SOLUTION BRIEF

mondoo

AIX and IBM Power Systems:

Fixing the Security Gap

General-purpose tools and manual processes are not enough

Many organizations, particularly in finance, healthcare, automotive, and manufacturing, rely on IBM Power Systems and AIX for their mission-critical enterprise applications, such as databases and SAP applications. In general, these comprise business-critical workloads with strict uptime requirements. This means that securing them is extremely important. However, securing AIX systems presents unique security challenges:

- They need to meet strict regulatory requirements such as PCI-DSS, HIPAA, SOC 2, CMMC, ISO 27001, NIS2, and DORA
- Long-running IBM Power Systems and AIX instances often contain established configurations that are prone to vulnerabilities
- AIX security hardening differs from standard Linux environments and requires specialized skills

Maintaining secure and compliant AIX and IBM Power Systems requires understanding of the nuances and challenges of these types of environments. General-purpose security tools either don't have -any-visibility, or lack the required specialized insights to detect and assess misconfigurations that endanger assets. To fill this gap, teams often have to revert to periodic manual assessments, rather than using a continuous and automated security solution.

Without proper controls, these assets tend to experience security configuration drift over time, especially in complex environments with multiple administrators. Given the importance of these systems, it's essential to close these security gaps.

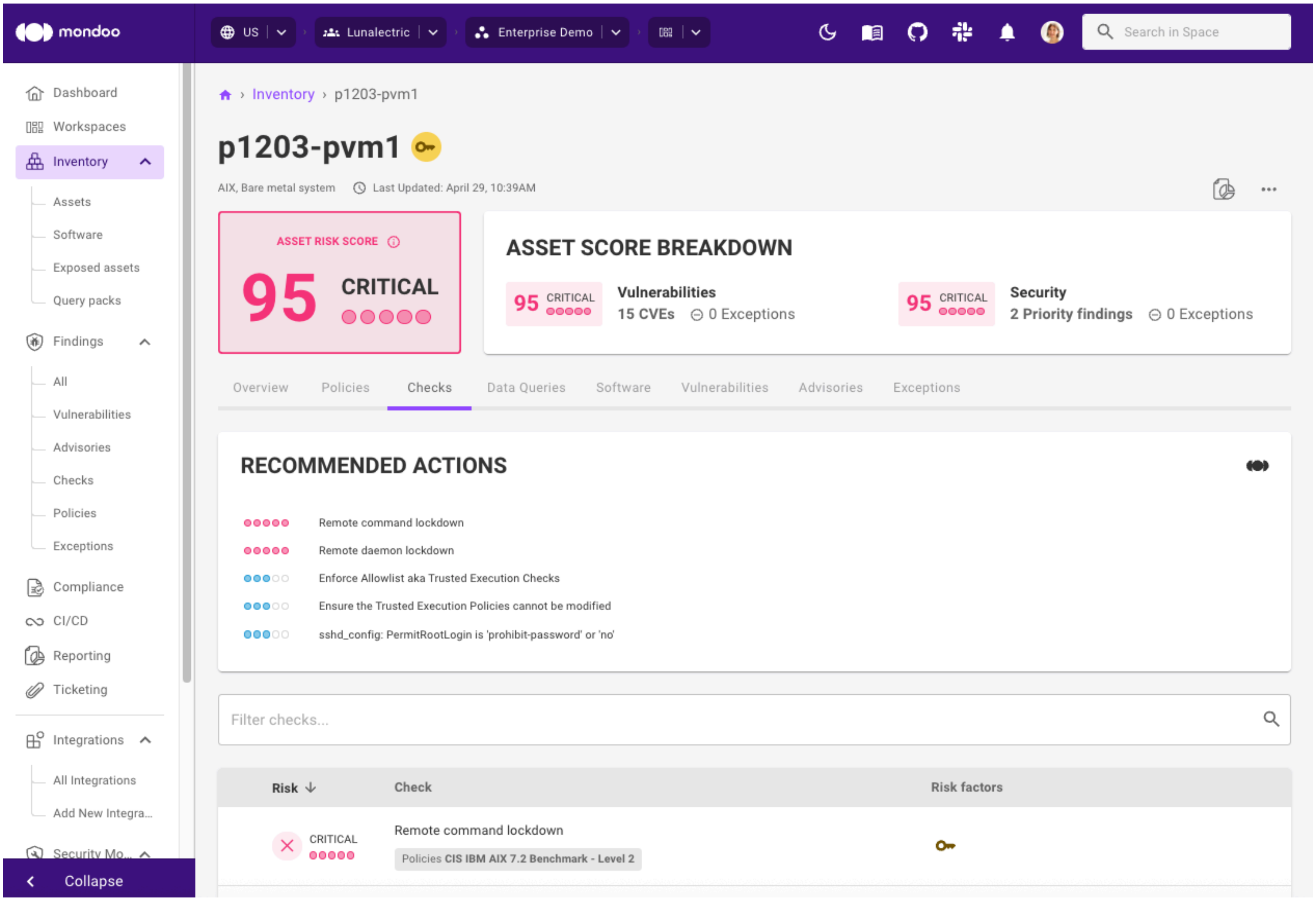
Recently two critical IBM AIX vulnerabilities – CVE-2024-56346 (CVSS 10) and CVE-2024-56347 (CVSS 9.6)—were identified, allowing unauthenticated remote code execution (RCE). Since these flaws could lead to full system compromise they posed a major risk to AIX environments. This left security teams scrambling to find and fix these vulnerabilities, significantly hampered by their lack of visibility and automated security. Mondoo helped several organizations quickly find and fix these vulnerabilities.

