Uptycs

Structured Security Analytics for Cloud Workloads

SELECT * for the Cloud: Simplify Cloud Security with Cloudquery

Saurabh Wadhwa, Senior Sales Engineer, Uptycs

Agenda

- Introduction
- Cloud Security/Visibility Challenges
- Structured Telemetry(Why do we need it?)
- Intro to osquery
- Intro to cloudquery
- Demo
- Wrap Up

Uptycs

Cloud Security Predictions

1.Through 2025, 90% of the organizations that fail to control public cloud use will inappropriately share sensitive data.

2.Through 2024, the majority of enterprises will continue to struggle with appropriately measuring cloud security risks.

3.Through 2025, 99% of cloud security failures will be the customer’s fault.

Cloud Security Observability Challenges

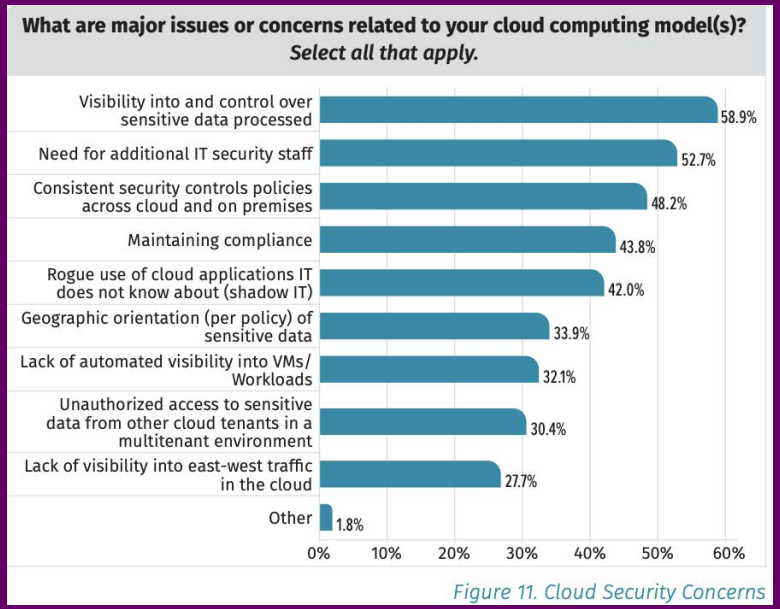
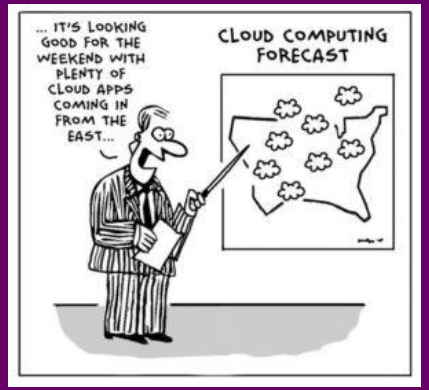


