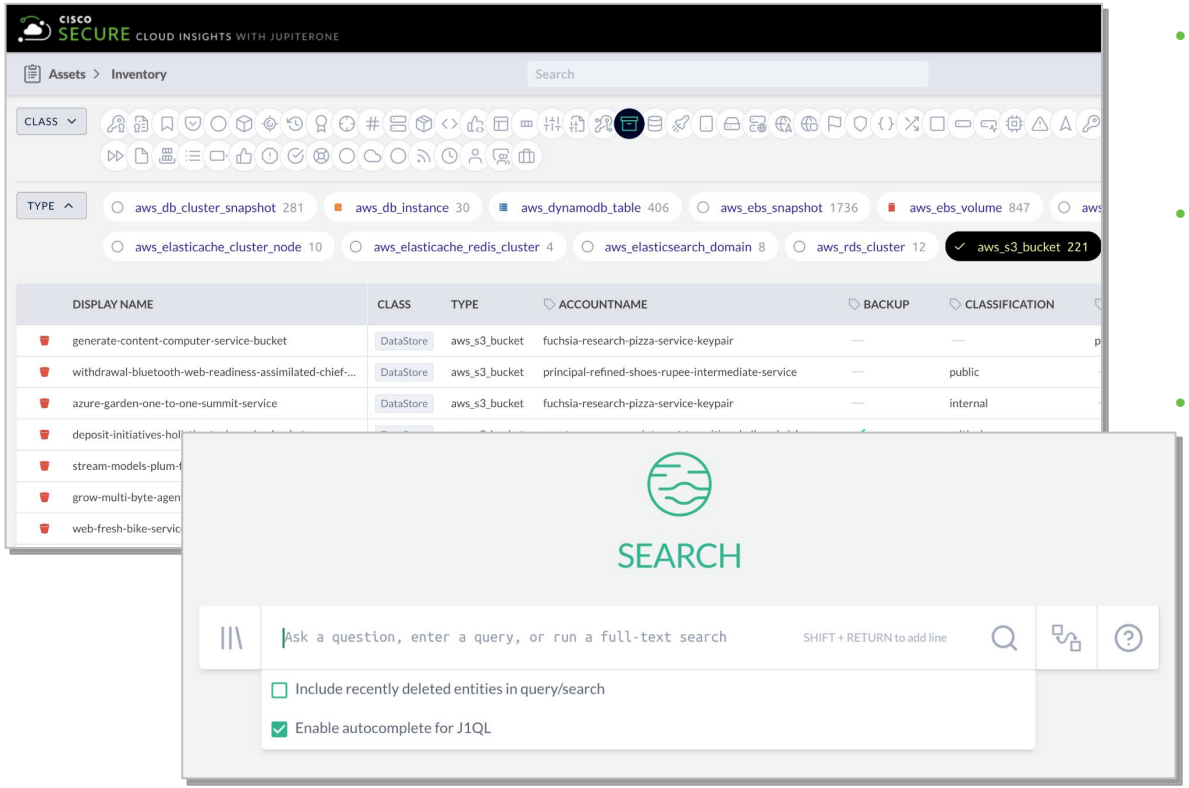


アセット間のリレーションシップを自動的にマッピング

左図は前のスライドの j1-gc-integration-dev-v3-super-secret-stuff をクリックしてグラフ表示した画面

- 各アイコンをクリックするとその役割やポリシー等が表示される
- アイコン右上の赤丸はコンプライアンス違反の発生を示している
  （クリックするとその詳細が表示される）

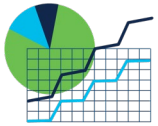
アセットやプロパティの検索



- クラスやタイプごと自動的にグループ化されるため、環境内のアセットを検索可
- 統合されたすべてのアカウントやクラウドで、検索ツールを使ってアセットやプロパティを検索
- 550以上のセキュリティおよびコンプライアンスに関する質問を含む、あらかじめ用意されたクエリライブラリを活用し、独自の質問を作成およびカスタマイズすることが可能

アタックサーフェス* 管理 (CAASM)