Mondoo: Purpose-built for IBM Power Systems and AIX

The Mondoo Actionable Exposure Management Platform is uniquely built to address the specific IBM Power Systems and AIX security requirements by providing:

Full Visibility with IBM and AIX Collectors

Comprehensive visibility is the foundation of any robust security discipline. Mondoo utilizes various collectors (Cloud, SaaS, K8s, Windows, Linux, macOS, Ansible, Terraform), including an IBM Power System and AIX-specific agentless scanner, to provide complete visibility into your environment. This collector deeply integrates with your existing IBM Power Systems and AIX security framework, allowing Mondoo to scan logical partitions (LPARs) and virtualized environments, discovering all IBM Power System and AIX-specific services, filesystems, vulnerabilities and security configurations.



RECOMMENDED ACTIONS

- Remote command lockdown
- Remote daemon lockdown
- Enforce Allowlist aka Trusted Execution Checks
- Ensure the Trusted Execution Policies cannot be modified
- sshd_config: PermitRootLogin is 'prohibit-password' or 'no'

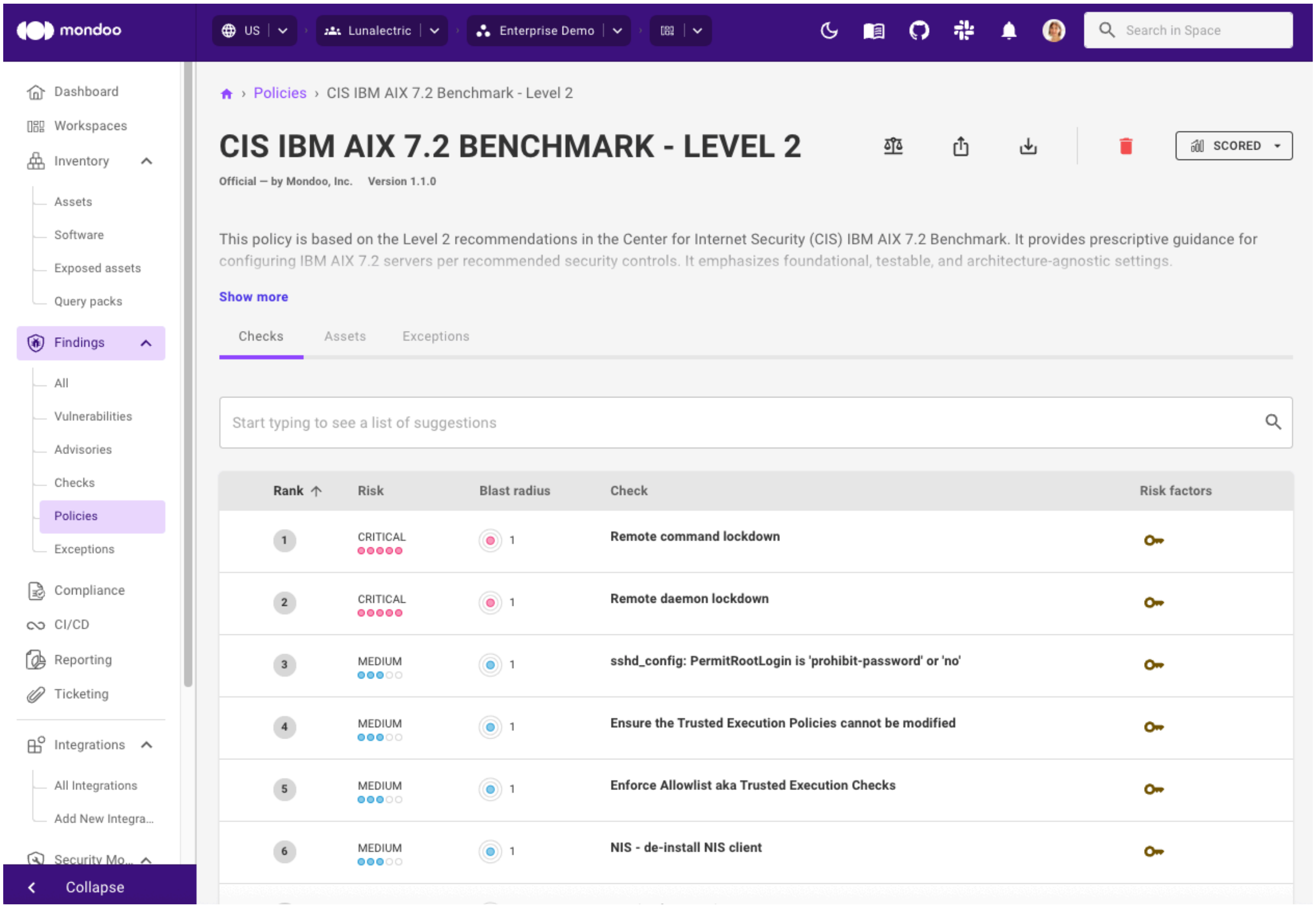
Risk ↓	Check	Risk factors
CRITICAL	Remote command lockdown Policies CIS IBM AIX 7.2 Benchmark - Level 2	

Mondoo highlights security risks on an AIX system

Continuous compliance checks

Mondoo continuously performs checks to ensure that AIX and IBM Power Systems comply with relevant regulatory frameworks (e.g. PCI-DSS, HIPAA, SOC 2, CMMC, ISO 27001, NIS2, DORA) and CIS benchmarks, including IBM Power Systems and AIX-specific CIS benchmarks. This includes checks such as:

- Verification of appropriate service hardening
- Detection of unnecessary services and ports
- Comprehensive configuration drift monitoring



CIS IBM AIX 7.2 BENCHMARK - LEVEL 2

Official — by Mondoo, Inc.   Version 1.1.0

This policy is based on the Level 2 recommendations in the Center for Internet Security (CIS) IBM AIX 7.2 Benchmark. It provides prescriptive guidance for configuring IBM AIX 7.2 servers per recommended security controls. It emphasizes foundational, testable, and architecture-agnostic settings.

