



## Exposure Management Validated by Your Network

### The Exposure Challenge

Organizations face a surge in new vulnerabilities as exploitation windows shrink. Security teams are forced to triage thousands of findings labeled as critical, despite limited insight into whether those vulnerabilities can be exploited in their environment.

Most exposure management approaches rely on severity scores and external threat signals but lack accurate network and enforcement context. As a result, teams spend time researching and patching issues that pose theoretical risk, while real, actionable security risks are overlooked.

### Solution Benefits

- **Focus on real risk** by identifying the 1–2% of vulnerabilities that are truly reachable and exploitable in your environment
- **Save time and costs** for both security and IT teams by eliminating false-positive vulnerabilities
- **Gain full visibility** into reachability and exploitability for every scanned vulnerability
- **Remediate faster** with guidance that goes beyond patching to firewall rule updates and other compensating controls

### Joint Solution: Check Point and Astelia

Check Point and Astelia shift exposure management from score-based prioritization to evidence-based decisions. The joint solution determines which vulnerabilities are truly exploitable by analyzing real network reachability, firewall enforcement, and exploit prerequisites together.

Astelia evaluates each vulnerability against your real network topology and controls. Check Point Firewalls and Check Point Multi-Domain Security Management software show how traffic is allowed, restricted, or segmented across domains. This combined view replaces assumptions with evidence-based exposure analysis.

## Why It Matters

By focusing on vulnerabilities that are both reachable and exploitable, you cut remediation volume without raising risk. Security and infrastructure teams gain a shared, defensible understanding of what must be fixed now, what can wait, and what is already mitigated by existing controls.

## Integration Overview

Astelia connects to Check Point Firewalls and Check Point Multi-Domain Security Management using read-only APIs. Firewall rules, NAT configurations, and domain policies are ingested to build an accurate model of effective network reachability.

Each CVE is then evaluated by Astelia’s agentic AI engine, which assesses technical exploit conditions and maps them against real traffic paths and enforcement points. Vulnerabilities that cannot be reached or exploited under current policy are deprioritized, while those that present genuine exposure are clearly surfaced.

For exposed vulnerabilities, Astelia provides remediation guidance that may include patching, firewall rule adjustments, or other compensating controls aligned with Check Point enforcement capabilities.

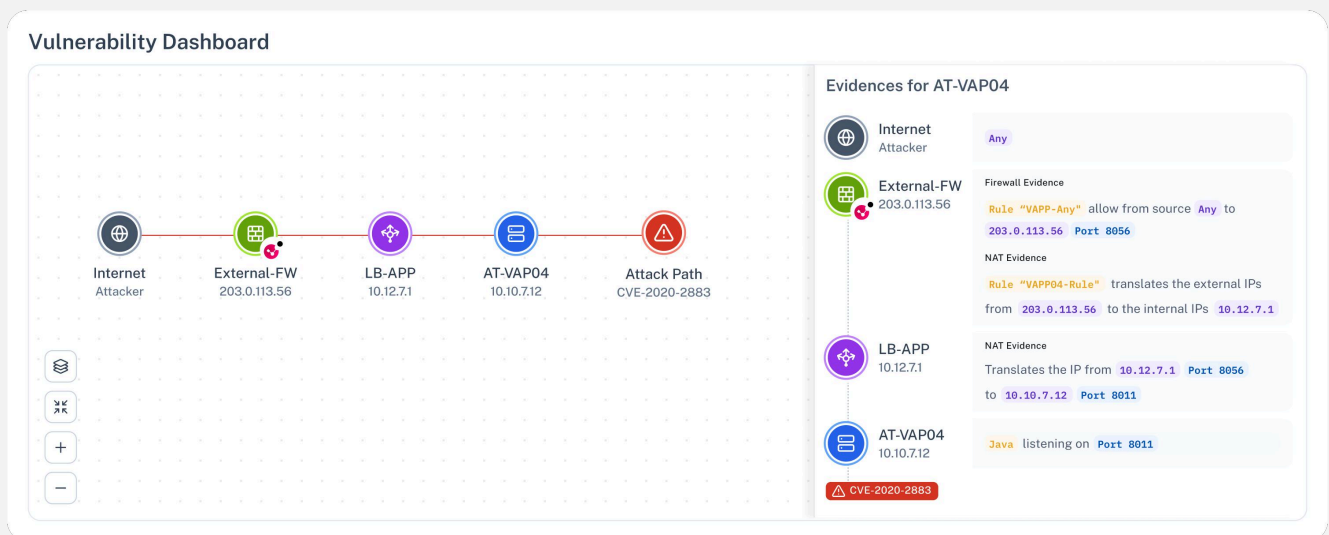


Figure 1: CVE reachability and exploitability analysis based on Astelia and Check Point

## Remediation Impact

The joint solution enables security teams to move faster without increasing operational risk. Instead of generating large volumes of tickets, teams can focus on a manageable set of high-impact issues supported by concrete evidence. Network and firewall teams receive precise, contextual requests rather than broad remediation demands.

This approach shortens remediation cycles, improves confidence in risk decisions, and supports measurable exposure reduction even in complex, multi-domain environments.

## About Check Point

[Check Point Software Technologies Ltd.](#) is a global cyber security leader protecting more than 100,000 organizations worldwide. Its mission is to secure enterprises' AI transformation. With a prevention-first approach and an open ecosystem architecture, Check Point helps organizations block advanced threats, prioritize exposures, and automate security operations across complex digital environments. The unified architecture simplifies protection across hybrid networks, multi-cloud environments, digital workspaces, and AI systems. Structured around four strategic pillars, Hybrid Mesh Network Security, Workspace Security, Exposure Management, and AI Security, Check Point delivers consistent protection and visibility across multivendor environments, enabling organizations to reduce risk, improve efficiency, and accelerate innovation without increasing complexity.

## About Astelia

Astelia is a cybersecurity company founded by former leaders of the Israeli National Red Team, combining deep offensive and defensive expertise with firsthand understanding of how vulnerabilities are actually exploited. Using proof-based reachability analysis, Astelia enables organizations to identify the critical 1-2% of reachable vulnerabilities in their environment and choose from multiple remediation paths.

[LEARN MORE](#)