*サイバー攻撃を受ける可能性のある領域



CAASM

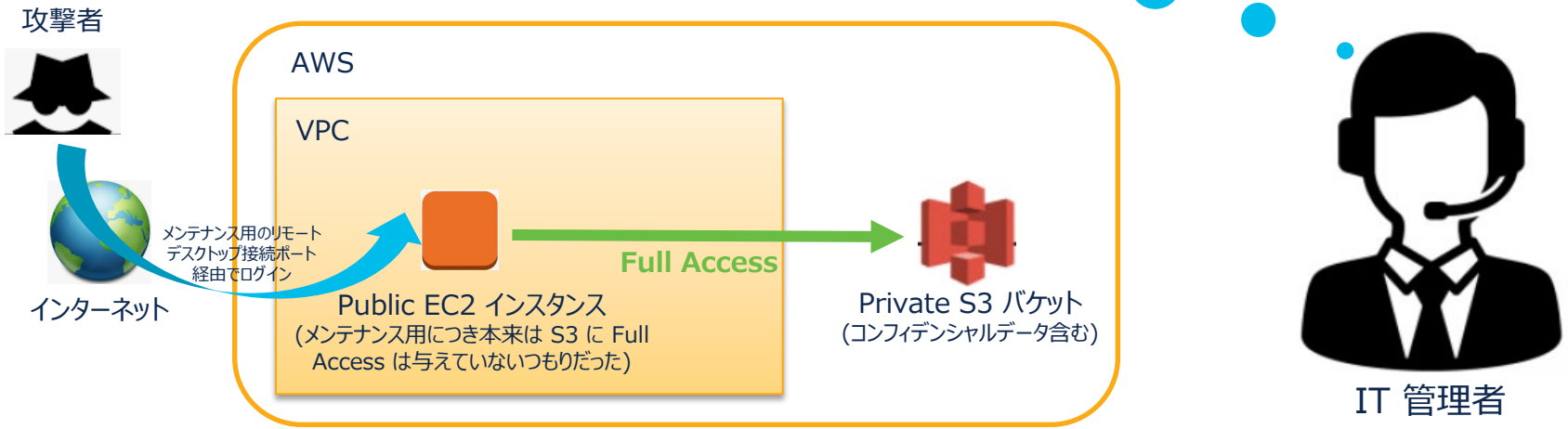
アタックサーフェスのマップ化

環境を横断した調査

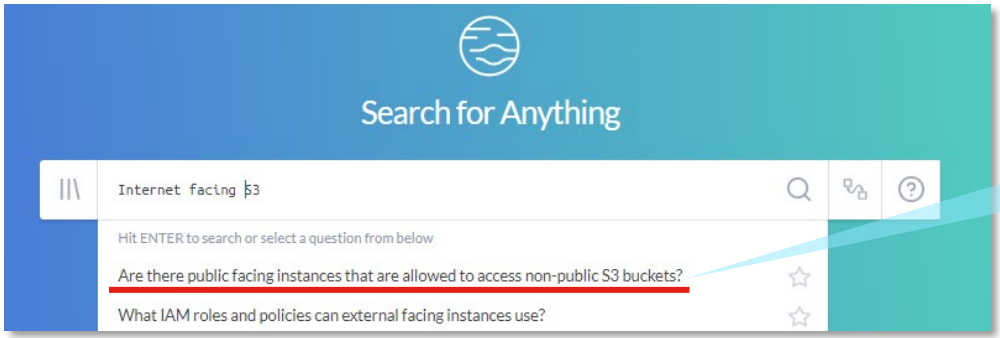
セキュリティポリシーアラート

リレーションシップマップによるアタックサーフェスリスクの検証

インターネットにさらされてしまっており、かつ非公開 S3
バケットにアクセスできてしまうインスタンスの有無を
確認したい or その設定構成があるとアラート通知させたい



