



MANAGEMENT PRESENTATION · JULY 2026

C4SAM Cockpit

Security, automation & management of your IT infrastructure — one platform, one view, under your control.

-
- One platform
 - Self-hosted
 - Made in Austria

Three forces hit every IT organization

01



Regulatory pressure

NIS2, GDPR, ISO 27001, DORA: more obligations, more evidence — and personal liability for management.

02



Tool sprawl & talent shortage

Dozens of point solutions without a unified view — and too few experts to operate them all.

03



Cost and expectation pressure

The business expects security, availability, and AI capabilities — on flat budgets.

The biggest risk is not any single threat — it is complexity itself.

THE ANSWER

One cockpit instead of dozens of consoles

C4SAM collects and normalizes data from all security and infrastructure tools into a single unified view — usable without deep security expertise.



Security

Detect vulnerabilities, attacks, and anomalies — across IT, OT, and IoT.



Observability

Service checks and infrastructure metrics — with a service tree that points to the root cause.



Automation

Patch, respond, configure — automated, consistent, auditable.



Management & Compliance

Assets, services, and evidence — anchored in the native CMDB.

One platform: **See** → **Assess** → **Act** → **Prove**

● Automates routine work

● Usable by non-experts

● Existing tools integrate

● Scales from SMB to enterprise



PLATFORM

A curated app catalog, one interface

Around 40 integrated open-source and proprietary solutions — centrally installed, configured, and kept current. C4SAM connects to the systems you already run instead of replacing them.

~40 curated apps

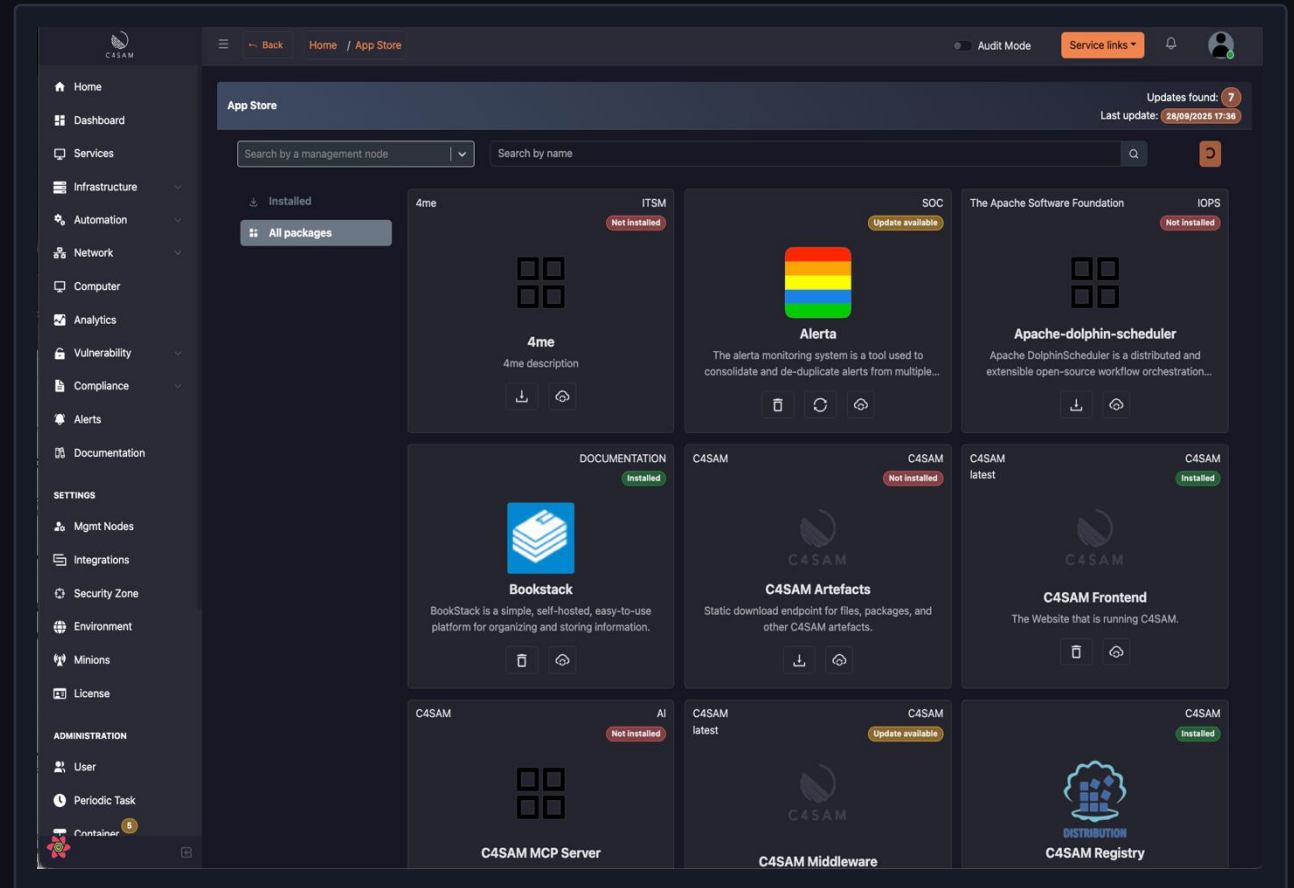
Open source and proprietary, one catalog.

