The bridge to possible

Cisco Attack Surface Management with JupiterOne

Benefits

- Gain complete visibility and understanding of your cloud security posture across multiple clouds
- Continuously monitor cloud environments to detect policy violations or misconfigurations
- Understand your entire attack surface by mapping relationships between assets
- Quickly investigate and remediate impacted assets by pinpointing your blast radius

The continued adoption of cloud-first and digital transformation strategies has fundamentally changed the way businesses operate. Organizations are migrating to new tools, systems, and processes to not only propel their businesses forward, but thrive in a rapidly changing world. This has helped improve agility, speed time to market, and increase productivity while reducing costs.

However, this has also created new problems for cybersecurity. As IT assets move beyond on-premises devices to the cloud, the ephemeral nature of the cloud has led to asset proliferation as well as increased scale and complexity. Moreover, there is no centralized view for an ever-expanding universe of cloud assets, and siloed security tools show only bits and pieces of the bigger picture.

This makes it difficult for security teams to answer even the most basic questions about their cloud environments and assets. How do you secure what you can't see or don't know you have? Visibility into cloud assets with rich context is critical to understanding your end-to-end attack surface, protecting your cloud environments from threats, and closing any potential security gaps.

The bridge to possible

Drastically reduce security and compliance risks

We have partnered with JupiterOne to address these challenges through our solution, Cisco Attack Surface Management (ASM). Cisco ASM provides complete visibility into your cloud environments to help you identify security and compliance gaps while accelerating threat investigation and response.

By building a comprehensive inventory of your assets Cisco ASM helps you understand your attack surface with relationship mapping to navigate cloud-based entities and access rights, and strengthens your cloud security posture while improving compliance with security and compliance reporting.

Moreover, Cisco ASM seamlessly operates with the rest of the Cisco Secure portfolio through seamless operability with Cisco XDR™, in addition to utilizing Device Insights capabilities built into Cisco XDR.

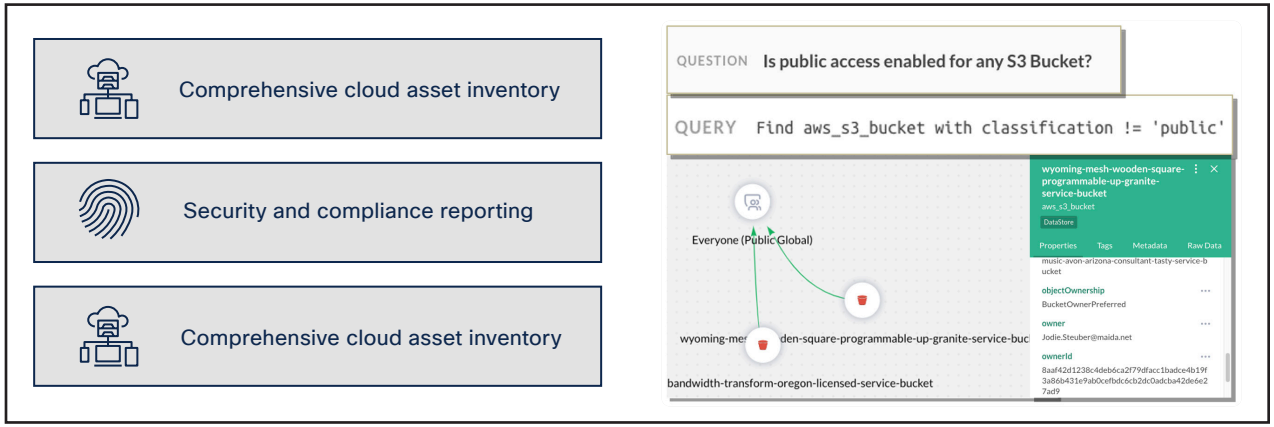

Figure 1. Introducing Cisco Attack Surface Management

Gain complete visibility into your cloud security posture

Cisco ASM gives you a comprehensive understanding of your cloud asset footprint, including your cloud security posture, through visibility into multiple cloud environments. This includes public cloud providers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud as well as containers and serverless environments.

It offers integrations with hundreds of industry-leading technologies to give you a single source of truth for your cloud assets. As a result, you can easily build an accurate, end-to-end inventory of your cloud assets, which includes deep context on asset relationships since Cisco ASM uses a graph-based approach allowing you to easily discover, map, visualize, and navigate relationships between your assets.

This is valuable because knowing the relationships between your cloud assets is as important as knowing what and where those assets are. These relationships can help you understand the impact and potential risks of cloud assets on your security environment. For example, you can use these asset visibility and contextual relationships to get end-to-end insights into your cloud attack surface. This allows you to map out, analyze, and understand complex attack surfaces that often span across multiple clouds.

The bridge to possible

Easily identify cloud security and compliance gaps

In addition to cloud visibility, Cisco ASM continuously monitors your cloud environments to detect policy violations and misconfigurations. Cloud environments are very dynamic, which means that your cloud assets, their configuration, and policies that govern them frequently change. This means that your cloud environments require continuous monitoring to notify you of any misconfigurations or compliance violations.

Cisco ASM keeps your security and compliance teams up to date on everything in your cloud environments by enumerating your cloud assets and performing deep analysis, alerting you to potential security risks, compliance drift, and cloud misconfigurations. It integrates directly with your Cloud Service Providers (CSPs) to continuously assess, audit, and evaluate configurations of your cloud resources. This allows you to reduce overall cloud security risks and rapidly detect compliance drift.