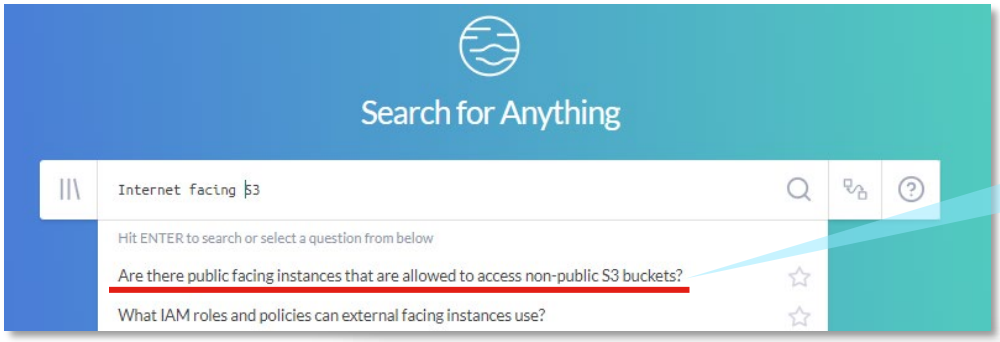
リレーションシップマップによるアタックサーフェスリスクの検証



インターネットにさらされてしまっており、かつ非公開 S3 バケットにアクセスできてしまうインスタンスは無いか？

550 のクエリの 1 つとして最初から定義済み

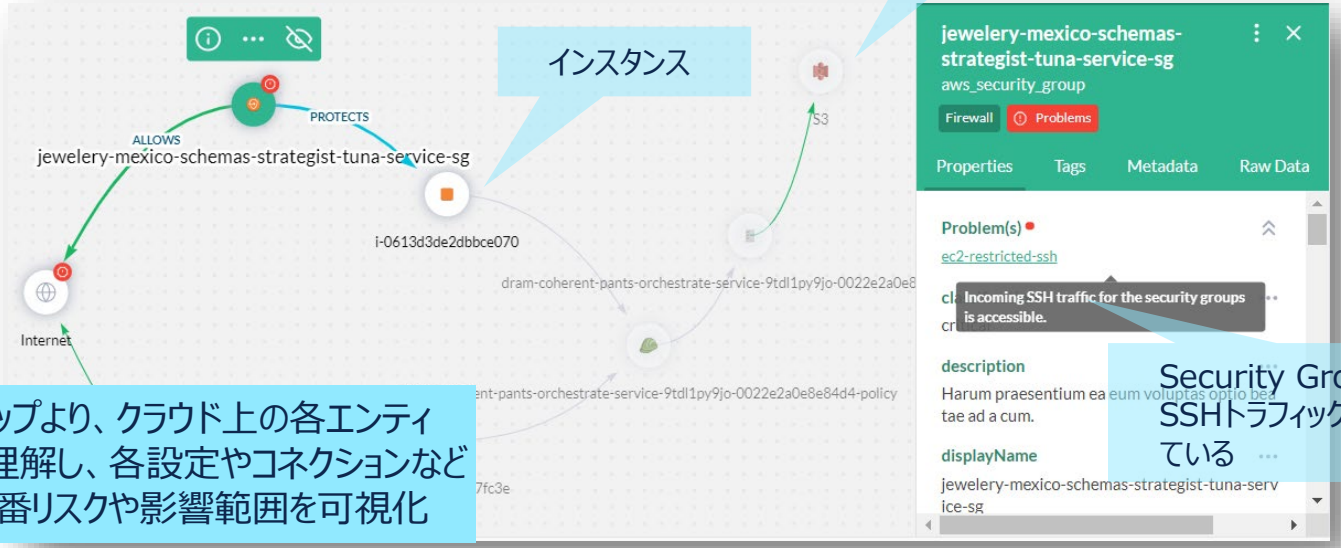
リレーションシップマップによるアタックサーフェスリスクの検証



インターネットにさらされてしまっており、かつ非公開 S3 バケットにアクセスできてしまうインスタンスは無いか？

非公開 S3 ストレージ

インスタンス

