



Free Open Source CSPM Being Released at BlackHat in August

Contents

- Cloud & Cloud Security Tools 101
- Why Magpie
- Architecture
- Security Rules
- Shadow Cloud Accounts
- Rook Plugin
- DMAP - Non-native apps and data store fingerprinting
- Roadmap & Blackhat Arsenal Release
- Demo
- Where to Find More Info

Cloud 101



Cloud 101

CLouDERA

 databricks

 snowflake

 netlify



 Azure

 Google Cloud

Cloud 101



Compute - virtual machines, containers, serverless ...

Storage - file, object, backup ...

Networking - SDN, VPC, DNS, CDN, load balancing, VPN ...

Databases - relational, non-relational, key value, time series ...

Big data and analytics - data warehouses, data lakes, processing, analytics, ML ...

Security - Identity and Access, KMS, firewalls, SIEM ...

How do I know
they are secure ?

The Shared Responsibility Model

6:02 PM Tue May 25

aws.amazon.com

89%

aws

Contact UsSupportEnglishMy AccountCreate an AWS Account

ProductsSolutionsPricingDocumentationLearnPartner NetworkAWS MarketplaceCustomer EnablementEventsExplore More

ComplianceSecurityCompliance ProgramsResourcesLatest NewsPrivacy

of the facilities in which the service operates. The customer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. Customers should carefully consider the services they choose as their responsibilities vary depending on the services used, the integration of those services into their IT environment, and applicable laws and regulations. The nature of this shared responsibility also provides the flexibility and customer control that permits the deployment. As shown in the chart below, this differentiation of responsibility is commonly referred to as Security “of” the Cloud versus Security “in” the Cloud.

AWS responsibility “Security of the Cloud” - AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS Cloud services.

Customer responsibility “Security in the Cloud” – Customer responsibility will be determined by the AWS Cloud services that a customer selects. This determines the amount of configuration work the customer must perform as part of their security responsibilities. For example, a service such as Amazon Elastic Compute Cloud (Amazon EC2) is categorized as Infrastructure as a Service (IaaS) and, as such, requires the customer to perform all of the necessary security configuration and management tasks. Customers that deploy an Amazon EC2 instance are responsible for management of the guest operating system (including updates and security patches), any application software or utilities installed by the customer on the instances, and the configuration of the AWS-provided firewall (called a security group) on each instance. For abstracted services, such as Amazon S3 and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data. Customers are responsible for managing their data (including encryption options), classifying their assets, and using IAM tools to apply the appropriate permissions.

CUSTOMER

RESPONSIBILITY FOR SECURITY IN THE CLOUD

AWS

RESPONSIBILITY FOR SECURITY OF THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA (ENCRYPTION & DATA INTEGRITY AUTHENTICATION)

