Monitoring your Devices… But Make It *Go*

osquery + *Go* for fun & compliance

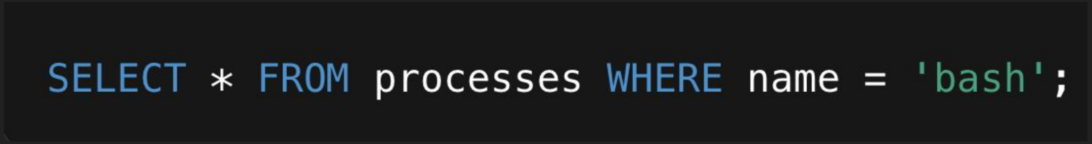
```
> whoami

name      : Mohammed Nafees
interests : cybersecurity, distributed
    systems, low-level computing, cloud
    and backend infra

github    : mnafees
X         : NafeDotEs
```

🧠 What’s osquery?

- Developed at Facebook
- Turns your system into a relational database
- You can query your device like



```sql
SELECT * FROM processes WHERE name = 'bash';
```

- Cross -platform: works on macOS, Linux, and Windows
- Great for monitoring, threat detection, inventory, etc.

🤯 Why osquery is cool

- Open source & powerful 💥
  - https://www.github.com/osquery/osquery
  - 8 years, 400 contributors, and 6,000 commits (and counting!)
- Live system insights with SQL syntax
- Structured, lightweight, and fast
- Tables for: processes, users, network, USB devices, security configs, and even sneaky kernel extensions
- Plug-in friendly: you can build your own tables and extensions

🧰 Meet osquery-go: Your Go-powered Sidekick

So you like osquery. Now imagine if you could teach it new tricks.

osquery-go is the Go SDK to create:

- 🧱 Custom tables
- 🎯 New data sources
- 🚀 Realtime monitoring magic

Think: Go + SQL + system internals = ❤️

🦴 Anatomy of a Custom Table in Go

```go
plugin.TablePlugin(
  "mood_table",
  []table.ColumnDefinition{
    table.TextColumn("mood"),
    table.TextColumn("reason"),
  },
  func(ctx context.Context, queryContext table.QueryContext) ([]map[string]string, error)
    return []map[string]string{
      {"mood": "happy", "reason": "running Go and osquery"},
    }, nil
  },
)
```

🧠 In plain English:

- Give your table a name
- Define the columns
- Return rows (as Go maps!)

Boom. You’ve got a working table. 🎉

🧪 Demo Time!

🧩 Fun with Profit – Real Use Cases

✅ Security Teams: Custom audit tables

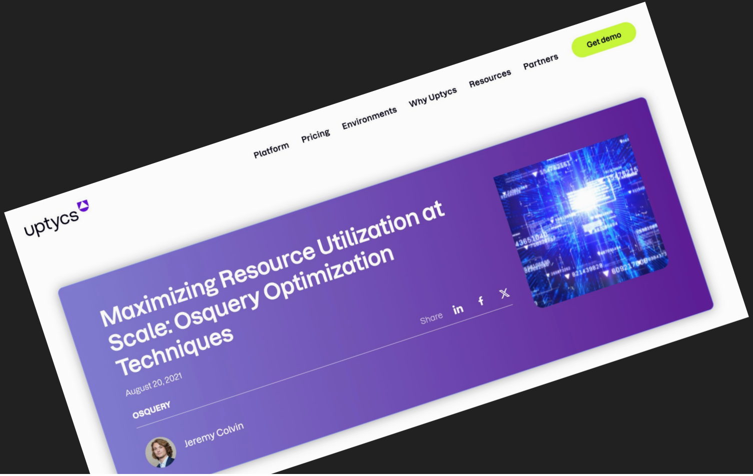
✅ SREs: Process health, disk alerts

✅ Hackers: Make your own spyware (for yourself... ethically!)

✅ Nerds: Monitor if Cursor is open too long 😅

🌍 Where in the World is osquery with Go extensions?

- Deployed on millions of devices globally
- Used across macOS, Linux, Windows
- Popular in:
  - Endpoint Detection & Response (EDR)
  - IT asset inventory
  - Compliance frameworks (SOC2, HIPAA, etc.)
  - Incident response & forensics

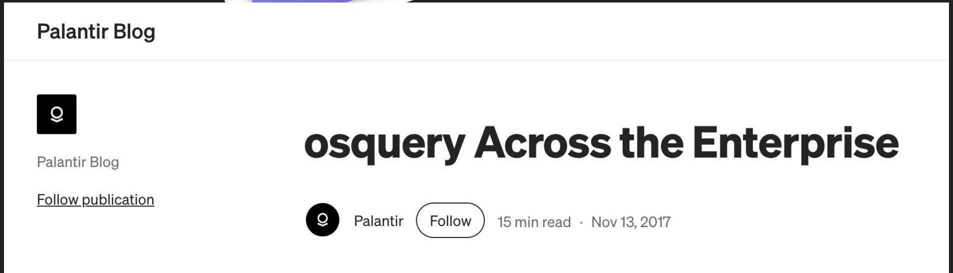


Maximizing Resource Utilization at Scale: Osquery Optimization Techniques

August 20, 2021

OSQUERY

Jeremy Colvin



Palantir Blog

osquery Across the Enterprise

Palantir · 15 min read · Nov 13, 2017

🧩 Why Go Is Perfect for osquery Extensions

- Static binaries
- Great stdlib for system access
- Fast startup and small footprint
- Plugin/RPC support is native
- Simple to test and reuse

osquery gives you the sockets. Go gives you the smarts. Together, you get a cross-platform monitoring agent you actually want to maintain.

🏁 Closing

“osquery-go lets you turn security into software engineering, not just ticket-tending.”

- Want more insights? Write a table
- Want real-time remediation? Wire up a scheduler
- Want to sleep well at night? Monitor everything

“Because in 2025, your fleet is your perimeter — and osquery-go is your best friend wearing a Go hoodie.”

Thank you!

Questions?