mondoo

CASE STUDY

PASSPORT TO RESILIENCE

How a leading European travel group brought 1,000 assets, from AIX to AWS, under continuous assessment with Mondoo, and reached same-day visibility with the team it already had.

A security program does not fall behind because it lacks a standard. It falls behind when proving the standard is manual work: sampled, exported, and already out of date by the time anyone reads it.

The teams that read the problem correctly build something different, so that evidence becomes a by-product of running security well rather than a project of its own.

The travel group in this case study did exactly that, and Mondoo is the platform that evidence runs on.

Six people now assess roughly 1,000 assets, from business-critical AIX to multiple AWS accounts. The seven-day blind window is gone, technical audit evidence collection dropped from months to days, and every AWS account in scope is now covered. The estate grew. The team did not.

AT A GLANCE

ORGANIZATION: Leading European travel group, multiple operating companies

SECTOR: Travel and tourism

SCALE: Seven countries, millions of travelers a year, more than 2,000

REGION: Europe

ENVIRONMENT: Hybrid: on-premises Linux, Windows, and business-critical AIX, plus multiple AWS accounts

SECURITY TEAM: Six people, covering security engineering and security operations

FRAMEWORKS & REGULATIONS: CIS, PCI DSS, ISO 27001, NIS2, GDPR

MONDOO'S ROLE: Continuous vulnerability, configuration, and compliance assessment across the fleet

This case study was reviewed and approved by the customer, who asked not to be named.

01
THE GROUP

CONTINUITY AND TRUST ARE THE SAME PROBLEM

A leading European travel group moves millions of travelers a year, operates across seven countries through a portfolio of companies, and employs more than 2,000 people. Its technology estate carries the whole customer journey: booking systems at the front end, and behind them the operational coordination that gets travelers to their destination and looks after them along the way.

Security sits at the intersection of two business imperatives. Continuity: an outage or attack could stop bookings, disrupt fulfillment and destination logistics, or leave travelers without timely information and support. Trust: the group handles sensitive personal data, including names, passports, dates of birth, and booking records. Five frameworks and regulations shape the program, CIS, PCI DSS, ISO 27001, NIS2, and GDPR. GDPR is particularly demanding in a sector that has to exchange customer data with partners in third countries.

Leadership's direction to the six-person security team is straightforward: make the company as secure as possible without preventing the business from operating.

02
THE CHALLENGE

A WEEKLY SCAN, A PDF, AND A SEVEN-DAY BLIND WINDOW

The old process was a chain of separate tools and manual follow-up. A weekly Tenable Nessus scan produced a PDF. Someone reviewed it, translated findings into tickets, chased the owners, and eventually ran another scan to see whether anything had changed. Credentialed remote scanning also meant provisioning and safeguarding a high-privilege account on every box in the estate.

Two problems compounded each other. Latency: because the scan ran weekly, a vulnerability could exist for up to seven days before anything found it, and a critical finding then took

another one to three business days to remediate. Coverage: the gaps were most acute on the business-critical AIX systems, where a deep review could occupy external specialists for days per sample and the native CIS scanner offered no useful remediation guidance. The team leaned on samples and expert judgment rather than continuously verified evidence.

There was no breach and no failed audit. Three things converged instead: a newly established cross-functional security team, a mandate to raise the security level across teams that had previously worked separately, and the decision to adopt CIS as the group's practical standard. That last decision was pivotal, and it needed a route that did not depend on manual collection and samples. Without a scalable platform, the choice was to accept incomplete fleet coverage or add an estimated four people.

> "Mondoo did not create the CIS goal. It made that goal operationally achievable."
>
> TEAM LEAD IT SECURITY

03
THE RESULTS

WHAT CHANGED, IN NUMBERS

~1,000	**6** people	**3–4** days
Assets under continuous assessment, up from fewer than 200	Running a program that would otherwise have required roughly four additional hires	Technical audit evidence, down from an effort measured in months

	BEFORE MONDOO	WITH MONDOO
Assessed assets	Fewer than 200	Roughly 1,000
AWS accounts	No coverage at all	All accounts in scope covered
Detection cadence	Weekly scan, up to a seven-day blind window	Continuous, with same-day action possible
Technical audit evidence	Months; one early effort took close to seven months	Three to four days for a defined scope
Team needed for that scope	An estimated ten people	The existing six
Basis for evidence	PDF exports, spread-sheets, and samples	Current fleet-wide technical proof

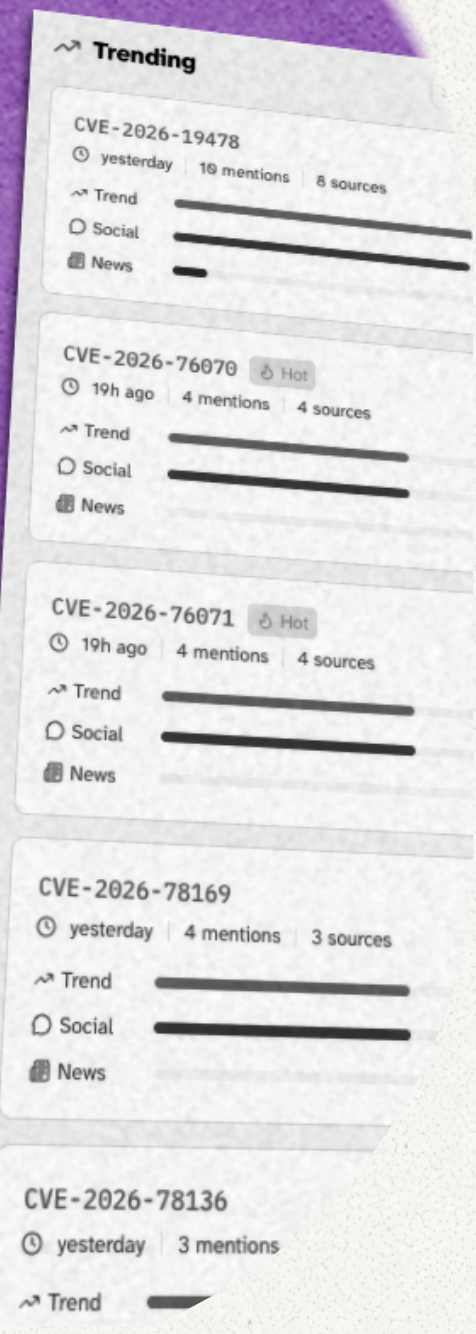
Part of the growth in assessed assets reflects the business growing too. The clearest business outcome is the ratio: **coverage scaled without the team scaling with it.**

