

Cisco Secure Cloud Insights

Cloud security posture, cyber governance and
attack surface management

SWA, Japan, Cisco Systems,
2022年2月



Contents

1. クラウド時代におけるサイバーガバナンスの課題
2. Secure Cloud Insightsの概要
3. 主要ユースケース
 - クラウドセキュリティポスチャ管理 (CSPM)
 - サイバーアセットの可視化
 - Attack Surface Management
4. インテグレーション
5. ユーザー事例
6. まとめ

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戦略を採用されている¹

監視すべき攻撃サーフェス(攻撃対象領域)* の拡大

*攻撃サーフェス：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

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

パブリッククラウドセキュリティ重大度脅威トップ11

セキュリティ脅威

標的型攻撃や脆弱性、不適切な

クラウドベースのリソースは複雑であるため

クラウド利用の戦略よりも短期間でクラウド

データ、システム等へのリソースに関する

1 データ侵害

2 設定ミスと不適切な変更管理

3 クラウドセキュリティのアーキテクチャと戦略の欠如

4 ID、クレデンシャル、アクセス、キー管理が不十分

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

ZDNet Japan

海外発 デジタル変革 CIO ITインフラ セキュリティ

クラウド環境の侵害、3分の2は設定ミスの見直しで防止できた可能性-- IBMレポート

Charlie Osborne (Special to ZDNet.com) 翻訳校正: 石橋啓一郎 2021-09-22 07:30

新たな調査で、クラウド環境で発生したセキュリティインシデントの3分の2は、アプリケーションやデータベース、セキュリティポリシーの設定が適切であれば回避できたことが明らかになった。

<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

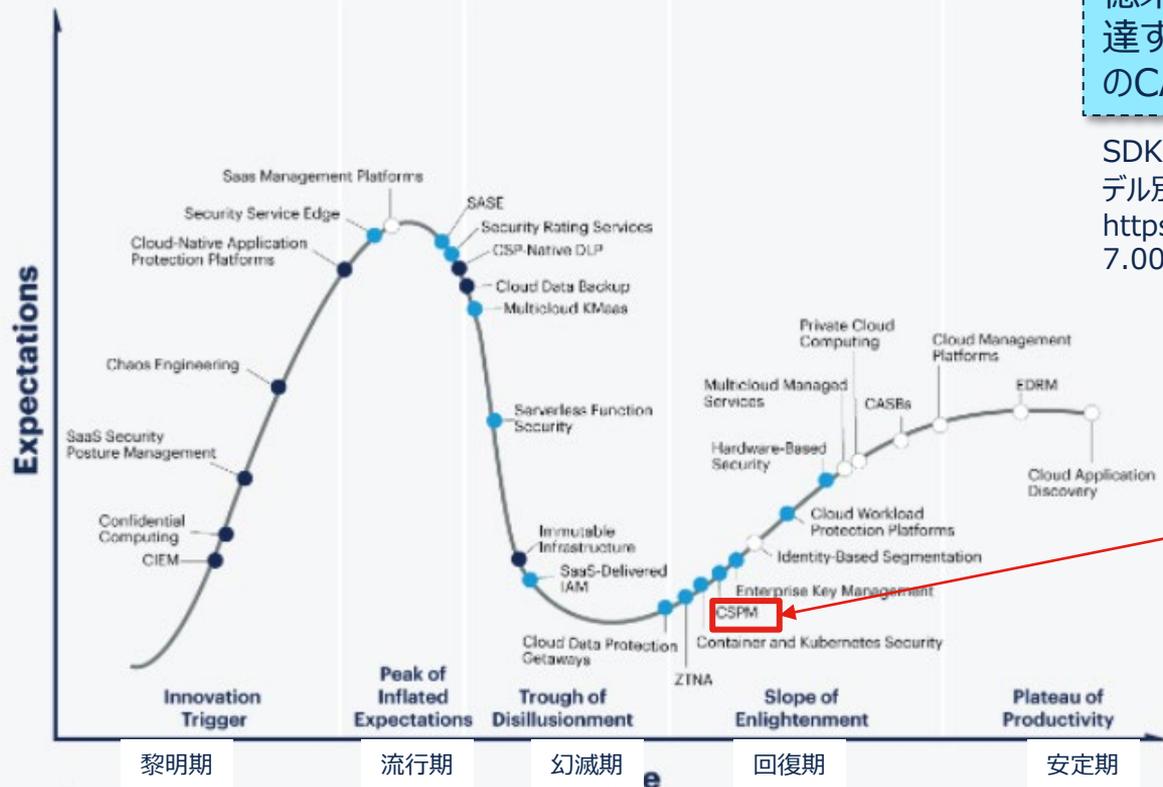
IaaSなどパブリッククラウドに対してAPI連携により、クラウド側の設定を自動的に確認し、セキュリティの設定ミスや各種コンプライアンスフレームワーク等への違反が無いかを継続してチェックする

➤ **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

Hype Cycle for Cloud Security, 2021



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-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-世界の予測2026年
<https://prtmes.jp/main/html/rd/p/000000237.000072515.html>