100% managed lifecycle

Installed, configured, and kept current centrally.

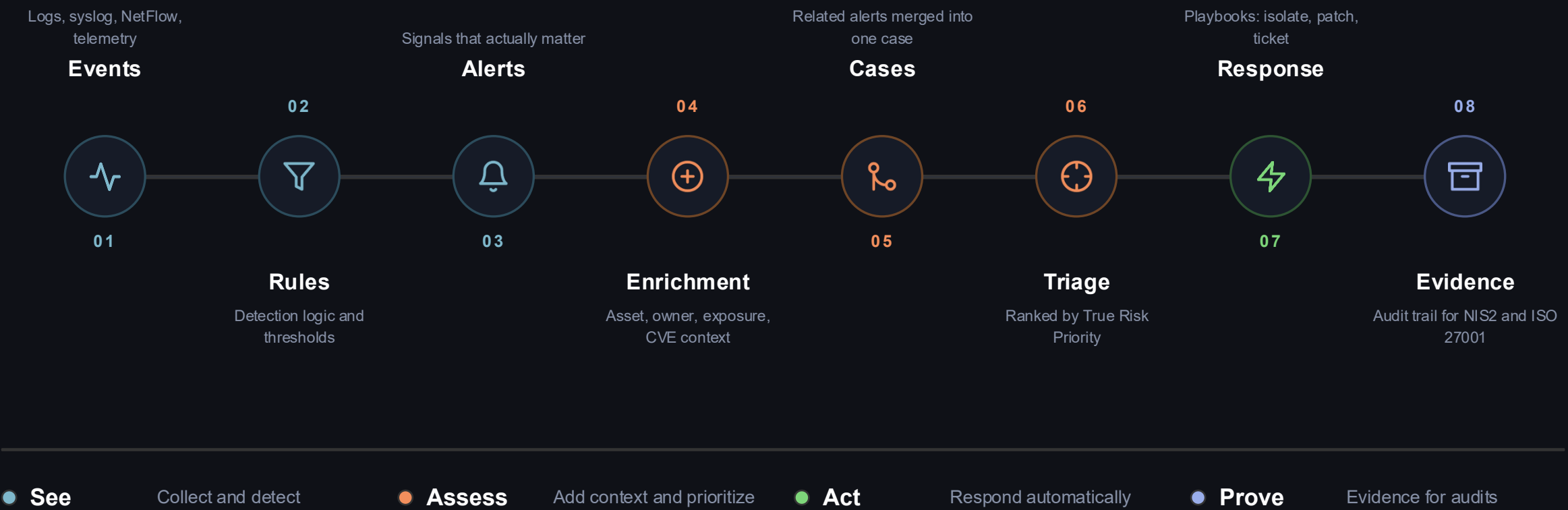
0 forced rip-outs

Your existing tools stay in place and are integrated — we replace only where it demonstrably saves cost.



From raw event to defensible evidence

Every signal runs through the same pipeline — reproducible, auditable, and identical across IT, OT, and IoT.



See it coming before the service goes down

Service monitoring from ICMP to full HTTP checks, hypervisor metrics, system performance, and network infrastructure — unified in the cockpit and the service tree.

