CVE INTEGRATION IN AI MAASTIK

🛡️ Security Intelligence Built Into Network Operations

EVERY DEVICE KNOWS ITS RISK

The moment a device is added, AI Maastik automatically maps:

- ✓ Model
- ✓ OS
- ✓ Version

…against known CVEs.

No manual lookup. No guessing.

CRITICAL THREAT VISIBILITY

🚨 **High-Risk CVEs? Instantly Flagged.**

Critical and high-severity vulnerabilities are automatically highlighted, giving users immediate visibility into security risks before issues escalate.

SECURITY STARTS AT ONBOARDING

🔍 **Security Check Starts on Day One.**

AI Maastik integrates directly with the CVE database to assess device security the moment it joins your network.

Onboarding = Risk Evaluation.

VULNERABILITIES IN TROUBLESHOOTING

Troubleshooting with Security Context.

While diagnosing issues, Al Maastik considers known vulnerabilities as part of its analysis.

Because sometimes the problem isn't config — it's exposure.

REAL-TIME RISK WARNINGS

⚠️ **Action Might Trigger a CVE Risk? You'll Know.**

Users are warned if an issue or action could be linked to an unpatched vulnerability, helping prevent risky decisions.

RISK-AWARE RECOMMENDATIONS

📊 Advice Based on Device Risk Posture.

Troubleshooting recommendations are adjusted based on the device’s security profile — smarter fixes, safer outcomes.

PROACTIVE PROTECTION WITH AI MAASTIK

🔐 AI Maastik Doesn’t Just Manage Networks

It Understands Their Security

From onboarding to troubleshooting, CVE intelligence is always active.

👉 Move from reactive fixes to proactive protection with AI Maastik.