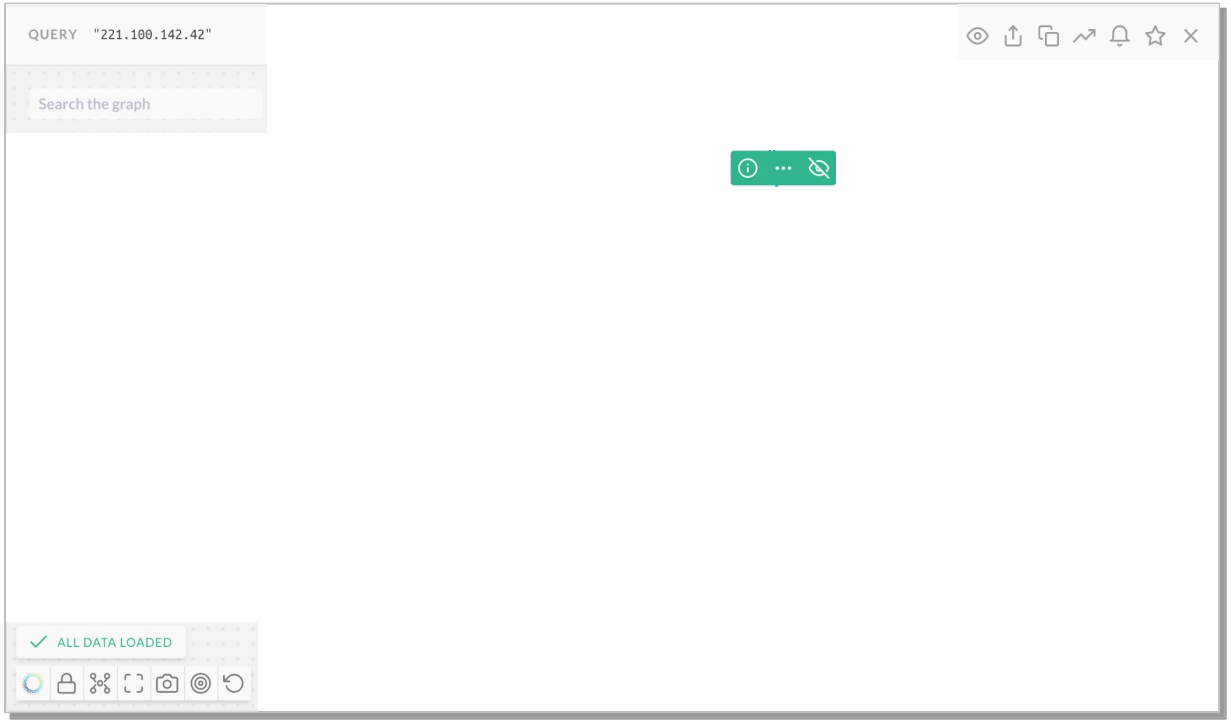


Security Group向け SSHトラフィックが許可されている

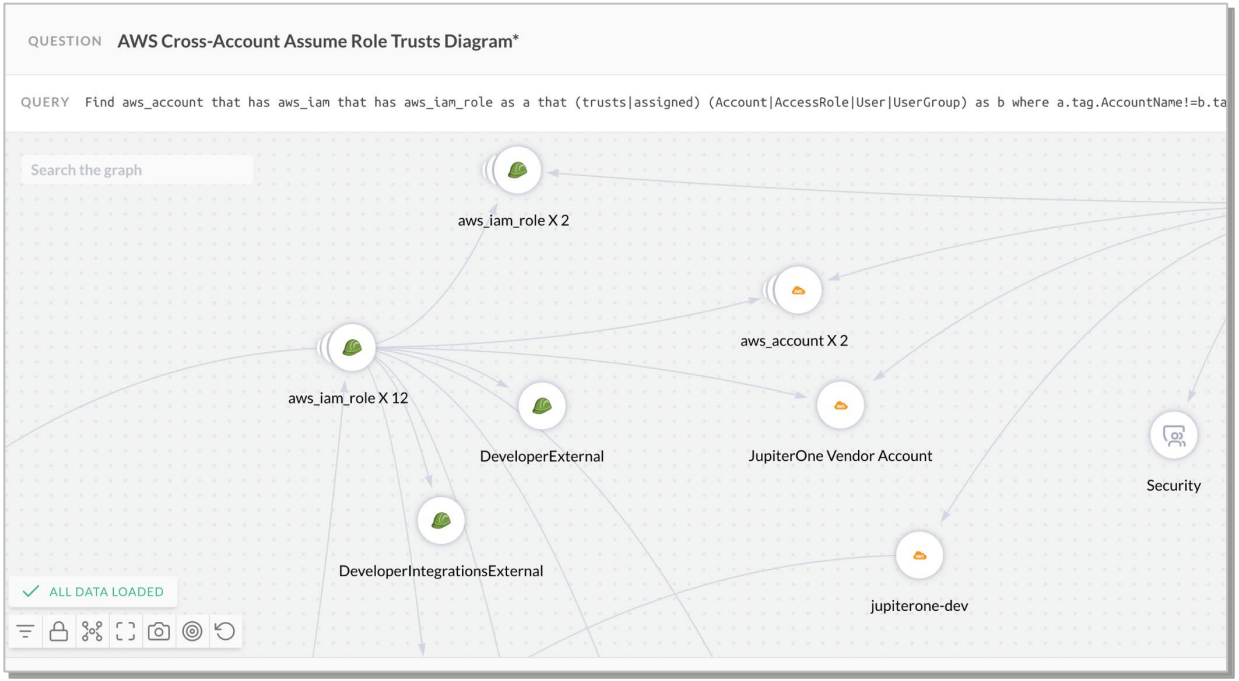
リレーションシップマップより、クラウド上の各エンティティの相関関係を理解し、各設定やコネクションなどを確認。脅威の伝番リスクや影響範囲を可視化

インシデントレスポンスのコンテキスト

- ノードを展開してデータのグラフを確認し、その関係性を見ることが可能
- 侵害されたアセットの影響を特定し、攻撃者が次に何をできるかを把握
- インシデントに関連するコンテキストを数秒で見つける