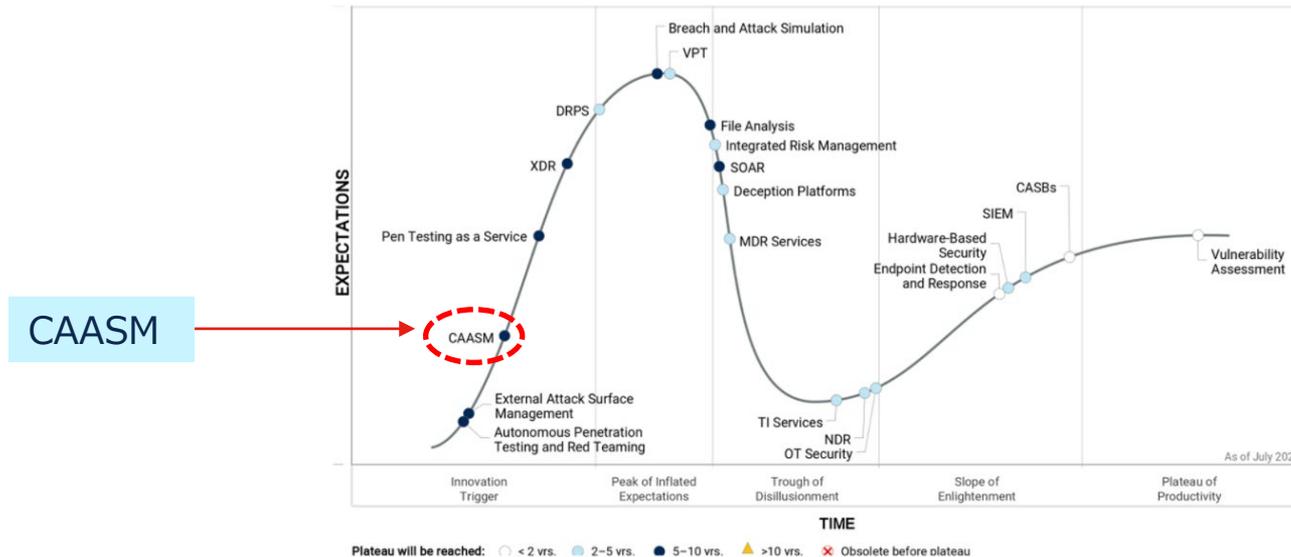
CSPM

Plateau will be reached:

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)

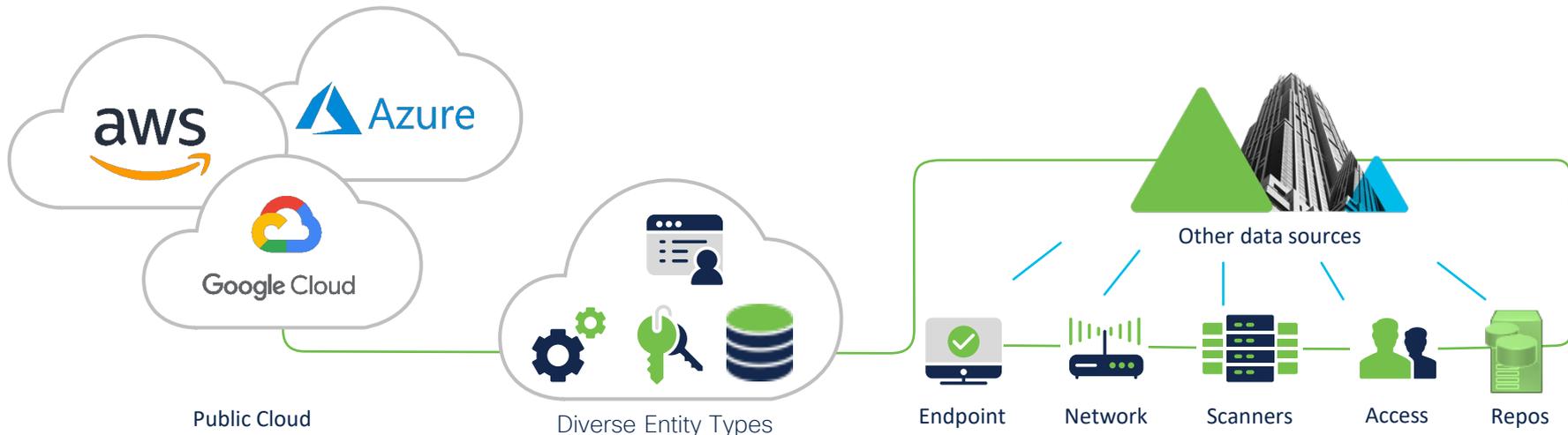
Figure 1: Hype Cycle for Security Operations, 2021



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=CjwKCAIA4veMBhAMEiW AU4XRr5LMqw6M2-WMWF9Mr63YhrnXissVg55beXSQqFkQ1oicQdtqWN0h0Cb5UQA4vD_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



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



3. アラートとレスポンス

アラートが検出されると、チケットングシステム等に通知

- 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

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)



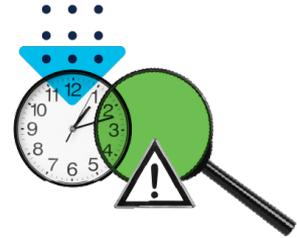
セキュリティポスチャの 完全可視化

- 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標準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