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

REGIONS

AVAILABILITY ZONES

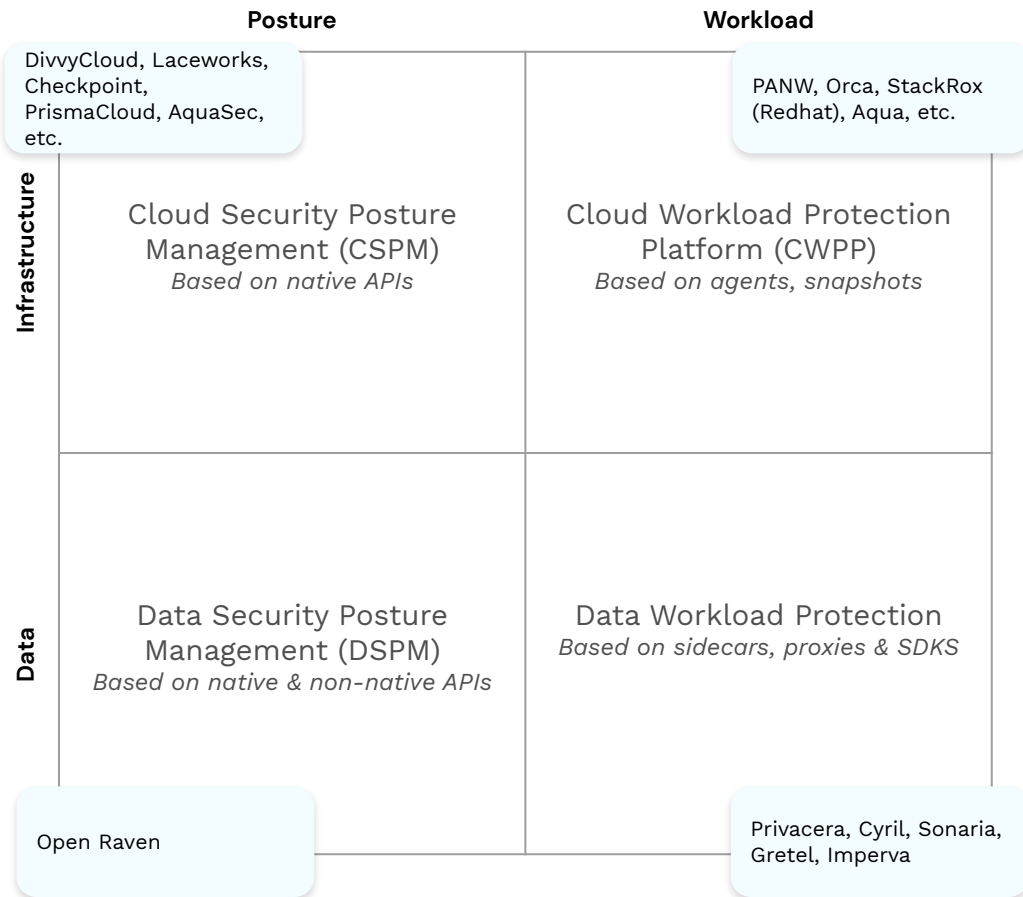
EDGE LOCATIONS

Category Landscape

The 2 existing cloud security segments are focused on infrastructure, broadly the infrastructure itself (CSPM) and then the workloads that runs on it (CWPP).

CSPM is generally defined as

- asset / service discovery
- security configuration management
- monitoring and remediation
- integration



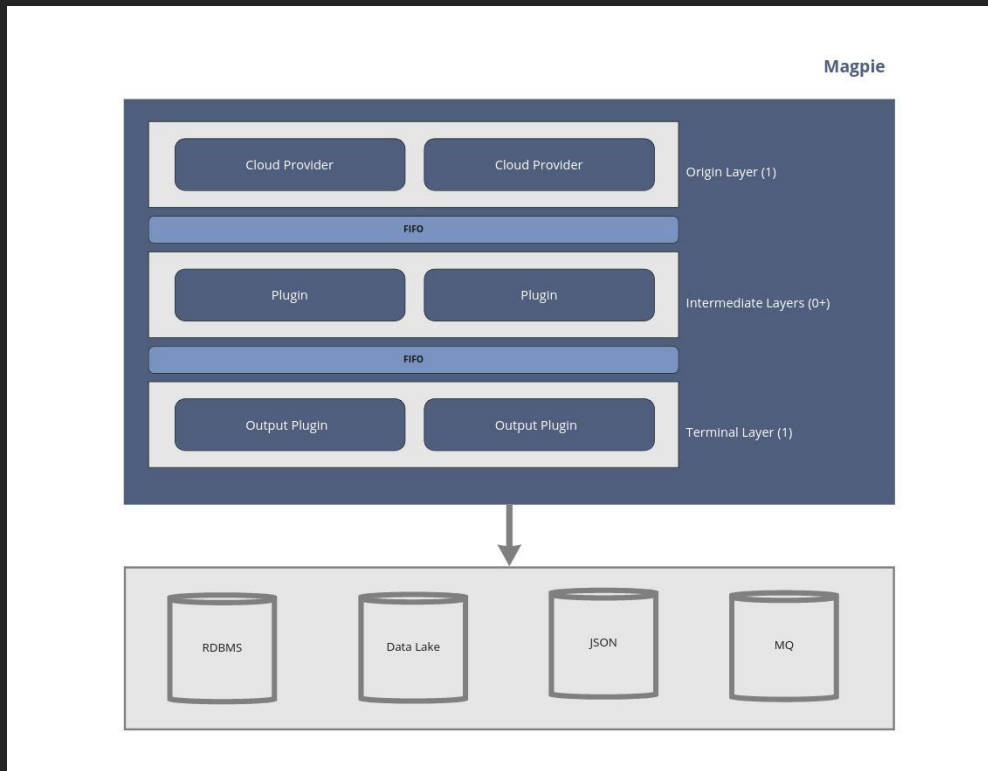
Why Magpie?

