



Structured Security Analytics for Cloud Workloads

SELECT * for the Cloud: Simplify Cloud Security with Cloudquery

Saurabh Wadhwa, Senior Sales Engineer, Uptycs



Agenda

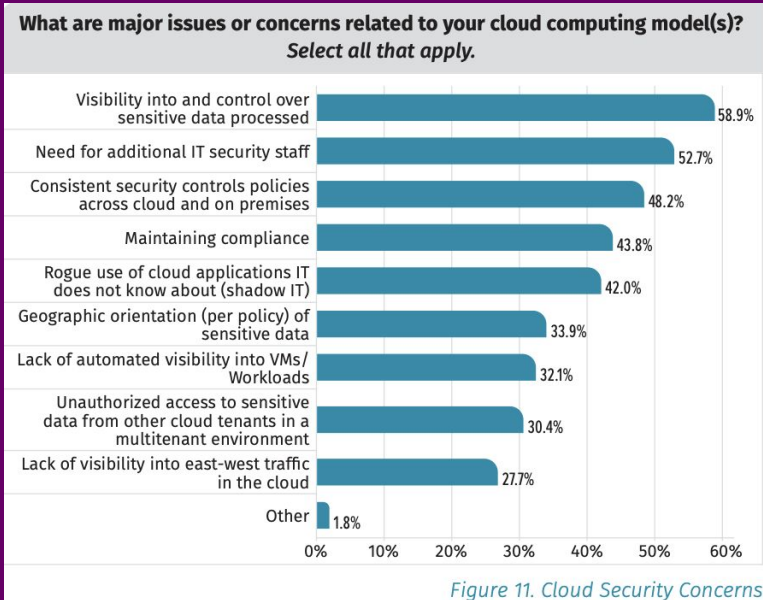
- Introduction
- Cloud Security/Visibility Challenges
- Structured Telemetry(Why do we need it?)
- Intro to osquery
- Intro to cloudquery
- Demo
- Wrap Up



Cloud Security Predictions

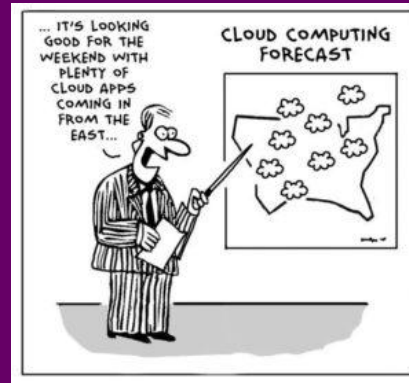
1. Through 2025, 90% of the organizations that fail to control public cloud use will inappropriately share sensitive data.
2. Through 2024, the majority of enterprises will continue to struggle with appropriately measuring cloud security risks.
3. Through 2025, 99% of cloud security failures will be the customer's fault.

Cloud Security Observability Challenges



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

Cloud



Apps - SaaS




Host, VM



Identity




Containers



cri-o
containerd

Kubernetes



Amazon EKS Google Kubernetes Engine

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]*



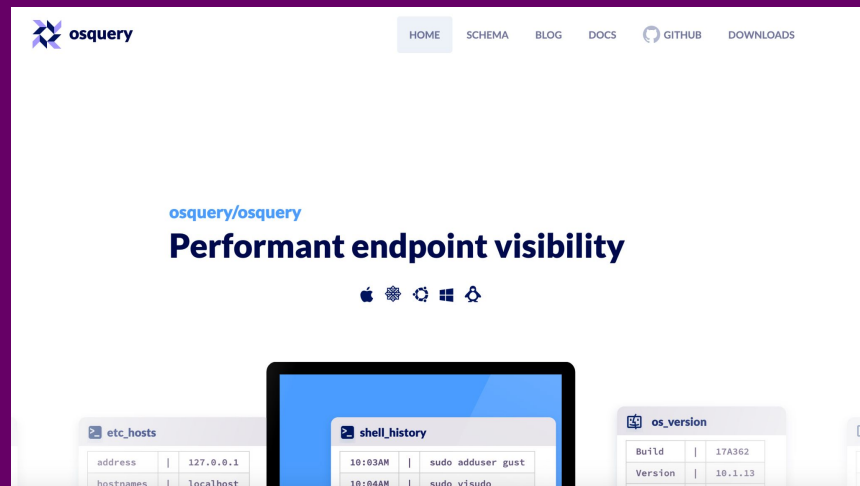
Structured Secur... Why?



