

CONTEXT IS EVERYTHING

How a cloud and managed services provider turned security findings into fixes with Mondoo, and cut audit preparation from months to weeks.

A security alert is only as useful as the context around it. Without context, every critical finding becomes an investigation, and the team spends its time proving which issues do not matter before it can fix the ones that do. The teams that read the problem correctly stop measuring how many findings they produce and start measuring how quickly they get from a finding to a fix. Evidence then becomes a by-product of that work rather than a project of its own.

The provider in this case study holds sensitive data on behalf of its customers, and Mondoo now sits at the center of how it finds, prioritizes, and fixes security issues.

Findings arrive with the context to judge whether they matter and with remediation guidance ready to apply. Secure VM templates are validated at build time. In the areas where Mondoo is in use, audit preparation has dropped from several months to around six weeks.

AT A GLANCE

ORGANIZATION: Cloud and managed services provider

SECTOR: Cloud computing, managed services, data and AI

ENVIRONMENT: Cloud and virtualized infrastructure, application code, and CI/CD pipelines

TEAMS USING MONDOO: DevOps and automation, platform, and security teams

FRAMEWORKS & REGULATIONS: ISO 27001, SOC 2 Type 2, a national cyber security certification; working toward an AI management standard

MONDOO'S ROLE: Context-aware vulnerability prioritization and remediation, secure VM template validation, and continuous compliance evidence

01

THE PROVIDER

TRUSTED WITH DATA, BUILT ON COMPLIANCE

The provider offers cloud computing and managed services and has grown over the years to add data and AI capabilities to its portfolio. Its customers trust it with their data, and that trust is the business. Preventing unauthorized access is not a feature of the service. It is the service.

Compliance is part of the culture. The provider has held ISO 27001 for many years, alongside SOC 2 Type 2 and a government-backed cyber security certification. As it builds its own AI capabilities, it is now working toward an AI governance standard.

Compliance also shapes how the provider buys technology. Every new supplier or tool is audited to make sure the data going into it is controlled, and only tools that meet those guidelines and are fit for purpose make it through. The security team works as an advisor rather than an enforcer, helping engineering teams understand problems and possible fixes instead of issuing mandates.

The provider's DevOps and automation team has a clear mandate of its own: automate manual processes so people can spend their time on higher-value work.

“If someone's trusting you with their data, it makes sense that you don't let unauthorized people access it.”

ENGINEERING LEADER, DEVOPS AND AUTOMATION

02

THE CHALLENGE

ALERTS WITHOUT CONTEXT, EVIDENCE BY HAND

Before Mondoo, the honest answer to “how secure is this asset?” was often “we’re not sure.” Scanning covered a limited set of systems. Development teams ran static analysis and dependency checks that blocked any push or deployment with a critical or high CVE. That protected the code, but beyond it much of the work was manual. The security team worked through asset lists by hand, checking which version each system was running and whether it carried known vulnerabilities.

Two problems compounded each other. Context: the previous tooling could flag a vulnerability, but not whether it actually mattered in the provider’s environment, so every serious alert had to be investigated before anyone knew whether it was real. Evidence: audits meant logging on to servers to pull configuration details and querying application databases by hand. Preparing for a single audit could take several months.

The cost was time, spent investigating issues, fixing them, and redoing work. For a team whose job is to automate manual effort away, that was the wrong direction.

“A lot of the tools before had no real context to them. That’s a big one.”

ENGINEERING
LEADER, DEVOPS
AND AUTOMATION

03

THE SOLUTION

WHAT CHANGED, IN NUMBERS

~6 weeks

Audit preparation in the areas using Mondoo, down from several months

10-20 min

From installing Mondoo to a new asset appearing in the platform

1 dashboard

Showing where to focus, replacing manual asset and version checks

BEFORE MONDOO		WITH MONDOO
Audit preparation	Several months	Around six weeks in the areas using Mondoo
Audit evidence	Manual server logins and database queries	Mondoo results used as evidence
Secure VM templates	Checked by hand	Checked automatically at build time
Vulnerability context	Alerts without context; investigation needed to rule issues out	Findings related to the specific environment
Remediation	Research the fix yourself	Ready-to-apply remediation guidance
Prioritization	Manual asset and version checks	One dashboard showing where to focus

Adoption started in focused pockets rather than as a big-bang rollout, so the results are strongest where Mondoo is already in use. The clearest outcome is the direction of travel: **less time proving what does not matter, more time fixing what does.**

04

THE SOLUTION

FROM FINDINGS TO FIXES, WITH CONTEXT

Mondoo works across the provider's many asset types and shows which issues actually relate to its environment, so teams spend their time on what is real instead of chasing what is not. Four things changed how the work gets done.