04
THE SOLUTION

ONE PLATFORM, ONE CURRENT VIEW OF THE FLEET

Mondoo runs agent-based assessment across the hybrid estate: on-premises Linux, Windows, and AIX, plus multiple AWS accounts. IT keeps vulnerability and compliance in one place instead of splitting them across tools and workflows. Three things decided it.

Open source at the core. The cnspec scanning component is open source, which means the team can inspect and understand what actually runs in their environment, and so can the wider community.



Open documentation also let them evaluate deployment and product quality before committing, without a sales gate.

A deployment that feels native. Mondoo installs through standard package managers such as apt and dnf, so rollout felt native to the group's Linux environment rather than bolted on. Compared with remote scanners, the agent also provides a more current view without distributing a high-value credentialed account across the estate.

One platform, both use cases. Vulnerability and compliance assessment sit on the same underlying data, which as coverage expanded began to support reporting, asset insight, and new automation too.

A vendor the team could reach. The commercial comparison mattered, but the relationship weighed just as heavily. The team could talk directly to knowledgeable engineers and to Mondoo's leadership, raise feature requests, and be heard.

> "We could speak directly with knowledgeable people and raise feature requests, and feel heard rather than feel like one customer among tens of thousands."
>
> TEAM LEAD IT SECURITY

THE CVE QUESTION, ANSWERED IN ONE PLACE

With the previous scanner, answering "are we affected?" meant finding the right plugin, configuring targets and credentials, running the scan, waiting, exporting results, then repeating all of it after patching to prove the fix had landed. With Mondoo the current estate-wide result is already in the tenant: the team filters it, assigns owners, and creates tickets directly from the platform. AIX system owners use the same data to raise hardening and compliance scores. MQL query speed and the sheer amount of operational work that now happens in one place were both positive surprises.

05
THE PROCESS

START WITH A GOAL, NOT A TOOL

The team assessed Rapid7, Tenable Nessus, and Qualys, alongside agent-based alternatives, against broad ecosystem and AIX coverage, CIS capability, a lightweight deployment model, current evidence, useful remediation information, transparency, and cost. The security team lead and the head of IT decided together that an agent was the right model, while recognizing that every agent must itself be evaluated as part of the attack surface.

A carefully prepared proof of concept did the rest: Mondoo asked what the team needed to see, ran concrete working sessions of an hour to ninety minutes, and demonstrated those workflows successfully, so production onboarding matched the expectations the POC had set. Getting systems in was unusually painless, with Spaces giving each team the right installation command and placing assets in the right context automatically. The hardest part was organizational: defining what 100% coverage means when you cannot be certain the CMDB contains every asset.

WHAT THE TEAM WOULD TELL A PEER

- Start with a goal, not a tool.
- Expect deployment to expose weaknesses in your CMDB. That is useful information, not a setback.
- Use risk and compliance scores to build momentum in the first weeks, when teams see their own improvements immediately.
- Take your time with hardening. Driving a score above 90% without understanding the operational impact can leave a system secure on paper and unavailable in practice.
- Use exceptions properly: documented, time-bounded, and reviewable.

On organizational buy-in, leadership trust was already earned. The team framed Mondoo as the means to reach the CIS and wider security goals on time and at reasonable cost, and chose a three-year horizon deliberately, wanting enough runway to deploy the platform properly and grow with it.

> “The business case was not a one-year feature checklist. It was sustainable coverage and operating leverage for the security program.”
>
> TEAM LEAD IT SECURITY

06
THE TAKEAWAY

mondoo.com
email
linkedin

COVERAGE CANNOT BE SAMPLED. IT HAS TO BE MEASURED.

The honest reading of the data matters as much as the headline. The evidence now rests on current technical proof rather than self-reported spreadsheets, which gives both the security and GRC teams more confidence in the conclusions. Remediation is not yet a clean apples-to-apples comparison. Critical MTTR stood at approximately eight days from CVE publication to remediation. The historical process combined a weekly scan with one to three business days of fixing, so the same critical finding took roughly eight to ten days to close. That assumed the scan surfaced it at all.
The structural improvement is the removal of the seven-day blind window, and the remediation trend is expected to follow as the program matures.

Mondoo is also becoming a source of record for a more reliable software and security CMDB, and stakeholders now pull the reporting they need directly instead of asking for another scan report that may already be out of date. The outcome the team values most, though, is not a number: confident visibility across almost the entire IT landscape, on premises and in the cloud, current enough to act on, with the technical basis for a finding visible rather than inferred from a stale report or a self-attestation.

THE ESTATE GREW.
THE RESPONSE GOT FASTER.
THE WORKLOAD DID NOT.