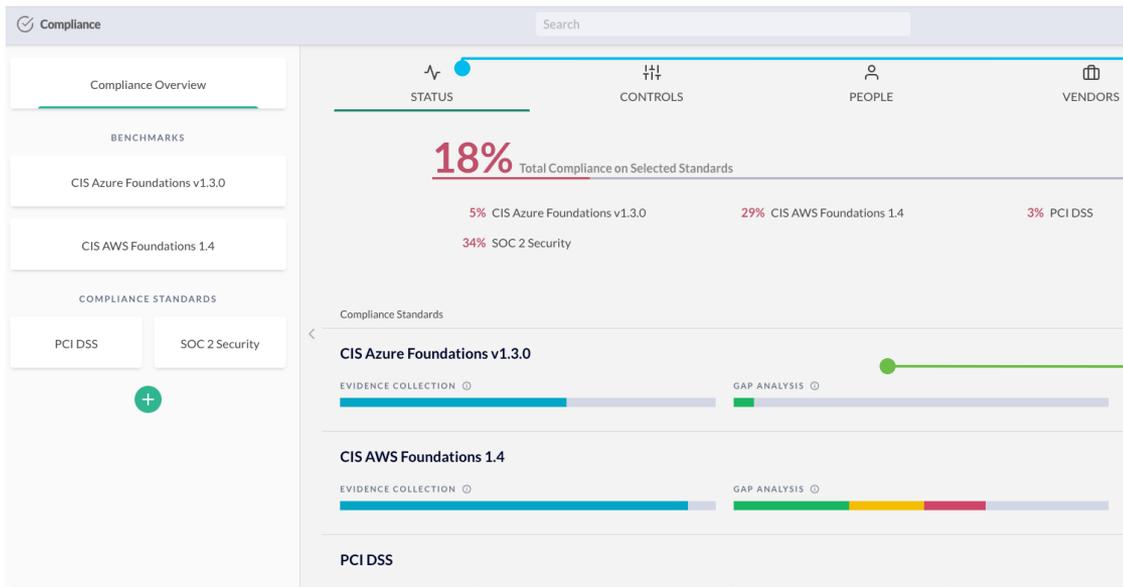
継続的なコンプライアンスレポート



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



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

aws **AWS**
CREATE CONFIGURATION SETUP INSTRUCTIONS

CONFIGURATION SETTINGS

Account Name
The account name or alias that uniquely identifies this integration configuration.

Description
A description of the configuration.

Polling Interval
The interval at which this integration will run.

- DISABLED
- THIRTY_MINUTES
- ONE_HOUR
- FOUR_HOURS
- EIGHT_HOURS**
- TWELVE_HOURS
- ONE_DAY
- ONE_WEEK**

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？



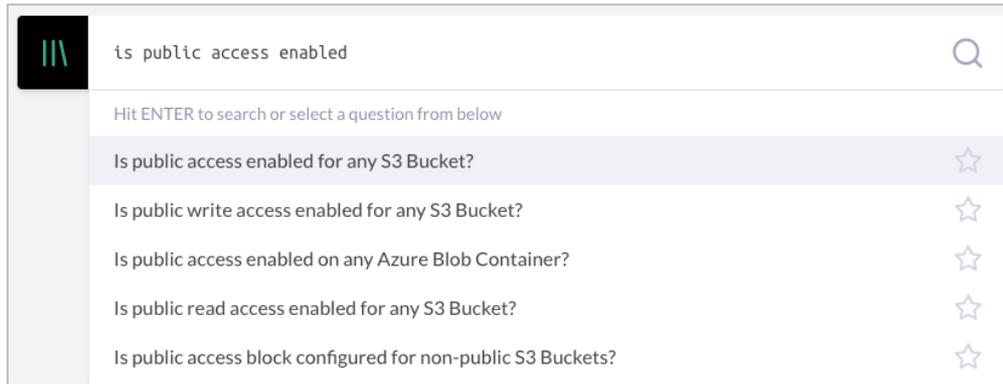
本番系インスタンスは？



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？



去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

Add Compliance Framework Specification

Display Name
The name or alias of this configuration

Specification
Paste your compliance framework file below in JSON or CSV format. See community examples at <https://github.com/JupiterOne/security-policy-templates/tree/main/templates/standards>.
CSV data containing the following keywords in the column headers will be auto converted into JSON: 'section' (or 'domain'), 'id', 'title' (optional), 'requirement' (or 'summary')

1	
---	--

You have used 5 out of unlimited Compliance Modules included in your subscription.

You must have obtained the necessary license and permission to use the framework for your organization. Licensing is not provided by JupiterOne.

新しいコンプライアンススタンドの作成や既存のカスタマイズが可能

Edit question

Queries

1	bad	Query results are Bad
<p>Query</p> <pre>find azure_role_definition with roleType='CustomRole' and actions =~ '*' and assignableScopes!~=('/resourceGroup/' and '/providers/')</pre>		

Compliance

1	CIS Azure Foundations	<p>Standard</p> <p>Requirement/Control Mappings</p> <p>1.23 <input type="button" value="x"/></p>
2	CIS Azure Foundations v1.3.0	<p>Standard</p> <p>Requirement/Control Mappings</p> <p>1.21 <input type="button" value="x"/></p>