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

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



The screenshot shows the osquery website homepage. At the top, there is a navigation bar with links for HOME, SCHEMA, BLOG, DOCS, GITHUB, and DOWNLOADS. The main heading reads "osquery/osquery" followed by "Performant endpoint visibility". Below this, there are icons for Apple, Linux, Windows, and FreeBSD. At the bottom, there are three preview windows showing SQL query results:

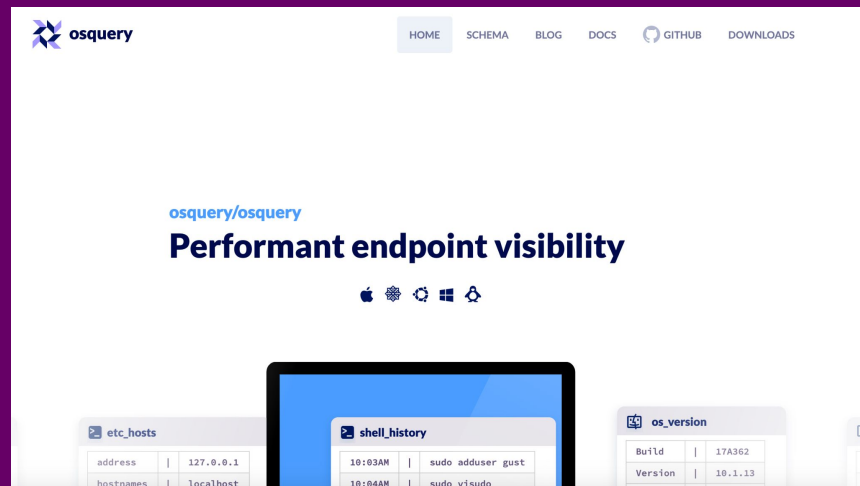
etc_hosts	
address	127.0.0.1
hostnames	localhost

shell_history	
10:03AM	sudo adduser gust
10:04AM	sudo visudo

os_version	
Build	17A362
Version	10.1.13

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



The screenshot shows the osquery website homepage. At the top left is the osquery logo. To the right is a navigation menu with links for HOME, SCHEMA, BLOG, DOCS, GITHUB, and DOWNLOADS. The main heading reads "osquery/osquery" in blue, followed by "Performant endpoint visibility" in bold black. Below the heading are icons for Apple, Linux, Windows, and a gear. At the bottom, there are three overlapping window-like displays showing query results:

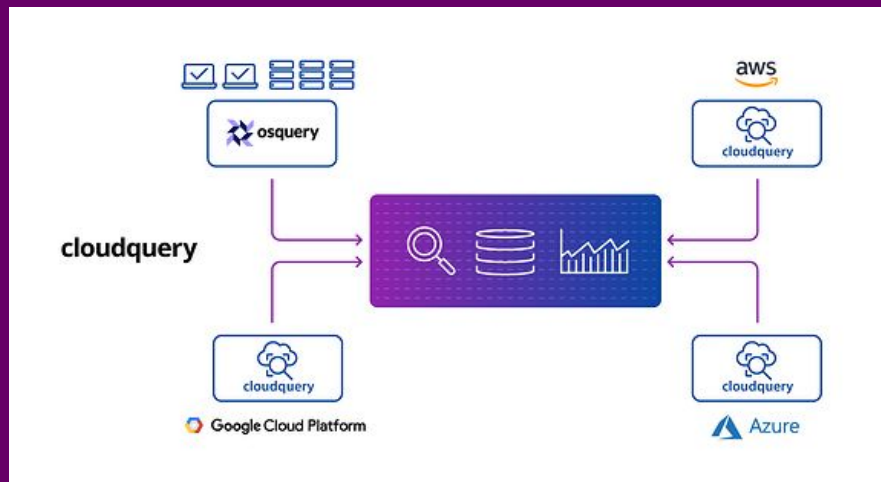
etc_hosts	
address	127.0.0.1
hostnames	localhost

