



COMPLETE VISIBILITY. SMARTER DECISIONS. STRONGER SECURITY.

MANAGED MONITORING • ALERTS • SECURITY HYGIENE • REPORTING

[Sales brochure](#)

Updated 19 September 2026

salixmonitor360.je

WHY SALIX

Monitoring should reduce uncertainty, not create another job.

Salix Monitor 360 connects outside-in service checks with inside-the-host evidence, routes the right alerts and keeps a usable operational record after the incident is over.

ONE VIEW

What is failing?

Websites, APIs, network services, databases and host signals sit in the same operating picture.

ONE RESPONSE

Who needs to act?

Warning and Critical rules, quiet hours, channels, acknowledgement, snooze and shared notes keep ownership visible.

THE RESULT

Fewer surprises. Quicker triage. Better evidence afterwards.

Built for IT teams, businesses and service providers that need practical monitoring without operating a heavyweight observability stack.

Outside checks

Host context

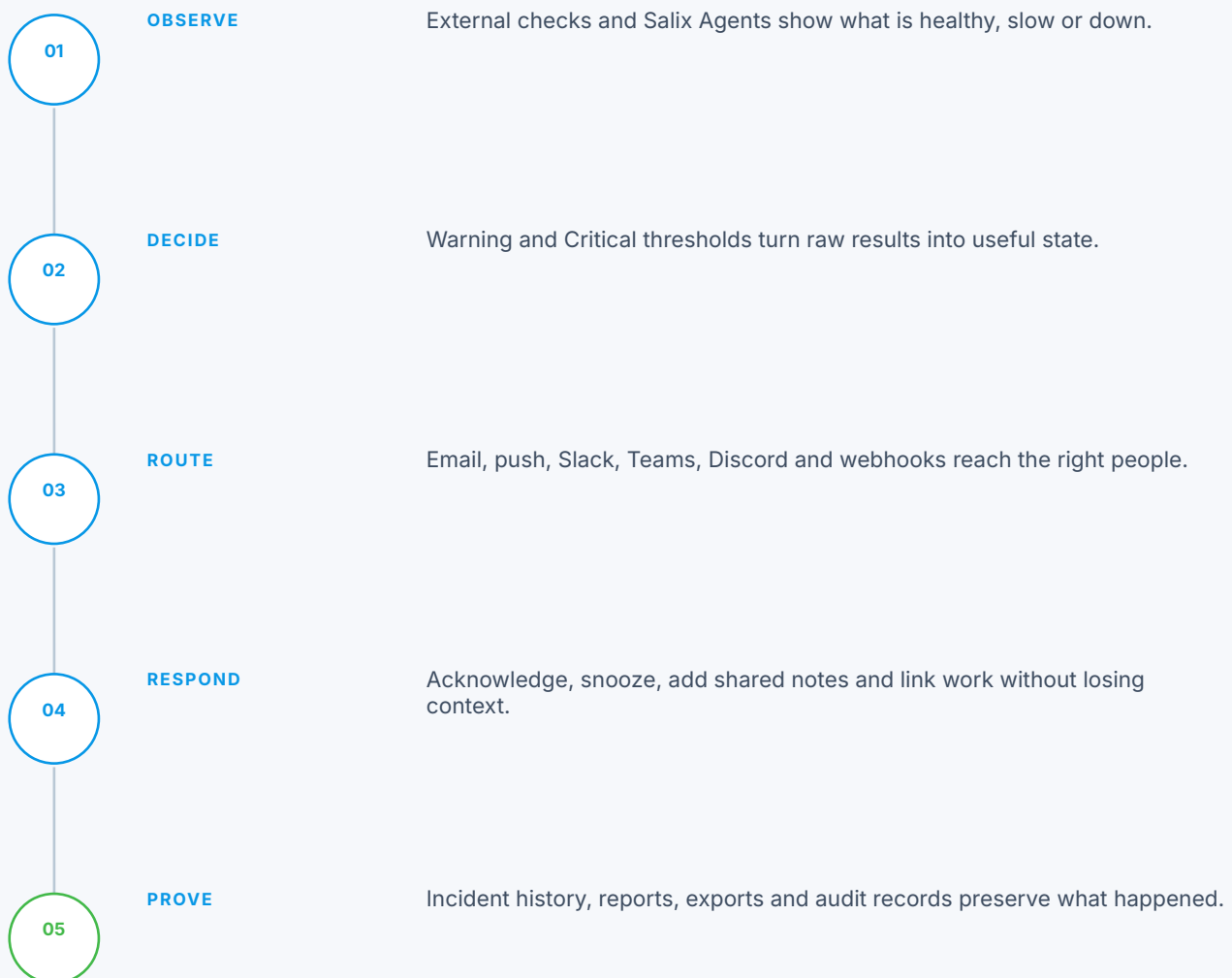
Actionable alerts

Evidence

A JOINED-UP OPERATING LOOP

From signal to resolution without losing the story.

Salix keeps the monitor, rule, organisation, actor, timestamps and follow-up work connected so the same evidence can serve operations, reporting and review.