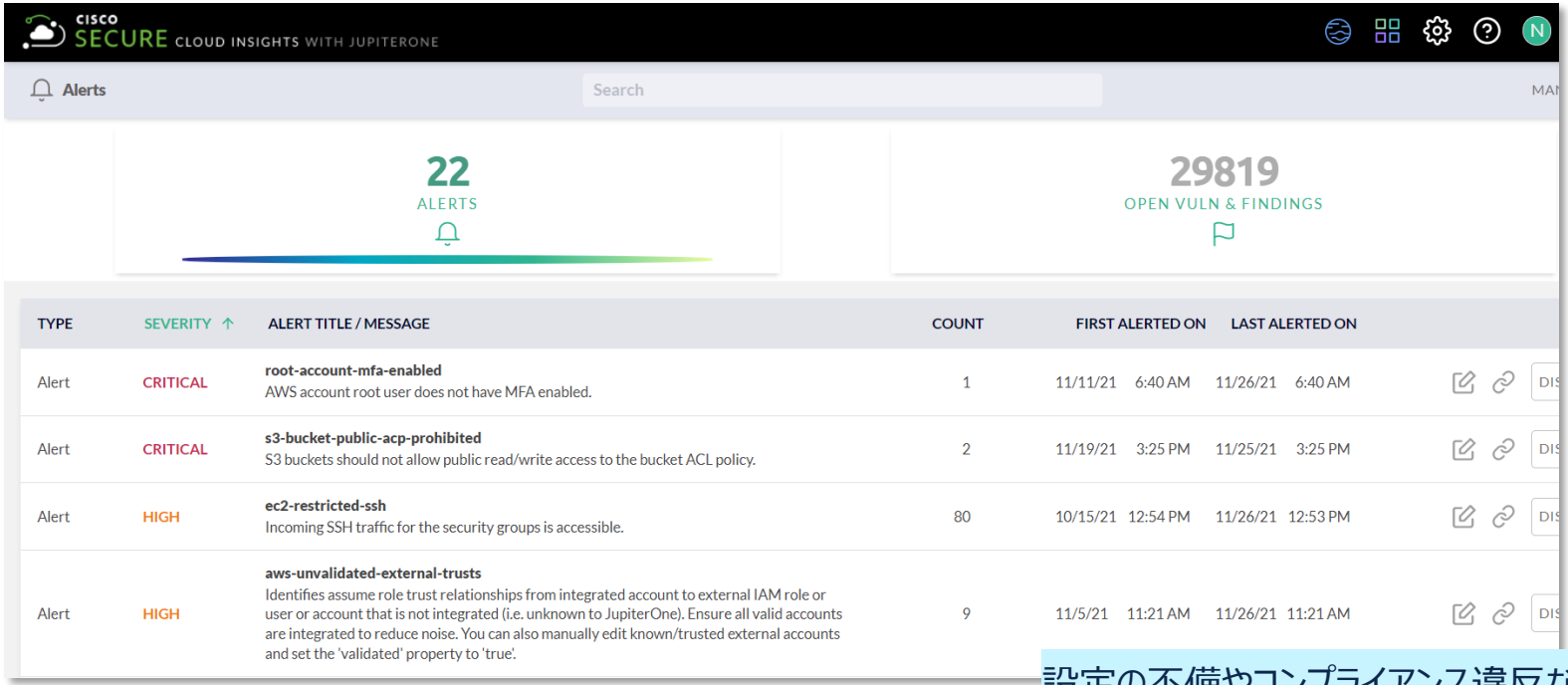


環境を横断した調査



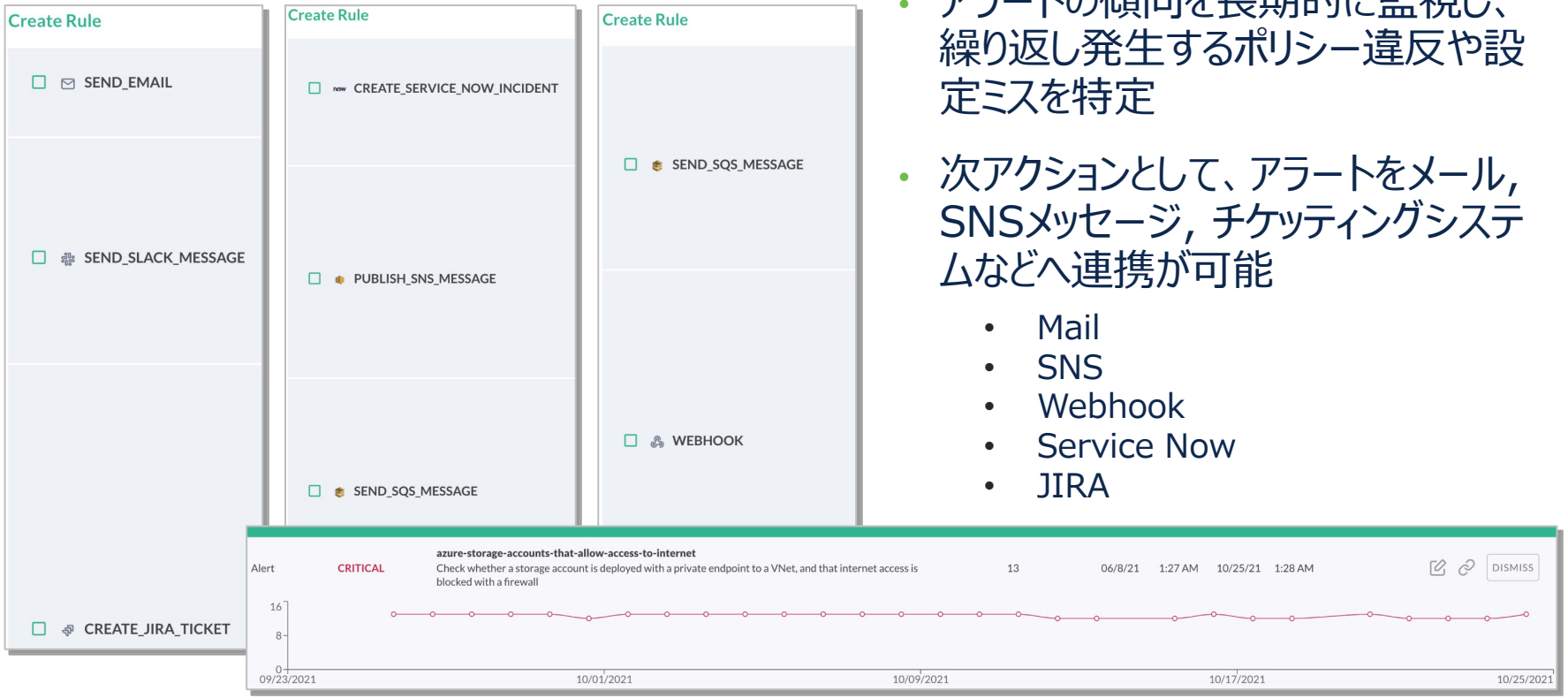
- 複雑な関係のクロスアカウントトラスト、vpcピアリング、vpcエンドポイントポリシー、IAMポリシー、ロードバランサーの設定など、すべてが自動的に発見される
- 環境を超えた「Blast Radius(影響範囲)」を発見し、脅威がクラウドのアカウントを超えて伝播するリスクを発見

