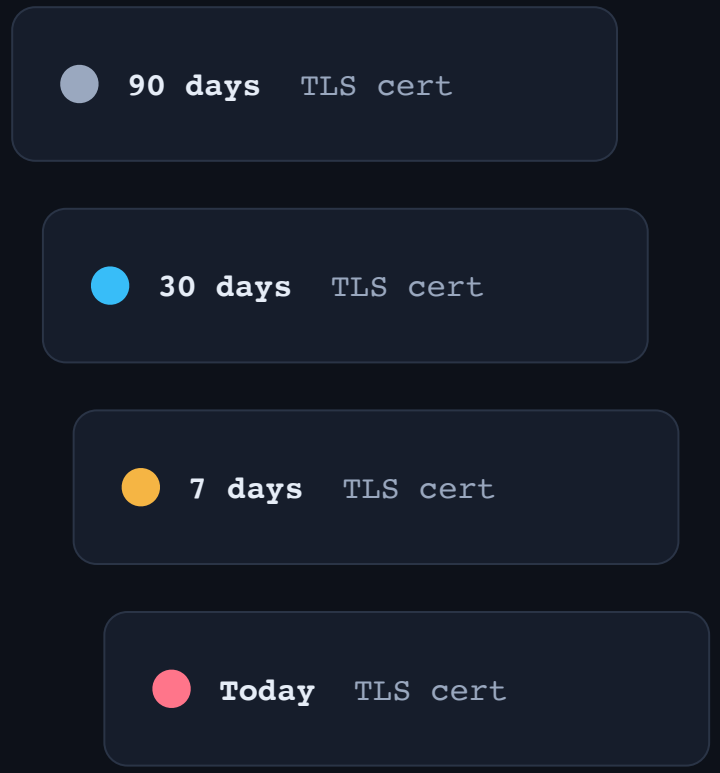
HYBRID INFRASTRUCTURE MONITORING

Know before your infrastructure fails at 2 AM.

CloudMonitor watches your environment, or your clients', for the problems that fail quietly — and tells you weeks before they become incidents.



14-day free trial · no credit card · read-only access

THE PROBLEM

The outages that hurt most fail quietly



Credential expiry

A secret, API key or certificate reaches its expiry date — and every call that depends on it fails at once.



Idle resources on autopilot

Every cloud makes it easy to spin things up. None remind you to spin them down. A forgotten VM can bill $300–$800 a month.



Silent endpoint failures

The status page says green. Customers start reporting errors. An HTTPS endpoint went down two hours ago.

None of these show up on a dashboard until it's too late — and there is no single place to watch a hybrid stack from.

WHAT WE WATCH

Everything that quietly breaks, in one place

Secret & cert expiry
Key vaults, secret managers, app secrets and certificates

Compute cost
Idle and oversized machines, with estimated monthly cost

Endpoint monitoring
HTTP/HTTPS checks, response times, TLS days left

Storage hygiene
Unattached disks, old snapshots, public buckets

Microsoft 365 & Entra
No-MFA users, stale accounts, unused licenses

Domains, DNS & email
Registration expiry, SPF/DKIM/DMARC, dangling DNS

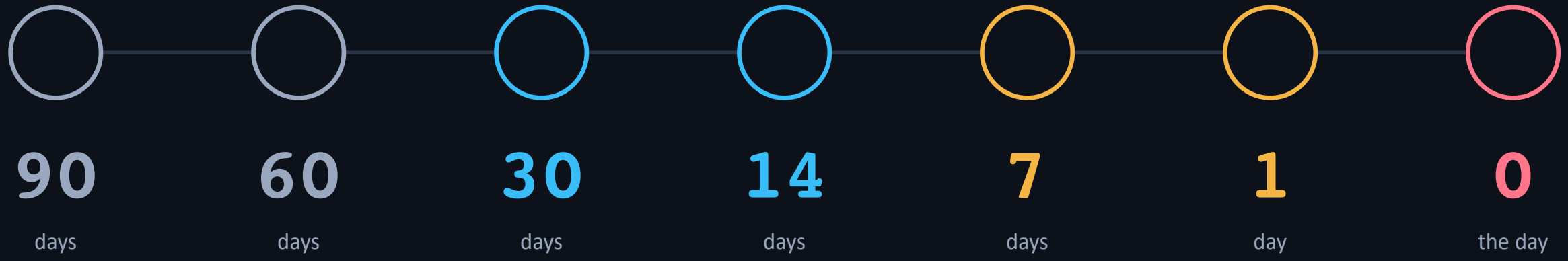
Cost & governance
Reservation expiry, anomalies, quotas, end-of-life OS

GitHub & CI/CD
Branch protection, security alerts, failing workflows

EXPIRY ALERTS

Warned on a fixed ladder, weeks ahead

Secrets, certificates, keys, app registrations, load balancer and gateway certs, on-prem server certs, public TLS and domain registrations — all on one schedule, across every connected platform.