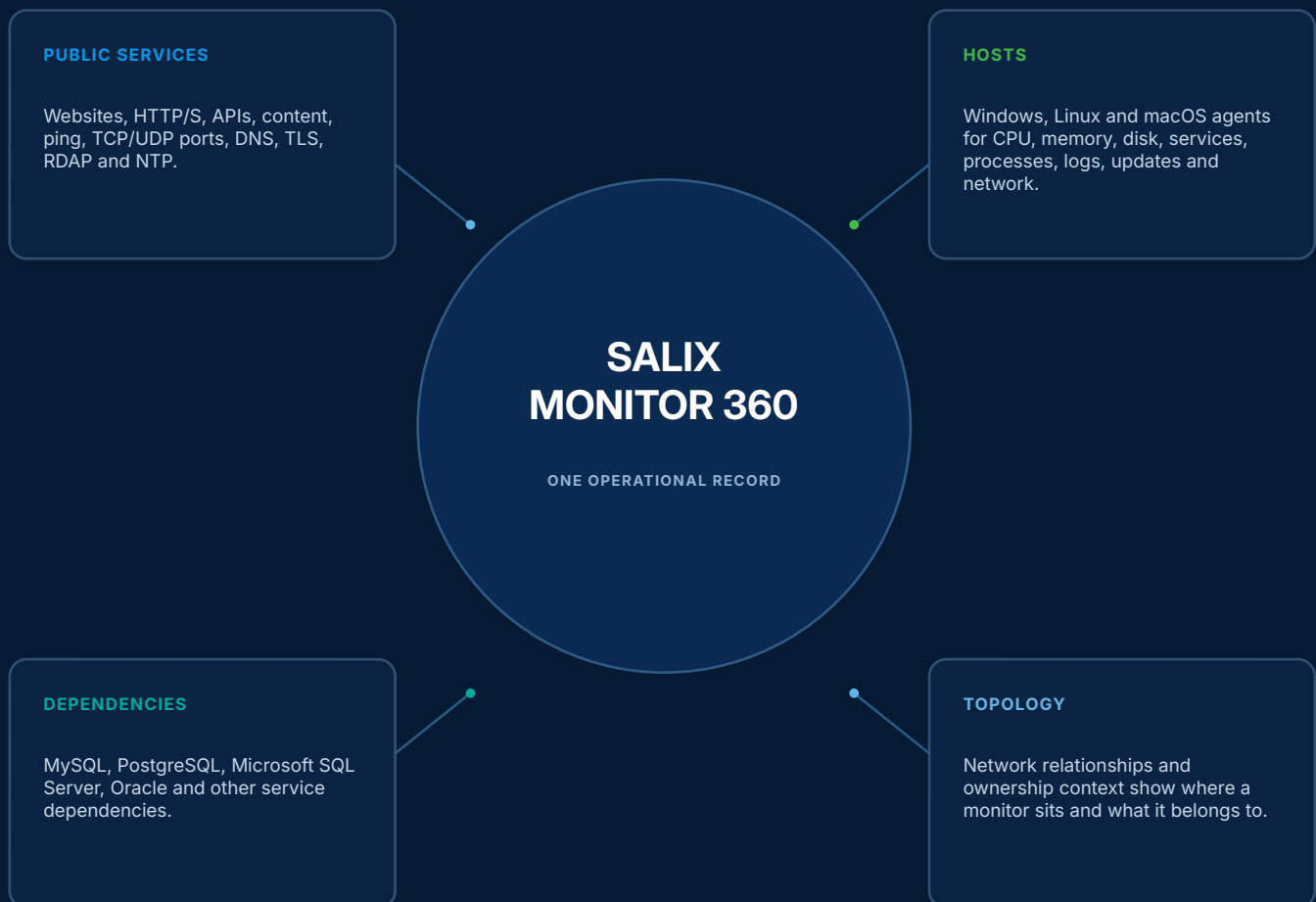


The same operating record follows the work across administrators, everyday users, web and companion apps.

ONE SERVICE, SEVERAL VANTAGE POINTS.

See the service from the outside and the host from the inside.

External availability, private host health, network relationships and key dependencies are easier to understand when they are reviewed together.