1. We needed to do cloud discovery at scale to support our commercial data security product
2. Our customers kept telling us that their current CSPM's sucked.
3. CSPMs are "compliance" focused and not "security" focused
4. CSPMs don't discover non-native apps / data stores (ie things deployed on compute)
5. CSPMs don't help with "shadow cloud" discovery
6. We think CSPM is table stakes but everyone needs it
7. We are an open core company

Architecture

- Desktop Edition
- Enterprise Edition

All Apache 2.0 License



Architecture

Stages

There are 4 stages:

Enumerate
Query
Transform
Output

Each stage is designated for a specific set of actions and is separated by a **FIFO** (queue).

FIFO

May be a local queue (Java Queue) or a remote queue (Kafka). This permits Nightglow installations to run within a single process or multiple processes spanning multiple machines.

Nightglow Stages



Enumerate

Determine what resources/infrastructure exist in a cloud environment.

Query

Query the cloud provider for details on the discovered resources.

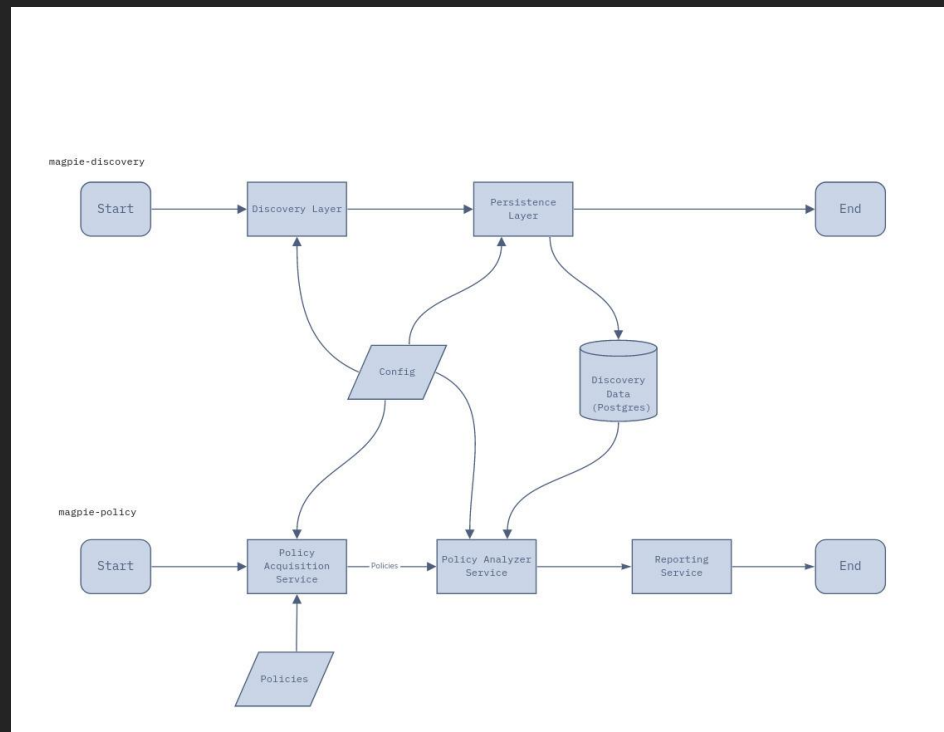
Transform

(Optional) Transform the existing query data into another format to be consumed downstream.