- 

From ICMP to full HTTP checks

Reachability, ports, TLS handshake, response content and latency thresholds.
- 

Hypervisor & system metrics

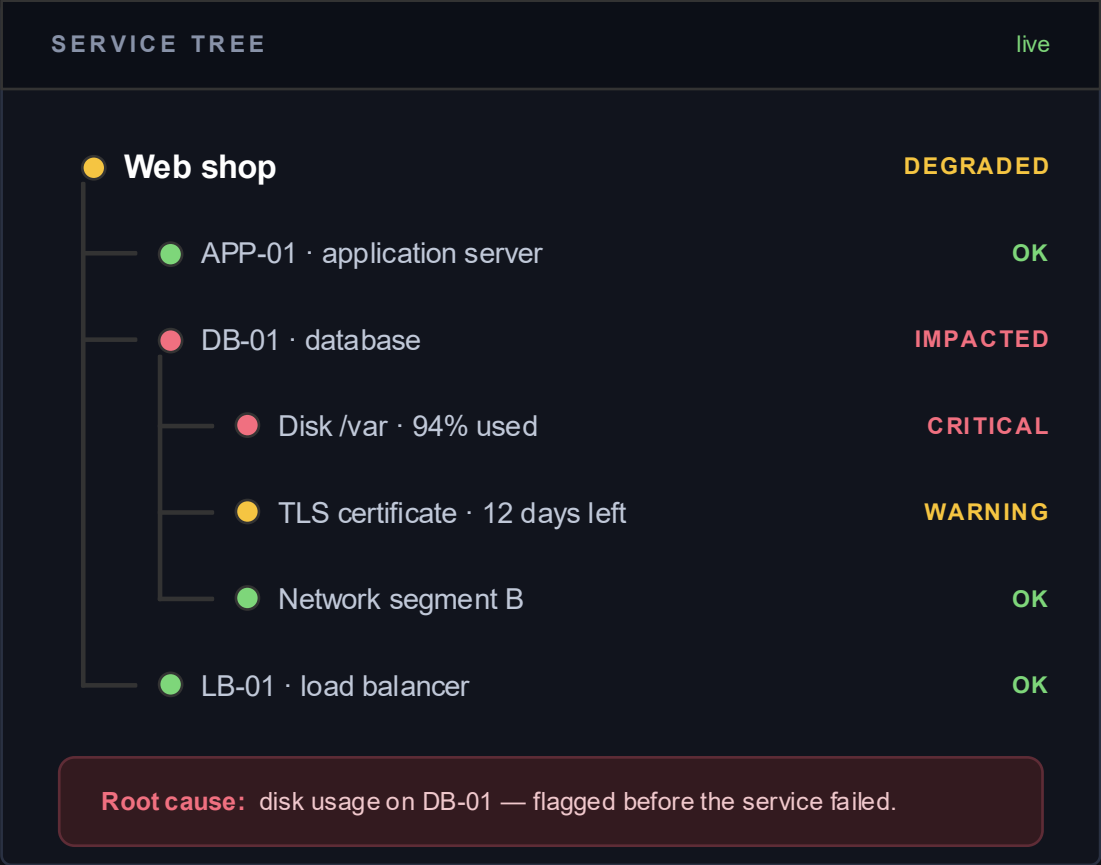
CPU, memory, storage and I/O across hosts, guests and containers.
- 

Network infrastructure

Switches, routers, firewalls and links via SNMP and NetFlow.
- 

Service tree

Every check mapped to the business service it supports.



What first? True Risk Priority answers it

True Risk Priority

Scanner scores alone say nothing about your business. C4SAM weighs exposure, business criticality, and reachability — then tells you what to fix first, and why.



Context over raw scores

Exposure, business criticality, and reachability weighed together — not a CVSS number in isolation.



Priority with reasoning

Every vulnerability gets a traceable priority — including the reasons that triggered it.



Binding deadlines

Audit-ready remediation timelines modeled on international standards (BOD-style).

Automation that removes the repetitive work

Plan.
Execute.
Verify.

Every routine task runs the same way, every time — with a full audit trail. How much manual effort this removes in your environment is measured during the assessment, with your own data.



Patch management

Plan, roll out, and verify automatically — systems stay current, without night shifts.



Incident response

Predefined reactions: isolate systems, adjust rules, notify owners — in seconds instead of hours.



Operations & configuration

Consistent environments without manual errors — from deployment to certificates.