Furthermore, Cisco ASM offers dashboards and reporting that lets you quickly review your security and compliance status while identifying gaps in your security and compliance frameworks. This includes several prebuilt standards and frameworks such as CSPM benchmarks, CIS, NIST, SOC 2, PCI DSS, and more. These security standards and compliance frameworks are mapped directly to your cloud assets and environments so you can take the guesswork out of the process and focus on the quickest path to strengthening your cloud security posture and achieving compliance.

Fast-track investigation and response

The AI-powered natural language search in makes it approachable for all teams, allowing users to ask questions and have them translated into specific queries on the fly. This means that teams can benefit from the asset insights generated by without needing to be experts in using the platform. Additionally, AI is utilized to provide compliance and security remediation guidance based on best practices and the organization's needs.

Some examples of the natural language search are:

- Are any of our S3 buckets in AWS exploitable?
- What new IAM users have been created in the last week?
- Are my cloud assets aligned with my CSPM benchmarks?
- Do I have data stores in any CSP that are internet facing?

The bridge to possible

Cisco ASM provides deep cloud asset and relationship context that speeds threat investigation and response. This rich contextual information helps you pinpoint the blast radius of a potential breach by understanding the impact and relationships of a vulnerable asset. For example, you can easily identify, prioritize, and remediate all cloud assets connected to a compromised device and/or user.

Cisco ASM also enriches and integrates with Cisco XDR. Cisco XDR is the industry's broadest, most integrated security platform that unifies visibility, simplifies threat response, and enables automation. It provides extended threat detection and response (XDR) capabilities that allow you to confidently move into automated response and remediation. Cisco XDR centralizes insights from multiple security products into a single console while offering additional context and integrated controls. Moreover, you can enable automated response with prebuilt and custom workflows that trigger a predetermined incident response playbook.

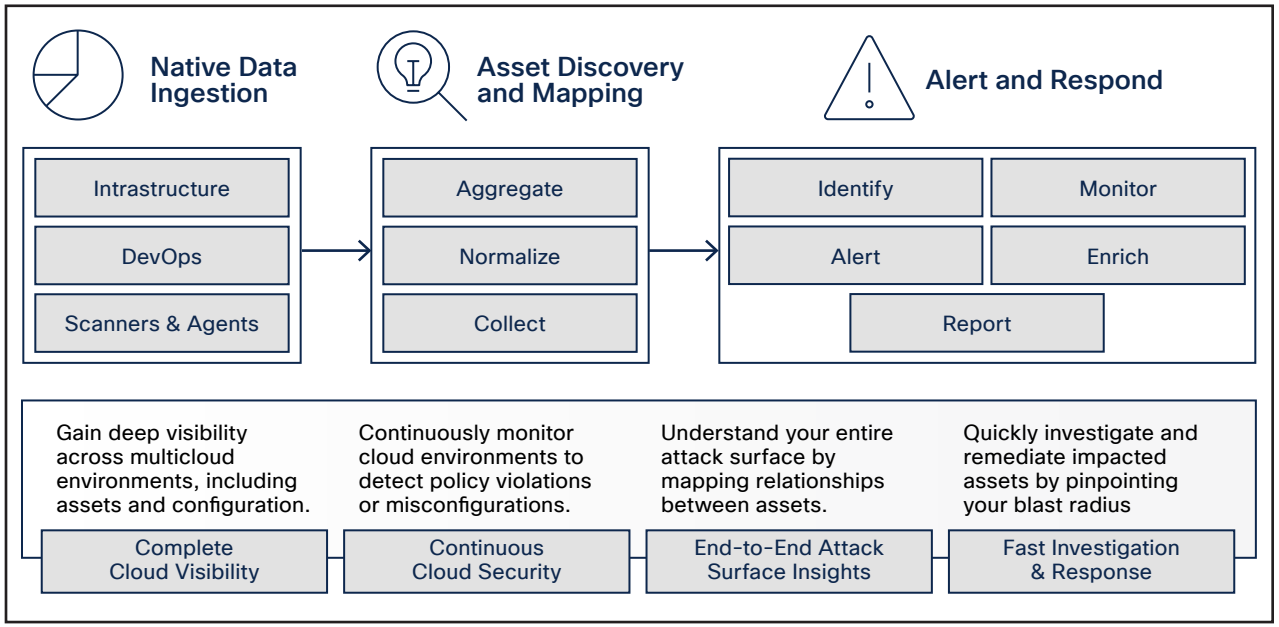

Figure 2. Cisco Attack Surface Management integration with the Cisco XDR

Cisco Attack Surface Management (ASM) adds valuable context on cloud assets and their relationships to each other that leads to higher-fidelity alerts while accelerating investigation and response. Moreover, Cisco ASM provides unparalleled visibility into both your cloud and on-premises assets when combined with Cisco XDR Device Insights. Device Insights gives you a comprehensive inventory of your on-premises assets by consolidating multiple device managers, endpoint detection and response, antivirus, and other endpoint security products into a single, unified view. This helps you quickly spot security gaps, simplify and automate investigations, and gain contextual awareness to identify and remediate compromised assets.

To learn more, please visit:

http://www.cisco.com.

C45-745019-01 02/24