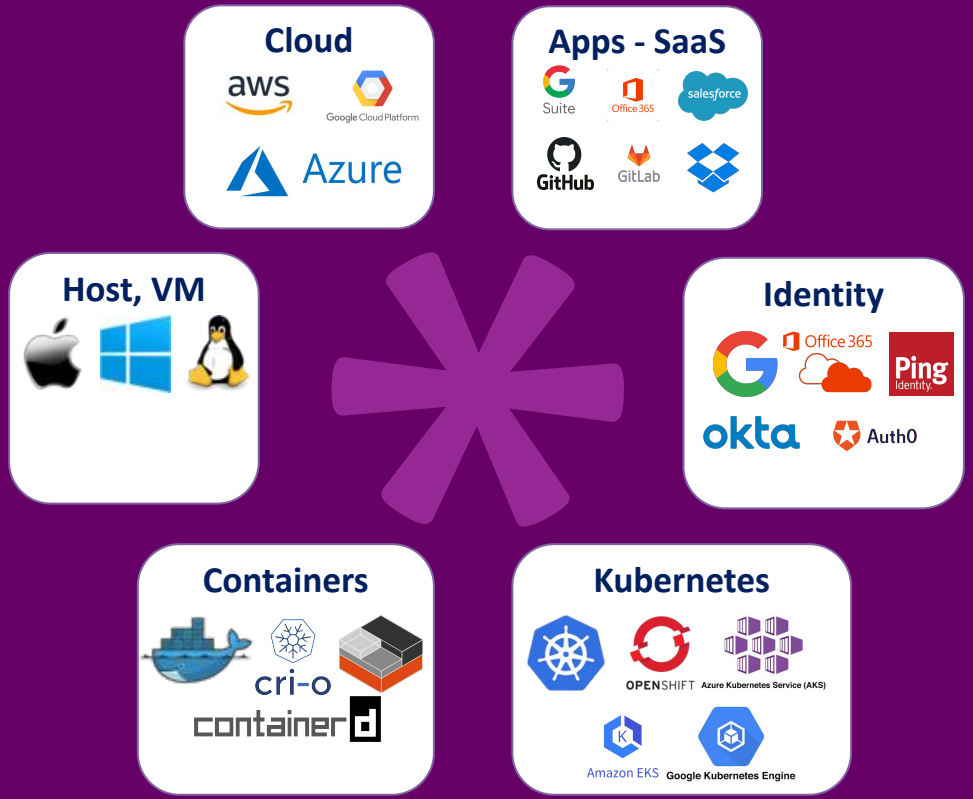
Figure 11. Cloud Security Concerns

via SANS 2020 CloudSec Survey

- Siloed tools and data
  - Explosion of native cloud services + tools
- Visibility across accounts
- Multi-cloud and hybrid cloud



The modern attack surface

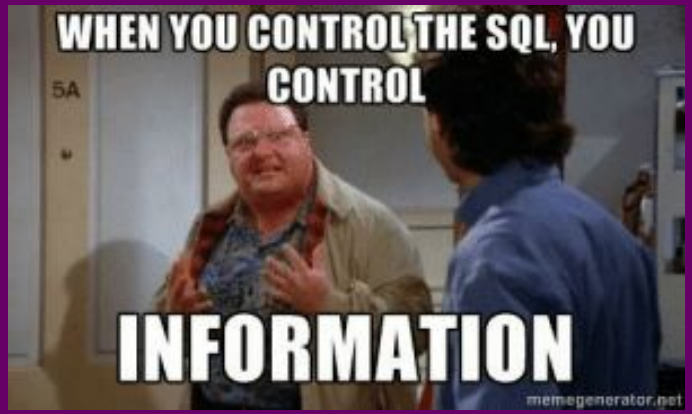


Structured Security Analytics

- Tool suite consists of:
  - **osquery**: Hosts, VM, Container visibility
  - **Kubequery**: Container orchestration visibility
  - **cloudquery**: Cloud provider visibility
  - **saasquery**: SaaS provider visibility *[future]*
  - **identityquery**: Identity provider visibility *[future]*

Uptycs

Structured Secur… Why?

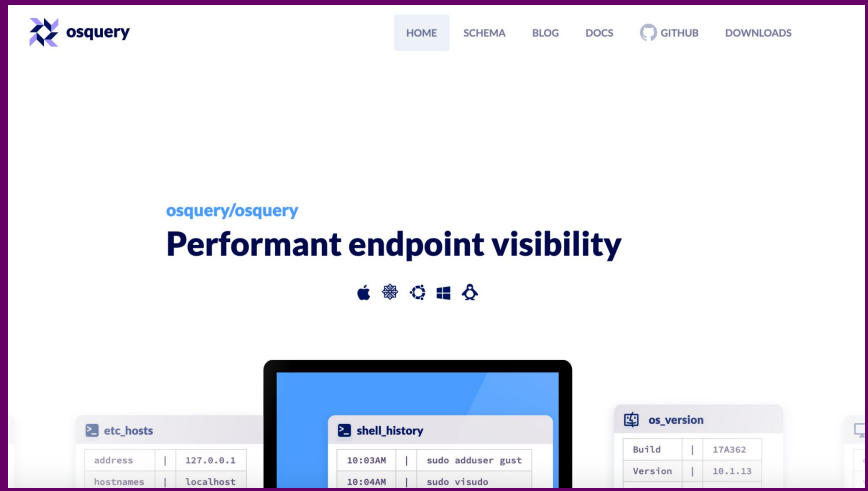


- Use existing familiarity with SQL
- Lessen impact of unfamiliarity with attack surface data sources
- Structure queries similarly across heterogenous OS & cloud platforms