サイバーアセットの可視化



インテグレーション

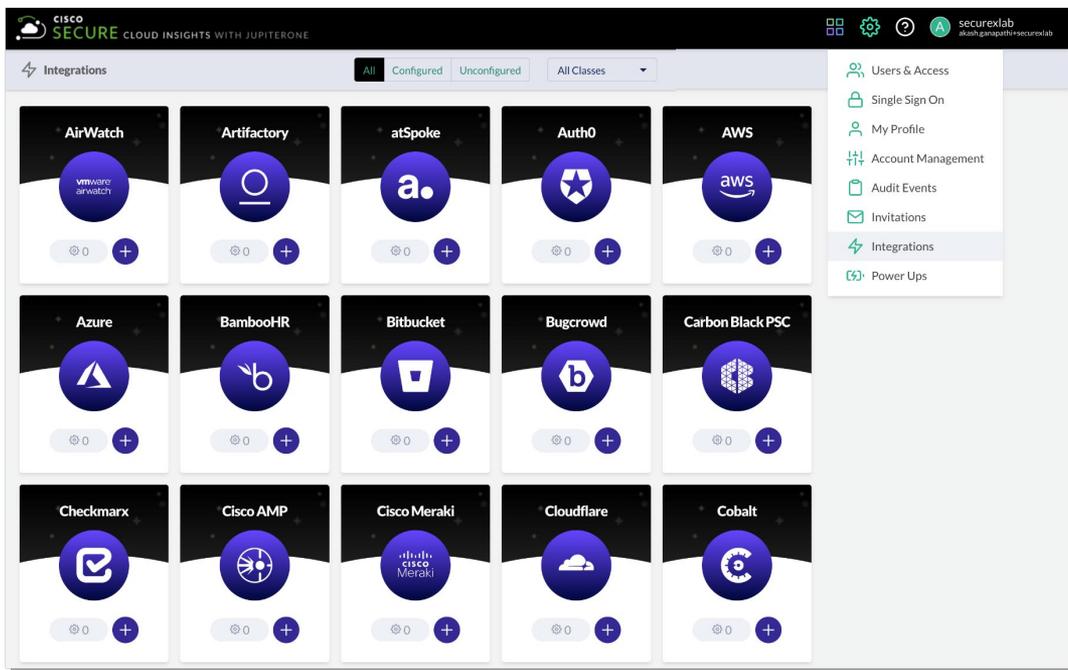


リレーションシップマッピング



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

The screenshot displays a dashboard with the following asset counts:

- 55 AccessKey
- 4377 AccessPolicy
- 1607 AccessRole
- 35 Account
- 22 Alert
- 67 Application
- 139 Assessment
- 2017 Backup
- 32 Certificate
- 24288 Change
- 113 Channel
- 59 Cluster
- 149 CodeModule
- 854 CodeRepo
- 1268 CodeReview
- 6564 Configuration
- 3561 DataStore
- 7 Domain

The detailed view shows a table of assets with the following columns: DISPLAY NAME, CLASS, TYPE, and ACCOUNTNAME. The table lists several assets, including those associated with Google Storage and Amazon EBS.

DISPLAY NAME	CLASS	TYPE	ACCOUNTNAME
j1-gc-integration-dev-v3-super-secret-stuff	DataStore	google_storage_bucket	j1-gc-integration-dev-v3
Rau - Schmidt-instance-vol-0j3sz47cqbbpk7fy-2020-0...	DataStore	Disk Image Backup	aws_ebs_snapshot fuchsia-research-pizza-service-keypair
specialist-nlue-illinois-transmit-service-464	DataStore	Disk Image Backup	aws_ebs_snapshot montana-compress-intranet-transitional-silver-bricks-a...
Kuhic - Wuckert-instance	DataStore	Disk	aws_ebs_volume montana-compress-intranet-transitional-silver-bricks-a...
Rau - Schmidt-instance-vol-0fp0kavt6r2s8nfwd-2020-0...	DataStore	Disk Image Backup	aws_ebs_snapshot shirt-handcrafted-keyboard-creative-interface-white-re...
administrator-money-stream-borders-refined-right-sze...	DataStore	Disk Image Backup	aws_ebs_snapshot fuchsia-research-pizza-service-keypair

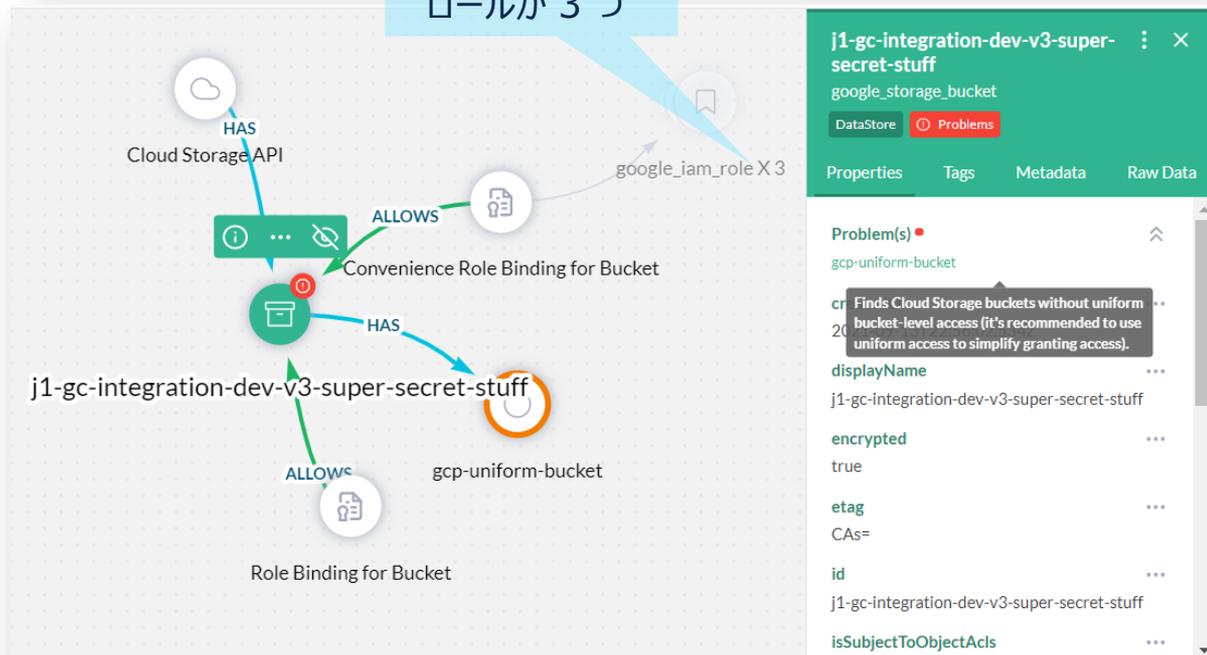
- ネイティブな統合機能により、セキュリティプログラム全体からアセットを簡単に発見することができる
- エンドポイント、データストア、ポリシー、セキュリティグループなど、さまざまなタイプのアセットを発見し、異なるパブリッククラウドやアセットのタイプを一元管理することができる