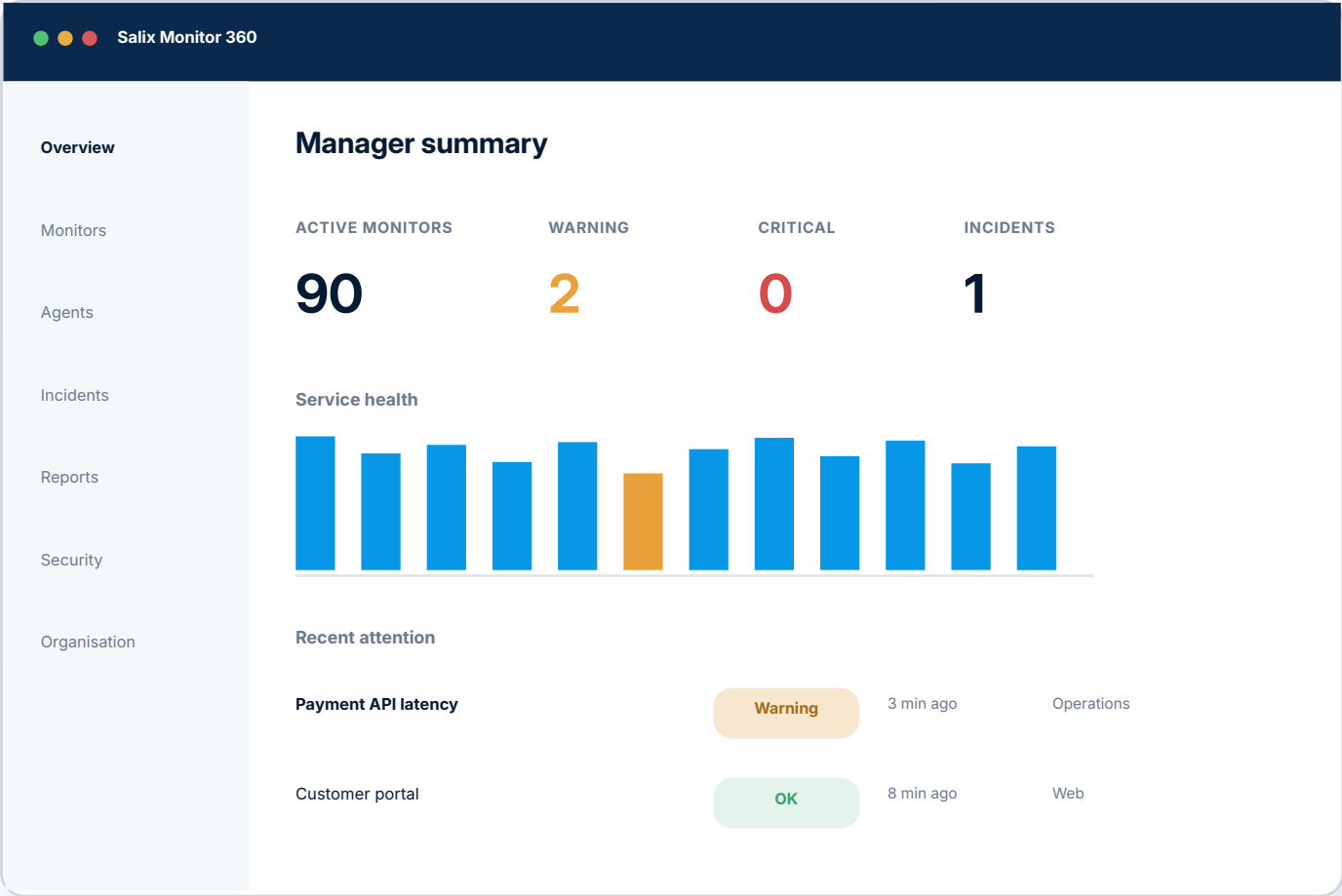


Practical coverage is the point: enough context to reduce guesswork when a service degrades.

A DASHBOARD BUILT FOR DECISIONS, NOT DASHBOARD THEATRE.

Current health first. Detail when you need it.

The admin dashboard brings service state, incidents, recent activity and ownership into one