Uptycs

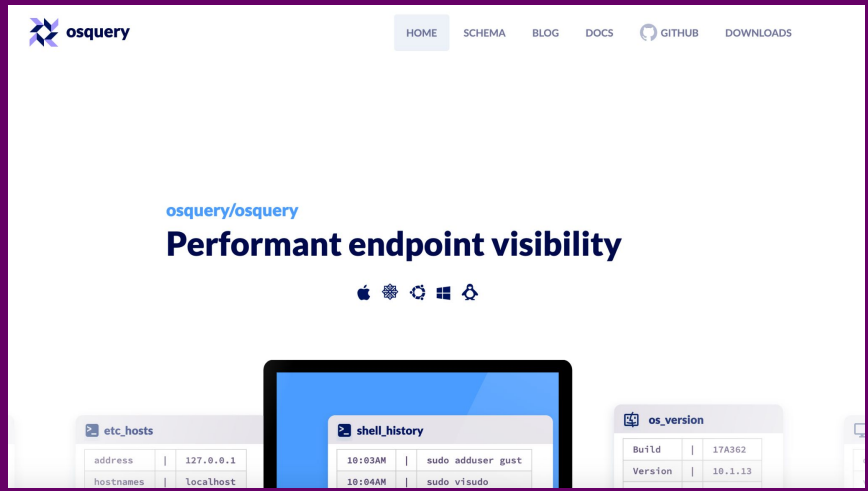
Intro to osquery

- Open-sourced by Facebook in 2014
- Project brought on by the Linux Foundation in 2019
- Supports macOS, Linux, and Windows (and FreeBSD)
- Low resource utilization
- Structures endpoint telemetry as SQL tables for querying
- Use cases
  - Endpoint detection
  - Investigation and threat hunting
  - Audit and compliance



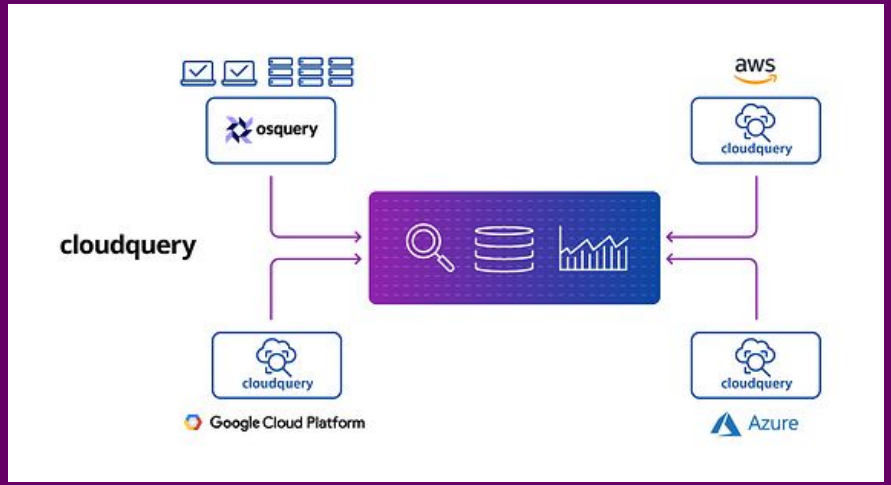
Intro to osquery, cont.

- Data cache using RocksDB
- Run scheduled queries (*osqueryd)*
- Run realtime + interactive queries (*osqueryi)*
- Deliver results to various destinations:
  - File/Socket
  - osquery TLS
  - Kinesis
  - Kafka