Output

Output the transformed data (files, Kafka, PostgreSQL, etc)

Architecture



Security Rules

<https://github.com/openraven/magpie/wiki/Magpie-RFC---Security-Rules-and-Policies>

Rules

Policies reference one or more "rules," which contain basic information, like name, description, and remediation steps, but also contain the actual logic used to evaluate the rule (more on this later). To enable reuse, rules can be shared and referenced in multiple policies.

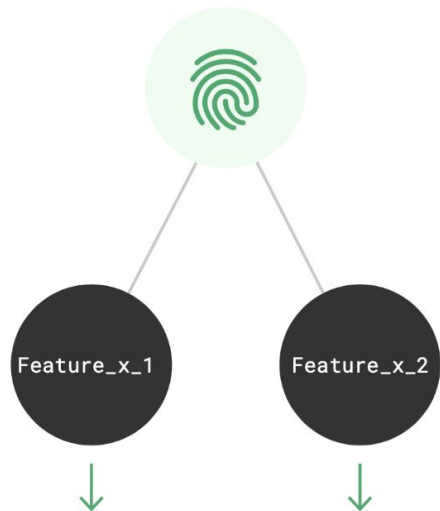
```
id: 2e443d91-c3c4-a96d-677e-7cb0da4ae64e
refId: CIS-1.2
type: asset
name: >
  Ensure multi-factor authentication (MFA) is enabled for all IAM users
  that have a console password
description: >
  Multi-Factor Authentication (MFA) adds an extra layer of protection on top of a
  username and password. With MFA enabled, when a user signs in to an AWS website,
  they will be prompted for their username and password as well as for an
  authentication code from their AWS MFA device. It is recommended that MFA be
  enabled for all accounts that have a console password.
severity: high,
enabled: true,
sql: >
  SELECT configuration->"arn" as arn
  from awsusercredentialreport
  where configuration->"password_enabled" = true AND
  configuration->"mfa_active" = false
remediation: >
  Perform the following to enable MFA:
  1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/.
  2. In the navigation pane, choose Users.
  3. In the User Name list, choose the name of the intended MFA user.
  4. Choose the Security Credentials tab, and then choose Manage MFA Device.
  5. In the Manage MFA Device wizard, choose A virtual MFA device, and then choose Next Step.
remediationDocURLs:
  - https://docs.openraven.com/remediations/enable_mfa
version: 0.1.3
```

The main part of the rule outlined above is the "SQL" statement that queries discovered assets and MUST return AT LEAST a field named "arn" for each asset that doesn't meet the policy rule (i.e., is "in violation"). In addition to the SQL statement, there may also be an OPTIONAL "script" statement (written in Python). See "Rule evaluation" below for how it operates.