Google Storage

Amazon EBS

アセットのリレーションシップマッピング

アクセス可能な
ルールが 3 つ



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

The screenshot displays the Cisco Secure Cloud Insights interface. At the top, it says 'CISCO SECURE CLOUD INSIGHTS WITH JUPITERONE'. Below that, there's a navigation bar with 'Assets > Inventory' and a search bar. A toolbar with various icons is visible. Underneath, there's a 'TYPE' filter section with several options: 'aws_db_cluster_snapshot 281', 'aws_db_instance 30', 'aws_dynamodb_table 406', 'aws_ebs_snapshot 1736', 'aws_ebs_volume 847', 'aws_elasticache_cluster_node 10', 'aws_elasticache_redis_cluster 4', 'aws_elasticsearch_domain 8', 'aws_rds_cluster 12', and 'aws_s3_bucket 221'. The main area shows a table with columns: 'DISPLAY NAME', 'CLASS', 'TYPE', 'ACCOUNTNAME', 'BACKUP', and 'CLASSIFICATION'. The table contains several rows of asset data. Overlaid on the bottom part of the screenshot is a 'SEARCH' overlay with a green logo and a search bar containing the text 'Ask a question, enter a query, or run a full-text search'. Below the search bar are two checkboxes: 'Include recently deleted entities in query/search' (unchecked) and 'Enable autocomplete for J1QL' (checked).

DISPLAY NAME	CLASS	TYPE	ACCOUNTNAME	BACKUP	CLASSIFICATION
generate-content-computer-service-bucket	DataStore	aws_s3_bucket	fuchsia-research-pizza-service-keypair	—	—
withdrawal-bluetooth-web-readiness-assimilated-chief...	DataStore	aws_s3_bucket	principal-refined-shoes-rupee-intermediate-service	—	public
azure-garden-one-to-one-summit-service	DataStore	aws_s3_bucket	fuchsia-research-pizza-service-keypair	—	internal
deposit-initiatives-hol					
stream-models-plum-f					
grow-multi-byte-agen					
web-fresh-bike-servic					

- 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

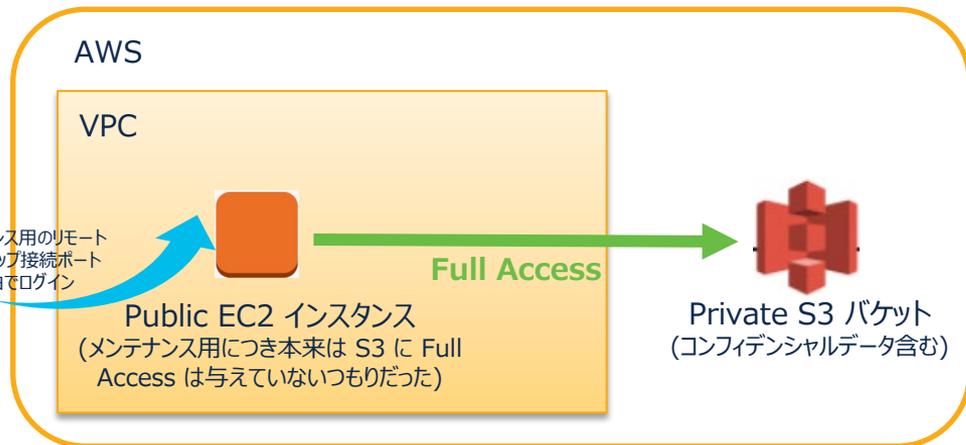
インターネットにさらされてしまっており、かつ非公開 S3 バケットにアクセスできてしまうインスタンスの有無を確認したい or その設定構成があるとアラート通知させたい

