Astelia adds network-level blocking of attack paths for unpatched vulnerabilities



Astelia has launched autonomous network mitigation, which blocks attack paths to reachable vulnerabilities through WAF or IPS/IDS rules, whether or not a patch exists. Actions are policy-bound, reversible and logged.

- The capability blocks the network path to a vulnerable system instead of changing the system itself.
- It relies on reachability analysis that maps real network topology and the conditions each exploit requires.
- In one enterprise deployment, about 40 million vulnerabilities narrowed to fewer than 2,000 reachable ones.
- Initial support covers WAF and IPS/IDS rules; firewall rules are planned.
- Mitigations are reversible, logged and auditable, and human approval can be required for chosen

> environments or actions.

Astelia has announced autonomous network mitigation, a feature aimed at the gap between the speed of AI-driven exploitation and the pace of patching. Rather than altering a vulnerable system, it blocks the route an attacker would use to reach it.

How it works

Astelia maps the organization's actual network topology and uses agentic AI to work out what each exploit requires. Correlating the two shows which vulnerabilities are reachable and by which paths. In one enterprise deployment, roughly 40 million vulnerabilities came down to fewer than 2,000 reachable ones.

For each reachable vulnerability, the tool identifies an effective choke point on the path and applies a rule there through the organization's WAF or IPS/IDS. One rule can protect every vulnerable server behind that point. Firewall rules are planned but not yet supported.

Controls and limits

The vendor says nothing changes on the protected asset, so business-critical systems, including OT, stay online, and the approach works even where no patch exists, such as end-of-life systems. Mitigations can be rolled back.

Organizations define the guardrails through Astelia Agents. They can require human approval for particular environments or actions, every action is logged and auditable, and mitigation uses scoped permissions that the organization enables. Analysis itself runs on read-only integrations.

The claims come from the vendor's announcement, so teams should validate them in their own environment. The model suits institutions that cannot patch quickly because of change windows, vendor delays or legacy platforms.

What to do now

1. Inventory systems that cannot be patched quickly, including end-of-life and OT assets, and record the compensating controls each has.
2. Check whether your WAF and IPS/IDS can take rules from an external tool, and who approves them under your change process.
3. If piloting any such tool, require rollback, full action logging and least-privilege permissions, and keep human approval for critical environments.
4. Prioritize vulnerabilities by network reachability as well as severity score, and validate the results against your own topology.
5. Align any temporary network mitigation with your ECC and SAMA CSF vulnerability and change

management procedures, with an owner and a review date.