

Managed Vulnerability Service



Bolster your security with expert-led vulnerability management

Is your organization struggling to get a handle on the many hundreds of security vulnerabilities in your environment? You're not alone. Most security and IT teams are overwhelmed by the sheer volume of vulnerability alerts. Even after prioritization, there are still so many critical issues that it's increasingly complex to know which ones to address first. This often leads to dangerous situations where critical vulnerabilities aren't fixed in a timely manner or at all, leaving organizations non-compliant and exposed to attacks and potential breaches.

From insights to action

To assist already overburdened security and IT teams and ensure they're focused on remediating the issues that pose the greatest risk to the business, Mondoo provides a managed vulnerability service that advances organizations from just detecting vulnerabilities to actually remediating them - ensuring that dangerous security weaknesses are addressed before they are exploited.

BENEFITS:

- ✓ Reduce # of vulnerabilities in your environment
- ✓ Accelerate Mean Time to Remediation (MTTR)
- ✓ Improve your security posture
- ✓ Ensure continuous compliance
- ✓ Free up IT and security teams
- ✓ More time for strategic initiatives

How it works

Mondoo experts act as an extension of your security and IT teams, taking the legwork out of vulnerability monitoring, prioritization, remediation, and reporting. By suggesting fixes that can easily be applied by your IT team, you can ensure that critical vulnerabilities and policy violations in your environment are addressed as fast as possible.



1 ONBOARDING & CUSTOMIZATION

Mondoo experts help your team set up and roll out the Mondoo platform in your environment, using your preferred deployment model. Once the connectors are in place, the platform will begin continuous asset discovery across your entire IT infrastructure (cloud, on-prem, endpoints, SaaS, network devices, and SDLC). Mondoo will then assist your team in scoping priorities to align with your business goals and risk appetite.

2 PRIORITY ISSUES

Our experts will triage alerts using Mondoo data queries to validate whether vulnerabilities actually pose a true risk in the environment. Dangerous zero-days, actively exploited CVEs, and other critical vulnerabilities reported by CISA or BSI will be triaged with extra urgency. Using a formal exceptions management process, Mondoo will adhere to your preferences for excluding certain assets or findings from remediation.

3 SUGGEST FIXES

Next, Mondoo experts use the platform to create tickets in your IT Service Management system, including details on the affected assets, reason for prioritization, as well as suggested remediation steps, code snippets (e.g., Ansible, PowerShell, InTune), and pull requests. If no fix is available, we'll suggest tailored mitigation instructions.

4 APPLY FIXES

Your IT team will review the suggested fixes and then apply them by either copying and pasting code snippets, or approving Mondoo-created pull requests in your Git-based Version Control System, such as GitHub. Your IT team remains responsible for the actual remediation, ensuring you retain 100% control over your environment.

5 VERIFY FIXES

Mondoo will rescan the environment to verify that the issue has been remediated. When verified, the ticket will automatically be closed. If drift occurs, the ticket will be reopened.

6 TRACK & REPORT

Mondoo will provide reports on KPIs and security posture, including # issues resolved, # open tickets, MTTR objectives, EOL horizon, patch status, integration health, certificate expiration, asset coverage, compliance status, and other agreed metrics.

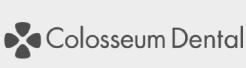
SERVICE INCLUDES:

- ✓ Weekly standups
- ✓ Customer Success Engineer
- ✓ Full access to Mondoo platform
- ✓ Monthly executive reports
- ✓ Bi-weekly system reports
- ✓ Custom dashboard
- ✓ Quarterly Business Reviews
- ✓ Trending CVE Escalation

About the Mondoo experts

Our experts are highly skilled professionals with extensive experience developing strategies that strengthen cybersecurity posture. Their experience includes years of hands-on work in areas like risk assessment, vulnerability management, IT ops, and incident response, along with deep knowledge of operating systems, networks, cloud environments, and compliance frameworks.

Trusted by companies around the globe



Want to learn more?

Schedule a talk with one of our experts.

mondoo.com/contact

FOLLOW US ON