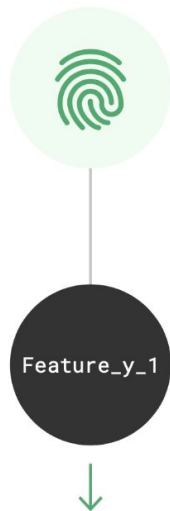
Rook Plugin

Non-native apps and data store fingerprinting

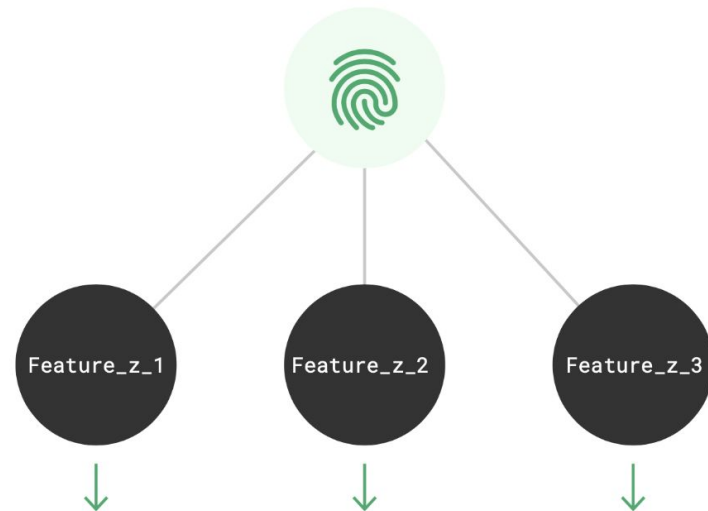
Fingerprint x



Fingerprint y



Fingerprint z



Decision Tree Classifier

AWS Fargate Cluster

Application X v1.0

Application X v1.0