NIS2 enforcement: the clock is ticking

Oct 1, 2026

In force in Austria

Austria's NISG 2026, published Dec 2025 — the transition period is running.

~5,000

Companies affected

18 sectors, from 50 employees or €10M revenue — plus the supply chain.

€10M

Maximum fine, or 2%

Of global revenue — with personal liability for management.

24/72h

Reporting window

Registration with the national authority; incident reporting within 24 and 72 hours.



C4SAM delivers the technical measures out of the box: asset inventory, risk management, incident detection and reporting — plus governance reports for audits and authorities.

AI for the business — no lock-in, no cloud-only



LLM gateway

Controlled access to cloud and local models: budgets, permissions, and usage per team — providers swappable at any time.



One frontend for everyone

A single interface for every model and agent — central user management, permissions per model and tool, full usage transparency.

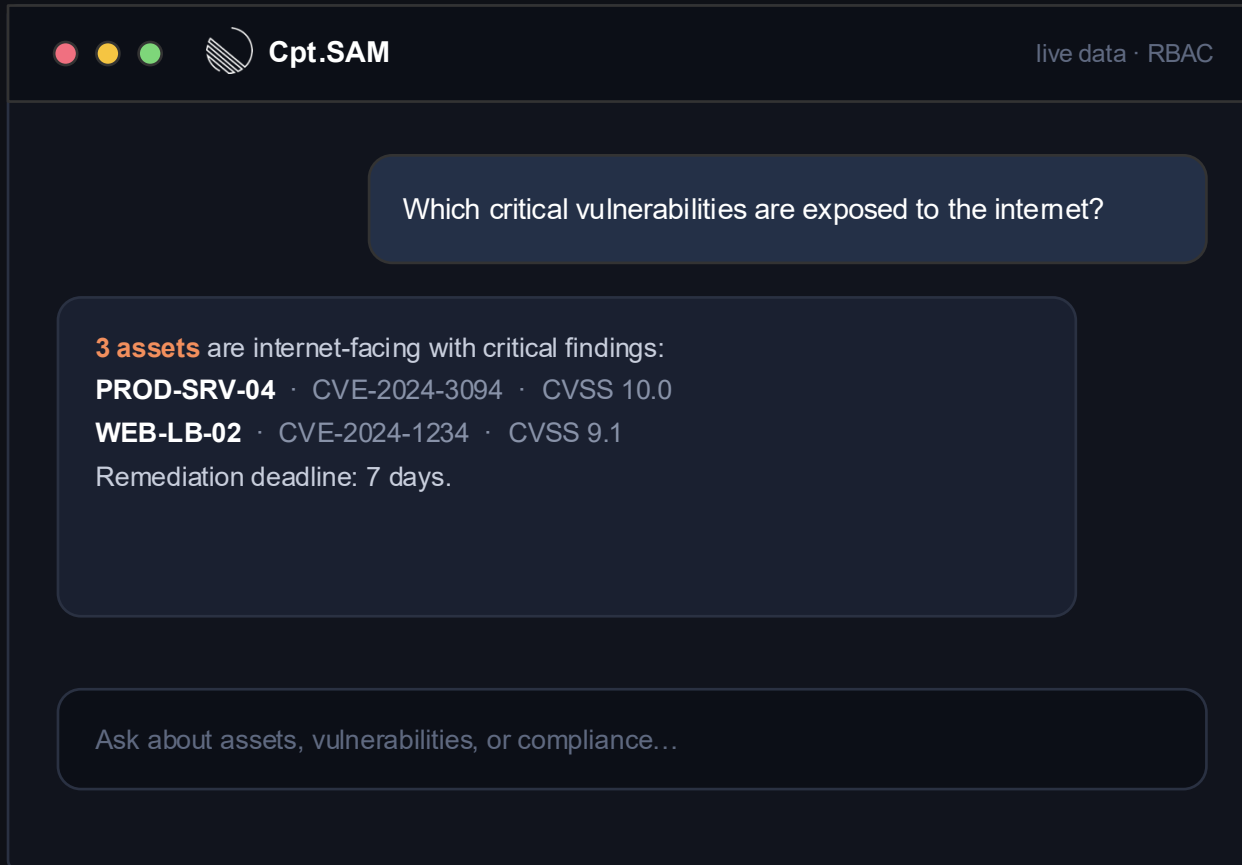


Personal AI agents

Every user gets their own isolated agent container — with scoped model access and securely managed credentials.