アラート表示(重大度の表示が可能)



設定の不備やコンプライアンス違反などをアラートのダッシュボードからも確認でき、優先的に対処すべきアラートを表示可能

アラート通知(アラート毎に通知先を柔軟に選択可能)



- アラートの傾向を長期的に監視し、繰り返し発生するポリシー違反や設定ミスを特定
- 次アクションとして、アラートをメール, SNSメッセージ, チケッティングシステムなどへ連携が可能
  - Mail
  - SNS
  - Webhook
  - Service Now
  - JIRA

インテグレーション

統合可能なプラットフォーム

2021年11月時点

Vulnerability Agents

Bugcrowd
Detectify
GitLeaks
HackerOne
NowSecure
Qualys
Rapid7
Snyk
Tenable
Threat Stack
Veracode
Vuls.io
WhiteHat

Endpoints

Carbon Black
Cisco AMP
Crowdstrike
Duo
Jamf
SentinelOne
Trend Micro
AirWatch
Wazuh

Clouds

Amazon AWS
Microsoft Azure
Google Cloud

Network

Cisco Meraki
DigiCert
Nmap
Whois
Shodan

People & Access

Google G Suite
JumpCloud
Microsoft Azure AD
Okta
OneLogin

Workflows

Jira
PagerDuty
Slack
ServiceNow

Custom

GraphQL + REST API
NodeJS SDK

Others

Github
KnowBe4
BambooHR
GoDaddy

Secure Cloud InsightsとSecureXの統合

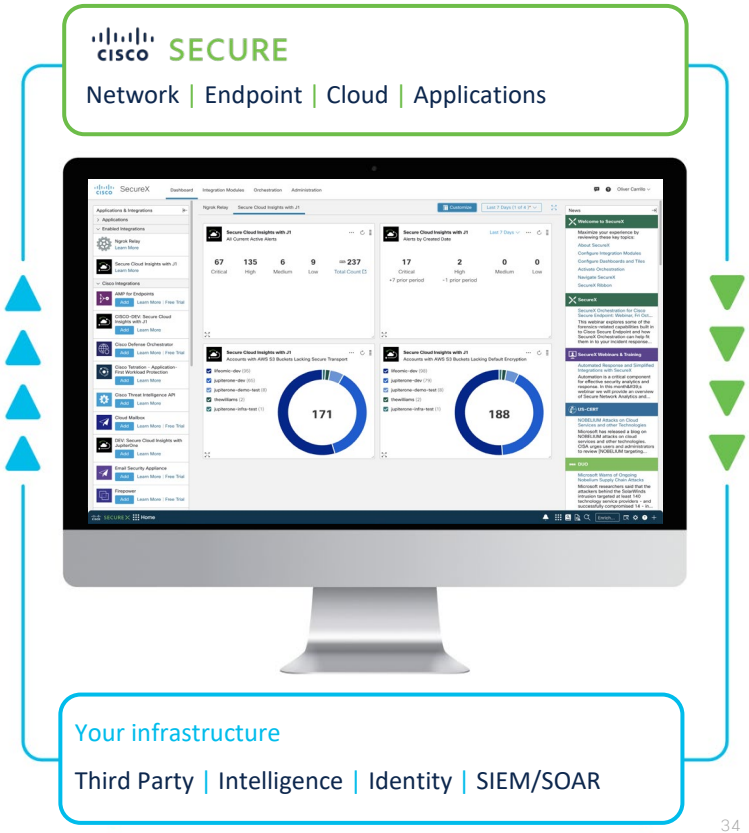
With SecureX:

- SecureX Sign Onを使用した認証と認可
- SecureX IntegrationモジュールとEntitlementが有効
- ユーザーはSecureXタイルを利用でき、2022年にはSecureXインシデント マネージャーとリボンの統合を2022年に予定

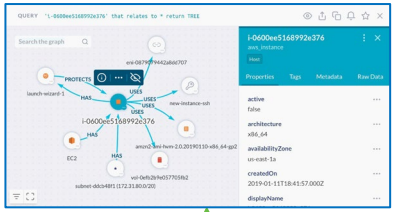
With Secure Cloud Insights:

- 4つのタイルが利用可能です。
  - 現在有効なすべてのアラート
  - 作成日によるアラート
  - セキュアなトランスポートを欠くAWS S3バケットを持つアカウント
  - AWS S3バケットのデフォルト復号化ができていないアカウント

さらに多くのタイルが順次追加されていきます



Secure Cloud InsightsとSecure Cloud Analyticsの Integration
－コンテキスト共有により、より正確な脅威の実態を把握

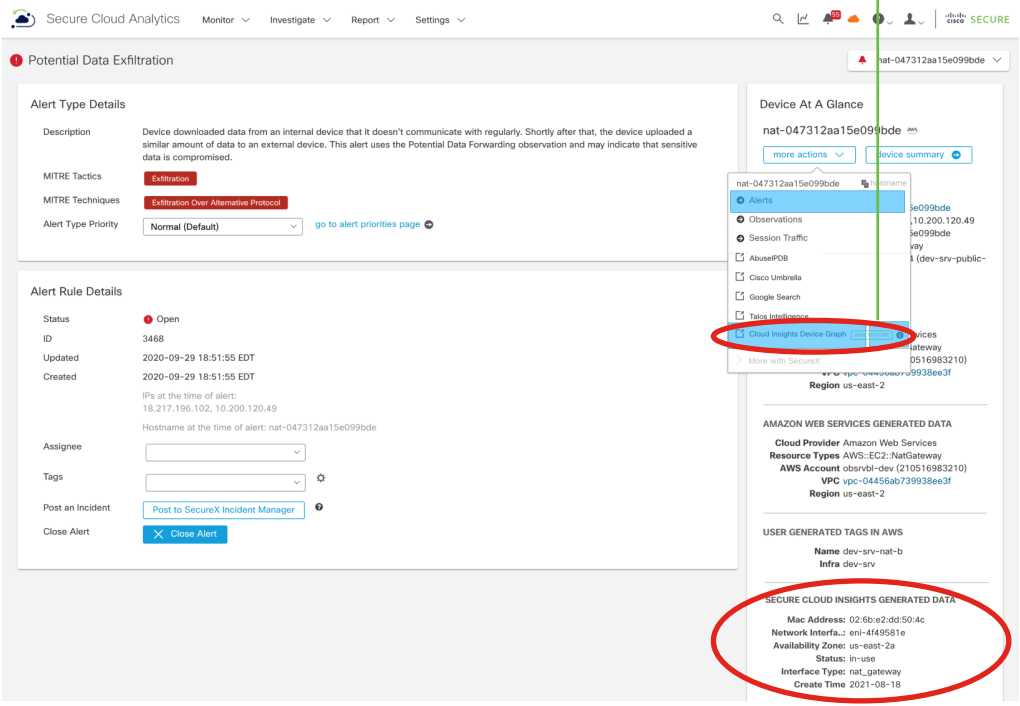


Secure Cloud Analytics

J1QL API Request for IP/ hostname data

J1QL API Response with metadata

Secure Cloud Insights



ケーススタディ (JupiterOne)

JupiterOne ユーザー事例
Databricks

databricks

AI、及び機械学習向け統合データ・アナリティクス・プラットフォームの提供企業

リレーションシップマッピング機能を利用し、AWS環境に対するプロアクティブなアタックサーフェス管理を実現

◆ お客様の課題／要件：

- 可視性、オープン性、拡張性を提供するクラウドフベースのサイバーアセット管理ソリューションが必要
- AmazonS3バケットのセキュリティ管理におけるリアクティブアラートと脆弱性管理