Application X v1.0

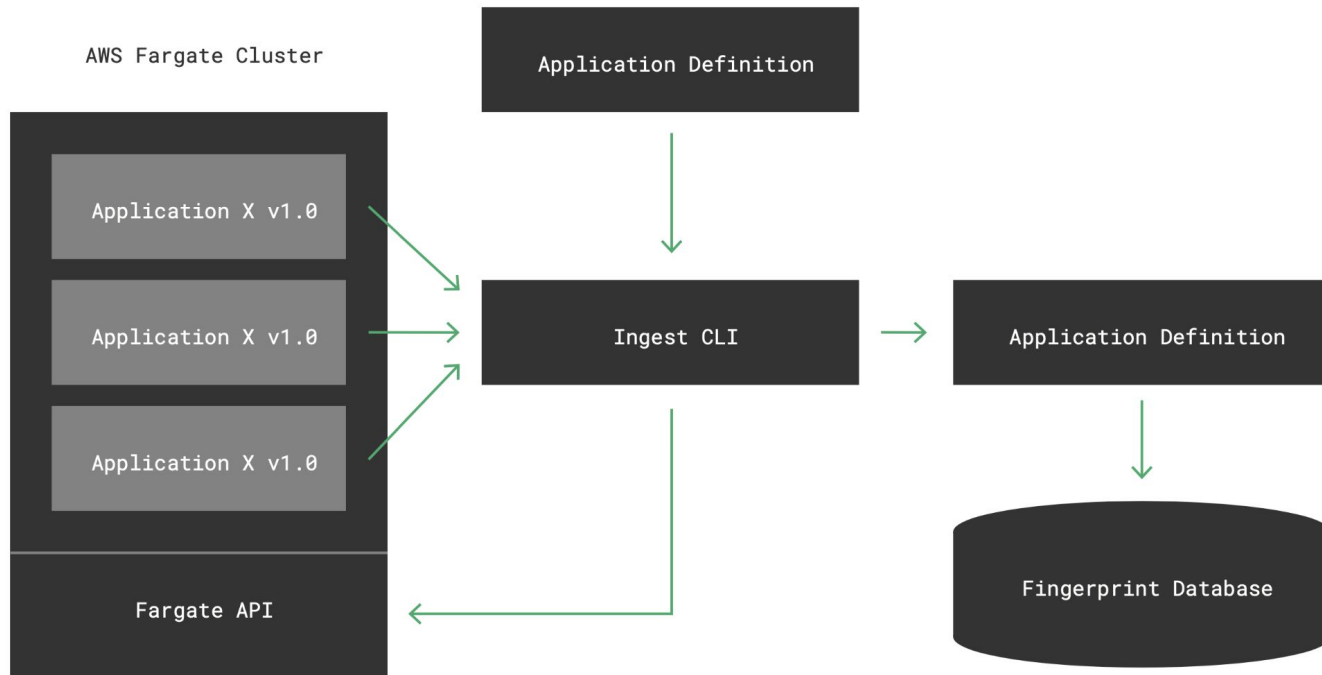
Fargate API

Application Definition

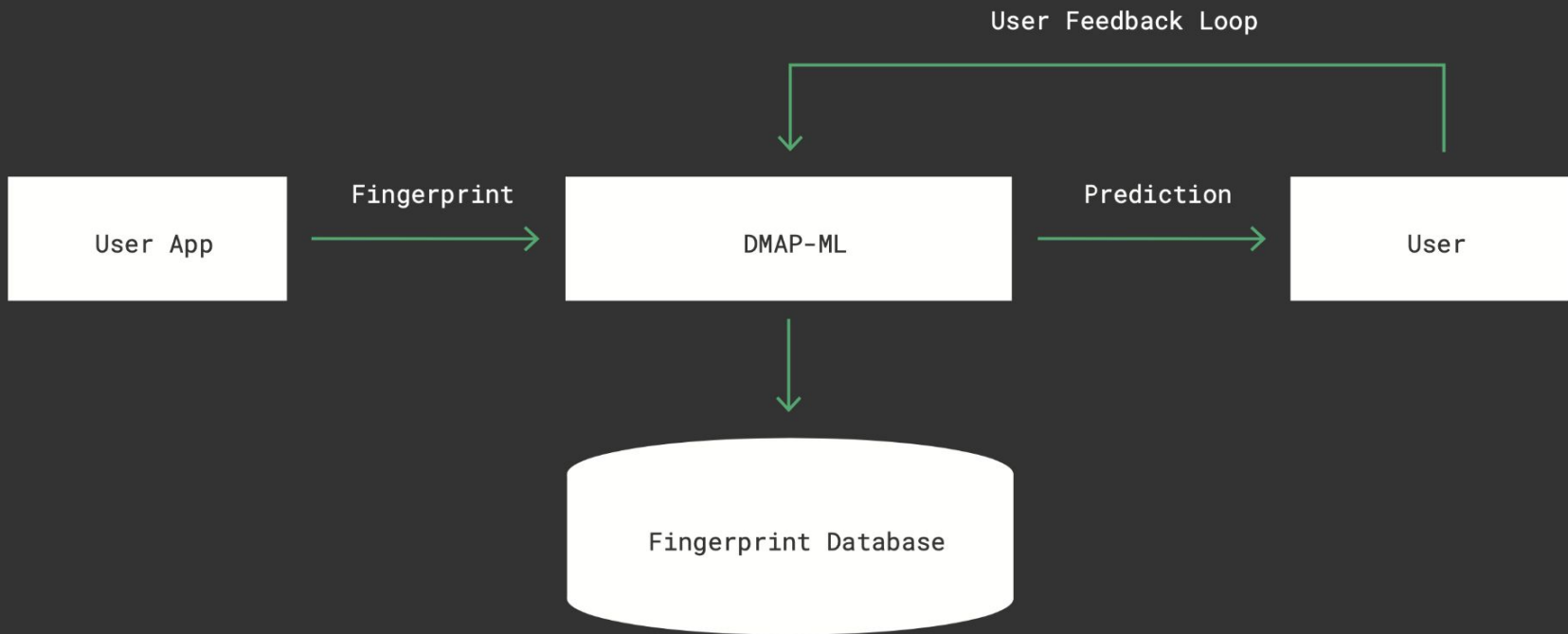
Ingest CLI

Application Definition

Fingerprint Database



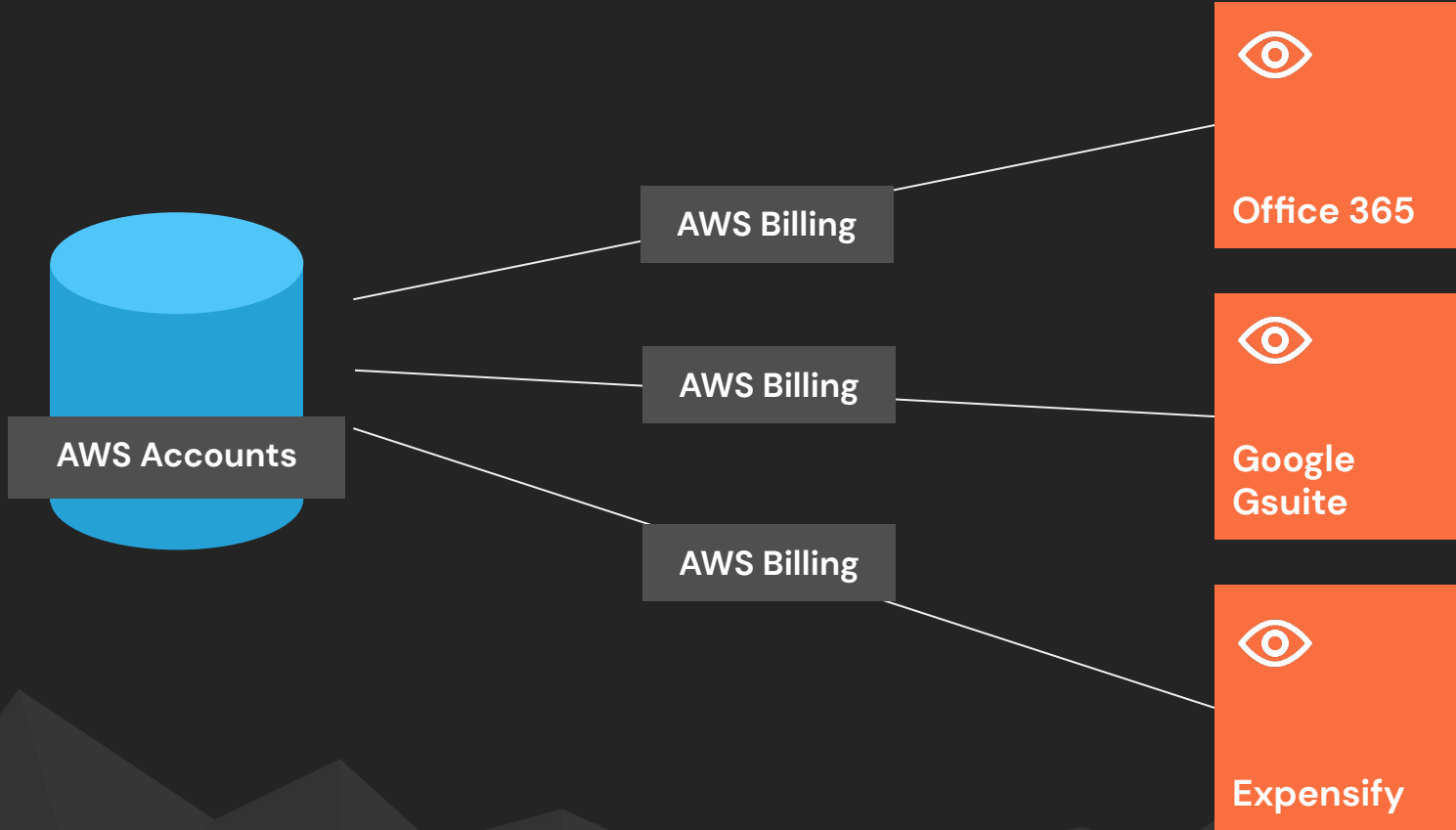
—