攻撃者



インターネット

メンテナンス用のリモート
デスクトップ接続ポート
経由でログイン



IT 管理者

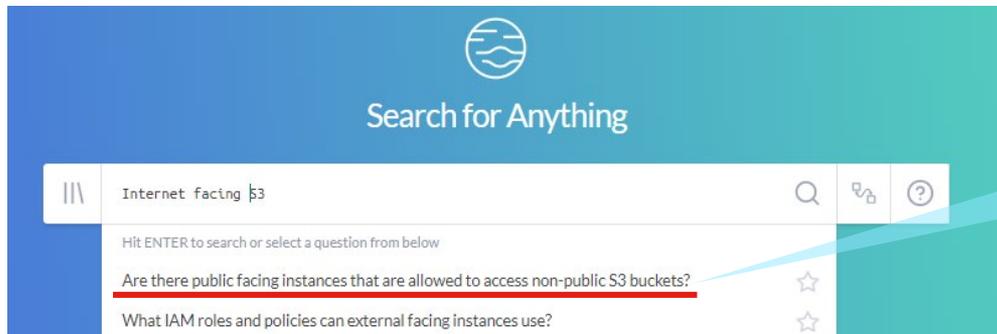
リレーションシップマップによるアタックサーフェスリスクの検証



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？

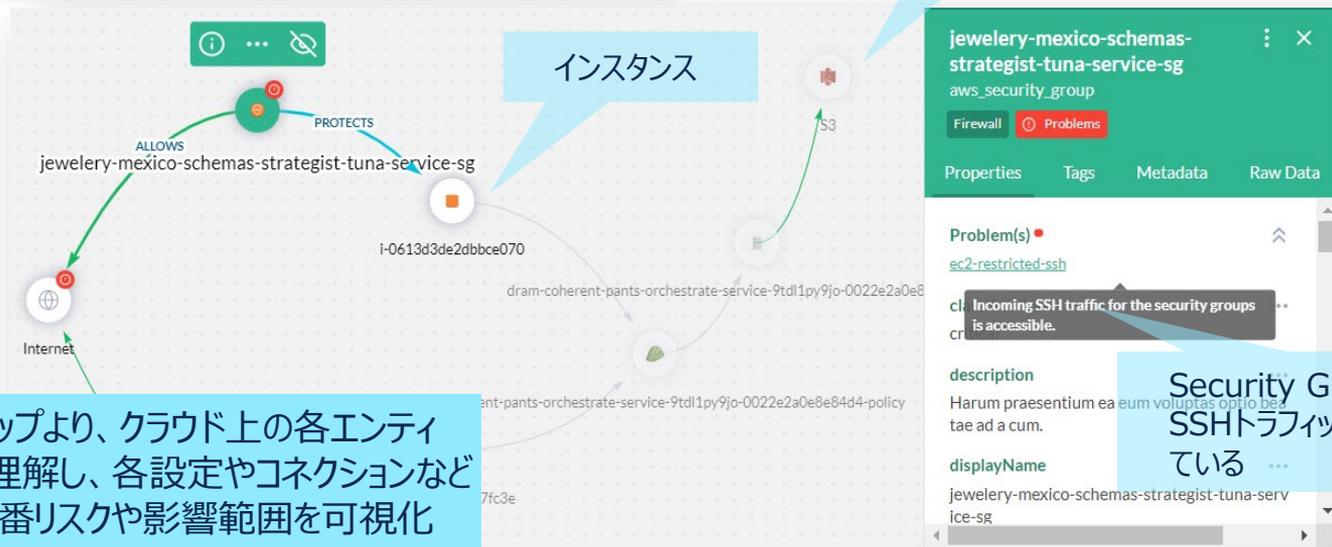
550 のクエリの 1 つとして最初から定義済み

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スは無いかな？

非公開 S3 ストレージ



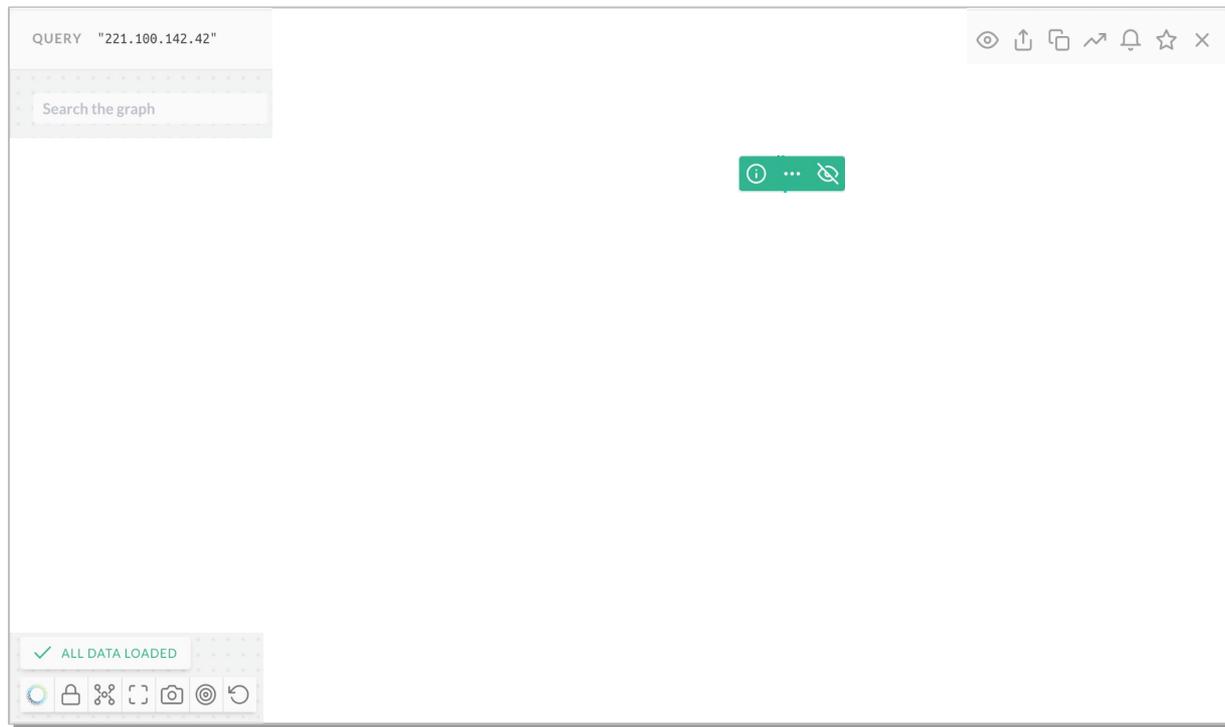
インスタス

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

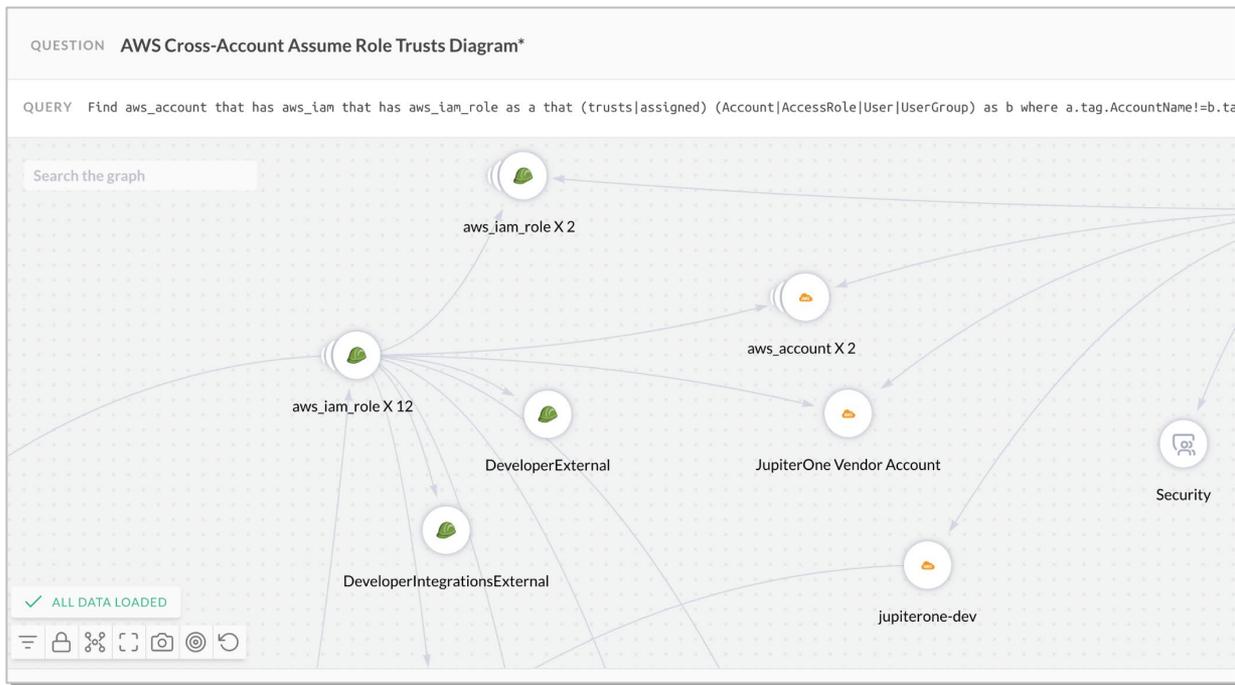