operational view. TV mode fits the same dashboard to a shared screen instead of inventing a second dashboard.



What it answers

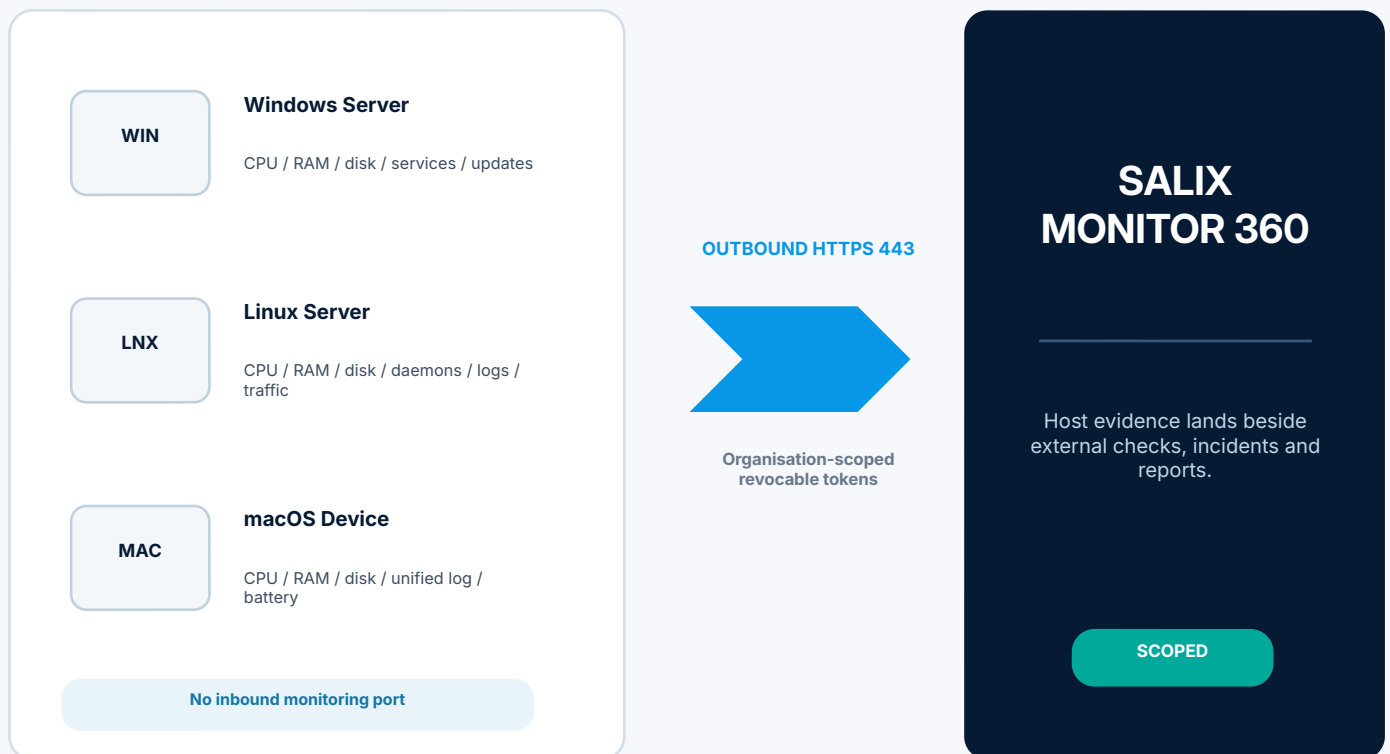
- What needs attention right now?
- Which service or organisation owns it?
- What changed and who has acted?
- What should be visible on the office TV dashboard?