Security built into the VM build pipeline. The provider's compliance requirements mandate that virtual machines are built from a secure template. Mondoo is now part of that process: each template is checked as it is built, and the results are passed on as evidence for the relevant control. Security validation happens automatically at build time instead of manually at audit time.

A dashboard that shows where to focus. Instead of piecing together asset lists and version checks, teams see in one place what needs attention. The team estimates this alone saves quite a few hours a day.

Fixes, not just findings. What surprised the team most was Mondoo's remediation guidance. Rather than pointing at a problem and leaving engineers to research the answer, Mondoo provides a fix that can be applied directly.

Platform and security teams working together. Platform teams manage their assets in Mondoo, and the security team uses the same findings to flag CVEs that need attention. That fits the way the provider's security team already works: advising and collaborating, not issuing mandates.

“ I'd never seen a tool do it. Mondoo was one of the first to give me a remediation fix, which was very helpful.”

ENGINEERING LEADER, DEVOPS AND AUTOMATION

THE CRITICAL CVE THAT WASN'T

In one recent case, a critical CVE turned out, after investigation, not to affect the provider at all.

The attack depended on a route that had already been closed off. Without context, every alert like that costs investigation time before anyone knows whether it is real, and the team still has to prove the answer afterwards.

That is the gap Mondoo is built to close. Findings are tied to the specific environment, so the question “are we affected?” starts with an answer rather than an investigation, and the remediation guidance is already there when the answer is yes.

05

THE PROCESS

START SMALL, THEN GROW OUTWARDS

The DevOps team's first hands-on work with Mondoo came when it built an internal application around the platform alongside other sources of context. Getting started was simple: install, run, and within about 10 to 20 minutes the asset appeared.

The learning curve was gentle, with everything easy to find and understand. Support has been just as smooth. The team describes it as fantastic, with colleagues who raise tickets getting answers and fixes quickly.

Rather than onboarding everything at once, the provider began with very specific use cases and expanded from there. The next step is extending Mondoo into more workflows across the business, particularly software development, infrastructure as code, and platform engineering.

WHAT THE TEAM WOULD TELL A PEER

- Begin with specific use cases and expand from there. The same approach works for internal buy-in.
- Get into every part of how the platform works and how its capabilities fit together.
- Tools do not replace understanding. Know what runs where, remain technically capable, and keep your skills up to date.
- Speed matters at every checkpoint. Look for comprehensive data, context around findings, and fast scanning.

Asked whether a peer should consider Mondoo, the answer was simple: **yes.**

06

THE TAKEAWAY

 mondoo.com

 [email](#)

 [linkedin](#)

ALERTS CANNOT BE TRIAGED BLIND. THEY HAVE TO COME WITH CONTEXT.

The honest reading of the results matters as much as the headline. Mondoo is not yet everywhere in the provider's estate. Adoption started in pockets, and the gains are clearest where it is already in use: audit evidence comes from current technical results rather than manual server logins, and template security is checked at build time rather than reconstructed at audit time.

Remediation is not yet a before-and-after comparison. Mean time to remediate currently sits at 7 to 10 days, and there is no reliable pre-Mondoo baseline to measure it against. That figure is a benchmark to improve on as adoption widens, not a claim of improvement.

The outcome the team values most is not a number at all. It is speed: getting from an idea, or a discovered problem, to a result as quickly as possible. In an Agile organization that iterates fast, every security gate is necessary, and every one slows things down. A tool that shortens those junctures without removing them is the one that earns its place.

“Anything that can help speed up those specific junctures is a massive plus.”

ENGINEERING LEADER, DEVOPS AND AUTOMATION

THE FINDINGS GOT CONTEXT.
THE AUDITS GOT SHORTER.
THE FIXES CAME READY.