Security Group向け SSHトラフィックが許可されている

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

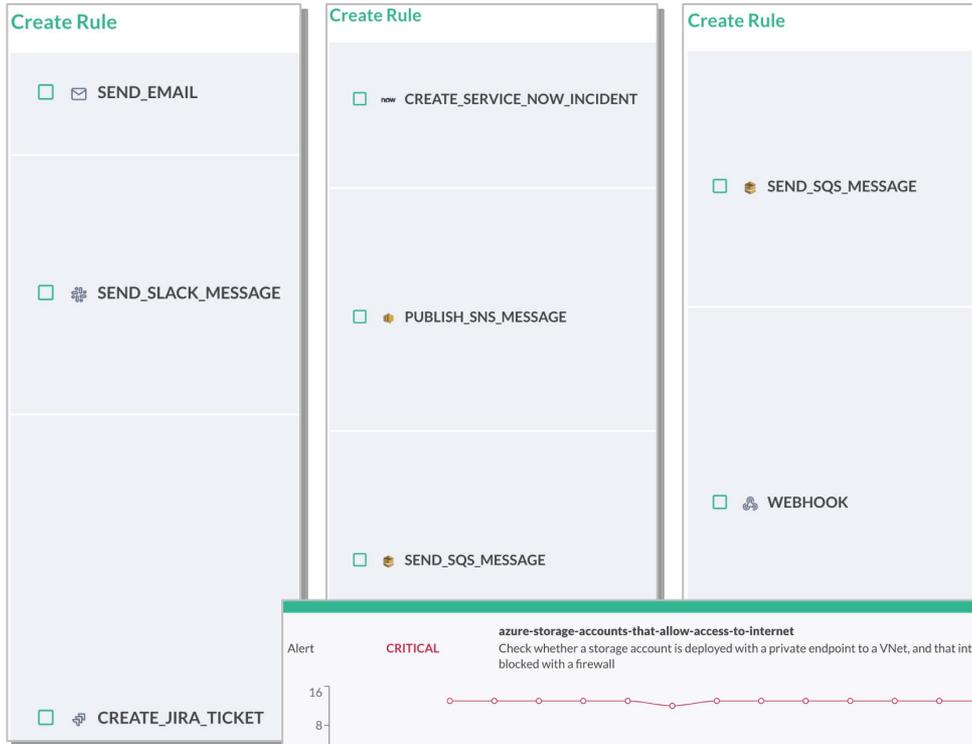
アラート表示(重大度の表示が可能)

The screenshot displays the Cisco Secure Cloud Insights with JupiterOne Alerts dashboard. At the top, there are navigation icons and a search bar. Below the navigation, there are two summary cards: one for '22 ALERTS' and another for '29819 OPEN VULN & FINDINGS'. The main content is a table of alerts.