INTERNAL VISIBILITY WITHOUT PUNCHING HOLES THROUGH THE FIREWALL.

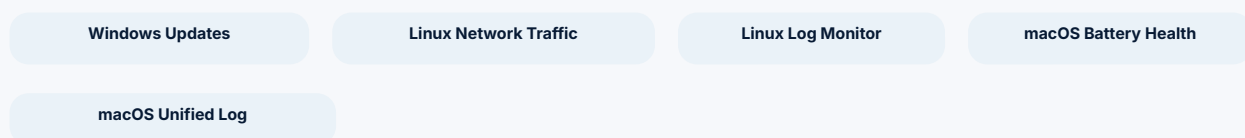
One lightweight agent per host.

Windows, Linux and macOS agents call out to Salix over HTTPS on TCP port 443. Private systems can report health without exposing an inbound monitoring port.

PRIVATE NETWORK



Expanded host-aware monitors



ALERTS WITH A STORY, NOT ANOTHER NOISY INBOX.

Route the signal, keep the context.

Salix links alert rules to monitors, organisations and incident history so responders can see what happened, who acted and what was done.



ROUTE WHERE PEOPLE ALREADY WORK

Email | Web push | Companion push | Slack | Teams | Discord | Webhooks

Incident 00431 **WARNING**

Payment API latency

Opened 21:14 | Owner: Operations | Monitor: API /payments

21:16 Acknowledged by Alex
21:18 Shared note added: provider status checked
21:22 Ticket INC-883 linked
21:31 Recovered and retained in incident history

