AI-RUN IT INFRASTRUCTURE

Reduce IT staff 50% while increasing cybersecurity 17%.

Fewer people. Better posture. The work that used to need a networking specialist is now a conversation with an AI that holds the API keys.

−50%
IT headcount required to run the same estate

+17%
Average improvement in measured security posture

24/7
Config audit and drift detection, every device, every night

Figures are averages from my own client engagements — not vendor benchmarks. Method, baseline and scope explained live.

David Radszuweit · linkedin.com/in/catalyzt

IT infrastructure with AI

Cisco Meraki exposes the whole network as an API. AI writes to it. The specialist becomes optional, not the security.

Cisco Meraki Dashboard API · Bidirectional cloud sync · Webhooks · Zero-touch provisioning

01 Anyone with little networking skill can set up and secure an entire network with AI.

Describe the outcome in plain language — the AI produces the VLANs, firewall rules, SSIDs and policies.

02 API connection straight to the cloud controller.

No CLI on 40 boxes. One authenticated call reaches every site at once.

03 Direct, bidirectional link — the AI reads state as well as it writes it.

It sees what actually happened, not what was intended. That is where the security gain comes from.

04 Continuous audit instead of an annual review.

Every config, every device, nightly. Drift, open ports and stale rules surface the same day.

05 New site in hours, not weeks.

Template, ship the hardware, plug it in — policy applies itself on first boot.

REAL CASE · ANSWERED LIVE

WORKED EXAMPLE · NIST CSF 2.0 & ISO 27001

Read report ↗ PDF Word

Exec summary · PDF Word

The questions you should be asking me.

Pick any of them. No slides behind this — I answer from the actual deployment.

01 Where exactly does the 50% come from — which roles go, and which stay?

02 How do you measure a 17% security improvement? Against what baseline?

03 What happens the first time the AI pushes a wrong change to production?

04 Who is accountable at 03:00 when the network is down and nobody is on staff?

05 Is this really a saving, or just salary cost moved into licences and cloud?

06 What does the AI see of our data, and where does that data physically go?

07 Can the remaining team still operate the estate if the AI is unavailable?

08 How long from decision to the first saving that shows up in the accounts?

09 What breaks when we go from 5 sites to 50 — and what does it cost to fix?

10 How does this survive an audit — NIS2, ISO 27001, cyber insurance?

Support

Most IT salary cost is not engineering. It is answering the same forty questions forever. That part is now self-serve.

Company-specific FAQ | Voice-first access | Tier-1 automation | Self-improving

Humans keep the exceptions — and the exceptions are where they were always worth paying for.

01 A support layer trained on **your** FAQ, not the internet's.

Your VPN, your printers, your onboarding, your naming conventions.

02 High-level voice chatbot as the front door.

Call a number, speak, get an answer. Nobody has to learn a portal or open a ticket.

03 Tier 1 resolved before a human ever sees it.

Password, access, device, "is it down?" — closed in the same minute the user asked.

04 Every unanswered question becomes tomorrow's FAQ entry.

Coverage compounds. Month three is materially cheaper than month one.

05 The escalation path stays human and stays named.

Reduced team, clearer ownership — that combination is what moves the security number up.