TYPE	SEVERITY ↑	ALERT TITLE / MESSAGE	COUNT	FIRST ALERTED ON	LAST ALERTED ON	
Alert	CRITICAL	root-account-mfa-enabled AWS account root user does not have MFA enabled.	1	11/11/21 6:40 AM	11/26/21 6:40 AM	DIS
Alert	CRITICAL	s3-bucket-public-acp-prohibited S3 buckets should not allow public read/write access to the bucket ACL policy.	2	11/19/21 3:25 PM	11/25/21 3:25 PM	DIS
Alert	HIGH	ec2-restricted-ssh Incoming SSH traffic for the security groups is accessible.	80	10/15/21 12:54 PM	11/26/21 12:53 PM	DIS
Alert	HIGH	aws-unvalidated-external-trusts Identifies assume role trust relationships from integrated account to external IAM role or user or account that is not integrated (i.e. unknown to JupiterOne). Ensure all valid accounts are integrated to reduce noise. You can also manually edit known/trusted external accounts and set the 'validated' property to 'true'.	9	11/5/21 11:21 AM	11/26/21 11:21 AM	DIS

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, チケット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

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

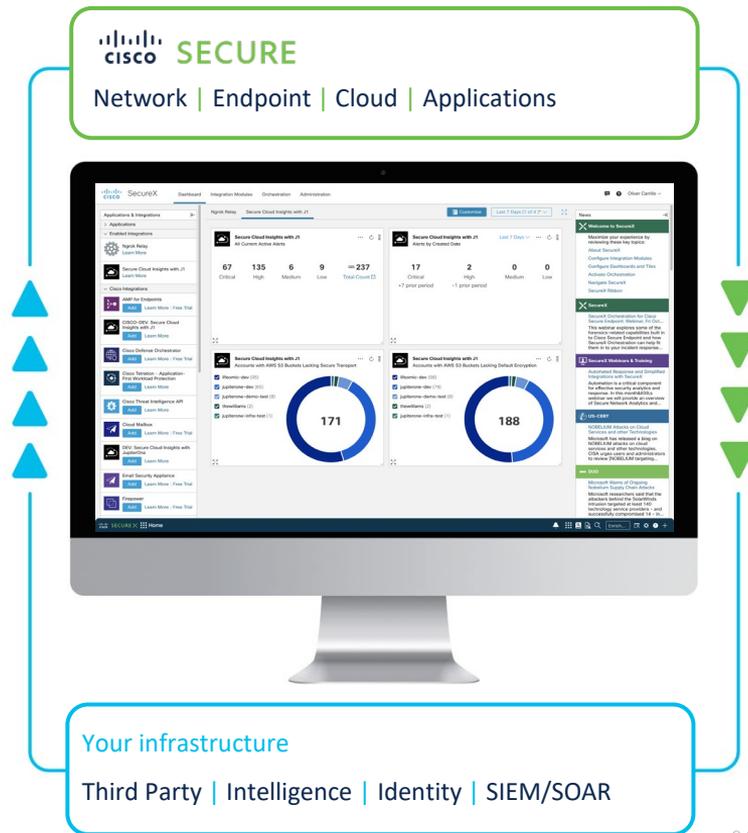
Secure Cloud InsightsとSecureXの統合

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:

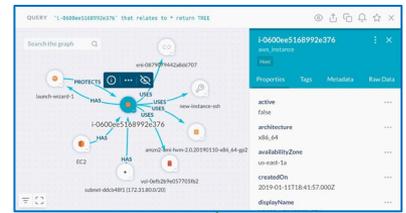
- 4つのタイルが利用可能です。
 - 現在有効なすべてのアラート
 - 作成日によるアラート
 - セキュアなトランスポートを欠くAWS S3バケットを持つアカウント
 - AWS S3バケットのデフォルト復号化ができていないアカウント
- さらに多くのタイルが順次追加されていきます





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

Secure Cloud Insights

J1QL API Request for IP/hostname data

J1QL API Response with metadata

The screenshot shows the 'Potential Data Exfiltration' alert details page. It includes sections for 'Alert Type Details' (Description, MITRE Tactics, MITRE Techniques, Alert Type Priority), 'Alert Rule Details' (Status, ID, Updated, Created, IPs at the time of alert, Hostname at the time of alert, Assignee, Tags, Post to Incident, Close Alert), and a 'Device At A Glance' sidebar. The sidebar lists various categories like Alerts, Observations, Session Traffic, AbusePDB, Cisco Umbrella, Google Search, and Talos Intelligence. A red circle highlights the 'Cloud Insights Device Graph' link in the sidebar. Below the sidebar, there are sections for 'AMAZON WEB SERVICES GENERATED DATA' (Cloud Provider, Resource Types, AWS Account, VPC, Region) and 'USER GENERATED TAGS IN AWS'. A second red circle highlights the 'SECURE CLOUD INSIGHTS GENERATED DATA' section, which includes Mac Address, Network Interface, Availability Zone, Status, Interface Type, and Create Time.

ケーススタディ (JupiterOne)

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

◆ 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

◆ 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

「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



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

◆ 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

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



SECURITY&TRUST

125,000

Combined Global Workforce



2,500

IT Applications



40,000

Routers



1,350

Engineering Labs



26,000

Remote Office Connections



500

Cloud Applications



Every day at Cisco, we protect our enterprise by securing:

In 170 Countries around the globe

Every day, this massive complex data system produces:

47TB

of Traffic

15B

Netflow Records

4.8B

DNS Queries

75M

Web Transactions

Cisco Security & Trust がJupiterOneを採用
クラウドセキュリティポスチャと攻撃サーフェス(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

マップ表示だとかんがえ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	✓					





60日間のフリーストライアル

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



SECURE