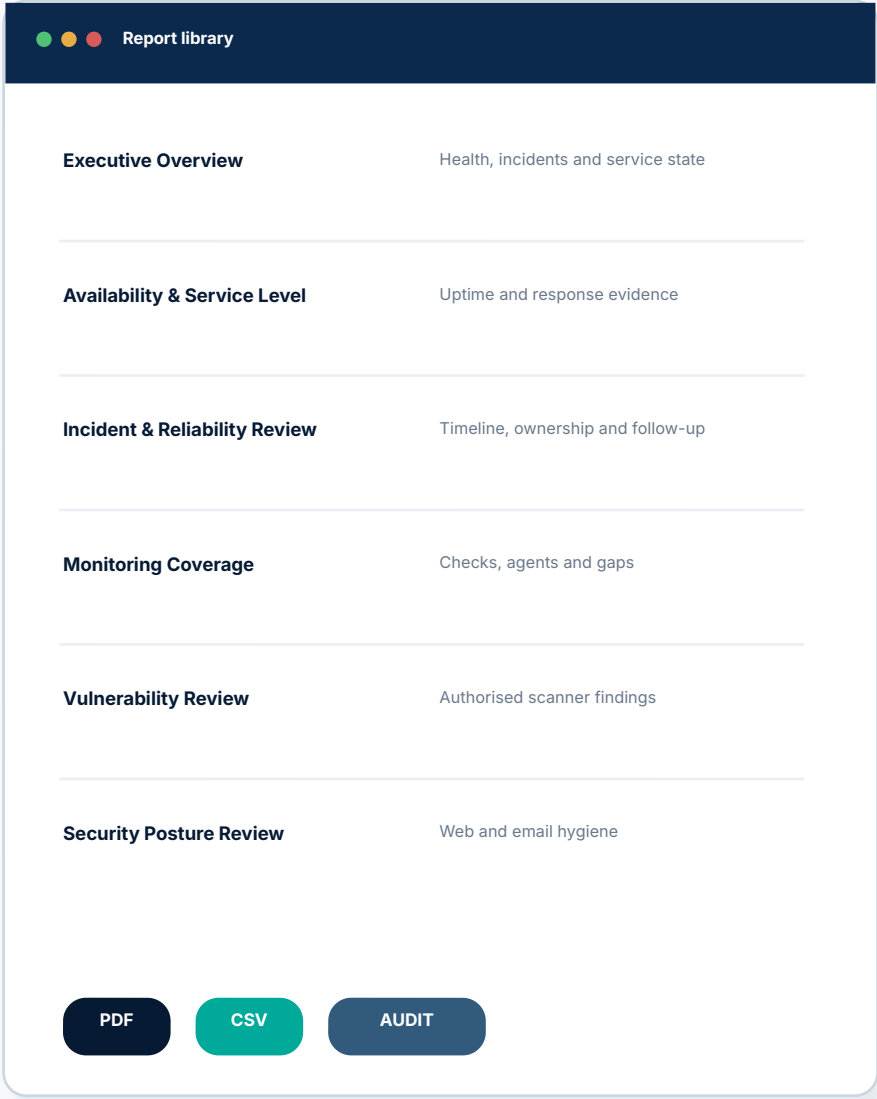
ACKNOWLEDGED
TICKET LINKED
RECOVERED

The alert never becomes an orphaned email: the operational record stays attached to the monitor and the work.

PURPOSE-BUILT REPORTS, NOT RAW-DATA ARCHAEOLOGY.

Turn daily monitoring into evidence people can actually use.

Salix keeps reports close to the operational record so teams can explain service health, incidents, security and administrative activity without reconstructing the month from scattered tools.



WHAT A USEFUL REPORT SHOULD ANSWER

01 What happened?

Monitor state, timing and operational context.

02 What did we do?

Acknowledgement, notes, linked tickets and ownership.

03 What changed afterwards?

Recovery, recurring patterns, posture or follow-up.

Monitoring data gains commercial and governance value when it becomes a concise, defensible record.

POSTURE FOR THE EVERYDAY. SCANNER EVIDENCE WHEN AUTHORISED.

Availability and security hygiene belong in the same conversation.

Salix keeps practical security checks beside service monitoring and can retain normalised evidence from approved vulnerability scans.

SECURITY POSTURE

Readable hygiene you can improve over time.

- Certificate inventory and expiry
- HTTPS, HSTS, headers and CORS
- Cookie flags and HTTP methods
- SPF, DKIM and DMARC email hygiene
- Public storage, dependency and script exposure checks
- History that shows regressions and improvement

AUTHORISED VULNERABILITY EVIDENCE

Scanner output becomes a reviewable operational record.

NMAP

Host and service discovery

Open ports, services and host evidence.

NUCLEI

Template-driven findings

Severity, evidence and remediation context.

ZAP

Web application findings

Normalised findings retained by host and time.

Important boundary

Scanning is for authorised targets only. Scope and heavier scanning workloads should be agreed before use.