Delivering AI is the CIO task of 2026: the business gets AI now — IT keeps costs, data, and control.

Captain.SAM: AI that knows your infrastructure



Your analyst in the cockpit

Natural-language questions, answered from live data — no application switching, no query language.



Security & compliance built in

Data access via the C4SAM MCP server with role-based access control — everyone sees only what they may see.



Runs locally

Executed in your own infrastructure — GDPR-compliant by architecture, not by contract.

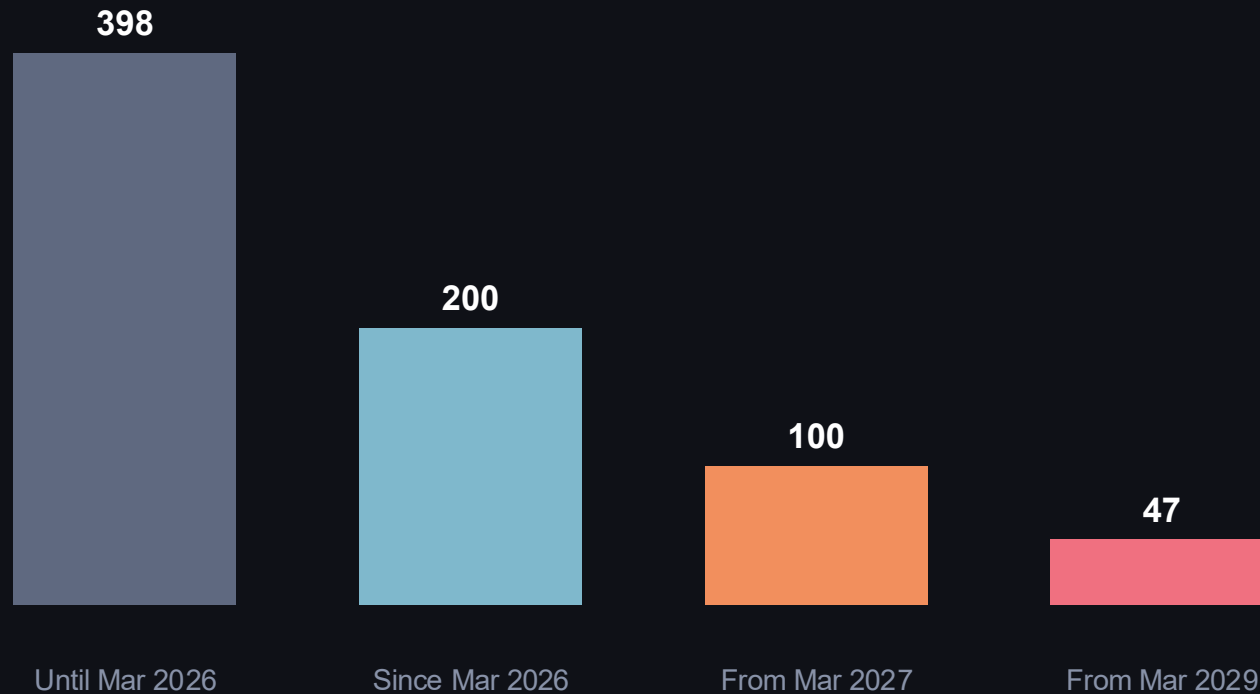
● Live demo available.



OUTLOOK

47-day certificates: automation becomes mandatory

Maximum TLS certificate validity, in days



Source: CA/Browser Forum, Ballot SC-081v3 (April 2025).

What it means

- 8× the renewal frequency — manual processes do not scale
- Forgotten certificates cause outages and lost trust
- Domain validation reusable for only 10 days from 2029



The C4SAM answer

Fully automated lifecycle: discovery, issuance, renewal, and deployment — including internal PKI, no internet dependency.

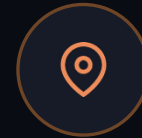
Your infrastructure, your data, your rules.

European data sovereignty is not a feature we added — it is how the platform is built.



Self-hosted & open source

Run on-premise or in your own cloud — no forced US SaaS, no black box.



Made in Austria

Developed and supported in Austria — GDPR and European law as the foundation, not an afterthought.



No lock-in

Open standards and interfaces: you stay in control at all times — including at exit.