shell_history	
10:03AM	sudo adduser gust
10:04AM	sudo visudo

os_version	
Build	17A362
Version	10.1.13

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

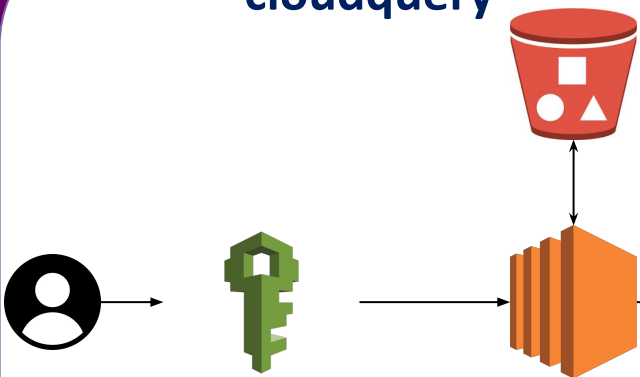



github.com/Uptycs/cloudquery



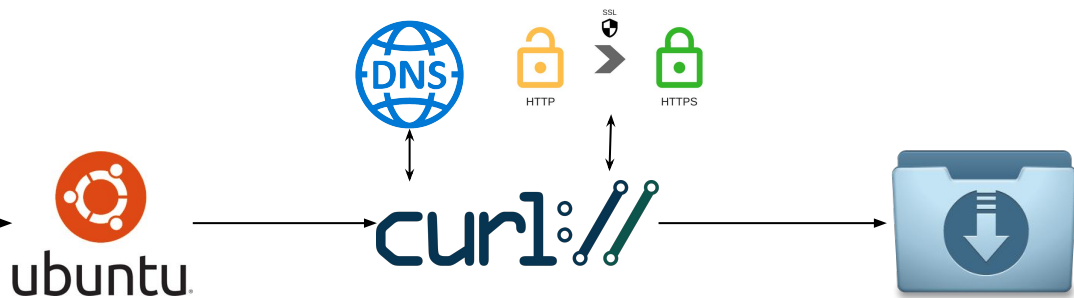
The Power of Structured Telemetry


cloudquery



	<code>aws_iam_*</code>
	<code>aws_ec2_*,</code> <code>aws_s3_*</code>
	<code>aws_cloudtrail_*</code>

osquery



	<code>process_events</code>
	<code>dns_lookup_events</code>
	<code>socket_events</code>



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



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



S3 Bucket Compliance?

1.20 Ensure that S3 Buckets are configured with 'Block public access (bucket settings)' (Automated)..... 62

2.1 Simple Storage Service (S3) 71

2.1.1 Ensure all S3 buckets employ encryption-at-rest (Manual) 72

2.1.2 Ensure S3 Bucket Policy allows HTTPS requests (Manual) 75



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;
```

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?

1.5 Ensure IAM password policy requires at least one uppercase letter (Scored)	19
1.6 Ensure IAM password policy require at least one lowercase letter (Scored)	21
1.7 Ensure IAM password policy require at least one symbol (Scored)	23
1.8 Ensure IAM password policy require at least one number (Scored)	25
1.9 Ensure IAM password policy requires minimum length of 14 or greater (Scored)	27
1.10 Ensure IAM password policy prevents password reuse (Scored).....	29
1.11 Ensure IAM password policy expires passwords within 90 days or less (Scored)	31



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;
```



DEMO TIME





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



GitHub:

 github.com/Uptycs/cloudquery

 github.com/Uptycs/kubequery



Questions?