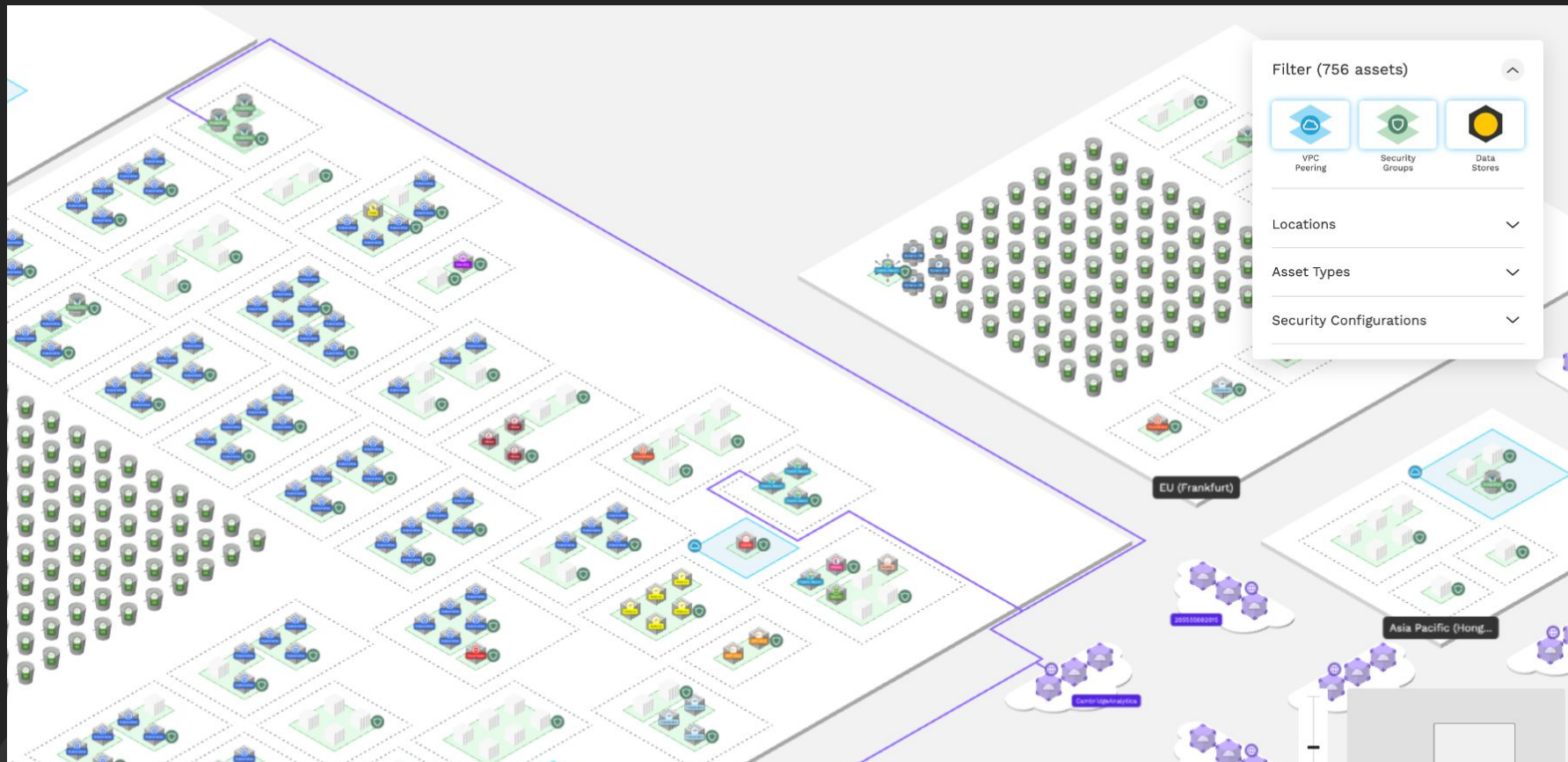


Shadow Cloud Accounts Plugin





3D Maps



BlackHat Arsenal Release & Roadmap

<https://github.com/openraven/open-raven/projects/1>



Demo

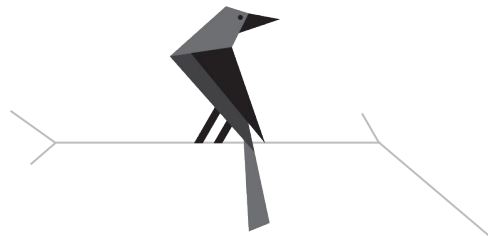


Where to Find More Info

GitHub - <https://github.com/openraven/magpie>

Slack -

https://join.slack.com/t/open-raven-research/shared_invite/zt-np27xiev-N5rL4AcTmrQt8YkE81Blaw



Thanks

Email : mark@openraven.com and jason@openraven.com

Twitter : [@curphey](https://twitter.com/curphey) and [@kickroot](https://twitter.com/kickroot)