Three reasons that matter in the boardroom

01



Consolidation & cost

One contract, one platform, one interface — instead of dozens of licenses and silos.

ONE VENDOR

02



Security & resilience

Detect faster, remediate by priority, respond automatically — measurably better response times.

FASTER RESPONSE

03



Future-proof & investment-friendly

We only replace what makes sense and saves money. AI and certificate automation: built in.

NO RIP-OUT

C4SAM turns IT security from a cost factor into a manageable, provable process.

NEXT STEPS

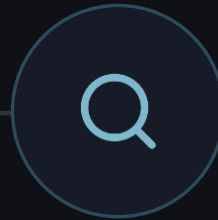
From first call to proof of concept



01

Initial call & impact analysis

NIS2 scope, certificate landscape, existing tools —
a shared picture of where you stand.



02

Assessment

Visibility across assets, vulnerabilities, and
compliance gaps in your environment.



03

Proof of concept

In your infrastructure — self-hosted, with your real
data.



C 4 S A M

C4SAM GmbH

Pülslgasse 4A, 1230 Vienna, Austria

+43 664 3518497

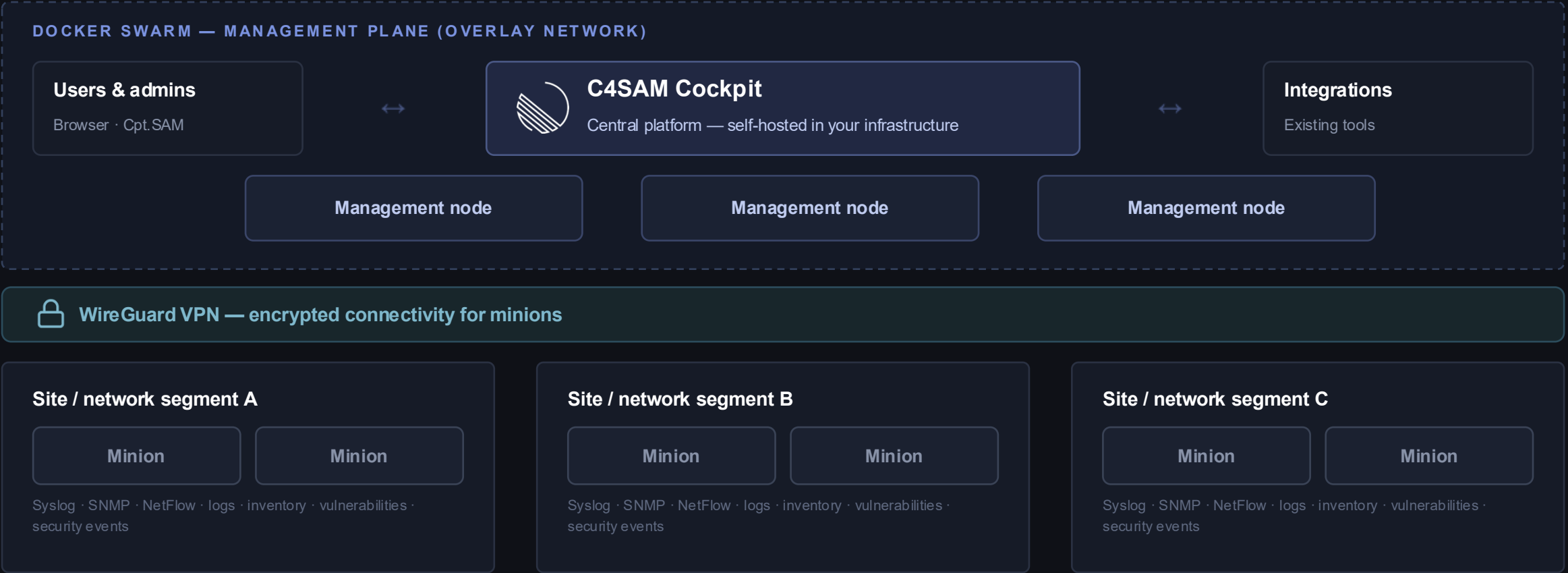
office@c4sam.com

www.c4sam.com



Deployment architecture: distributed, encrypted, self-hosted

The cockpit and the management nodes form a Docker Swarm (overlay network). Minions in sites and network segments connect via WireGuard VPN.



Scales by adding management nodes and minions — multi-tenant across sites, subsidiaries, or customers.