◆ 結果/導入効果：

- JupiterOneを導入してから1時間以内に重要で正確なデータを可視化
- リレーションシップマップにより、クラウド上のアセットの状態とその依存関係について、より詳細な情報を得ることができ、プロアクティブな脆弱性管理を実現

◆ J1のユースケース/主なインテグレーション対象

- リレーションシップマッピングによるAWS上のアセット可視化
- 定義済クエリによる課題や脆弱性の迅速な発見
- AWS、Qualys, Knowbe4

「私たちは、S3バケットを誰が所有しているか、それらが別のサービスを介してパブリックからアクセス可能かどうかなどを迅速かつ正確に知る機能を必要としていた。また脆弱性管理においてリアクティブからプロアクティブに移行したかった。そのための唯一の方法は、AWS環境のリソース間の関係を調べることでした」

Caleb Sima, VP of Security at DataBricks

https://info.jupiterone.com/resources/case-study-databricks

JupiterOne ユーザー事例
CODOXO

CODOXO
AI Solutions for Healthcare

医療費不正請求等を検知するためのAIベースのSaaSプラットフォームの提供企業

コンプライアンススタンダードの活用により、従来かかっていた多大な時間やコスト、リソースを大幅に削減、短期間で認証を取得

◆ お客様の課題／要件：

- SaaSプラットフォームに対するSOC2のコンプライアンス準拠やヘルスケア認証取得のために多大な時間とコスト、リソースを要していた
- 旧来の資産管理ツールやGRC(ガバナンス, リスク＆コンプライアンス)製品の導入には多大なコストや運用ワークロードがかかる

◆ J1のユースケース/主なインテグレーション対象

- ビルトインコンプライアンススタンダードの活用
- 定義済クエリによるコンプライアンス課題の発見
- AWS、Qualys, Jira, Snyk, KnowBe4, Jamf

https://info.jupiterone.com/resources/case-study-codoxo

◆ 結果/導入効果：

- 従来のセキュリティツールに比べわずかなコストで、セキュリティプログラムの成熟度、サイバーアセットの可視性、およびセキュリティガバナンスの向上を実現
- SOC2準拠やヘルスケア認証に必要な分析やエビデンスの50%以上を自動的かつ継続的に収集
- その結果、6か月未満でSOC2コンプライアンス、2か月未満でヘルスケア認証を達成

「以前はその場しのぎで探していた統合機能やデータの一部がJupiterOneに組み込まれていることが信じられませんでした」 Witt Cunningham, Head of Security, Codoxo

Cisco Security & Trust がJupiterOneを採用
クラウドセキュリティポスチャとアタックサーフェス(攻撃対象領域)管理における重要な課題を解決

デプロイメント:
- ~3,400 AWSアカウント
- ~1,500 Google Cloudアカウント
- ~ 800 Azureアカウント

ユースケース:
- セキュリティとポリシーの監視
- 既存のワークフローやレポートのニーズと容易に統合可能
- 社員のアクセスコントロール

まとめ

まとめ　Cisco Secure Cloud Insights の優位性

- **CAASM (Cyber Asset Attack Surface Management)**

  ・CSPM 機能に加え、種類が異なる IaaS のアセット情報を一元的に管理してリスクを把握するアタックサーフェス管理機能（CAASM）も有する

- **CSPM & CAASM での出力結果をマップ表示**

  ・構成の問題点だけでなく影響範囲まで迅速に把握できる
  ・マップ表示を維持したまま構成情報を把握できるため画面遷移を最小化できる
  ・仮に出力件数が多い場合も全体像を容易に把握できる

マップ表示だととにかく分かりやすいためユーザエクスペリエンスで大きなアドバンテージ

Competitive Overview

Use Cases and Functionalities	Cisco Secure Cloud Insights	Axonius	Wiz.io	Tugboat Logic & Vanta	Prisma Cloud	Divvy Cloud
Cyber Asset Visibility & Governance (cloud, non-cloud asset inventory)	✓	✓	✓		✓	✓
Cloud Native Security (Configuration, policy-as-code violations)	✓		✓		✓	✓
Governance, Risk, & Compliance (security audits, evidence collection, etc)	✓	✓	✓	✓	✓	✓
Security Operations (threat modeling, IR)	✓				●	
Vulnerability Management	✓				●	●
Configuration Monitoring & Alerting (IAM, IAG, infrastructure and endpoint monitoring)	✓	✓			●	●
Relationship graphs visibility	✓					

● Indicates the solution supports partial coverage or the solution does not provide integrations into 3rd party/external ecosystems

60日間のフリートライアル

- Sign up for a 60-day free trial
- Learn more https://www.cisco.com/c/en/us/products/security/secure-cloud-insights/index.html


CISCO
SECURE