Rank ↑	Risk	Blast radius	Check	Risk factors
1	CRITICAL ●●●●●	1	Remote command lockdown	🔑
2	CRITICAL ●●●●●	1	Remote daemon lockdown	🔑
3	MEDIUM ●●●○○	1	sshd_config: PermitRootLogin is 'prohibit-password' or 'no'	🔑
4	MEDIUM ●●●○○	1	Ensure the Trusted Execution Policies cannot be modified	🔑
5	MEDIUM ●●●○○	1	Enforce Allowlist aka Trusted Execution Checks	🔑
6	MEDIUM ●●●○○	1	NIS - de-install NIS client	🔑

Mondoo performs continuous security checks, including IBM- and AIX-specific CIS controls

Validating data protection settings

Mondoo checks for misconfigurations within your Data Protection settings:

- Is your data encryption policy implemented correctly?
- Is your backup and recovery process soundly implemented?
- Is there exposure risk of sensitive data?

Ensuring user account security

Mondoo evaluates and assesses user accounts in IBM Power Systems and AIX environments to ensure they meet security requirements:

- Evaluation of user account security policies and dormant or unauthorized accounts
- Assessment of password policies and implementations
- Detection of shared or service accounts without proper controls

Ensuring correct system logging and permissions

Mondoo validates your privilege management, file system permissions, and network access controls.
It verifies:

- Completion of audit configuration
- Assesses your log retention policy and integrity controls
- Identifies logging gaps or possible blind spots

Providing guided remediation

Mondoo enables immediate action on identified vulnerabilities and misconfigurations through:

- Automated ticket creation in your existing ITSM system (e.g. Jira, ServiceNow, GitLab, GitHub) with all the necessary context
- Detailed, step-by-step remediation guidance for each vulnerability and misconfiguration, ensuring your team has clear instructions
- Prioritized remediation recommendations based on risk severity and potential impact
- Integration with your existing IBM Power System and AIX system management workflow for streamlined resolution

Integrating IBM and AIX security into your CI/CD pipeline

Mondoo helps establish sustainable security through:

- Automated pull request generation for your Ansible playbooks, incorporating the required security fixes
- Integration with your CI/CD pipeline to ensure security configurations are maintained with each deployment
- Continuous validation that ensures fixes remain implemented over time
- Templates and Policy as Code (PaC) that can be applied across your entire IBM Power Systems and AIX estate

Easy deployment

Mondoo uses an IBM Power System and AIX-specific agentless scanner to effortlessly connect to your environments without requiring any agent installation.

Conclusion

Using comprehensive insight and built-in policies aligned with IBM Power System and AIX security best practices, Mondoo assesses every aspect of your environment, detecting misconfigurations and IBM Power Systems as well as AIX-specific vulnerabilities. Mondoo not only ensures that your critical IBM Power Systems and AIX environments are secure, but also that they stay secure through automated, repeatable processes.

> **Mondoo helped us tremendously to quickly find and fix the recent critical vulnerabilities on our customers' IBM Power Systems and AIX systems.**
> *Rainer Rogoll, Senior Consultant IBM Power Systems at SVA System Vertrieb Alexander GmbH*
>
> **Mondoo played a pivotal role in swiftly identifying and remediating critical AIX vulnerabilities that had gone undetected by our other security tools. With Mondoo's guided remediation, we significantly reduced our exposure window and now benefit from continuous assurance that our mission-critical AIX assets remain secure.**
> *Jens Polifka, Deputy Head of IT of a German Tour Operator*

About the Mondoo Platform

Mondoo identifies, prioritizes, and addresses vulnerabilities and misconfigurations in your entire IT infrastructure and SDLC from a single interface—covering on-prem, cloud, SaaS, and endpoints. Unlike siloed approaches that require you to continually switch consoles, Mondoo unifies findings in a single platform, surfacing the most critical risks across your entire environment so you can effectively optimize security efforts.

But Mondoo doesn't just detect vulnerabilities and misconfigurations and then leave you on your own. Instead, Mondoo:

- Tells you what to tackle first for the biggest impact
- Explains exactly how to do it
- Generates and tracks tickets to ensure completion

By making the process of risk detection and resolution as easy and automated as possible, Mondoo reduces manual work, customizes to fit your business needs, optimizes efforts, and accelerates mean time to resolution (MTTR).

1
2
3
DISCOVER
SCOPE
PRIORITIZE
ACT
REPORT

Want to learn more?

Schedule a demo with one of our experts:

mondoo.com/contact

FOLLOW US ON