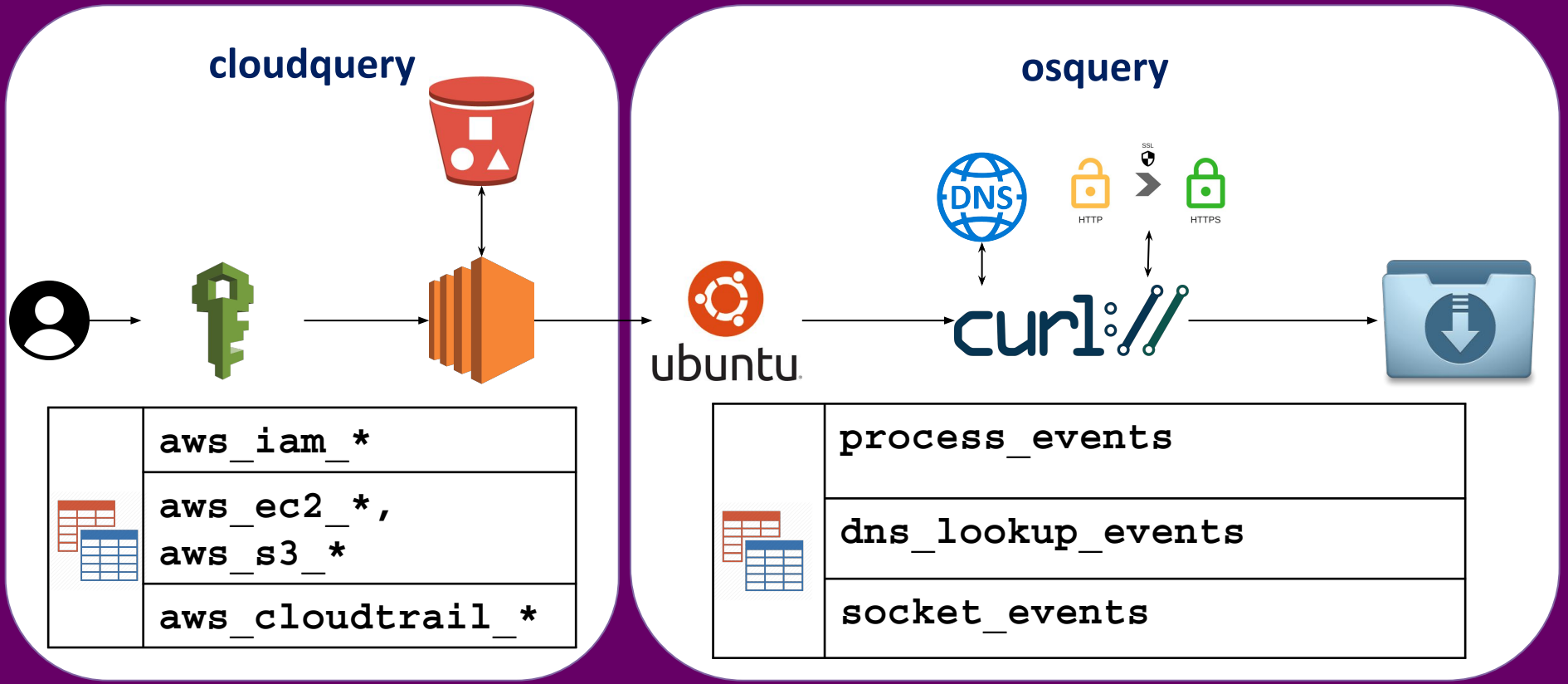
Intro to cloudquery

- Open-source extension to osquery released in 2021
- Extends SQL-based analytics to cloud infrastructure
- Support for AWS, GCP, and Azure
- Scheduled and real time queries
- Use Cases:
  - Resource Visualization
  - Monitoring configuration and drift
  - Compliance
  - Investigation



github.com/Uptycs/cloudquery

The Power of Structured Telemetry



Uptycs

What (else) can you cloudquery?

- AWS:
  aws_ec2_image
  aws_ec2_instance
  aws_ec2_security_group
  aws_ec2_volume
  aws_iam_group
  aws_iam_policy
  aws_iam_role
  aws_iam_user
  aws_s3_bucket
  aws_cloudwatch_alarm
  aws_kms_key
  aws_eks_cluster
  aws_ecs_cluster
  aws_elb_loadbalancer

Uptycs

What (else) can you cloudquery?

- GCP:

  gcp_compute_disk
  gcp_compute_image
  gcp_compute_instance
  gcp_compute_network
  gcp_compute_route
  gcp_compute_vpn_tunnel
  gcp_dns_managed_zone
  gcp_iam_role
  gcp_iam_service_account
  gcp_sql_database
  gcp_sql_instance
  gcp_storage_bucket

Uptycs

S3 Bucket Compliance?

Uptycs

Let’s check!

```
SELECT name,
   CASE
      WHEN server_side_encryption_configuration IS NOT NULL THEN
'ok'
      ELSE 'alarm'
   END status,
   CASE
      WHEN server_side_encryption_configuration IS NOT NULL
      THEN name || ' default encryption enabled.'
      ELSE name || ' default encryption DISABLED.'
   END reason,
   region_code
FROM aws_s3_bucket;
```

Uptycs

BCDR/Safety: S3 versioning

```
SELECT name,
   CASE
      WHEN versioning_status = 'Enabled' THEN 'ok'
      ELSE 'WARN'
   END status,
   'Versioning is ' || versioning_status || '.' as reason,
   region_code
FROM aws_s3_bucket
ORDER BY name;
```

Password Compliance?

No trust, only verify

```
SELECT CASE
   WHEN minimum_password_length IS NULL
        THEN 'No password policy set.'
   WHEN minimum_password_length >= 14
      AND password_reuse_prevention >= 5
      AND require_lowercase_characters = 'true'
      AND require_uppercase_characters = 'true'
      AND require_numbers = 'true'
      AND max_password_age <= 90
      THEN 'Strong password policies configured.'
   ELSE 'WARN: Strong password policies not configured.'
   END status
FROM aws_iam_account_password_policy;
```

Uptycs

DEMO TIME

Uptycs

Recap

- Cloudquery extends osquery to deliver data about cloud infrastructure in a structured format
- Converts AWS, Azure, & GCP infrastructure + telemetry into SQL tables for querying
- Stream data as JSON to an upstream aggregator for FULL POWER
- Use cases
  - Cloud security investigation and threat hunting
  - Audit and compliance
  - Visibility

Uptycs

GitHub:

github.com/Uptycs/cloudquery

github.com/Uptycs/kubequery

Uptycs

Questions?