Severity rises as the date gets closer, so the alert you get at 7 days looks different from the one at 90.

BEYOND THE SCAN

Findings you can act on, wherever you work

Diagnostics



Related signals fuse into one story instead of three alerts. AI Insights explains each cause in plain English.

Alerts where you already work

Chat & paging Email, Slack, Teams, Discord, PagerDuty, webhooks

PSA tickets ConnectWise, Autotask, HaloPSA, NinjaOne

Open by default

Read-only REST API, SSO over OIDC or SAML 2.0, unlimited users with admin and read-only roles, an activity log and full data export.

FOR MSPS AND IT TEAMS

One environment or fifty

Isolated tenant per client

Each client sits in its own tenant under your MSP account.

One cross-client worklist

Everything critical or expiring, across every client, in one queue.

One-time onboarding links

Send a link; the client connects read-only access themselves.

Read-only client portal

Each client sees their own findings — nothing else.

Your brand on monthly reports

The MSP bundle adds your name and logo, emailed monthly.

CROSS-CLIENT WORKLIST · ILLUSTRATIVE

CLIENT	FINDING	DUE
Dental practice	TLS cert · portal	1 day
Freight co.	App secret · payroll	7 days
Law firm	Domain registration	14 days
Dental practice	Public storage bucket	Now
Clinic group	Idle VM · ~$410/mo	Review

SETUP IN MINUTES

Three steps to full coverage

01

Create your account

Sign up with your email — no password to set. Your tenant is isolated. 14-day free trial, no credit card.

02

Connect your platforms

Least-privilege, read-only access: a service principal, a read-only IAM user, a service account. Per-platform guides.

03

Findings land

Endpoint checks start within minutes; exposure findings within the hour; expiry and cost with the next nightly scan.

No agents to install. No policy changes. Just read-only access.

SECURITY AND TRUST

Read-only by design. Your data stays yours.

Read-only, least privilege

We ask only for read access. Nothing in your cloud is changed.

Encrypted credentials

Connection credentials are stored encrypted.

Isolated tenants

Every customer — and every MSP client — in its own tenant.

Your identity provider

SSO over OpenID Connect or SAML 2.0, admin and read-only roles.

Activity log

A record of who did what, on every account.

Full export

Take all of your data with you whenever you want it.

What it isn't

- Not an APM, log or tracing tool
- Not a compliance certification or audit
- Not a replacement for your on-call

It's the second pair of eyes that catches what those tools don't watch.

PLATFORM COVERAGE

Honest about how deep we go

PLATFORM	DEPTH	NOTES
Azure · Microsoft 365 · Entra ID	**DEEPEST**	Run for real every day
AWS	**BROAD**	Verified against emulators; live accounts next
Google Cloud	**NARROWER**	Verified against emulators; live accounts next
Kubernetes · Docker · MuleSoft	**NARROWER**	Core checks; growing
On-prem servers	**BETA**	Collector in beta
Domains · endpoints · GitHub	**INCLUDED**	No cloud account needed

The coverage table on each product page lists exactly what is and isn't checked per platform.

SIMPLE PRICING

Priced by the size of what we monitor

Flat monthly bands, sized in units: a VM, database or cluster is 1 unit; a secret, bucket or IP is 0.2 — five of them make one.

STARTER	TEAM	BUSINESS	SCALE	ENTERPRISE
$29 /mo	$99 /mo	$299 /mo	$749 /mo	Custom
Up to 25 units	Up to 100 units	Up to 500 units	Up to 2,000 units	2,000+ units, quoted

- ✓ Every scanner
- ✓ All alert channels
- ✓ Unlimited users
- ✓ API on every band
- ✓ Cancel any time

Prices in US$. AI Insights included from Team up; the MSP bundle and compliance evidence pack are optional add-ons. Not sure of your size? Start the trial — your findings tell you.



Your infrastructure deserves a second pair of eyes.

Start a free 14-day trial. No credit card. No agent installs. Connect your first cloud or cluster in a few minutes.

cm.peripatetical.com/subscribe

Questions? cm.peripatetical.com/contact