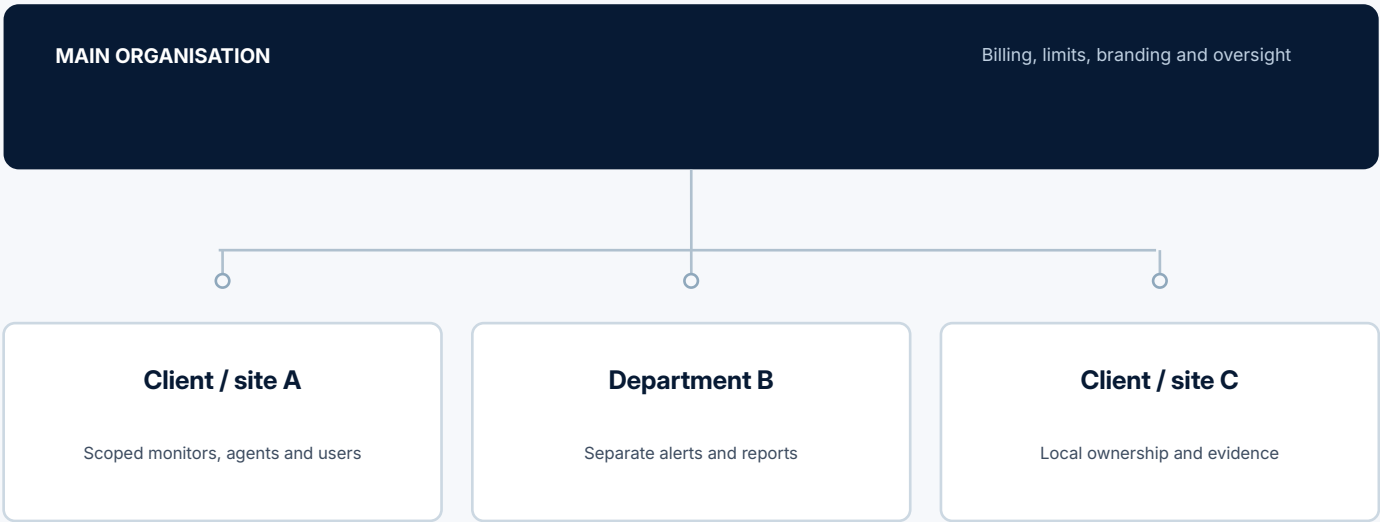
The goal is not a vanity score. It is a visible backlog, a history of change and evidence that supports sensible review.

BUILT FOR THE WAY REAL ORGANISATIONS SPLIT RESPONSIBILITY.

One subscription can support several operational workspaces.

Main organisations, linked sub organisations, teams and roles keep monitoring, people, reports and evidence in the right scope while allowing authorised oversight across the wider account.

STRUCTURE



WORK THE WAY THE TEAM NEEDS TO

Roles and teams	Branding and status pages	Four interface languages	Companion apps
Control who can view, change and respond.	Present the right identity and selected service status.	English, French, Spanish and German across the web and companion experience.	Windows, Android, iPhone and iPad keep the active alert queue close.

ONE ACCOUNT RECORD

Language and device choice change how people work with Salix - not where the underlying operational record lives.

CLEAR HOSTED PLANS, PLUS IN-HOUSE OPTIONS.

Start free. Add capacity when the monitoring proves its value.

The hosted service is the quickest route in. Established organisations can also discuss an in-house licence on infrastructure they control.

HOSTED SAAS

PLAN	PRICE	CAPACITY	ORGANISATIONS
Free	£0 / month	5 monitors 2 agents 3 users	1 main organisation
Standard	£50 / month	50 monitors 10 agents 10 users	Up to 5 linked organisations
Professional	£150 / month	150 monitors 30 agents 30 users	Up to 10 linked organisations
Business Unlimited	£300 / month	No normal published caps	Fair-use sizing

Paid hosted plans include direct Willow Software support for the hosted service. Free accounts are intended for trial use.

IN-HOUSE LICENCE

Business

from £7,500 / year

Supported in-house licence for organisations with their own IT team: installation guidance, updates, onboarding and priority support.

Managed / Enterprise

from £15,000 / year

Adds higher-touch support and an agreed level of bespoke engineering, custom monitoring and closer technical involvement.

In-house supply is subject to a suitability review. Annual licence commitment; invoice schedule can be annual, quarterly or monthly if agreed.

NEXT STEP

READY TO SEE WHAT SALIX CAN DO FOR YOU?

Start with your real services, not a demo checklist.

Create a free organisation with 5 monitors, 2 agents and 3 users. Add the websites, APIs and hosts that matter to you, then decide whether the hosted service, a paid plan or an in-house deployment is the right next step.

START FREE

salixmonitor360.je/signup

Create an organisation and begin with real monitoring.

OPEN THE APP

monitor.salixmonitor360.je

Use the hosted service as the operational control centre.

TALK TO WILLOW

info@willowsoftware.co.uk

Ask about in-house deployment, bespoke monitors, integrations or support scope.

Willow Software**+44 7797 751170**

Thrifty Hollow, Mont Nicolle, St. Brelade, Jersey, JE3 8GP

salixmonitor360.je | monitor.salixmonitor360.je | willowsoftware.co.uk